Intrusion Detection & Vulnerability Assessment

Group Test (Edition 1)

An NSS Group Report

First published December 2000 (V1.0)

Published by The NSS Group
Oakwood House, Wennington, Cambridgeshire, PE28 2LX, England

Tel : +44 (0)1487 773307
Fax : +44 (0)1487 773268
E-mail : info@NSS.co.uk
Internet : http://www.NSS.co.uk

TABLE OF CONTENTS

TABLE OF FIGURES

The NSS Group

The NSS Group is Europe's foremost independent network testing facility and consultancy organisation.

Based in Cambridgeshire, England, and with an advanced "super lab" and conference centre in the South of France, The NSS Group offers a range of specialist IT, networking and security-related services to vendors and end-user organisations throughout Europe and the United States.

The Group consists of three wholly-owned subsidiaries :

- *NSS Network Testing Laboratories*
- *Network Security Services*
- *NSS Consultancy Services*

NSS Network Testing Laboratories are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

NSS Network Testing Laboratories also operates certification schemes for vendors and certification bodies, and currently provides certification of firewalls, VPN's, crypto products and PKI products.

Output from the labs, including detailed research reports, articles and white papers on the latest network-related technologies, are made available free of charge on our web site at http://www.nss.co.uk

The conference centre in Moux in the south of France is the ideal location for sales training, general seminars and product launches, and NSS can also provide technical writing services for sales, marketing and technical documentation.

Network Security Services provides a range of security-related services to vendors and end-users including security policy definition, firewall and VPN implementation, network security auditing and analysis, and penetration testing.

NSS Consultancy Services offers a range of network consultancy services including network design, strategy planning, directory design and Internet connectivity

Foreword

A note on terminology.

There has been much indignant letter writing in the computer press recently over the distinction – or increasing lack thereof – between the terms *hacker* and *cracker*. In theory, a hacker is a benign coder whose interest lies only in hacking code (as in *producing* or *playing with*, rather than *compromising*) and not attacking other people's systems. The person who launches the Denial of Service attacks against your network or tries to penetrate your firewall - he (or she) is known as a cracker.

I accept and agree with the distinction in principle, but feel that to the vast majority the word *hacker* is the one that is associated with the bad guy and the attack he launches is a *hack*. Perhaps the word *crack* as an alternative has too many other, even less salubrious, connotations? Whatever the reason, since most people identify with the word hacker more readily, this is the term I shall use throughout this report to indicate the "bad guy", and I do not expect to receive any irate e-mails about it, if it's all the same to you.

Years ago, the phrase "*gay bachelor*" meant something completely different to what it does today! And there is nothing you can do to reverse this process. Some words and phrases are simply hijacked by the proletariat, and *hacker* is one of them.

Get over it.….

Bob Walder

INTRODUCTION

Whenever a company connects its network to the Internet, it opens up a whole can of worms regarding security. As the network grows, it will play host to numerous bugs and security loop holes of which you have never heard - but you can bet intruders have.

Many organisations are recognising the value of a good security policy to define what is and is not allowed in terms of network and Internet access Then they deploy a number of tools to enforce that security policy – usually in the form of a firewall or two.

Firewalls may be billed as commodity items, but the “shrink wrap” element certainly doesn’t extend to their configuration. A detailed knowledge of what a hacker can do and what should and shouldn’t be allowed through the firewall is required before embarking on the configuration adventure, and a slip of the mouse is all it takes to open up a hole big enough for your average hacker to drive the proverbial bus through. The problem is, a badly configured firewall can be worse than no firewall at all, since it will engender a false sense of security.

To protect an organisation completely, therefore, it is necessary to audit the network on a regular basis, and in order to achieve this, a whole new category of software has emerged in the last couple of years: ***Intrusion Detection Systems (IDS).***

When it comes to computer and network security, there are a number of analogies that can be drawn with the “real world”. Such analogies are particularly useful for answering such questions as “*I already have a firewall, why do I need Intrusion Detection Systems as well?*”.

Depending on how you approach the security of your home, for example, you may opt for high quality locks on your doors and windows. That will help to keep intruders out, and could be thought of as the equivalent of the firewall – perimeter defences. It’s nice to feel secure, but the determined burglar can often find ways around these measures. He can always throw a brick through your back window, for instance, and get in that way – or perhaps you simply forget to lock your door one day.

Once he is inside your home he is free to wreak havoc, perhaps making it obvious he has been there by stealing or wrecking things, or perhaps simply taking copies of any keys he finds so he can come and go later at his leisure. Whatever happens, you don’t want your first knowledge of the break-in to be when you return home to the ransacked contents.

That is why many people install a burglar alarm as well. Should the intruder gain access through the perimeter defences, the burglar alarm alerts you or your neighbours to the break in immediately, and provides an additional deterrent to the would-be thieves.

IDS, therefore, are the equivalent of the burglar alarm. To be used alongside firewalls, they are a recognition of the fact that you can never have a 100 per cent secure system. However, should someone be clever enough to breach your perimeter defences, you want to know about it as soon as possible. It would also be nice to know what they have been up to while they were inside too.

The final part of the analogy is the vulnerability scanner, which is the equivalent of your local crime prevention officer, testing your security and advising you of any potential weaknesses.

Intrusion Detection and Vulnerability Assessment are becoming increasingly important as the stakes become higher. In the 1980s and early 1990s, denial-of-service (DoS) attacks were infrequent and not considered serious. Today, successful DoS attacks can shut down e-commerce-based organisations like online stockbrokers and retail sites.

Within the IDS market place there are four broad categories of product:

Vulnerability Assessment Scanners (VA)

Also known as “risk assessment products”, these take two forms.

The first is a “*passive*” or “*host*” scanner, which usually allows the network administrator to define a security policy for the machines on his network (perhaps a different policy for each operating system or type of server). The scanner then audits every machine automatically, producing a report that details exactly where each machines security settings differ from the defined policy and what needs to be done to fix the problem.

The second type of VA scanner takes quite a proactive stance – a sort of “hacker in a box” – providing a number of known attacks (Web server exploits, Denial of Service attacks, and so on) with which a network administrator can probe his or her network resources. By probing a network with an “*active*” or “*network*” scanner, the network administrator can often obtain a clear picture of potential weaknesses in his system, and even an indication as to how those weaknesses can be eliminated.

Some of these systems will make multiple passes of a network, using information gleaned on early passes to effect a more comprehensive attack in subsequent attempts. For example, a scanner may find an unprotected password file on a desktop machine in one pass. In the next pass it could actually use those passwords on the same – and other – hosts in an attempt to gain access to protected resources as an administrator. You would be surprised how often this works!

Host IDS (HIDS)

These employ an agent that resides on each host to be monitored. The agent scrutinises event logs, critical system files and other auditable resources looking for unauthorised changes or suspicious patterns of activity. Whenever anything out of the ordinary is noticed, alerts or SNMP traps are raised automatically.

For instance, they will monitor attempted logins and take note of when an attempt is made to access an account with an incorrect password. If the attempt fails too many times within a short time span the system may conclude that someone is trying to gain access illegally and an alarm can be raised.

Another thing they can do is monitor the state of system and application files, or the Windows Registry. They do this by making an initial pass of a clean system and storing a condensed “snapshot” of how that system should look.

If an intruder – or some sort of Trojan Horse - does manage to gain access to the system and make changes, the IDS will spot this (maybe not in real time) and raise an alert. There are systems on the market that specialise in this type of operation, and they tend to be referred to as *File Integrity Assessment* (FIA) products. Host-based systems tend to be *reactive* rather than *proactive* – that is they often have to wait until something has actually happened before they can raise the alarm.

Network IDS (NIDS)

These monitor traffic on the wire in real time, examining packets in detail in order to spot denial of service attacks or dangerous payload before the packets reach their destination and do the damage. They do this by matching one or more packets against a database of known "attack signatures". These databases are updated regularly by the vendors as new attacks are discovered.

When suspicious activity is noticed, a network based scanner is capable of both raising alerts and terminating the offending connection immediately (as are some host-based scanners). Some will also integrate with your firewall, automatically defining new rules to shut out the attacker in future.

Most of the network-based IDS available to date work in what is known as "*promiscuous mode*". This means that they examine every packet on the local segment, whether or not those packets are destined for the IDS machine (much like a network monitor, such as Sniffer). Given that they have a lot of work to do in examining every single packet, they usually require a dedicated host on which to run due to their heavy use of system resources.

For instance, most attacks are not based on the contents of a single packet, but are made up of several, sometimes sent over a lengthy period of time. This means that the IDS has to store a number of packets in an internal buffer in order to compare groups of packets with its attack signature database. This is known as "*maintaining state*", and allows IDS to compare new packets against its signature database in the context of what has happened previously in a particular session, rather than examining every packet in isolation.

You will also need one Network IDS sensor per segment, since they are unable to see across switches or routers, and some have problems keeping up with heavily loaded Fast Ethernet segments (never mind Gigabit).

Network Node IDS (NNIDS)

Recently we have seen a new type of "hybrid" IDS agent appear which overcomes some of the limitations of the network-based IDS.

This new agent works in a similar manner to the network-based IDS in that it takes packets from the wire and compares them against database entries. However, this new "micro agent" is only concerned with packets targeted at the network node on which it resides, thus giving rise to the term *Network Node IDS (NNIDS)*.

Rather confusingly, it is also occasionally referred to as "host-based", but usually only by those who are looking at the industry purely from a Network IDS viewpoint.

As far as we are concerned, Host IDS is to do with monitoring of log files and behavioural analysis, whereas both Network and Network Node IDS are concerned with TCP analysis – the only difference is that one (NIDS) is running in promiscuous mode whilst the other (NNIDS) is not.

The fact that the NNIDS system is no longer expected to examine every single packet on the wire means that it can be much faster and take less system resources, and this allows it to be installed on existing servers without imposing too much overhead. It also makes it particularly suitable for heavily loaded segments, switched network environments, or VPN implementations with encrypted traffic on the wire, all areas where traditional network-based IDS have problems.

Obviously you will now need a number of these NNIDS agents – one for every server you wish to protect – and they will all have to report back to a central console. Most systems may well opt for a combination of the two – NNIDS on individual servers in switched server farms, and traditional NIDS on less heavily used segments, where a single IDS can protect a large number of hosts.

For those with a reasonable security budget, we would recommend purchasing a firewall and at least one product from each of the above categories. The firewall guards your perimeter, whilst the IDS' monitor what is happening on your network, guarding against slip-ups by the firewall as well as internal mischief-makers.

Both host-based and network-based scanners are worth investing in, since they each have their own strengths. Network-based IDS will monitor the wire for suspect packets and are adept at spotting Denial of Service type attacks and unwelcome probes – usually from outside our network. Host-based systems, on the other hand, are watching the "crown jewels" – the actual data on the file servers, monitoring for inappropriate logins or changes to critical files from unauthorised sources.

Although network-based products seem to get most of the publicity at the moment, given that the FBI figures still point to over 70 per cent of hack attacks coming from inside a network, the host-based system can often be more valuable.

Problems With IDS

So, you have been out and bought your shiny new IDS system and installed it somewhere on your network. You are now secure and immune from attack, right? Wrong!

To begin with, deployment of IDS requires careful thought and planning if you are to get the most from it. What kind of resources are you protecting? If you have a DMZ containing only Unix-based Web servers, you could disable all IDS signatures to do with Windows NT or DNS servers. Some IDS products will go so far as to try and perform this step automatically for you depending on what operating systems and services are found during a network scan.

To do the job properly, however, you should acquire some good Vulnerability Assessment tools and scan your own network. This should give you a good starting point in determining which machines need protecting, and from what sort of attacks. Are you worried about intruders breaking through your firewall and launching DoS attacks against your machines?

Then perhaps a Network or Network Node IDS would be a good buy. Or are you more concerned about Trojans on your desktops and file servers? File Integrity Assessment would be the best bet. Or perhaps you are worried about your own users making off with company secrets? In which case, Host IDS would be the right choice. Most likely you will actually need a combination of all these technologies.

Having selected your products, where are you going to install them? Host and Network Node IDS are simple - you put them on the hosts that need protecting. But Network IDS is another matter. Placing a network interface card into promiscuous mode generates an awful lot of material to be processed. All the traffic passing by on the subnet being monitored has to be collected and examined by the IDS sensor and compared against a database of known attack signatures.

Nor is it enough to simply look at this traffic on a packet by packet basis, since some attacks are spread over several packets, or may be fragmented deliberately to confuse the IDS. This necessitates a time- and memory-consuming process of buffering packets and maintaining state tables to keep track of individual sessions. To defeat the common IDS evasion techniques such as packet fragmentation, out-of-order fragments and so on, it is also necessary to perform some heavy-duty processing within the IDS itself to reassemble packets back into the form that will eventually be seen by the target host (or capture the packets at a higher level in the TCP stack of the sensor machine). Both of these options are likely to slow the detection process, but only then can the true packet contents be determined and compared against the signature database.

And all this must be done whilst eliminating – or at least keeping to a minimum – the risk of the "*false positive*". In an ambiguous situation, there is no point in raising an alert "just to be on the safe side", otherwise the IDS runs the risk of crying wolf once too often and eventually being ignored altogether. Quite a bit involved behind the scenes then, and whilst most IDS products could quite happily keep up with traffic on a 10Mbit network, leased-line or DSL connection, it is much more difficult to do all this at wire speed on a 100Mbit network.

Gigabit presents even more problems. Not only are we now looking at a significant increase in bandwidth – and thus a significant increase in the volume of traffic to be analysed – but we have also moved into the realms of the purely switched network. Don't forget that the promiscuous mode sensor can only see traffic on its own segment, and in a switched environment, every connection to the switch is, effectively, a single segment. In the 10Mbps or 100Mbps world, this can be overcome by the use of *network taps* or mirroring all the switch traffic to a *span* port, to which is attached an IDS sensor. But with Gigabit, the result would be a seriously overloaded sensor. Building IDS technology into the switch hardware itself, allowing the sensor to grab traffic directly from the backplane, is one solution. Another is to move to a pure Network Node IDS implementation, where the agents are concerned only with the traffic directed at the host on which they are installed.

Companies that make extensive use of VPN's will also find problems with Network IDS, since the traffic picked from the wire will obviously be encrypted, thus rendering any pattern matching or protocol analysis completely useless.

If it is not acceptable to decrypt data at the network border, then once again the only solution is to install Network Node IDS, so that the IDS agent has access to the data stream as it is decrypted at the VPN end-point.

Going forward, then, Network Node IDS is likely to be the favoured technology in high-speed, switched networks, or networks that carry a lot of encrypted traffic. Does that mean that Network IDS is a redundant technology? Not at all. With careful selection of the appropriate product, NIDS still provides the most cost-effective solution for intrusion detection on unencrypted networks – both switched (using taps or span ports) and shared – up to 100Mbps.

Detection Methods

Of course, not every IDS bases its alerts on pattern matching packet contents against a database of known signatures. Some products approach the problem in a completely different way by doing a full protocol analysis on the data stream. Although this may seem like using a sledgehammer to crack a nut, it does have the advantage of highlighting anomalies in packet contents much more quickly than doing an exhaustive search of a signature database. It also has the advantage of being much more flexible in capturing new variants of old attacks – attacks which would normally require a new signature in the database for the "traditional" IDS architecture, but which would be caught by a complete protocol analysis.

Yet another approach is to forget about trying to identify the attacks directly, and concentrate instead on ignoring everything that is considered "normal". This is known as "*anomaly-based*" – as opposed to "*signature-based*" – IDS, and the basic principle is that, having identified what could be considered "normal" traffic on a network, then anything that falls outside those bounds could be considered an "intrusion" – or at the very least, something worthy of note.

The primary strength of anomaly detection is its ability to recognise previously unseen attacks, since it is no longer concerned with knowing what an attack looks like – merely with knowing what does not constitute normal traffic. Its drawbacks, of course, include the necessity of training the system to separate noise from natural changes in normal network traffic (the installation of a new – perfectly legitimate - application somewhere on the network, for example).

Changes in standard operations may cause false alarms while intrusive activities that appear to be normal may cause missed detections. It is also difficult for these systems to name types of attacks, and this technology has a long way to go before it could be considered ready for "prime time".

The Circle of Strife

Once you have your IDS deployed and working effectively, that is not the time to sit back and relax. In fact it is only the beginning of a cycle that must be constantly repeated if security is to be maintained.

IDS is a valuable component of an organisation's security plan, but it is just that – a component. The first point of defence may well be the firewall, and behind the Network and Network Node IDS system may well be additional port monitoring and File Integrity Assessment products to alert you as to when an intrusion attempt has been successful.

All of these components must operate within the confines of a strict security policy, which should determine what is and is not allowed on the corporate network. This, in turn, will help specify how the individual components are to be deployed and configured, as well as offer guidelines as to how alerts are to be handled. There is no point in using the latest IDS technology only to have it log intrusion attempts to a file that is only examined once a month.

There should be differing levels of importance assigned to different types of intrusion attempts, and the alert and response procedure should be scaled accordingly. There is little point in raising the roof should you discover your network is being port scanned by someone using nmap - that happens all the time, and it is enough to log that for periodic examination just to make sure it is not happening too often within a set time interval.

On the other hand, a successful BackOrifice ping that elicits a reply from somewhere within your organisation indicates a serious compromise, and for that you may deem it appropriate to page the security administrator any time day or night. Between those two extremes are various other possible responses such as e-mail, SNMP alerts, session termination, firewall reconfiguration, and so on – use them to the full, and make sure that your security staff take the time to examine the various log files at regular intervals to keep tabs on the more mundane intrusion attempts.

Intrusion Detection Systems are good at sounding alarms, but unless there is someone around who is prepared – and trained - to respond, it is no better than a car alarm that everyone ignores. An effective response is every bit as important as detecting the attack in the first place.

Maintenance is equally important. Security is certainly not static, and new vulnerabilities are being discovered and exploited all the time. This should result in new signatures for your IDS and VA tools, patches for your operating systems and updates for your firewalls. Even so, it is a wise security administrator that keeps an eye on the various underground hacking sites and security alert mailing lists for himself. Between the point of discovery to the point where a patch is issued and applied, there is a window of opportunity for the hacker to exploit. It is up to the security administrator to minimise this window as much as possible.

If an OS vendor is slow in bringing out a patch for a new vulnerability, for example, perhaps the administrator can reconfigure the corporate firewall to eliminate the sort of traffic that could exploit that vulnerability, or add a temporary custom signature to the IDS in order to detect it. Certainly as soon as new IDS signatures are made available from the vendor, they should be downloaded and deployed to every appropriate sensor on the network.

Finally, you should be using Vulnerability Assessment tools to continually test your defences and update your security policies accordingly. A VA scan may well highlight additions or changes to the network and its applications which might necessitate a rethink on how IDS sensors are deployed and which signatures are monitored by each sensor.

Monitor - evaluate – modify. Then back to the beginning. It is a cycle that must be repeated over and over if you want to keep your network as secure as possible. Only by continual vigilance and refinement will you stay one step ahead of (or at least no more than one step behind) the hackers.

PRODUCT REVIEWS

In this section of the report we move from general IDS/VA information to detailed evaluations of some of the market-leading products.

For this important group test we invited all the major vendors in the IDS/VA market place. Twelve agreed to take part, with some vendors entering multiple products in more than one category:

In total, we tested fifteen products, including:

- **Axent Enterprise Security Manager 5.1**
- **Axent Intruder Alert 3.5**
- **Axent NetProwler 3.51**
- **Axent NetRecon 3.0.9**
- **BindView HackerShield 2.0a**
- **Cisco Secure IDS 2.5 Model 4210 (with netForensics)**
- **Cisco Secure IDS 2.5 Model 4230 (with netForensics)**
- **Computer Associates eTrust Intrusion Detection 1.4.5**
- **CyberSafe Centrax 2.4**
- **ISS RealSecure 5.0**
- **Network Associates CyberCop Scanner 5.5**
- **Network ICE BlackICE Sentry 2.1**
- **Network Security Wizards Dragon Sensor 4.1**
- **Networks Vigilance NV e-secure 2.1**
- **TripWire 2.2.1 (with HQ Connector)**

Vendors will also be encouraged to submit new releases for testing, thus allowing us to update this report at regular intervals and maintain an accurate appraisal of the IDS/VA market place.

We also hope that those vendors who declined to participate in this group test will agree to put products forward for the next one in 2001. This is a relatively immature, yet fast-moving market place, and potential customers need as much information as they can lay their hands on when selecting and deploying such an important part of their security systems.

This report is currently the only source of comprehensive, yet completely independent technical evaluations of the leading products in the IDS/VA arena, and is likely to become ***the*** definitive guide to the market place and a major source of information and advice to security professionals.

PRODUCT REVIEWS – IDS

AXENT INTRUDER ALERT 3.5

Intruder Alert (ITA) is the host-based IDS part of Axent's security suite that also includes network IDS (NetProwler, with which it integrates closely), vulnerability assessment (NetRecon), and security policy auditing and enforcement (Enterprise Security Manager).

Architecture

As with NetProwler, Intruder Alert utilises a multi-tiered distributed management and configuration infrastructure that allows it to scale in the largest network environments.

The ITA architecture is made up of four components:

- **Agent –** This is installed as a Unix daemon, Windows NT Service or NetWare Loadable Module (NLM) and is used to monitor events on the host on which it is installed, and perform defined actions based on applied security policies.
- **Manager –** This is a Unix daemon or Windows NT Service which provides the middle layer of communication between multiple Agents, the Event Viewer and the ITA Administrator. It is used to organise Agents, administer policies and manage the event database.
- **Event Viewer –** This provides a graphical view into the ITA event database, which contains all the events captured by various ITA Agents. The Event Viewer can be used to both query the event database to generate reports and send commands to Agents.
- **Administrator –** This is the graphical console that provides centralised control over the Intruder Alert system, used to organise and configure Agents in Domains, and create and administer security policies.

Intruder Alert is Axent's host-based IDS which complements NetProwler. The two can be configured to integrate closely, and there is now a central management console that lets users monitor both network-and host-based IDS systems enterprise-wide via a multi-tiered distributed architecture.

An SNMP-Collector utility must be installed within Intruder Alert in order for it to respond to NetProwler events. From within Intruder Alert's management interface, administrators can view multiple NetProwler events and hundreds of Intruder Alert agents, enabling them to react to either network- or host-based violations from a single console.

Installation

Installation is straightforward enough for Windows users. For Unix platforms, there are a number of different install programs on the CD depending on the version of Unix – these are to install the Manager and Agents (either can be installed individually, or both can be installed on the same machine). The Event Viewer and Administrator are also available for both Windows and Unix platforms.

Note that none of the components will work under Windows 2000 at the time of writing – the test platform for this evaluation was therefore Windows NT4 Service Pack 6a.

Documentation is excellent, and is provided as hard copy manuals in the box as well as electronically. The Installation Guide provides plenty of information on installing the components of ITA on various platforms, whilst the User Guide provides detailed reference and tutorial material on all aspects of configuring, managing and running ITA.

Configuration

Graphical interfaces are provided for both the ITA **Event Viewer** and the **Administrator**.

The Administrator is used to define and deploy security policies throughout a distributed ITA system, and employs a dual-pane approach – the left containing a hierarchical tree display containing Managers, Agents, Domains and Policies, whilst the right hand pane contains the configuration details of each object selected.

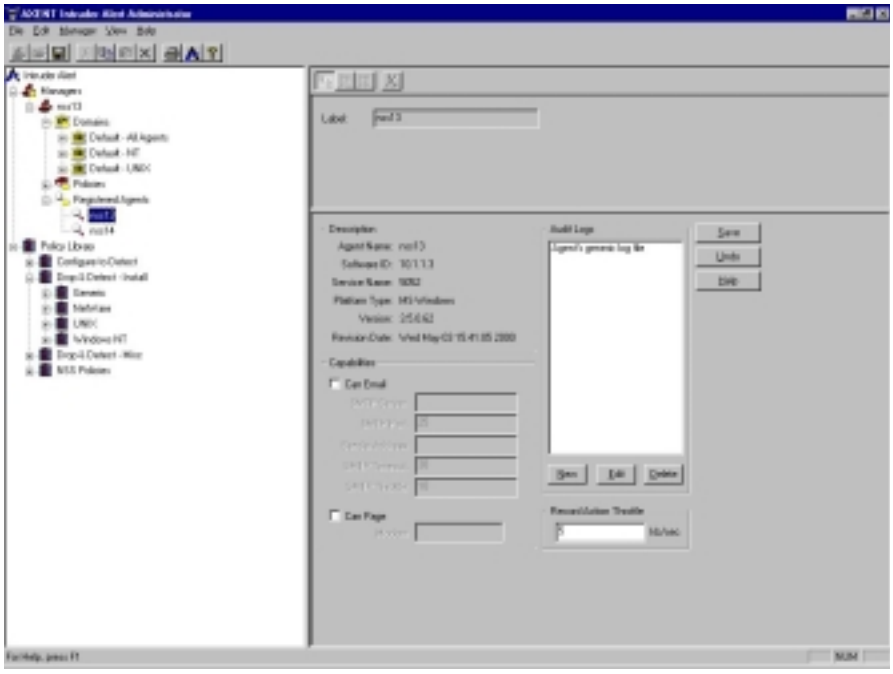

Figure 1 - The Intruder Alert Console

When first launching the Administrator program, it is necessary to connect to a specific Manager by providing a user name and password – all available Managers are listed in the tree view in the left-hand pane. Once connected, the configuration details for that Manager are retrieved and displayed, allowing you to view the Domains, Policies and registered Agents for that Manager. Each Manager is capable of controlling up to 100 Agents. As with NetProwler, it is not immediately apparent what is going on in the Administrator interface – Policies seem to be duplicated far too many times, for example. However, with a bit of thought, it all comes together quite well, and is actually easier to master than the NetProwler interface.

Security Policies are available in the main Policy Library, which serves as the repository for all policies shipped with Intruder Alert as well as any new ones that are developed by the administrator. The library is divided into three sections – Configure To Detect, Drop & Detect (Install) and Drop & Detect (Miscellaneous).

Think about them, and they are self explanatory. Configure To Detect policies require some custom configuration by the administrator before they can be deployed. Drop and Detect, on the other hand, are ready to go as they stand, and those in the "Install" section cover a range of common vulnerabilities on various OS platforms. These are deployed and activated automatically at install time, thus providing instant protection as soon as ITA has been installed.

As an example, intruders will often attempt to replace critical system files with "Trojan Horses", or alter those files to create "back doors" into the host system. ITA is pre-configured to detect changes to mission-critical files on Unix and NT systems via the built-in *File Tampering* Policies, and these Policies are automatically activated during Agent installation. It is quite a simple matter, however, to add your own files to these Policies (or create your own custom Policies based on them) in order for ITA to monitor in-house application and data files.

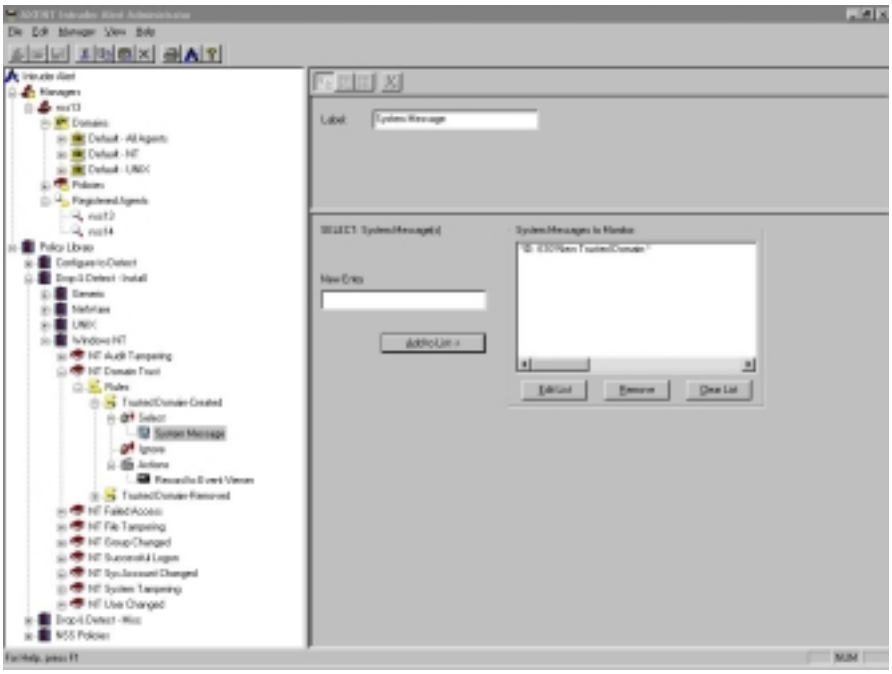

Figure 2 - Creating policies

Intruder Alert has different event sources for each supported operating system. The event sources on Unix include syslog, wtmp, process accounting and, where available, btmp and C2 audit logs. Event sources for NT include System, Application and Security logs, whilst for NetWare the event source stems from a number of event types registered with the NetWare operating system.

Of course, every system is different so, unlike network IDS, host-based systems need to be customised frequently to provide optimum cover for the host on which they reside.

This customisation is not always straightforward, but it has been made as easy as possible with ITA whilst retaining a high degree of flexibility.

Existing Policies can be changed or new Policies can be defined from scratch, and these are made up of a number of rules that detect and respond to events. In turn, these rules are comprised of three parts – a select clause (determining which events are to be included), an ignore clause (to exclude certain events) and an action clause (to perform if the select and ignore clauses yield a positive result). Select clauses can be used to match search strings against ITS Status messages, SNMP traps (including alerts from NetProwler) or events stored in the system logs of whichever OS is installed on the host. So, for instance, you can create a *select* clause that looks for all messages that contain the phrase "*Failed Admin login*".

The *ignore* clause provides power and flexibility, since it is possible to set timers or raise flags in response to a particular *select* clause and subsequently ignore events that have a flag raised or which have occurred within a particular time frame. So, for instance, you could look for all failed login events, but only perform an action if you get more than thirty in a one minute period. This ability to raise flags and perform selective actions based on the state of those flags is known as Event Context Capturing, and provides the ability for ITA to distinguish between different events of the same type, perhaps sorting out five failed administrator logins out of the thirty failed logins that occurred in the last minute.

Finally, the *action* clause provides the means for ITA to act on what it considers to be a positive alert. The following options are available:

- *Record to Event Viewer*
- *Raise/Lower Flag*
- *Send E-mail*
- *Pager*
- *Append to File*
- *Notify (on-screen pop-up)*
- *Start/Cancel Timer*
- *Execute Command*
- *Run Shared Action (chain to another Rule)*
- *Disconnect Session*
- *Disable User*

Any number of rules and clauses can be combined to make a Policy, and rules can even be chained together, subsequent rules depending on the output of preceding ones. This makes Intruder Alert one of the most flexible scanners we have seen to date.

Once a new Policy has been created in the Policy Library, it can be deployed to a particular Manager by simply dragging it from the Library into the Policies branch of the tree view under the appropriate Manager (actually, Policies can be created directly in the Manager section of the tree hierarchy, which may be appropriate in certain circumstances, such as when a Policy will only ever apply to a single Manager). The Manager branch lists previously connected Managers, and the ITA Administrator allows you to connect to multiple Managers at the same time.

Listed under the Manager branch of the configuration tree are the **Policies** (dragged from the Policy Library or created from scratch), **Registered Agents** (listing each of the Agents controlled by a particular Manager), and **Domains** that apply to that Manager.

A Domain is simply a logical grouping of machines on your network and ITA creates default ones according to platform – NT, NetWare, Unix and All Agents. It is a simple matter to rearrange these or to create your own – perhaps by department (finance, sales, etc.) or server function (FTP, Web, mail, etc) – depending on how you have designed your policies. Hosts can belong to more than one domain if required.

Once a Policy has been placed in the Policy folder of a particular Manager, it can be quickly deployed to every Agent in one or more Domains by right clicking on the Policy and selecting the Domains to which you want to deploy it. Once a Policy has been applied to a Domain, it is automatically deployed to all the Agents within that Domain and monitoring begins immediately.

At any point, it is a simple matter to expand the tree hierarchy and see which Agents are in which Domains, and which Policies apply to which Domains. The *Shared Actions* Policy provides a number of Actions which can be used from within any Policy on the system, allowing all actions to be administered from a central location. For instance, there will probably be only one way to e-mail the administrator, so it only needs defining once in the *Shared Actions* Policy, and can be re-used over and over from any other Policy.

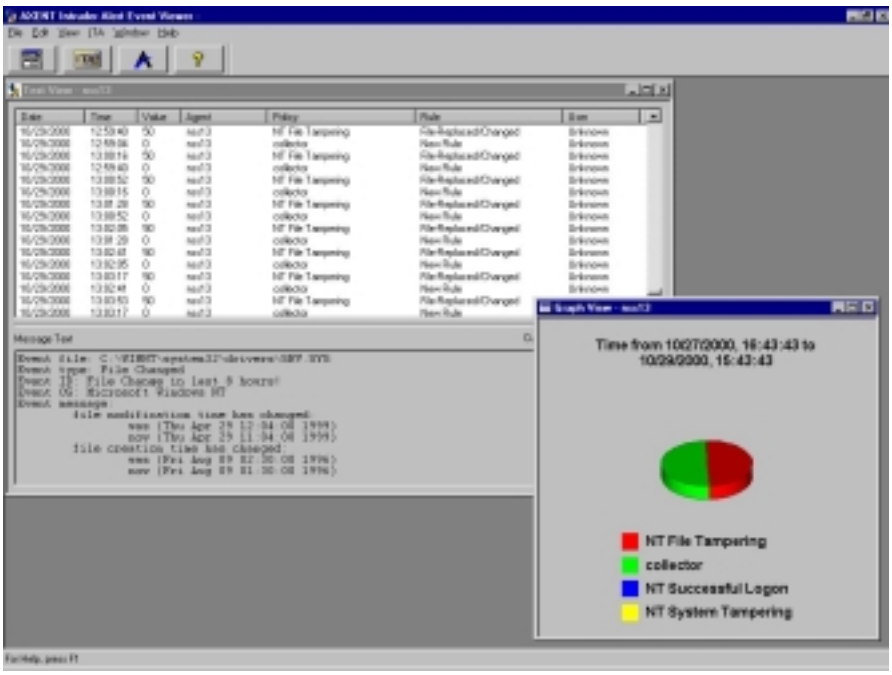

Figure 3 - The ITA Event Viewer

Bandwidth is always an issue in a distributed hierarchy such as that employed by ITA, where multiple Agents have to communicate with Managers, and Managers have to communicate with central consoles. However, ITA provides the means to throttle back traffic generated as a result of Agents recording events to the Manager database, and Agents sending e-mail alerts.

Reporting and Analysis

Two vehicles for reporting and analysis are provided in Intruder Alert: the **Event Viewer** and the **Report Generator**.

Event Viewer

Intruder Alert Event Viewer is a separate graphical utility (on Unix and Windows platforms) that is used to query and view event data captured by Agents. Event Viewer gathers its data from events recorded by Agents in the event database located on a Manager system.

Event Viewer has advanced data filtering capabilities allowing you to select and display specific data of interest in several formats, including bar chart, line graph, pie chart, text view and report view. Using ITA Event Viewer it is possible to query the database and view selected events as they happen (or take historical snapshots of the data).

The Query Builder wizard guides the administrator through the process of defining a query and generating a view. The events can then be filtered by Agent, user, Policy, rules, rule value, date, time or specified text, and the results displayed using one of a number of pre-defined views, or via a custom view (which can be saved and re-used). The Event Viewer can also be used to send internal commands to Agents.

Report Generator

As part of the Event Viewer, ITA also offers a report generator. ITA reporting provides considerable scope for creating user-defined reports if required. It is capable of consolidating security data from hundreds of systems (host IDS) as well as NetProwler (network IDS) systems and securely displaying this data according to risk priority (high, medium and low), by a variety of charts as well as data tables for drill-down analysis.

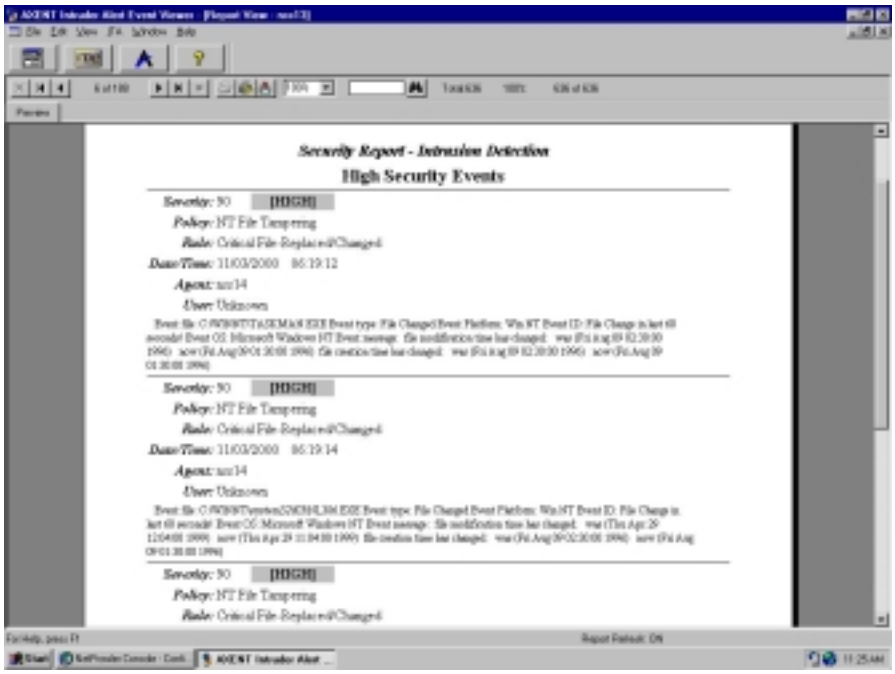

Figure 4 - Viewing ITA reports

Data can even be filtered using user-defined queries for conducting post event analysis on historical data, and it is possible to identify security trends and repeat offenders.

A number of different reports categorise and document attacks by system, by user and by time, and organise this data for various levels of target audience. Out of the box, the following reports are available:

- ***Management Report*** – Non-technical summary of attacks detected
- ***Technician Report*** – Technical summary detailing all attacks
- ***Security Events Report*** – Lists all detected events, sorted by se*verity*
- ***Agent Report*** – Compares events on different Agents
- ***Security Report*** – Compares severity of Events by Agent, user and date.
- ***User Report*** – Compares severity of Events by user, users on an Agent, or date.

As with the Event Viewer, reports are generated through the Query Builder Wizard, where the administrator selects the report view type, and defines the parameters of the query. The body of the report contains various report elements, including charts, graphs, and listings of individual events, and these are presented in the Crystal Reports Viewer for on-screen browsing. Custom reports can be produced via the usual Crystal Reports templates (if you have the Crystal Reports Designer software), and reports can be exported in a variety of formats, including CSV, Excel and Word, amongst others.

Also, Intruder Alert includes a feature called *Incident Response Help*. For each security event recorded to the powerful real-time monitor, Intruder Alert now documents the risk associated with each event and makes meaningful recommendations on how to counter or prevent the vulnerability from re-occurring and causing loss – very useful.

Verdict

Intruder Alert provides the means to monitor a range of hosts and operating system platforms throughout a large organisation. Anything that can be monitored and reported by your host operating system (via event logs or syslog) is fodder for Intruder Alert, and the multi-tiered architecture allows it to scale well.

Given the fact that it is not a simple matter to define your own policies from scratch, it is nice to see that Axent has included a number of useful policies that are deployed out of the box with no configuration or intervention required. This means that ITA can be deployed, and be immediately productive, with a minimum of security knowledge.

To get the most out of it, however, you need to get to grips with Policy definition. Although this can require almost a “programmer’s mentality” to produce the most effective Policies, the user interface is actually quite logical and straightforward, and plenty of help is provided both on-line and via the excellent documentation.

Despite being initially complex and perhaps a little daunting, Intruder Alert will prove to be extremely flexible and powerful once you get used to it. The combination of Intruder Alert and NetProwler together is a potent one.

Contact Details

Company name: AXENT Technologies, Inc.

E-mail: info@axent.com

Internet: www.axent.com

Address:
2400 Research Boulevard
Rockville, Maryland 20850
USA

Tel: +1 (301) 258-5043
Fax: +1(301) 670-3586

AXENT NETPROWLER 3.51

NetProwler is the network IDS part of Axent's security suite that also includes host-based IDS (Intruder Alert), vulnerability assessment (NetRecon), and security policy auditing and enforcement (Enterprise Security Manager).

Architecture

NetProwler implements a three-tier architecture to provide maximum scalability across large networks. The three components are:

- **Agent** – this component is installed on a dedicated PC to monitor traffic on the subnet to which it is attached. It compares network traffic with known attack patterns in its database and with a set of rules that determine which hosts are to be monitored for which attacks. When an attack is detected against a monitored host, an alert is sent to the Manager.

- **Manager** – this is a repository (SQL database) for configuration information and attack alert information. It executes configuration instructions from the Console and relays attack information from multiple Agents under its control to the Console.

- **Console** – the NetProwler Console displays attacks detected by all the Agents under its control via multiple Manager stations. It allows the administrator to configure and manage all the Agents attached to a specific Manager.

It is possible to integrate NetProwler with Intruder Alert via an SNMP collection agent which takes alerts generated by NetProwler and passes them on to Intruder Alert for further processing. Intruder Alert supplements NetProwler by providing additional response actions and host-based protection for the NetProwler Agent.

NetProwler employs SDSI technology which separates the session processing and analysis from the signature database. This enables NetProwler to dynamically load new updates, whether from the Axent Information Security SWAT team (via the automated Web update capability) or custom attack signatures created by the administrator, without the need to take the system off-line.

Installation

Installation is reasonably straightforward, though more long winded than most thanks to the multi-tier architecture. Although all three components can technically be installed on the same host if required (perhaps for a test environment or for very low volume monitoring purposes) a dedicated machine is recommended for each Agent and Manager. The Console can reside on a shared host. A password is normally required to access the Manager and Agent, though these components can be set to automatically logon providing they are kept in a secure location.

All the components installed quickly and easily from CD using the standard Windows InstallShield. Note that none of the components will work under Windows 2000 at the time of writing – the test platform for this evaluation was therefore Windows NT4 Service Pack 6a.

The documentation – which is provided as hard copy as well as electronically – is excellent, and offers a wealth of advice on installation and deployment in a range of environments, including switched networks. A number of sample "case studies" provide practical advice on deployment issues, including how to install the Agents in "stealth mode".

Configuration

The NetProwler Console is divided into two panes – ***Configure*** and ***Monitor***.

The ***Configure*** pane provides the means to configure Managers, add and manage Agents, define security policies and alert actions, and create and view reports. Unfortunately, it is also a rather daunting and occasionally confusing user interface, and certainly takes some getting used to initially. This potential for confusion arises out of the modularity of the system, which also provides tremendous power and flexibility, however.

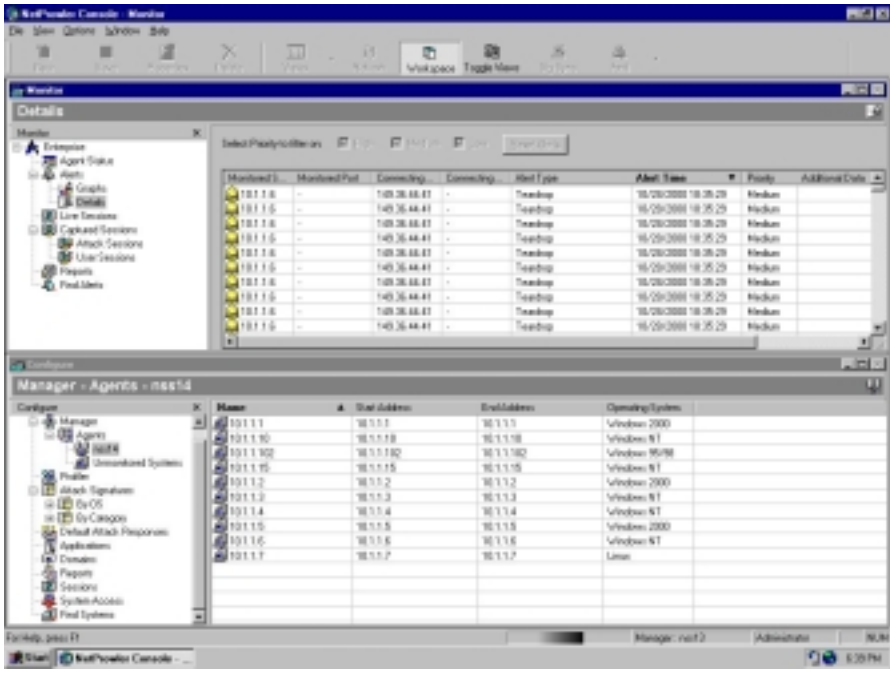

Figure 5 – Monitoring alerts via the NetProwler Console

There is no automated remote installation of Agents, which could make large-scale deployment a painful process. Once installed on the remote host, Agents are defined to the Console by entering a name, IP address and password, as well as a range of IP addresses to monitor. This is the first hint of major differences to other IDS products, since the NetProwler engine does not automatically monitor everything that passes on the wire.

Instead, each Agent has one or more IP addresses associated with it for monitoring purposes, and each of the addresses monitored has an appropriate range of attack signatures associated with it (depending on the host operating system).

Although this provides tremendous flexibility (for instance, the monitoring on heavily loaded segments can be split between several agents), it does at first sound like a horrendous configuration task. It isn't, however, thanks to an automated configuration tool called the "Profiler".

This tool scans the network for live systems and determines the host operating system and services running on them. From this information, it determines which attack signatures from the database should be associated with which hosts and performs the association automatically. Naturally, the scanned properties of each host can be examined and additional services and attack signatures can be associated and saved against them if required.

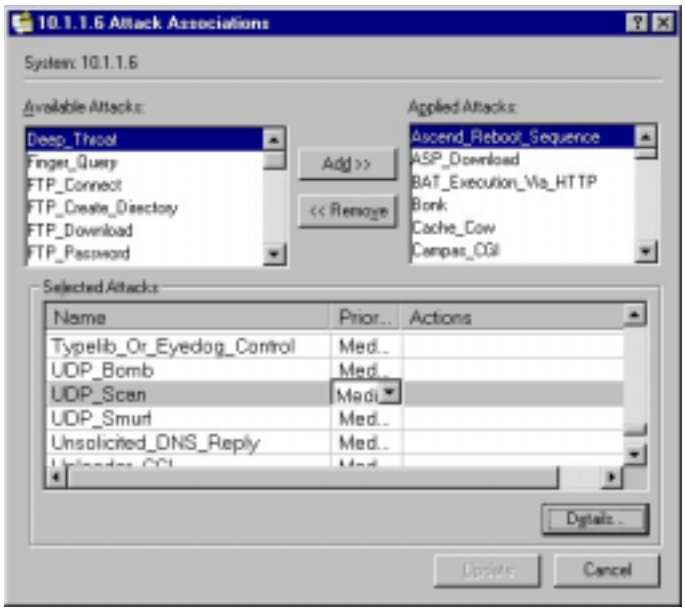

Figure 6 - Manually editing attack associations

The process of manually associating specific attack signatures with multiple hosts is made easier by the concept of Domains. The Administrator can create as many Domains as required (for instance, one domain for FTP servers, one for SMTP servers, one for Web servers, and so on) and each one can be populated with any number of hosts and attack signatures. Domain associations are then applied over and above the automatic Profiler associations. All attack signatures are applied cumulatively, so that if you add specific signatures or services to a particular host then re-profiling that host at a later date does not remove them. However, if you should remove signatures that NetProwler has associated automatically, then the next time the profiler runs those signatures will be re-applied.

This combination of Agents monitoring certain hosts and applying a subset of the complete attack signature database should provide the means to handle larger and more heavily loaded networks more effectively. However, it is also the most confusing aspect of NetProwler configuration, since associating signatures is not particularly intuitive and it is never immediately apparent which set of attack signatures are associated with which hosts. This means the administrator has to place an extraordinary amount of trust in NetProwler getting this right, or spend a lot of time checking each host individually to make sure (the NetProwler documentation does provide some help here).

Of course, the make-up of any network can change on a daily basis causing such “fixed” configurations to become quickly outdated. To combat this, Profiler jobs can be scheduled to run at regular intervals to keep things up to date and ensure that the latest configuration settings and signatures are always applied to the most appropriate machines. NetProwler is thus designed to have a “fluid” configuration, and the concept of fixed “security policies” which are applied to IDS sensors around the network in other products on the market simply does not apply here.

As you would expect, new attack signatures are provided at regular intervals by the Axent SWAT team, and can be incorporated into NetProwler via the Web-based Signature Sync capability. It is also possible to create custom attack signatures from scratch via a GUI interface in the Console, although a fairly detailed knowledge of your network protocols is required before undertaking this. It is nice to see the facility included, however. Any new signatures – whether custom built or provided by Axent - are automatically applied to the appropriate systems the next time the Profiler is run.

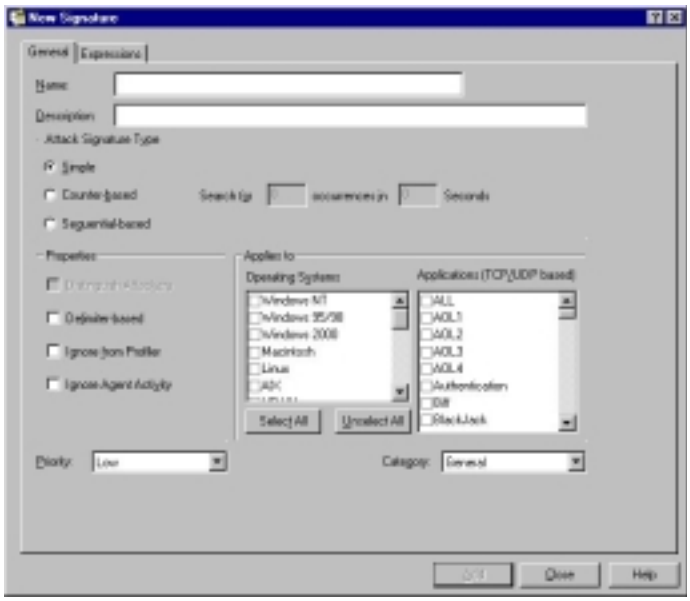

Figure 7 - Creating custom attack signatures

Once a particular set of Agents, hosts to be monitored and attack signature associations has been saved, the configuration data is transmitted via the Manager to the appropriate Agents and they begin monitoring accordingly. Each Agent has a graphical screen displayed on the host PC which shows details of packets monitored, packets dropped (a useful indication of how busy the network is and how overloaded the Agent is), attacks detected, and so on. This information can be displayed in graphical or text format, but it is not possible to make any changes to the configuration from this interface. The same information is passed to the Manager responsible for each Agent, where it is stored before being reported back to the central Console.

The ***Monitor*** pane in the Console provides the means for the administrator to see a real-time view of network attacks and intrusions. Individual Agent status can be determined, and alerts are flagged using red, yellow or green “spinning lights” to indicate high, medium or low risk. The administrator can choose to see every instance of an alert reported, or can employ “repetitive alert suppression”, whereby multiple alerts within a specified time frame are reported as a single instance.

A list of alerts can be displayed, and detailed information on each type of attack is available at the click of a mouse. In addition to the real-time notification to the Console, NetProwler can be configured to provide a number of other automated responses including e-mail, paging, SNMP trap, session termination, session capture, spawn an external command and firewall hardening (Axent Raptor and CheckPoint Firewall-1). SNMP traps can be processed by a local SNMP collection agent that integrates with Intruder Alert, which can then provide additional reporting and alerting capabilities if required.

Session capture records details of suspect sessions which can be replayed later via the Console or Agent interfaces. This capability can be extended to provide live session monitoring, which provides the same session monitor and capture capability for all TCP/IP session types (not just suspect sessions) such as FTP, Telnet and HTTP as they occur in real time. Full protocol decode is provided, and sessions can be captured to file for review later – this is a very powerful feature, and one that is not particularly common in the IDS market place.

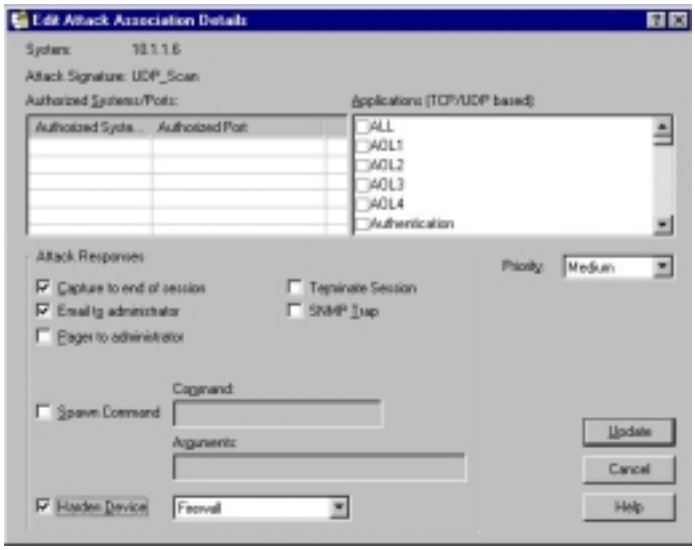

Figure 8 - Specifying attack responses

NetProwler allows the administrator to define most response actions by individual attack signature and by priority level. The growing number of attack signatures, however, can make configuring actions for individual attacks quite time consuming, and so the simpler approach is to configure responses by priority level. Thus, for High priority attacks, you may e-mail, and page the administrator and harden the firewall; Medium priority may trigger only an e-mail; Low priority attacks may simply be logged for later reporting. Unfortunately, the Terminate Session, Capture to end of session and Spawn Command response actions cannot be configured by priority level.

Finally, NetProwler can also be used to restrict traffic on one or more TCP/IP-based applications on a monitored system by time of day or day of the week. This can be used to restrict FTP access to an internal server to certain times of the day (working hours only, perhaps) or to certain workstations, providing an element of access control in addition to intrusion detection.

Reporting and Analysis

In addition to the excellent real-time statistics, NetProwler provides a range of reports via the ubiquitous Crystal Reports engine. Unfortunately, this is probably the weakest part of the package.

The first thing that hits you is that it is only possible to schedule reports for regular runs – there is no ad hoc reporting capability. This means that if you need a report quickly, you have to schedule it to run in one minute's time – this is unnecessary hassle.

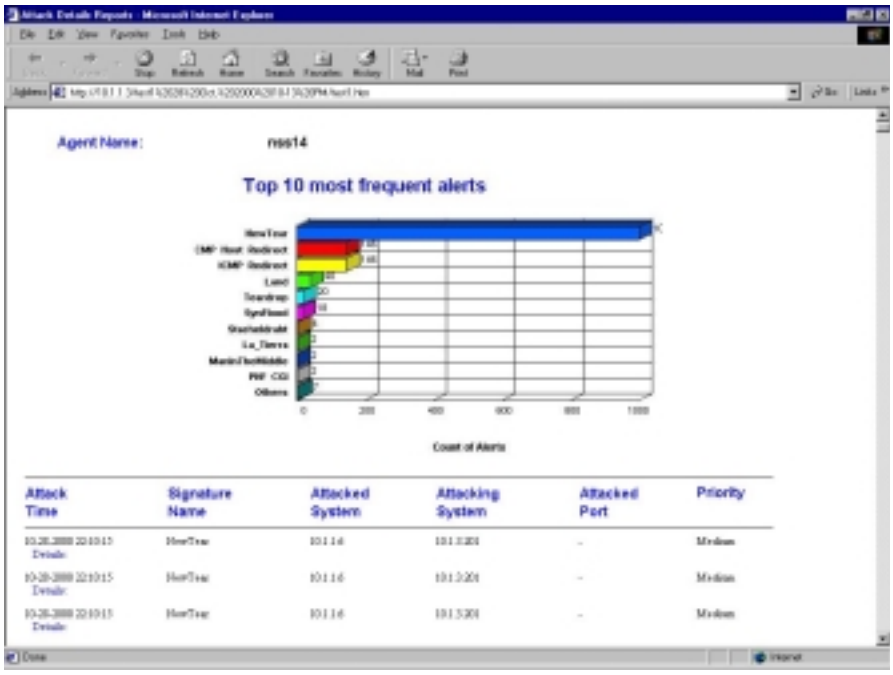

Figure 9 - Viewing NetProwler reports

We also came across severe limitation in NetProwler's reporting. As part of our testing we were launching in excess of 20,000 attacks against each IDS engine per test, and when it came time to report on the activity during the testing the report came back with "Too many records to be retrieved". The slowest period of activity produced around 15,000 records whilst the highest was in the region of 47,000 records. We don't consider these to be excessively large numbers, and feel that NetProwler reporting should be able to handle them.

The Report Wizard provides three general report categories:

- **Quick Reports –** the content and format of each report is fixed. Quick reports include information from all Agents associated with a single Manager and only in HTML format.

- **Pre-Formatted Reports –** provide a more flexible layout. Pre-formatted reports let you choose which Agents you want to gather information from, what kind of alerts you want reported, and what kind of export file format is required (HTML, Excel, Word, plain text or Crystal Reports).

- **Custom Crystal Report –** allows you to schedule a custom report designed using Crystal Reports Designer.

The types of reports available within these categories include Alert Summary, Attack Signatures Alert Summary, Daily/Weekly/Monthly Executive Summary, Attack Details, Unauthorised Access, Session Start/End, and Cost Analysis. Each report contains a graph followed by a simple list of the attacks or sessions. Unfortunately, it is not possible to access further information on attacks mentioned in the report via hyperlinks – a feature which is common in other products.

One analysis feature that we did like is the Find Alerts capability. This allows the administrator to query the database of stored alerts for all alerts of a particular type, for a particular target, or in a particular time range, and have these displayed instantly in the Monitor pane.

Overall, however, reporting needs to be improved.

Verdict

NetProwler is a complex product that initially takes some getting used to. The administration interface is not particularly intuitive and you can spend some time trying to figure out how to do certain operations, such as the best way to associate attack signatures with hosts. Certain aspects of the reporting also need to be improved.

That said, the complexity is there because Axent has spent some time designing an architecture that is flexible and scalable, with a multi-tiered control structure and the ability to selectively apply signatures to hosts, and selectively associate hosts with Agents. This provides an extremely granular approach to configuration, meaning that you could have a single agent monitoring a single host for a small subset of attacks if you felt so inclined. Multiple Agents installed on the same subnet monitoring different hosts for different attacks are thus one way around IDS performance problems on heavily loaded network segments. The only thing that is missing here is the Network Node IDS method of operation (currently in development) where the Agent resides on the host to be monitored – NetProwler Agents currently operate in promiscuous mode only.

Once you have mastered the initial complexity, NetProwler offers a powerful and flexible IDS system that is extensively customisable – right down to the ability to add your own attack signatures. The real-time monitoring capabilities are also excellent, with a very useful GUI interface on the Agent itself as well as excellent monitoring via the central Console.

Contact Details

Company name: AXENT Technologies, Inc.

E-mail: info@axent.com

Internet: www.axent.com

Address:
2400 Research Boulevard
Rockville, Maryland 20850
USA

Tel: +1 (301) 258-5043
Fax: +1(301) 670-3586

CA ETRUST INTRUSION DETECTION V1.4.5

Formerly known as SessionWall, eTrust Intrusion Detection has a new name – if not a new look – since the acquisition of Abirnet by Computer Associates (CA).

Offering more than just IDS, eTrust Intrusion Detection provides surveillance, intrusion and attack detection, inappropriate URL detection and blocking, alerting, logging, and real-time response in a single software package.

It offers:

- **Network usage reporting** ranging from high level statistics down to specific user usage.
- **Network security** including content scanning, intrusion detection (service denial attacks, suspicious activity, malicious applets, viruses), blocking, alerting and logging.
- **Web and internal usage policy monitoring and controls** to monitor and enforce Web access and inter-company policies by user ID, IP address, domain, group, content, and control list.
- **Company preservation** - often referred to as litigation protection - monitoring e-mail content, logging, viewing and documentation.

eTrust IDS can be installed on any network-attached Windows 95/98 or NT 4.0 machine and can process the network traffic from one or more Ethernet, Token Ring and FDDI local network segments. Although the documentation mentions Windows 2000 support, we could not get it to run under Windows 2000 on our test network. We are assured that the problem will be resolved by the time you read this.

Architecture

eTrust Intrusion Detection includes policy folders for Web access, for monitoring/blocking/alerts, for intrusion detection, and for attack detection, malicious applets, and malicious e-mail. These policy folders contain the rules that eTrust Intrusion Detection uses when scanning network communications. The rules specify the patterns, protocols, addresses, domains, URLs, content, etc. and the actions to be taken should these be encountered.

eTrust Intrusion Detection includes the same detection engine and signatures that are used in CA's InoculateIT anti virus product. Using this engine and signatures, eTrust Intrusion Detection detects all known viruses and monitors network traffic to detect their entry into or movement around the network

The URL Category List is composed of hundreds of thousands of URL’s determined to belong to one or more of 27 categories, as defined by Secure Computing's Web Tools Division. Although the categories represent general content types encompassing an often wide variety of material, all are deemed potentially inappropriate for today's typical workplace

eTrust Intrusion Detection Enterprise

The Enterprise version provides the ability to centrally monitor and manage multiple distributed eTrust detection engines, and to consolidate selected information in a common relational database.

This is achieved by installing eTrust agents on different segments of the network (local and remote), which are controlled by a central station from which the administrator can view and generate reports based on the consolidated information collected by the agents.

eTrust Intrusion Detection Central allows a single remote administrator to monitor and manage multiple local and remote eTrust Intrusion Detection hosts. Using this capability, the administrator sees alerts on the console and has the ability to remotely control specific eTrust hosts as if they were local.

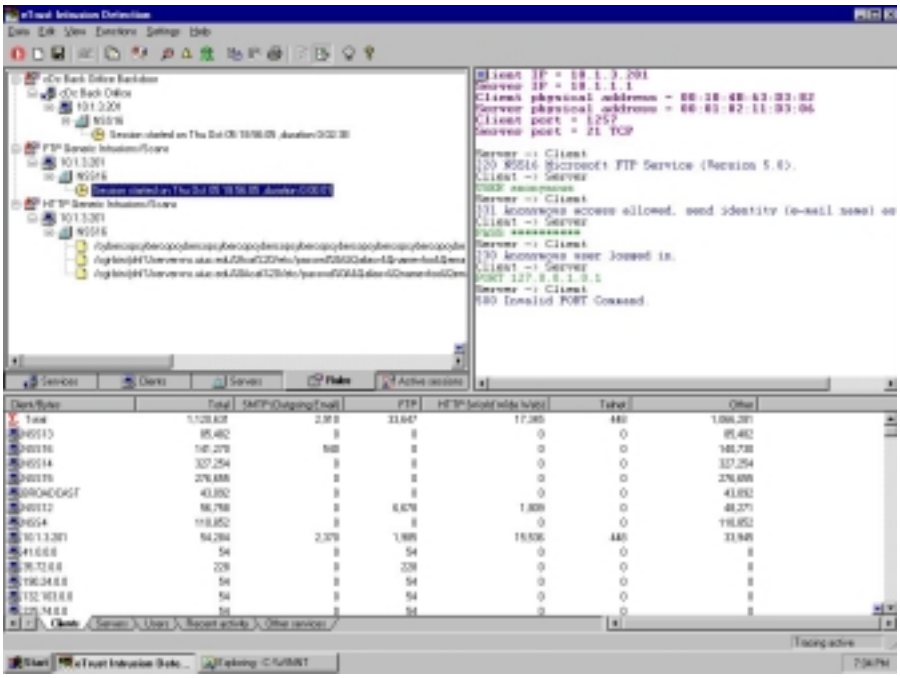

Figure 10 - The eTrust console

The main Central component operates on Windows 95, Windows 98 or Windows NT/2000. It receives, sorts and displays alerts generated by one or more remote agents and allows the administrator to connect to and operate the agent.

Communication between the central console and remote hosts is achieved via Central Agents installed on all stations running Enterprise software. The Central Agent operates in the background on the remote host, receives alerts from the local eTrust ID, and sends these alerts to eTrust ID Central.

eTrust Intrusion Detection Remote allows remote control of eTrust Intrusion Detection via dial-up or direct network connections

Finally, **eTrust ID Log View** allows users to monitor usage details over an extended period of time by targeting a specific database and browsing and viewing the archived information. Users can also consolidate session information from multiple eTrust stations in a relational database.

The system includes the database front end and distributed collection components that are invoked by events in eTrust Intrusion Detection based on eTrust Intrusion Detection rules.

The eTrust ID Log View consists of three main components:

- The **Data Client**, which collects the data and transfers it to the archive.
- The **Log View Database Server** component which controls the archived data on the same or different computer utilising a relational database product (Oracle or SQL).
- The **Log View Viewer** which can reside on any Windows NT system and provides the user with an interface for viewing the archived logs.

Installation

Installation is the usual straightforward Windows InstallShield routine. Inserting the CD brings up a menu of installation choices which provides the option to install a stand-alone engine or the eTrust Intrusion Detection Enterprise components.

The eTrust Intrusion Detection engine is installed as a native NT service and operates in stealth mode to make it difficult to detect on the wire. An on-line registration function finishes the installation routine, and this was our only gripe with installation, since if your network connection is down at the time of install it could cause problems.

Documentation could only be described as basic, with a Getting Started Guide in PDF format on the CD. However, it has to be said that eTrust IDS is fairly simple to get up and running, so more extensive documentation is probably unnecessary.

Configuration

Once installed, eTrust Intrusion Detection immediately starts its surveillance for intrusion attempts and suspicious network activity and begins logging all e-mail, WEB browsing, news, Telnet, and FTP activity using a default security policy. New rules can easily be added or the existing rules can be changed using menu driven options. All network activity that is not associated with a rule is identified for statistical and real-time analysis, often identifying the need for additional rules.

When it comes to editing the various detection rule sets, anyone familiar with the FireWall-1 rules definition user interface will be quite at home with eTrust Intrusion Detection. It's not that it is similar - it's identical. CA has a development relationship with Checkpoint that allows it access to the actual FireWall-1 code for rules maintenance.

Any number of eTrust users can be defined to the system, each one authorised to perform only certain actions if required – one user may be allowed to create new rules, for example, whereas another might only be able to run reports.

Its just as well that rules definition is so straightforward, because there is a lot of it to do.

eTrust does a lot more than Network IDS, and there is a set of rules for each or its major functions:

- *Intrusion Detection*
- *URL Access Monitoring and Control*
- *Monitor/Block/Alert*
- *Content Inspection*

eTrust Intrusion Detection checks each session against the rules until either the session terminates or a match occurs.

The first place to start is to define the various network objects – specific hosts, networks, users, domains, workstation, and so on - that will be referred to by name in the rule sets – and those services which will be excluded from detection. For instance, you might decide that all NetBIOS services over TCP for the internal network need not be examined by eTrust.

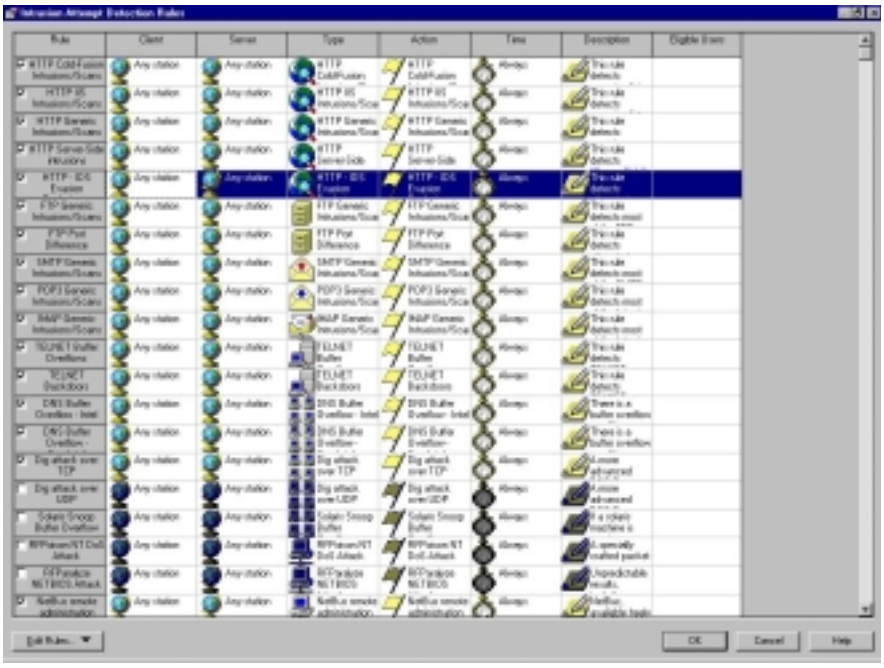

Figure 11 - Defining rule sets

Once you have this basic information entered, you can begin defining the rule sets for each of the above capabilities. What you would refer to as “signatures” in other products are “Rule Types” in eTrust, and the Intrusion Detection rule set contains just over 360 signatures at the time of writing, which is considerably less than some of the competition. CA is working hard to catch up in an area that is relatively new to it, and new signatures can be downloaded regularly from the CA Web site.

Rule Types can be Service or Content-based, and a number of different parameters can be added instructing eTrust to check session content for “active” components, such as Java or ActiveX, or compare session data with strings or commands that are specified as part of the rule. It is incredibly easy to add new signatures of your own, making eTrust Intrusion Detection one of the most readily extensible products we have seen.

The actual rules are created from these Rule Types (attack signatures) combined with a source and destination, an action and a time when the rule is applicable. If any of the characteristics of the session correspond with the rule conditions, a match occurs. This match triggers an Action, which can include logging to file, blocking the session, raising an alert, writing to the NT event log, audio alert, NT message, running an external program, sending an e-mail, fax, SNMP trap, pager, syslog, and reconfiguring your firewall (eTrust, Cisco or any OPSEC-compliant firewall), amongst others. Any combination of these Actions can be triggered from a single event, and this is probably the widest range of alert types we have seen in a single product.

Rules can be turned on and off in the rule set by clicking on a check box, allowing them to be disabled temporarily on the fly for testing purposes without having to delete them.

When you choose to log details of an event in the Tree Window, you can decide whether the log should include the contents of the session and whether the contents should be encrypted or signed. If you choose to include the contents of the session, you will be able to see these details in the View window when you select the session in the Tree Window.

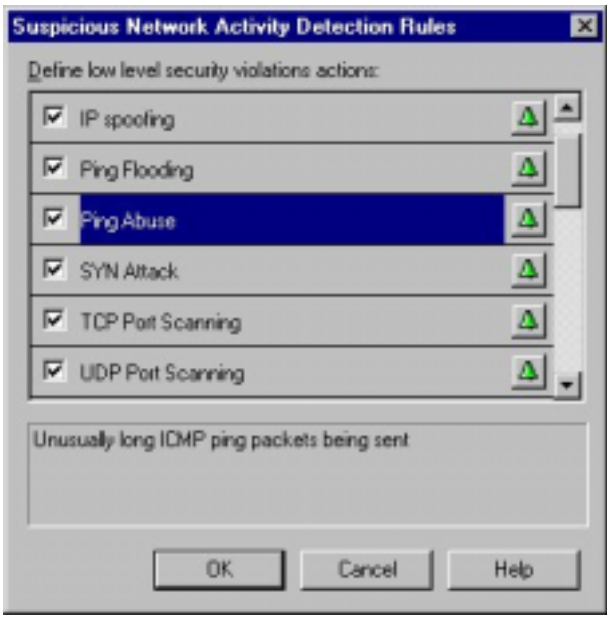

Figure 12 - Suspicious Network Activity Detection Rules

In addition to the high-level **Intrusion Detection** rules, there are also a number of lower-level predefined security violations, covered by the **Suspicious Network Activity Detection** rule set. These cover such activities as IP spoofing, SYN flooding, ping attacks, port scanning, WinNuke, Land, Teardrop, Smurf, distributed DoS attacks, and so on. When eTrust Intrusion Detection detects one of these violations, the Show Security Violations button in the toolbar blinks and clicking this button displays a window with details of the violation. There are less than thirty of these Security Violations currently defined in the product, and this is an area that needs improvement if eTrust is to be brought in line with the IDS market leaders.

eTrust Intrusion Detection offers a number of other useful features that are not normally found in “traditional” IDS’, and these are covered by a number of other rule sets.

Content Inspection Rules are used to check for active HTML components and viruses in e-mail attachments, news group postings , FTP downloads and HTTP pages and binaries. In the Content Inspection Rules grid, the administrator can choose which components eTrust will search for, and the action that will be taken when one of these components is detected. eTrust Intrusion Detection also uses the InoculateIT scanning engine to detect and block network traffic containing computer viruses.

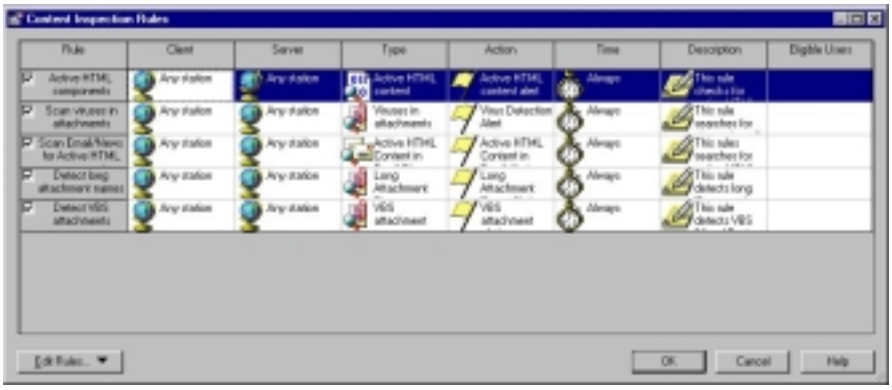

Figure 13 - Defining Content Inspection Rules

One of the more advanced features in this section of the product is the ability to monitor e-mail traffic, right down to the point of being able to read the messages themselves or compare message content against a list of key words and phrases. This may send shivers down the collective spines of many corporate Directors, who may not like the idea that the network administrator can simply lift any message – incoming or outgoing – off the wire.

Of course, Director’s e-mail could always be serviced by a separate segment not monitored by SessionWall or encapsulated within a VPN. Once you have set aside such fears, however, this capability can help to ensure that there are no corporate secrets, offensive material or mass mailing of CV’s going out of the organisation.

URL Access Monitoring And Control Rules monitor and log access to sites that are deemed “unproductive” and have a specific rating. The administrator chooses which categories (i.e. games, dating services, gambling, sport) are not work-related and which sites eTrust Intrusion Detection will monitor based on their ratings. Four levels of extremity can be selected for sites categorised as violence, sex, nudity and language.

Finally, **Monitor/Block/Alert Rules** are used to log activity for all the protocols and to allow blocking of specific Web sites. eTrust can even be configured to block network games such as Doom and Quake automatically – a real killjoy package, this one! The administrator can view the logged and blocked events in the Tree Window.

Reporting and Analysis

The GUI interface is divided into three windows. The top left window is called the **Tree Window**, and displays a hierarchical tree of the logged or blocked sessions. Tabs along the bottom of this window allow the view to be sorted by services, clients, servers, rules or active sessions. Clicking on a session in the Tree Window brings up the details of that session in the **View Window** on the right-hand side of the screen.

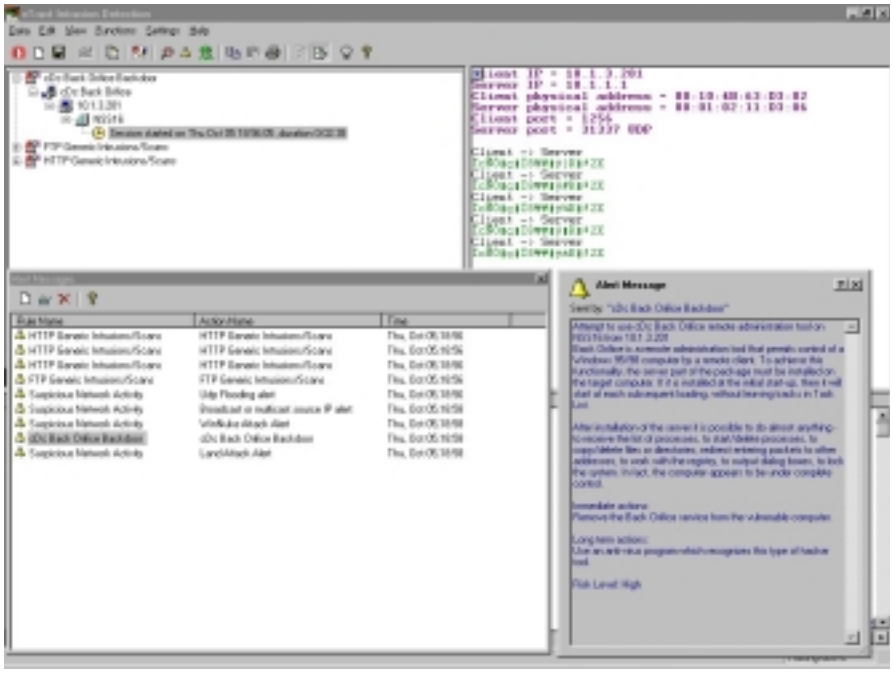

Figure 14 - Monitoring alerts

While session details are being displayed, right-clicking the mouse button switches between viewing the data in the formatted and unformatted form (ASCII, EBCDIC and hexadecimal). In the View Window it is also possible to view a real-time network activity graph, enable/disable a rule, and create a blocking rule on the fly based on the contents of that particular event.

The final window at the bottom of the screen is called the **Statistics Window**. It displays statistics on the usage of protocols by clients and servers on the network, a log of the first time a station was detected using a specific protocol, a log of recent network activity, details of NT workstation users and a separate log of other services not included in the Tree Window.

Toolbar buttons for Security Violations and Alert Messages will flash if any alerts have been received and not yet displayed. Clicking on the buttons brings up the appropriate windows, and all the alerts are in plain English and are very easy to understand (some other IDS vendors should take note). In the Alert Messages window, right-clicking on an alert allows it to be cleared manually or for a wonderfully detailed description of the alert condition to be displayed. In the Security Violations window, right-clicking on a violation allows it to be cleared, or it can be marked to ignore that violation in future.

With all these windows and different views onto the same set of data, eTrust provides one of the best real-time monitoring systems of any IDS we have seen.

Although reports are obviously useful for detailed analysis, if you should ever come under attack it is essential to have a good real-time indication of what is happening. Very few IDS systems provide this at all, and none are as comprehensive as eTrust.

It is just as well that the monitoring is excellent, because the reporting is barely adequate – at least as far as intrusion detection is concerned. There are, in fact, a large number of pre-defined reports, but they betray the history of the product inasmuch as the majority of them relate to the general network and session monitoring and URL blocking capabilities.

There is an extensive set of reports covering such subjects as characterisation of protocols used, identification of services being used (i.e. specific Web sites, e-mail, FTP, Telnet, etc.) and a list of blocking situations which have occurred. However, only three reports relate directly to intrusion detection covering *Suspicious Network Activity*, *Suspicious Network Activity Over Time*, and *Detected Intrusions Per Server*. A report scheduler provides the means to have key reports run automatically at regular intervals, and reports can be run against the current live data set or “snapshots” of archived data.

In typical Crystal Reports fashion the finished reports can be exported in a variety of data formats, including plain text, Word documents, HTML and so on. Data can also be exported for use in third-party reporting tools such as WebTrends or Telemate. A certain amount of customisation can be carried out on each report, but the basic content cannot be changed within eTrust, meaning we are limited to the three IDS basic reports until CA updates the product (although Crystal Reports would allow extensive customisation).

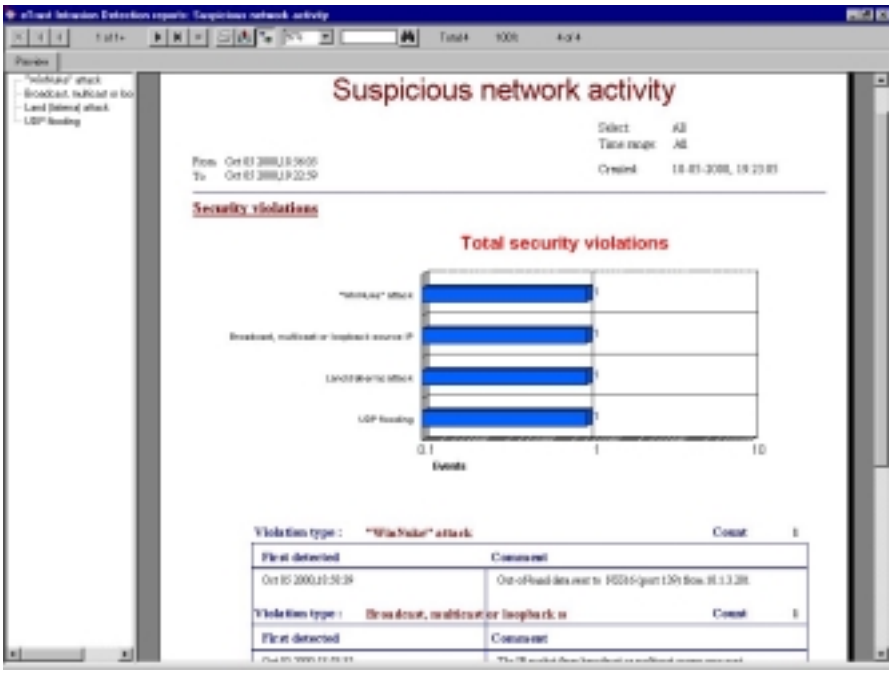

Figure 15 - The Suspicious Network Activity report

In most cases, however, those three – along with the excellent real-time monitoring – will get you by. You are unlikely to be able to perform much forensic analysis after the fact using eTrust, however.

Verdict

eTrust Intrusion Detection has a hard time of it in the IDS market place. It's not that it isn't a good product – it is – but it started life as a content analyser and URL blocker, and sort of drifted into intrusion detection because at its heart was a promiscuous mode engine that was adept at sniffing packets off the wire, comparing their contents with a database of rules and signatures, and taking appropriate action depending on what it found there.

True, it does work at a different layer of the protocol stack than some of its IDS competition, but its main fault, to be honest, is that as a pure IDS product it lacks some of the advanced features and refinements of its "thoroughbred" rivals. It also does not appear to be as slick as some in the area of enterprise-wide deployment and remote management, focussing more on consolidating reports across multiple eTrust engines. Unfortunately we were unable to verify this through testing, since we did not have access to the Enterprise components that provide this functionality.

However, where it does excel is in the user interface and real-time monitoring and alerting capabilities that put many of the competition to shame. The on-screen displays of alerts and attacks are clear and well laid out, and a single click provides detailed descriptions. Where an on-screen display is not required, eTrust provides the widest range of remote alerting options we have seen in a product of its type. The rules definition interface cannot be faulted, and is probably one of the best known in the security industry thanks to the code base shared with FireWall-1. Adding your own custom signatures is also fairly straightforward.

Many organisations will buy eTrust IDS for its powerful content analysis and blocking capabilities, at which it excels, and accept the IDS functionality as a bonus. If you don't think you need the power of the high-end IDS products, then eTrust will serve you well.

If you do need a full-blown IDS, you might still want to evaluate eTrust to run alongside it to perform all the functions that a "traditional" IDS cannot.

Contact Details

Product name: eTrust Intrusion Detection V1.4.5 (Build 10)

Company name: Computer Associates

Internet: http://www.cai.com

Address:
One Computer Associates Plaza
Islandia, NY 11749

Tel: +1 516-342-5224

UK Address:
Ditton Park, Riding Court Road
Datchet
Berkshire SL3 9LL

Tel: +44 (1)753 577733
Fax: +44 (1)753 825464

CISCO SECURE IDS V2.5

Cisco Secure IDS (formerly known as NetRanger) is a network-based IDS, which means that it monitors all traffic on a subnet and compares individual or groups of packets against known attack signatures in an attempt to identify illegal activity.

Cisco Secure IDS is different from most other IDS on the market, however, since it is supplied as a dedicated network appliance, with all hardware and software necessary to get you up and running.

Architecture

The IDS sensor comes in three flavours, each running a heavily modified version of Sun Solaris, with new packet drivers written to cope with up to 100Mbps of traffic on network interfaces in promiscuous mode:

- **Cisco Secure IDS-4210 Sensor** - optimised to monitor 45 Mbps environments and is ideally suited for monitoring multiple T1/E1, T3, and 10Mbit Ethernet environments. It comes in a 1U high chassis which contains a Celeron 566MHz processor, 256MB RAM and two auto sensing 10/100BaseT (RJ-45) Ethernet interfaces – one for monitoring and one for management.

- **Cisco Secure IDS 4230 Sensor** - optimised to monitor 100Mbps environments and is ideally suited for monitoring traffic of switch Switched Port Analyser (SPAN) ports and Fast Ethernet segments. It is also suitable for monitoring multiple T3 environments. The additional performance is provided by Dual Pentium PIII 600MHz processors, 512MB RAM, and once again it sports two auto sensing 10/100BaseT (RJ-45) Ethernet interfaces for monitoring and management.

- **Catalyst 6000 IDS Module** - designed specifically to address switched environments by integrating the IDS functionality directly into the switch and taking traffic right off the switch back-plane, thus bringing both switching and security functionality into the same chassis. Sporting 256MB RAM, it is designed to monitor 100Mbps of traffic.

Management is designed to be performed over a dedicated network using one of the two network interfaces in the Sensor. The remaining network interface is used purely for packet sniffing on the live network to be monitored.

Multiple sensors can be deployed around the network and managed from a single, central console running one of two pieces of software:

- **Cisco Secure Policy Manager v2.2 -** This Windows-based software application provides integrated management of firewalls, virtual private networks, and intrusion detection. The IDS component of Cisco Secure Policy Manager (CSPM) provides robust device management and configuration as well as real-time event monitoring. Communication between the CSPM console and the Sensors is encrypted via IPSEC-compliant VPN tunnels where required.

- **Cisco Secure Intrusion Detection Director -** This UNIX-based software application plugs into an existing Hewlett Package OpenView Network Node Manager console, running on an HP-UX or Sun Solaris operating system. This solution provides Cisco Secure IDS device configuration and topology-based event monitoring for existing HPOV users.

Installation

Installation tasks are minimal thanks to the turnkey appliance approach. All that is required is to attach a PC to the serial port of the Cisco Secure IDS box and set the date, time and IP addresses of the two interfaces before plugging it into the network. It starts monitoring straight away with a default policy.

In order to see what it is monitoring, of course, it is necessary to install the Cisco Secure Policy Manager (CSPM) software on an NT Server which is connected to the *management* interface of the IDS Sensor. We had just the one CSPM server, and so a stand alone implementation was used - this is simply a matter of inserting the CD and following the installation wizard. Client-server and distributed implementations can also be deployed, though these are no more difficult to get up and running, merely requiring more steps to install the distributed components.

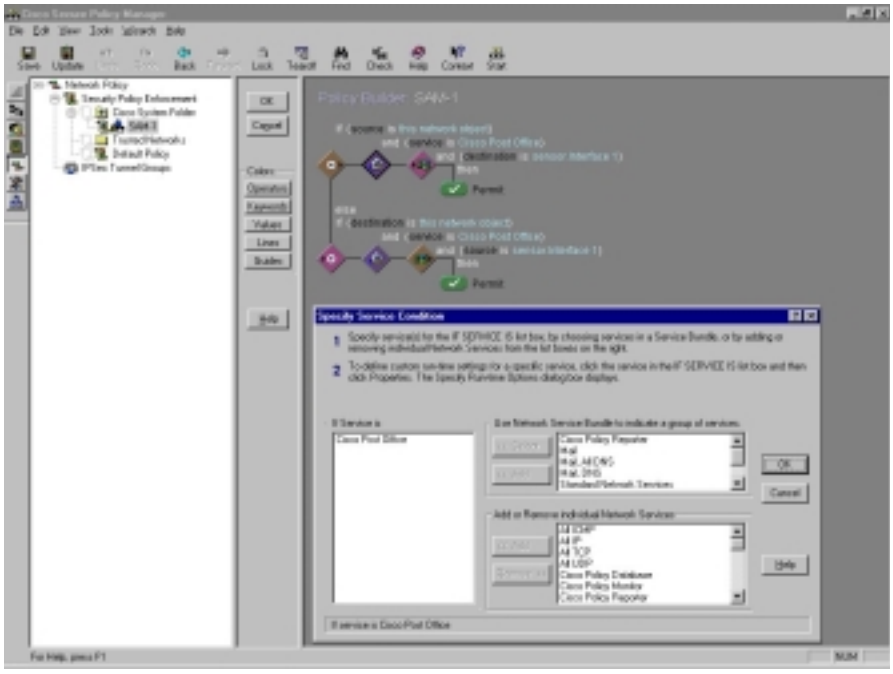

Figure 16 - Cisco Secure Policy Manager

For our tests, we also installed the netForensics server (see *Reporting & Analysis* section), which was considerably more involved given the need to install Linux and Oracle before we could get everything talking. However, netForensics also provide a plug-and-go appliance solution too, in which case – as with the Cisco Secure IDS Sensor – installation requires nothing more than plugging it in and setting a couple of parameters.

Despite the loss of the nice hard copy manual that used to accompany the previous Cisco Secure IDS product (which, admittedly, concentrated on the HP OpenView plug-in), the quality of the Cisco documentation supplied is more than adequate. The new documentation obviously concentrates more on the CSPM software than the sensor itself, but then there is not much involved in operating the sensor, over and above that which is covered in the hard copy installation notes included in the box. Operation and configuration of the sensor via CSPM is covered in plenty of detail, and there are a number of AVI “training” videos included also.

Configuration

For centralised, remote management and monitoring, Cisco provides a couple of management options in the shape of the Windows-based Cisco Secure Policy Manager (CSPM) - which provides consolidated management of firewalls, site-to-site VPN’s, and intrusion detection systems - and the UNIX-based Cisco Secure IDS Director, providing integrated IDS management into an HP OpenView network management system (NMS).

As part of this test, we used CSPM for IDS configuration. CSPM is a scalable, powerful security policy management system that effectively provisions security services throughout a corporate network. CSPM configures Cisco firewalls and Virtual Private Network (VPN) routers in a consistent and uniform manner that is independent of whether the device is a Cisco Secure PIX Firewall or a Cisco router supporting firewall capabilities. Cisco Secure Policy Manager allows customers to define, distribute, enforce, and audit network-wide security policies from a central location.

CSPM streamlines the tasks of managing complicated network security elements such as perimeter access control, Network Address Translation (NAT) and IPSec-based VPN’s . CSPM also simplifies the deployment of security services throughout corporate networks.

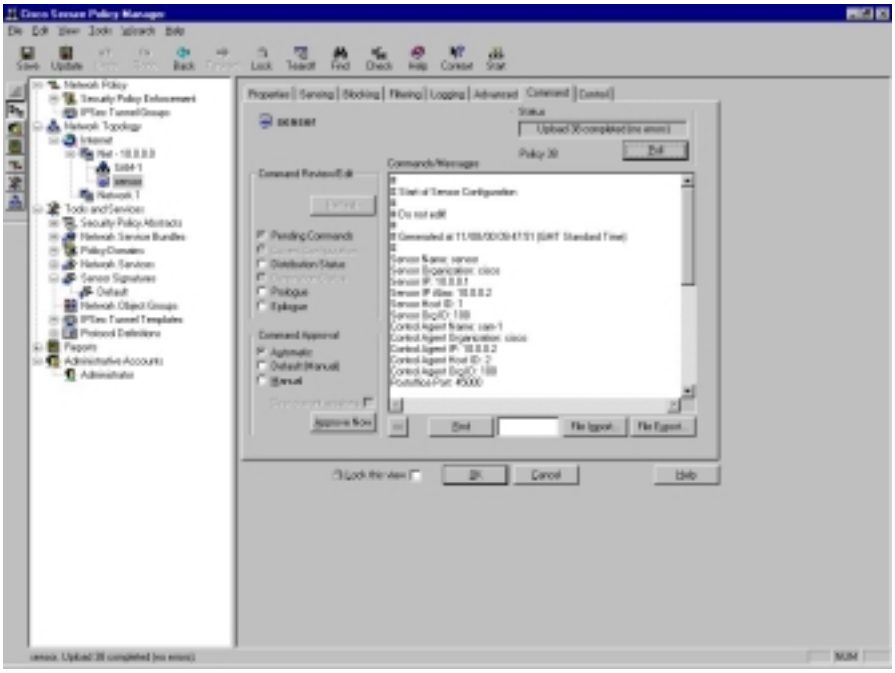

Figure 17 - Distributing policies to Cisco’s Secure IDS sensors via CSPM

CSPM's graphical user interface allows administrators to visually define high-level, end-to-end security policies for multiple Cisco firewalls and VPN routers within a network. CSPM translates these policies into the appropriate device configurations with the proper syntax for the various devices within the managed network. These configurations can then be distributed automatically, eliminating the costly time-consuming practice of implementing security commands on a device-by-device basis. CSPM also provides system-auditing functions including event notification and a Web-based reporting system.

Most of the features currently available within CSPM are thus aimed at firewalls and VPN's – Cisco Secure IDS is one of the more recent additions and the functionality is not quite as complete. For instance, there are no Web-based reporting capabilities available for IDS devices, and much of the policy management stuff simply does not apply.

This means that much of the hierarchical tree display in the left hand pane can be ignored when configuring the Cisco Secure IDS system. In the *Network Topology* section it is necessary to define a network address range (so the IDS can determine whether attack are coming from the "inside" or "outside"), as well as creating entries for the CSPM server itself and all IDS Sensors.

For each Sensor, it is possible to determine which IDS policy is currently being used, how addresses are to be blocked, whether event log files should be generated, and which attack signatures should be filtered out and ignored from which IP addresses (this would allow port scans to be run from internal machines without triggering IDS alerts, for instance).

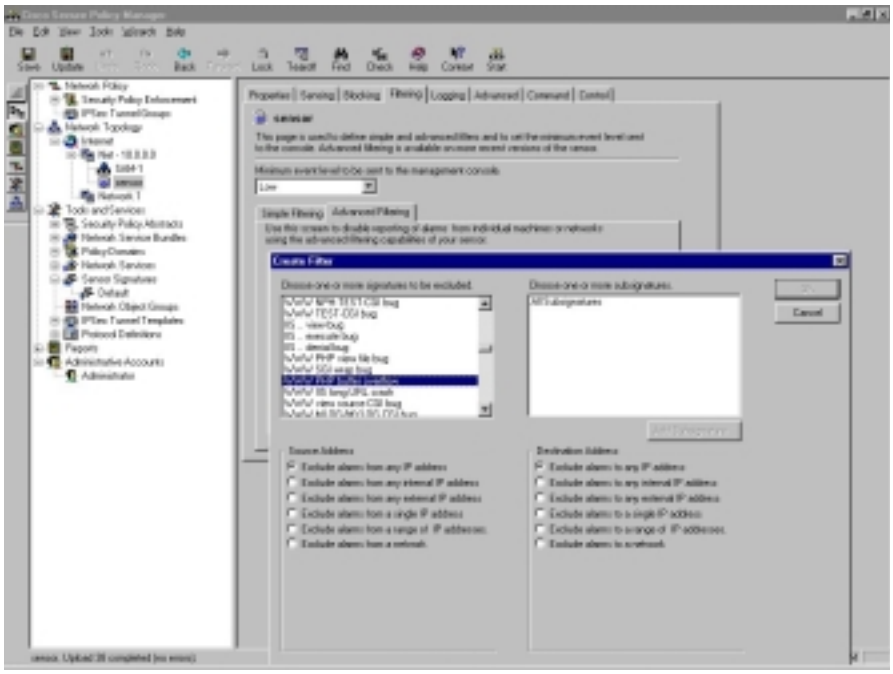

Figure 18 - Filtering attack signatures

The most important branch of the policy tree is headed *Sensor Signatures*, and here is where IDS security policies can be defined. Over three hundred attack signatures are available as part of the Cisco Secure IDS product covering a range of attack categories.

These include:

- *Exploits* - Activity indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking
- *Denial-of-service (DoS)* - Activity indicative of someone attempting to consume bandwidth or computing resources to disrupt normal operations, such as Trinoo, TFN, and SYN floods
- *Reconnaissance* - Activity indicative of someone probing or mapping the network to identify "targets of opportunity," such as ping sweeps and port sweeps - usually a precursor to an actual exploit attempt
- *Misuse* - Activity indicative of someone attempting to violate corporate policy. This can be detected by configuring the sensor to look for a custom text strings in the network traffic

The latest version of the Cisco Secure IDS also includes IP fragmentation reassembly and “Whisker” anti-IDS detection capability support. Curiously, this is switched off by default, presumably because of the potential performance penalty involved. All signatures are updated on a regular basis to remain current with emerging hacker exploit techniques.

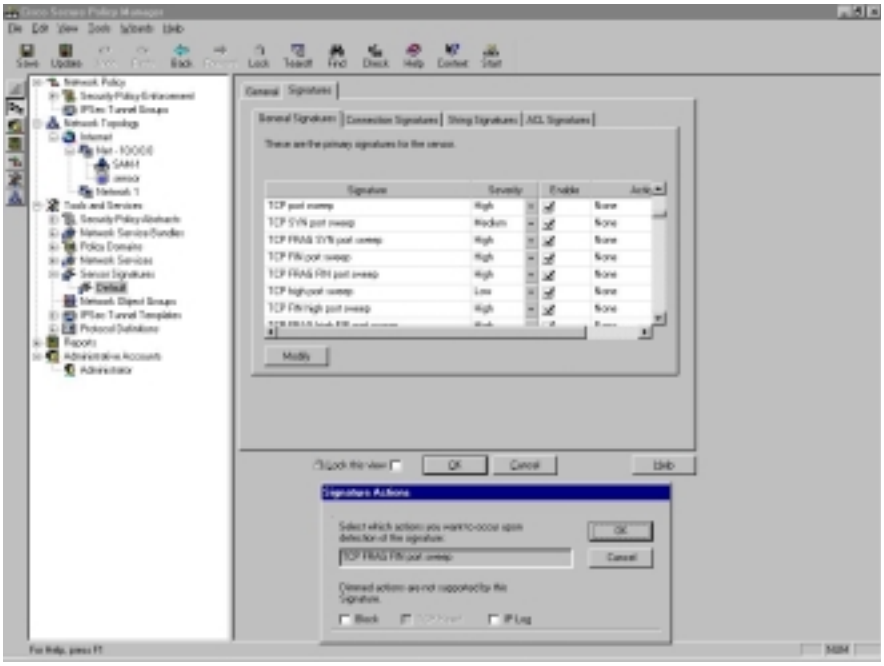

Figure 19 - Enabling/disabling General attack signatures

All of the “*General*” signatures are enabled by default, and it is possible to change the severity code (High, Medium or Low) and the Actions (Block, TCP Reset or Log to file). When an attack is noted, as well as logging to file and alerting to the CSPM console, the Sensor can instantly cut TCP sessions, and dynamically manage a Cisco router’s access control list to “shun” intruders, thus preventing further attacks from that source. This feature can be temporary, if desired, or maintained indefinitely. The rest of the network traffic will function normally - only the unauthorised traffic from internal users or external intruders will be removed.

Clearly this feature needs to be managed carefully, particularly where there is the chance of false positive alerts – you don't want to accidentally cut off your entire accounts department from their network just because someone typed a password incorrectly. To prevent this sort of mistake, a panel in the CSPM configuration allows the administrator to define certain addresses that will never be blocked.

In addition to the General signatures, it is also possible for the administrator to define additional signatures based on *connection details*, *string expressions* or *ACL's*. *Connection* signatures provide the means to raise alerts on any TCP or UDP connection to any port, allowing the administrator to monitor unauthorised Telnet usage, for example.

String signatures enable the administrator to create custom signatures based around regular string expressions directed to or from specific ports, thus enabling a quick and dirty method of trapping viruses such as "ILOVEYOU" by watching for the offending string in packets destined for port 25.

Finally, *ACL* signatures are user-configurable attack signatures based on policy violations recorded by network devices in the syslog stream (which requires that your routers be configured to log ACL violations and the sensor be configured to accept syslog traffic from the router).

Creating IDS security policies is thus extremely straightforward in CSPM – the interface is simple, uncluttered, intuitive and very easy to use and there is rarely any need to refer to documentation. Applying them is simply a matter of clicking on the "*save & update*" button, at which point they are transferred to all Sensors that use that particular policy automatically.

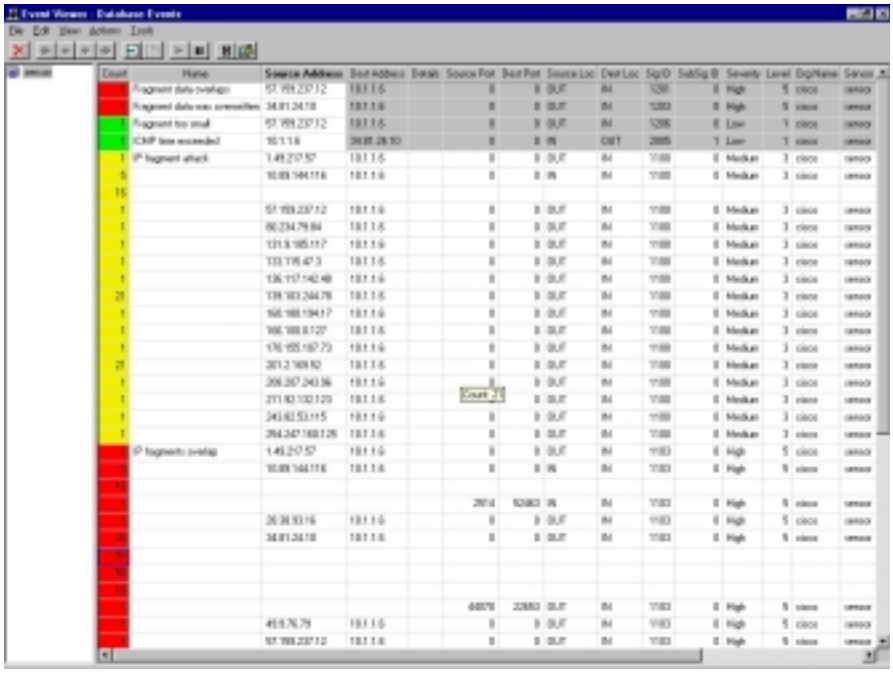

Figure 20 - Real-time alert console

As soon as a policy has been applied, the Sensor will begin sending alerts to the CSPM console that has been designated as its manager. The real-time alert console under CSPM provides instant notification of all alerts from all managed sensors.

It displays information such as date and time of attack, attack name, attack details and parameters used, source and destination address, source and destination port, attack ID and severity. Multiple occurrences of the same attack within a short period of time are consolidated into a single row with a count of the total number of occurrences against it.

Right clicking on a consolidated row brings up a context menu that can be used to expand the row showing the individual attacks if required. The same menu can be used to collapse rows, delete rows, add or remove columns from the display, and pull up detailed HTML-based attack information from the Cisco Network Security Database (NSDB). This provides instant access to specific information about the attack, hotlinks, and potential countermeasures. Because the NSDB is an HTML database, it can be personalised to a user to include operation-specific information such as response and escalation procedures for specific attacks.

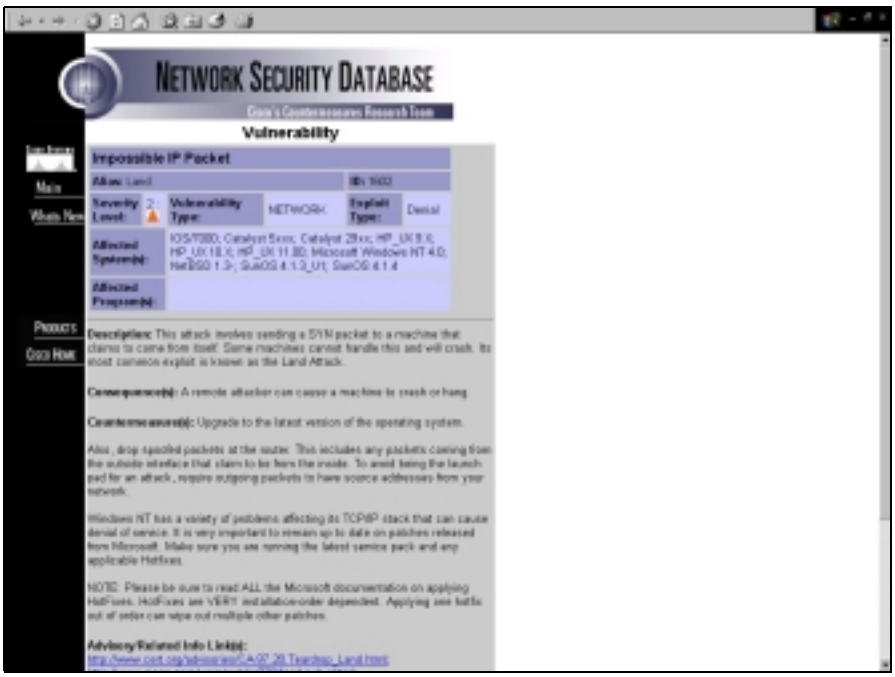

Figure 21 - Detailed information on attacks from the NSDB

The way the attacks are reported could be a little confusing for those that are not steeped in the dark arts of security lore. Eyebrows may have been raised at the mention above that there are just 300 attack signatures in the database, but this does not tell the whole tale. These are generic “group” signatures, each one covering one or more actual attack types. This means that Cisco Secure IDS is more likely to be able to spot new variants of old attacks without signature updates, but it does mean that the reported attack names are very non-specific. For example, our *Land* attack was reported as an “*Impossible IP Packet*” attack. Technically correct, of course, but not very specific for those who do not know their onions (or their impossible IP packets).

However, this has to be the way forward for the majority of IDS vendors. The difficulty of pattern matching packets against an ever-growing database of signatures in a reasonable (i.e. *very* small) amount of time means that a more generic approach to detecting attacks is required.

The advantage is a higher level of performance, fewer signature database updates required, and more chance that new variant of an old attack will be spotted immediately.

The main problem with the real-time alert console is not the general purpose attack names, but the fact that the rows can only be grouped according to the first column, and clicking on various column headings will only sort items within the overall first column groups. If you would like to see all the attacks from a particular IP address together, for instance, you need to drag the Source IP column to position number one in order to sort the table accordingly.

Bearing in mind that this is the only means that the administrator has to get IDS attack and alert information out of the CSPM database, it does need to be made as flexible and easy to use as possible. It would be far better to follow the standard Windows convention of simply allowing the user to sort unconditionally on **any** column by clicking on the column heading. Once this minor glitch has been fixed, the real-time alert console will prove to be an extremely useful tool.

Reporting and Analysis - netForensics

As with its predecessor, the latest version of the Cisco Secure IDS is completely devoid of any form of reporting and analysis or alerting capability. It has an excellent real-time monitoring capability at the console, and a basic log viewer to examine the log files (there is a log action that can be associated with individual signatures), but nothing more.

Some reporting will be built in to CSPM at some point in the future – as it has been already for PIX, for instance – but Cisco will continue to rely on partners for the heavy-duty stuff.

And heavy duty reporting, analysis and alerting for the Cisco Secure IDS is provided by netForensics.com with its *netForensics* product, a comprehensive security infrastructure management platform for network managers. It has been designed to collate information from multiple network services, such as firewalls, intrusion detection devices, web servers, routers, and authentication servers and present it in a style useful for executive management and security experts alike.

netForensics augments an enterprise-wide security system by providing an interactive and real-time interface that enables reporting, correlation, and forensics. The network manager can access this information from any browser on the intranet (via an authenticated session) and use this tool to quickly and easily sort through large volumes of raw information to focus on the high-risk threats. The key features of netForensics include:

- *Event Analyser - provides reporting and correlation analysis on the events and alarms generated by the various network devices and applications*
- *Alarm Console - provides a real-time status of the monitored devices with a detailed scrolling Alarm Viewer accessible from any Java-enabled browser*
- *Back-end Database - provides for historical trend analysis and archiving capability*

Devices that can be monitored and analysed by netForensics Version 2.0 include Cisco Secure IDS, Cisco PIX Firewall and AAA Server.

netForensics runs on Solaris or Linux platforms, and will shortly be appearing on NT. Three versions are available – *Lite*, *Workgroup* and *Service Provider* – each offering additional capacity, horsepower and facilities over the previous version, and software-only and appliance-based implementations can also be had. Looking at what is involved in getting the system running under Linux (although it is all documented in detail, and the documentation is excellent), we would tend to favour the appliance route.

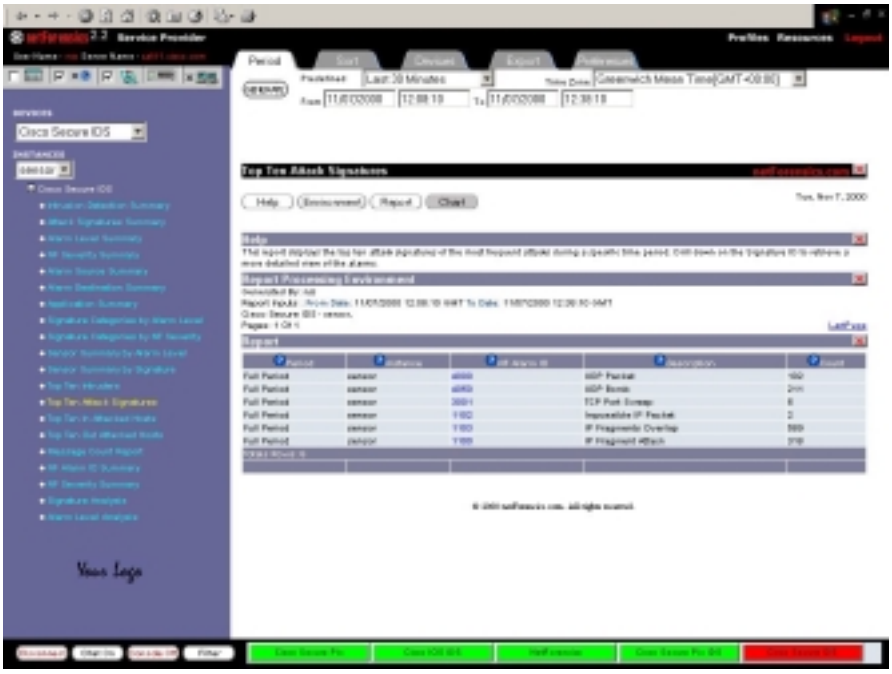

Figure 22 - Top Ten Attack Signature report

The high-end versions are based on Oracle, and access to the data is provided via an Apache Web server that makes a JDBC connection to the underlying database. This means that there is plenty of opportunity for customising the settings to tune the performance for different environments. netForensics can be configured on a single box for a workgroup-type of installation, handling up to 200 messages per second. Workgroups are defined as a maximum of five devices per workgroup.

netForensics components - the Oracle database, the Apache Web server and the netForensics engine - can also be distributed across multiple servers to increase the message handling capabilities up to five times the workgroup configurations. It can also be arrayed in a distributed hierarchical architecture to handle centralised management and monitoring of hundreds of security devices across an enterprise

Access to the reports and alerts is available to any machine on the network via a Java-enabled browser. Java is not usually our favourite user interface, being resource-hungry and all too often slow. However, the netForensics interface seems to have been well-designed and, apart from a lengthy delay when first attaching to the Web server, is very fast and easy to use.

The administrator is presented with a dual-pane display that does a very good job of emulating a Win32 application in appearance and operation. The left hand pane contains a hierarchical tree display with top-level headings of *Security*, *NFReports* and *Administration.*

The *Administration* menu allows you to manage sensor devices, alarms, events, user accounts, log files/databases and reports. Any number of user accounts can be created to authenticate to the netForensics server, and each one can be restricted to viewing certain devices – we had our administrator configured to only view Cisco Secure IDS sensors, for instance, which meant that the PIX and IOS devices did not show up on the report menus. The real-time console can be configured to filter and display only certain types and severity of alarms and events, and standard reports can be scheduled for regular repeating runs.

Notification methods can be configured from a choice of SNMP traps, pager and e-mail, and the Console can be configured to perform event aggregation, if required. This combines multiple events occurring within a specified time frame into a single line in the real-time Console, making them much easier to manage. By double clicking on any aggregated event, the line is expanded into the individual events for further examination.

Finally, netForensics can be configured to perform regular database housekeeping tasks, such as purging and archiving event records. Database backup and recovery, however, is initiated from the command line outside the netForensics environment.

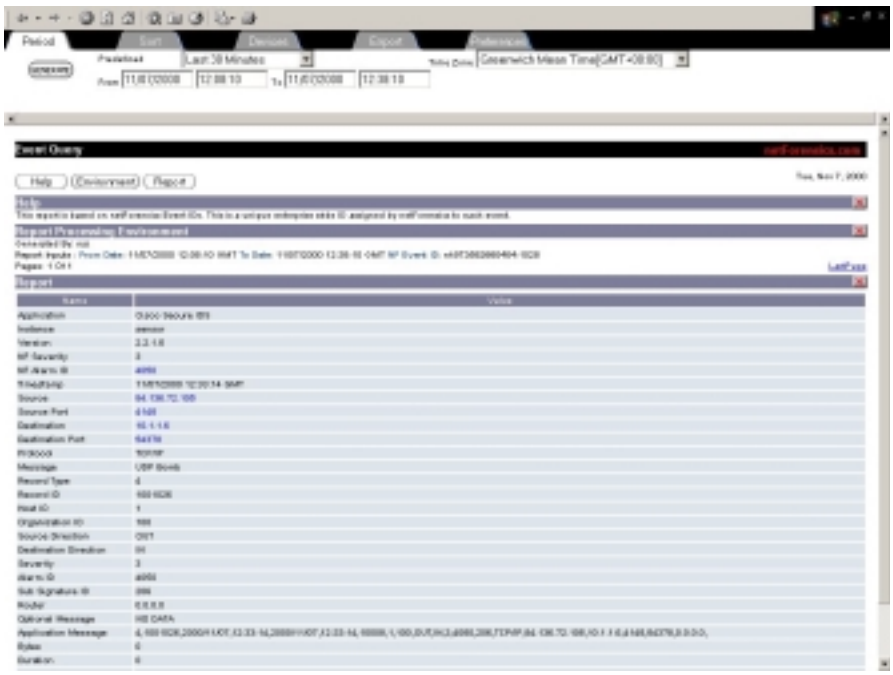

Figure 23 - Querying individual alert events

The NFReports menu contains a small number of reports which cover the events, alerts and messages specific to the netForensics server itself, whilst the Security menu contains reports of wider interest to the security administrator. In this section, there are sub-menus for each of the types of security device being monitored – PIX firewall, IOS device, IDS and so on.

Over 250 reports and summaries are available for Cisco Secure PIX Firewalls and Cisco Secure IDS. These target the needs of engineering, operations, senior management and forensic evidence gatherers.

Because we had restricted our administrator account to see only the Cisco Secure IDS devices, we only had the IDS reports available in this section. It is also possible to select a device-specific menu which will show only the reports available for a specific device (useful when many different device types and devices are being monitored from a single console).

Reports available for Cisco Secure IDS include:

- *Intrusion Detection Summary – takes events generated by Cisco Secure IDS and maps them the netForensics severity levels for reporting*
- *Attack Signatures Summary – high-level count of the various attack signatures seen by Cisco Secure IDS*
- *Alarm Level Summary – Cisco Secure IDS alarms summarised and displayed by alarm level*
- *NF Severity Summary – summary statistics displayed by netForensics severity levels*
- *Alarm Source Summary – summarises messages by source IP address and severity level*
- *Alarm Destination Summary – summarises messages by destination IP address and severity level*
- *Application Summary – lists severity of alarms by application (FTP, DNS, HTTP, etc.)*
- *Signature Categories by Alarm Level – displays alarms based on their signature category (IP header attack, Denial of Service, TCP header attack, etc.) along with their alarm level*
- *Signature Categories by NF Severity – displays alarms based on their signature category sorted by the netForensics severity level*
- *Sensor Summary by Alarm Level – summary of multiple IDS sensor devices with alarm levels and counts for each device*
- *Sensor Summary by Signature – summary of multiple IDS sensor devices with attack signatures and counts for each device*
- *Top Ten Intruders – lists the top ten host addresses of the most frequent intruders over a specified time period*
- *Top Ten Attack Signatures – lists the top ten attack signatures of the most frequent attacks over a specified time period*
- *Top Ten In Attacked Hosts – list the top ten IP addresses of hosts on the inside network that have received the most number of attacks coming from an outside host*
- *Top Ten Out Attacked Hosts – list the top ten IP addresses of hosts on the outside of the protected network that have received attacks coming from an inside host*
- *Signature Analysis – logs messages and counts by attack signature*
- *Alarm Level Analysis – logs messages and counts by alarm levels*

Unfortunately, it is not possible to add custom reports, but the range of reports available should be adequate for most uses. Each report has a number of settings including time period which should be covered (time and date), sort order, which devices should be included in the report and which columns should be included. Output can be as text or graphics, and in addition to the browser-based display, reports can also be exported as HTML files, PDF files, CSV files or XML.

All reports are normalised across different time zones, to ensure that the administrator running the report in London gets meaningful local times against events reported from a sensor in New York. This is an extremely useful capability for global operations.

Another very useful feature that minimises the need for the ability to define your own reports is the *drill-down* capability. When any report is run, certain key fields are highlighted as live hyperlinks. Clicking on any of these allows another level of report to be generated based on that particular item of data. For example, when running the *Top 10 Attacked Hosts* report, it is possible to click on the IP address of any host and generate a further drill-down report showing all attacks against that particular host. From there, you could select any source address, and generate another drill-down report showing all attacks emanating from that address.

This drill-down can continue indefinitely, allowing netForensics data to be "sliced and diced" in any number of different ways, and this is one of the product's most powerful and useful features. At any point where an attack signature is included in a report, it is also possible to select the signature ID and display in-depth details about that particular attack signature taken from the Cisco Network Security Database.

But it is not just historical reporting that can be performed with netForensics, since the product also provides a real-time Alarm Console that is capable of taking a feed directly from the IDS Sensor at the same time as the CSPM system.

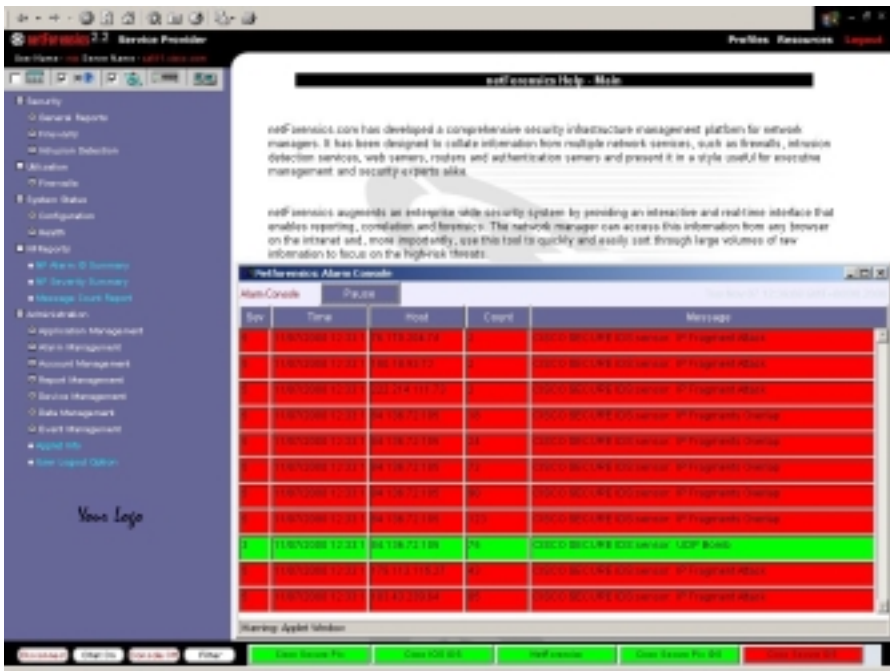

Figure 24 - netForensics real-time Alarm Console

Once an administrator has connected to an IDS device, a "traffic light" display along the bottom of the screen provides an instant indication of device status (*red* for alerts, *yellow* for warnings, *green* for normal), whilst the Alarm Console screen displays the individual events as they happen. This console is capable of handling 125 messages per second or, 10 million messages per day, and provides extensive filtering capability based on IP address, port numbers, message type, and device.

The Alarm Console shows a list of messages with time and date of attack, source IP address, count and attack signature. By default, one entry on the console corresponds to a single alert event, but when attack aggregation is turned on, netForensics consolidates multiple attacks of the same type within a specified time period into a single console entry, which makes it much easier to follow when many attacks are being recorded in a short space of time.

Double clicking on an individual entry presents the administrator with a detailed event query. Once again, key fields are offered as live hyperlinks for further drill-down if required.

The final feature of note is the real-time chat window, which allows administrators in different locations to communicate instantly about events they are viewing via the Console.

Verdict

Although the Cisco solution could be considered a little on the expensive side compared with some basic IDS products, this needs to be balanced against the fact that you get all the Sensor hardware and software included in the price. There is also a range of products available now, with different capabilities and at different price points. Taking this into account, along with the lower installation and ongoing maintenance costs provided by the appliance approach, the Cisco Secure IDS could actually work out to be an extremely cost-effective solution in the long run.

One of the biggest negative factors of previous releases – the reliance on HP OpenView for configuration and alerting – has been eliminated with the latest release. Although the HPOV plug-in is still available, the new Cisco Secure Policy Manager provides a more familiar (for many) Windows management and alerting environment with an extremely slick and intuitive interface. Installing and configuring Cisco Secure IDS Sensors is nothing if not straightforward.

As with previous incarnations, however, Cisco offers nothing in the way of alerting (other than to the CSPM Console) reporting and analysis, and prefers to work with partners in this area. If you are considering the Cisco offering as your IDS, you should consider budgeting for additional reporting products such as netForensics as reviewed here.

netForensics is an excellent tool for real-time monitoring, historical reporting and analysis, and alerting. Based on a robust Oracle database platform, netForensics provides a scalable solution with a range of options capable of managing a single device up to a complete enterprise. There is a wide range of reports available to cover all eventualities, and the drill-down capabilities make netForensics an extremely powerful and flexible offering.

It should also be borne in mind that it is capable of monitoring more than just IDS, providing a centralised means of reporting across all your Cisco security devices.

Most sites will need to seriously consider the acquisition of some form of third-party monitoring and reporting tool to go with Cisco Secure IDS – even if they are monitoring a single device, managing even an average number of alerts can be daunting, but with an entire network of devices to manage some additional help will almost definitely be required. If this should prove to be the case, netForensics is well worth a look.

Contact Details

Company name: Cisco Systems, Inc.

Internet: www.cisco.com

Address:
San Jose World Headquarters
170 West Tasman Drive
San Jose, CA 95134-1619
USA

Tel: +1 408 526 4000

Cisco Systems
3, The Square
Stockley Park
Uxbridge
UB11 1BN
England

Tel: +44 (0)20 8756 8000

Company name: netForensics.com, Inc.

Internet: www.netForensics.com

Address:
200 Metroplex Drive
Edison
New Jersey 08817
USA

Tel: +1 732-393-6000

CYBERSAFE CENTRAX 2.4

CyberSafe Centrax is probably one of the most complete solutions we have looked at as part of this test, in that it includes audit policy control, Host-based IDS (with both real-time and batch policies), Network-based IDS, Network Node IDS and even basic Vulnerability Assessment.

The Command Console runs on Windows NT/2000 and target agents are available for Microsoft Windows NT 3.51 and 4.0, Windows 2000, Sun Solaris 2.5.1, 2.6, 7 and 8, HP-UX 10.2 and 11.0, and IBM AIX 4.2.1 and 4.3.2.

Architecture

Centrax comprises a central ***Command Console*** which controls a number of ***Target Agents***.

The Command Console is used to define security policy and control the remote Target Agents, as well as to monitor and respond to real-time alerts raised by the Agents. The Console also controls vulnerability assessments of the Targets, how often log files are collected, and how frequently reports are run.

The Command Console consists of three parts: the GUI, the collection engine, and the detection engine. The graphical user interface is used to manage all aspects of the Command Console and to communicate with the clients. The collection engine receives all files from the target agents and forwards them to the detection engine. The detection engine analyses the audit data, populates the database and archives off the original audit data

Target Agents are the “business-end” of Centrax, the bits that do the actual monitoring and alerting. Where Centrax scores is in its provision of a wide range of Target Agents, including both host-based and network-based, and when Agents are first installed they become immediately active with a default security policy. Audit data is reduced based on pattern matches of detected activity signatures and then stored in a database for later analysis and reporting.

There are two types of host-based Agents – *Batch-Mode* and *Real-Time*. Batch-Mode Agents collect data and store it at the target host for periodic collection by the Command Console, and parsing of the data is not performed until it is has been collected from the target. Real-Time Agents, on the other hand, perform the same host-based functions but report anomalies and alerts back to the Command Console immediately. This arrangement provides a much more scalable solution than many Host-IDS systems.

For instance, many host-based systems are typically reactive, in that they store data to be analysed at a later date, by which time it may be too late to do anything about it. However, if you want to do everything in real time, you run the risk of overloading both the host itself and the subnet on which it resides. Centrax provides the perfect balance. Both Batch-Mode and Real-Time Agents can use identical policies, allowing them to monitor the same events. However, by splitting the functionality, it is possible to have a small, manageable policy for real-time alerting – monitoring only the most critical events – and a much larger Batch-Mode policy that can collect all the data necessary for forensic investigation at a later date.

There are also two types of network targets – *Network* and *Network Node* which broadly follow the functionality description from the Introduction. Network Agents work in promiscuous mode, monitoring all traffic on a particular network segment (and generally require a dedicated machine on which to run), whilst Network Node Agents monitor traffic specific to a particular server or workstation as it arrives at that host's network card. Both network Agents send alerts directly back to the Command Console for processing.

Centrax uses TCP/IP to communicate between the Command Console and Target Agents. All transmissions of audit policies, collection policies and counter-measure responses between the Console and Agents are encrypted using DES or Triple-DES.

Installation

Installation of Centrax is remarkably easy. Starting off with the Command Console, it is the usual "put in the CD and go" type of Windows installation. After that it gets quite clever. From the Command Console GUI the administrator can create "Target installations" on the Console machine, which can then be shared via Windows Explorer.

All that is then required to install the Target Agents is to access the share from the target host and run the SETUP program. Unix installations are performed in a similar way, usually by copying the install directory created at the console to the target and running setup.sh. Of course, it is also possible to use the installation CD to install remote detectors too, but the share method is a nice idea. It would be even nicer if it was possible to push the Agent installation from the Console to the remote hosts, which would offer a much more scalable approach to deployment in large, distributed networks. Apparently, CyberSafe is working on such an approach for the next release, whilst in the mean time the product is integrated with Microsoft's SMS to assist in distribution.

When running SETUP at the remote host, choices are offered as to which Agent (or Agents) is to be installed – Batch, Real-Time or Network. Installing Real-Time also forces an install of the Batch Agent, since that is used to perform the actual event collection. Installation of the Network Agent forces an install of all three components, since the Real-Time Agent is used by the Network Agent for alerting purposes. The same Network Agent is used for Network and Network Node operation, and the choice of which mode is employed is determined from the Command Console.

We installed the Agents on Windows 2000 platforms, and so didn't even need to reboot once we had finished – very impressive.

Configuration

The Command Console provides the interface to communicate with the remote target agents, the detection engine and a view into the database.

The GUI provides editors to define the different policies available to Centrax. These different policies define the both how host operating system will gather information and how Centrax will migrate and process that information.

To the uninitiated, Centrax can appear complicated thanks to the bewildering array of policies that it is possible – and necessary – to define. The Console GUI provides three panes when started. The top window is the Alert Manager, which is used to display all batch, real-time, network and network node alerts. Columns for each alert display the Priority, Alert Type, User or Source IP Address, Activity ID, Date, Description and Details of the alert. Alert filters can be defined in order to reduce the amount of information displayed in this window if required.

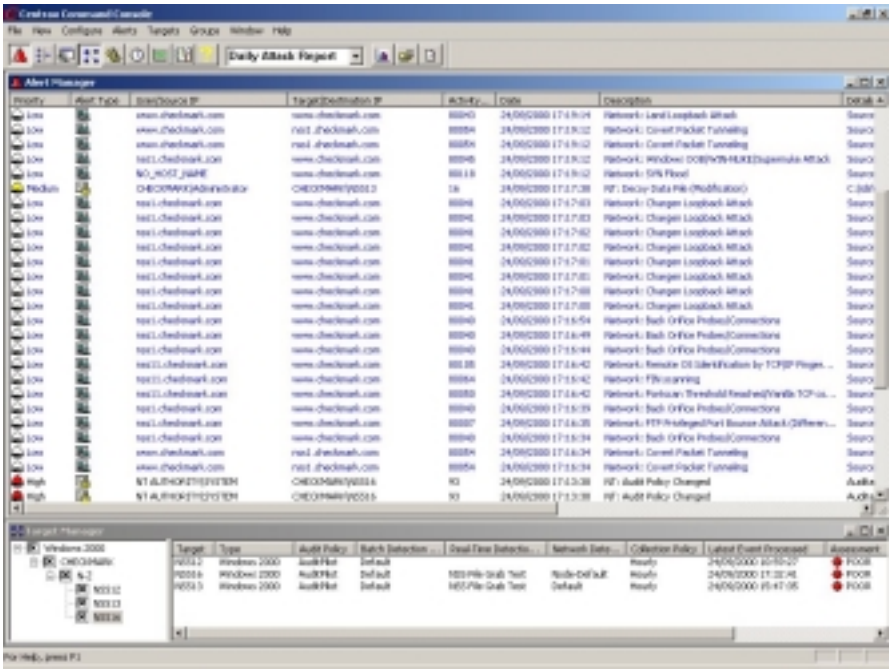

Figure 25 - The main Centrax console

Double-clicking an alert message brings up additional information which is limited to a brief description of the problem and three possible solutions, labelled Critical, Concerned and Cautious. These often turn out to offer almost the same advice for each category, and in many cases are not as helpful as they might be. For instance, when bringing up the extra information window for one particular type of DoS attack, all the advice it could offer was “watch out for excessive ACK packets” – no explanation of what they signify or how to avoid them.

The bottom window is the Target Manager, split into two panes and showing which machines are being monitored and their current configuration. The left hand pane is a hierarchical tree view of the Target Agents sorted by operating system, domain/workgroup and machine name. Targets can be grouped together logically using this window, and check boxes at each level of the tree allow the administrator to quickly and easily focus on groups of machines or individuals, which are then displayed as a list in the right hand pane.

This list shows each target, along with the policies that have been applied, the date and time of the last event processed, and the current assessment status. It is the number of possible policies that can be confusing to the uninitiated.

Policy Definition

The first, and possibly most important, is the **Audit Policy**. Audit Policies define which user and system activities are recorded in the security event log. The great thing about Centrax is that it provides the only sensible means for managing audit policies across an enterprise-wide network. In the NT world, for example, you can imagine the amount of work involved in specifying, applying and maintaining audit policies across every machine in the company. NT simply does not provide any centralised means of doing this, and so the administrator is faced with the task of accessing each and every machine individually in order to apply the appropriate audit parameters. The potential for error when trying to apply a single policy across an organisation is very real.

Centrax allows one or more audit policies to be defined in the Command Console and then applied in a single stroke across the entire organisation, or across groups of machines as defined in the Target Manager. Audit Policies can be defined for AIX, HP-UX, NT and Solaris, and a number of sample policies are provided covering Administrative Activity, File Browsing, Computer Access, Hacking Attempts, and so on.

When creating audit policies, the policy definition screens are identical in look and feel to the native NT audit dialogues – covering auditable events (logon/logoff, file and object access, security policy changes, etc), individual file auditing, and registry key auditing, thus making them easy to get to grips with. Naturally, slightly different settings are available for the Unix environments. In the NT world, the NT security event log is used to store audited events, whereas in the Unix world, the usual insecure syslog mechanism is replaced by a secure binary C2 audit trail. Policies can also be merged, making it easy to group sets of audit requirements together into a single policy.

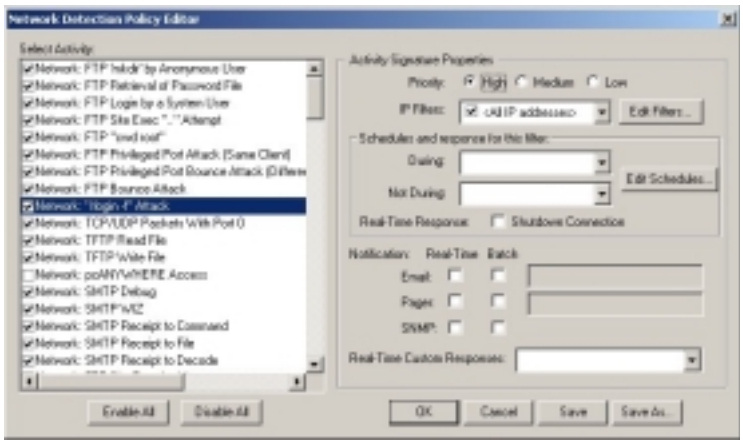

Figure 26 - Configuring network detection policies

Closely related to the Audit Policy is the **Detection Policy**. This policy defines rules by which the Detection Engine will scan the raw audit trails in order to determine what constitutes an alert. It is important to note the distinction between Audit and Detection policies in terms of the information they process. In an extreme case, for instance, an administrator could ask the OS to audit absolutely every event, thus creating a complete (and incredibly cumbersome) audit trail for forensic purposes.

The Detection engine then filters and reduces that audit trail to individual attack or misuse alerts as defined in the Detection Policy.

The advantage of this approach is that should an alert be raised, it is possible for the administrator to dig deeper into the full audit trail in order to provide more information about the attack. This makes Centrax a good tool for forensic examinations.

Once again, a number of sample detection policies are available for each OS platform, and these are split into **Batch** and **Real-Time** policies. This is another advantage of Centrax, since although the same options are available for the two types of policy, it is possible to specify a comprehensive detection policy to run in batch mode - thus reducing the load on the target host and on the network - whilst ensuring that a smaller subset of critical events are reported in real time. Note that it is possible for each Target Agent to have either a Batch policy or a Real-Time policy applied to it, or both – or even neither of them, if required.

A huge number of pre-defined activities (over 800) are available for each type of detection policy (i.e. to monitor access to individual files, to monitor failed logon attempts, to monitor administrative access, and so on), and it is possible to define your own custom events, though this entails editing of cryptic text files. The procedure is well documented, but it would be nice to see a GUI custom event editor added to the package. Against each event is a set of Activity Signature Properties, classifying the event as High, Medium or Low priority, and determining the system response should that event be detected.

Built-in responses are limited to logging off the user, logging off and disabling the account, and running a TripWire scan (if TripWire is installed on the target host) to check that no files have been altered. Custom responses can be created if required – perhaps running a script to trigger a batch run of an anti-virus scanner. It is also possible to specify a notification option, choosing from e-mail, pager or SNMP trap.

A group of activity events can be selected and saved as part of a custom-designed detection policy, or one of the pre-defined sample policies can be selected and applied,

It is worth noting that in order for the Detection Engine to do its work, it needs the raw security events to be logged initially, and this means the audit policy has to ensure the correct events are logged. Since not all administrators are familiar enough with the auditing process to make sure this happens, the usual approach would be to “audit everything” just to be on the safe side. For this reason, CyberSafe has introduced a special audit policy called *AuditPilot*. AuditPilot works backwards from the detection policy and automatically creates the correct audit policy to provide all the necessary raw audit events. This completely removes the burden of defining effective audit policies from the shoulders of the administrator.

Of course, Centrax is a Network IDS as well as a Host IDS, so there are **Network** detection policies too, which can be applied to all Target hosts with the Network Agent installed. The events in here cover the more typical NIDS territory such as alerts for certain DoS attacks, FTP password grabbing, Web phf attacks, CGI scans, BackOrifice scans, and so on. Though the common ones are covered, Centrax has a much more limited attack signature database than the more specialised NIDS. New signatures cannot be added by the administrator, the only modification possible to a Network policy being the ability to enable or disable each signature check.

Once again, it is possible to select a subset of the available signatures and create new custom policies, and individual or groups of signatures can be restricted to certain address ranges (perhaps you are not interested in checking for CGI scans from your internal network, for example). An additional response has also been added to network policies – the ability to tear down a connection.

Target Agents can be designated as **Network** or **Network Node** agents. The same Agent is used for each operation, and the distinction is made from the Command Console. It is recommended that promiscuous-mode Network Agents are on a dedicated host, for performance reasons.

The final policy is the **Collection Policy**. As its name implies, the Collection Policy defines how data from the Target Agents is retrieved by the Collection Service. In reality each Target Agent sends its data in a push type manner, which is generated from either a request from the Command Console GUI or from the Collection Policy.

The Target Agent communicates with the Collection Service through a 56 bit DES or 168 bit Triple-DES encrypted channel. The secret key is generated when the Command Console is first installed, and that key is pushed out to the Target Agent when it is installed.

The Collection Service receives files from the Target Agent and stores them in the Collection directory, where they are processed by the Detection Engine with respect to the Detection Policy, looking for suspicious activity.

Vulnerability Assessment

As well as the Detection policies, Centrax also includes some basic security assessment capabilities, providing an indication of where your security policies need tightening up.

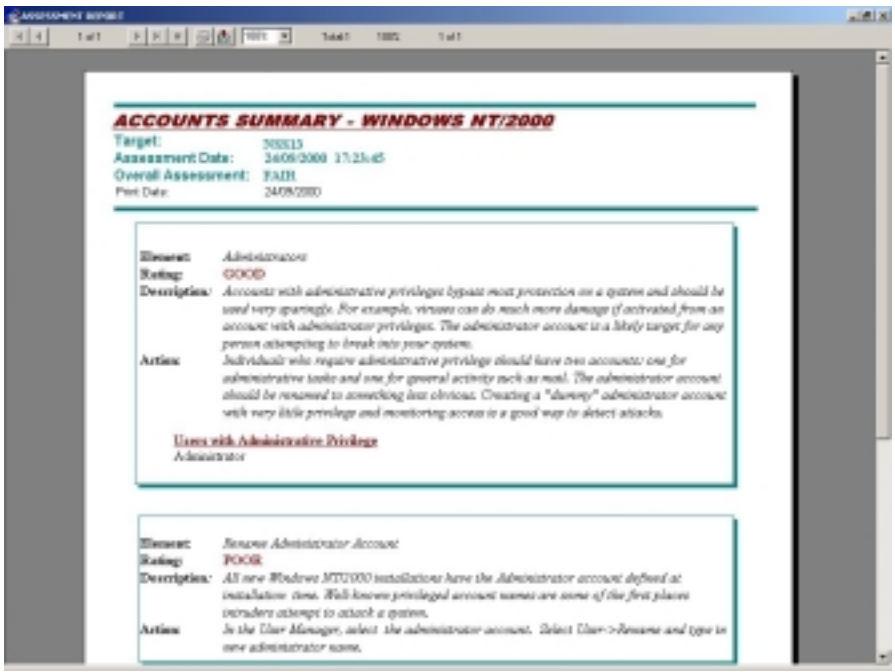

Figure 27 - Vulnerability assessment report

For instance, you are rated as *Poor*, *Fair* or *Good* in a number of categories (posture, login configuration, drive configuration, passwords, screen savers, accounts and system configuration) depending on such things as how long your default passwords are, whether you have a guest account enabled, whether you have renamed your administrator account, whether you allow all users to access the NT system directory, and so on.

Security Assessments can be scheduled for regular runs, allowing administrators to keep on top of new and existing machines and monitor how their security posture changes over time.

In addition to a simple on-screen “traffic light” display (red for poor, yellow for fair, and green for good) of security assessments, it is possible to run detailed reports against individual hosts which provide extensive information on the vulnerabilities found and how to fix them. An Enterprise Assessment Report pulls together a summary of all machines that have had assessments run against them.

It should be remembered that this is a fairly basic assessment tool, and not in the same league as more specialised offerings from ISS and NAI. It concentrates more on operating system settings relating to security posture rather than the more extensive “hacker in a box” approach. However, the inclusion of such functionality in an intrusion detection package should be seen as a definite bonus, and the simplicity this feature will certainly mean it will be used regularly, helping to enforce security policy across an organisation.

Policy Application

Once the Command Console has been started, it will automatically display all host machines that have a Target Agent installed, each of which will have a default detection policy applied and running automatically at install time. By right-clicking individual Targets or groups of Targets it is possible to apply Audit, Detection and Collection policies to each target as required. Policies are selected from a drop-down menu of available policies which have been previously defined, and it is also possible to select no policy if required.

Once policies have been applied in this way, real-time alerts will appear in the Alert Manager window as soon as they are detected. Alerts extracted from the Batch detection policies are displayed in the Alert Manager window when they are collected by the Collection Service at intervals defined by the Collection Policy. It is also possible to force an immediate collection from one or more Target Agents, as well as trigger an immediate assessment.

One nice feature – of the utmost importance in large-scale enterprise-wide deployments – is that whenever a source policy is amended in the Command Console, Centrax will examine all Target Agents to see which ones have that policy applied. It will then provide the option to have the new policy applied automatically to all the appropriate Targets – if only all IDS worked that way.

Scheduler

The Scheduler service provides the means for the administrator to force a number of events to be run at regular intervals:

- **Assessment** – run regular vulnerability assessments to track security posture over time
- **Audit Policy** – reapply audit policies at regular intervals to ensure that all Targets have the most up-to-date policies
- **Report** - have suspicious activity reports run overnight and written to disk or sent to the printer
- **TripWire scan** – for sites with TripWire installed, this option will force file integrity checks to be run as specified intervals.

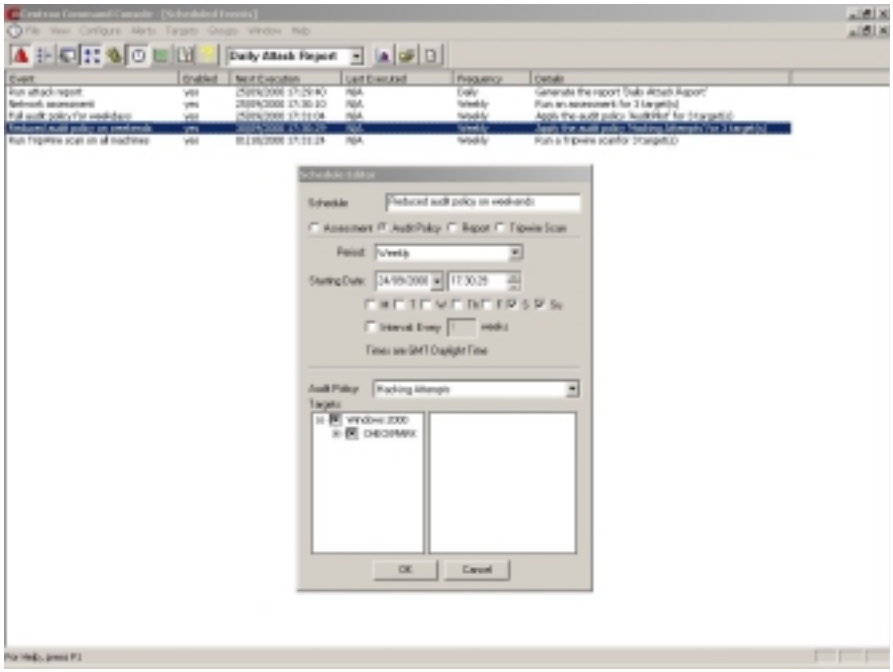

Figure 28 - Scheduling regular Audit Policy changes

For each type of event, it is possible to restrict the scheduled operation to a single Target, a group of Targets or apply the event to all Targets.

Reporting and Analysis

Bearing in mind the volume of information that can be collected by Centrax, it is important to be able to filter and report on this in an intelligent manner. The ubiquitous Crystal Reports provides the reporting engine.

A number of predefined reports are available, and these can be filtered by Target Agent or by individual users, and run for a specific data range. An “Advanced” tab provides a list of all available attack signatures and events, allowing the administrator to home in on particular type of suspicious activity.

Output can be to the screen, printer or disk file, and disk file output can be in a range of formats, including plain text, Microsoft Word or HTML.

The latter option would allow reports scheduled overnight to be published directly to an internal Web site for access by a number of users if required. Once all the report parameters have been selected, they can be saved as a report template, which can then be run from a drop-down menu of available reports in the main Command Consol GUI.

Figure 29 - Network Activity report

Completed report templates can be run regularly by adding them to the Scheduler service, and a number of data management tools are provided for housekeeping and archiving of data.

Verdict

At first sight, Centrax can appear to be complex product with a less-than-intuitive interface. However, it is worth getting to grips with that complexity for the power it offers the administrator in providing Intrusion Detection cover for the largest organisation. In fact, one of the nicest features is the fact that once the various policies have been defined, the Collection and Scheduler services will automate most of the day to day tasks, providing a system that virtually runs itself – Centrax refers to this as “hands-free IDS”.

Its most powerful features are clearly in the areas of Host IDS and audit policy management across an enterprise, and with the latter feature Centrax has a unique and valuable advantage over its competitors. The ability to create and deploy audit, IDS and Vulnerability Assessment policies across a corporate network from a single, central location is incredibly useful. This centralised management, plus a combined real-time and “store and forward” architecture for host-based alerts, also makes it very scalable.

It is less strong in the area of Network IDS, where it currently offers a fairly limited range of signatures, and the Vulnerability Assessment capability is best thought of as a “bonus”. In its present incarnation, you would certainly not purchase Centrax solely as a Network IDS product – although this feature is improving quickly with each new release, it still has some way to go.

On the other hand, take a look at the top Network IDS products – how many of those include Host IDS and Vulnerability Assessment products out of the box? They are usually provided as completely separate offerings.

If your main concern is to protect your network from the infamous “70 per cent of attacks which are internal” that is regularly reported by the FBI, then Centrax is a powerful and flexible product, with advanced Host IDS and Audit Policy management capabilities.

Contact Details

Company name: CyberSafe Corporation

E-mail: sales_center@cybersafe.com

Internet: www.cybersafe.com

Address:
1605 NW Sammamish Road
Issaquah
WA 98027-5378
USA

Tel: +1 425-391-6000
Fax: +1 425-391-0508

For additional contact details, see the CyberSafe Web site at http://www.cybersafe.com/company/contact.html

ISS REALSECURE 5.0

ISS was one of the first to produce a commercial Network Intrusion Detection System and RealSecure still tends to be the standard by which other NIDS products are measured.

Architecture

RealSecure 5.0 consists of the following components:

- **Workgroup Manager -** The Graphical User Interface (GUI) and the collected database from the sensors. This includes the RealSecure Console.
- **Console -** The central controlling point for the Sensors. The Console maintains a master database from which reports can be run, and it manages the Sensors deployed across the intranet.
- **Network Sensor -** This Sensor runs on a network segment, analysing the traffic flow and looking for intrusions and signs of network abuse. When an intrusion is detected, RealSecure can respond in a number of ways, including:
  - *recording the date, time, source, and target of the event*
  - *recording the content of the event*
  - *notifying the network administrator*
  - *reconfiguring the firewall*
  - *terminating the event automatically*
- **OS Sensor -** This Sensor runs on a crucial computer system, monitoring user and administrator activity and watching for signs of improper system use or suspicious behaviour which might indicate an attacker has gained access. When an intrusion is detected, RealSecure can respond in the following ways:
  - *suspend the account*
  - *disable the account*
  - *send a text message to the intruder with a warning that an intrusion has been detected*
- **RealSecure Manager for HP OpenView 1.3 for NT -** This product allows control of RealSecure Network Sensors with HP OpenView. This is an optional product.
- **RealSecure Manager for HP OpenView 1.0 for Unix -** This product allows control of RealSecure Network Sensors with HP OpenView. This is an optional product.
- **RealSecure Manager Plus for Tivoli -** This product allows control of RealSecure Sensors with Tivoli TES desktop. This is an optional product.

Communications between the console and engines are fully authenticated and encrypted, and RealSecure will automatically lock down the Real-Secure-specific portions of the NT Registry to prevent the installation from being compromised in any way.

Please note that this review concentrates only on the *Workgroup Manager* and *Network Sensor* components.

By the time this report is published, *RealSecure 5.5* will be available, the most noteworthy enhancement being the addition of a *Network Node IDS* component (known as the *Server Sensor*).

Installation

Installation is very straightforward on the NT platform (the only platform we tested), with separate sub-directories on the CD for the Console and various Sensors. In an ideal world, the Console and Network Sensors should have dedicated machines (a combined Console and Network Sensor machine can be installed for evaluation purposes), whilst the OS Sensors can obviously be installed on any existing server. The Microsoft Database Access Components (MDAC) 2.5 and Internet Explorer 4.0 (required for the Help system) need to be installed on the Console machine if they are not already there.

On all Sensor hosts, the ISS daemon is automatically installed as a Windows NT service or Unix daemon during installation. The daemon accepts commands from the Console and manages the Sensor. The output from the Sensor is directed to the appropriate log handlers. After a Sensor has been installed on a remote system, it is necessary to copy one or more of the Console's public authentication keys to that system before the Sensor and Console can communicate over a secure channel.

Great care needs to be taken when sizing the machine for the Network Sensor, since the number and power of the CPU's and amount of available RAM can have a huge effect on the detection rate. A dedicated host is a must, and ISS recommends a minimum specification of Pentium II 300MHz with 256MB RAM – our advice would simply be to install the biggest and most powerful host with as many processors and as much RAM as you can afford if you are running RealSecure Network Sensor, since it is much more dependent on the power of the host than other products we have tested.

The OS Sensor is a lightweight application, typically using 5 MB RAM and less than one per cent of the available CPU, since it is designed to reside on servers that are also being used for other tasks. The OS Sensor will run on NT 4.0 Server or Workstation Solaris SPARC 2.5.1, 2.6 and 7, IBM AIX 4.3.2 or 4.3.3, and HP-UX 11.0.

Documentation is excellent – provided only as PDF files – and includes a *Getting Started Guide*, plus separate *User Guides* for the Console, Network Sensor and OS Sensor, and an excellent guide to the available signatures, with plenty of detailed information on what each attack is, and how it can be protected against. ISS also runs a range of excellent training courses on its products – including RealSecure.

Configuration

The Console consists of several windows, all of which display different types of information and provide access to different functions:

- *Main banner and toolbar*
- *High, Medium and Low Priority Alert windows*
- *Activity Tree window*
- *Sensor window*

These are arranged in a default layout on starting RealSecure, and can be rearranged, activated or deactivated by clicking on menu entries or toolbar buttons.

To monitor a Network or OS Sensor, an entry must be made in the Sensor window. A single Sensor can report to multiple Consoles at the same time, although only one Console is granted “master status”, which allows it to make changes to the Sensor’s configuration. Obviously, a single Console can also monitor multiple Sensors at the same time. However, one annoying problem in the current version of RealSecure is that each time you exit and restart the Console (which is necessary to clear the Activity Tree window, believe it or not) the list of Sensors is cleared. For an administrator whose job it is to monitor tens or hundreds of Sensors, this can be more than a little frustrating.

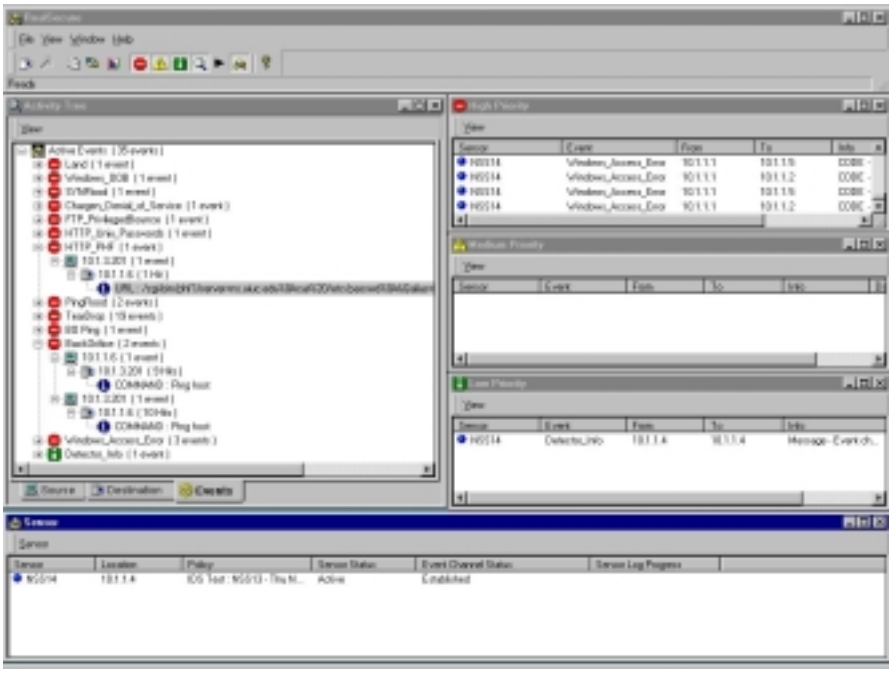

Figure 30 - The RealSecure console

Right clicking on a particular Sensor allows access to a configuration menu. The most important configuration task is to assign a security policy, and eight default – and fixed – policies are provided with the system:

- *Maximum Coverage*
- *Attack Detector*
- *DMZ Engine*
- *Engine Inside Firewall*
- *For Windows Networks*
- *Protocol Analyser*
- *Session Recorder*
- *Web Watcher*

Most administrators will select one of the first two for safety, but this is not such a good idea on a heavily loaded network. RealSecure is a great hogger of resources and cannot handle a heavy network load on a 100Mbps segment when monitoring all attacks. Some thought thus needs to go into defining realistic policies that watch for a subset of the available attack signatures.

Policy definition is certainly one area where RealSecure scores over many of its rivals. Select one of the existing policies and click on "*Derive New Policy*", give it a name, and you are free to create your own policy using that as a template. There are four tabs on the policy definition screen:

- *Security Events*
- *Connection Events*
- *User Defined Events*
- *Filters*

The *Security Events* tab lists all the available attacks in the signature database, and these can be enabled or disabled by clicking on a check box next to each one.

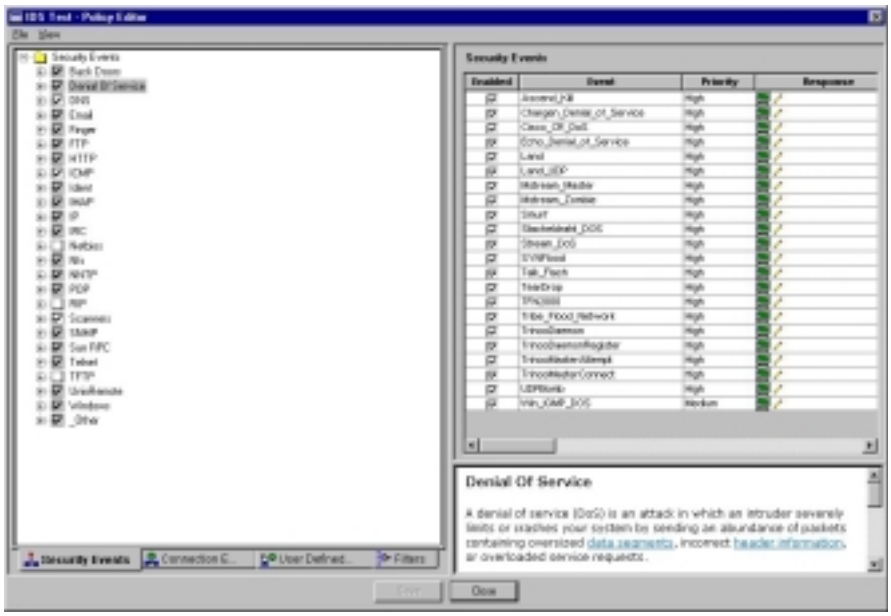

Figure 31 - Defining security policies

Selecting an individual attack brings up a detailed description of the attack (including its effect and how to counteract it) and a configuration screen. There is a wide range of attacks available, and new ones are added at regular intervals through the efforts of the ISS X-Force team. The Web-based update procedure is very straightforward and easy to use, and allows the administrator to download new signature files to the network and update individual RealSecure installations from those (the new signatures cannot be applied across the network, however, it is necessary to visit each Console to do it).

The attack priority determines in which of the three Priority Alert windows it will appear, and for each event there are a number of responses available. These include:

- *Notify console*
- *Log to database*
- *Log raw data*
- *Send e-mail notification*
- *Kill connection*
- *View session*
- *Lock firewall*
- *Send an SNMP trap*

Kill connection resets the IP connection to terminate the attack immediately, whilst the lock firewall option works with Checkpoint's FireWall-1 to automatically reconfigure the firewall to prevent further attacks. Responses can be set globally for the policy, and then overridden on individual signatures if required.

There is also an Advanced properties screen that provides the means to edit any additional parameters that might apply to a specific attack signature, as well as define how multiple events should be handled and propagated from Sensor to Console (rapidly occurring attacks can be consolidated into a single alert to prevent network floods)

RealSecure can be used to monitor more than just security problems by using the *Connection Events*. These are generic events such as HTTP, FTP or SMTP activities, and can be filtered by source or destinations address, source or destination port, or protocol. One possible example of how this could be used would be if the administrator suspected certain employees of playing network Doom in company time. RealSecure could be configured to monitor for TCP port 666 and log the source and destination addresses of the perpetrators, perhaps killing the process too.

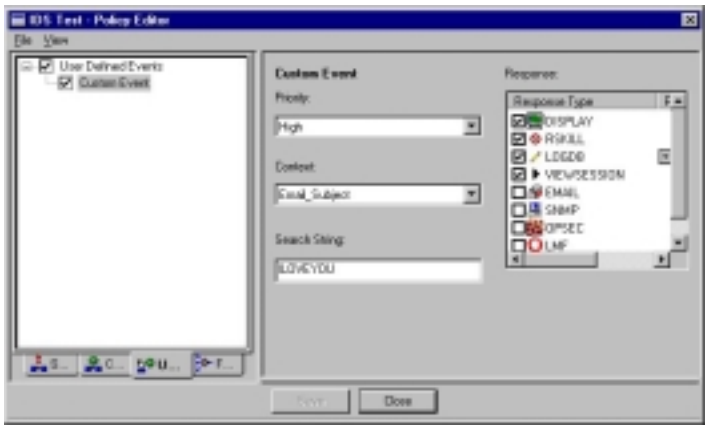

Figure 32 – RealSecure allows user-defined signatures

User-defined signatures allow the administrator to apply regular expression string matching on certain fields within a packet (login name, URL data, e-mail subject, etc.) to determine suspicious content. We used this as a "quick and dirty" virus checker by creating a signature that raised an alert every time it saw a packet with an e-mail subject containing the string "ILOVEYOU".

Finally, if there are genuine events which are raising false alarms via RealSecure, the Filter tab allows the administrator to define which packets should be ignored for alerting purposes, based on protocol, port or IP address.

Once policies have been defined at the console they are applied to each engine as appropriate. Different policies can be applied to each engine, if required, depending on the expected traffic on any given segment, or perhaps depending on the importance of a segment. Unfortunately, having made changes to an existing policy it is left to the administrator to locate the Sensors that are using that policy and apply the changes to each one individually. It would be nice if RealSecure could operate in the same way as CyberSafe Centrax and inform the administrator of all the Sensors affected by the changes that have been made, and offer to apply those changes automatically.

Once a Sensor is up and running with a policy applied, alerts are logged locally on the Sensor and transmitted in real time to the Console, where they are displayed in the Low, Medium or High priority Alert windows depending on their assigned severity level. Sensor log files can be synchronised with the Console logs at regular intervals for permanent storage.

Events are also displayed in the hierarchical Activity Tree window, sorted and grouped by source address, destination address, or event description. Expanding the branches of the tree allows the administrator to drill down for more detail, and the Event Inspector window displays complete details of individual events, showing source and destination addresses, packet contents and actions taken. The session playback facility allows recorded sessions (recorded as a result of the appropriate action being set on an attack signature) to be replayed and viewed in real-time or packet by packet.

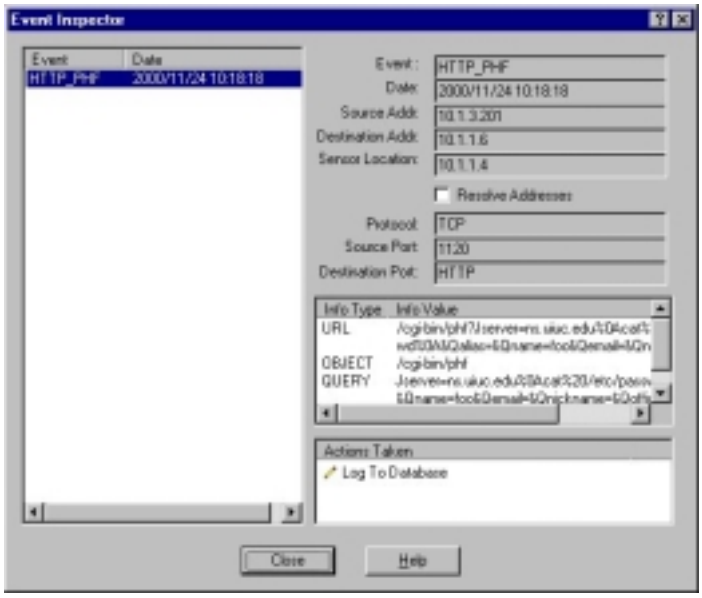

Figure 33 - Inspecting individual events

Unfortunately, if you want to clear the Activity Tree window, the only way to do this is to close down and restart the RealSecure Console, and this necessitates reselecting all the Sensors to be monitored – highly inconvenient.

There are also some other rough edges to the user interface where some standard Windows conventions are not followed – there are no maximise/minimise window buttons when defining policies, for instance, and there is inconsistent use of right-clicking and double-clicking in some places. The interface requires some tidying up.

Reporting and Analysis

After Sensor logs have been synchronised and uploaded to the Console log (the Console log consolidates log files from all Sensors that report to it), the administrator can generate a number of text and graphical reports that summarise network activity. These reports essentially record the date, time, source and target of attacks.

There are a number of built-in reports available:

- **Common reports:**
  - Event Name - Lists details of events sorted by event name.
  - Event Priority - Lists details of events sorted by priority first, then by time.
  - Destination IP - Lists details of events sorted first by destination IP address, then by time. Allows examination of network events sorted by the hosts that were the targets of the events.
  - Top 20 Events - Graphs the top 20 event occurrences.
  - Top 20 Destinations - Graphs the top 20 IP destinations, ranked by the number of events associated with each address.
  - Event Priority Frequency Graph - Graphs the number of high, medium, and low risk intrusion events that were detected over the specified time frame.
- **OS Sensor Reports:**
  - Login/Logout History - Shows login, logout, shutdown, and restart events. The data is sorted by computer and user.
  - NT Admin Activity - Shows all NT administrative activity events. The data is sorted by computer and user.
  - Unix Syslog Monitoring - Shows Unix syslog events. The data is sorted by computer.
  - User Activity - Shows all user activity. The data is sorted by computer and user.
  - Suspect Connections - Graphs the number of suspicious connections for each computer.

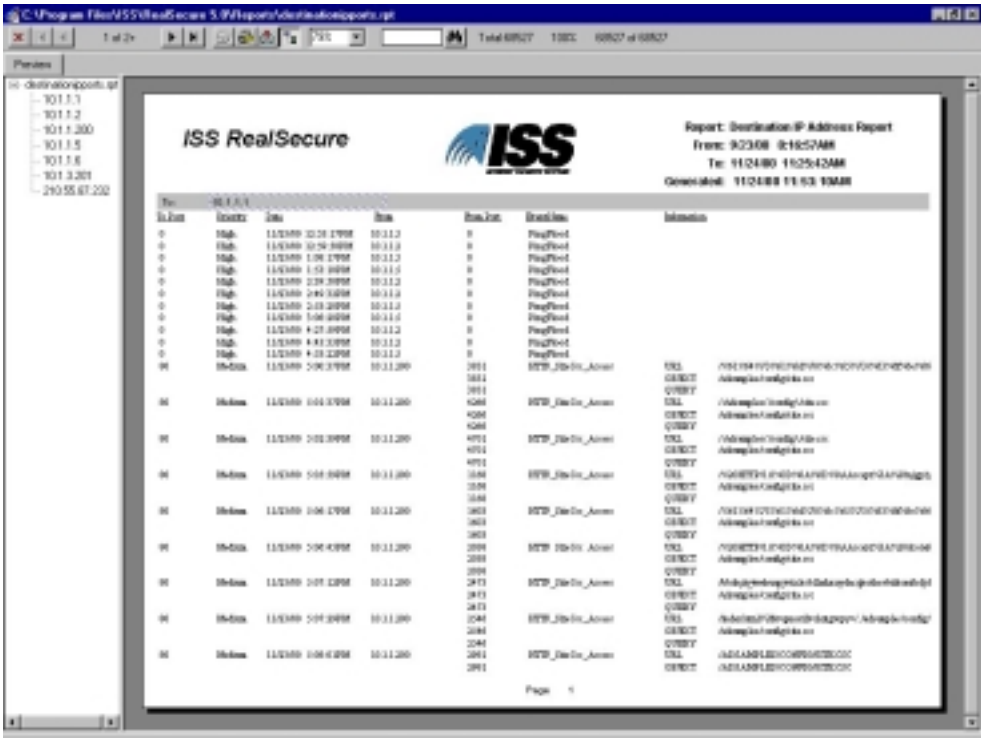

Figure 34 - Viewing reports

- **Network Sensor Reports**
  - Destination IP with Ports - Lists details of all events sorted by destination IP address first, then by time. Allows examination of network events sorted by the hosts that were the targets of the events, including ports.
  - Event Name with Ports - Lists details of all events, including ports. Sorted by event name.
  - Event Priority with Ports - Lists details of all events, including ports, sorted first by priority, then by time.
  - Source IP - Lists details of events sorted by source IP address first, then by time. Allows examination of network events sorted by the hosts that initiated them.
  - Source IP with Ports - Lists details of events, including ports, sorted first by source IP address then by time. Allows examination of network events sorted by the hosts that initiated the event.
  - Top 20 sources graph - Graphs the top 20 IP sources, ranked by the number of events associated with each address.

Reports can be viewed on screen, printed, or exported in a range of formats including plain text, Lotus 123, Excel, and Word, amongst others. There is very little scope for customisation within RealSecure itself – you would need to purchase the Crystal Reports Designer software to achieve that. There is also not much in the way of hyperlinked data or drill-down capabilities with the on-screen reports, making forensic examination more difficult than it should be.

Verdict

As we mentioned in the introduction, RealSecure is often the standard against which other NIDS products are measured. However, in some areas it does not quite measure up itself.

The current version struggles to maintain detection rates at high network loads (though we are promised that this will improve), necessitating careful thought and planning by the administrator to determine which signatures should be monitored by which Sensors on heavily loaded networks. The net result is that it is usually necessary to deploy multiple RealSecure Sensors on heavily loaded network segments in order to provide comprehensive attack coverage.

However, at least the modular architecture allows this to happen, and policy definition is extremely friendly and flexible, making RealSecure one of the most straightforward and intuitive IDS to manage that we have seen. With clear and unambiguous alerting, a wide range of alert responses, and excellent real-time console and extensive attack signature database, RealSecure is still well worth considering when placed in the right environment.

Contact Details

Company name: Internet Security Systems

E-mail: sales@iss.net

Internet: http://www.iss.net

Address:
6600 Peachtree-Dunwoody Road
Building 300
Atlanta, GA 30328
USA

Tel: +1 (678) 443-6000
Fax: +1 (678) 443-6477

ISS EMEA:
Buro & Design Centre
Suite 526
Heysel Esplanade
B-1020 Brussels
Belgium

Tel: + 32 2 479 6797
Fax: 32 2 479 7518

NETWORK ICE BLACKICE SENTRY 2.1

ICEpac is a suite of products from Network ICE Corporation that offers a choice of Network IDS and Network Node IDS in the same product – the first, to our knowledge, that provided this feature – along with centralised reporting, management and installation capabilities.

Architecture

The key components in ICEpac are:

- **BlackICE Agent –** provides high performance end node intrusion detection, hacker identification, and protection for all Windows 9x and NT systems (a Windows 2000 version will be available shortly). Because of its very small memory footprint and efficient use of CPU resources, BlackICE Agent has minimal impact on the performance of the end system.

- **BlackICE Sentry –** provides high performance intrusion detection and hacker identification for non-Windows based systems (though it still requires a dedicated Windows-based host on which to run), or anywhere where the use of an end-node agent is not desired. BlackICE Sentry is a probe-based solution for use on shared segments or connected to the monitoring port on Ethernet switches. When installed on a properly configured PC system, BlackICE Sentry can detect intrusions on a heavily loaded Ethernet network.

- **ICEcap Manager–** a browser based reporting, alerting, and protection system to provide large-scale data collection, automated report generation, intrusion alerting, and distributed protection for all BlackICE Agent systems. All BlackICE Agents and BlackICE Sentry probes can be configured to be controlled by an ICEcap console, and ICEcap stores the information in a MS-SQL/Access database. ICEcap has a browser-based interface so it can be accessed remotely from anywhere on the Internet by authorised users. It also has several different alerting options, including pager and email alerts and can remotely install and update BlackICE Agents and BlackICE Sentry probes in many situations. ICEcap also includes the InstallPac utilities described below.

- **InstallPac –** a set of three utilities used to automatically install, update, or remove BlackICE Agents from end systems. These utilities can be used to easily install or update BlackICE Agent on a single system, a Microsoft Workgroup, an NT Domain, or on a range of IP addresses. This installation or update is invisible to the end user, and does not impact their current activities on their computer. Thus, all BlackICE Agents can be easily updated with new detection algorithms without impacting the end users. InstallPac can be installed on the ICEcap system, or on any other system within the corporate network to ease the installation of BlackICE Agents.

Pattern Matching v Protocol Analysis

One of the main architectural differences between BlackICE (the agent code) and competing Network IDS products is that BlackICE performs full seven-layer protocol analysis rather than simple pattern matching. This approach comes from the fact that the founders of Network ICE are all ex-Network General employees who worked on the original Sniffer product.

You may think that a full protocol decode on every packet would be slow, and it is compared with a straight pattern match on a single packet. However, as the number of attack signatures grows (some products have in excess of 1000 signatures in their attack database) it takes longer and longer for a packet to be compared against the ever larger signature database, and this poses problems for the standard pattern matching architectures. The usual answer is to install multiple IDS sensors and have each sensor watch for a subset of the available attack signatures.

The advantage that BlackICE has is that many attacks are nothing more than variations on a theme. Since protocols and operating systems are built around standards, the protocol analysis engine understands how to process a packet. Unlike pattern matching, the algorithm decodes the suspicious packet and inspects them dynamically for protocol correctness. For example, hackers will often use variable size buffer overflows to evade traditional IDS systems, and some pattern matching software will miss these "new" attacks because it is looking for a static buffer overflow size. Each small change to an attack requires a new signature in a pattern matching system – and every signature imposes additional overhead on the detection process.

On the other hand, a protocol analysis algorithm can dynamically identify all "incorrect" or "oversize" packets – no matter what size the buffer overflow - and drop the packet before it reaches the TCP/IP stack. Of course, when new undiscovered vulnerabilities, attacks, or exploits are found, Network ICE still needs to update the protocol analysis algorithm by adding a new protocol to watch, or by changing a variable to the algorithm that is specific to a certain protocol. The downside of this approach is that it can sometimes take longer to do this than to add a new pattern matching attack signature to a database.

However, updates to Network ICE are needed far less often for most new attacks and exploits because they are often variants of older attacks. Using a protocol analysis approach thus takes less updating and patching, and is capable of higher levels of performance as "traditional" IDS' struggle with larger and larger attack signature databases.

Of course, the other vendors have spotted the same problem, and so we are seeing an increase in systems that pattern match against "generic" signatures in an attempt to improve performance and reduce the number of updates required to accommodate new attacks. This approach may not always be as accurate or as highly performing as the full-blown protocol decode – it has to say something that BlackICE is the only product we looked at that automatically enabled every signature in its database for checking without having to worry about the performance hit, even when working as a Network Node IDS.

The other advantage is that the protocol decode approach allows BlackICE to handle out-of-order and fragmented packets better than some of the competition. Unless session state is maintained and monitored over multiple packets, and unless packets are reordered correctly and fragments reassembled, pattern matching simply does not work. Packet reassembly is an integral part of BlackICE, whereas some of the competition is now having to modify their products to handle this.

Installation

All ICEpac components are provided as single executable files to be downloaded from the Network ICE Web site. Installation is usually a matter of simply running the executable and accepting the defaults.

For BlackICE Sentry installations, Network ICE recommends installing the software onto a dual-processor machine – one processor dedicated to packet capture and the second dedicated to protocol analysis – with two network interface cards. This requires a few additional steps following installation of the Agent software.

Firstly, the processor affinity needs to be set in NT to ensure that each processor is dedicated to its allotted task. Secondly, the NIC which is to be used for packet capture should be removed from the NT network configuration and put into promiscuous mode in the BlackICE Sentry configuration file. The second NIC should be given an address on a private "management" only network on which the ICEcap server is located. Thus, the packet capture NIC becomes "invisible" on the main network, and management and reporting traffic is kept to a second network which would not be vulnerable to attack. Network ICE is looking at automating these additional procedures in a future release.

Centralised Deployment via InstallPac

In larger corporate environments, InstallPac can be used to install agent software onto target hosts remotely, thus removing the need to perform individual installations.

For NT systems, the InstallNet push program works very effectively for installing and automatically starting BlackICE Pro on a large number of systems simultaneously. For Windows 9x systems that have not been configured for remote disk access, the AgentUpdate pull program allows those systems to "pull" a copy of BlackICE Agent. The AgentUpdate program can be included in a logon script on a network server, so that Windows 9x clients automatically pull the software the next time they log in to the server

ICEpac documentation is only available on-line as PDF files, not as hard copy. The documentation is comprehensive, however, and includes a *Getting Started Guide* for the ICEpac suite, a *User Guide* for the BlackICE Agent, *Administrator Guides* for ICEcap and InstallPac, and a *Reporting and Reference Guide* for ICEcap.

Configuration

With the basic BlackICE Agent installation there is virtually nothing required in the way of configuration before the product will run. Whereas other IDS products require the administrator to define security policies containing the attack signatures to look for and the hosts to be monitored, BlackICE Sentry simply looks at every packet on the wire and always watches for every attack in its database.

Although there is limited scope for configuration via the graphical interface, there are some key text-based configuration files that can be edited manually (by those who know what they are doing) to fine tune the operation of BlackICE.

Whilst it is not possible to define new attack signatures per se (since BlackICE does not use pattern matching) it is possible to modify the behaviour of the protocol decode by defining new “rules” that can specify what objects or resources the engine should monitor.

For instance, it is a simple matter to have BlackICE watch a specific file, directory or Windows registry key for tampering (and a number of sensible defaults are included in the standard configuration). It is also possible to alter settings such as failed login counts or SYN flood thresholds to suit the characteristics of your own network. It would be nice to see the GUI developed further to provide the means to modify these parameters within the application rather than via editing text files, however.

BlackICE GUI

The default installation includes a simple graphical interface on the host PC with a number of different tabbed views. The **Attacks** window shows details of all attacks including date and time, attack name, intruder ID, victim ID and a count of the number of attacks seen. Unfortunately, we found the count information to be one of the less accurate of the IDS systems tested, but this is not due to BlackICE missing packets. Because it is designed to operate at high speeds (it can handle 100 per cent network load of 148800 packets per second on a 100Mbit network) there is a certain amount of what is known as “pre-filtering” and “coalescing” of events when a serious attack is underway. The most obvious result of this is that multiple attacks will begin to be shown on a single line with a source IP address of 0.0.0.0 instead of on separate lines, and the count information seems to be approximate at best once this starts to happen.

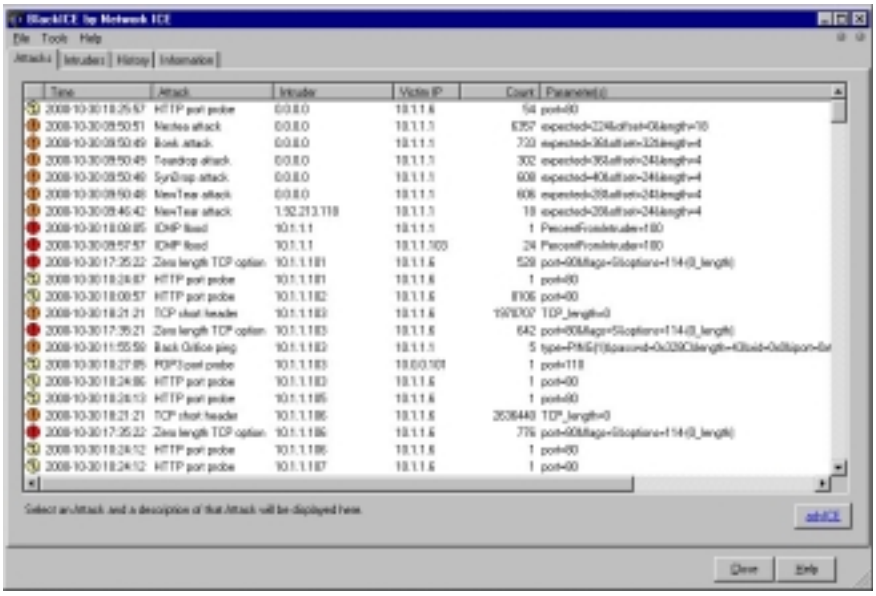

Figure 35 - Viewing attacks in the BlackICE console

Additional columns can be added to the Attacks display (attack parameters, attack ID, severity, etc) by right-clicking on the column headers, and columns can be re-ordered and re-sorted as required. Each severity level is colour coded (red, yellow, or green) and audio-visual alerts can be triggered at the console depending on the severity. By selecting any attack, a brief description is displayed at the bottom of the GUI.

A more detailed description – including further reference material and occasionally suggestions for fixing the problem – can be obtained by clicking on the “Advice” button. Unfortunately, none of this information is installed locally – BlackICE has to go off to the Network ICE Web site to retrieve it (which might be a problem if the attack has brought down your Internet connection).

The next tab is the **Intruders** display, which displays a list of attackers, together with any details BlackICE has been able to determine by means of “*back tracing*”. This feature, which can be disabled if performance is paramount, enables BlackICE to trace back to the attacker in an attempt to discover as much about him as possible. Along with the IP address (which could be spoofed, of course), BlackICE will display the DNS name, NetBIOS name, Windows Workgroup/Domain name, node name, and even the MAC address if they can be determined.

Figure 36 – Viewing attack history in the BlackICE console

The third tab is the **History** tab, which displays graphs of attacks, suspicious activity and network traffic over a user-selectable period of time. When BlackICE installation is controlled by InstallPac, it is possible to install a “silent” version of the Agent with no GUI. This makes the Agent completely invisible to users of the host machine, whilst still allowing control of the Agent from the ICEpac management console.

Firewall

Unlike most other IDS systems, BlackICE also incorporates a firewall. This can operate as a personal firewall, with BlackICE Agent, or as a network perimeter firewall with BlackICE Sentry when installed on a dual-NIC host.

There are two parts to BlackICE protection: the *standard protection filter*, and the *dynamic protection filter*. Standard protection filtering stops many common attacks before they can get started. This includes blocking corrupt packets, badly fragmented packets, and other potentially damaging transmissions. The standard filters include configurable filters for IP addresses, TCP and UDP ports.

Dynamic protection filtering works much like an IP address filter used on routers and other network devices. When a malicious attack is detected, BlackICE adds the hacker's IP address to a dynamic address table, following which, any traffic from the hacker's IP address is rejected at the network stack level.

Right clicking on any attack or intruder in the BlackICE display allows the user to immediately trust or block a user, and ignore or block an attack. Ignoring attacks or trusting certain IP addresses provides the means to run automated scanning tools on the network without triggering false alarms on all the BlackICE Agents.

Logging

In addition to the trusting and blocking settings, the only other parameters that can be configured via the GUI interface relate to *packet logging* and *evidence logging*.

When packet logging is enabled, BlackICE Agent records all system traffic into log files, the size of the files and rotation characteristics controlled via the *Packet Log* tab in the BlackICE settings. It is important to note that packet logging keeps track of ALL system traffic, not just intrusions, which can result in some large files. Packet logs are encoded as "sniffer" style trace files, and will require a decoding application (which is not included) to view the contents.

If you want to be more selective in what is recorded, you can employ evidence files, which are also controlled via the BlackICE settings. Whenever an attack is detected, BlackICE Agent captures network traffic specific to the attack in progress and stores that information in an evidence file. These files also require a trace file decoder to view the contents.

Management via ICEcap

Although each BlackICE Agent or BlackICE Sentry can be managed via the GUI interface, larger networks will benefit from the use of ICEcap to centralise the management and reporting tasks, thus providing the means to track trends and issue network-wide security measures. Once an Agent has been configured to report to an ICEcap server it is no longer possible to configure anything locally. Centralised control also allows deployment of "silent" Agents with no GUI, making them invisible to the user of the host PC.

The ICEcap Management Console is a flexible Web-based administrative system that integrates with BlackICE Agents, gathering, storing and analysing intrusion data from all the Agents on the network. Although the individual Agents will continue to report attacks on the local GUI (unless they are "silent" Agents), from a single browser-based interface the administrator can run security reports that show hacking statistics across the entire network. And because ICEcap has an "enterprise-wide" view of network intrusions it can identify hacking activities that a single BlackICE agent might miss.

ICEcap can also command remote BlackICE Agents to block or permit network transmissions for a specific IP address or network port. For example, let's say a hacker attempts to break into your web server. BlackICE detects the hacker, back traces his IP address and raises an alert.

With a few configuration changes and the click of a button, a single network administrator can command all BlackICE agents on the network to block any traffic from the hacker's machine. Even if the hacker should make it through the corporate firewall, none of the computers running BlackICE will allow the hacker access. Communication between Agents and the ICEcap server is ensured by regular transmission of encrypted HTTP packets between them, known as "heartbeats". The bi-directional nature of these heartbeats could cause problems in some networks, however, particularly across dial-up or on-demand links which may only operate in one direction.

ICEcap can be configured to show alerts as they are reported from the various BlackICE Agents around the network in the browser window. Since it is not always convenient to logon to ICEcap and pull up a report, however, ICEcap also includes a basic Alerter utility. The Alerter is a miniature browser window that checks the ICEcap server every ten seconds for an alert. When an alert is detected, the browser window flashes.

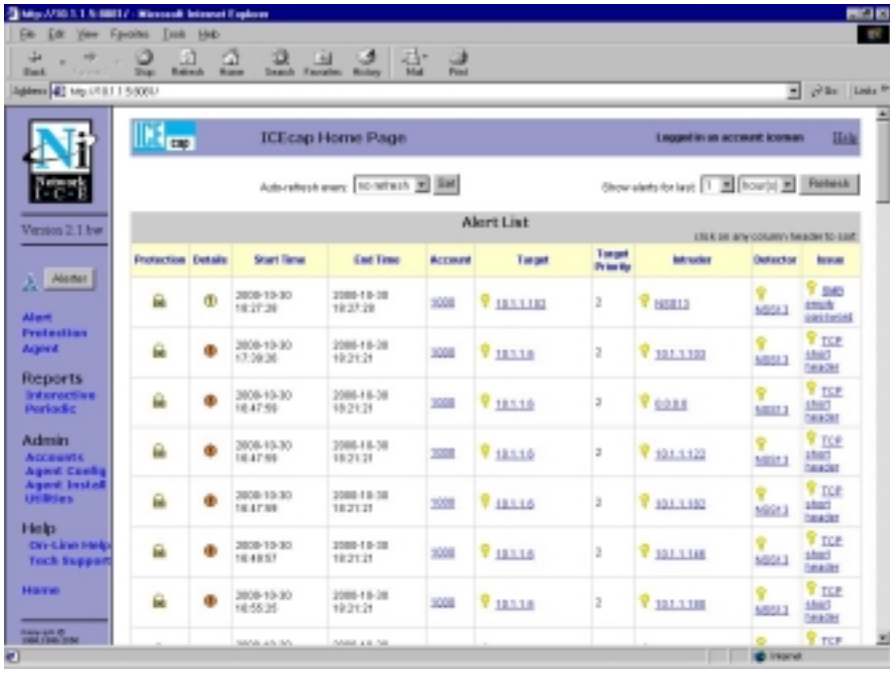

Figure 37 - Viewing alerts in ICEcap

Computers can be logically bound together in Groups under ICEcap for administrative and reporting purposes, and the administrator can create Policies (which associate an event with a severity level) and Enforcements (which bind Policies to Groups). This allows certain events and hosts to be designated higher or lower priority as required. These policies are then automatically applied to all BlackICE Agents in a particular Group.

When ICEcap issues an alert it can send an e-mail, a page, an SNMP trap, or invoke an executable file. Alerts are issued based on events received that meet the Alert Threshold defined for each account. *Contacts* identify what ICEcap should do when issuing an alert (for instance, defining the e-mail or pager address of the administrator for a particular Group), and it is possible to establish more than one contact for an account (which would allow you to send both an e-mail to the Group administrator, and a pager message to the ICEcap administrator for a particularly serious alert).

Default Agent configurations can be named and saved within ICEpac too, allowing the administrator to specify all the parameters for how an Agent is installed on a remote system. This includes such information as default login account, installation path, blocked addresses and the state of features like packet logging, evidence logging, back tracing and so on. The Agent Configuration Record (ACR) also allows the administrator to override the per-Agent text-based configuration parameters we mentioned earlier.

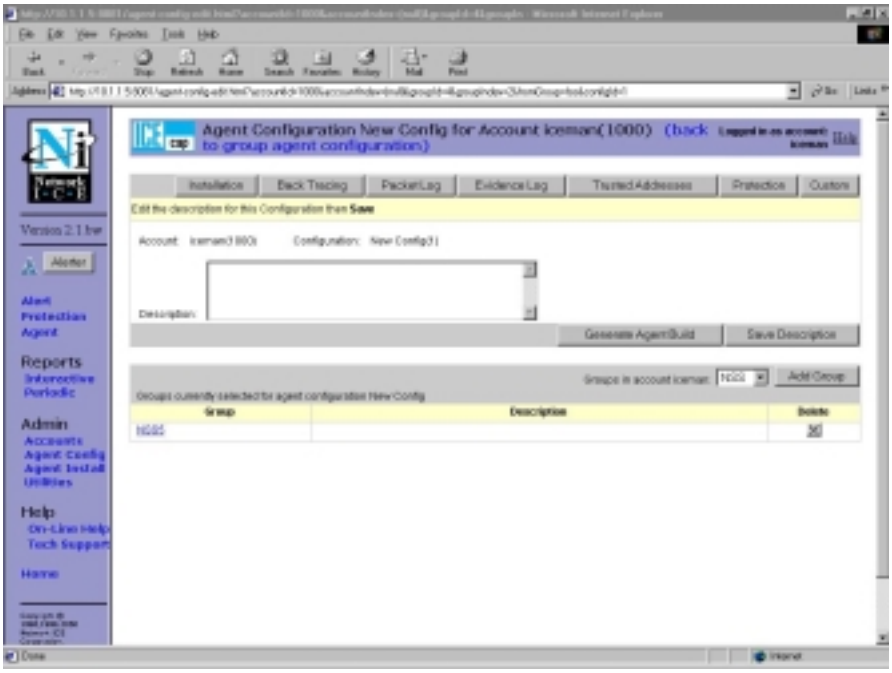

Figure 38 - Configuring remote BlackICE Agents in ICEcap

Once an ACR has been created and associated with a Group, it can automatically be distributed to the hosts within that group and installed – usually without even rebooting the target machines. Any number of ACR's can be created and associated with Groups which can contain anything from one host to an entire subnet, thus allowing configurations to be applied in a fine-grained or broad-based manner as required. Changes to, and removal of, BlackICE Agents are handled in exactly the same way, allowing the administrator to handle all the installation, configuration, security and removal of BlackICE software from a single point. InstallPac can also be employed to achieve the same ends, but via a command line interface.

Although there is extensive on-line help and the documentation is fairly good, we found the ICEcap interface to be confusing and not particularly intuitive. The biggest problem is with its Web-based nature which, although it does allow it to be run from anywhere on the network via a standard browser, makes it all too easy to get lost within the various screens as you follow the numerous hyperlinks. This is one area that could be improved.

Having said that, the remote management, installation and configuration features makes ICEpac well worth the trouble to get to know.

Reporting and Analysis

Without ICEcap, the BlackICE Agent or Sentry modules provide only the most basic reporting and alerting capabilities via the GUI interface. There is certainly no means to provide historical or trend reporting without employing the services of ICEcap.

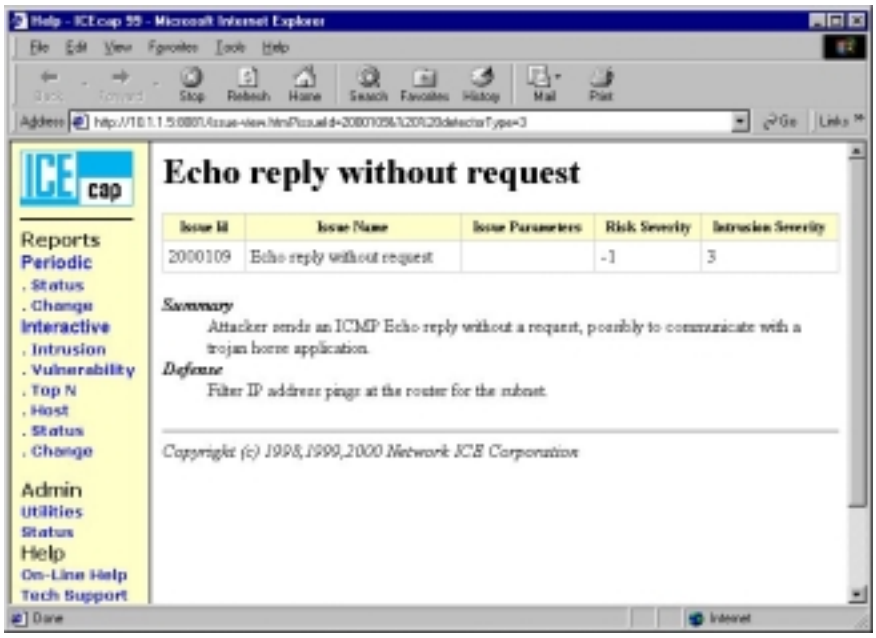

Figure 39 - Running ICEcap reports

All data is reported back to the ICEcap server under specific accounts. There is one master account – *iceman* – and only this account is capable of consolidating and reporting on data across all the other accounts. This means that it is possible to have different sections of your network reporting back to ICEcap independently of each other, and administrators in each of those sections would only be able to view their own data. Only the ICEcap administrator would have the capability to see everything.

Reports are divided into *interactive* and *periodic*: interactive reports work on the live data, whilst periodic reports work from regularly scheduled "snapshots". There are a number of reports available, including:

- ***Intrusion Status Report*** *– a list of all intrusions in a given time period*
- ***Intrusion Change Report*** *– a list of new intrusions based on a comparison of two time periods*
- ***Top N Report*** *- allows you to look at the most extreme issues, intruders, or systems over a period of time. (For example, top 20 most serious intrusions, or the Top 5 Intruders on the network.)*
- ***Host Report*** *- detailed data about systems on the network that have either reported events, were the victims of an attack or have carried out attacks.*
- ***Status Report*** *– shows all events reported to ICEcap during a specified time period*
- ***Change Report*** *– shows new vulnerabilities or intrusions based on comparisons of two time intervals*
- ***Agent Report*** *– displays information about BlackICE Agents*
- ***Alert Report*** *– this is the report that is displayed when ICEcap is first started, and shows all the alerts that have been triggered.*

All reports are presented in a clear, easy to read tabular format in the browser window, and certain columns are re-sortable in ascending or descending order. This allows many of the reports to be edited “live” in order to present the information in the most meaningful format. Many of the entries on each row of the report are also live hyperlinks, enabling the administrator to drill down to acquire more detail. For instance, in a list of alerts, the *victim’s IP address* will be a hyperlink, and clicking on the link will bring up details of that particular host, whilst clicking on the hyperlink of the *attack name* will bring up detailed information on the attack itself.

Figure 40 - Viewing detailed attack information in ICEcap

Some fields will also contain a golden key icon. Clicking on this icon against the *victim’s IP address* will bring up another report detailing all the attacks made against that particular address. Clicking on the same icon against the *attack name*, however, will bring up a report of all the attack of that particular type made within the requested time period. This flexible means of resorting and drilling down into ICEcap reports makes for a powerful reporting environment.

Once again, the use of the browser-based interface with multiple hyperlinks on a page can make it confusing when running reports. However, the biggest problem with ICEcap’s reporting is that the output is to the browser window only, with no means to provide a nicely formatted printed output or export facility. This is another area that requires improvement, although the actual content of the reports is more than adequate.

Verdict

Overall, ICEpac is an extremely impressive IDS, combining as it does powerful Network IDS and Network Node IDS components, along with firewall and remote management capabilities.

There are one or two minor niggles, such as the need for an improvement in the BlackICE Agent/Sentry GUI to allow more extensive configuration of the Agent software without having to resort to editing text files.

We also found the browser-based interface in ICEcap to be confusing, and there is a definite requirement for a properly formatted printed output, as well as an export facility to other file formats. If we were to get really picky, we would like to see the detailed attack information installed locally rather than accessed purely over the Web, and feel that a product of this quality deserves a hard copy documentation set.

But the most important part of any IDS is the ability to capture packets, accurately identify attacks and report on them, even under conditions of heavy load. This ICEpac does extremely well, thanks to the protocol analysis-based architecture and highly optimised network drivers. This meant that the BlackICE Sentry machines were capable of detecting all attacks, even with a network load of 148000pps on our 100Mbit test LAN, whilst the BlackICE Agent machines could handle high levels of attacks against a particular host without consuming excessive amounts of CPU power. This latter feature, together with the “silent” mode of remote installation via ICEcap, means that you could have a BlackICE Agent installed on every single desktop in your organisation and your users wouldn’t even know it.

Highly recommended, and we are looking forward to seeing Agents appear for Linux (currently in the development pipeline)

Contact Details

Company name: Network ICE Corporation

E-mail: sales@networkice.com

Internet: http://www.networkice.com

Address:
2121 South El Camino Real
Suite 1100
San Mateo
CA 94403
USA

Tel: +1 650-532-4100
Fax: +1 650 341-0719

Network ICE International and EMEA Headquarters
Royal Albert House
Sheet Street, Windsor, Berks
SL4 1BE
United Kingdom

Tel: +44 (0)1753 705140
Fax: +44 (0)1753 705148

NSW DRAGON SENSOR 4.1

Dragon Sensor is a packet-based Network Intrusion Detection System (NIDS) based on the Unix platform. A host-based version of the product – called *Dragon Squire* – is also available, but was not put forward for testing.

As of version 4.1, the supported operating systems consist of several Unix variants on both the Intel and Sparc platforms, including FreeBSD, OpenBSD, Linux and Solaris. An HP-UX port is also underway, and a port of the Server product for this platform is already available.

Ethernet protocols are also the only network media supported in version 4.1 - however, FDDI, ATM and Token Ring are all in development at the time of writing.

Architecture

Dragon Sensor switches the host network card into promiscuous mode in order to collect all traffic from the subnet (or switch port) to which it is attached. At a high level, Dragon takes two configuration files named *dragon.net* and *dragon.sigs* and uses them to determine rules for saving captured traffic for local logging to the hard drive.

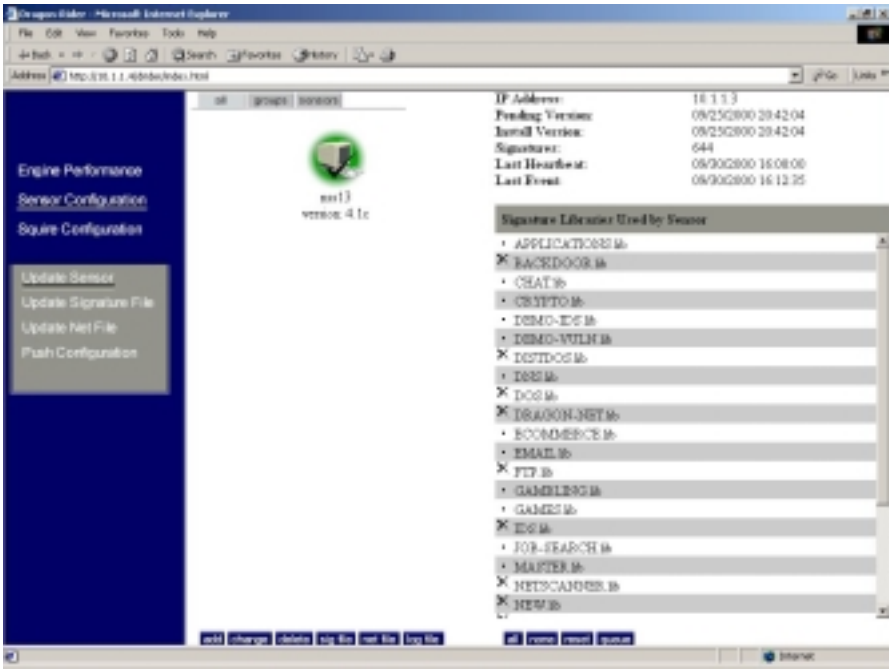

Figure 41 - The Dragon Rider interface

It is important to note that Dragon uses local network APIs to collect traffic and not third-party libraries such as *libpcap*, and this provides it with very high levels of performance. Dragon can also operate in a 'stealth' mode, when it is deployed on a host PC with two network interface cards. The IP stack can be removed from the monitoring interface, making it very difficult to detect with remote IP scans or target with DoS attacks. The second interface connects to a secure out-of-band network with the IP protocol. And this is used for management and reporting.

It is possible to employ a single Dragon Sensor in a stand-alone mode and manage it either from the command line or built-in Web interface. Reporting can also be carried out on the Sensor itself, and this makes it a good choice for those organisations wishing to place a single network sensor on a shared segment.

However, most organisations will deploy multiple Sensors across multiple routed or switched subnets or ports, and so the ability to control a number of Sensors from a single central console is important. This is provided via the *Dragon Rider* component, which consists of a client for each of the remote Sensors and a Server component. These are used to forward events to the central Server and send configuration information down to the Sensors. According to "official" sources, a target ratio to ensure reasonable performance is 25 Sensors to one Server. However, ratios of 200 to 1 are currently employed out in the field – your mileage may vary.

Communications between the client and server components are encrypted using the Blowfish algorithm, secured by a shared secret key specified at install time. Unfortunately, this shared secret is then stored as plain text in the client configuration file on the Sensor machine, which does not seem a particularly secure approach. Client-server communications occur over fixed TCP ports which can be changed at install time, and the Dragon Rider server also includes IP-level security to protect against spoofed IP connections.

Once the *Dragon Client* engines connect to the *Dragon Server*, it is possible to deploy the two key configuration files from a central location to all Sensors on the network. As the Sensors detect potential attacks, they will send the appropriate alert events back to the Server as they occur, and as fast as possible. The down-side to this approach is, of course, that if a network is under attack, the frantic reporting of alerts from Dragon Rider Client to Server will obviously burden the network with an additional load right at the point it could do without it. If a link fails, however, the Dragon engines will attempt a configurable back-off approach for reconnection.

Once alerts have been received by the Server, they are stored in date-named subdirectories under the */usr/dragon/DB* directory. From here they can be processed by the numerous command line analysis tools that make up the Dragon IDS package, or via the *Dragon Fire* Web interface. In the standard Dragon package, there is currently no way to consolidate reports across multiple Dragon Servers. Portcullis – the UK distributor - is working on an additional reporting tool (in beta at the time of writing) to provide just such enterprise-wide consolidation capabilities, and this will find its way into the standard Dragon distribution once released.

Heartbeat packets are transmitted between Dragon Rider Clients and Servers at regular intervals, ensuring that the administrator quickly finds out should a Sensor suddenly become unavailable for any reason. The same heartbeat packets are also used to transmit Sensor performance statistics to the central console.

Installation

Installation – whilst not quite the InstallShield we know and love from the Windows world – is very straightforward even for those with limited Unix experience.

The documentation is more than adequate, though is currently provided only as PDF files on the distribution CD. Portcullis is aware of the limitation of this approach and – rather against the current trend in the software industry, it has to be said – is producing hard copy manuals which will be a welcome inclusion in the standard Dragon package in the not too distant future.

Installing the appropriate package for your Unix environment (ours was Red Hat Linux 6.2) creates the directory structure and places the files appropriately. A Perl install script is created for the Dragon Rider components and it is important to use the installation script provided so that a preliminary configuration file is built. After the installation, however, the configuration can be modified by editing the Dragon Rider client configuration file (driderc.cfg) if required.

Configuration

For anyone *au fait* with Unix and happier with a command line than a GUI, Dragon can be configured and run entirely from the command line if required. For mere mortals, a Web-based interface is provided, and this in itself is split into two separate components: ***Dragon Rider*** for configuration and ***Dragon Fire*** for reporting.

Dragon Rider provides a Web-based administration interface to the Dragon Rider Server component, enabling remote Sensor (both network and host based) configuration and performance reporting.

The first task can be a bit laborious in large networks, in that it is necessary to manually add details of each Sensor to the Dragon Rider console – it would be nice to see some form of auto-detection here to ease deployment across larger networks.

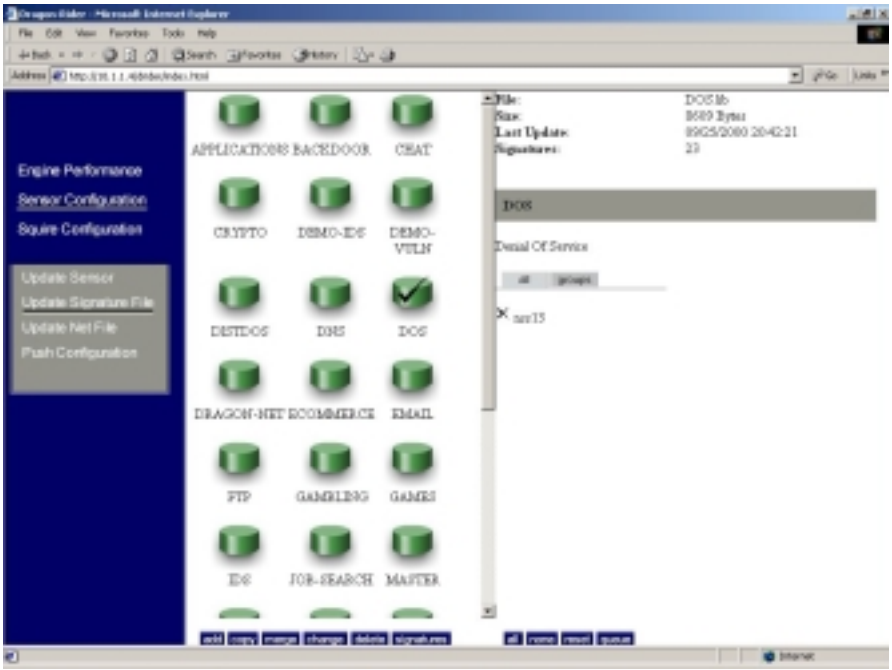

Figure 42 - Applying signatures to a sensor

There is a comprehensive range (over 1050 at the time of writing) of attack signatures available within dragon.

These signatures identify unique data patterns in network traffic which can be used to identify network attacks, misuse and vulnerabilities, and a subset of these can be applied via the *dragon.sigs* file. It has to be a subset, because each Sensor can have a maximum of 1000 signatures applied to it, and this limit is hard coded. Now that the "master" library contains over 1000 signatures itself, and as hardware gets more and more powerful, the restriction is being removed and a more performance-related limit is replacing this functionality. For now, if you would like to deploy every signature in all libraries, you will need more than one Sensor to do it.

Signatures are split into a number of different "libraries", covering a number of different alert and attack possibilities such as DNS, FTP, Web, Denial of Service, e-mail, games, back-door/Trojans, and even porn. Each signature consists of up to eleven fields specifying direction of traffic, protocol, binary or text, port number, event name and a search string, amongst other things.

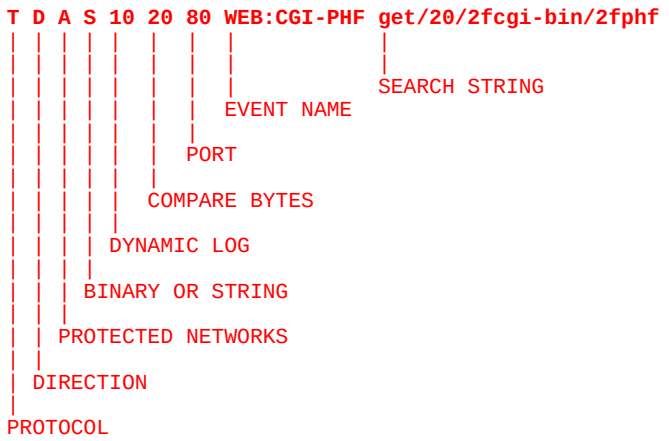

Figure 43 - Defining new signatures

These fields can be defined quickly and easily via the Dragon Rider Web interface in order to change existing signatures or create brand new ones specific to a particular corporate environment. For instance, it would be a simple matter to watch for a packet containing logon information to a sensitive area of a restricted Web server and mark it as an alert if an attempted login comes from outside a particular subnet. Custom signatures can be added to a special custom signature file which is loaded after the standard Dragon signatures (though the maximum 1000 signatures per Sensor still applies).

As an example of how flexible Dragon can be, there are even a small number of Virus signatures included. Whilst Dragon is not intended as an anti virus scanner, it would provide the means for an administrator to incorporate a quick-and-dirty defence against certain types of viruses on the network whilst waiting for an update to the corporate AV software.

The administrator can pick and choose individual libraries of signatures to apply to a particular detector or group of detectors, and then queue them up for deployment from Dragon Rider. Signature libraries are updated regularly, and certain libraries may be designated as "auto update" if required. With auto update, a Web site is queried nightly and new signatures downloaded for review by the administrator before they are actually applied.

Dragon does not rely solely on a library of signatures for its anomaly detection, however. There are also a number of anomaly signatures pre-

defined in the Dragon program which are designed to detect many layer three or protocol violations.

Examples include port scan, port sweep, suspicious fragmentation, IP source routing and many other types of multiple packet behaviours. This allows Dragon to perform advance packet reassembly if required in order to outwit all of the currently available IDS evasion techniques. Also included in this section are a number of complex application-specific protocol decodes such as FTP hijacking, finger bounce attacks, suspect RIP packets, NT logon events, SYN bombs, Ping of Death and various other DOS attacks.

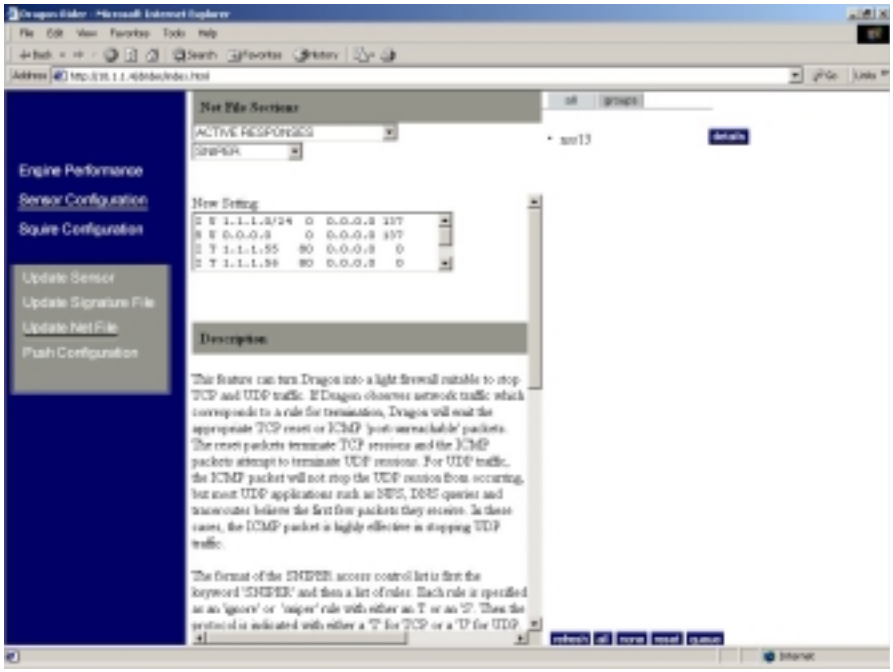

Figure 44 - Configuring network IDS parameters

Unfortunately, because there are no specific signatures for each DOS attack, this generic network layer detection produces a single alert to cover a range of attacks, and leaves the administrator to figure out what the attack was. Of course, if you care more about the fact that you have been attacked, rather than what the attack actually was, this is not an issue.

In response to attacks and suspected port scans, the Dragon Sensor can selectively terminate suspect sessions and also emit false responses from servers to confuse scanners and act as a lightweight firewall. It can also be configured to dynamically log a certain number of packets following a suspected attack, perhaps grabbing a complete suspect FTP session.

Whereas signatures are fairly easy to get to grips with, the network section of Dragon is incredibly complicated. There is extensive help both in the documentation and in the program itself when it comes to setting the network-related parameters, but it is a fact that you really need to have a good idea of what you are doing before you wander in to this part of the program – it took us a few attempts to get the IDS evasion stuff working, for example.

One wrong setting and you could end up overloading Dragon by asking it to log absolutely everything, and thus causing it to miss legitimate attacks. There are some rules in there that will help improve performance too, and here the opposite could be the case – that if you are not careful, you could finish up excluding traffic that you should be monitoring.

Not all the defaults are sensible either, and so we would have to conclude that Dragon out of the box is not the easiest of IDS' to configure compared to most of the others we have looked at here. On the other hand, it ***is*** one of the most flexible and configurable, so this is a real swings and roundabouts call, balancing power and ease of use.

Once the appropriate signatures have been chosen for download to the Sensor, and the appropriate network parameters have been specified, the administrator can choose one or more Sensors from the GUI interface (and these can be grouped where necessary for ease of administration) whereupon Dragon Rider queues the two configuration files.

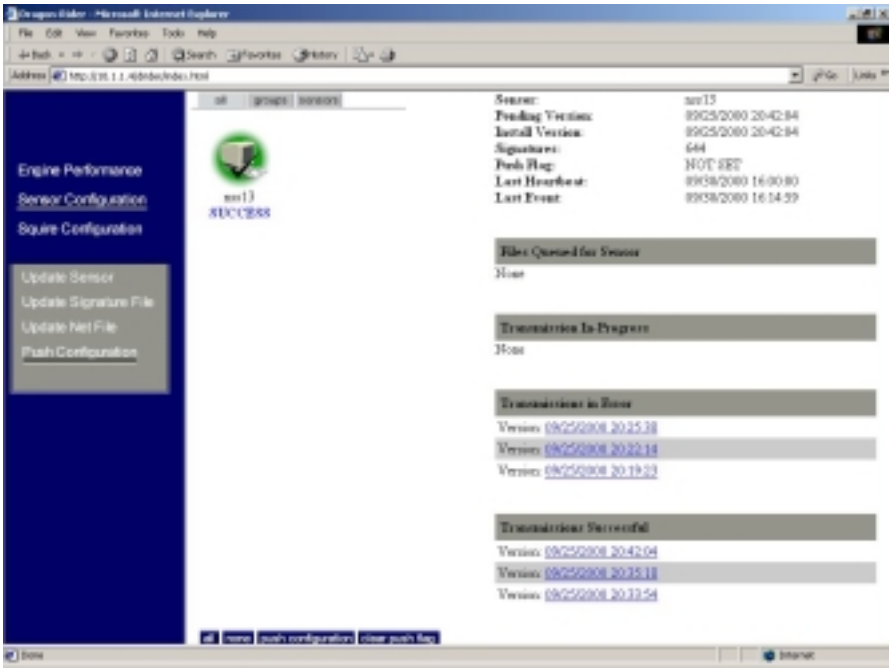

Figure 45 - Pushing configuration files to the sensor

When the "push configuration" option is selected, the files are compressed and encrypted before being transferred securely to the appropriate Sensors. Dragon Rider client will automatically stop the Dragon engine, load the new configurations and report back any problems should they occur.

If a problem does occur, the Dragon Rider client will copy the original configuration files back and attempt to restart the Dragon engine, thus ensuring continuity of coverage.

Reporting and Analysis

Dragon has a complex set of rules that are applied to each captured packet, and when a rule matches a particular packet or data stream, the information is logged. When attacks occur, Dragon attempts to collect as much information as possible on the subsequent network traffic, although there is obviously a limit to the amount of traffic that can be realistically collected.

There are two types of logging. The first type is a *'syslog'* style log containing all of the relevant information for each captured event, stored in a text-based file called *dragon.log*. The second type of logging stores a binary copy of each packet in a proprietary database in the DB directory for more extensive analysis.

A new subdirectory is created automatically each day, and that day's logs are stored within it. Once the day is over, Dragon never accesses the particular subdirectory again allowing the contents to be deleted, moved or archived for long term storage. Tools to alert on low disk space are available at the customer support site.

A variety of command line tools are included as part of the Dragon package to process the logged data and report on the contents in various ways. Some tools are designed to quickly identify problems, whereas others are designed to extract specific information about network events. It's up the administrator to decide how much analysis is required. A number of Perl scripts are provided to drive these reporting and analysis tools, and obviously they can be driven from custom scripts if required to automate the entire reporting process.

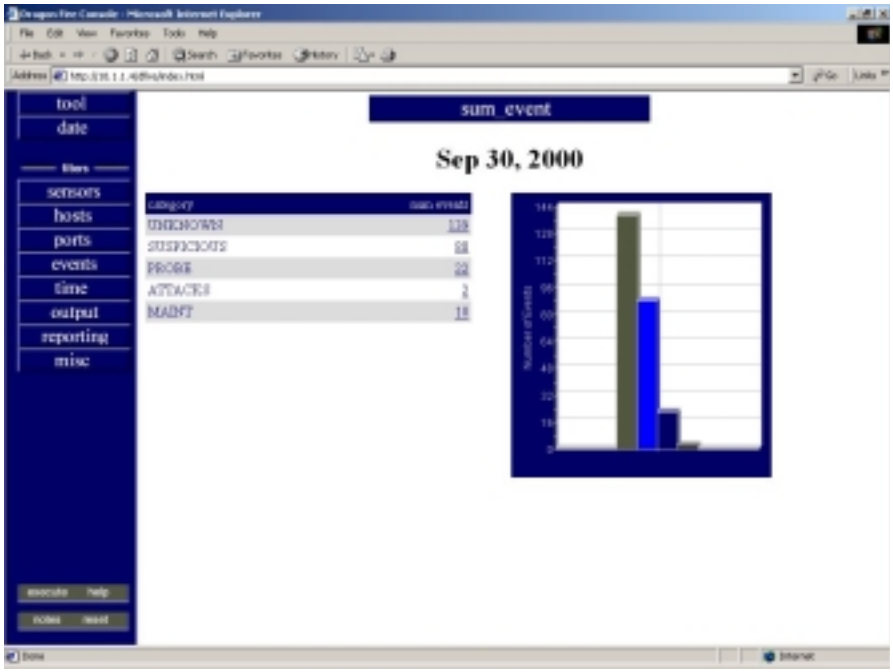

Figure 46 - Summarising attacks via the Dragon Fire interface

For those who prefer a more interactive form of reporting away from the rigours of the command line, the Dragon Fire utility provides a Web-based front end for the command line tools. A menu bar down the left of the screen allows the administrator to specify which Sensor (or group of Sensors) are to be reported on, a date range, and which reporting tool to use. Output can then be further filtered or sorted as required, and some tools have multiple reporting options.

For example, when running a query for all of the events from a particular IP address, the result may be displayed line by line or packet by packet. In other cases, particularly with the sum_event tool, a higher level view of the data may be used to represent groups of events, such groupings making use of the configuration information contained in the *dragon.conf* file. The higher level groupings allow for easier drill-down of collected events, and will often include graphical as well as text-based data.

Once a basic report has been displayed, it is possible to drill down to more detailed levels via a number of on-screen hyperlinks if required. For instance, having displayed a summary of attacks, clicking on an attack name will produce a list of individual packets. Clicking on one of those packets can show packet contents, source and destination details, and a detailed description of the attack itself, including Bugtrack and CVE information.

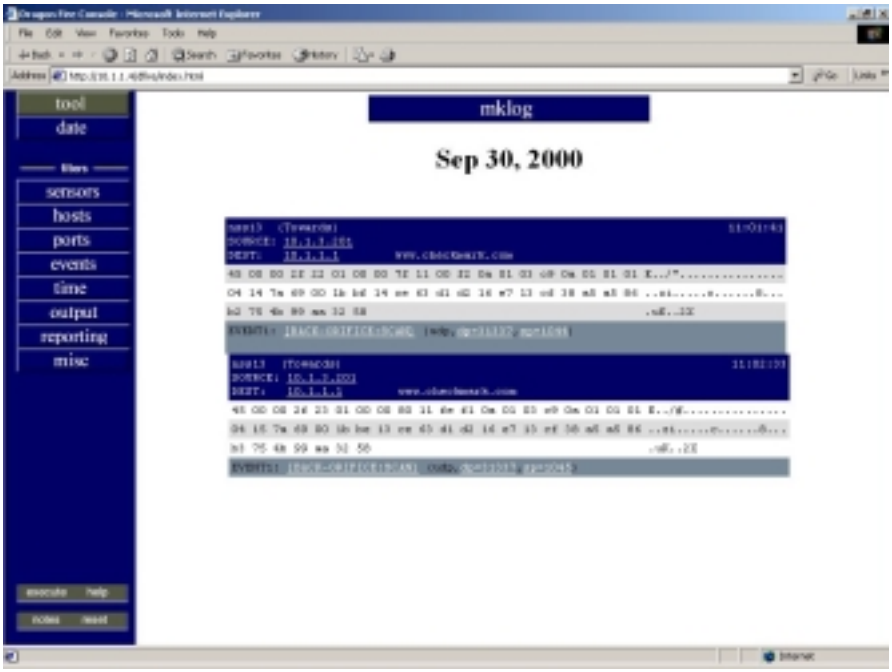

Figure 47 - Viewing contents of a BackOrifice scan packet

Clicking on the source or destination address will show all other recorded packets collected in relation to that address. Following the links in this way allows the administrator to perform a more detailed forensic examination of the log file contents following a suspected attack. Unfortunately, there is no information given on how to fix problems, and there is certainly no “auto fix” capability.

Nor, is there a specific print option available, so it is necessary to run the report and then use the print function within the browser (unless you go back to using the command line version of the tools, of course). Probably our biggest gripe, however, would be the confusing way some attacks are reported, presenting the administrator with three or four different alerts from a single attack and leaving him to deduce exactly what has happened. As we said before, at least Dragon is spotting the attacks – no problems with that – but they way it presents its results could be a little friendlier in places.

Unfortunately, there are also several problems with the Dragon Fire interface when run from Internet Explorer. We realise that Dragon is designed with Unix in mind, so Netscape is probably the browser of choice for its developers, but according to our Web site statistics, over 70 per cent of users out there are using IE. Patchy support for the most popular browser is inexcusable.

Neither Dragon Server nor Dragon Fire send or receive any SNMP traps, SYSLOG messages or email alerts. Instead, all of this functionality is available in an add-on utility known as Alarmtool.

This utility watches the dragon.log file, or the Dragon Server Export log and raises alerts based on a complex set of filtering rules. Alerts can be sent via SNMP, SYSLOG or SMTP.

Verdict

Dragon IDS is a strange product in some ways. It is unlikely to appeal immediately to sites that do not have Unix expertise, but it would be unwise to let that put you off. True, you would get the best out of the product by knowing something about Unix and by being willing to experiment with some of the advanced command line options. But for most situations, you could do everything you need to do via the Web-based interfaces *Dragon Rider* and *Dragon Fire*.

There are one or two rough edges to smooth out – the poor support for Internet Explorer, an auto-detect mechanism for the Sensors, the limit of 1000 signatures per Sensor (hopefully removed by the time you read this) and the occasionally confusing method of reporting alerts.

However, these are fairly minor gripes compared to the potential of the product. A bewildering array of configuration options may leave the uninitiated feeling a little punch drunk and daunted, but they provide tremendous power and flexibility in allowing you to make Dragon behave in exactly the way you want it.

Slightly more serious was the problem we had with erratic performance at high network loads. This was narrowed down to an issue with our 3Com cards and/or the Linux drivers, and Dragon technical support was working hard on the problem at the time of publication. We would advise testing Dragon thoroughly on your own hardware configuration, but once a stable configuration is achieved it should perform flawlessly, since it demonstrated excellent attack recognition capabilities as well as a complete resistance to all known IDS evasion techniques.

Contact Details

Company: Network Security Wizards

E-mail: sales@securitywizards.com

Internet: http://www.securitywizards.com

Address: 7060 Oakland Mills Road, Suite I, Columbia, MD 21046
Tel: +1 410-381-2101
Fax: +1 410-381-2103

UK Distributor: Portcullis Computer Security Ltd.

E-mail: enquiries@portcullis-security.com

Internet: http://www.portcullis-security.com

Address: The Grange Barn, Pikes End, Pinner, Middlesex, HA5 2EX
Tel: +44 (0) 20 8868 0098
Fax: +44 (0) 20 8868 0017

TRIPWIRE V2.2.1

Unlike the other host-based IDS systems under test here, Tripwire is very specifically a *File Integrity Assessment* (FIA) product.

Tripwire works by first creating a database of important system files - a "*snapshot*" of a computer system in a known secure state. The administrator can specify the directories and files that should be monitored, and the properties (last write time, file size, access permissions) for each of these that should be stored in the Tripwire database file.

Once this "*baseline*" database is created, Tripwire can be used at regular intervals to compare the current state of the system with the information stored in the database. Any changes to the system outside of specified boundaries will be detected and reported. If these changes are valid, the administrator can update the baseline database with the new information. If malicious changes are found, appropriate steps can be taken.

Architecture

Previously, Tripwire consisted purely of a stand alone program that ran on an individual host, which made centralised control of multiple hosts extremely difficult and time consuming.

Earlier this year, Tripwire began to ship the HQ Connector software, that provides distributed agents and a central console to manage and report on multiple Tripwire clients.

The distributed Tripwire architecture is made up of the following components:

- ***Tripwire HQ Manager -*** a Windows NT application with a graphical user interface (GUI) that enables system administrators to manage multiple installations of Tripwire software from a central location. The HQ Manager is made up of two components:
  - The *HQ Console* enables an administrator to pass commands to machines that have Tripwire 2.2.1 and HQ Agent software installed.
  - The *HQ Reporter* enables an administrator to view and manage Tripwire reports from all of the machines in the network.
- ***Tripwire HQ Connector -*** a self-contained integrity assessment system installed on each machine that the HQ Manager monitors. Each Connector is made up of two components:
  - *Tripwire 2.2.1 -* integrity assessment software, which monitors critical system files, directories, and registry objects, and reports any additions, deletions, or modifications.
  - *Tripwire HQ Agent -* manages communication between the Tripwire HQ Manager and Tripwire software installed on the machine. On Windows NT machines, the Agent is an NT service; on UNIX machines, the Agent is a daemon.

Each HQ Connector is controlled by a single Manager, and each Manager can manage up to 250 Connector nodes.

Each Connector in the network can also be operated individually from that machine's command line since the Tripwire FIA component is identical to the command-line driven stand alone version.

All communication between Tripwire HQ Manager and HQ Connector machines is secured using Secured Sockets Layer (SSL) technology with 168-bit Triple-DES encryption.

To protect against unauthorised modification, important files on each HQ Connector are stored in a binary-encoded and signed form. Tripwire database, policy, configuration, and (optionally) report files are protected with El Gamal asymmetric cryptography with a 1024 bit signature.

Installation

Installation is far more straightforward these days than it used to be, following the usual InstallShield route on Windows platforms.

Tripwire software is supported on Windows NT 4.0/2000, SGI IRIX 6.5, Solaris (SPARC) 2.6, 7.0 & 8.0, Compaq Tru64 UNIX 4.0, IBM AIX 4.2 & 4.3, Solaris (Intel) 2.6 & 7.0, HP-UX 10.20 & 11.0, and Linux (officially Red Hat 5.2 and 6.0, though other distributions should work also).

During installation the administrator is prompted for several important configuration parameters such as e-mail server, reporting level (from "one line" to "detailed"), whether to reset access times on files touched by Tripwire to the original settings (this preserves the forensic integrity of Tripwire systems), whether to write Tripwire results to the Windows event logs, and which editor to use for Tripwire files. All of these can also be set or changed later from the Tripwire HQ Console.

The administrator must then provide site and local pass phrases, which are used to generate 1024 bit keys to encrypt and sign various Tripwire files.

When installing just the basic FIA software, that is all that is necessary. If the HQ Connector is to be used, then each host to be managed must have the HQ Agent software installed on top of Tripwire. The HQ Console must then be installed on one (or more) machine(s) on the network and each Agent must be registered to it by providing the host name, IP address and port number on which to connect.

Documentation is very good and covers all the separate components (with some overlap), though it is provided only as PDF files.

Configuration

For anyone used to the original command-line driven version of Tripwire, nothing has changed. The software can still be driven from the command line if required (making it ideal for incorporation into batch file or shell script programs), and it is not difficult to do. A useful Command Reference Card is provided listing all the commands for the various utilities in an easy-to-read format.

A *policy file* is configured by the administrator using a text editor such as NOTEPAD, and this file describes the expected behaviour of various system, application and data files.

Each *rule* in the policy file specifies a system object to be monitored, and describes which changes to the object should be reported, and which ones can be ignored.

Creating the policy file is the most time consuming part of Tripwire configuration and with the use of variables, rule arguments, stop points and conditional directives it can almost begin to resemble a programming language. There is no simple GUI interface to aid in creating policy files – it's just you and the text editor - but the HQ Console documentation does include an entire chapter to guide you through the process. There is also a very extensive default policy file included out of the box, covering a wide range of critical system files, directories, applications and registry settings. It is a simple matter to edit or comment out sections of this, and to add similar sections to accommodate custom applications of your own.

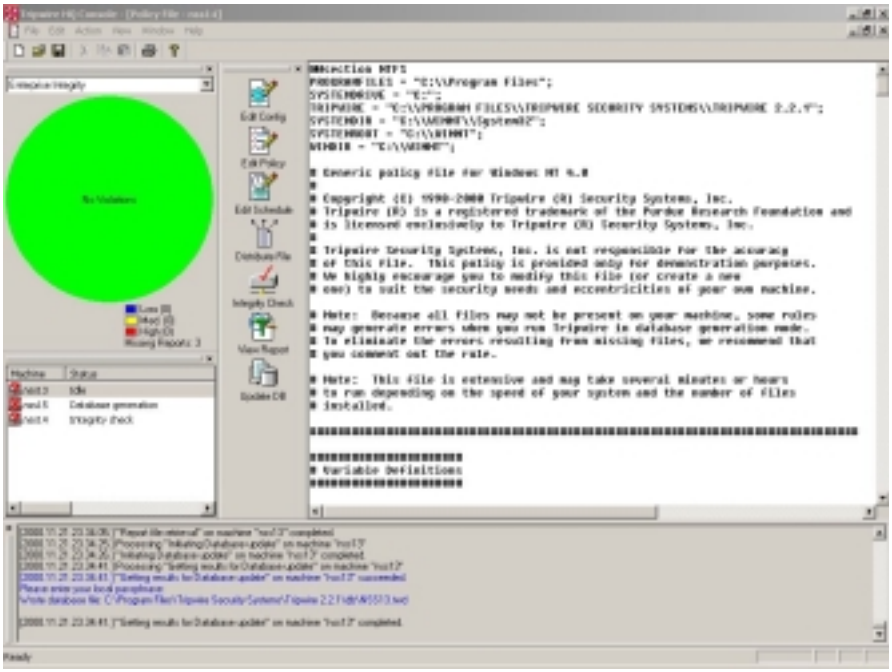

Figure 48 - Editing the Policy file from HQ Console

The *database file* is at the centre of the integrity assessment strategy. When the Tripwire software is first installed, the rules in the policy file are used to create a "*snapshot*" of a computer system in a known secure state. Then, during subsequent integrity checks, this "*baseline*" database is compared against the current state of the system to determine what, if any, changes have occurred.

Considering the amount of work that is being performed, Tripwire turns in an impressive performance during integrity checks. However, since Tripwire is not intended to be a real-time monitoring product, the speed of integrity checks and baseline generation is not often an issue, and is obviously always going to be dependent on the host machine on which the software is installed.

If a policy violation is detected, it is identified and described in a violation report, which is sent via e-mail or syslog to an administrator, or viewed on-screen in a text editor.

If the violation is actually an authorised change (such as the installation of a new application or a software upgrade), the administrator can instruct Tripwire to update the database with the change so it no longer triggers a violation. Such updates are performed incrementally and do not necessitate a regeneration of the baseline database.

This cycle of *policy definition – integrity check – evaluate – update* can be repeated as often as is required to refine the policy file to suit a particular environment. This is a nice feature of Tripwire – it is not necessary to get the policy file 100 per cent correct at the first try, and it is always preferable to include too much in there and remove unwanted "violations" during the update phase, than to include too little and risk missing something.

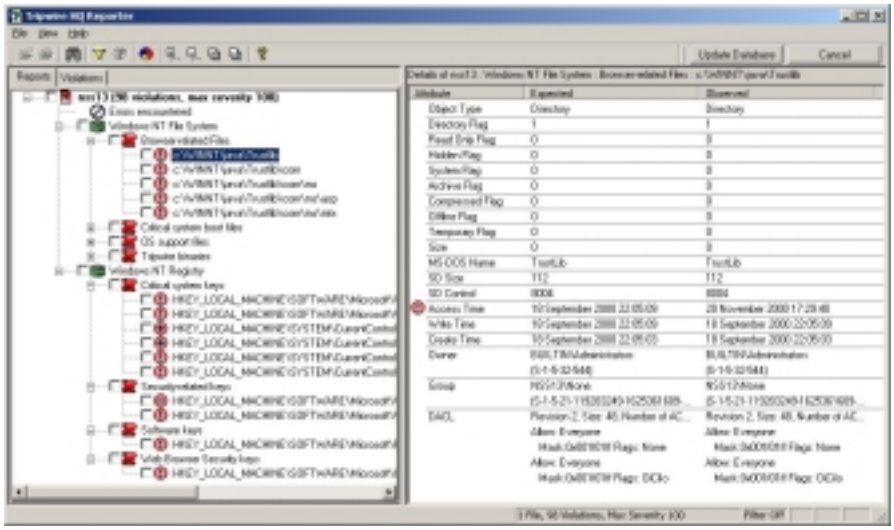

Figure 49 - Updating the database with authorised changes

Various other command line utilities are also available, enabling the administrator to print signed and encrypted database and report files, edit the various configuration files, and so on.

What is difficult with the command-line-only version of Tripwire is to ensure that all machines across the network have a consistent security policy applied, and consolidating and assessing multiple reports for different machines.

These issues have been addressed via the HQ Connector software. All of the files used for integrity assessment are located on the individual Connector machines, each machine storing a customised copy of each of the main Tripwire files. These files can be edited from the HQ Manager, or from the individual HQ Connector machines.

In stark contrast to the stand alone command-line-only Tripwire, HQ Console provides an intuitive, easy-to-use graphical interface for controlling a distributed Tripwire implementation. In addition to the standard Toolbar and Status bars, the Console contains a number of specialised windows that can be can hidden, moved, or resized to customise the appearance of the Console and make the information easier to digest.

Remote HQ Agents are registered with HQ Console in the *Machine List* window.

Details of registered machines are shown there along with information such as current status (connected, busy, idle, etc.), latest task accomplished, operating systems, and so on. An icon against each machine in the list also reflects its current state:

- **Red -** the latest report file for this machine contains one or more high severity violations.
- **Yellow -** the latest report file for this machine contains one or more medium severity violations.
- **Blue -** the latest report file for this machine contains one or more low severity violations.
- **Green -** the latest report file for this machine contains no violations.
- **Unavailable -** this machine cannot be contacted by the HQ Console because of network or configuration problems.
- **Unknown -** this machine has not yet been polled for status, or has no current report file.

The *Quick Status* window displays pie charts summarising the states of the registered machines, and the *Output* window displays various messages generated by Tripwire operations, including information about current jobs, the beginning and completion of tasks, and any errors that are encountered during normal operation. The contents of this window are also recorded in a log file for later reference.

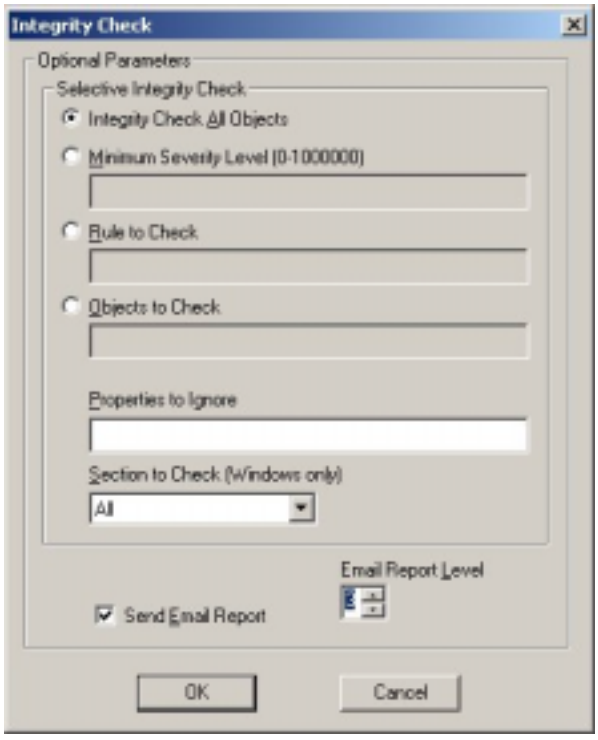

Figure 50 - Running an Integrity Check from HQ Console

The *Action Bar* is a iconised menu bar that provides easy access to commonly-performed operations (all of which can also be accessed through the Action menu, or by right-clicking the Machine List). Typical of the available tasks on the Action Bar are the *Edit Configuration File* and *Edit Policy File* options. The latter retrieves the policy file from a registered host and presents it in the main Console window for editing. Integrity checks can be triggered from this menu, and it is also possible to create a schedule for regular unattended runs.

Once created, configuration, policy and schedule files can be distributed to all machines under the control of the Console, to ensure that integrity checks are run regularly and corporate policies are enforced right across an enterprise network. Once files have been distributed, all integrity checks and other tasks are run transparently on the remote machines in the background via the HQ Agent.

Following a successful run, violations can be viewed immediately at the console (text-based reports can also be e-mailed to the administrator direct from each machine as the integrity check is completed) and remote databases can be updated to remove false alarms from future runs.

Reporting and Analysis

Once an integrity check has been completed on a remote machine, HQ Reporter (accessible from the Console Action Bar or from a separate option in the Windows Start menu) can be used to retrieve the Tripwire report and display it at the Console.

Two main reports are available: *Report Tree* and *Violations List*. On selecting the *Report Tree* tab, a tri-pane display appears with the left hand pane containing a root node for each report file, with a list of the violations and errors encountered during an integrity check.

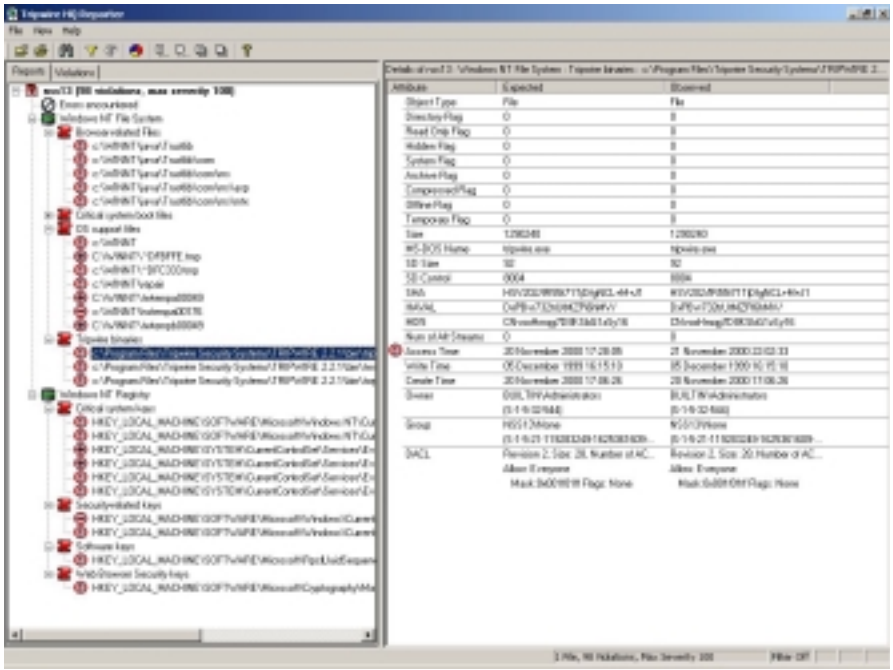

Figure 51 - Viewing reports in HQ Reporter

Selecting an item in the Report Tree displays all of the child items in the *Objects Window*. By double-clicking an item in the Objects Window, it is possible to “drill down” to see more details. Selecting an individual violation brings up further information in the *Detail Window*. Two records from the Tripwire database are displayed for comparison for each violation. The first record is the original “baseline” of the network object (file, directory, or registry setting), and the second shows the new values with a warning icon to highlight the fields that have changed.

Selecting the *Violations List* tab, displays rule violations for all reports that are open in the Report Tree window. Each entry lists:

- *An icon showing the type of violation (add, delete, or change)*
- *The name of the object causing the violation*
- *The report containing the violation*
- *The rule name associated with the violated rule, if applicable*
- *The severity level of the violated rule, if applicable*
- *The write time of the object causing the violation, expressed in the time zone of the HQ Console.*

Reports can be sorted on any of the column headings, and can also be searched or filtered to home in on violations that are of particular interest. Summary results can also be displayed graphically if required.

Verdict

Tripwire is a fairly unique product amongst those reviewed in this report. Although some IDS systems include elements of File Integrity Assessment, there are none that take it as far as Tripwire. Even Cybersafe Centrax, a host-based IDS that includes some FIA capability, provides full integration with Tripwire, automatically triggering Tripwire scans should it spot anything amiss.

Tripwire can be used in a wide range of applications outside of the field of intrusion detection. For example:

- *System and Policy Compliance –* Ensure that systems meet corporate IT standards by monitoring system files for any changes. By comparing machines to a baseline database generated from an ideal system, it is possible to detect potential security holes or configuration problems.
- *System Lockdown –* Verify that no new, unauthorised software has been installed on a system. Once a machine has been “locked down”, Tripwire software can monitor that system for unauthorised software or applications.
- *Damage Assessment and Recovery –* Tripwire can be used to assist in assessing the damage in the event of a successful attack. An administrator can use the reported violations as a list of files to repair or replace.
- *Forensics –* Tripwire reports can be used to establish a chain of evidence necessary to prosecute offenders after an attack has occurred.

Tripwire’s history – that of a hard-to-use Unix-based product – has possibly made it less attractive to many organisations to date – especially those with little or no Unix expertise. The fact that every Tripwire host had to be maintained individually would also pose problems in large corporate networks.

The latest HQ Connector product, however, removes all these objections in one fell swoop. Our only criticism of the current product offering is the lack of any GUI “Wizard-like” interface for creating policy files, a process which could still prove difficult for the less-experienced administrator. Apart from this, however, Tripwire proved itself to be easy to deploy, easy to configure and easy to manage on a day-to-day basis. Well worth considering if you require the ultimate in FIA technology.

Contact Details

Company name: Tripwire Inc.

E-mail: sales@tripwire.com

Internet: http://www.tripwire.com

Address:
326 SW Broadway
3rd Floor
Portland
OR 97204
USA

Tel: +1 503 223 0280
Fax: +1 503 223 0182

UK Distribution:
Peapod UK
The Harlequin Centre
Southall Lane
Southall
Middlesex
UB2 5NH

Tel: +44 (0)208 606 9990

PRODUCT REVIEWS – VA

AXENT ENTERPRISE SECURITY MANAGER 5.1

Axent Enterprise Security Manager (ESM) provides a combination of Vulnerability Assessment (VA) and security policy enforcement.

Its main task is to scan machines throughout the corporate network – Windows NT, several variants of Unix, NetWare and Open VMS platforms are supported - report on vulnerabilities, and aid in bringing systems into conformance with a standard corporate security policy.

Architecture

In common with other Axent products, ESM employs a three-tiered architecture for maximum flexibility and scalability.

Agent

The ESM Agent is the workhorse of the ESM system, gathering and interpreting data that pertains to a system's security. It does this periodically under the control of an ESM Manager. Security modules in the Policy analyse the configuration of the workstation, server, machine node where the Agent resides or the system where the Agent acts as a proxy and return the data to the Manager which initiated the request. The Manager then stores the data in its local database ready to be accessed by the Enterprise Console.

In addition to information gathering, the Agent is also capable of storing and maintaining snapshot files of system-specific and user account information. An ESM Agent on a NetWare server can optionally run security checks on the entire NDS tree or just a portion of the tree.

Each Agent is made up of a number of **ESM Modules**, the actual executable programs that do the checking at the workstation or server level. Modules can be customised by enabling or disabling individual Security Checks, changing the name lists associated with the checks, and by editing related Template files.

Security Modules assess a particular aspect of system security, such as user accounts and authorisation, network and server settings, or file systems and directories. **Query Modules**, on the other hand, gather general information that does not necessarily relate to security policies, information that could help in general systems administration. A Query Module could thus list all users in a particular group, or users with administrator privileges.

A number of Security Modules make up a **Security Policy**, each module addressing a different aspect of system or network security. These Policies can then be mapped to **ESM Domains**, which are groups of Agents. Initially, ESM creates a number of Domains based on host operating system, but additional ones can be created to facilitate queries and policy application to specific groups of computers – perhaps by location (UK, USA, etc.), department (finance, admin, etc.) or function (Web server, mail server, etc.).

Manager

Each ESM Manager controls a number of Agents. It controls and stores policy data, and passes the data to an ESM Agent or the ESM Console as required. It also gathers and stores security data from one or more Agents and passes this to the ESM Console on request.

The ESM Manager comprises several components, including the **CIF Server** (which controls access to Control Information Files containing data about Manager access, Domains, Agents, Policies, policy runs and templates), the **Job Starter** (which executes policy runs), the **Net Server** (which provides CIF Server, local file and Agent server access to remote systems), and the **Command Line Interface** (CLI – which provides an alternative method of executing ESM command other than via the Console).

Enterprise Console

The Enterprise Console is the primary means for the administrator to interact with ESM. The Console receives input for the administrator and sends requests to the other ESM components. As data returns, the ESM Console formats the information for display, creating spreadsheet reports, pie charts and bar charts.

Installation

In any distributed system of this kind, installation needs care and thoughtful planning, but providing the excellent Installation Guide is followed, things are very straightforward.

The basic idea is to install ESM Manager and Agent software on each machine that will be designated as an ESM Manager (these components can be installed on NT, OpenVMS, or Unix hosts, and the Agent only can be installed on NetWare hosts).

The next job is to install the Console (which works on Windows 9x and NT/2000 systems only) which can then use any of the installed Managers to do remote Agent installations on the remaining NT systems (only) on the network.

Other Agents can be installed from the CD, and the installation program will automatically attempt to register a new Agent with an existing Manager.

The documentation is excellent, and in addition to the *Installation Guide*, there is also an extensive *User Manual*, and both are provided as hard copy as well as electronic formats.

Configuration

Most of the interaction with ESM will be via the Enterprise console, which provides a three-pane interface that will be fairly familiar to users of other products in the Axent security suite.

The ESM Console has a separate console account and user environment for each user allowing different levels of administrative access. Each Manager also has its own set of user account information, so the “super user” of each Manager can restrict other users to certain Agents, Policies, Domains, Templates, and so on.

No security information can be accessed until the Console is connected to one or more Managers. By specifying connections to all Managers, it is possible to make the Console function enterprise-wide, whilst by limiting the number of ESM Manager connections on a per-user basis it is possible to create different environments for specific areas of responsibility.

Where many Managers are accessed from a single Console, it is possible to cache the user names and passwords of each Manager, and these are encrypted and stored under the Console user name and password combination.

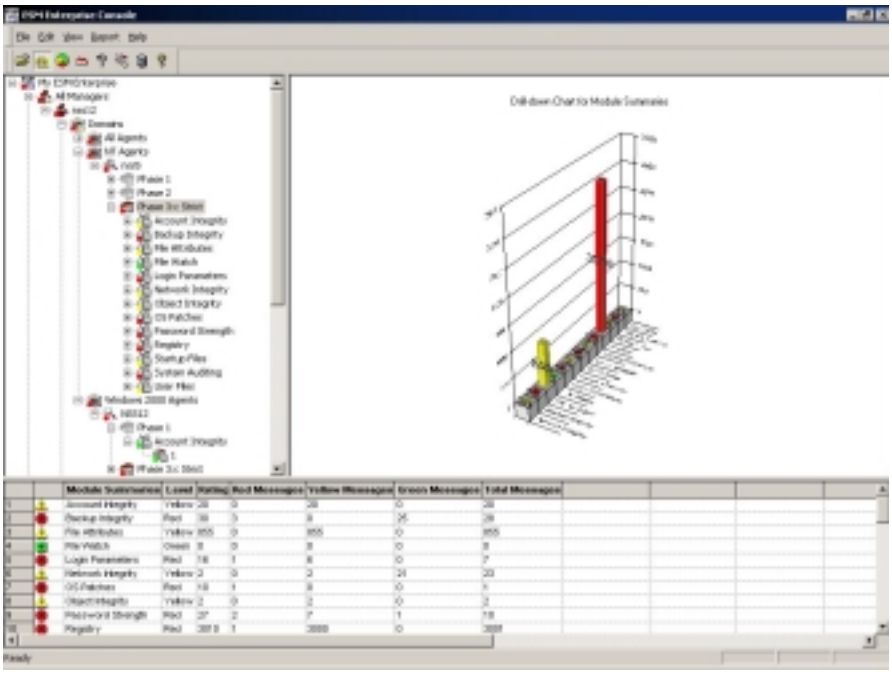

Figure 52 - The ESM Enterprise Console

The left-hand pane contains the familiar hierarchical “Enterprise Tree” display. Summary chart information is shown in the right-hand pane, whilst more detailed data is displayed in a spreadsheet grid format in the lower pane.

In the Enterprise Tree, there are four main branches – ***Summary***, ***Policies***, ***Policy Runs*** and ***Templates***.

Summary

The *Summary Branch* contains details of all the Managers and Agents accessible from the Console under the current user name. Any number of *Regions* can be created in order to group Managers together logically if required.

Under each Manager is a list of *Domains*, and this is populated automatically by ESM when Agents are installed, based on the host operating system. So to start with, you will have one Domain for each OS you have on your network (providing it has an Agent installed) and one called “All Agents”.

It is possible to create as many additional Domains as required in order to logically group Agents in any way you like – perhaps by region, or function, for instance – and Agents can be dragged and dropped between Domains (it is possible for an Agent to exist in more than one Domain at a time, if required).

Policies

As we saw in the Architecture section, an ESM Policy is made up of a number of *Security Modules*, each of which contain individual checks that are specific to the operating system against which the Policy will be applied.

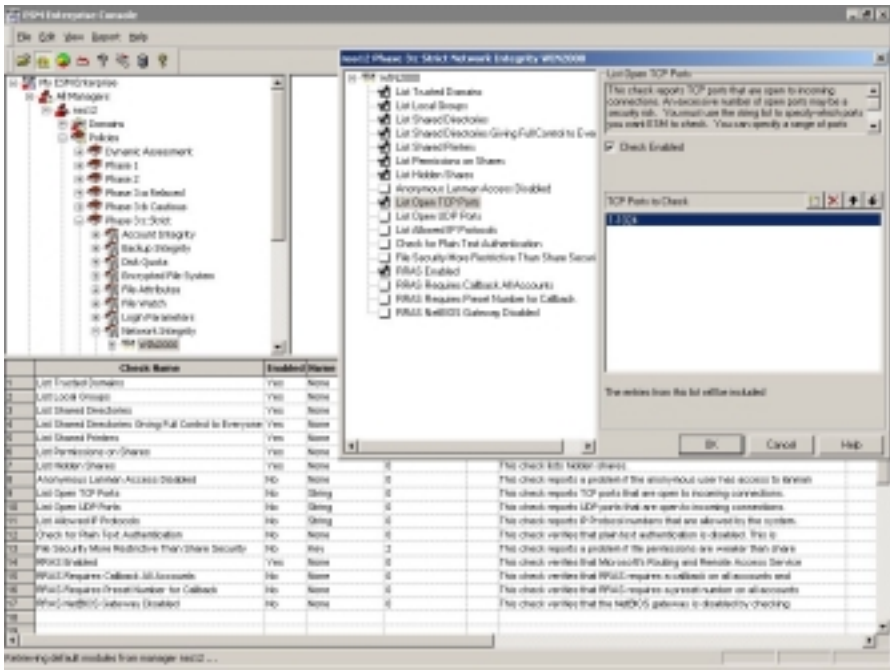

Figure 53 - Modifying policies in ESM

Creating new Policies is as simple as right-clicking under the Policies branch and then selecting the Security Modules to make up the Policy. These can be chosen from an extensive list (not all of which are available under every operating system) including:

- *Account Information (Queries)* – Retrieves information on user accounts
- *Account Integrity* – Identifies account privileges that exist outside of the established security policy
- *Login Parameters* – warns of potential break-ins and failed login attempts
- *Password Strength* – ensures that passwords conform to company security policy in length and strength
- *User Files* – identifies suspicious files in user directories
- *Backup Integrity* – ensures backups are done on a regular basis
- *Discovery (Queries*) – scans and reports on open TCP ports on the network
- *Network Integrity* – examines vulnerable network points of system entry (Internet connections, NFS, etc.)
- *Object Integrity* – checks for weaknesses or inconsistencies in ACL support, as well as identifying new devices, deleted devices and device changes.

- *OS Patches* – ensures that the latest OS patches and service packs are applied
- *Startup Files* – ensures that only authorised programs and services are started at boot time
- *System Auditing* – ensures that auditing and system accounting is enabled correctly
- *System Mail* – checks for known problem areas in Unix and verifies the security of the mail system
- *System Queues* – checks Unix *cron*, *batch* and *at* utilities, as well as file integrity, to prevent potential break-ins
- *File Access* – examines permissions of user-specified files and identifies which accounts can access those files.
- *File Attributes* – checks for changes in system file attributes including read, write and create privileges, as well as file create time and date.
- *File Find* – prevents the unauthorised use of files or systems by checking executables and other files for anomalies such as viruses, Trojan horses, Unix sticky bits set, and other corruptions
- *File Information (Queries)* – lists users and their effective rights to specified directories and files
- *File Watch* – compares files found on the network against Templates or previously taken Snapshots looking for unauthorised changes
- *Registry* – runs CRC/MD5 checks on Windows Registry values

Each and every System Module contains a number of Security Checks (specific to each OS) that can be enabled or disabled by selecting the appropriate check box.

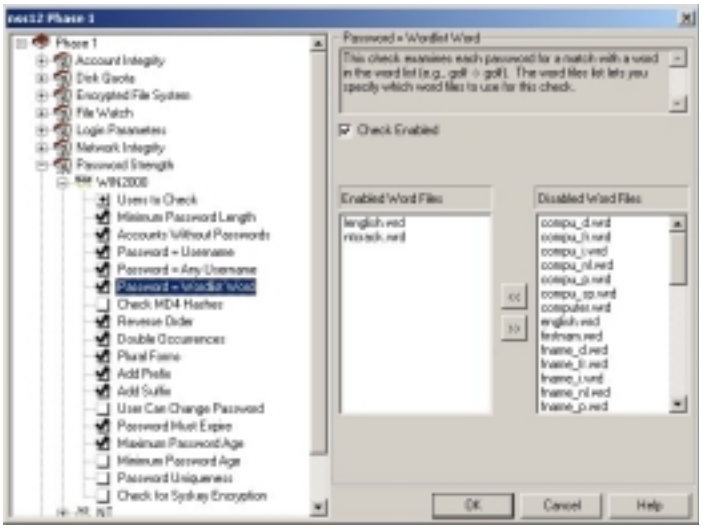

Figure 54 – Security Checks

For example, the *Password Strength* module contains such checks as:

- *List of user names to include/exclude*
- *Minimum password Length*
- *Check password is not the same as user name*
- *Check password is not in one of the "common password" lists*
- *Maximum password age*
- *Ensure password expires*
- *Can user change password?*
- *And more….*

As you can see, the combination of Security Modules and Security Checks provides the means to create some incredibly comprehensive and complex Security Policies, as well as Policies that allow incredibly fine-grained control over your corporate security stance.

Luckily, Axent has provided a number of default Policies out of the box that provide an excellent start in ensuring your corporate network is not wide open to attack :

- *Phase 1* – checks the most significant and potentially problematic security areas on any system
- *Phase 2* – includes all the available ESM Modules, but only the key Security Checks in each Module
- *Phase 3: Relaxed* – identical to the Phase 2 Policy
- *Phase 3: Cautious* – the *Relaxed* version, with additional Security checks enabled
- *Phase 3: Strict* – enables *all* the security in *all* the modules available to your operating system.
- *Queries* – lists information about users and accounts, as well as identifying systems on the network that are candidates to have ESM and Intruder Alert components installed.

These policies correspond to the increasing levels of security that you can apply to your systems.

Policy Runs

Policies are applied to Agents by simply dragging and dropping the entire Policy (or an individual Security Module) onto the appropriate point on the Summary branch, thus creating a *Policy Run*. There is also a Policy Run Wizard to take you step by step through creating a new Policy Run from scratch, and Policy Runs can be scheduled to run regularly and automatically.

The scope of the run is determined by the point on the Summary branch at which the Policy is applied. For instance, dragging a policy to an individual Agent runs the Policy against that machine alone, whilst applying the Policy to the branch named *NT Agents* or *All Agents* creates Policy Runs across multiple machines. Which modules are applied is obviously determined by the host operating system of the Agent matching the OS-specific modules within each Policy.

All of this is completely automatic – all the administrator needs to do is to decide that he wants to run a minimum password length check against every machine on his network, and drag the appropriate Module or Policy to the appropriate point on the Summary branch. The Console transmits the appropriate instructions to the various Managers, which in turn instruct the Agents under their control to run the specified security checks.

Once a Policy Run has completed, the Agents return the data to the Managers, and this is immediately accessible via the Console in a uniquely numbered folder underneath the Policy Runs branch. This basically represents a “snapshot” of the current security profile of the target machine. Double-clicking on the appropriate entry will bring up a window showing the current state of the Policy Run, and the Agents to which it was applied. Clicking on any of the Agents allows the administrator to view exactly which Security Modules were run by each Agent.

Details of each Policy Run are also stored automatically in the Summary branch beneath each applicable Agent, and each applicable Region. It thus does not matter how the administrator chooses to browse the Enterprise Tree within the ESM Console, the relevant information is always quickly to hand. We found the ESM user interface to be the most intuitive of all the Axent products, despite the underlying complexity.

Against each Policy run the Console shows the Security Modules that were carried out and the results are presented in a “drill down” interface that allows the administrator to navigate quickly through different levels of charts and text displays. The end result is spreadsheet-style grid report containing a list of the individual Security Checks with a red, yellow or green “flag” against each one to highlight the status of the test, together with more detailed information on what was found.

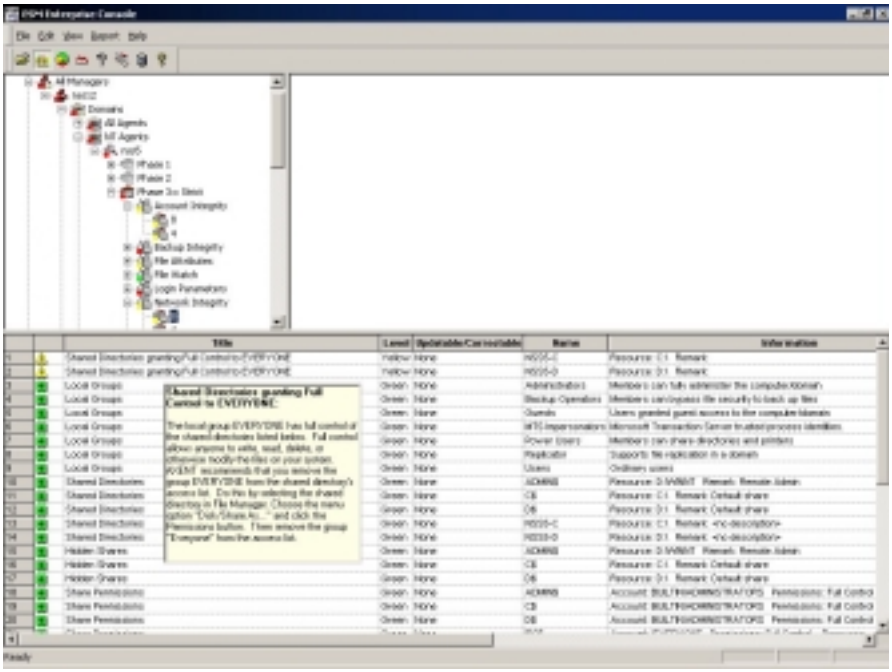

Figure 55 - Viewing Policy Run results

The severity and number of the flags is taken into account when applying an overall rating to the Policy Run, and an appropriate coloured flag is raised against the Policy branch above it. ESM repeats this process, rolling level and rating information up from Policy to Agent, from Agent to Domain, and onwards all the way up the Enterprise Tree. This provides an immediate visual indication of where the security problems lie when viewing the ESM Console at any level.

ESM does more than just report on security problems, however, it can also help you bring your system into conformance with your chosen security policy.

This is done via a context menu accessible from the grid report. One option is “Correct”, which allows the administrator to correct ownerships, permissions and user privileges of certain files (or Registry settings) on an Agent system. When such changes are made, any previously-taken Snapshots can be updated with the change, and there is also an “undo” option available.

Should the administrator decide that the reported variance in policy is acceptable, it can be marked as “suppressed” so that it will not appear on future reports. Finally, if ESM finds a system that is capable of hosting an ESM Agent, but which currently isn’t, it will provide the option to perform a remote install.

Templates

When an ESM Module runs on an Agent, it looks for exceptions to the security policy determined by the administrator. Exceptions can either be as a result of non-compliance to the policy or differences between the baseline Snapshots of the system (as established by the administrator and stored in the ESM database), and the current system state when the policy is run.

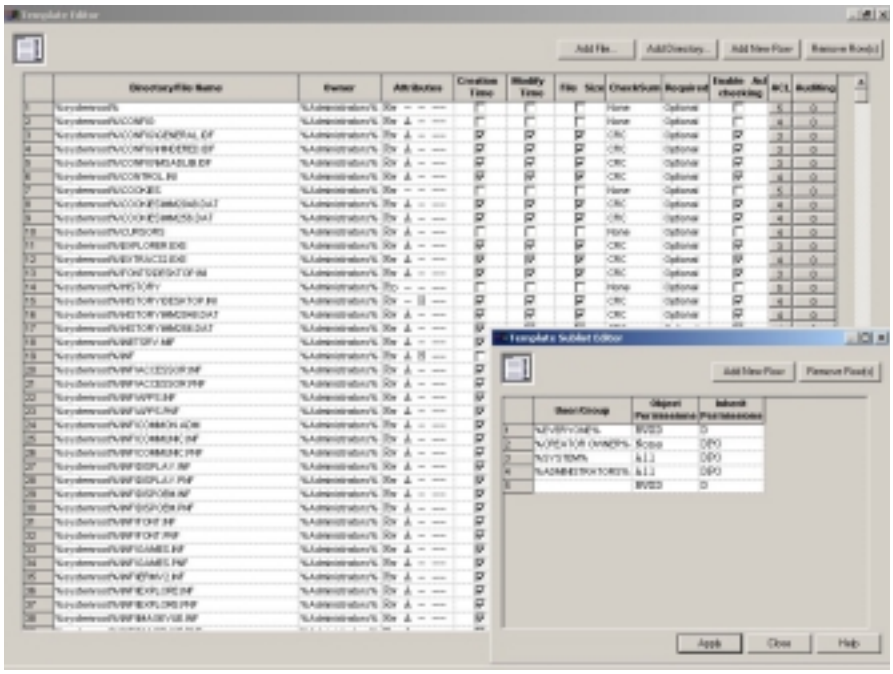

Figure 56 - Template editor

Some ESM Modules use Templates to determine non-compliance to policy. A Template is simply a list containing definitions of objects (files, OS patches, Service Packs, etc.) and their expected state.

This provides ESM with the totally flexible means to compare current state of any part of the network against expected state and thus report on any deviations from policy.

Snapshots are simply “special” Templates that are produced automatically by ESM as a result of scanning the system, and which contain a “picture” of the system state at any given point in time, against which future runs can be compared.

Reporting and Analysis

There are a limited number of reports included within ESM, producing a standard HTML report of information included in the Console grid and chart views.

Unfortunately, there is no means to print any of these reports (unless you count printing from the browser, which is far from satisfactory for Internet Explorer users prior to release 5.5), and if you need to produce customised reports, it is necessary to import ESM's Summary Database into third-party reporting applications such as Crystal Reports or Microsoft Access.

The following standard report types are available:

- *Security Report –* presents non-complaint security-related information in summary and detailed formats
- *Domain Report –* lists all Agents in a Domain together with important information about each Agent, including the Agent's operating system, version, network protocol, network port and system type
- *Executive Report –* a one page summary that displays the enterprise's conformity (as a percentage) to each Security Module
- *Policy Report –* provides information about individual Policies, including the number of Policies, Modules, and Security Checks
- *Policy Run Report –* contains the start and completion time, Policy name and Domain name for all jobs run on the Manager
- *Template Report –* list all objects in a specific Template

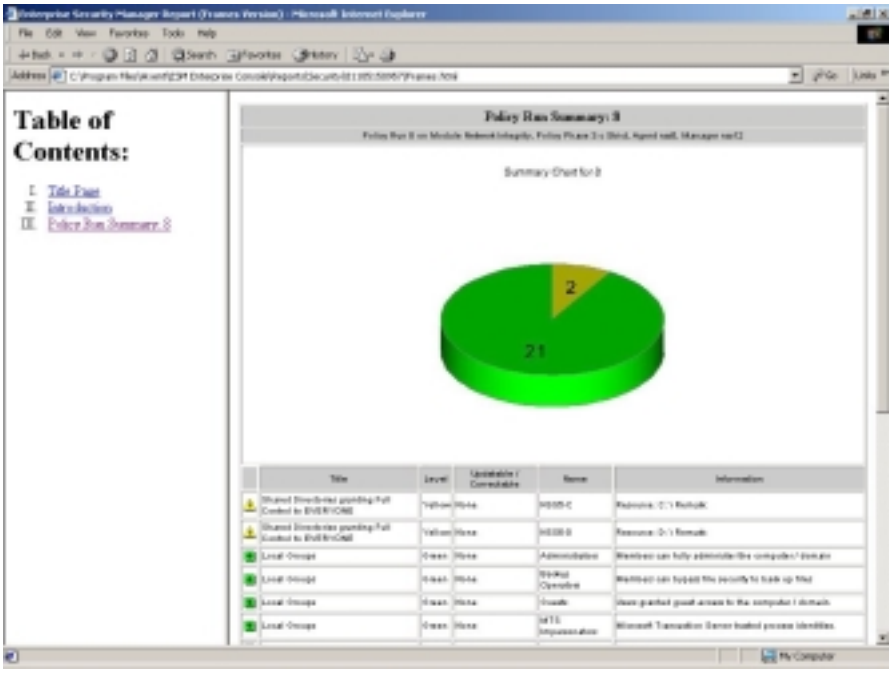

Figure 57 – Viewing the Policy Run report

Each report contains the following sections:

- *Title page (can be customised with the organisation name and logo)*
- *Table of contents*
- *Introduction*
- *Report body*

The body of the report is certainly detailed, and the built in reports will suffice for most organisations. It would be nice to have the ability to print a report from within ESM, however.

Verdict

Enterprise Security Manager goes far beyond most VA and auditing tools to provide a complete environment for defining, auditing and ensuring conformance to a corporate security policy.

Whilst is does not cover exactly the same ground as “hacker in a box” active VA tools such as NetRecon, that would be too much of a duplication in functionality, given that Axent already has such a product in its arsenal. Instead, ESM opts for integration with NetRecon, incorporating all vulnerabilities found by NetRecon into its own security analysis.

Our only criticism of the product would be the lack of a printed report option within ESM itself, but apart from that there is not much with which we can find fault.

The user interface is very clear and intuitive, and the idea of rolling security ratings from the individual Policy Runs all the way up the Enterprise Tree to give an instant visual indication of conformance is excellent. Policy definition is simple to do, and applying Policies and running security checks is just as easy, whether for a single check on a single machine, or a whole range of checks across the entire network. Policies can be incredibly complex and provide extremely fine-grained control of security, but the excellent documentation provides a complete reference of every single Security Module and Check.

Cross platform support is also extensive, and it is hard to see how any organisation can do without a tool like this.

Contact Details

Company name: AXENT Technologies, Inc.

E-mail: info@axent.com

Internet: www.axent.com

Address:
2400 Research Boulevard
Rockville
Maryland 20850
USA

Tel: +1 (301) 258-5043
Fax: +1(301) 670-3586

AXENT NETRECON 3.0.9

NetRecon is the vulnerability assessment part of Axent's security suite, designed to analyse and report holes in network security. It achieves this through conducting an external assessment of network security by scanning and probing systems on the network. NetRecon re-enacts common intrusion or attack scenarios to identify and report network vulnerabilities, while suggesting corrective actions.

Other products in the suite include network IDS (NetProwler), host-based IDS (Intruder Alert), and security policy auditing and enforcement (Enterprise Security Manager).

Architecture

There are three main components to the NetRecon architecture: the *GUI*, the *scan engine* and the *scan modules*.

- ***Graphical User Interface -*** This provides the means for the administrator to configure and initiate scans, examine the results on-screen, and run reports to provide more detailed analysis. Data is stored in an MS Access database as well as in NetRecon .NRD files.

- ***Scan Engine -*** The scan engine stores and processes the data generated by the modules. The scan engine consists of a data repository where the data is stored (MS Access), a data processor, and agents that monitor input from and output to the modules. The data processor receives data from the modules in the form of records, and decides whether that data should be added to the repository. The data processor also decides which records in the data repository should be sent to which modules. The ability of the scan engine to process data from multiple objectives, allowing them to share information with one another quickly and efficiently, is referred to as *Progressive Scanning* technology.

- ***Scan Modules -*** Modules perform all the network scanning. There are several modules that allow NetRecon to run individual objectives more quickly (by permitting only relevant scanning to be performed), and allow a complete scan to run more quickly (by performing many scanning operations in parallel). Modules use NetRecon records as both their input and output. New vulnerability checks can be added quickly and easily by Axent as new scan modules, and these can be obtained via the automatic Web-based update process from the Axent Web site.

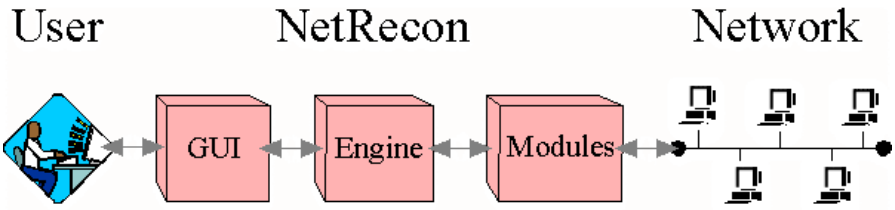

Figure 58 - NetRecon architecture

Progressive Scanning technology executes checks in parallel and shares information obtained during the scan to search for deeper weaknesses. In addition, it learns as it goes, adapting the penetration strategy based on previous results.

The idea is that whereas other scanners can identify security weaknesses, NetRecon can exploit those weaknesses and show which potential threats demand immediate countermeasures.

An example of *Progressive Scanning* might be:

- *System A is discovered by NetRecon and identified as a Unix system.*
- *NetRecon discovers NIS services on System A.*
- *The NIS files, which contain encrypted passwords, are sent to NetRecon.*
- *NetRecon uses the small and large dictionaries to crack the user's password.*
- *NetRecon then tries the user ID and cracked password on all other systems in the network. Since users often use the same passwords, the network's security is compromised even deeper.*
- *NetRecon determines the level of access (root, admin, etc.) and assigns a risk value.*

In short, where other scanners might report a number of unrelated potential vulnerabilities, NetRecon attempts to combine those (even across multiple machines) to gain real access to a system or highlight the potential for a Denial of Service (DoS) attack, thus providing, in theory, a much more useful set of results.

Below are a few of the vulnerabilities NetRecon checks for:

- ***Resource discovered -*** Normally the first vulnerability checked for is whether or not a network resource can be discovered. For TCP/IP systems NetRecon sends a ping broadcast over the network to see which systems respond. Other protocols such as IPX are used to discover NetWare systems.
- ***Exec service enabled -*** The exec service (also called rexec) provides remote command execution facilities with authentication based on user names and passwords. NetRecon checks for many other common services that are known to be vulnerable to attack.
- ***SMTP decode alias enabled -*** Including a decode mail alias in */etc/aliases* makes it easier to send and receive binary files by e-mail. Unfortunately, a decode mail alias can be used to create or overwrite files on the system. NetRecon checks for a number of vulnerabilities in the smtp service and related programs (such as sendmail).
- ***Null session access obtained -*** In Windows NT networks with multiple domains, some Windows NT programs and services use null session connections to enumerate account names and available shares. NetRecon checks for this.
- ***User level access obtained –*** This vulnerability exists if NetRecon can login to a network resource as a valid user. NetRecon uses login names and passwords it obtains from various sources to attempt access regardless of the system type (e.g., Windows NT, UNIX, NetWare). The first step in gaining administrative access to a machine is usually to get access as a normal user. With NetWare, Windows NT, Samba servers, and others, NetRecon attempts to enumerate all exposed file systems (possibly using null session connections) and connect with the shared directory using known login names and passwords.

- ***Discovered system type –*** Discovering the system type is a big help to someone trying to break in. For example, if attackers can detect that a system is running Windows NT 4.0 without service pack 3, they can exploit a number of well-known vulnerabilities.
- ***NIS encrypted password obtained –*** The NIS service (also sometimes called yp, for yellow pages) allows transfer of information between hosts that share administrative control. NIS servers typically contain databases (also known as maps) of passwords. If attackers can locate NIS servers and obtain password maps, they can extract encrypted passwords to crack using any resources available to them.
- ***Password cracked using small/large dictionary –*** If an attackers can obtain encrypted passwords from a system they can encrypt passwords from a dictionary and compare them to the passwords obtained from the victim, thereby guessing any passwords that match words in the dictionary. NetRecon uses a small dictionary (for speed) and a large dictionary (for completeness) to try to guess passwords.
- ***Local disks mountable via SMB –*** SMB (server message block) is a standard message format used by many operating systems to share files, directories, and devices. Windows NT 4.0 with no service packs by default allows SMB clients (such as Samba) to mount any local drives with read/write permission. An attacker can use this method to gain unrestricted access to the local disks of an NT workstation.
- ***Ports active –*** Active ports indicate services in use, and in many cases, an inquiry to an active port causes the service to return information about itself (such as its name and version). NetRecon performs separate scans for privileged ports (1-1023), which indicate services running with administrative rights, and non-privileged ports (1024-65535).

NetRecon can be integrated with Axent's Enterprise Security Manager (ESM) via the ESM integration module, feeding all the discovered vulnerabilities into the policy enforcement engine of ESM for further analysis.

Installation

Installation is very straightforward, requiring only a single Windows NT 4.0 machine (workstation or server) with 64MB RAM and 40MB of hard disk space.

Axent has adopted an extremely user-friendly and cost-effective method of licensing. A limited (254 node) license or unrestricted license can be purchased for a single organisation (compare this with the per node license model used by some competitors), and a consultant's license can also be obtained for unlimited use in multiple organisations.

Documentation is not particularly extensive, but to be honest, it is not required. The *Installation and Getting Started Guide* which is provided as hard copy out of the box is more than adequate to get you up and running.

The NetRecon installation routine attempts to determine if ESM is installed on the system, and if it finds an ESM Agent, it asks if it should install the ESM/NetRecon integration software, whereupon it will prompt for a user name, password and ESM Manager ID. This registers the integration module to a particular ESM Manager, which can be on a remote system.

Configuration

The graphical interface bears some strong similarities to the other products in the Axent security suite, and is very easy to master. It consists primarily of one main window, which is broken up into three panes - the *Control* pane, the *Graph* pane, and the *Data Table* pane.

The Control pane is where the administrator initiates scans. Listed in a hierarchical tree display are a number of “objectives”, under the headings of *Light*, *Medium* and *Heavy* scan. There is very little to do in the way of configuration, since the policies are fixed and there is no way to change them or to meddle with the settings of the individual scanning modules.

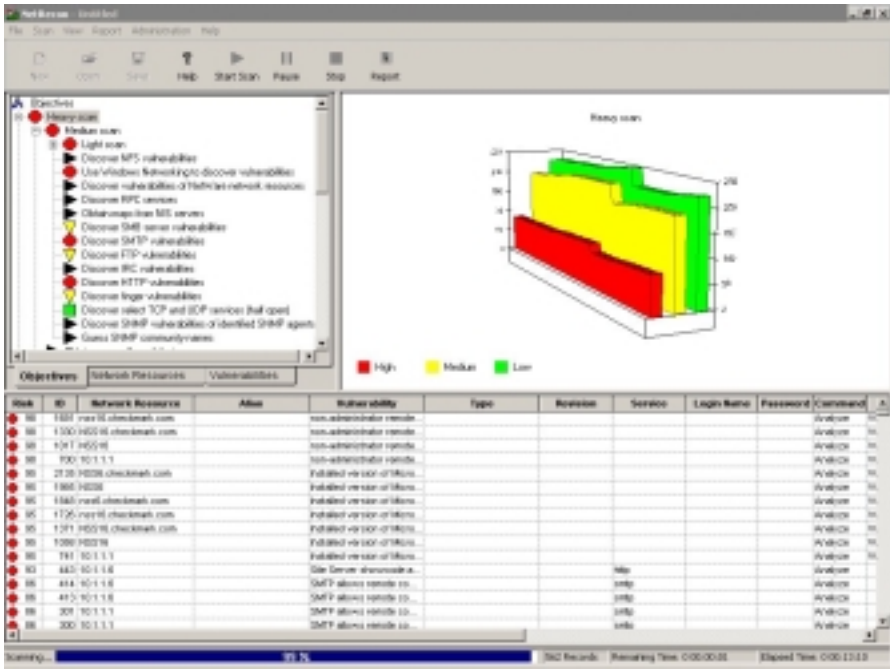

Figure 59 - The NetRecon Console

The *light intensity* scan will identify network resources including alias information, operating system, version, and so on. It simulates the first logical stage of an attack, looking for problems that are simple to detect, unlikely to cause target systems to fail, and likely to yield results quickly. It finds information that can be used to focus the second stage of an attack, and thus elimination of vulnerabilities reported by a light scan should discourage or complicate the second stage of an attack. It will also use Windows Networking to find vulnerabilities and employ a selective scan for services known to have vulnerabilities such as SMTP.

A *medium intensity* scan will simulate the first and second stages of an attack (each level of attack automatically includes all the modules from the level before it). In order to extract more detailed and complete information than a light scan, a medium scan will try things that are less likely to yield results and are more time consuming. The medium scan will perform a complete TCP and UDP port scan (both half-open and full connect) and look for a broad range of vulnerabilities in common service protocols such as NIS, HTTP, NFS, SMB, and FTP.

A *heavy intensity* scan should ultimately identify most security problems that can be detected remotely with a reasonable level of safety. Heavy scans are not as cautious as light and medium scans, and are therefore more likely to cause accounts to be locked out, or network resources to become unresponsive. No intentionally dangerous checks are performed in a heavy scan, however, since NetRecon does not contain any true DoS or “crash” code, but heavy scans may stress sensitive software and hardware.

Once the appropriate scan level has been selected, a dialogue box appears prompting for the range of machines to be scanned. Host names and addresses (single, multiple or ranges) can be entered, or NetRecon will ping sweep the subnet to build a list of suggested resources. A scheduling function is provided to schedule scans to execute after a predetermined amount of elapsed time, or at a specific day and time.

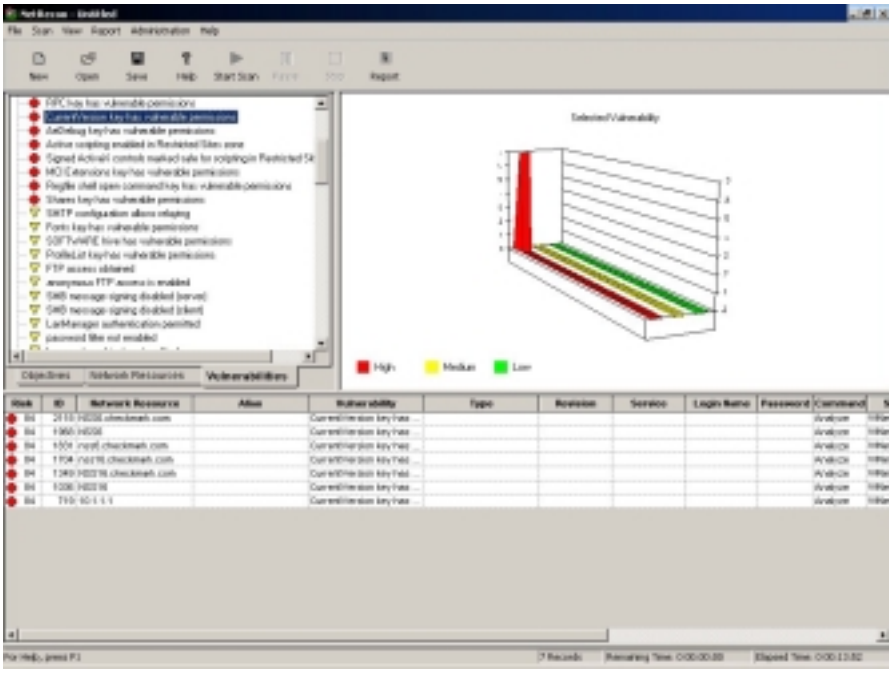

Figure 60 - Examining individual vulnerabilities

During and after execution, the Data Table lists individual vulnerabilities and potential problems in detail, whilst the Graph window summarises these pictorially, categorising vulnerabilities into high, medium, and low risks. The Graph pane, therefore, gives a quick visual overview of the scan results, whilst the Data Table pane is a view into the data repository (part of the scan engine). The Data Table provides information such as the risk ID, network resource name/IP, vulnerability name and ID number, service details, port number, version number, protocol, and all banner/connection responses, and can be sorted on any one of the columns. The icons against each scan module in the Control pane also turn different colours depending on the results of the scan for an instant visual notification of problems.

Once the scan is completed, the data can be viewed in a number of different ways. For example, as individual scan modules are selected in the Control pane, the full display of all vulnerabilities in the Data Table is replaced by just the vulnerabilities relating to that particular scan.

Another tab in the Control pane is labelled *Network Resources*, and this shows a list of all resources discovered during the scanning operation. Selecting individual resources brings up a list of vulnerabilities in the Data Table relating only to that resource.

The final tab in the Control pane is labelled *Vulnerabilities* which, as you might expect, contains a list of all vulnerabilities discovered during the last scan. Selecting any of those brings up a list of all instances of that particular vulnerability in the Data Table.

Each time a new list is generated in the Data Table, the Graph pane is updated to show charts of the new contents. The interaction of the contents of the tabs in the Control Pane, the Data Table and the Graph pane makes it very easy to drill down and view the nature of the vulnerabilities found during a NetRecon scan.

The drill down capability is taken one step further in the Data Table too. Right clicking on a vulnerability brings up a context menu from where it is possible to display a detailed description of the vulnerability along with any potential solutions and links to further information, and the Path Analysis.

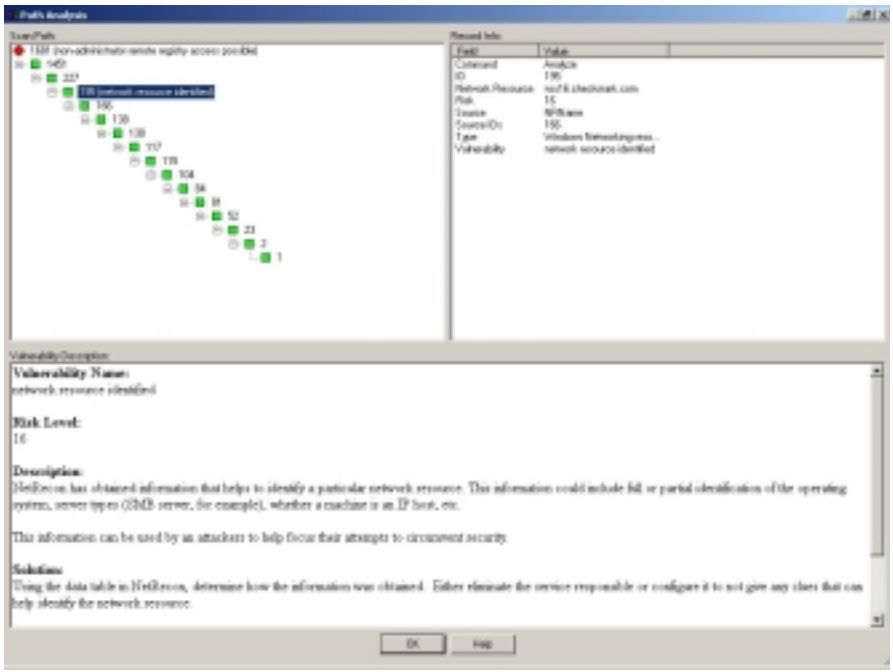

Figure 61 - Path Analysis

The Path Analysis provides the means to see not only what vulnerabilities were discovered on the network, but also *how* those vulnerabilities were discovered. Since NetRecon uses some vulnerabilities to discover others via its Progressive Scanning capability, it's often useful to know exactly what steps it took to perform a particular exploit. This is what the Path Analysis display shows, allowing the administrator to determine exactly which vulnerabilities are acting as "gateways" that can lead to other information gathering and exploits. This is a unique feature amongst the scanners we have seen, and is potentially very useful.

Reporting and Analysis

Despite the excellent on-screen analysis of scan results, it is always useful to be able to produce printed reports.

Crystal Reports are now provided with NetRecon, and there is a small number of built-in report templates that generate standard reports targeted for varying audience levels. The user has the ability to select between three report formats: *Executive Report*, *Detail Report by System*, and *Detail Report by Vulnerability*.

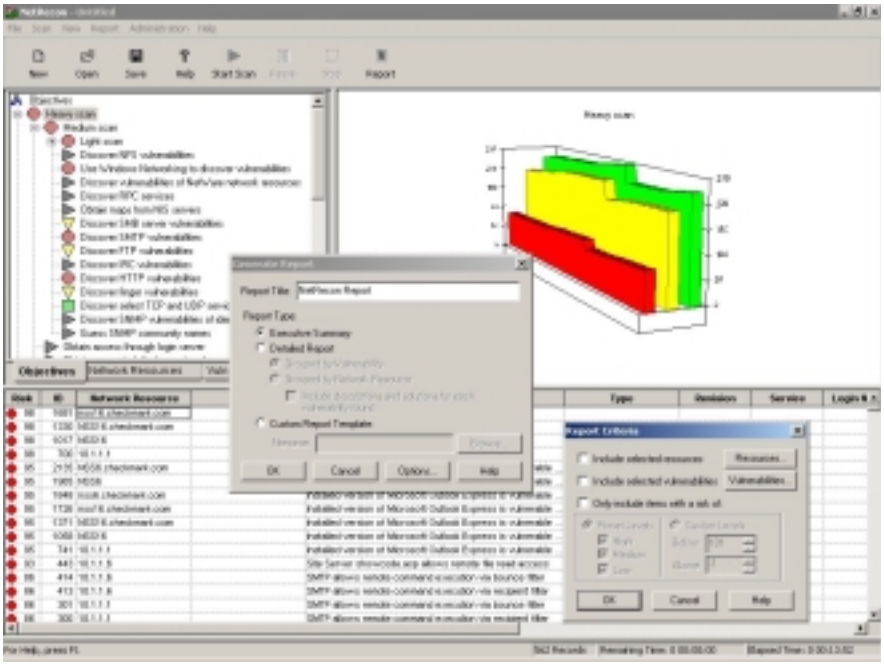

Figure 62 - Creating reports

Reports may be viewed on line with the Crystal viewer, which provides a hyperlinked navigation tree in the left hand pane – grouped by vulnerability or host – and the report detail in the right hand pane. After viewing on screen, reports can be printed or exported to a variety of formats including Word, HTML, Excel, rich text format and others. Custom reports may also be used in NetRecon if you have the Crystal Reports Designer.

In addition to the scan data reports, there are also two “static” reports included with NetRecon which administrators will find very useful. *View Objective Descriptions* provides details of what each of the scan objectives is trying to achieve, whilst *View Vulnerability Descriptions* provides a detailed list of all the vulnerabilities covered by NetRecon together with solutions and links to additional information.

It is not possible to customise the contents of any of the built in reports within NetRecon, nor is there a huge choice of available reports. However, most of the information you will need is contained within the few reports available – adequate is the best way to describe NetRecon’s reporting capabilities.

Verdict

In use, NetRecon is fairly simple, and it does not appear to be necessary to have a detailed knowledge of hacking in order to run it, unlike some of the competition. Of course, without the means to tweak and configure your own set of test parameters, NetRecon might overlook something, but there will always be a trade-off between flexibility and ease of use – NetRecon is extremely easy to use. However, on its "Heavy Scan" setting, it will frequently produce a list of far more discovered vulnerabilities than competitors with much larger vulnerability databases, which can make the reports cumbersome and difficult to wade through.

At the end of the day, NetRecon is actually quite a different prospect to the more traditional "hacker in a box" type of VA Scanner. It's vulnerability database is not as extensive as some (though with over 440 it is not doing badly), and it is not possible to tweak the parameters of a test or perform DoS attacks directly. However, it supports NetWare and VMS, as well as NT and Unix, and its *Progressive Scan* technology provides a means to look beyond individual vulnerabilities to identify real threats.

This provides a systematic understanding of how network vulnerabilities are interrelated and how high risk vulnerabilities may be caused by other lower risk vulnerabilities in the network. This unique feature means you can focus on the true cause of your vulnerabilities for immediate correction without having to decipher exhaustive lists of symptoms of the problem.

NetRecon is thus geared less for the security specialist and more for the network administrator, or perhaps novice security administrator (although the Path Analysis output from the Progressive Scanning technology could be of tremendous use to anyone, no matter how experienced). It also complements ESM perfectly, providing network-based assessment to integrate with ESM's host-based assessment.

Contact Details

Company name: AXENT Technologies, Inc.

E-mail: info@axent.com

Internet: www.axent.com

Address:
2400 Research Boulevard
Rockville, Maryland 20850
USA

Tel: +1 (301) 258-5043
Fax: +1(301) 670-3586

BINDVIEW HACKERSHIELD 2.0A

If anyone should know about security auditing it is BindView, having produced a very successful line of NetWare and NT auditing tools over the years. It is only natural, therefore, that they should venture into the Vulnerability Assessment market place.

HackerShield takes a slightly different approach to the normal “hacker in a box” type products however. Aimed more at the network administrator than the security professional, it combines elements of vulnerability assessment, security policy enforcement, system auditing and file integrity checking in a single package.

Installation

Installation is straightforward, with nothing in the way of options to sidetrack or confuse you. Simply log in as a user with admin privileges, pop in the CD and click on “Install”.

Once installation has finished, you have the chance to run the product on an evaluation license, or to install a license key to determine the number of IP addresses that can be scanned.

Configuration

HackerShield presents the administrator with an Outlook-style three-pane interface. The icons in the left-hand pane provide access to Reports, Targets, Jobs and Archive. On the right is a network map and a list of target hosts.

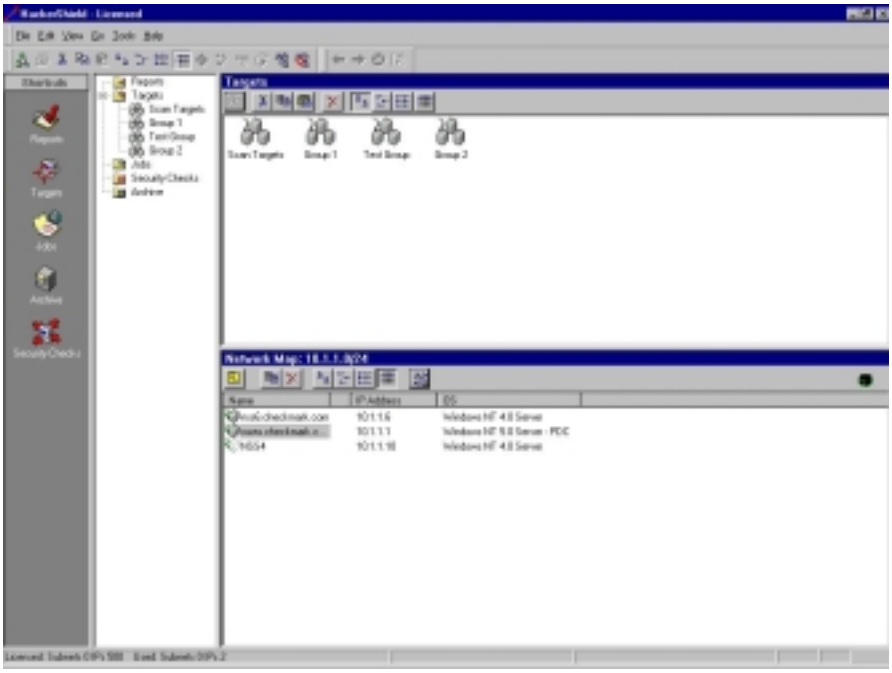

Figure 63 - The HackerShield Console

Just as with Outlook, it is possible to have both an iconised “shortcuts” toolbar or a hierarchical folder display down the left side of the screen (or both if you wish).

It is also possible to quickly add or remove items from the shortcut toolbar in order to personalise it – again, just as with Outlook. This user interface will certainly offer a high degree of familiarity to anyone familiar with Microsoft's mail client.

The Network Map window is where HackerShield goes out to the network and discovers hosts in order to make them available for scanning. This can make getting your first scan going a slower and more fiddly process than it needs to be if you actually know what you are doing and which hosts you want to scan. However, the ability to list all the hosts on a subnet can make life easier for those who are not as confident in such areas.

Initially, the Network Mapper scans only the local subnet, but additional subnets can be added by right-clicking with the mouse and entering the IP and net mask details. Once added, these subnets too can be scanned by the Mapper. For hosts which you know exist, but which are not showing up on Mapper scans for some reason, it is possible to manually add a host.

Once you have your network mapped, you need to drag the individual hosts or complete subnets across to the Target pane before you can scan them. Multiple target groups can be created to logically group machines together for scanning, allowing you to run separate scans easily on your "*Sales*" PC's and "*Finance*" PC's, for example. It is also possible for the same host to exist in multiple groups. The Target window behaves as your "licensed hosts pool", and the number of available units is reduced automatically each time one or more hosts is dragged from the Network Map to the Target window.

Once you have your Target Groups assembled, right clicking on either a group or an individual host within a group brings up the scanning menu. A small number of pre-defined scanning policies are available for immediate use:

- ***Normal*** *– a subset of common checks*
- ***All*** *– a comprehensive scan (all checks enabled, including dangerous DOS attacks)*
- ***Latest Update*** *– when RapidFire Update is installed, this policy reflects the new checks from the latest update*
- ***Quick*** *– a minimal set of checks*
- ***Password Cracker*** *– password cracking only*

These are enough to get most administrators off and running with a minimum of fuss, and all that is required is to select a policy and confirm your choice in order to initiate a scan. During the scan HackerShield brings up a very informative real-time status window showing the scan progress for every machine selected, including which module is currently running and how many vulnerabilities have been found so far.

Existing policies can be amended and new policies created in the Security Checks window. This is a fairly straightforward process, even for the non-security minded, since there is not much scope for modification or customisation. This means that it has limited scope for the true security professional, but makes the product much more attractive to the average network administrator who is not a security specialist.

The available checks are divided into a number of categories such as Denial Of Service (DOS), DNS, C2, FTP, mail server, Web server, file sharing, passwords, user accounts and information gathering (amongst others), with something of a bias towards NT-specific vulnerabilities.

It is also apparent that there are nowhere near as many vulnerability checks included in this product as there are in some of the mainstream VA products, but BindView is working hard to rectify this.

Entire sections can be selected or deselected using a single check box, or individual tests can also be included or excluded in the same way. Each vulnerability test has a brief description against it, along with a more detailed (and often very extensive) description available at the click of a button. It also has a Security Check Configuration box associated with it, but for most tests this is greyed out and unused.

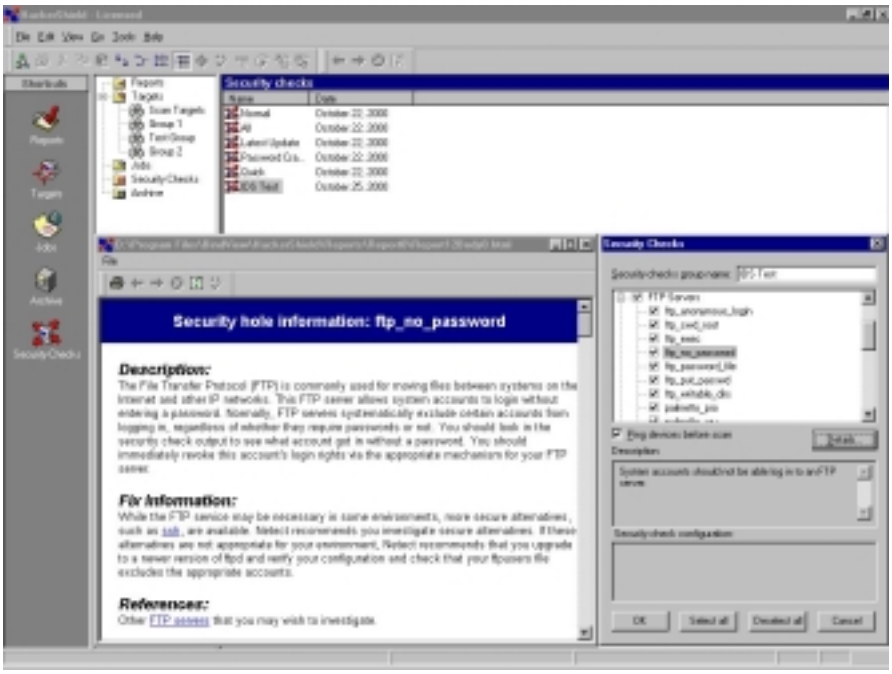

Figure 64 - Modifying scan policies

One example of where HackerShield will prove too limited for a real security professional is with TCP port scanning. You would expect the Security Check Configuration to allow you to select the range of ports to be scanned, as well as the type of scan to carry out (full connect, SYN stealth, FIN stealth, and so on). Unfortunately, HackerShield allows none of this, and nor is there any clear indication of what sort of port scan is performed or over what range of ports.

However, as we have already said, whilst this lack of flexibility may be an issue for some, it certainly has the effect of making the product very easy to run by almost anyone – no hacking knowledge required. Some of the competition requires an in depth knowledge of what the tests are actually doing in order to configure them effectively, and that could lead to incorrect configurations resulting in some of the tests being invalid. HackerShield is obviously designed to steer the administrator in the right direction wherever possible.

Another example of this is the Scan Wizard, which hand-holds the user through all the steps just described, in order to create a new scan job. Once completed, scans can be run immediately or saved as jobs for scheduling at off-peak times or for repeated running.

This provides the means for an administrator to maintain a constant watch over his network, continuously scanning for security holes that can occur when hardware, software and users are added to or modified on the network.

When security holes are discovered during a scheduled scan, HackerShield automatically issues an alert via e-mail or an SNMP trap. One very powerful feature of HackerShield is the ability to auto-fix certain problems it finds during a scan. There is nothing worse than a vulnerability scan throwing up tens or even hundreds of potential problems in your Registry or file permission settings, leaving the poor administrator to work his way through them and apply the suggested changes manually. Not only is this time consuming, but it is error-prone too.

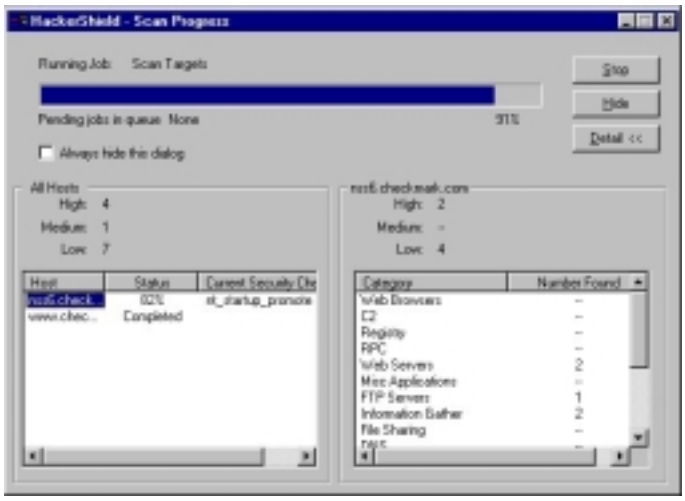

Figure 65 - Monitoring the progress of a scan job

HackerShield can be configured to auto-fix problems with Registry values, file permissions and Registry permissions whenever they are found. If the administrator decides that the fixes were inappropriate for any reason, however, there is also an “undo” feature that allows restoration to a previous configuration by undoing fixes that have been carried out from a past date up until the current date and time.

A RapidFire Update option provides regular updates to the vulnerability database, and these can be applied automatically via a scheduled process. BindView uses secure, PGP-signed email to deliver updates of the latest security threats directly to HackerShield. New security checks are automatically incorporated into HackerShield’s database and run during the next scan.

Reporting and Analysis

Once the scan has finished, the resulting report can be accessed from the Reports icon in the shortcut toolbar, which provides a number of very flexible viewing and configuration options. The reports are generally excellent, provided in HTML format and can be viewed directly from the console (albeit slowly in some cases, presumably due to the HTML output).

Selecting a job from the job list brings up the appropriate report in the main Report window, with a navigation frame to the left, that allows you to sort the report into different views (by host, by IP address, by vulnerability, and so on) as well as include or exclude individual sections at the click of a button.

All the detected vulnerabilities are displayed with full explanations accessible via hyperlinks, and if the security check produced any output (such as the list of open TCP ports from the port scan) then this too is available via a hyperlink. Finally, if an auto-fix is available, this can also be triggered from the report.

Reports are saved in the Reports windows once they have been completed, and remain there until they are no longer needed, whereupon they can be deleted or moved to the Archive window. HackerShield also provides the means to compare two reports in order to assess the progress of your security policy over time by monitoring changes in detected vulnerabilities between two scans.

Reports can be printed directly from the console (there is a print preview facility available too) and various options are available to allow you to include or exclude report sections such as summary information, the detailed security check descriptions, auto-fix information, and so on. A number of pre-defined report templates are included, or new ones can be created as required.

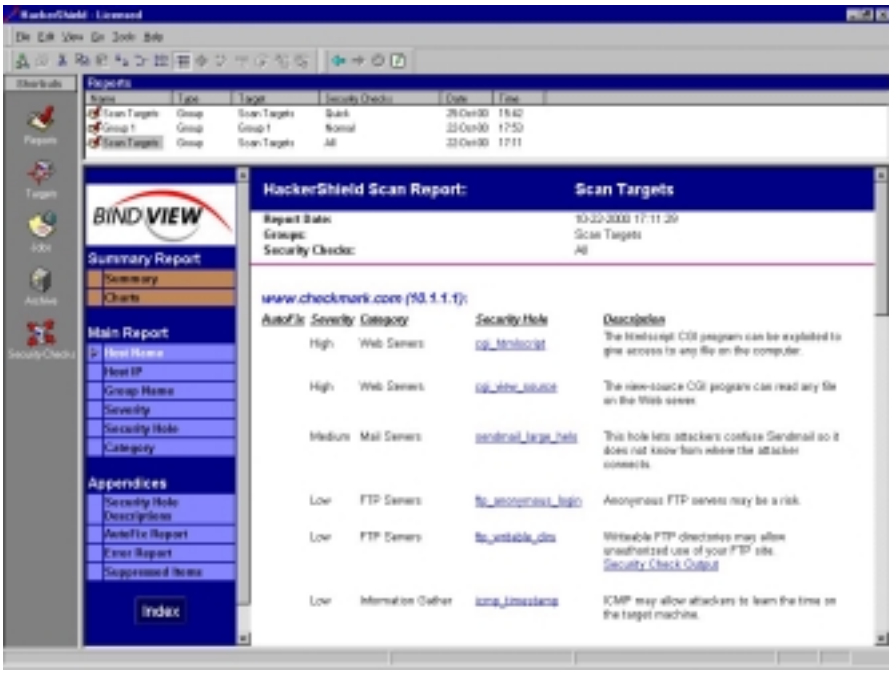

Figure 66 - Viewing HackerShield reports

Reports can also be exported in a variety of formats, including HTML, Crystal Reports, MDB (Microsoft Database files) or Word documents. We tried a straight export to HTML, but found that the resulting “report” was nothing more than a jumble of HTML files with no single index file to pull the whole thing together. Not particularly useful.

Verdict

All in all, HackerShield is extremely easy to use and provides an excellent tool for a continuous, automated security scan with the ability to fix some problems automatically and raise alerts on others (though it does not detect as many vulnerabilities as the other VA products we have tested).

In general, HackerShield is much more of a security – and particularly **NT** security – auditing tool than the "hacker in a box" that is provided by some of the competition.

The bias towards NT security checks (including the C2 tests) plus the auto-fix of Registry and file permission problems makes HackerShield a good choice for NT shops, and is the reason that some organisations may well want to purchase this product along with one of the more "traditional" VA scanners.

Contact Details

Company name: BindView

E-mail: info@bindview.co

Internet: http://www.bindview.com

Address:
5151 San Felipe
Suite 2100
Houston
Texas 77056
USA

Tel: +1 713-561-4000
Fax: +1 713-561-1000

UK Distribution:
Peapod UK
The Harlequin Centre
Southall Lane
Southall
Middlesex
UB2 5NH

Tel: +44 (0)208 606 9990

NAI CYBERCOP SCANNER 5.5

CyberCop Scanner is the Vulnerability Assessment offering from Network Associates, which offers a number of unique features such as a hostile DNS server, Custom Audit Scripting Language (CASL) and extensive IDS evasion testing capabilities.

Architecture

CyberCop Scanner can run on either a Windows (NT or 2000) or Unix (Red Hat Linux) platform, and can be used either as a stand alone scanner or as a component product within the Active Security suite.

The Active Security integrated product family is comprised of the following Network Associates products:

- **CyberCop Scanner** is the network security assessment component that can scan devices on the network for more than 700 vulnerabilities. CyberCop Scanner should be configured to search for the vulnerabilities that are of particular concern in accordance with the corporate security policy. CyberCop Scanner is known as a *sensor* component because it is essentially concerned with monitoring and collecting data.
- **Event Orchestrator** receives messages from sensors on the network and then, based on the security policy, processes them and decides whether to send action messages to the Active Security *actor* components in response to them. Event Orchestrator is configured to respond to particular vulnerabilities in a manner that best enforces the corporate security policy. Event Orchestrator is known as an *arbite*r. In addition to delegating actions to external actor components, Event Orchestrator is able to take certain kinds of action on its own. For example, it can send out an email message about a vulnerability it's been informed of, run a custom Visual Basic script, or raise a trouble ticket via the McAfee HelpDesk product (available separately).
- **Gauntlet Firewall** for Windows NT and Unix are known as *actor* components, because they are capable of acting on events supplied by arbiters. Gauntlet takes instructions from the arbiter and responds in a manner designed to enforce security policy – for example, by restricting access to certain servers or services.
- **Net Tools PKI Server** supports secure, strongly authenticated communication among the sensor, the arbiter, and the actors by furnishing each product with X.509 certificates.

Another component installed as part of the CyberCop Scanner package is the *Security Management Interface (SMI).* This provides a single console window, called the *SMI console window*, from which it is possible to manage all NAI security applications, whether they are installed on local or remote computers.

An NAI security application is inserted into the SMI console as a "snap-in" program. The SMI console can then be used to install, configure and run the snap-in program on network hosts.

From an SMI console, it is possible to:

- *Install and configure NAI security applications on the local computer*
- *Connect to computers on the network to install and configure NAI security applications remotely*
- *Monitor program activity and change program settings*
- *View security results collected in an event database on a remote computer*
- *Retrieve security results from a remote computer or from a central event server*
- *Generate reports using pre-defined report templates*
- *Configure the console window by setting one of four console modes*

Installation

On Windows platforms (as tested) installation is simply a matter of inserting the CD and following the installation Wizard, or activating the self-extracting EXE file if downloaded from the Internet.

During installation, both CyberCop Scanner and SMI components are installed. All packet driver components necessary for the correct operation of CyberCop Scanner are also installed automatically.

Oddly enough, if you wish to use the CASL interpreter, you must manually add an environment variable to point to it once everything else has been installed. It seems strange that this could not have been automated during the main installation routine.

There is an excellent *Getting Started Guide* which provides all the information you need to get you going with CyberCop Scanner. This is provided in electronic format as a PDF, and as a hard copy version in the box.

Configuration

The user interface has changed somewhat in the latest release of CyberCop Scanner, though it retains – and even improves upon - the ease of use factor that has characterised previous versions.

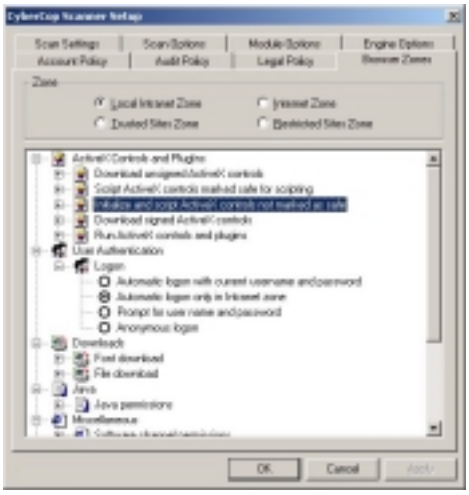

Figure 67 - Scan Settings

There are three sets of configuration options to be concerned with when starting a scan: scan settings, module settings and application settings. A Wizard steps you through most of the important stuff when defining a new scan job, or it is possible to configure everything manually.

Application settings cover basic operational parameters such as scanner working directories, main screen display attributes, and how to report results (always, never or vulnerable modules only).

Scan settings cover operational settings pertaining to the current job, such as host range to scan, whether to perform operating system identification and whether to disable or enable scan modules based on the OS found. Four of the available tabs are there to allow the administrator to define security policies relating to user accounts, system auditing, legal captions and browser zones. These will be compared against corresponding settings on every Windows platform in order to report on deviations from standard security policy.

The final tab provides the means to control a number of important settings relating to the security modules, such as the DNS domain name, TCP and UDP port scan ranges, which password files to use during password cracking operations, and so on. Scan settings can be saved in *Template* files for recall and reuse at a later date if required. This provides the means to have a specific group of policy settings for a specific range of hosts saved in a single template file.

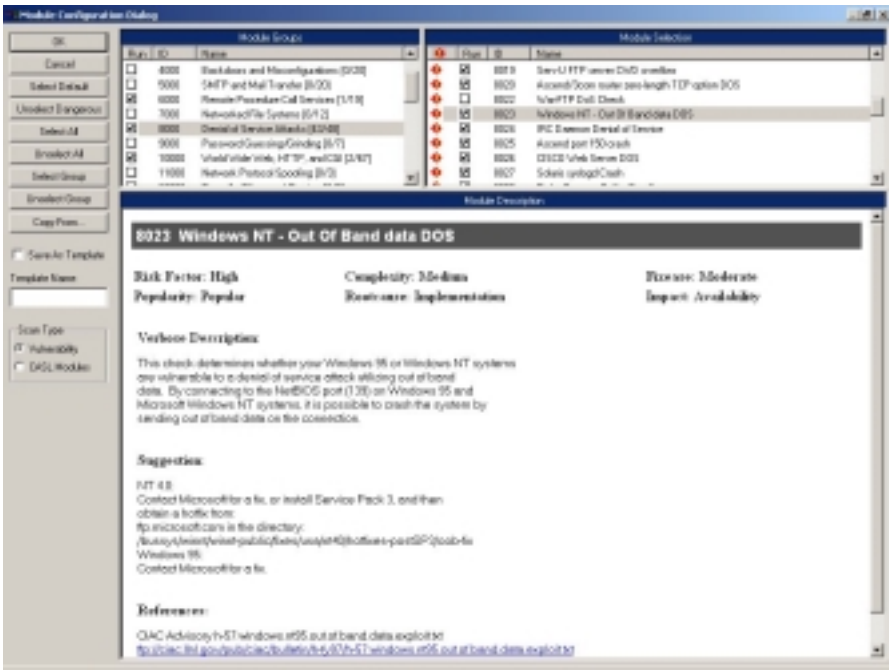

Figure 68 - Module settings

Module settings allow you to determine which attack signatures will be employed during the scan. CyberCop Scanner works by running security *modules* against a target system. Modules are pieces of code that either check for vulnerabilities on the target system or attempt to exploit the vulnerabilities of the target system. They are grouped into *module classes* according to their function – Denial of Service, information gathering, Web, FTP, and so on.

There are also a group of tests for checking the effectiveness of firewall filtering rules, which are used in conjunction with a special remote “listening” utility that is installed behind the firewall.

CyberCop Scanner includes operating system detection capabilities which can identify the operating system types of hosts on a network. Once operating system types are identified, CyberCop Scanner can optionally disable modules not pertaining to specified operating systems when scanning hosts.

Other modules initiate hostile Denial of Service attacks, which look for vulnerabilities that can only be detected properly if an attack is actually launched against a target host.

There are over 700 modules in the current vulnerability database, and additional checks can be added via the automated module update capability. This can be achieved via an FTP or LAN connection, and can be scheduled for automatic regular update. Network Associates is one of the few vendors which makes it simple for you to download an update file from the FTP site once, place it on an intranet server, and then update all copies of CyberCop Scanner from that one update file. This means it is not necessary for every CyberCop Scanner user to go to the NAI FTP site independently to perform updates, making the whole process much more efficient.

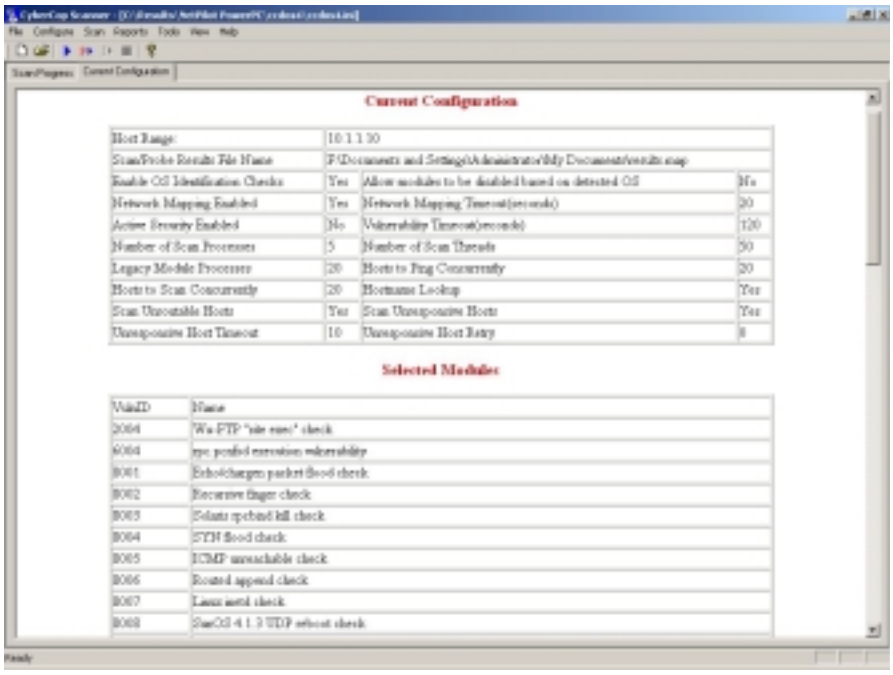

Figure 69 - Configuration settings can be saved as Templates

Modules are grouped together into their module classes, and individual attacks or entire groups can be selected via a single check box against an attack or group heading. Selecting an individual attack brings up an excellent detailed description of the vulnerability together with suggested fixes, and complex configurations can be saved as *Template* files to be used repeatedly. It is also possible to edit the entry in the vulnerability database by right-clicking on a vulnerability, though this is aimed more at altering the way the information is presented on screen and in reports than changing functionality in any way.

Having created template files for module and scan settings, the combination can be saved as a "*configuration file*". When starting a new scanning operation, opening a single configuration file will automatically apply all the appropriate settings in one go. Once configuration is complete, all module settings and variables can be confirmed in the *Current Configuration* tab, which can also be printed out for reference.

Once all the settings have been established, the tool bar provides buttons for "*begin scan*" and "*begin probe*". Probes detect responsive hosts on a network without scanning them for vulnerabilities. The probe will be performed on the hosts specified in the currently loaded configuration file, and this feature can be used to generate a network map and to troubleshoot hosts.

For each host, probing identifies if the host is responsive, determines the operating system type, and performs a trace route to generate a network map. Results during a probe can be viewed on the *Scan Progress* tab, which will list hosts that are found to be responsive (together with their operating system type, if OS identification is enabled), along with unresponsive hosts that have been skipped.

Clicking on "*begin scan*" performs a full-blown vulnerability scan of all hosts specified in the scan settings, using all modules specified in the module settings. It is possible to restrict CyberCop to performing only the scans that apply to the OS identified for a particular host, and modules for which a target is found vulnerable will return data specific to that test – an SMTP or FTP banner, for example, or a list of shares enumerated.

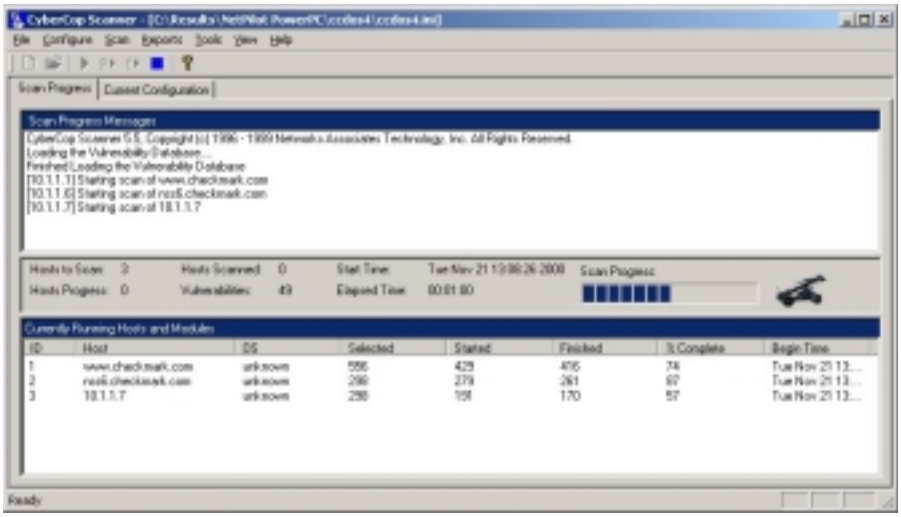

Figure 70 - Monitoring scan progress

During a scan, progress is monitored in the Scan Progress window, and a real-time indication of vulnerabilities found in the scanned hosts can be seen in the *Scan Results* tab if this has been activated. Once the scan is complete, results can be queried immediately on-screen via the Scan Results tab. Here, a tri-pane display shows a hierarchical tree display of all the hosts which have vulnerabilities, with all the vulnerabilities listed against each host. Selecting an individual vulnerability will bring up a display of the output produced from that module, and a full description of the vulnerability and suggested fixes.

Certain modules are designated as "*Fix It*" modules used in conjunction with Windows NT Registry checks. These modules can perform a fix to Registry values to correct potential vulnerabilities detected by CyberCop Scanner. After a scan is completed, Fix It modules are highlighted with a blue "wrench" icon, and individual modules (or all those found in a single scan) can be selected for automatic fixing. Unfortunately, there does not appear to be an "undo" function, so this feature should be employed with care.

CyberCop Scanner makes use of the SMI event database for storing security results during a scan. Once a scan is completed, SMI provides a report viewer which allows you to query the database, preview data, and generate reports. This can be accessed either from the SMI console or from the standard CyberCop Scanner console in the View Reports menu.

There are a few other features and tools which are available from the console menus. CyberCop Scanner includes two programs - *Crack* and *SMBGrind* - that use brute force password guessing functions to determine if user accounts on a network are vulnerable to intruders.

The *Crack* program attempts to break into a computer by guessing a user's encrypted password. It does this by comparing a list of possible passwords with an actual account file for a network, thereby potentially gaining access to a user account. The *SMBGrind* program actually attempts to log on to a computer remotely by grinding through a list of possible passwords. If a match is found it then logs on to the computer. Note that there is no password decryption utility providing Lophtcrack-type functionality – only brute force methods are available.

The remaining features are unique to CyberCop Scanner in the VA market place. The first is the hostile DNS server, which allows you to audit a DNS server for cache corruption attacks.

There is also a set of tests specifically designed to exercise Intrusion Detection software. The IDS testing tool provides a basic attack signature that can be represented in a number of ways on the wire that are designed specifically to evade detection by IDS programs. It does this by fragmenting packets, sending fragments out of order, introducing additional SYN packets, overlapping fragments, and so on. A "baseline" script provides the means to ensure that the basic attack can be seen by the IDS, following which you can run the remaining scripts to determine the effectiveness of your IDS system against such evasion techniques.

The final feature worthy of note is the Custom Audit Scripting Language (CASL) that allows you to construct your own TCP/IP packets and attacks. Individual TCP/IP packets can be constructed in the CASL GUI tool within CyberCop Scanner and broadcast across the network, or entire attacks can be scripted in a text editor using the high-level scripting language, details of which are provided in the documentation. In fact, some of the attacks within CyberCop Scanner itself – the IDS tests and firewall packet filtering tests - are CASL scripts.

Reporting and Analysis

Following a scan, the Network Map window provides a graphical view of the network as determined during the scan, which – apart from looking pretty - serves no useful purpose as far as we can see.

The real meat is in the various reports that can be generated which are extensive, clear and easy to read. The following reports are available:

- **Differential Report by Host -** Allows comparison of results for two hosts specified by IP address.
- **Differential Report by Scan Session -** Allows comparison of results for two scan sessions specified by date and time.
- **Graphical Summary -** Provides a graphical summary report with pie charts for different report categories (Complexity, Ease of Fix, Impact, Popularity, Risk Factor, Root Cause). For example, the Risk Factor pie chart shows the proportion of vulnerabilities found with Low, Medium, and High risk factors. Graphical Summary is a management report which contains only general network status information for a scan.

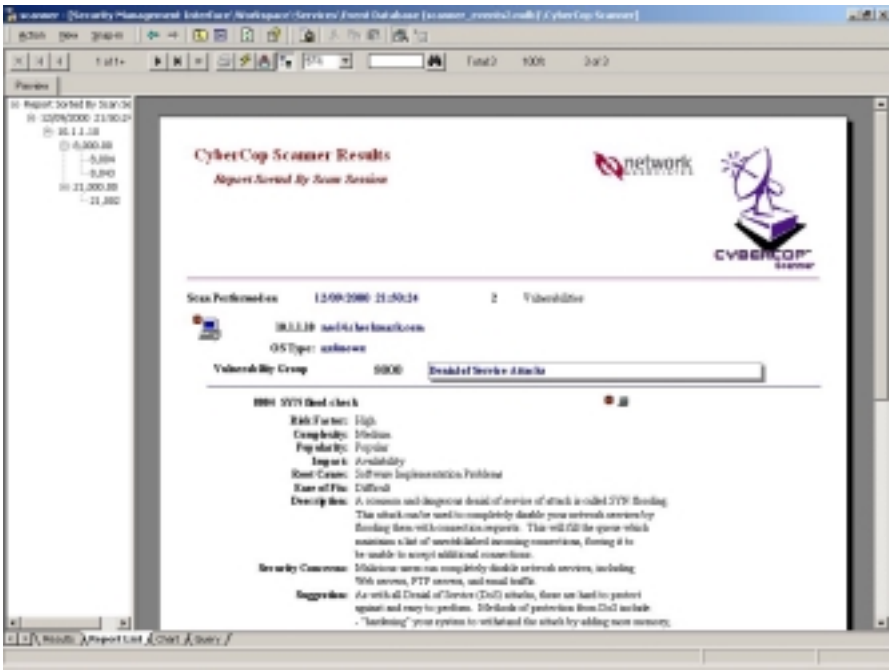

Figure 71 - Viewing reports by scan session

- **Report by Complexity -** Displays results by the difficulty involved in exploiting a vulnerability (Low, Medium, High).
- **Report by Ease of Fix -** Displays results by the ease of fixing a vulnerability (Trivial, Simple, Moderate, Difficult, Infeasible).
- **Report by Host -** Displays results by host IP address.
- **Report by Impact -** Displays results by the specific threat posed by a vulnerability (System Integrity, Confidentiality, Accountability, Data Integrity, Authorisation, Availability, Intelligence).
- **Report by OS Type -** Displays results by operating system type.
- **Report by Policy Violation -** Displays results by type of policy violation.
- **Report by Popularity -** Displays results by the likelihood that a vulnerability will be exploited (Obscure, Widespread, Popular).
- **Report by Risk Factor -** Displays results by the severity of the threat posed by a vulnerability (Low, Medium, High).
- **Report by Root Cause -** Displays results by the underlying cause of a vulnerability (Configuration, Implementation, Design).
- **Report by Scan Session -** Displays results by scan session date and time.
- **Report by Vulnerability ID -** Displays results by module number.

- **Vulnerability Guide -** Displays an indexed tree view of all modules in the Vulnerability Database. It is possible to click on a module number to view a detailed module description, or the entire Vulnerability Guide can be printed as a report.

Limited customisation options are available when generating reports. Customising a report allows the administrator to specify which database records will be included in the report, which database fields will be included for those records, and how the database fields will be sorted. It is also possible to remove repeated information from the body of a report and display it in an appendix at the end.

When a report is generated, it is first displayed in a preview window which includes an indexed tree view of sections in the report. The indexed tree can be used to navigate quickly to different sections in the report and the previewed report can be filtered to create sub-reports for easier viewing on-screen.

Reports can be printed direct from the viewer, or can be exported for use by other applications. Reports can be exported in a variety of formats, including **DOC** (Microsoft Word), **RTF** (Rich Text Format), and **HTML** (Web Browser).

Verdict

The latest release of CyberCop Scanner shows some minor, but nice, improvements over the previous one. The user interface is as clean and easy to use as ever, and the reporting is extensive and very readable.

CyberCop Scanner offers a policy definition interface that combines ease of use with flexibility, and the scans are fast and accurate. In addition, CyberCop offers a host of features over and above simply scanning for vulnerabilities.

The hostile DNS server provides the means to scan effectively for a host of DNS-related vulnerabilities, and it is possible to use the public version which NAI has made available in the Internet, or to install your own internally. The ability to test IDS products using various packet fragmentation techniques is a first for commercial VA scanners, as is the CASL scripting tool that allows you to create and run your own custom attacks.

The excellent user interface, detailed reports, open licensing model and additional features such as these still make CyberCop Scanner one of the best VA scanners on the market.

Contact Details

Company name: PGP Security, A Network Associates Business

E-mail: customer_service@nai.com

Internet: www.pgp.com

Address:
3965 Freedom Circle
Santa Clara, CA 95054, USA

Tel: 1.888.PGP.3011

NETWORKS VIGILANCE NV E-SECURE V2.1

Networks Vigilance NV e-secure is a vulnerability scanner with a difference. In addition to providing the usual host scanning capabilities, it also provides remote probes to test networks on both sides of a firewall, as well as testing the filtering rules of the firewall itself.

Architecture

NV e-secure is the only VA product we have come across that has anything different in the way of “architecture”. Whereas most VA products are single-point devices designed to scan individual or multiple remote IP hosts, NV e-secure provides a distributed console-agent architecture which allows not only scanning of subnets behind a firewall, but also a complete evaluation of the firewall filtering rules in place between scanning agent and console.

Console

The Console is the “command control centre” for all security testing, reporting and problem solving. From this point, the administrator can define a testing environment, configure a testing session, monitor a test, and generate reports.

There are various modules that plug-in to the NV e-secure Console:

- ***Network –*** provides the capability to scan for vulnerabilities on all hosts across the network, regardless of operating system. Vulnerabilities are reported in detail, with guidelines provided to fix the problems immediately. The network scanner consists of a number of modular “Test Cases” which probe all network hosts, just as a hostile attacker would, and quickly report on which hosts are vulnerable and why. Test cases act like any intruder - attempting to obtain information about the system, and then trying any open backdoor through an unsecured service or inherent weakness in a particular version.

- ***System -*** specifically targeted at OS performance. The System module tests the OS to make sure that it is free from security weaknesses, following which it will recommend the steps needed to remove the weakness. This may be anything from directing the administrator to the appropriate upgrade or OS patch resides on a vendor site, to a complete restructuring of the system itself.

- ***Firewall -*** Allows the administrator to create security policies for testing a remote network, separated from the Console host by one or more firewalls or routers. In order to do this, the Firewall module utilises an installed component on both Intranet and Internet sides of the network, giving the ability to automatically analyse the filtering rules currently defined in the Firewall or filtering equipment located between itself and its probe. The Firewall module does not simply scan the firewall’s IP address, therefore, but provides end-to-end testing of the Firewall's security readiness.

Firewall Probe

The NV e-secure Firewall Probe is installed on the Intranet side of the firewall or on the DMZ, and all communication between Console and Probe is conducted over TCP on a designated open port (9999). All such communication is encrypted using SSL3.

The Probe acts as a client to connect to the Console, and this prevents the creation of a potential security hole, since the connection is always made from *inside* the firewall – the Probe will not accept a connection at all, and will only participate in sessions which it initiates. The Probe must, of course, have the correct permissions to connect to the Console, and the Probe also handles masquerading of internal IP addresses.

When the Probe has connected to the Console, the Console can instruct it to scan the internal network and create an internal map of hosts and active services. The Console can then play the network test cases to check for operating system and server vulnerabilities.

The Probe also plays a part in the automatic detection of the firewall's filter rules. The purpose of this phase is to automatically detect which rules have been implemented in the firewall to block or reject packets. The Console and the Probe can both monitor their local network, so each of them can detect whether or not a packet sent by the other one passed through the firewall.

The packets that are sent by the Console or the Probe are either standard packets (which are used to determine a global rule such as “Deny all ICMP requests”) or calculated packets. Calculated packets are built from the Probe's internal scanning results, and are used to find logical rules such as “Allow incoming connection to port 80/tcp of server S only” (this is usually implemented as two physical rules).

The probe cannot find 100 per cent of the filtering rules - in particular, rules based on the source IP address are not detected. Thus if the firewall protects an Intranet without any server, the generated report could be very small.

Distributed Scanning Engine

As with the Firewall Probe, the Distributed Scanning Engine is installed on remote subnets (usually behind a firewall) and acts as a client to the Console. In order to facilitate communication through firewalls, all data transmitted between Engine and Console is passed over TCP on port 9999 (this port can be changed) and encrypted using SSL3.

Any number of Engines (depending on the license) can be controlled from a single Console, and once an Engine has connected to the Console, it can be instructed to scan the internal network and create an internal map of hosts and active services. Via the Console, the administrator will determine the scanning policy and the appropriate Test Cases are passed to the remote Engine. The Engine then runs the scans to check for operating system and server vulnerabilities, and passes the results back to the Console.

Networks Vigilance NV e-secure is the only commercial VA scanner we know of which provides this distributed client-server architecture in order to facilitate scanning through firewalls, as well as firewall rule verification.

The ability to divide scanning tasks between multiple machines across multiple subnets also allows NV e-secure to scale much better in large corporate environments.

Installation

Installation of NV e-secure is simple. It requires a Windows NT/2000 platform on which to run (though it can naturally scan any TCP/IP host, no matter what OS it runs), and uses the familiar InstallShield process.

During set-up, three installation options are provided: *Console*, *Firewall Probe*, and *Distributed Scanning Engine*. All necessary raw packet drivers are installed automatically if either of the latter two are selected.

Once the remote Probe/Engine has been installed, all that is required is to start it running, and enter the IP address of the Console and the port on which to communicate (defaults to 9999).

One problem we did note – which is a known problem – is that on a multi-homed host, both the Console and remote scanning Engines will bind to the first available network adapter. This can cause problems with the Probe and Engine since there is no way to specify to remote components which network addresses they should operate one. You may therefore find that when asking a Probe to perform a network scan for available hosts, it actually looks at the wrong subnet.

It can also cause problems with licensing, since the MAC address of the host is used to generate the license information. If you should remove an adapter from a multi-homed machine – or even change an adapter in a single NIC machine – NV e-secure will no longer run. This is a ridiculous restriction to put on licensing – a NIC could fail, or a complete host could fail, and it should not be necessary to obtain a new license key before the software can be installed on another machine.

In other respects, NV e-secure is licensed by IP address range per class C type subnet. For one license, you thus have the ability to scan all the available hosts on that subnet.

Configuration

All configuration and management is performed via the NV e-secure Console, which has an extremely useful and intuitive interface, if a little busy when all the windows are on view. Toolbar buttons for “instant toggle” of individual windows allow you to tidy things up when you need to focus on one particular area, and we really like the full-screen-view toggle button – every application should have one.

When first starting the Console, you are presented with the session dialogue box, allowing you to choose between the predefined or user-defined sessions. There are only three predefined sessions: two generic Safe Scans using either the Network or Firewall modules (see *Architecture*) or “*New Session*”, which allows you to define your own. The “*Existing Sessions*” tab enables you to load previous scan sessions – including individual job results – for further analysis.

When creating a new session, the administrator is guided through a Wizard. After naming the session, and selecting whether to use the Firewall Probe or perform a straight Network scan, you are given a choice between a LAN or WAN-based scan. At present, the only difference between the two is more lax timeouts on a WAN session to cope with potentially slower links, but in future releases, there will be different Test Cases introduced depending on this selection.

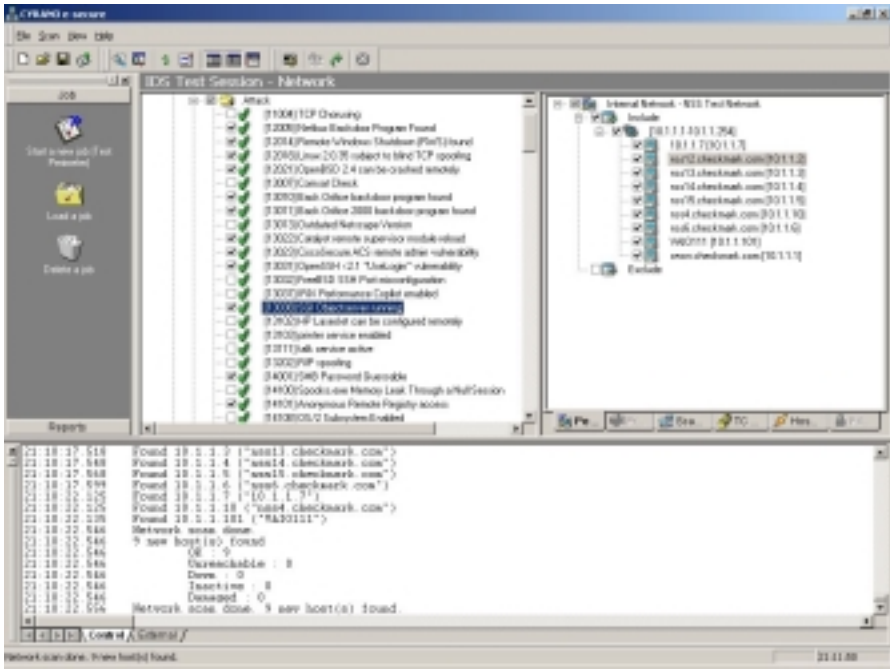

Figure 72 - Defining scan job parameters in the e-secure console

The next screen allows selection of the scan "perimeter", which is simply a range of network addresses. A new perimeter can be defined at this point if required, and any number can be defined within the license range, thus allowing logical groupings of machines for scanning purposes. Note that the perimeter only specifies the range of addresses which are *available* for scanning, the actual selection of machines to scan occurs later.

The Policies screen provides a small selection of pre-defined Policies from which to choose: ***Safe*** (all Test Cases except the Crash and DoS), ***Quick and Safe*** (all high vulnerability Test Cases excluding Crash and DoS), and ***Full*** (all Test Cases). Each Policy contains a set of Test Cases (vulnerabilities) sorted according to various categories, and it is possible to define your own custom Policies. NV e-secure allows you scan for vulnerabilities by:

- *Impact* – Attack, Crash, Denial of Service, Gather Info, Gain Root, Full Log
- *Risk* – High, Medium, Low
- *Platform* – Windows, Linux, various flavours of Unix, numerous hardware devices
- *Service* – All common services such as HTTP, FTP, SNMP, SMTP and so on
- *ID name*

Within each sub-category are a large number of Test Cases which represent the individual vulnerabilities to check for, but the Policy definition screen only allows Policy to be defined down to the sub-category level. For example, it is possible to create a Policy that just performs *Information Gathering* Test Cases, and nothing else, but you cannot specify that you only want to perform banner checks. A future release will allow Policy definition down to individual Test Case level, and this would be a very welcome addition. It would also be nice to be able to manage Policies from the main NV e-secure program – at present, they can only be created in the initial Session Wizard, and they cannot be subsequently edited or deleted, which is not particularly efficient.

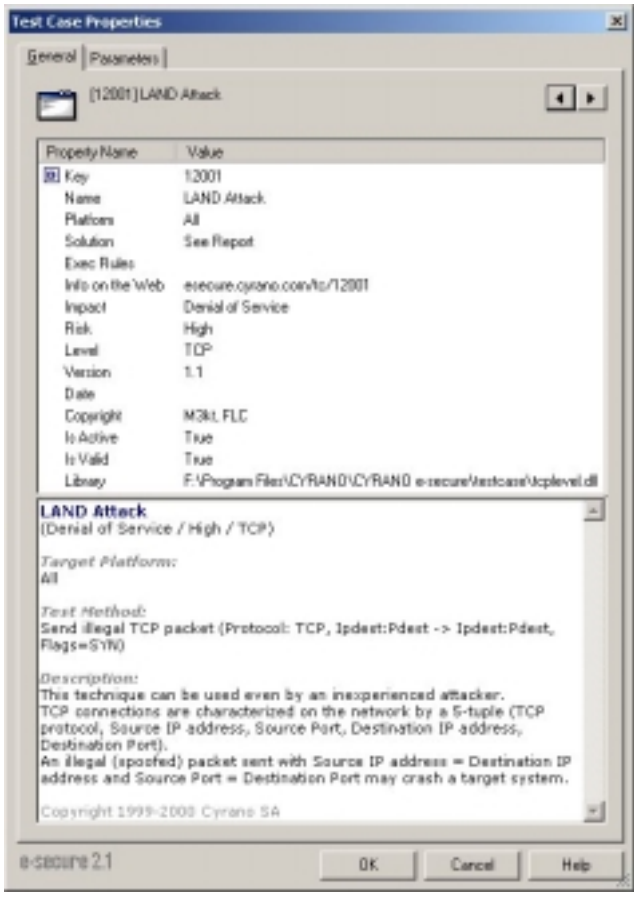

Figure 73 - Viewing Test Case properties

Once the wizard has finished, you are deposited in the main NV e-secure screen, which contains a number of panes:

- *Shortcuts bar -* displays icons that allow you to start a test run or generate reports of test results.
- *Policies pane -* shows the tests that you can run under the current security policy
- *Perimeters pane -* allows you to specify the host machines that you want to test.
- *Results pane -* displays the results of running the test cases you selected against the hosts you selected, in a variety of formats.
- *Output pane -* displays messages logging the progress of NV e-secure, and messages about its report generation.

As we have mentioned before, the screen can get rather cluttered making some of the windows difficult to read, but it is possible to toggle all of the windows on or off via toolbar buttons, as well as toggle a full-screen view.

The Policy pane lists all the test cases that are available, sorted into the sub-categories mentioned previously, and allows the administrator to select which ones are to be run by checking and un-checking boxes. New Test Cases can be downloaded from the Networks Vigilance *SecureServices* Web site and incorporated into NV e-secure automatically.

An entire category of Test Cases can be selected by checking the category box (such as Denial of Service, for example), or individual Test Cases can be selected as required. It is also possible to view the properties of the current Policy, where the administrator can set ping timeout values and high/low ports for port scans, amongst other things. Double-clicking on individual Test Cases brings up a very detailed description of the vulnerability plus, unusually, a description of the test method itself.

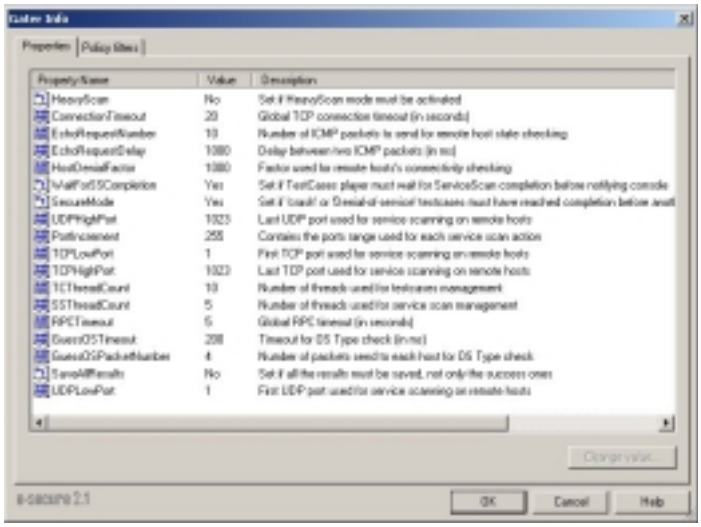

Figure 74 - Viewing Policy properties

Whenever applicable, a Parameters tab allows important settings to be modified for each Test Case (such as first port, last port, packet count and inter-packet delay for the Land attack). These parameters are set to sensible values and are fairly well hidden, thus keeping them out of the way of the less security-literate user who just wants to select the “Quick Scan” Policy and run off the resulting reports. For the real “hacker”, however, NV e-secure provides a simple way to explore the methodology behind the individual Test Cases, as well as a means to tweak the operational parameters.

Unfortunately, once you have finished modifying the currently selected Policy, it is not possible to save it – when you finish the scanning session and exit from NV e-secure, all the changes are lost (this “feature” will be rectified in release 2.2, which should be available by the time this report is published). The only place to make permanent Policy changes is thus when you first create them and, as we mentioned before, at that stage it is not currently possible to select individual Test Cases (or the parameters that apply to them). Policy definition is thus too inflexible at present, though this is the only area where we could find serious fault with NV e-secure.

The address range(s) available for scanning are listed in the Perimeter pane, and it is possible to add individual hosts or multiple hosts manually within the Perimeter, or NV e-secure can perform a network scan to determine which hosts are available. Once the Perimeter pane has been populated with the available hosts, one or more can be selected by using the check boxes alongside each one, following which the scan can be triggered.

When performing a Firewall probe (or when using the Distributed Scanning Engine), the Probe tab is used instead of the Perimeter tab, and it is necessary to select at least one host located on the opposite side of the firewall to the Console. This time it is the remote Probe that will be performing the scanning process (allowing hosts on the inside of the firewall to be scanned, as well as the inside of the firewall device itself), and in addition, it will also attempt to pass packets backwards and forwards between itself and the Console in order to determine which packets (if any) are allowed through the firewall.

The scan itself is split into two phases. The first phase involves ping sweeps and port scans to determine which hosts are alive and what services they are running. From this, NV e-secure determines the likely operating system and the potential vulnerabilities, and thus can decide which Test Cases are to be run against which hosts.

During the scanning process, NV e-secure keeps you well informed with an extremely useful real-time display consisting of several parts. The *Control* tab in the Output pane contains detailed text messages informing you of the port scan status, which ports were found, which test cases are being run against which hosts, and what results are returned. This can be saved as a plain text log to provide further analysis at a later date if required.

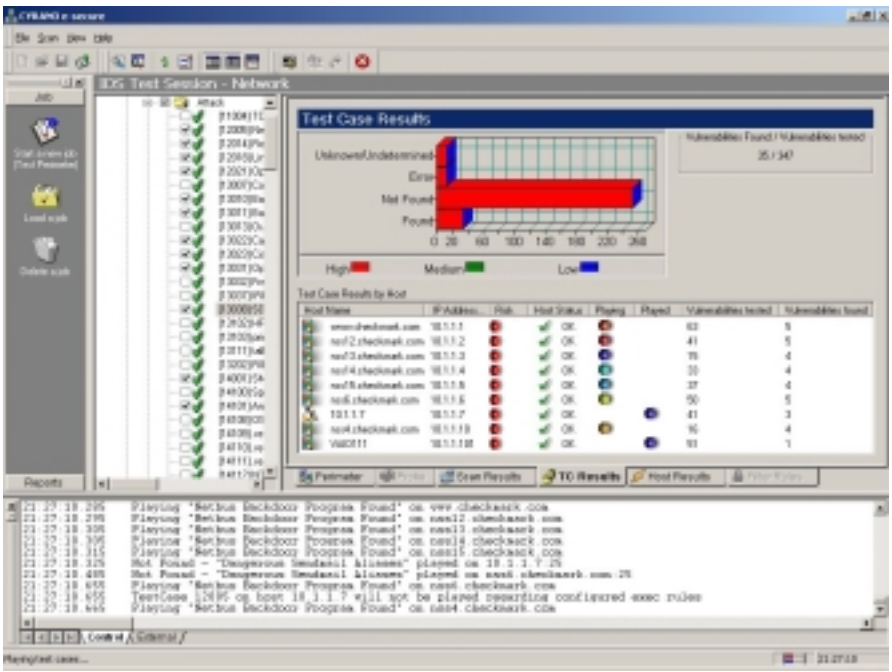

Figure 75 - Monitoring the progress of a scan job

The *Scan Results* tab shows a real-time graph of the port scanning status – number of TCP/UDP ports scanned and number of active services found – along with a list of the scan results broken down by host.

The *Test Case Results* tab shows another real-time graph of the number of Test Cases that have found vulnerabilities, along with a list of vulnerabilities found broken down by host. Right clicking on any host entry brings up detailed information about that particular host, including host name, IP address, operating system and full list of available services amongst other things.

The *Hosts Results* tab is probably the most important. This displays a list of hosts, along with their current status and details of how many vulnerabilities were found. Selecting any one of them will bring up a list of Test Cases that produced a vulnerability, encountered a system or network error or have an *undetermined* status. It reports the Test Case ID, the result of the test, the risk that the Test Case presents, the type of impact it has (attack, info gathering only, etc.), whether there is further information available (such as when banner text has been returned) and the port on which access was obtained.

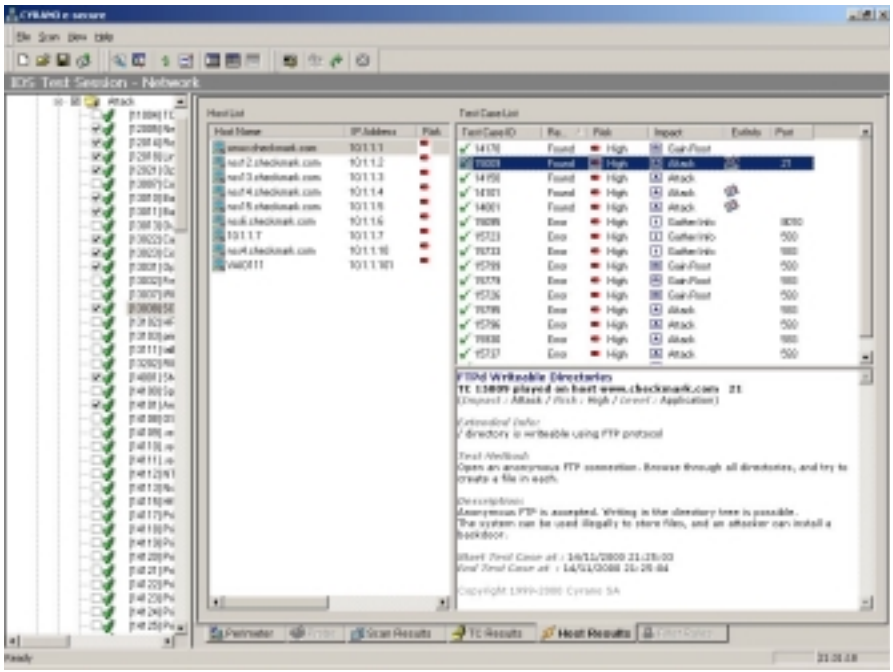

Figure 76 - Viewing Test Case results

Selecting any individual Test Case brings up the properties of that Case with full details of the vulnerability tested for, how it was tested, and what results were returned. Release 2.2 of NV e-secure will provide filtering on this window allowing only "*found*" vulnerabilities to be displayed, and eliminating the clutter of "*errors*" and "*undetermined*" when required.

The final tab only comes into play when a *Firewall Probe* has been run. The *Filters* tab is similar in look and operation to the *Host Results* tab, except this time we are looking at missing filter rules in the firewall configuration between the Probe and the Console. With a Firewall Probe, the Test Cases work by trying to send a packet through the firewall. If the *Result* column shows "*Found*", then the packet in question was able to get through, which may indicate a security failure. Not every successful Test Case indicates a security failure, of course, but the results presented by NV e-secure should be consistent with your own security policy.

By clicking on the *Generate Filer Rules* button once the test has completed, NV e-secure will display the filter rules it has been able to identify based on the test cases it has run. These rules can be saved in Linux/ipchains, Linux/ipfwadm or Cisco IOS 11 format. The firewall testing capability of NV e-secure is unique amongst VA scanners as far as we are aware, and is an incredibly useful feature.

Once a scan has been completed, the results are saved automatically in the underlying SQL database for reporting purposes. Each set of saved scan results is known as a *job*, and each time a previously-saved session is recalled and a scan run then a new job is created. Any job can be loaded into NV e-secure for historical reporting purposes, and NV e-secure will compare multiple jobs to provide trend and comparison reports.

The Manage Sessions option allows the administrator to delete previously-saved sessions once they are no longer required. From there, it is also possible to schedule sessions for regular unattended runs, and the reports can be e-mailed automatically to the administrator at the end of each run.

Reporting and Analysis

The reporting section of NV e-secure Console allows you to generate several types of reports from the latest job that has been run (or loaded into the Console from previous sessions).

The following reports are available:

- **General –** top level “index” that provides hyperlinked access to each of the other reports. There is also a link to the Vulnerabilities List, with a list of all vulnerability ID’s and descriptions in the NV e-secure database.
- **Administrator -** detailed information for each host, each vulnerability, and all the steps necessary to resolve problems discovered
- **Delta –** a report of new vulnerabilities that have been detected on the network since the last time the report was run
- **Host Report –** summary of each host tested, listing active services and all vulnerabilities found on that host
- **Manager –** high level (non-technical) summary of vulnerabilities that exist on the network, sorted in descending order of seriousness
- **Services Report –** lists vulnerabilities found in any services on the hosts that were tested
- **Historical –** shows the results of a number of runs of the same test, listing host status and the number of vulnerabilities detected of each type for each job selected.
- **Filter Rule –** summary of the filter rule Test Cases that succeeded in sending a packet across the firewall (only appears following a Firewall Probe scan)

All reports are generated in HTML format, and are displayed in the default Web browser, as well as being saved automatically to disk. The only way to print them out, however, is via the browser’s own print facility, which is not exactly the best way to do it.

Each vulnerability carries detailed information against it (the same information that is available when viewing from the console) and also provides hyperlinks back to the *SecureServices* Web site to provide more up-to-date information and detailed instructions on how to eliminate the vulnerability wherever possible.

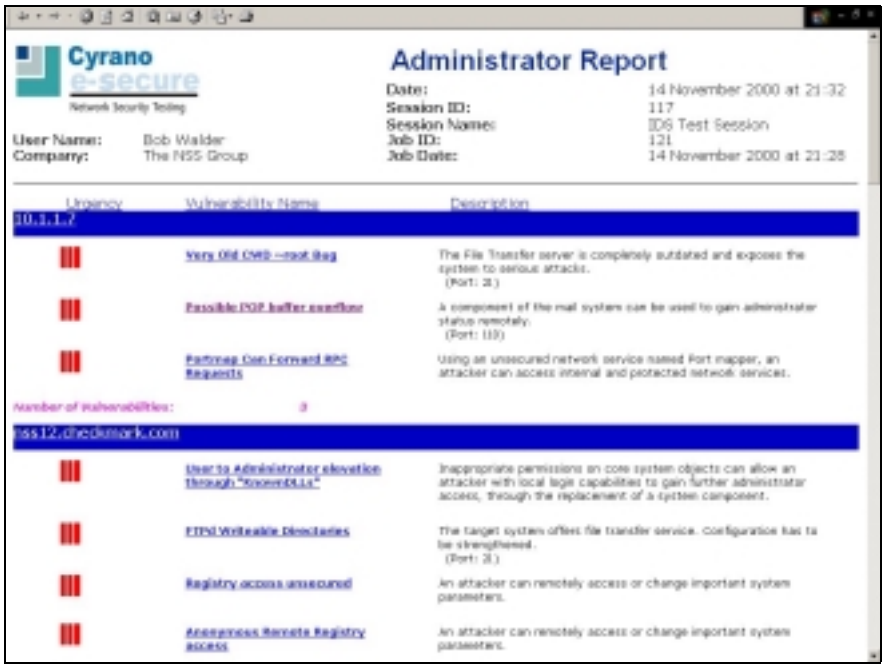

Figure 77 - Viewing the Administrator Report

The NV e-secure reporting is clear, comprehensive and easy to read. Some might object to the fact that it is not possible to create new reports or customise the existing ones, but there is enough information presented within the eight standard reports to suit most purposes.

Verdict

Networks Vigilance is not the best known name in the Vulnerability Assessment market place (the company is a spin-off from Cyrano – itself not particularly well known), and on this showing it is hard to see why that should be the case.

NV e-secure is a well-crafted piece of software with a simple-to-use, intuitive user interface, and a wide range of vulnerability signatures backed up by regular Web-based updates (probably the most frequent updates of all the products we have seen in the last year). These signatures do seem to focus on real “hacking attacks” as opposed to OS vulnerabilities (such as misconfigured guest accounts, inadequately secured administrator accounts, or poor password policy), so some sites might like to consider running NV e-secure alongside an OS auditing tool of some sort for complete coverage if this is an issue.

The only part of the product that is something of a let down in the current release is the Policy definition, which is neither completely intuitive, nor flexible enough for a product of this stature.

Reports too, whilst excellent, might benefit from being replaced by the ubiquitous Crystal Reports, to provide more flexibility and scope for expansion (especially since there is a full-blown SQL database underpinning the product). Finally, we would like to see the licensing process divorced from the host MAC address.

However, these minor niggles aside, NV e-secure offers the most comprehensive real-time analysis tools we have seen on any product of its kind, together with a perfectly adequate set of reports that are well presented and easy to read. It provides a basic set of default policies which can be run with little or no “hacking” knowledge, yet also makes available detailed descriptions of the vulnerability checks and the means to tweak the operational parameters for those who know what they are doing. NV e-secure seems to strike a rare balance between ease of use for the novice, and power and flexibility for the security expert.

Where NV e-secure really scores, however, is with its distributed architecture that allows remote scanning of large networks from a single, central console via multiple Scanning Engines. In addition, the Firewall Probe provides similar remote scanning capabilities which allows it to not only scan hosts on the inside of a firewall, but also use a number of special Test Cases to attempt to pass packets from Probe to Console – and vice versa - through the firewall, thus determining the effectiveness of the filter rules in place.

To our knowledge, the distributed scanning and firewall probing capabilities are unique amongst commercial firewall tools at the time of writing, and these make it an ideal tool for scanning large, distributed corporate networks from a single location, right down to scanning the local subnet for half a dozen hosts.

This should be considered an essential part of any security administrator’s tool kit - if you want to perform VA scans, you should be looking at NV e-secure.

Contact Details

Company name: Networks Vigilance S.A.

E-mail: sales@networksvigilance.com

Internet: http://www.networksvigilance.com

Product Web site: http://e-secure.networksvigilance.com

Address:
123 rue de Tocqueville
75017 PARIS
France

Tel: +33 (0) 1 56 33 40 00
Fax: +33 (0) 1 56 33 40 01

The US, UK, and French distributor for e-secure is Cyrano.

Addresses follow:

Cyrano Inc.
26 Parker Street
Newburyport, MA 01950-4010

Tel: + 1 (978) 462 0737
Fax: +1 (978) 462 4755

Cyrano UK
19 Thatcham Business Village
Colthrop Way
Thatcham
Berkshire RG19 4LW
UK

Tel: +44 (0)1635 876876
Fax: +44 (0)1635 873910

Cyrano France
123 rue de Tocqueville
75017 PARIS

Tel: +33 (0)1 56 33 40 00
Fax: +33 (0)1 56 33 40 01

PERFORMANCE TESTING

In addition to thoroughly evaluating each product in a controlled environment that was as close to a real-life network as we could make it, we also performed extensive tests against the Network IDS products, and more limited testing against the Host-based IDS and VA scanner products.

How We Tested – VA

We evaluated each VA product carefully paying particular attention to a range of key features. The feature set we evaluated against also represents the sort of questions you should be asking your VA vendor:

- *Ease of installation*
- *Ease of deployment over a large enterprise*
- *Architecture*
- *Authentication between console and scanning engines (if appropriate)*
- *Policy definition*
- *How policies are distributed to scanners*
- *How policy changes are handled (automatic deployment or manual)*
- *Number of attack signatures*
- *Whether custom attack signatures are allowed*
- *How new attack signatures are obtained and deployed, and frequency of updates*
- *Console interface – ease of use, real-time monitoring of scan progress*
- *Depth and accuracy of advice on preventative/corrective action when vulnerabilities are discovered*
- *Capability to auto-fix certain vulnerabilities*
- *Integration with other scanning/IDS/firewall products*
- *Log file/database maintenance*
- *Management reporting – range of reports/custom reports/the ease with which detail can be extracted and reported*
- *Limitations and restrictions on enterprise-wide alerting and reporting. Is it possible to combine reports from several scanners?*
- *Documentation – What documentation is included? On-line or hard copy? Supplemental information available on-line?*
- *Licensing and pricing model*
- *Maintenance*

We put these questions directly to each of the vendors, and the replies are reproduced unedited in Appendix A.

Performance Testing - VA

Our standard test bed for this project consisted of Pentium III 700MHz PCs each with 256MB RAM running Windows 2000 SP1, Windows NT Server 4.0 SP6a, or Red Hat Linux 6.2 (depending on the requirements of the product under test). All installations were on “clean” machines, restored between tests from a standard *Symantec Ghost* image.

The network was 100Mbit Ethernet with CAT 5 cabling, Nortel 10/100Mbit hubs, and 3Com 3C905 auto-sensing 10/100 network cards installed in each host. In all cases, the drivers that were auto-detected when the host operating system was installed were used during the test.

A range of scanning hosts were installed across multiple subnets behind a router and an open firewall in order to test deployment, management and scanning features.

Three test hosts were installed “out of the box” including as many of the “default” services bundled with the product as possible (Web server, mail server, FTP server, DNS server, etc.):

- *Windows 2000 Server*
- *Windows NT4 Server (with IIS, etc)*
- *Red Hat Linux 6.2 (with Apache, sendmail, FTP, etc)*

We then performed scans from the scanning hosts using the default settings and the “heaviest” scan mode available, recording the time taken to complete the scan and the number of vulnerabilities discovered.

Test Results – VA

This was an extremely difficult test to evaluate, since we found we were not really comparing “apples with apples” in most cases.

Some VA products are designed as “active” – or network-oriented - scanners, behaving like a “hacker in a box” in trying to discover and exploit as many vulnerabilities as possible. Others were more passive – or host-oriented - concerned mainly with highlighting incorrect or weak configurations in the host operating systems.

Axent Enterprise Security Manager

We did not include Axent ESM in the performance test runs, since it is purely a host-based scanner, more concerned with enterprise-wide policy auditing and enforcement.

It performed well in our overall evaluations, however, proving itself to be powerful, flexible and easy to use, with excellent reporting capabilities. It also supports a wide range of host platforms, and would make an ideal companion to any of the more “conventional” VA products tested here.

Axent NetRecon

NetRecon was the product that gave us most cause for concern. Concern, that is, in that it made our test systems appear almost trivial to break into, reporting, as it did, over 1700 vulnerabilities on the first run!

Operating System	Vulnerabilities Found
Windows 2000	1139
Windows NT4	497
Red Hat Linux 6.2	118
Total	1754

Time taken to scan 3 machines: 11 minutes 41 seconds

The problem with being so thorough, of course, is that the resulting report is simply too large to handle and so is almost as bad as having no report at all.

To be fair to Axent, it was our methodology that was largely at fault here, since we insisted on running the heaviest scan available on all products. Axent recommends you start with the *Light* scan, fixing the problems found there before moving on to the *Medium* scan. Having fixed the problems discovered there, only then should you attempt to run the *Heavy* scan, by which time the resulting report should be much smaller.

When we re-ran the tests using the *Medium* scan instead, we came up with the following results:

Operating System	Vulnerabilities Found
Windows 2000	98
Windows NT4	73
Red Hat Linux 6.2	18
Total	189

This proved to be a much more manageable report, and NetRecon found all the obvious security flaws we had left in place following our default installations.

The reports were clear and easy to read (if somewhat extensive on occasion) and the simple operation makes it straightforward to use by those administrators who are not security specialists.

BindView HackerShield

With HackerShield we created a new Security Check group that included every check in every category **except** for the unsafe Denial of Service checks.

On running this we were presented with a fairly short report, compared to the other products on test, with the following results:

Operating System	Vulnerabilities Found
Windows 2000	10
Windows NT4	13
Red Hat Linux 6.2	10
Total	33

Time taken to scan 3 machines: 12 minutes 14 seconds

These results are a little worrying, and indicate that BindView still has some way to go to increase the HackerShield vulnerability database to a similar standard to the competition.

The reports were accurate in the information they returned, however, and were very clear and easy to read. HackerShield also provides an auto-fix capability for some vulnerabilities, and that feature, combined with the simple reports and user interface, may appeal to the less security-literate administrator (although it would have to be compared carefully against NetRecon if such a consideration were paramount).

NAI CyberCop Scanner

With CyberCop Scanner we created a new Template containing all the "default" vulnerability checks – this is a "safe" setting within CyberCop that selects every check except those which are likely to crash the machine being scanned.

The following results were obtained:

Operating System	Vulnerabilities Found
Windows 2000	83
Windows NT4	19
Red Hat Linux 6.2	12
Total	114

Time taken to scan 3 machines: 2 minutes 55 seconds

This report was clear, easy to read, and contained all the vulnerabilities we expected to find. In addition, CyberCop Scanner allows a high degree of "tweaking" of the scan configuration as well as a scripting language that can be used to create custom attacks, thus making it much more attractive to the security professional (though it is no more difficult to use than any of the other products tested).

The most outstanding feature of this set of results is the time in which they were achieved – less than three minutes to scan all three machines.

Networks Vigilance NV e-secure

For the NV e-secure test we selected the default policy named "*Safe Scan*". This includes all Test Cases (vulnerability checks) except those that will cause Denial of Service on the machine being scanned.

The following results were obtained:

Operating System	Vulnerabilities Found
Windows 2000	29
Windows NT4	37
Red Hat Linux 6.2	14
Total	80

Time taken to scan 3 machines: 22 minutes 22 seconds

There is probably still some work to be done to increase the size of the e-secure vulnerability database (and to improve the performance), but it is hard to perform a direct comparison with other products because e-secure reported in some detail on a number of Test Cases that were run and returned an "undetermined" status rather than an absolute fail, and these were not included in the above figures. Some VA products might report these as vulnerabilities to err on the side of caution.

However, we determined that the number of vulnerabilities discovered was acceptable, and all those which we expected to be found were included in the e-secure reports. The reports are clear and easy to read, and e-secure also provides the most complete on-screen monitoring and analysis capability of the products tested here.

In addition, it is the only product we tested that is capable of using remote scanning engines to perform scans behind firewalls in a distributed environment, as well as determine the exact firewall filter rules in effect between the scanner console and remote firewall probe.

That, together with the high degree of flexibility in configuring test parameters, should make e-secure of great interest to most security professionals. The fact that the more esoteric scanning parameters are well hidden behind a Wizard-type interface, will also make e-secure attractive to the less security-literate administrator.

Summary – VA Performance Testing

The range of results returned in the various reports make it impossible for us to reproduce a straight comparison of the products tested in a document such as this.

We felt that of all the products tested, only *HackerShield* under performed, finding just 33 vulnerabilities across all three machines. It could be argued that Axent's *NetRecon* "over performed" on the "*Heavy*" scan setting, returning far too much information to be really useful. However, in selecting the "*Medium*" scan, we were presented with a far more usable report that more closely matched that of *CyberCop Scanner* and *NV e-secure*.

We also particularly liked the *Progressive Scan* feature that attempted to use information from one exploit to perpetrate another. In extreme cases, this could actually map out a potential route from low-level access on one machine to administrator access on another, and this could obviously prove very useful.

CyberCop Scanner and *NV e-secure* produced the most usable and accessible results, identifying all the most important vulnerabilities that would allow external hackers to gain access to your systems (writeable FTP root directories, vulnerable Web and mail servers, etc.). However, neither of these were as good at auditing NT Servers as *HackerShield* or *NetRecon*.

Where they had the edge was in their more advanced features that are simply not included in other VA products. *CyberCop Scanner*, for example, provides the built-in IDS testing capability and the CASL scripting language. The latter feature in particular would be of interest to many security professionals who would like to script their own attacks, and a number of CASL scripts aimed at exploiting firewall filtering rules are included, together with a remote "listening" component which can be installed inside a firewall.

NV e-secure takes this latter feature to its logical conclusion and provides a true multi-tiered architecture with remote scanning engines that can be deployed on multiple subnets, and behind firewalls, throughout a corporate network.

Not only can *NV e-secure* then run remote scans from any or all of those distributed engines, but the firewall probe component provides the ability to initiate a full analysis of the effectiveness (or otherwise) of the firewall rules in effect between the scanner and the probe. In our opinion, this makes *NV e-secure* a very desirable product indeed.

At the end of the day, there was a huge difference in the range, accuracy and content of the reports across all the products tested. Judgement of the effectiveness of these products is therefore largely subjective, and we would recommend that you evaluate carefully in your own environment to determine if the results that are being returned from scanning your own machines are useful.

As with anti-virus products, there is often considerable overlap between VA products, but each one has specific strengths and weaknesses. To provide maximum coverage, most organisations would be well advised to consider the purchase of more than one VA product, or to supplement a commercial offering with one of the various "underground" tools that are freely available on the Internet (not one of the tools on test, for example, possessed a port scanning capability that could in any way be considered a match for *nmap*).

One product tested as part of the VA evaluation which should be considered by every organisation with more than a handful of desktops to administer is Axent's *Enterprise Security Manager*. This is a fairly unique product amongst those tested in that it focuses more on cross-platform policy auditing and enforcement, and would thus make an ideal companion product to any of the VA scanners.

How We Tested - IDS

As with VA products, we evaluated each IDS product carefully paying particular attention to a range of key features. These are the sort of questions you should be asking your IDS vendor:

- *Architecture*
- *Ease of installation – host- and network-based engines*
- *Ease of deployment over a large enterprise – can IDS sensors be deployed and configured initially from a central console?*
- *Ease of management – once installed, remote sensors should be manageable from a central console*
- *Authentication and encryption between console and remote sensors for secure communication*
- *Policy definition*
- *How policies are distributed to engines*
- *How policy changes are handled (automatic deployment or manual)*
- *Number of attack signatures*
- *Whether custom attack signatures are allowed*
- *How new attack signatures are obtained and deployed, and frequency of updates*
- *Reporting from engine to console - range of action/alert options*
- *Console interface – attack notifications and alerts. How easy is it to filter and extract individual events?*
- *Whether the product allows capture and recording of suspect sessions*
- *Whether the product provides full protocol decodes of suspect sessions*
- *Whether the product includes an option to record everything for "forensic" investigation*
- *Corrective action during attack – connection reset, firewall configuration*
- *How are alerts reported? A single concise alert per attack in plain English is preferable. Some products display multiple "cryptic" or "generic" alerts per attack making them less useful to the administrator who is not security literate*
- *Accuracy and depth of advice on preventative action to ensure the attack does not happen again*

- *Integration with other scanning/IDS products*
- *Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.*
- *Management reporting – range of reports/custom reports/the ease with which detail can be extracted and reported*
- *Report management – can reports be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?*
- *What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector?*
- *Documentation – What documentation is included? On-line or hard copy? Supplemental information available on-line?*
- *Licensing and pricing model*
- *Maintenance*

We put these questions directly to each of the vendors, and the replies are reproduced unedited in Appendix A.

Performance Testing - IDS

Our standard test bed for this project consisted of Pentium III 700MHz PCs each with 256MB RAM running Windows 2000 SP1, Windows NT Server 4.0 SP6a, or Red Hat Linux 6.2 (depending on the requirements of the product under test). All installations were on "clean" machines, restored between tests from a standard *Symantec Ghost* image.

The network was 100Mbit Ethernet with CAT 5 cabling, Nortel 10/100Mbit hubs, and 3Com 3C905 auto-sensing 10/100 network cards installed in each host. In all cases, the drivers that were auto-detected when the host operating system was installed were used during the test.

We installed one network agent or one system agent on a dual-homed PC on the target subnet. There was no firewall protecting the target subnet.

The IDS agents were bound to one network interface in "stealth mode" wherever that was supported (i.e. no IP address) and the second interface was used to connect the IDS sensor to the management console on a private subnet. This ensured that the IDS sensor and console could communicate even when the target subnet was subjected to heavy loads, as well as preventing attacks on the console itself.

A range of remote IDS sensors were installed across multiple subnets behind a router and an open firewall in order to test deployment and management features.

IDS Test 1 – Basic Competency

The following range of tests were run using various commercial and "underground" scanning products (boping/bosting, targa, nmap, CyberCop Scanner, Aggressor, etc.):

- *IP port scan*
- *SYN stealth port scan*
- *FIN stealth port scan*
- *UDP port scan*

- *Nmap remote OS ID attempt*
- *CyberCop scan*
- *Chargen attack*
- *SYN Flood DOS*
- *WinNuke OOB attack*
- *BackOrifice probe*
- *FTP Bounce attack*
- *Web PHF attack*
- *Bonk attack*
- *Land attack*
- *Nestea*
- *NewTear*
- *SYNdrop*
- *Teardrop*
- *Jolt2*

All attacks were aimed at a single machine on the target subnet (not the IDS sensor) and the attacking machine was on the same subnet in order to provide maximum performance.

All attacks were run once with no load on the network and no IP fragmentation as a baseline to determine how effective the products were at detecting a basic level of attacks.

We would expect all the attacks to be reported in a similar manner to how they are listed above – it should not be necessary for the administrator to deduce that these attacks have taken place from examining obscure log entries.

IDS Test 2 – Performance Under Load

The IDS was expected to detect all alerts with 0 per cent network utilisation. The tests mentioned in section one above were then repeated with increasing levels of background network load at :

- *25 per cent network utilisation (37000pps)*
- *50 per cent network utilisation (74000pps)*
- *75 per cent network utilisation (111000pps)*
- *100 per cent network utilisation (148000pps)*

In addition, we utilised *boping* to produce a stream of 10,000 BackOrifice pings at half second intervals to the target server, which had *bosting* installed. *Bosting* counted all BackOrifice pings received, thus enabling us to provide accurate detection figures related to the number of alerts actually seen on the wire (bear in mind that at high network loads, even our attacking programs would have problems inserting packets on the wire).

The *boping/bosting* tests were also repeated with increasing levels of background network load as above, and the percentage of alerts discovered at each load level was recorded.

Packet generation was accomplished using an **Adtech AX/4000 Broadband Test System** with a 100Mbps module. We used the AX/4000 controller software to create a 64 byte packet with valid source and destination addresses on the target subnet (64 byte packets were needed to achieve rates of 148000 packets per second).

A constant stream of these packets was then injected onto the target segment during our tests, and the percentage load and pps figures were verified with two independent network monitoring tools before each test began.

For more information on the Adtech AX/4000, see Appendix B or visit the Spirent Web site at http://www.spirent-communications.com.

IDS Test 3 – IDS Evasion Techniques #1

We ran common attacks (WWW PHF/Back Orifice scan/etc.) across a router with normal IP forwarding in place to establish a baseline.

The test was then repeated seven times running the attacks through *fragrouter* and employing various IDS evasion techniques such as:

- ***frag-1 :*** *Send data in ordered 8-byte IP fragments.*
- ***frag-2 :*** *Send data in ordered 24-byte IP fragments.*
- ***frag-3 :*** *Send data in ordered 8-byte IP fragments, with one fragment sent out of order.*
- ***frag-4 :*** *Send data in ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet.*
- ***frag-5 :*** *Send data in out of order 8-byte IP fragments, duplicating the penultimate fragment in each packet.*
- ***frag-6 :*** *Send data in ordered 8-byte IP fragments, sending the marked last fragment first.*
- ***frag-7 :*** *Send data in ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it. This amounts to the forward-overlapping 16-byte fragment rewriting the null data back to the real attack.*

IDS Test 4 – IDS Evasion Techniques #2

We ran a basic WWW CGI scan of the target machine using *Whisker* to verify that the IDS could detect such an attack.

We then repeated the test six times using the following IDS evasion techniques:

- ***Mode 1:*** *URL encoding*
- ***Mode 2:*** */./ directory insertion*
- ***Mode 3:*** *Premature URL ending*
- ***Mode 5:*** *Fake parameter*
- ***Mode 7:*** *Case sensitivity*
- ***Mode 8:*** *Windows \ delimiter*

IDS Test 6 – Host Performance

We ran a series of attacks against a host-based system which were designed to generate a large number of alerts. CPU and memory usage were monitored during this phase in order to gauge the impact the host engine had on system performance.

Network load was also monitored when the host engine reported its findings to the central console in order to gauge the impact the host engine has on network performance.

Test Results – IDS

This section concentrates purely on the results of the Network IDS tests, since we found all the Host IDS products performed well, with an acceptable impact on the host on which they were installed, and generating acceptable amounts of traffic between agent and console.

Axent NetProwler

Network load	0%	25%	50%	75%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	74000	110000	148000
IP port scan	✓	✓	✓	✓	✓
SYN stealth port scan	✓	✓	✓	✓	✓
FIN stealth port scan [1]	✓	✓	✓	✓	✓
UDP port scan	✓	✓	✓	✓	✓
Nmap remote OS ID attempt [2]	✓	✓	✓	✓	✓
CyberCop scan	×	×	×	×	×
Chargen attack [3]	✓	✓	✓	✓	✓
SYN flood DoS [4]	✓	✓	✓	✓	✓
WinNuke OOB	✓	✓	✓	✓	✓
BackOrifice probe	✓	✓	✓	✓	✓
FTP Bounce attack [5]	✓	✓	✓	✓	✓
Web PHF attack	✓	✓	✓	✓	✓
Bonk [6]	✓	✓	✓	✓	✓
Land	✓	✓	✓	✓	✓
Nestea	×	×	×	×	×
NewTear	✓	✓	✓	✓	✓
SYNdrop [7]	✓	✓	✓	✓	✓
Teardrop	✓	✓	✓	✓	✓
Jolt2 [8]	✓	✓	✓	✓	✓
High volume boping (10,000 pings)	100%	100%	100%	100%	100%

Notes:
1. Reported as *SYN snipping*
2. Reported as *conflicting TCP flags*
3. Reported as *Stacheldraht*
4. Reported as *ICMP Redirect*
5. Reported as *man in the middle attack on the FTP port*
6. Reported as *DNS Zone Transfer*
7. Reported as *Tribal Flood Network 2K*
8. Reported as *ping reply flood*

IDS Evasion - fragrouter	Detected?
Ordered 8-byte IP fragments	×
Ordered 24-byte IP fragments	×
Ordered 8-byte IP fragments, one fragment sent out of order	×
Ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet	×
Out of order 8-byte IP fragments, duplicating the penultimate fragment in each packet	×
Ordered 8-byte IP fragments, sending the marked last fragment first	×
Ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it	×

IDS Evasion – Whisker	Detected?
Mode 1: URL encoding	×
Mode 2: /./ directory insertion	✓
Mode 3: Premature URL ending	✓
Mode 5: Fake parameter	✓
Mode 7: Case sensitivity	✓
Mode 8: Windows \ delimiter	✓

Axent NetProwler performed exceptionally well in the network load tests, detecting 100 per cent of all attacks at 100 per cent network load. However, although it did spot all of the attacks (except for Nestea and the CyberCop scan) it misrepresented far too many of them, and some of the descriptions were entirely inaccurate (though always consistent).

NetProwler does not provide packet reassembly and so failed to spot any fragmentation attacks launched through *fragrouter*. Performance against other IDS evasion techniques was mixed, handling most of the Whisker attacks quite well (though missing the *URL encoding* mode for some reason).

On the plus side, the monitoring screen on the Agent GUI shows packets processed and packets dropped, which is an extremely useful indication of when an Agent is being overloaded (though we did not see this happen in our tests).

The attack counts are also very accurate, making it very easy to determine exactly how many attacks have been detected.

CA eTrust Intrusion Detection

Network load	0%	25%	50%	75%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	74000	110000	148000
IP port scan	✓	✓	✓	✓	✓
SYN stealth port scan [2]	✓	✓	✓	✓	✓
FIN stealth port scan	×	×	×	×	×
UDP port scan	✓	✓	✓	✓	✓
Nmap remote OS ID attempt 3	✓	✓	✓	✓	✓
CyberCop scan	×	×	×	×	×
Chargen attack [4]	✓	✓	✓	✓	✓
SYN flood DoS	✓	✓	✓	✓	✓
WinNuke OOB	✓	✓	✓	✓	✓
BackOrifice probe [5]	✓	✓	✓	✓	✓
FTP Bounce attack	✓	✓	✓	✓	✓
Web PHF attack	✓	✓	✓	✓	✓
Bonk [6]	✓	✓	✓	✓	✓
Land	×	×	×	×	×
Nestea	✓	✓	✓	✓	✓
NewTear [7]	✓	✓	✓	✓	✓
SYNdrop [7]	✓	✓	✓	✓	✓
Teardrop	✓	✓	✓	✓	✓
Jolt2	✓	✓	✓	✓	✓
High volume boping (10,000 pings)	100%	100%	100%	N/A [1]	N/A [1]

Notes:
1. We were unable to obtain completely accurate alert counts at high network loads since eTrust suddenly began counting multiple alerts per attack. However, we did launch many of the individual attacks at both 75 and 100 per cent loads and eTrust detected all of them
2. Reported as *SYN attack*
3. Reported as *suspicious TCP flags*
4. Reported as *UDP flooding*
5. Required a custom signature
6. Reported as *Teardrop*
7. Reported as *Nestea/Jolt/Teardrop*

IDS Evasion – fragrouter	Detected?
Ordered 8-byte IP fragments	✓
Ordered 24-byte IP fragments	✓
Ordered 8-byte IP fragments, one fragment sent out of order	✓
Ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓

Out of order 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓
Ordered 8-byte IP fragments, sending the marked last fragment first	✓
Ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it	✓

IDS Evasion – Whisker	Detected?
Mode 1: URL encoding	✓
Mode 2: /./ directory insertion	✓
Mode 3: Premature URL ending	✓
Mode 5: Fake parameter	✓
Mode 7: Case sensitivity	✓
Mode 8: Windows \ delimiter	✓

There was a certain amount of misrepresentation of attacks in the eTrust alerts, but nothing too serious or inaccurate. We were disappointed to see it miss the FIN stealth port scan and the Land attack, but hopefully this will be remedied in a future signature update.

CA eTrust has excellent real-time alerting, so it is simple enough to see the attacks as they arrive in the alerting window, but there is no accurate count either in the real-time monitoring screens or via the reports.

We attempted to count manually a reduced number of alerts, but it is still not possible to count manually at higher network loads since there seems to be extensive event aggregation occurring, with no way to disable it. This meant we were unable to obtain completely accurate performance statistics for the high-volume attack tests.

However, given the fact that eTrust had no problem detecting the numerous individual attacks we launched at high network loads (we had to launch far more individual attacks manually in order to prove this) we decided to give it the benefit of the doubt and assert that eTrust detected 100 per cent of all attacks at all network loads, as well as handling all IDS evasion techniques and packet reassembly with ease.

Cisco Secure IDS

Model 4210 (rated at 45Mbps)

Network load	0%	56%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	66000
IP port scan	✓	✓	×
SYN stealth port scan	✓	✓	×
FIN stealth port scan	✓	✓	×
UDP port scan	✓	✓	×
Nmap remote OS ID attempt [1]	✓	✓	×
CyberCop scan	×	×	×
Chargen attack	✓	✓	×
SYN flood DoS [2]	✓	✓	×
WinNuke OOB [3]	✓	✓	×
BackOrifice probe [4]	✓	✓	×
FTP Bounce attack	✓	✓	×
Web PHF attack [5]	✓	✓	×
Bonk [6]	✓	✓	×
Land [7]	✓	✓	×
Nestea [8]	✓	✓	×
NewTear [6]	✓	✓	×
SYNdrop [6]	✓	✓	×
Teardrop [6]	✓	✓	×
Jolt2 [9]	✓	✓	×
High volume boping (10,000 pings)	100%	31%	1%

Model 4230 (rated at 100Mbps)

Network load	0%	25%	50%	75%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	74000	110000	148000
IP port scan	✓	✓	✓	✓	✓
SYN stealth port scan	✓	✓	✓	✓	✓
FIN stealth port scan	✓	✓	✓	✓	✓
UDP port scan	✓	✓	✓	✓	✓
Nmap remote OS ID attempt [1]	✓	✓	✓	✓	✓
CyberCop scan	x	x	x	x	x
Chargen attack	✓	✓	✓	✓	✓
SYN flood DoS [2]	✓	✓	✓	✓	✓
WinNuke OOB [3]	✓	✓	✓	✓	✓
BackOrifice probe [4]	✓	✓	✓	✓	✓
FTP Bounce attack	✓	✓	✓	✓	✓
Web PHF attack [5]	✓	✓	✓	✓	✓
Bonk [6]	✓	✓	✓	✓	✓
Land [7]	✓	✓	✓	✓	✓
Nestea [8]	✓	✓	✓	✓	✓
NewTear [6]	✓	✓	✓	✓	✓
SYNdrop [6]	✓	✓	✓	✓	✓
Teardrop [6]	✓	✓	✓	✓	✓
Jolt2 [9]	✓	✓	✓	✓	✓
High volume boping (10,000 pings)	100%	100%	100%	100%	100%

Notes:
1. Reported as *SYN/FIN/NULL packets*
2. Reported as *ICMP flood*
3. Reported as *impossible IP packet*
4. BackOrifice probe does not trigger an alert. BackOrifice alert is only triggered by a response from a BackOrifice server. A custom signature was required to allow us to run our high volume boping/bosting tests.
5. **Also** reported as a *general CGI-BIN attack*
6. Reported as *IP fragment attack + fragment overlap*
7. Reported as *NetBIOS OOB data*
8. Reported as *UDP bomb/flood + fragment attack*
9. Reported as *fragmented traffic/fragment overlap/large ICMP traffic*

IDS Evasion - fragrouter	Detected?
Ordered 8-byte IP fragments	✓
Ordered 24-byte IP fragments	✓
Ordered 8-byte IP fragments, one fragment sent out of order	✓
Ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓
Out of order 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓
Ordered 8-byte IP fragments, sending the marked last fragment first	✓
Ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it	✓

IDS Evasion – Whisker	Detected?
Mode 1: URL encoding	✓
Mode 2: /./ directory insertion	✓
Mode 3: Premature URL ending	✓
Mode 5: Fake parameter	✓
Mode 7: Case sensitivity	✓
Mode 8: Windows \ delimiter	✓

The Cisco Secure Policy Manager Console made it very easy to follow the attacks in real-time and to determine exactly how many attacks had been detected.

The **Model 4210** is limited to 45Mbps so we could not perform the full range of tests using this model. We created a new network load test of 66000pps which corresponds to just under 100 per cent load for the 4210, but it could not detect any attacks at that load.

In fact, the 4210 could only detect around 30 per cent of attacks at 37000 pps which means we could only recommended it for use on very lightly loaded networks or for protecting restricted bandwidth Internet connections. Cisco believe that we could have been experiencing problems with a pre-production unit of a brand new product, and are working on the problem at the time of writing.

On the other hand, the 100Mbps-rated **Model 4230** performed flawlessly right up to 100Mbps loads, detecting 100 per cent of all attacks even at 100 per cent load.

Both products displayed excellent attack recognition capabilities, handling all the IDS evasion techniques extremely well – in fact the Cisco Secure IDS product produced the most comprehensive list of individual Web attacks that go to make up each combined Whisker attack.

The reporting of alerts was fairly generic in some circumstances (all the Teardrop-style attacks were reported as “fragment overlap” attacks, for example) but accurate nonetheless.

CyberSafe Centrax

Network load	0%	25%	50%	75%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	74000	110000	148000
IP port scan	✓	✓	✓	✓	×
SYN stealth port scan	✓	✓	✓	✓	×
FIN stealth port scan [1]	✓	✓	✓	✓	×
UDP port scan	✓	✓	✓	✓	×
Nmap remote OS ID attempt [2]	✓	✓	✓	✓	×
CyberCop scan	×	×	×	×	×
Chargen attack	✓	✓	✓	✓	×
SYN flood DoS	✓	✓	✓	✓	×
WinNuke OOB	✓	✓	✓	✓	×
BackOrifice probe	✓	✓	✓	✓	×
FTP Bounce attack	✓	✓	✓	✓	×
Web PHF attack	✓	✓	✓	✓	×
Bonk	×	×	×	×	×
Land	✓	✓	✓	✓	×
Nestea	×	×	×	×	×
NewTear	✓	✓	✓	✓	×
SYNdrop	×	×	×	×	×
Teardrop	✓	✓	✓	✓	×
Jolt2	✓	✓	✓	✓	×
High volume boping (10,000 pings)	N/A[3]	N/A[3]	N/A[3]	N/A[3]	N/A[3]

Notes:
1. Reported as *IP half scan*
2. Reported as *TCP fingerprinting*
3. Accurate attack detection counts were not possible

IDS Evasion - fragrouter	Detected?
Ordered 8-byte IP fragments	×
Ordered 24-byte IP fragments	×
Ordered 8-byte IP fragments, one fragment sent out of order	×
Ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet	×
Out of order 8-byte IP fragments, duplicating the penultimate fragment in	×

each packet	
Ordered 8-byte IP fragments, sending the marked last fragment first	×
Ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it	×

IDS Evasion – Whisker	Detected?
Mode 1: URL encoding	×
Mode 2: /./ directory insertion	×
Mode 3: Premature URL ending	×
Mode 5: Fake parameter	×
Mode 7: Case sensitivity	×
Mode 8: Windows \ delimiter	×

With no individual attack count capability we found it impossible to provide accurate detection counts for our high-volume *boping* attacks. However, we did note that all recognisable attacks appeared to be detected up to the 75 per cent network load point. Detection was erratic at 100 per cent load.

The Centrax Network Agent did not provide any packet reassembly capabilities or defence against the *Whisker* IDS evasion techniques, and it missed a few common attacks – Bonk, Nestea and SYNdrop – since at the moment it could not be considered to have a "full" signature library.

This is not really to the product's detriment given that its main focus at present is on host-based intrusion detection, and that the network Agent is a relatively new development and could be considered more as a "bonus" inclusion in an excellent Host IDS system. We certainly would not recommend purchase of Centrex for the Host IDS component alone.

Nevertheless, we are promised a rapid signature update for those attacks we noted were missing, and CyberSafe will continue to develop the network agent to bring it into line with the NIDS competition.

ISS RealSecure

Network load	0%	25%	50%	75%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	74000	110000	148000
IP port scan	✓	✓	✓	✓	✓
SYN stealth port scan	✓	✓	✓	✓	✓
FIN stealth port scan	✓	✓	✓	✓	✓
UDP port scan	✓	✓	✓	✓	✓
Nmap remote OS ID attempt	✓	✓	✓	✓	✓
CyberCop scan	×	×	×	×	×
Chargen attack	✓	✓	✓	✓	✓
SYN flood DoS	✓	✓	✓	✓	✓
WinNuke OOB	✓	✓	✓	✓	✓
BackOrifice probe	✓	✓	✓	✓	✓
FTP Bounce attack	✓	✓	✓	✓	✓
Web PHF attack	✓	✓	✓	✓	✓
Bonk [1]	✓	✓	✓	✓	✓
Land	✓	✓	✓	✓	✓
Nestea [1]	✓	✓	✓	✓	✓
NewTear [1]	✓	✓	✓	✓	✓
SYNdrop [1]	✓	✓	✓	✓	✓
Teardrop	✓	✓	✓	✓	✓
Jolt2	×	×	×	×	×
High volume boping (10,000 pings)	100%	100%	91%	48%	33%

Notes:
1. Reported as *Teardrop*

IDS Evasion - fragrouter	Detected?
Ordered 8-byte IP fragments	✓
Ordered 24-byte IP fragments	✓
Ordered 8-byte IP fragments, one fragment sent out of order	✓
Ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓
Out of order 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓
Ordered 8-byte IP fragments, sending the marked last fragment first	✓
Ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it	✓

IDS Evasion – Whisker	Detected?
Mode 1: URL encoding	✓
Mode 2: /./ directory insertion	✓
Mode 3: Premature URL ending	✓
Mode 5: Fake parameter	✓
Mode 7: Case sensitivity	✓
Mode 8: Windows \ delimiter	✓

Attack recognition was generally very good with RealSecure (though it missed the Jolt2 attack) and the descriptions were clear and accurate. Real-time monitoring was excellent, with very exact detection counts. RealSecure also includes full packet reassembly capabilities and resistance to common IDS evasion techniques, and thus handled both the *fragrouter* and *Whisker* attacks flawlessly.

However, detection capabilities fell off steadily at high loads. It did continue to detect some signatures, so at least it did not fail completely under pressure. However, its rate of detection fell off quite rapidly above 50 per cent network load.

We could only recommend RealSecure for installation in lightly loaded networks unless multiple engines are installed on a single subnet, each monitoring a subset of the attack signature database.

Network ICE BlackICE Sentry

Network load	0%	25%	50%	75%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	74000	110000	148000
IP port scan	✓	✓	✓	✓	✓
SYN stealth port scan	✓	✓	✓	✓	✓
FIN stealth port scan	✓	✓	✓	✓	✓
UDP port scan	✓	✓	✓	✓	✓
Nmap remote OS ID attempt	✓	✓	✓	✓	✓
CyberCop scan	✓	✓	✓	✓	✓
Chargen attack	✓	✓	✓	✓	✓
SYN flood DoS	✓	✓	✓	✓	✓
WinNuke OOB	✓	✓	✓	✓	✓
BackOrifice probe	✓	✓	✓	✓	✓
FTP Bounce attack	✓	✓	✓	✓	✓
Web PHF attack	✓	✓	✓	✓	✓
Bonk	✓	✓	✓	✓	✓
Land	✓	✓	✓	✓	✓
Nestea	✓	✓	✓	✓	✓
NewTear	✓	✓	✓	✓	✓
SYNdrop	✓	✓	✓	✓	✓
Teardrop	✓	✓	✓	✓	✓
Jolt2	✓	✓	✓	✓	✓
High volume boping (10,000 pings)	100%	100%	100%	100%	100%

IDS Evasion - fragrouter	Detected?
Ordered 8-byte IP fragments	✓
Ordered 24-byte IP fragments	✓
Ordered 8-byte IP fragments, one fragment sent out of order	✓
Ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓
Out of order 8-byte IP fragments, duplicating the penultimate fragment in each packet	✓
Ordered 8-byte IP fragments, sending the marked last fragment first	✓
Ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it	✓

IDS Evasion – Whisker	Detected?
Mode 1: URL encoding	✓
Mode 2: /./ directory insertion	✓
Mode 3: Premature URL ending	✓
Mode 5: Fake parameter	✓
Mode 7: Case sensitivity	✓
Mode 8: Windows \ delimiter	✓

BlackICE Sentry had an excellent GUI console that made it very easy to see which attacks (and how many) had occurred, and the attack descriptions were correct in every case. It also offered very complete and easy to read reporting and high levels of performance.

The only product in our tests to detect every single one of our attacks accurately, it also managed 100 per cent detection rates at 100 per cent network loads with ease. Couple this with an extremely low CPU utilisation on the host, perfect fragmentation reassembly and resistance to IDS evasion techniques, and you have an outstanding product.

Dragon Sensor

Network load	0%	25%	50%	75%	100%
Background traffic load – 64 byte packets (packets per second)	0	37000	74000	110000	148000
IP port scan	✓	✓	✓	✓	N/A[1]
SYN stealth port scan	✓	✓	✓	✓	N/A[1]
FIN stealth port scan	✓	✓	✓	✓	N/A[1]
UDP port scan	✓	✓	✓	✓	N/A[1]
Nmap remote OS ID attempt [2]	✓	✓	✓	✓	N/A[1]
CyberCop scan	×	×	×	×	N/A[1]
Chargen attack	×	×	×	×	N/A[1]
SYN flood DoS	×	×	×	×	N/A[1]
WinNuke OOB	×	×	×	×	N/A[1]
BackOrifice probe	✓	✓	✓	✓	N/A[1]
FTP Bounce attack	✓	✓	✓	✓	N/A[1]
Web PHF attack	✓	✓	✓	✓	N/A[1]
Bonk [3]	✓	✓	✓	✓	N/A[1]
Land [4]	✓	✓	✓	✓	N/A[1]
Nestea [3]	✓	✓	✓	✓	N/A[1]
NewTear [3]	✓	✓	✓	✓	N/A[1]
SYNdrop [3]	✓	✓	✓	✓	N/A[1]
Teardrop	✓	✓	✓	✓	N/A[1]
Jolt2	×	×	×	×	N/A[1]
High volume boping/bosting (10,000 pings)	100%	100%	32%	N/A[1]	N/A[1]

Notes:
1. The sensor became unreliable at 75 per cent load and crashed at 100 per cent. The vendor believes it to be a problem with the 3Com card or driver under Red Hat Linux 6.2 and is working on a solution at the time of writing.
2. Reported as *TCP flags*
3. Reported as *fragment overlap*
4. Reported as *same IP address*

IDS Evasion - fragrouter	Detected?
Ordered 8-byte IP fragments	✓
Ordered 24-byte IP fragments	✓
Ordered 8-byte IP fragments, one fragment sent out of order	✓
Ordered 8-byte IP fragments, duplicating the penultimate fragment in each packet	×
Out of order 8-byte IP fragments, duplicating the penultimate fragment in each packet	×
Ordered 8-byte IP fragments, sending the marked last fragment first	✓
Ordered 16-byte IP fragments, preceding each fragment with an 8-byte null data fragment that overlaps the latter half of it	×

IDS Evasion – Whisker	Detected?
Mode 1: URL encoding	✓
Mode 2: /./ directory insertion	✓
Mode 3: Premature URL ending	✓
Mode 5: Fake parameter	✓
Mode 7: Case sensitivity	✓
Mode 8: Windows \ delimiter	✓

Dragon Sensor provides no real-time monitoring of attacks – it all has to be done via reporting. Nor it is easy to clear down or filter out old attacks, making it very cumbersome to try and determine the exact number of attacks detected.

Despite having the biggest library of signatures (over 1000) of the products tested, Dragon surprised us by missing Chargen, SYN Flood, WinNuke and Jolt2 attacks, and also offered incomplete fragmentation reassembly (missing some of the *fragrouter* attacks), though all the *Whisker* IDS evasion attacks were detected effectively.

Unfortunately we noticed erratic behaviour of the Sensor at network loads in excess of 50 per cent, and a complete failure of the Sensor (causing a total machine crash) at 100 per cent loads. This is a bizarre fault to have in a shipping product, and we believe that we experienced a rare configuration problem that may be related to the combination of 3Com 3C905 cards under Red Hat Linux 6.2. The vendor is working on a solution at the time of writing.

We would not dismiss Dragon Sensor completely because of this apparently isolated problem, but would certainly advocate careful evaluation in your own environment prior to purchase.

Summary – IDS Performance Testing

Note that for this test we are not counting failure to perform fragmentation reassembly (to handle *fragrouter* attacks) or to handle IDS evasion techniques as a serious problem, since most vendors are still in the process of implementing these capabilities. Next year, we will take an entirely different view, of course, and for now, it would always be wise to select a product that can perform full fragmentation reassembly and handle all common evasion techniques, all other things being equal.

In the performance tests we noticed a range of results from the excellent to the really rather poor. The problems with Dragon Sensor were hopefully isolated configuration or driver issues, since in every other respect the product was excellent. Likewise, the Cisco Secure IDS 4210 may well have been suffering from pre-production problems. Both of these products will hopefully be re-evaluated in our labs at some point in the future when the problems have been ironed out.

In the meantime, you should evaluate them carefully under load in your own environment if you are considering purchase.

RealSecure also demonstrated problems with handling detection on a saturated network, causing it to miss attacks under load. Does this make RealSecure a bad IDS? Maybe not. It was very easy to deploy and configure, and provided excellent real-time alerting and reporting capabilities that might well make it an attractive proposition to some. You would need to ensure it is used in a lightly loaded environment, or spend much more time and effort (and money) in deploying multiple sensors on the same subnet and restricting the number of signatures detected by each individual sensor.

Of course, each time an update to the signature library is applied you would have to re-allocate the new signatures, and there may be a point where one of the reduced sensors begins to get overloaded again. The management overhead is thus much greater if the maximum network load cannot be handled by a single sensor. (Note that RealSecure also includes a host-based IDS capability that was not tested).

And, of course, there were plenty of products that acquitted themselves well in our tests, detecting attacks – and even performing packet reassembly in some cases – right up to 100Mbps network loads.

NetProwler is the odd one out in this remaining bunch, since although it performed well under load, it tended to misrepresent many of the attacks detected and was the only one of the group that could not detect the fragrouter attacks.

Cisco Secure IDS 4230, CA eTrust and BlackICE Sentry all offered the highest levels of performance, and each one provides unique features that may tip the balance in their favour.

Cisco Secure IDS is the only turnkey appliance (and offered some of the best reporting capabilities when partnered with the netForensics product), CA eTrust offers more in the way of general network monitoring and URL blocking capabilities than any other pure IDS product, and BlackICE Sentry provides the best overall performance under all circumstances, coupled with a small footprint and very low CPU utilisation.

The host-based IDS were slightly more straightforward, since all performed their allotted tasks well. Of the three, Tripwire stands out as being unique, since it is focussed purely on File Integrity Assessment, and could thus always be considered as complimentary to any other host-based IDS you may purchase.

Of the remaining two, Centrax is the one which would appear to offer the strongest solution, providing a combination of audit policy enforcement, Host IDS, Network IDS, Network Node IDS and even basic Vulnerability Assessment in a single package.

Without a doubt, CyberSafe's long experience in the host-based IDS market is evident in the Centrax product, and whilst the Network IDS component is not as strong as some of those on test here and you would never choose Centrax over the more mainstream VA scanners for that task alone, these are worthy inclusions in the overall package, making it the most well-rounded and comprehensive of all the IDS products we have tested.

SUMMARY

It is indisputable that the security market has taken off in the last couple of years as Internet connectivity becomes an essential part of every business and home user's communications armoury. Unfortunately for the potential purchase of security solutions, the market is simply not mature enough to make purchasing decisions as simple and safe as they should be.

Everyone now accepts that they need a firewall if they are going to connect computer systems to the outside world, but it is only recently that the firewall market has reached sufficient levels of maturity that the products could be considered "commodity" or "off the shelf" items. And some would argue that, given their complexity, they should never be considered in such a light.

At this year's NSS Group conference on *Internet Security and eCommerce* held in Monaco we were fortunate to witness a panel of distinguished experts in the field of Intrusion Detection. Rather shockingly, they concluded that the IDS market is still probably four years behind the firewall market in terms of maturity. That is a lot of catching up to do for these products, and there will undoubtedly be some singed corporate fingers on the way.

But it is not all doom and gloom. The technology is improving all the time and we are seeing new products appearing on a regular basis. It is certainly not worth waiting four years to see what happens – if we accept the analogies raised in the introduction to this report, then would you really want to risk not installing a burglar alarm in your home or office, just because it is difficult to do?

Most of the press coverage seems to focus on Network IDS, because that is the "fashionable" or "sexy" technology of the moment. But FBI figures are still pointing to the fact that over 70 per cent of all "hacks" are perpetrated by insiders. These are not "script kiddies" who are trying to break through your firewall or launch Denial of Service attacks against your servers. They are your own users trying to sneak a look at the payroll files, or steal vital product design data or customer names and addresses to take with them when they leave to work for your competitor at the end of the month.

To tackle these problems, the "old fashioned" Host IDS is what you need, a technology that has been around for a long time and is now enjoying something of a resurgence thanks to the interest in IDS in general brought about by the new and sexy network-based products. In most organisations today, host-based IDS should be the first IDS product you consider purchasing.

The security administrator who wants to cover all his bases will undoubtedly install both network- and host-based IDS, however. To date, there is not one single vendor who has managed to produce a top-performing product in all sectors (though if you are a fan of one-stop-shopping, Axent certainly has all the bases covered). Therefore, do not be afraid to mix best of breed products in order to provide optimum coverage.

One example would be to choose CyberSafe Centrax as your host-based system, Tripwire for File Integrity Assessment and BlackICE Sentry for high-performing Network IDS. Certainly when selecting your network-based IDS product, you should concentrate mainly on the performance and detection rates (and packet reassembly capabilities) rather than the prettiest GUI.

Not even the number of signatures matters as much as you might think, since many products are capable of employing more of a “generic” detection mechanism (and BlackICE uses protocol decodes) in order to detect a number of different attacks from a single signature.

The VA market place also suffers from some serious misconceptions. With VA products, it is important to differentiate between the host-based assessment products – such as Axent ESM – and the network-based assessment products – such as NetRecon, CyberCop Scanner, e-secure, and so on. Though network scanning tools are maturing, they are fundamentally different from host-based assessment tools. Host-based tools provide a privileged view of security from the inside, whilst network-based tools provide an unprivileged outsider's view of the same systems. Most security experts would agree that there is a place in most organisations for both.

It is also apparent from the testing we have carried out for this report that there is an enormous difference in coverage and quality of reporting of VA scanners from product to product. Organisations that are serious about their security assessment practices would be well advised to consider purchasing two different commercial products, as well as supplementing those with some of the more reputable *freeware* products from the Internet.

Finally, it would be remiss of us not to cover the most essential element of your security coverage. We mentioned earlier in this summary that some products employ a “generic” signature database that allows them to raise alerts for multiple attacks based on a single signature. This approach is essential as signature databases grow and grow – matching every attack to a unique signature is no longer efficient and reduces the chances of detecting attacks under load. The problem is that the administrator may be faced with an alert that simply says “*impossible IP packet*”. What does this mean? It could be a Land attack (chances are that it is, at the time of writing), but as new variants appear, that same message could be triggered by a number of different attacks.

The administrator who is not security literate might well look at the alert and decide that he has already patched his systems for that particular attack and thus neglect to apply a more recent patch that addresses a more recent variant. More likely, the non-security literate administrator will simply have no idea what an *impossible IP packet* is, and will thus ignore it.

So, what is the solution? Having already decided that it is no longer possible to have an all-encompassing signature database, the only component that is capable of being improved is – the administrator. Education is the key, and all the wonderful graphical interfaces and slick deployment methods in the world will not make these products simple to use, because they deal with a complex subject.

Before any administrator is let loose on a corporate network with a VA scanner or an IDS – in fact, even before such products are purchased - he or she should be thoroughly educated in the basics of security and hacking. What sort of attacks are possible – both from the inside and the outside. Where to go to research the latest vulnerabilities and acquire the most up-to-date patches. How to perform an effective VA scan, and how to deploy a Network IDS in the most efficient manner in both a switched and shared network environment.

Without such a basic grounding, they could cause more harm than good.

APPENDIX A – VENDOR QUESTIONNAIRES

The following questionnaires are fairly self-explanatory, and are reproduced here in their entirety, unedited, and as provided by the vendors. We have attempted to ensure that no blatant untruths are being perpetrated here, but the reader is advised to verify the answers before relying on them. Note that no questionnaire was returned for Axent's ESM product.

IDS Questionnaires

Axent Intruder Alert

Brief product description
Intruder Alert is a host-based IDS. It monitors system events (syslog, successful & failed logins, NT/W2K audit trails & events, etc.), performs file integrity monitoring, and monitors arbitrary applications for security events through text-based logs (databases, web servers, etc.)

Architecture
Host-based IDS. Scalable 3-tier architecture: Elements are Agents (perform collection & analysis), Managers (communications hub and database), and Consoles (Event monitoring and Administration)

At what layer of the protocol stack is the product working?
N/A

Documentation
Hard copy: User's Guide, Installation Guide, Release Notes. Online Help available within the product. On the web: User's Guide (http://www.axent.com/Axent/Public/Main?nav=Support&detail=/MainspanScripts/0/Axent/AxentWomSession/AxentWomSecureSession/D09O6L76CVA13C0M038BEH2643/ia35user0700.pdf) & Release Notes (http://www.axent.com/Axent/Public/Main?nav=Support&detail=/MainspanScripts/0/Axent/AxentWomSession/AxentWomSecureSession/0CBO6L76CVA13C0M038BEH2643/ITA35RNUnix0700.pdf)

What are the minimum/recommended console OS and hardware requirements?
NT 4 – SP3, or SP5+
HPUX 10.20
Solaris 2.5, 2.5.1, 2.6, 7

Is a dedicated machine required/recommended?
No.

Will it work on Windows 2000?
Agents and Managers are currently supported on Windows 2000, Consoles are not.

What are the minimum/recommended agent OS and hardware requirements?
Agents:
Solaris 2.5, 2.5.1, 2.6, 7
HPUX 10.20, 11.0
AIX 4.2, 4.3, and 4.3.1
Windows NT 4 – SP3, or SP5+
Windows 2000
Tru64 (Digital UNIX) 4.0D+
IRIX 6.2, 6.5
NCR UNIX SVR4 3.0
Sequent DYNIX/ptx 4.4.2
NetWare 4.11, 4.2, 5.0, 5.1
RedHat Linux available in December 2000
Managers:
Solaris, HPUX, AIX, NT, Windows 2000 (versions as above)

Is a dedicated machine required/recommended?
Agents: no dedicated machine. Managers: recommended, not required.

Will it work on Windows 2000?
Yes

What components are installed on a detector
Agents and Managers run as NT services, UNIX daemons, or NetWare NLM's.

Which network types are supported
Intruder Alert is a host-based IDS and can communicate over any physical network topology that supports TCP/IP.

Any specific recommendations for monitoring Gigabit networks with your product?
N/A

Which OS platforms are actively monitored?
Solaris 2.5, 2.5.1, 2.6, 7
HPUX 10.20, 11.0
AIX 4.2, 4.3, and 4.3.1
Windows NT 4 – SP3, or SP5+
Windows 2000
Tru64 (Digital UNIX) 4.0D+
IRIX 6.2, 6.5
NCR UNIX SVR4 3.0
Sequent DYNIX/ptx 4.4.2
NetWare 4.11, 4.2, 5.0, 5.1
RedHat Linux available in December 2000

Can sensors/detectors be deployed and configured initially from a central console?
Intruder Alert can be remotely deployed using a third-party deployment tool such as Microsoft SMS or Tivoli. Once deployed, the product can be remotely upgraded from a single console without using any third-party products.

Once deployed and configured, can sensors be managed from a central console?
Yes. Up to 1000 agents can be managed from 1 console.

Authentication between console and engines? What algorithm/key lengths?
Yes. User authentication is through username/password pairs. Diffie-Hellman key exchanges (128 bit keys), 400 bit Blowfish encryption on data.

Secure logon for policy management?
Yes.

How are policies distributed to engines?
Drag and Drop from single console.

How are policy changes handled?
Drag and Drop from single console.

Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
N/A

How many attack signatures?
400+

Can the administrator define custom attack signatures?
Yes. Very complex signatures and responses can be defined.

How are new attack signatures obtained and deployed?
Policies can be written/modified by users from a single console, new policies can be downloaded from the Axent SWAT website.

Frequency of signature updates?
14 new policy sets in the last year

Provide dates of all updates in the last year.
10/5/00 (3 policy sets)
9/22/00 (1 policy set)
8/29/00 (2 policy sets)
8/14/00 (1 policy set)
6/28/00 (1 policy set)
6/26/00 (2 policy sets)
3/23/00 (2 policy sets)
2/18/00 (1 policy set)
1/21/00 (1 policy set)

What infrastructure do you have behind the signature update process
Signature Updates are researched and created by Axent's dedicated team of security experts, the Information Security SWAT Team.

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
One signature file can be downloaded and then distributed to an entire enterprise from a single console.

Can signature updates be scheduled and fully automated?
No.

What network protocols are analysed?
N/A

What application-level protocols are analysed?
N/A

Can the product perform protocol decodes?
N/A

Can the product perform session recording on suspect sessions?
N/A

Block/tear down session?
N/A

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
N/A

Monitor changes in critical system files?
Yes. Intruder Alert monitors a short list of files every 30 seconds and a longer list of files every 8 hours (time periods and checksum types are user-definable).

Monitor changes in user-defined files?
Yes. Users can add arbitrary files to the list of critical files provided by Axent.

Monitor changes in Registry?
Yes, using NT Registry Auditing.

Monitor unauthorised access to files?
Yes.

Monitor administrator activity (creation of new users, etc)?
Yes.

Monitor excessive failed logins?
Yes.

List any other resources/locations that are monitored.
NT Application Log and sublogs, NT Security Log, NT System Logs and sublogs, UNIX syslog, wtmp, btmp, C2 logs, any user-defined text-based logfile (DB logs, web server logs, etc.), NetWare OS call-backs are used to monitor system activity on NetWare.

Track successful logins, monitoring subsequent file activity, etc?
Intruder Alert can track successful logins. Subsequent file activity can be monitored in a limited fashion via NT file audit messages and/or the Intruder Alert FileWatch utility.

Detect network-level packet based attacks?
N/A

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
N/A

Detect and report on nmap OS fingerprinting?
N/A

Perform packet reassembly? Resistance to known IDS evasion techniques?
N/A

Reconfigure firewall? If so, which firewall(s) and how?
N/A

Option to record everything for "forensic" investigation? Where is this data stored? How is it secured from tampering?
All collected date is stored in a database on the manager and can be used for forensic information. It is encrypted and communications are authenticated to prevent spoofing.

Reporting from engine to console - range of action/alert options
There are 14 Actions that can be used to respond to an event:
Record to Database
Send Email
Send Page
Append to Text Log File
Notify User via Pop-up Message
Execute Any Command or Script
Perform a Pre-defined Group of Responses
Kill Process
Disconnect Session
Disable User
Raise Flag (for event correlation)
Lower Flag (for event correlation)
Start Timer (to define time intervals for attacks)
Cancel Timer (to define time intervals for attacks)

What provision is made for temporary communications interruption between detector and console?
If communications are interrupted, events are locally cached until communications are restored.

Where are alerts stored?
On the agent or manager in question

Is the repository secure?
Yes, the files are protected via system permissions and are encrypted.

Can alerts be reported to the central console in real time without the use of third party software?
Yes, this is how Intruder Alert normally operates.

How easy is it to filter and extract individual events?
Intruder Alert has powerful querying abilities that can filter on numerous variables.

Does the software offer advice on preventative action to ensure the attack does not happen again?
The on-line documentation (http://www.axent.com/customersupport/intruderalert/docs/35/info/policydoc.html provides a growing body information on the vulnerabilities and countermeasures, organized by Intruder Alert policy name.

Integration with other scanning/IDS products?
Yes. Intruder Alert can integrate with most any IDS via SNMP or text-file monitoring.

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
Intruder Alert manages the size of its own copy of syslog. The event database is archivable, and reports can be generated from archived logs.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail?
Intruder Alert reporting uses its own powerful querying and filtering mechanism coupled with the Crystal Reports runtime engine to generate reports. There are pre-defined report templates that can use custom-defined ranges and filters to generate an infinite variety of reports. Custom report templates can be created as well if the user owns the Crystal Reports Report Designer.

Different reports for technicians and management/end users?
Yes.

Report management – can they be scheduled for automatic production?
No.

Can they be e-mailed to administrators or published straight to a Web site?
No.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
Alerts can be sent anywhere within an enterprise. Reports are generated at the manager level, and are limited to the 100 agents associated with that manager.

Define custom reports?
Yes.

How is it licensed? How is the license enforced?
Intruder Alert is licensed for each Agent and Manager. Consoles are free. The product enforces licensing through the Console.

End user pricing information
Agents: $995 per server, $395 per workstation
Managers: $1995 each
Consoles: Free

Ongoing cost of maintenance/updates
Basic Maintenance: 15% of purchase price – Includes all product updates and phone support
Extended Maintenance: 22.5% of purchase price – Includes updates and 7x24 phone support.

Axent NetProwler

Brief product description
NetProwler is a network-based IDS. It protects e-business by continuously watching IP based network segments for patterns of misuse or abuse. If these systems are threatened, NetProwler can notify you and even take precautionary actions to prevent information theft or loss.

Architecture
NetProwler is designed using a 3-tier architecture with Agents, Manager and the GUI console

At what layer of the protocol stack is the product working?
NetProwler is not bound to the NT Operating system stack. The NetProwler Agent driver uses an IP stack that has been specially developed to conceal the Agents presence from the network. NetProwler can monitor the entire IP packet from the Network layer on up.

Documentation
The NetProwler product is shipped with a hard copy set of Release Notes, Installation Manual and User Guide. The documentation is also available on the CD-ROM media in Acrobat PDF format.

What are the minimum/recommended console OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
Supported Manager Platforms
Windows NT 4.0
Requires: PII 300mhz 128 MB RAM, 70 MB Disk Storage + 50 to 500MB Additional Storage to hold NetProwler events and configuration information

Supported Agent Platforms
Windows NT 4.0
Requires: PII 300mhz 128MB RAM, 50-100 MB Disk Storage + 50 to 500MB Additional Storage to hold NetProwler events and configuration information

Supported Console Platforms
Windows NT 4.0 - 2000+
Requires: PII 300mhz 128 MB Ram, 10MB Disk Storage
A dedicated machine is recommended for each Agent and Manager Component. The Console can be installed on any workstation.

What are the minimum/recommended agent OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
As above

What components are installed on a detector
NetProwler installs a packet level driver and accompanying files for the SDSI attack detection engine, logging, authentication, encryption and a GUI.

Which network types are supported
NetProwler Supports 10 and 100mb Ethernet

Any specific recommendations for monitoring Gigabit networks with your product?
AXENT recommends evaluating the network environment and placing multiple agents in critical areas to provide coverage. AXENT is currently teaming with 3rd party vendors to bring a complete Gigabit solution to market.

Which OS platforms are actively monitored?
NetProwler monitors network traffic and identifies common attempts to exploit known vulnerabilities on numerous operating systems and applications, including Unix, Linux and VMS. It can also identify company-specific applications through its attack signature definition interface. While the Network IDS solution is not tied to any specific OS, it monitors all network based traffic, NetProwler will detect and apply OS specific signatures to the following types of operating systems:
Windows 95/98/NT/2000, Macintosh, Linux, AIX, HP-UX, Solaris, SUN-OS, BSDI BSD/OS, OSF 1, Free BSD, IRIX, NET BSD, OpenBSD, SCO UnixWare, Ultrix, VAX/VMS, SCO OpenServer, Netware

Can sensors/detectors be deployed and configured initially from a central console?
Sensors (Agents) can be configured from a central console. Agents must be directly installed on the intended host machine.

Once deployed and configured, can sensors/detectors be managed from a central console?
Sensors (Agents) can be managed from a central console.

Authentication between console and engines – Is it available? What algorithm/key lengths?
All communications between the Agent, Manager, and Console are secure via an authenticated Diffie-Hellman handshake, 56 bit Blowfish encryption and digital signatures using MD5.

Secure logon for policy management?
NetProwler supports password authenticated administrative consoles so that only privileged administrators can control the system.

How are policies distributed to engines?
The NetProwler Manager is responsible for automatically pushing all configuration and policy changes to each Agent via secure transports.

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
The Manager is a centralized repository which contains event and configuration data. The Manager is also responsible for automatically directing and deploying the configuration policies to the Agents. In addition, the Manager collects and compiles the event and alert information and makes this available for review on the Console. Any changes to policy are automatically deployed to the Agent which is responsible for implementation.

How many attack signatures?
Currently NetProwler has over 200 attack signatures.

Can the administrator define custom attack signatures?
Yes. Administrators can extend NetProwler's capabilities by utilizing its custom attack signature definition (ASD) user interface and its attack definition wizard help. The interface supports drag and drop key words, reserved keywords(related directly to the IP protocol), arithmetic operators and strings to build immediately deployable definitions without requiring programming. This tool allows for complex and sequential based attack signatures to be created and automatically deployed, not just simple string searches.

How are new attack signatures obtained and deployed?
NetProwler's signature update feature is called Signature Sync. This feature provides automatic web-download services. The signatures are intelligently distributed to ALL of the NetProwler Agents, and assigned to all of the proper systems. This of course all happens real-time for the Agents which never stop protecting the network to which they are assigned

Frequency of signature updates? Provide dates of all updates in the last year.
AXENT's signature update team, SWAT has released 7 signature updates this year.

Security Update 13 08/09/2000
Security Update 12 05/08/2000
Security Update 11 04/26/2000
Security Update 10 03/29/2000
Security Update 9 03/10/2000
Security Update 8 02/11/2000
Security Update 7 02/10/2000

What infrastructure do you have behind the signature update process
The Axent SWAT team, dedicated and separate from the product development team, researches security issues and vulnerabilities and creates new signatures for all of AXENT's signature related products. There is a dedicated website at www.axent.com/swat .

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
The update files can be placed upon and then downloaded from a local web server. The update only needs to be imported once into the centralized Manager, which then automatically deploys the new signatures to all of the Agents.

Can signature updates be scheduled and fully automated?
While the signature update process is fully automated (see question above) currently the initial download is manual.

What network protocols are analysed?
NetProwler supports TCP/IP on 10 and 100mb Ethernet networks

What application-level protocols are analysed?
NetProwler is not dependent on application level protocols, it can look at all IP based traffic including all application level protocols.

Can the product perform protocol decodes?
NetProwler can decode FTP, TELNET, SMTP, POP3, chat, rshell, and rlogin for session display.

Can the product perform session recording on suspect sessions?
Yes

Block/tear down session?
NetProwler's proprietary TCP/IP driver/stack, can create, on the fly, all necessary packets to stealthily send TCP/IP resets to any server. These packets contain only the information that the client would normally send when it would stop the session. Upon he receipt of the RST packet, the sever will shut the session down.

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
NetProwler has the ability to monitor any user-defined session, including custom applications.

Monitor changes in critical system files?
This is a host based function. Axent's host based product ITA ,covers this area.

Monitor changes in user-defined files?
This is a host based function. Axent's host based product ITA ,covers this area.

Monitor changes in Registry?
This is a host based function. Axent's host based product ITA ,covers this area.

Monitor unauthorised access to files?
This is a host based function. Axent's host based product ITA ,covers this area.

Monitor administrator activity (creation of new users, etc)?
This is a host based function. Axent's host based product ITA ,covers this area.

Monitor excessive failed logins?
Yes. NetProwler has signature designed to monitor failed logins.

List any other resources/locations that are monitored.
NetProwler monitors entire network segments for all traffic.

Track successful logins, monitoring subsequent file activity, etc?
This is a host based function. Axent's host based product ITA ,covers this area.

Detect network-level packet based attacks?
Yes.

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
NetProwler currently detects syn, udp, and full connect based scans.

Detect and report on nmap OS fingerprinting?
Yes.

Perform packet reassembly? Resistance to known IDS evasion techniques?
NetProwler does not currently perform reassembly. Future releases will address this feature.

Reconfigure firewall? If so, which firewall(s) and how?
The NetProwler Agent has built in functionality to harden Raptor and Checkpoint FW-1 firewalls. For Raptor, NetProwler uses the Raptor designated methodology for firewall hardening, including authenticating to the Raptor, and sending the information by encrypted mean. For Checkpoint, NetProwler uses the OPSEC compliant SAMP protocol to send the hardening commands. NetProwler is OPSEC 4.0 compatible.

Option to record everything for "forensic" investigation? Where is this data stored? How is it secured from tampering?
Yes. Recorded data can be used for potential litigation or to facilitate the design of new, custom attack signature definitions. It is stored on the Agent. File based security is recommended for securing the data since encrypting the data or otherwise modifying the data may render it inadmissible as evidence.

Reporting from engine to console - range of action/alert options (detail these)
When NetProwler identifies an attack, it can log the event, terminate the session, harden a Firewall, and notify an administrator via pager, SNMP or email. It can also start another program, record the session, forward event notification to the AXENT Intruder Alert manager and console to update its dynamic summary, and graph reports. In addition, it can update SNMP management consoles through the Intruder Alert Manger. All of these response configurations are fully determined by the administrator.

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
NetProwler Agents are self contained units. If at any time communication links between the Manager and Agents are severed(detected via heartbeat monitoring) , the Agent will continue to provide IDS services. Thus, any events being collected by an Agent will be reported to the Manager immediately upon resumption of Agent to Manager connectivity.

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
Agents respond to events in real-time and pass alerts of the events to the Manager directly, through secure transport. NetProwler includes a find alerts option which allows the database to be queried. Criteria includes alert type, specific signature names, agent names, priority, attacked system, attacking system, port number, date and time.

Does the software offer advice on preventative action to ensure the attack does not happen again?
Yes. Attack signatures include detailed information about the attack and direct signature specific links to the SWAT website. That site includes references to CERT, BugTraq, CVE, SANS and other sources as well as counter measures directly related to the attack.

Integration with other scanning/IDS products?
NetProwler includes event level integration with Intruder Alert.

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
NetProwler provides the facility to purge the SQL database. Other database maintenance functionality can be achieved through the included SQL database tools.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
NetProwler has extensive reporting capability. Included out of the box are many preformatted reports that cover a wide variety of system aspects. There are pre-formatted reports designed for system administrators, accountants, and executives. In addition, the customers can use their own Crystal Report templates directly from the NetProwler Report Wizard. This allows the customer to extract exactly the information they desire, and format it to their own specifications.

Report management – can they be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?
NetProwler supports the scheduling of reports from interval (minutes/hours) to daily to monthly. Reports can be emailed to administrators. A command can be spawned upon the generation of the Report, and that command could include the publishing of files to a website. The reports are placed with the centralized manager and are available to all of the authorized NetProwler consoles.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
NetProwler can consolidate information from each detector into a single report, which includes information about attacked servers.

Define custom reports?
Customers can use their own Crystal Report templates directly from the NetProwler Report Wizard. Standard SQL tools can be also be used to extract the exact dataset required.

How is it licensed? How is the license enforced?
The following license types are available:
Evaluation licenses that incorporate expiration dates. This is included in the product. The applications can be run unhindered for 45 days from the time of installation.
Permanent licenses that are applied to a specific manager and agent systems. Each license represents installing the application on a single host machine.
NetProwler consists of the following components: NetProwler Agent, NetProwler Manager, and NetProwler Console. The Windows NT Console and Manger are "Free" – AXENT does not charge for the NT console or manager and the customer can install and run as many consoles as they wish.

The Customer can purchase a version of the product called NetProwler Enterprise, available in three licensed tiers based on the number of nodes monitored by the Agent . In the Enterprise version all three components are delivered on the same CD. In addition, each Enterprise CD also contains an Intruder Alert Manager and Agent.

End user pricing information
The NetProwler Enterprise versions are $2,995- $8995US depending on the number of nodes monitored by the Agent.. Console and Manager are free. International pricing is available as a conversion from US dollars at the time of purchase.

Ongoing cost of maintenance/updates
Basic Maintenance: 15% of purchase price – Includes all product updates and 5x8 phone support
Extended Maintenance: 22.5% of purchase price – Includes updates and 7x24 phone support.

Cisco Secure IDS

Brief product description
The Cisco Secure IDS is a network-based IDS using a dedicated security appliance as the 'sensor'. Sensors, which are high-speed security analysis devices, analyse packets traversing the network to determine if the traffic is authorised or malicious. If the data stream in a network exhibits unauthorised or suspicious activity, such as a SATAN attack, a ping sweep, or the transmission of a secret research project code word, sensors can detect the policy violation in real time, terminate the offending session(s), and send alarms back to a central management console. The management console is a scalable software-based management system that centrally monitors the activity of multiple sensors, provides a visual alarm display, and acts as a remote system configuration utility.

Architecture
The appliance has one interface to promiscuously monitor the traffic and a second interface for communication to the NT based 'Director' control software, CSPM. ('Director' software running on HP/OV on Solaris or HP/UX is also available)

At what layer of the protocol stack is the product working?
Up to layer 7

Documentation
A User Guide manual is supplied in hard copy. All Documents are supplied on CD-ROM and are also available on-line

What are the minimum/recommended console OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
The basic requirements of the Director are Windows NT with Service Pack 6a, IE 5.0, 200MHz Pentium, 96M RAM. Full details are at http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver22/install/overview.htm

What are the minimum/recommended agent OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
The IDS sensor is packaged as a turnkey, "plug-and-play" security appliance. The complete hardware and software package is manufactured, tested, and supported by a single vendor.

What components are installed on a detector?
The Sensor comes with both the Operating System and IDS application pre-loaded and configured. There is no need for the user to be aware of the OS.

Which network types are supported
10/100 Ethernet

Any specific recommendations for monitoring Gigabit networks with your product?
For very high speed IDS Cisco recommends the 'blade' version of the product that works within the Catalyst 6500 Switch. Multiple 'blades' can be added to achieve Gigabit speeds

Which OS platforms are actively monitored?
NT, Novell, Solaris

Can sensors/detectors be deployed and configured initially from a central console?
No. During installation, the operator is required to enter six parameters on the appliance (e.g., IP address, mask, locator Ids, etc.). For security reasons, physical access to the appliance is required for initial configuration.

Once deployed and configured, can sensors/detectors be managed from a central console?
Yes. They can be remotely configured and updated from the Cisco Secure Policy Manager console (or other management options).

Authentication between console and engines – Is it available? What algorithm/key lengths?
This can be achieved via external encryption routers/firewalls. All the data is UDP port 45000. Optional IPSec encryption is supported.

Secure logon for policy management?
Yes

How are policies distributed to engines?
Policy is distributed to the Sensor via a control agent. From the central policy database, configurations for each managed Sensor is held and maintained. When the operator changes any parameter in the Sensor configuration, a new file is transfer to the Sensor. Standard policy templates can be concurrently applied to multiple Sensors in the policy domain.

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
If a change is made to an active policy on a Sensor(s), the central policy server will reapply the updated policy after confirming the action with the operator. There is a one-to-one or one-to-many mapping of policies to Sensors so operator intervention is required

How many attack signatures?
The Cisco Secure IDS ships with over 300 generic group signatures each covering one or more specific signatures

Can the administrator define custom attack signatures?
Administrators can add custom string match signatures on any port.

How are new attack signatures obtained and deployed?
The updated signatures are obtained via our website. You can subscribe and receive an email when a new signature update is posted.

Frequency of signature updates? Provide dates of all updates in the last year.
Approximately every 60 days. 2.2.1.2 on Dec/99; 2.2.1.3 on Mar/00; 2.2.1.4 on Apr/00; 2.2.1.5 (including IP fragmentation reassembly support and “anti-IDS” whisker support) on Aug/00. This release 2.5.0.102 on Oct/00

What infrastructure do you have behind the signature update process
We have a dedicated team of engineers working on all aspects of IDS, scanning and Security Posture Assessment.

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
Once the ‘Director’ management station has the new signature set it downloads it to all the ‘Sensors’

Can signature updates be scheduled and fully automated?
It is important that the network operators know that a new signature set is deployed, updates are invoked manually from the central ‘Director’

What network protocols are analysed?
The Cisco Secure Intrusion Detection System can monitor all of the major TCP/IP protocols, including IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP). It can also statefully decode application-layer protocols such as FTP, Simple Mail Transfer Protocol (SMTP), HTTP, Domain Name System (DNS), remote procedure call (RPC), NetBIOS, NNTP and Telnet

What application-level protocols are analysed?
n/a

Can the product perform protocol decodes?
No

Can the product perform session recording on suspect sessions?
Yes

Block/tear down session?
Both TCP reset (sent to attacker and attacked host) and/or reconfiguration of an Access Control List on a router are optional and can be configured on a per signature basis.

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
No, but you can look for a specific string (e.g. the banner) from an FTP server

Monitor changes in critical system files?
No

Monitor changes in user-defined files?
No

Monitor changes in Registry?
No

Monitor unauthorised access to files?
No

Monitor administrator activity (creation of new users, etc)?
Yes

Monitor excessive failed logins?
No

List any other resources/locations that are monitored.
n/a

Track successful logins, monitoring subsequent file activity, etc?
No

Detect network-level packet based attacks?
Yes

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
Yes

Detect and report on nmap OS fingerprinting?
Yes

Perform packet reassembly? Resistance to known IDS evasion techniques?
Yes

Reconfigure firewall? If so, which firewall(s) and how?
No, but in the current release ACLs can be added to Cisco IOS Firewall, just as they can to Cisco routers. In a future release ACLs can be added to the Cisco Secure PIX Firewall.

Option to record everything for “forensic” investigation? Where is this data stored? How is it secured from tampering?
Optionally on both the hard drive in the ‘Sensor’ and in the ‘Director’, physical security is assumed

Reporting from engine to console - range of action/alert options (detail these)
Alert and/or log and/or TCP reset and/or reconfigure router ACL

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
Data is stored on the hard drive on the ‘Sensor’

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
All events go to the screen in real-time. Filters can be applied on each signature and also be based on source IP address.

Does the software offer advice on preventative action to ensure the attack does not happen again?
There is a configurable on-line HTML database. Apart from full details about each signature there is a section which can be customised so that a user knows exactly what to do with any particular signature

Integration with other scanning/IDS products?
Cisco has integrated host-based data using a third party management console. Integration of our scanning product is planned

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
Archival and purging can be scheduled via the browser.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
Reporting for the Cisco IDS is provided through third-party applications like netForensics and TeleMate.Net

Report management – can they be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?
See above

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
See above

How is it licensed? How is the license enforced?
There are no licensing restrictions on the 'Sensor'. The 'Director' has no restrictions – except the Lite version which is restricted to managing three devices ('Sensors', Cisco IOS Firewall routers or Cisco Secure PIX Firewalls)

End user pricing information
Sensor 4210 $8000
Sensor 4230 $19000
List price of CSPM lite (3 devices) $2000, [full CSPM $14995].
End user price of netForensics Workgroup software from $14,995 for 5 devices

Ongoing cost of maintenance/updates
Annual List Price of SMARTnet for 4210 from $1656. Annual List Price of CSPM Software Application Support $400, [full CSPM $3000]. Annual end user price of netForensics software subscription from $1,500.

CA eTrust Intrusion Detection

Brief product description
Network Based Session Sniffer with wide range of capabilities. 3rd generation firewall

Architecture
Single engine. Enterprise management components also available.

At what layer of the protocol stack is the product working?
Layer 2 / MAC

Documentation
Its on the CD

What are the minimum/recommended console OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
Win NT, Win2000, PII500MHZ min. depending on size of network and traffic. Dedicated machine always recommended.

What are the minimum/recommended agent OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
Win NT, Win2000, PII500MHZ min. depending on size of network and traffic. Dedicated machine always recommended.
What components are installed on a detector (i.e. Windows NT packet driver, NT service, Linux daemon, etc)
EID, sw3servc service, Sandis.rv driver

Which network types are supported
TR, 10/100 Ethernet, FDDI

Any specific recommendations for monitoring Gigabit networks with your product?
Spread load across multiple agents and collectively manage through console manager

Which OS platforms are actively monitored?
Any that uses TCP/IP including MAC OS

Can sensors/detectors be deployed and configured initially from a central console?
Must be installed at collector manually or via remote control and can be configured via Central.

Once deployed and configured, can sensors/detectors be managed from a central console?
Yes

Authentication between console and engines – Is it available? What algorithm/key lengths?
Yes, Blowfish 128 Bit

Secure logon for policy management?
Yes

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
Manually

How many attack signatures?
Over 300

Can the administrator define custom attack signatures?
Yes

How are new attack signatures obtained and deployed?
Automatic download from website. Usually over 10 per update

Frequency of signature updates? Provide dates of all updates in the last year.
Minimum once a month. No dates.

What infrastructure do you have behind the signature update process (i.e. dedicated team of engineers? How many? Does it have a name?)
CA, CVE and Bugtraq

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
Yes,

Can signature updates be scheduled and fully automated?
No.

What network protocols are analysed?
TCP/IP

What application-level protocols are analysed?
None, unless it passes through a NIC over a TCP/IP port.

Can the product perform protocol decodes?
No

Can the product perform session recording on suspect sessions?
Yes

Block/tear down session?
Yes

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
Yes

Monitor changes in critical system files?
No

Monitor changes in user-defined files?
No

Monitor changes in Registry?
No

Monitor unauthorised access to files?
No

Monitor administrator activity (creation of new users, etc)?
No

Monitor excessive failed logins?
No

List any other resources/locations that are monitored.
Anything that's network based and using TCP/IP

Track successful logins, monitoring subsequent file activity, etc?
No

Detect network-level packet based attacks?
Yes

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
Yes

Detect and report on nmap OS fingerprinting?
Yes

Perform packet reassembly? Resistance to known IDS evasion techniques?
Yes

Reconfigure firewall? If so, which firewall(s) and how?
FW-1, CA FW

Option to record everything for "forensic" investigation? Where is this data stored? How is it secured from tampering?
Yes, SALOG, Proprietary Encryption

Reporting from engine to console - range of action/alert options (detail these)
Unknown

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
Yes, it's secure. Auto-Reconnect

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
Yes, relatively easy

Does the software offer advice on preventative action to ensure the attack does not happen again?
Very good advice. CVE

Integration with other scanning/IDS products?
No

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
Yes, workspace switching

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
Many canned reports, easy to customize and add new reports. Yes.

Report management – can they be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?
Yes, via Report Scheduler

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
Yes, via LogView and LogView Browser

Define custom reports?
Yes

How is it licensed? How is the license enforced?
Concurrent Sessions. It will not monitor any more sessions above model limit.

End user pricing information
(Not supplied)

Ongoing cost of maintenance/updates
(Not supplied)

CyberSafe Centrax

Brief product description
Centrax is a comprehensive hybrid intrusion detection system offering host and network-based intrusion detection and response for enterprise networks. Centrax gives you the power to monitor hundreds of Microsoft Windows 2000, Microsoft Windows NT, Sun SparcStation Solaris, IBM AIX, and Hewlett-Packard HP-UX targets in your network for security assessment, misuse detection, and response.

Architecture – Host/network/network node-based and a brief description of the architectural elements (management/reporting servers, etc).
The Centrax product is comprised of a Command Console and one or more Target Agents. A Target Agent may be either a host-based Agent, which resides on each workstation or server you want to monitor, a network Agent, which sits anywhere on a network segment you want to monitor, or a network node agent which watches network packets destined to or from a mission critical host.

At what layer of the protocol stack is the product working?
Centrax works at the application layer for Host Based agents and at the network layer for Network Based and Network Node agents

Documentation – "Getting Started"? Admin/Reference Guide? On-line or hard copy? Supplemental information available on-line?
The Centrax Users Guide, available on-line, is a comprehensive guide to the product which includes topics covering the areas mentioned above.

What are the minimum/recommended console OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
Software
Microsoft Windows NT Server or Workstation Version 4.0, Service Pack 6A or later; or Windows 2000
Microsoft Data Access Components (MDAC) version 2.5 (Windows NT only, provided during Centrax installation process if not already installed)
Hardware
550 MHz Pentium processor computer
800 x 600 (minimum) VGA display
256 MB
256 MB virtual memory
20 MB available disk space plus additional space for collecting and storing alerts in the log database
CD-ROM drive
Optional: SCSI hard disk (to provide faster disk access)
We recommend that you install Centrax command console on a standalone Windows NT/2000 server, not on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC). For larger enterprise deployments, the Centrax console benefits from additional processing and memory power.

What are the minimum/recommended agent OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
OS requirements for Windows 2000 and Windows NT agents
Microsoft Windows NT Workstation or Server Version 4.0 Service Pack 3 or later; or Windows 2000
Windows Packet Filter required for NID and NNID agents (included on the installation CD)
We recommend a dedicated machine be used for Network ID although this is not required for Network Node ID
Hardware requirements for Windows 2000 or NT agents
200 MHz Pentium processor computer (minimum)
800 x 600 (minimum) VGA display (required when installing the target service)
64 MB RAM
128 MB virtual memory
32 MB available disk space (maximum Event Log size)

CD-ROM drive (if the Target Service is to be installed via diskette)
3½" disk drive (if the Target Service is to be installed via diskette
For desktop computers, PCI Ethernet or PCI Fast Ethernet card (NID and NNID)
For laptop computers, CardBus (32-bit) PCMCIA network interface card (NID and NNID)
OS requirements for Solaris agents
Solaris 2.51, 2.6, 7.0, or 8.0 with all current patches applied
Hardware requirements for Solaris agents
Sun Microsystems SparcStation
Display and memory suitable to run Solaris
3 MB available disk space
/var/audit set for 500 MB (estimated requirement based on collecting audit data four times per day)
OS requirements for AIX agents
AIX 4.2.1 or 4.3.2 with all current patches applied
Hardware requirements for AIX targets
IBM RS/6000, or equivalent
Display and memory suitable to run AIX
3 MB available disk space
/var/audit set for 500 MB (estimated requirement based on collecting audit data four times per day)
OS requirements for HP-UX targets
HP-UX 10.20 or 11.0 with all current patches applied
Hardware requirements for HP-UX targets
Hewlett-Packard HP9000 workstation, or equivalent
Display and memory suitable to run HP-UX
3 MB available disk space
/var/audit set for 500 MB (estimated requirement based on collecting audit data four times per day)
Tripwire Requirements

What components are installed on a detector
Services running on the command console (Windows2000 or Windows NT):
Detection Service
Scheduler Service
Target Service
Real-time Service (optional)
Network or Network Node Service (optional)
The Network and Network Node Services also require the Windows Packet Filter protocol be installed as a prerequisite which is included on the product CD.

Services running on the agents (Windows 2000 or Windows NT):
Target Service
Real-time Service (optional)
Network or Network Node Service (optional, requires WPF protocol as above)

Daemons running on the agents (Sun Solaris, AIX, HP):
Target daemon
Real-time daemon (optional)

Which network types are supported
Centrax network based IDS agents support 10/100 Ethernet, network node agents support > 100 MB/s Ethernet networks

Any specific recommendations for monitoring Gigabit networks with your product?
We recommend installing network node agents for networks > 100 MB/s

Which OS platforms are actively monitored?
Windows 2000, Windows NT, AIX, Sun Solaris and HP/UX.

Can sensors/detectors be deployed and configured initially from a central console?
Target installation images are built at the console for all agents.

Windows 2000 and Windows NT agents are usually deployed by connecting to a network share at the console and running the setup program. For Unix agents, the installation directory needs to be copied to the host where the setup program is then executed. Agents can also be deployed using SMS in Microsoft networks.

Once deployed and configured, can sensors/detectors be managed from a central console?
Yes.

Authentication between console and engines – Is it available? What algorithm/key lengths?
All transmissions of audit policies, collection policies, and counter-measure responses between the Management Console and Target Agents are encrypted. The authentication mechanism between the console and the agents occurs through a shared key authentication encrypted with triple-DES at 128 bits by default, though the quality of protection may be specified for lesser encryption algorithms.

Secure logon for policy management?
This capability is provided by a separate CyberSafe Secure Single Sign-on solution called ActiveTRUST.

How are policies distributed to engines?
Policies are distributed either by selecting one or more agents at the command console GUI and right clicking on the apply policy button, or in a 'hands-free' automated fashion using the in-built scheduler for audit policy deployment.

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
All target machines affected by the change are detected automatically by the central command console where the option to deploy the new policy is given on a per agent basis or for all affected agents.

How many attack signatures?
Centrax comes with a library of over 770 host-based signatures for Windows NT/2000, Solaris, AIX, and HP-UX, and over 116 network-based signatures for TCP/IP networks. Each of these signatures is highly customisable based on files, users, and individual computers to create a virtual library of infinite size.

Can the administrator define custom attack signatures?
Centrax provides the capability to define and customize detectable patterns of misuse for detection. In addition, CyberSafe is always willing to design those attack signatures to the specifications of a customer for their use.

How are new attack signatures obtained and deployed?
Centrax Network Signature Update is available for updating network attack signatures from the Cybersafe web site.

Frequency of signature updates? Provide dates of all updates in the last year.
(Not supplied)

What infrastructure do you have behind the signature update process
Centrax signatures are developed by CyberSafe's Security Research Group (SRG).

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
Centrax Network Signature Updates can be downloaded to the local network once and deployed using the Centrax policy management capabilities.

Can signature updates be scheduled and fully automated?
This is in the Product Roadmap for future release.

What network protocols are analysed?
The TCP/IP protocol is analysed by Centrax.

What application-level protocols are analysed?
Centrax monitors application services such as HTTP, Telnet, FTP, SMTP, POP3, IMAP, Rlogin, Shell, Portmapper, NIS, PCNFS, AdminD, Selection Service, Statd, YPUpdateD, Rwho, Talkd, TFTP, Finger, DNS and dfstab files on Solaris.

Can the product perform protocol decodes?
Centrax is currently incapable of performing this function.

Can the product perform session recording on suspect sessions?
No.

Block/tear down session?
Yes.

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
Yes.

Monitor changes in critical system files?
Yes.

Monitor changes in user-defined files?
Yes.

Monitor changes in Registry?
Yes.

Monitor unauthorised access to files?
Yes.

Monitor administrator activity (creation of new users, etc)?
Yes.

Monitor excessive failed logins?
Yes.

List any other resources/locations that are monitored.
Centrax strictly monitors operating systems audit logs with respect to host based intrusion detection. In addition, TCP/IP traffic is monitored as a means of performing network based intrusion detection.

Track successful logins, monitoring subsequent file activity, etc?
Yes. Centrax hosts can monitor the authentication activities of all users. All user logon and logoff activity on a Centrax host can be recorded on a per user basis.

Detect network-level packet based attacks?
Yes.

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
Yes.

Detect and report on nmap OS fingerprinting?
Yes.

Perform packet reassembly? Resistance to known IDS evasion techniques?
This is part of the product roadmap for release in 2001.

Reconfigure firewall? If so, which firewall(s) and how?
Through the use of the custom response mechanism in Centrax, firewalls can be configured using user-defined scripts which invoke responses particular to the predetermined scenario.

Option to record everything for "forensic" investigation? Where is this data stored? How is it secured from tampering?
Yes. Centrax stores the information locally on the target until it is transmitted to the Command Console. As previously mentioned, this transmission is secure. While the information is stored on the targets, it is secured by NT's inherent functionality as the event logs cannot be modified. Additionally, on UNIX machines the logs are all C2 logs, so they too cannot be subverted. Additionally, Centrax monitors all of its agents to alert if they are being compromised or if the audit data is under attack.

Reporting from engine to console - range of action/alert options (detail these)
When an activity signature is detected, notifications can be triggered automatically.
Alerts - MAPI/SMTP mail, Pager (via TAPI), SNMP
Responses – logoff user, disable user account, shutdown machine, terminate connection, initiate Tripwire scan, custom responses

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
Communication loss between detector and console is highlighted at the console. In the event of a communications interruption, alerts are queued at the detector until communications are re-established. It is also possible to establish a fail-over console should a primary console fail.

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
Centrax offers both batch and real-time alerting as part of the core components.
The alert filter built in to the product can be used to easily extract and filter alerts by agent/detector, user, priority, time period and by number of alerts

Does the software offer advice on preventative action to ensure the attack does not happen again?
Yes, each alert displayed at the console offers advice and actions for preventative measures Centrax provides a natural language description and suggested corrective actions for each security configuration element and signature that it detects.

Integration with other scanning/IDS products?
Yes – Tripwire 2.2.1.

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
Centrax's Audit Policy Management provides the ability to define, deploy, and maintain global enterprise-wide heterogeneous security through the use of native operating system auditing. The management of audit policies, which includes the definition, deployment, and subsequent maintenance of these policies, is governed from a central location, the Centrax Command Console. All audit logs are collected and deposited to a central point. Housekeeping utilities for automatic rotation and archiving of raw audit trails are also provided on the product CD. Centrax also provides database utilities for database archival, compaction and archive reporting tools.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
Centrax 2.4 includes an extensive reporting capability that allows the user to perform forensic analysis of evidentiary audit trails. Centrax software contains a built-in report generator for accessing intrusion detection data and generating customized reports. These reports can be automatically edited through the use of our report generator.

Report management – can they be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?
Reporting can be fully automated using the Centrax scheduler. Reports can be published straight to a Web site, sent to a printer/file or formatted into many different formats including MS Word, Excel, CSV amongst many others.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
The reporting mechanism consolidates information from every server and detector, regardless of operating system and configuration.

Define custom reports?
Centrax publishes the database schema so that users can build their own custom reports and queries. Using the GUI at the console , users can build their own customised reports by user(s), host(s), activity(s) and event(s) which can then be saved as templates for either manual use or in an automated fashion using the in-built scheduler.

How is it licensed? How is the license enforced?
Centrax is licensed at the console only. It is based on both time and the number of agents with which it communicates. Time is only enforced during demo periods. It is not necessary to reinstall any license keys on distributed target agents.

End user pricing information

Centrax 2.4 Command Console 1 License	£2,500.00
Centrax 2.4 Command Console 2-4 License	£1,495.00
Centrax 2.4 Command Console 5+ License	£995.00
Centrax 2.4 Server Target 1-25	£800.00
Centrax 2.4 Server Target 26-50	£750.00
Centrax 2.4 Server Target 51-100	£700.00
Centrax 2.4 Server Target 101-250	£650.00
Centrax 2.4 Server Target 251-500	£600.00
Centrax 2.4 Server Target 501-1000	£550.00
Centrax 2.4 Server Target 1000+	£500.00
Centrax Network Target	
Centrax 2.4 Class B Network License	£7,500.00
Centrax 2.4 Class C Network License	£2,500.00

Ongoing cost of maintenance/updates
Maintenance is 20% / year and includes phone support and updates.

ISS RealSecure

Brief product description
RealSecure provides a comprehensive intrusion detection solution by combining host- and network-based intrusion detection into a single platform. RealSecure uses a standards-based approach, comparing network traffic and host log entries to the known and likely methods of attackers. Suspicious activities trigger administrator alarms and other configurable responses.

Architecture – Host/network/network node-based and a brief description of the architectural elements (management/reporting servers, etc).
RealSecure uses a distributed architecture. Network and host-based sensors perform filtering and monitoring functions on a given network segment or host computer. Consoles display events passed from the sensors, manage the individual sensors, and provide a centralized database for the collection of event information, and reporting capabilities.

At what layer of the protocol stack is the product working?
Network Sensor: The Network Sensor works at the lowest layer, grabbing raw packets directly off the card, making it completely independent of the TCP/IP stack of the host system for interpretation of the packets being analysed. You can unbind TCP/IP from the card you are monitoring to run in "stealth mode", and we recommend this for ultra-secure operation.

Server Sensor: The Server Sensor analyses some packets at the same low layer as the Network Sensor, right as they come off the network. This is for malformed packet attacks and denial of service attacks. However most of the signatures are done at a fairly high level up in the stack, after reassembly and such has gone on. This has the advantage that we know the results of reassembly EXACTLY the way the target will interpret them.

Documentation
RealSecure comes with a Getting Started Guide, a User's Guide, and a Signature Reference Manual. These are available on-line and hard copy.

What are the minimum/recommended console OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
Minimum Processor: Intel Pentium II 300 MHz.
Operating System: Windows NT 4 Workstation with Sp6a recommended (SP3 – SP6a supported).
Memory: 256MB recommended (128MB minimum).
Disk Space: 100MB per sensor managed from console.
Dedicated system recommended.
The console works on Windows 2000 and will be officially supported in Q4 of 2000.

What are the minimum/recommended agent OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
System Requirements for Windows NT Network Sensor
Minimum Processor: Intel Pentium II 300 MHz.
Operating System: Windows NT 4 Workstation with Sp6a recommended (SP3 – SP6a supported).
Memory: 128MB Minimum (256MB recommended)
Disk Space: 150MB.
NIC: PCI adapter capable of promiscuous mode.
Dedicated system required.
The Network Sensor works on Windows 2000 and will be officially supported in Q4 of 2000.

System Requirements for Solaris SPARC Network Sensor
Platform: UltraSPARC 2.
Operating System: Solaris SPARC 2.6 or Solaris SPARC 7.
Memory: 128MB Minimum (256MB recommended).
Disk Space: 150MB.
NIC: Sbus or PCI adapter capable of promiscuous mode.
Dedicated System required.
System Requirements for Server Sensor and OS Sensor for Windows NT
Operating System: Microsoft Windows NT 4.0 SP3 (SP6a recommended)
Memory: 64MB
Disk Space: 50MB
Dedicated system not required.
Will run on Windows 2000 and will be officially supported in Q4 of 2000.

System Requirements for Server Sensor and OS Sensor for Solaris SPARC
Operating System: Solaris SPARC 2.6 and Solaris SPARC 7
Disk Space: 50MB
Dedicated system not required.

System Requirements for OS Sensor for IBM AIX
Operating System: AIX 4.3.2 or AIX 4.3.3
Disk Space: 50 MB
Dedicated system not required.

System Requirements for OS Sensor for HP-UX
Operating System: HP-UX 11.x
Disk Space: 50 MB
Dedicated system not required.

What components are installed on a detector?
The Windows NT Network Sensor runs as a service and uses a Windows NT packet driver.
The Solaris Network Sensor runs as a daemon.

Which network types are supported?
RealSecure operates on Ethernet networks (10 Mbps), Fast Ethernet networks (100Base-T only, 100 Mbps), FDDI (100 Mbps), and Token Ring networks (4 Mbps to 16 Mbps on NT only).

Any specific recommendations for monitoring Gigabit networks with your product?
Multiple RealSecure Network Sensors connected to a Top Layer AppSwitch will monitor a Gigabit network.

Which OS platforms are actively monitored?
The host-based Server and OS Sensor have been ported to NT, Solaris, AIX and HPUX. Network Sensor runs on NT and Solaris but protects your entire network.

Can sensors/detectors be deployed and configured initially from a central console?
Sensors are deployed manually and initially configured from the central console.

Once deployed and configured, can sensors/detectors be managed from a central console?
Yes. RealSecure Sensors are controlled and managed from a central console.

Authentication between console and engines – Is it available? What algorithm/key lengths?
Yes. Authentication is available between the console and sensors and is based on public key exchange. RealSecure uses Certicom's 239-bit elliptic curve public-key technology for UNIX and NT Sensors. Additionally on NT, you may also use encryption algorithms called through Microsoft's Cryptographic API, which will use whatever encryption technology is available through that API. Microsoft's default CSP is based on RSA technology and provides 512-bit or 1024-bit public encryption keys.

Secure logon for policy management?
Yes. The RealSecure Console handles Policy Management. The management capabilities of the Console are only accessible to the user who initially installed the Console.

How are policies distributed to engines?
Policies are pushed from the Console to the individual sensors over a secure channel.

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
Policy changes are enacted at the console and are manually pushed down to the individual sensors.

How many attack signatures?
RealSecure has over 430 attack signatures.

Can the administrator define custom attack signatures?
Yes. RealSecure provides the ability to define custom attack signatures.

How are new attack signatures obtained and deployed?
ISS X-Press Updates provide new signature for RealSecure Sensors. These updates are downloaded from a secure web site and are deployed to the sensors from the console.

Frequency of signature updates? Provide dates of all updates in the last year.
ISS has released three X-Press Updates since the capability was added to RealSecure in June 2000.
1.1 on July 7, 2000 added SubSeven_Scan
1.2 on August 3, 2000 updated existing signatures only
1.3 on September 29, 2000 added 31 new signatures

What infrastructure do you have behind the signature update process
The ISS X-Force is a dedicated team of over 60 security experts researching and coding new signatures for RealSecure.

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
Signature update files are downloaded to the console machine and deployed to the sensors from the console.

Can signature updates be scheduled and fully automated?
No.

What network protocols are analysed?
The Network Sensor can filter and monitor any TCP/IP protocol.

What application-level protocols are analysed?
RealSecure can interpret web, e-mail, file transfer, remote login, chat, talk and a host of other network services. In addition, the Network Sensor can monitor and decode Microsoft CIFS/SAMBA traffic for Windows networking environments.

Can the product perform protocol decodes?
Yes. RealSecure performs decode based on UDP, TCP, and ICMP.

Can the product perform session recording on suspect sessions?
Yes. RealSecure Network Sensors offer the ability to record the raw, binary content of an entire network session. This data is stored in a log file and can be replayed through the Workgroup Manager interface. It is played back exactly as it was received, keystroke for keystroke, so that the administrator can see how the attack or session unfolded.

Block/tear down session?
Yes. The RealSecure Server Sensor will block/tear down sessions.

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
RealSecure provides the ability to define and monitor connection events based on protocol (TCP, UDP, ICMP), source port, destination port, source IP address, and/or destination IP address.

Monitor changes in critical system files?
Yes, RealSecure Server Sensor will monitor any file for changes. It also provides the capability of copying back the correct version of the file from a safe place. This can be useful for monitoring web pages for hacks

Monitor changes in user-defined files?
Yes, RealSecure Server Sensor will monitor any file for changes.

Monitor changes in Registry?
Yes, RealSecure Server Sensor will monitor the registry for changes.

Monitor unauthorised access to files?
Yes, RealSecure Server Sensor will monitor access to any file.

Monitor administrator activity (creation of new users, etc)?
Yes, Real Secure Server Sensor will monitor both usual and unusual administrator activity.

Monitor excessive failed logins?
Yes, RealSecure Server Sensor will monitor excessive failed logins.

List any other resources/locations that are monitored.
RealSecure can also monitor Solaris BSM Logs, any arbitrary text log file, and syslogs forwarded from another Unix box or other equipment (such as a Cisco routers).

Track successful logins, monitoring subsequent file activity, etc?
Yes, RealSecure Server Sensor will monitor successful login and will monitor some file activity.

Detect network-level packet based attacks?
Yes, RealSecure Network Sensor will detect network-level packet based attacks.

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
Yes, RealSecure detects all types of port scans(full connect, SYN stealth, FIN stealth, and UDP).

Detect and report on nmap OS fingerprinting?
Yes, RealSecure provides a signature for the nMap OS fingerprinting tool.

Perform packet reassembly? Resistance to known IDS evasion techniques?
The RealSecure Server Sensor monitors traffic from several layers of the IP stack allowing it to see traffic before it goes up the stack as well as when it has been reassembled. This technique allows Server Sensor to monitor traffic EXACTLY the way the target will interpret them, so it cannot be fooled by any of the tricks outlined in the infamous SNI Paper ("Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection"

Reconfigure firewall? If so, which firewall(s) and how?
The RealSecure Network Sensor will send a message to the FireWall-1 management server instructing it to prevent the attacking source address, port and/or service from traversing the firewall boundary for a user-specified period of time. The communication between the RealSecure Network Sensor and the FireWall-1 management server is done using SAMP, Check Point's suspicious activity monitoring protocol, which is part of the OPSEC framework. This communication can also be authenticated, if desired.

Option to record everything for "forensic" investigation? Where is this data stored? How is it secured from tampering?
Yes. RealSecure Network Sensors offer the ability to record the raw, binary content of an entire network session. This data is stored in a log file in a secured directory and can be replayed through the Workgroup Manager interface.

Reporting from engine to console - range of action/alert options (detail these)
Send the event to the RealSecure Console.
Terminate the attack automatically.
Terminate the user session.
Disable the user account.
Reconfigure a CheckPoint Firewall-1 to reject traffic from the attacking source address.
Send a secure real-time alarm to the Lucent Managed Firewall Security Management Server (SMS)
Send an alarm to the RealSecure Console indicating that the event occurred.
Send an SNMP trap to an off-the-shelf management platform.
Log the event, including date, time, source, destination, description, and data associated with the event.
View the raw content of the session in real-time (or record for later playback).
E-mail a notification to the administrator.
Execute a user-specified program.

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
The RealSecure Sensors do not need to be connected to the console. Events are stored locally in a database and log files, stored in a secured directory, and are synchronized with the console database on demand.

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
Alerts are reported to the console in real time without the need for any third party software. The events are displayed in different views based on priority, type of event, or source or destination addresses providing the ability to extract individual events.

Does the software offer advice on preventative action to ensure the attack does not happen again?
The RealSecure Help describes each signature, tells why it is important, and gives preventative measures. RealSecure has context-sensitive help so information about a particular signature may be easily obtained when it shows up in an event window.

Integration with other scanning/IDS products?
RealSecure is part of the SAFEsuite family of products. Results from RealSecure sensors are gathered into the SAFEsuite Decisions database where they are correlated with vulnerability assessment data from Internet Scanner, Database Scanner, and System Scanner, providing an overall view of the security of a network.

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
RealSecure Sensor logs are a set length and are archived to a database at the console.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
RealSecure provides 17 different reports with 5 graphical summaries. Reports are filtered by time and date and may be sorted by the destination or source IP or type or priority of events. There are also reports for Login/logout history, admin activity, Log monitoring, user activity, and suspect connections.

Report management – can they be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?
RealSecure reports cannot at this time be scheduled for automatic report production.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
RealSecure consolidates the event data from all of the monitored sensors into a database at the console. RealSecure data may be gathered into a SAFEsuite Decisions database for further consolidation and correlation with vulnerability assessment data.

Define custom reports?
Custom reports may be created using Crystal Reports 7.0.

How is it licensed? How is the license enforced?
RealSecure is licensed on a per-sensor basis. The license is enforced through the use of a license key.

End user pricing information
(Not Supplied)

Ongoing cost of maintenance/updates
(Not Supplied)

Network ICE BlackICE Sentry

Brief product description
BlackICE Sentry is an intrusion detection system developed to detect malicious activity on high speed networks.

Architecture
BlackICE Sentry is a network based IDS solution. It has the ability to work as a stand-alone system or work in a "manager" to "agent" relationship.

At what layer of the protocol stack is the product working?
The device driver used for BlackICE can be described as a Microsoft intermediary driver. BlackICE Sentry intercepts packets directly from the NDIS drivers.

Documentation
All documentation for the BlackICE Sentry can be found on-line at www.networkice.com. Supplemental information regarding security can also be searched on the www.advice.networkice.com site.

What are the minimum/recommended console OS and hardware requirements?
Hardware:
200 MHz Pentium class processor
64 MB RAM
3 MB of Disk Space
Operating System:
Windows NT Workstation 4.0
Windows NT Server 4.0
Windows NT 2000
Database:
Microsoft SQL Server 6.5 or higher
Microsoft SQL Workstation 6.5

Is a dedicated machine required/recommended?
It is recommended, but not required. It depends on the number of total "agents" or "Sentry" machines reporting into it.

Will it work on Windows 2000?
Yes.

What are the minimum/recommended agent OS and hardware requirements?
Hardware:
400 MHz Pentium class processor
3Com 3C905 Ethernet card
Operating System:
Microsoft NT Server 4.0 or Workstation 4.0

Is a dedicated machine required/recommended?
Yes.

Will it work on Windows 2000?
No.

What components are installed on a detector
BlackICE Driver and NT Service

Which network types are supported
10/100 Ethernet, and Gigabit Ethernet (not shipping, but announced)

Any specific recommendations for monitoring Gigabit networks with your product?
BlackICE Sentry can be used with a TopLayer switch to provide Gigabit IDS. BlackICE Gigabit Sentry is an appliance that will be able to hook directly into a switch to perform Gigabit IDS.

Which OS platforms are actively monitored?
BlackICE Sentry monitors protocols verses OS platforms.

Can sensors/detectors be deployed and configured initially from a central console?
Yes. Utilizing the ICEcap Manager, a BlackICE Sentry build can be deployed over the network to a pre-configured Windows machine.

Once deployed and configured, can sensors/detectors be managed from a central console?
Yes.

Authentication between console and engines – Is it available?
Yes.

What algorithm/key lengths?
Blowfish for encryption using 56-bit key and Diffie-Hellman for key exchange.

Secure logon for policy management?
Yes, username and password.

How are policies distributed to engines?
By using ICEcap, BlackICE Sentry updates can be made remotely.

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
N/A

How many attack signatures?
500 +

Can the administrator define custom attack signatures?
No

How are new attack signatures obtained and deployed?
New attacks are updated with frequent software upgrades.

Frequency of signature updates? Provide dates of all updates in the last year.
There has been one major signature upgrade every quarter this year. Dates of the 2000 updates are March 2000, September 2000, November 2000, and one for December 2000 (coming out of Beta).

What infrastructure do you have behind the signature update process
Internal engineers provide the update process for attack signatures.

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
A file can be downloaded to the ICEcap Manager and pushed out to multiple BlackICE Sentries.

Can signature updates be scheduled and fully automated?
No.

What network protocols are analysed?
HTTP, FTP, IMAP4, POP3, BOOTP/DHCP, ARP, AOL IM, Finger, Gopher, ICMP, ICQ, Identd, MIME, MS RPC, NNTP, PCAnywhere, RealAudio, Rsh/rlogin/rexec, SMB, SMTP, SNMP, S/NTP, SOCKS, MS SQL , Telnet, TFTP, Numerous Sun RPC protocols: portmapper, nfs, mount, lockd, statd, cmsd, bootparam, admin, sadmin, automount, ToolTalk, NIS/YP, and a couple of rarer ones

What application-level protocols are analysed?
See list above.

Can the product perform protocol decodes?
No (the detection engine uses protocol decodes to detect attacks, but session decodes are not made available to the user)

Can the product perform session recording on suspect sessions?
Yes.

Block/tear down session?
No.

Ability to monitor user-defined connections
N/A

Monitor changes in critical system files?
N/A

Monitor changes in user-defined files?
N/A

Monitor changes in Registry?
N/A

Monitor unauthorised access to files?
N/A

Monitor administrator activity (creation of new users, etc)?
N/A

Monitor excessive failed logins?
Yes

List any other resources/locations that are monitored.
N/A

Track successful logins, monitoring subsequent file activity, etc?
N/A

Detect network-level packet based attacks?
Yes.

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
Yes.

Detect and report on nmap OS fingerprinting?
Yes.

Perform packet reassembly?
Yes.

Resistance to known IDS evasion techniques?
Yes.

Reconfigure firewall? If so, which firewall(s) and how?
No.

Option to record everything for “forensic” investigation? Where is this data stored? How is it secured from tampering?
Yes. Sniffer trace files are stored on the BlackICE Sentry for forensic use. It uses the default Windows NT security to provide authentication and data integrity.

Reporting from engine to console - range of action/alert options (detail these)
The ICEcap manager is capable of sending e-mail, a visual alert via http, and snmp traps.

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
If there is an interruption between the console and detector, the “events” are stored locally on the sensor until they can be forwarded to the manager.

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
Yes. Alerts are sent to the console in real time. Multiple filtering reports can be used to sort through the event data.

Does the software offer advice on preventative action to ensure the attack does not happen again?
Network ICE provides AdvICE web pages as support documentation to answer and aid in the prevention of many know attacks. Also, BlackICE Agents will block attacks in real-time or be manually upgraded to block certain attacks as they are detected.

Integration with other scanning/IDS products?
None at this time.

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
The log file is kept on a SQL database. Any NT rotation or archiving tool can be used to back up the database and sort through the data.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
There is over 10 different management reporting "views". Technicians and management can select through different levels of reporting for granular details regarding attacks, IP information, attack type, and attack victim.

Report management – can they be scheduled for automatic production?
Yes.

Can they be e-mailed to administrators or published straight to a Web site?
No.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
Each detector (Sentry) has the capability to display alert information. The ICEcap manager can display alert information as well as generate custom reporting.

Define custom reports?
Users can define different parameters in creating reports with ICEcap. Users are not restricted by a one template report.

How is it licensed?
Per device.

How is the license enforced?
End user license agreement.

End user pricing information
US. Pricing - BlackICE Sentry with ICEcap Manager: $7995.00
GBP Pricing - BlackICE Sentry with ICEcap Manager: £5,586.00

Ongoing cost of maintenance/updates
Maintenance: First year is included, 16% of MSRP thereafter.

NSW Dragon Sensor

Brief product description
Dragon IDS is a system for your network to detect Intrusion on your network. It does this by monitoring network traffic and key files upon servers. There are three main parts, Dragon Sensor (NID), Dragon Squire (HID) and Dragon Server (management console).

Architecture
Dragon is made up of Host and network sensors which all report to a central management machine, which used to configure all sensors. The server is also where are the logged information is stored and can also send alerts either as email, snmp or syslog.

At what layer of the protocol stack is the product working?
The NID works at the Network layer, so that it can analyse all network traffic

Documentation
There is an Installation guide and documentation all available the Web plus PDF versions of the online documentation are included on the CD. Hard copies are available upon request.

What are the minimum/recommended console OS and hardware requirements?
The minimum specs of the Server depends on the speed of the network and the number of sensors it has to manage but should be at least a P3 500 with 128mb ram and 10 gb hard disk and a dual P3 700 and 256 mb of ram and 40 gb hard-disk for a set up of 30 sensors and 100 squires. The OS has to be either Linux, OpenBSD, FreeBSD, Solaris (sparc or intel) and HP-UX.

Is a dedicated machine required/recommended?
Recommended

Will it work on Windows 2000?
No but you can manage it remotely using a web browser on a w2k box

What are the minimum/recommended agent OS and hardware requirements? Is a dedicated machine required/recommended?
As above but the sensor (NID) depends on the link it's monitoring from a P2 for a T1/10 mbs to a P3 700 for a 100 mbs connection. Squire is designed to run with minimum impact so there isn't a minimum spec.

Will it work on Windows 2000?
There should be a version of Squire (HID) for NT/2000, hopefully available by the end of 2000.

What components are installed on a detector
On the detectors there are two daemons running, one that does the work and one that communicates to the Server.

Which network types are supported
Ethernet and Gigabit Ethernet are currently supported and the Token Ring and FDDI support will be available shortly (currently in beta testing).

Any specific recommendations for monitoring Gigabit networks with your product?
For Monitoring Gigabit Ethernet the machines have to be high spec and you will need multiple sensors. It is also advisable not to overload the sensor with too many signatures to enable it to keep up.

Which OS platforms are actively monitored?
The HID is designed to protect the OS it's installed, currently on the UNIX's mentioned above. The NID can detect Windows based attacks and Unix based attacks.

Can sensors/detectors be deployed and configured initially from a central console?
No

Once deployed and configured, can sensors/detectors be managed from a central console?
Yes

Authentication between console and engines – Is it available? What algorithm/key lengths?
Yes, a Blowfish encrypted link that authenticates with a shared secret.

Secure logon for policy management?
The Interface for Management is web based, and it recommended by us that this is secured with SSL so that you have to authenticate to the server to remote administrate the Central Server.

How are policies distributed to engines?
The Policies are 'Pushed' to all the remote sensors from the Central Server over the blowfish encrypted link.

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
The central console knows the configuration of each sensor but any changes to the policy must by done manually on the server and re 'pushed', the human step therefore ensures that the policy change can be properly reviewed.

How many attack signatures?
Currently 1101 NID signatures and squire has about 550 signatures.

Can the administrator define custom attack signatures?
Yes

How are new attack signatures obtained and deployed?
They can downloaded from the Internet or can be automatically downloaded to the Server. They are deployed by the user on the Server and sent out to the sensors.

Frequency of signature updates? Provide dates of all updates in the last year.
Signatures are updated as and when new attacks are published, this is a continuous process and is therefore difficult to give exact dates of when these updates occur.

What infrastructure do you have behind the signature update process
The signatures are written by a team of NSW in house engineers also because of the open nature of the signature, many customer write their own signatures and send them back to the developers where they can be included in the signature libraries.

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
All the signature libraries can be downloaded to the central server where they can be easily distributed to the sensors connected.

Can signature updates be scheduled and fully automated?
Yes, the signatures can be scheduled to download to the Central server but it will not automatically send them to the sensors. This is so they can be checked first before sending them out.

What network protocols are analysed?
IP, TCP, UDP, RIP,RPC and Netbios

What application-level protocols are analysed?
All IP protocols such as TELNET, FTP, HTTP,etc.

Can the product perform protocol decodes?
No

Can the product perform session recording on suspect sessions?
Yes, follows on packets are logged depending on the signature, so that the session is logged and can viewed later.

Block/tear down session?
Dragon can respond to certain events or IPs with reset packets therefore terminating the session.

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
Yes dragon can be configured to log traffic on a certain IP and port. Plus custom signatures can be written to fit the needs of your network.

Monitor changes in critical system files?
Dragon Squire will checksum and monitor changes in key system files such as /etc/passwd and /var/log/messages.

Monitor changes in user-defined files?
Yes, Squire can monitor any file you define.

Monitor changes in Registry?
As there is no Registry under UNIX then no. However hopefully when the NT/2000 version is available this will monitor registry changes.

Monitor unauthorised access to files?
Under Unix you will be unable to access file you don't have permission to without escalating your privileges and Dragon would notice this.

Monitor administrator activity (creation of new users, etc)?
Yes as this would change key files such as /etc/passwd.

Monitor excessive failed logins?
Yes as failed logins get reported in /var/log/messages and there are signatures for this file.

List any other resources/locations that are monitored.
Cisco messages can be report to a Syslog server and with Squire it can monitor messages from your router and PIX firewall. Also it can look in the logs of Apache web servers, SQUID, SSH, ipfilter, ipchains and IPFW etc.

Track successful logins, monitoring subsequent file activity, etc?
Doesn't normally monitor successful logins but it could be made to with a custom signature.

Detect network-level packet based attacks?
Yes

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
Yes

Detect and report on nmap OS fingerprinting?
Nmap is a port scanner and Dragon detects port scanning. It does not however directly detect nmap. Nmap used to have unique flaws in it artificial packets which could be used to ID its use, but Dragon basically picks up on all forms of port scanning and sweeping whether it is slow, fragmented, randomised or spoofed with multiple decoy scans. As for OS fingerprinting, this usually involves sending TCP flags with odd combinations or sending traffic to port zero. Dragon picks up on this. Subtle attempts to id an OS based on frag reconstruction time-out, maintaining the don't-frag bit set, or padding data in ICMP unreachable pings are not supported though.

Perform packet reassembly? Resistance to known IDS evasion techniques?
Both

Reconfigure firewall? If so, which firewall(s) and how?
No

Option to record everything for "forensic" investigation? Where is this data stored? How is it secured from tampering?
Yes, it is stored on the central server but could be exported to a SQL database for long term storage. There is no anti-tempering as such but a third party program such as Tripwire could be used on the data.

Reporting from engine to console - range of action/alert options (detail these)
All events logged are forwarded to the Central Server where they can be analysed centrally. From here the alerting can be done for any events you want to be alerted on. Alerts can be SNMP,SMTP or SYSLOG.

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
Dragon sensor stores all information locally and can lag the forwarding of the events if the network is overloaded. These are stored in databases just like on the Server and can even be accessed remotely if dragon fire is installed on the sensor.

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
All events are forwarded to the Server in real time and using the Dragon fire interface it's easy to filter and analyse these events.

Does the software offer advice on preventative action to ensure the attack does not happen again?
The events all have description of what they mean and will give the relevant Bugtraq or CVE web link (if known) so you can find more about the problem and if necessary guide you in fixing the problem.

Integration with other scanning/IDS products?
Not yet, there are plans for the dragon server to receive SNMP alerts from other IDS.

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
This can be done with a variety of scripts available on the Customer support site.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
Better reporting including 2d/3d reporting for management and non-technical staff is to be included in the Server in the near future.

Report management – can they be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?
No

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
On the server you able to choose a particular sensor and view the events logged for it and produce reports for each sensor. You all also can produce a report based on all sensor to give a complete picture, the limitation of this is that the report is usually very big and would take longer to analyse.

Define custom reports?
Dragon can present data in different ways using the different analysis tools and summarising tools, in the future there will be a 2D/3D tool that will be able to customise and present the data in a easy to read and non-technical way.

How is it licensed? How is the license enforced?
The license is per server and sensor, a key file is needed for every sensor and server.

End user pricing information
PENS Dragon Sensor:
1 - 100 units : $6,500.00 (£4,545.45)
100 + units : $POA (£POA)

PENS Dragon Server
1 - 100 units : $8,500.00 (£5,944.06)
100 + units : $POA (£POA)

Ongoing cost of maintenance/updates
The First year of maintenance is included in the initial price. Additional maintenance contracts are available at 20% per annum, of the then current list price.

Tripwire

Brief product description
Tripwire is a file integrity product, the software runs on a individual system, these are usually servers or systems where file integrity assurance is critical. Tripwire works by digitally signing critical files and attributes (user selectable via a policy file), with the first occurrence being called the baseline. Subsequently when Tripwire is run a report is generated that outlines "differences" between the current state of files/attributes and the previous state.

Architecture
Tripwire as run on a individual system is a command line capability, to provide better management of a large number of systems installed with Tripwire a capability called HQManager is available. HQManager is a graphical interface that talks to Tripwire enabled systems via a "connector", this provides a encrypted link for reporting / managing Tripwire on target systems. HQManager is currently a WindowsNT facility, but will be available as a Unix capability Q1 2001. HQManager interacts with up to 250 Tripwire enabled systems

At what layer of the protocol stack is the product working?
Not Applicable, i.e. independent

Documentation
Full manual set plus on-line help re: commands. HQManager also has integrated Help.

What are the minimum/recommended console OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
No requirements as it runs on target system.

What are the minimum/recommended agent OS and hardware requirements? Is a dedicated machine required/recommended? Will it work on Windows 2000?
Tripwire is Independent of OS

What components are installed on a detector
Tripwire is an application that is independent of any other service. It is scheduled via AT or CRON and does not affect any part of the OS.

Which network types are supported
Not relevant

Any specific recommendations for monitoring Gigabit networks with your product?
Not relevant

Which OS platforms are actively monitored?
Solaris, Windows NT, HP-UX, Linux, AIX, W2000 (Professional now, Server Q1 2001), SGI and Compaq

Can sensors/detectors be deployed and configured initially from a central console?
No

Once deployed and configured, can sensors/detectors be managed from a central console?
Yes, by using HQManager

Authentication between console and engines – Is it available? What algorithm/key lengths?
Yes, Each Tripwire has a local Pass phrase, plus there is a site Pass phrase.

Secure logon for policy management?
Physical access is required to either Tripwire system or HQManager. Security is handled by local system e.g. Unix needs Root, NT required Admin privileges.

How are policies distributed to engines?
HQManager sends configuration information via encrypted link

How are policy changes handled? Will the central console detect which agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually?
Manual

How many attack signatures?
Not Applicable

Can the administrator define custom attack signatures?
Not Applicable

How are new attack signatures obtained and deployed?
Not Applicable

Frequency of signature updates? Provide dates of all updates in the last year.
Not Applicable

What infrastructure do you have behind the signature update process (i.e. dedicated team of engineers? How many? Does it have a name?)
Not Applicable

Can one signature update file be downloaded to the local network and used to update all IDS engines from a central location, or is it necessary to initiate a live connection to the Internet download server for each engine?
Not Applicable

Can signature updates be scheduled and fully automated?
Not Applicable

What network protocols are analysed?
Not Applicable

What application-level protocols are analysed?
Not Applicable

Can the product perform protocol decodes?
Not Applicable

Can the product perform session recording on suspect sessions?
Not Applicable

Block/tear down session?
Not Applicable

Ability to monitor user-defined connections (i.e. report on an FTP connection to a specific server?)
Not Applicable

Monitor changes in critical system files?
Tripwire monitors all files, a "Policy File" can be tuned to include / exclude files. It also signs files with a variety of signatures to detect tampering.

Monitor changes in user-defined files?
As above.

Monitor changes in Registry?
Tripwire monitors Registry for changes / tampering

Monitor unauthorised access to files?
Tripwire monitors ALL access to files, it is up to administrator to identify unauthorised

Monitor administrator activity (creation of new users, etc)?
Not Applicable

Monitor excessive failed logins?
Not Applicable

List any other resources/locations that are monitored.
N/A

Track successful logins, monitoring subsequent file activity, etc?
Not Applicable

Detect network-level packet based attacks?
Not Applicable

Detect all types of port scans (full connect, SYN stealth, FIN stealth, UDP)?
Not Applicable

Detect and report on nmap OS fingerprinting?
Not Applicable

Perform packet reassembly? Resistance to known IDS evasion techniques?
Not Applicable

Reconfigure firewall? If so, which firewall(s) and how?
Not Applicable

Option to record everything for "forensic" investigation? Where is this data stored? How is it secured from tampering?
Tripwire records the status of system by snapshot system at regular intervals, the signatures of files / registry are stored in an encrypted form to protect them from tampering.

Reporting from engine to console - range of action/alert options (detail these)
E-Mail, SNMP to be added Q1 20001

What provision is made for temporary communications interruption between detector and console? Where are alerts stored? Is the repository secure?
Not Applicable

Can alerts be reported to the central console in real time without the use of third party software? How easy is it to filter and extract individual events?
Not Applicable

Does the software offer advice on preventative action to ensure the attack does not happen again?
Not Applicable

Integration with other scanning/IDS products?
Other IDS products – such as CyberSafe Centrax – can call Tripwire to perform integrity scans in response to alerts

Log file maintenance – automatic rotation, archiving, reporting from archived logs, etc.
Basically the only output is the reports, normal archiving is applicable

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
Various reports can be scheduled for different times e.g. a Full check can be done daily, but critical database file can be done hourly. Various policy files can be created

Report management – can they be scheduled for automatic production? Can they be e-mailed to administrators or published straight to a Web site?
Tripwire operates by scheduling a update, the exact time is determined by user (AT or Cron). The administrator is notified by E-mail if attention is required

What are the limitations and restrictions on enterprise-wide alerting and reporting? Can reports consolidate output from every 1) server, 2) detector
Reports can be consolidated across multiple

Define custom reports?
Reports are generated as a result of the Policy File, thus to get specific information into a report the PF is tuned.

How is it licensed? How is the license enforced?
By platform, currently no enforcement

End user pricing information
Pricing is on application as it depends on number of systems, site licenses, prmotions, etc..

Ongoing cost of maintenance/updates
Support contract is normally in the order of 15-20% depending on configuration

VA Questionnaires

Axent NetRecon

Brief product description
NetRecon is a network vulnerability assessment tool that discovers, analyses and reports holes in network security.

Architecture
NetRecon has three main components, a graphical user interface (GUI), a scan engine, and scan modules

Documentation
NetRecon includes the following documentation: Installation and Getting Started Manual (hard and soft copy), Release Notes (hard and soft copy), On-line Help File (F1 Help), Vulnerability List (soft copy), Vulnerability and solution (fix) recommendations in each report (soft copy), Supplemental information online at www.axent.com/netrecon such as FAQs, Security Update vulnerability descriptions online at "www.axent.com/swat --> Security Updates --> NetRecon" or , http://www2.axent.com/swat/index.cfm?Doc=Product_NR&Section=SecurityUpdates
Release Notes for each security update (soft copy)

What are the minimum/recommended console OS and hardware requirements?
The minimum hardware system requirements are:
Windows NT 4.0 with Service Pack 3 or greater
Pentium 200 MHz CPU
64 MB RAM (128 MB recommended)
40 MB hard disk space
Note: NetRecon will not install or run on Windows 95/98.

On what platforms is this certified to run? Will it work on Windows 2000?
Runs on Windows NT 4.0 and Windows 2000.

At what layer of the protocol stack is the product working? Is a raw packet driver installed?
NetRecon can scan any systems accessible from any protocol found in the Windows NT Network Neighbourhood. A raw packet driver is also installed for both NT and Windows 2000 for fast port scans.

Can multiple scanning engines be deployed and configured from a central console, i.e. define a single scanning policy centrally and deploy this to all scanners automatically?
No.

Authentication between console and engines – Is it available? What algorithm/key lengths?
Not applicable. NetRecon is a stand-alone application with the console and engine integrated into a single product. NetRecon does not contain any strong encryption.

Secure logon for policy management?
Yes. The user is prompted for a password before using the product.

In addition to the login password, NetRecon uses a series of different approaches to protect users from abuse by hackers or crackers. These protections include, but are not limited to the following:
Scan footprints remain on systems scanned by NetRecon
Individual copy of NetRecon tied to registration license
License Key sent to email account
Time limit of 30-days for Evaluation license
Evaluation license can only run scans under 15 minutes (most Medium and Heavy scan objectives require more than time)
NetRecon scans are designed NOT to crash your system or the systems scanned

How are policies distributed to scanners?
Editing certain text files can modify policies.

How are policy changes handled? Will the central console detect which scanning agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually? Can it be done once from a central location or do all scanners have to be updated individually?
Not applicable. Scanning agents are not used.

How many attack signatures?
NetRecon 3.0 with SU9 has 445 vulnerability signatures.

Which platforms (i.e. NT, Windows 2000, Linux) and network resources (i.e. firewalls, routers, printers, Web/mail/FTP servers) are covered by the attack signatures?
NetRecon scans most OS, including Windows 95/98/NT/2000, Unix (HP-UX, Solaris, AIX, IRIX), NetWare, (Bindery and NDS) and Linux. It also scans network devices such as firewalls, routers, hubs, printers, Web servers, mail servers and FTP servers.

Can it perform accurate OS detection?
Yes. It can also detect many network devices using their login banners and other data for unique identification.

What types of port scans can be performed?
NetRecon performs both half-open and full-connect scans. Half-open scans discover TCP and UDP services. This is also referred to as a fast-port scan or a raw port scan. Full-connect scans discover both privileged and non-privileged TCP services.

Can the administrator define custom attack signatures?
No. With some skill and an executable, three .INF files can be edited with a text editor to change scan objectives and add new signatures.

Can it perform true DoS attacks?
NetRecon detects several DoS attacks. It does not actually perform DoS attacks. These are true checks, not just banner grabbing.

How are new attack signatures obtained and deployed?
New attack signatures are distributed via monthly security updates. Security Updates must be manually downloaded from the AXENT SWAT site, www.axent.com/swat, then executed.

Frequency of updates? Provide dates of all updates in the last year.
New signatures are made available monthly.

NetRecon 3.0 SU9:	9 Oct 2000
NetRecon 3.0 SU8:	14 Aug 2000
NetRecon 3.0 SU7:	9 Jun 2000
NetRecon 3.0 SU6:	9 June 2000
NetRecon 3.0 SU5:	8 May 2000
NetRecon 3.0 SU4:	3 Mar 2000
NetRecon 3.0 SU3:	17 Feb 2000
NetRecon 3.0 SU2:	10 Feb 2000
NetRecon 3.0 SU1:	28 Jan 2000

Can one signature update file be downloaded to the local network and used to update all scanners from a central location, or is it necessary to initiate a live connection to the Internet download server for each scanner?
Each security update, once downloaded, must be run on each NetRecon system to apply the updates. A live connection to the Internet download server is NOT required for each scanner.

Can signature updates be scheduled and fully automated?
No. NetRecon users are notified via email when new security updates are made available. They must request to be notified at time of download and/or product registration.
With the acquisition of AXENT by Symantec, use of their Live Update technology would be a logical extension to NetRecon.

Are scan results available in real time during scan?
Yes

Are scan results (even as a summary) available on-screen following a scan without having to run a separate report?
Yes. Vulnerability records are displayed as the data is discovered in real-time. The data can be filtered and analysed as well, even as the scan is in progress.

Advice on preventative/corrective action when vulnerabilities found?
Yes.

Capability to auto-fix certain vulnerabilities? If so, is there an "interactive mode" and/or an undo facility?
No

Automatic alerting if severe vulnerabilities are found during a scan?
No

Integration with other scanning/IDS products?
Yes – Axent ESM

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
Crystal Reports are provided with NetRecon. These report templates generate standard reports targeted for varying audience levels. The user has the ability to select between three report formats: Executive Report, Detail Report by System, and Detail Report by Vulnerability.

Report filters are also provided. Reports can easily be filtered to contain one or more vulnerabilities, one or more systems, and/or one or more risk levels, etc. If customers would like to create custom reports, it will require a copy of Crystal Reports.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Is it possible to combine reports from several scanners?
The NetRecon Limited license can scan up to a Class C network. The Unlimited license can scan any size network. It is recommended that no more than 3 class C networks are scanned at a time. Scans can be paused and resumed, however individual scan reports cannot be combined from several scanners.

Report management – archiving? Can historical scans be consolidated/compared for trend analysis/comparisons
Yes. Scans can be archived for later recall. NetRecon extracts the scan data from the MS Access database and stores it in a NetRecon Data File (*.NRD). Using AXENT's ESM product, multiple NetRecon scans can be compared with the trend analysis functionality.

Can scans/reports be scheduled for automatic production? Can the results be e-mailed to administrators or published straight to a Web site?
Yes. NetRecon has a GUI scheduler for scans. Scan results can be exported into HTML for publishing to the web. This feature is not automated. No mechanism exists to automatically email scan results.

Does the product incorporate IDS evasion techniques to test IDS effectiveness? If so, describe in detail how these are implemented.
No

How is it licensed? How is the license enforced?
Evaluation License: You may scan an unlimited number of network resources from one system. Each scan is limited to ten minutes unless otherwise authorized by Licensor, and the evaluation license expires in fifteen days unless otherwise authorized by Licensor.
Limited License: You may scan Your small network (up to 254 unique network resources) from one system.
Unlimited License: You may scan Your large network (an unlimited number of network resources) from one system.
Consultant License: You may scan multiple networks belonging to Your customers as long as permission is obtained before such scan, but such scan shall last for no longer than seven days per customer and Product must be removed thereafter.
Not For Resell (NFR) License: You may scan multiple networks belonging to Your customers so long as permission is obtained before such scan, but such scan shall last for no longer than fifteen minutes per customer and Product must be removed thereafter.
Single Engagement (SE) License: You may scan a network belonging to a single customer for no longer than thirty (30) days. This license is good for use on one (1) of Your customers only and You must obtain permission before such scan. Such scan may only be for delivering assessment services.

NetRecon is licensed by the size of the network as defined by the number of network resources (or nodes). A network resource is defined as individual IP addresses, NetWare servers, NetBIOS systems, routers, and hubs. The license permits execution of NetRecon on a single NT workstation/server to scan a number of network resources (nodes).

Licenses are activated when the correct serial number matches the generated license key. Limited licenses are enforced through the legal agreement and can be audited if abuse is suspected.

End user pricing information
NetRecon is licensed and priced by the size of the network as defined by the number of network resources (or nodes). A network resource is defined as individual IP addresses, NetWare servers, NetBIOS systems, routers, and hubs. The license permits execution of NetRecon on a single NT workstation/server to scan a number of network resources (nodes).

Evaluation	$Free
Limited	$1,995
Unlimited	$9,995
Consultant (12 Month)	$17,995
Single Engagement	$1,495
NFR (12 Month)	$Free

Ongoing cost of maintenance/updates
One year of Standard maintenance is 15% of product cost. One year of Priority maintenance is 22.5% of product cost. Maintenance is not required.

BindView HackerShield

Brief product description
HackerShield is a vulnerability scanner (also called a network scanner or security scanner). HackerShield is a Windows NT application that examines devices on IP networks for security holes that hackers could use to break-in. It examines devices of all types (servers, workstations, routers, hubs, printers, etc.). As long as the device has an IP address (and therefore is part of a TCP/IP based network), then HackerShield will examine it for security holes.

Architecture
HackerShield is a console based IP scanner running from a central location. HackerShield consists of 6 components: the console, the database, and the four HackerShield services (all installed on the host where the console is installed.)

Documentation
A getting started guide is provided in hard copy. The admin/reference guide plus tutorial are electronic and included with the product. Additional information is provided on Bindview's website.

What are the minimum/recommended console OS and hardware requirements?
200 MHz Pentium II or greater
128 MB RAM
40 MB Free Disk Space
TCP/IP network with an Ethernet card on the HackerShield computer
Access to a CD-ROM drive (for installation from CD)
Windows NT 4.0
Service Pack 4 for NT 4.0 (included on CD) or higher
Microsoft Internet Explorer 4.01 (included on CD)
Administrator privileges for the computer on which HackerShield will be installed
An Internet e-mail account (required for RapidFire Updates)

On what platforms is this certified to run? Will it work on Windows 2000?
HackerShield runs under Microsoft Windows NT v4.0 with Service Pack 4 or better. Internet Explorer v4.01 or greater is also required but does not have to be the default browser. Version 3 will support installation on Windows 2000 (ship date 1q2001)

At what layer of the protocol stack is the product working?
Network

Is a raw packet driver installed?
Yes

Can multiple scanning engines be deployed and configured from a central console, i.e. define a single scanning policy centrally and deploy this to all scanners automatically?
HackerShield is a centrally based IP scanner running from a single location. The current shipping version does not support multiple scanning engines. A scalar architecture is planned for the version 4 release.

Authentication between console and engines – Is it available? What algorithm/key lengths?
n/a

Secure logon for policy management?
No

How are policies distributed to scanners?
n/a

How are policy changes handled? Will the central console detect which scanning agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually? Can it be done once from a central location or do all scanners have to be updated individually?
N/a

How many attack signatures?
HackerShield currently detects over 700 security vulnerabilities, covered by our 300+ internal security probes.

Which platforms (i.e. NT, Windows 2000, Linux) and network resources (i.e. firewalls, routers, printers, Web/mail/FTP servers) are covered by the attack signatures?
Once HackerShield is installed it will scan any machine on the network for security holes regardless of platform (i.e. UNIX, Windows NT/2000, Windows 95/98 and other platforms). As long as a device has an IP address, HackerShield will scan it for security holes.

Can it perform accurate OS detection?
Yes

What types of port scans can be performed?
(Unanswered)

Can the administrator define custom attack signatures?
Not currently supported. Version 4 will provide a method of user defined attack signatures.

Can it perform true DoS attacks
If a DoS vulnerability can be accurately detected by inference techniques (including banner analysis and other data gathering techniques), HackerShield will do so in order to minimize impact on end systems. However, there are cases in which the only way to accurately determine risk is to perform a true DoS attack on the host. HackerShield categorizes such security checks as "Live Fire DoS" checks and provides the user with the ability to select or deselect this group of checks. By default, the Live Fire DoS checks are not enabled.

How are new attack signatures obtained and deployed?
RapidFire Updates are HackerShield's protection against the latest hacker threats. BindView's security research team (Razor) sends out regular updates that include the latest security threats and how to close them. RapidFire Updates can be sent via secure email and automatically integrated into the HackerShield database of security checks. RapidFire Updates can also be downloaded from the BindView website.

Frequency of updates? Provide dates of all updates in the last year.
Updates are sent as dictated by events in the security industry. On the average, updates are sent monthly.
(No dates were provided)

Can one signature update file be downloaded to the local network and used to update all scanners from a central location, or is it necessary to initiate a live connection to the Internet download server for each scanner?
No

Can signature updates be scheduled and fully automated?
Yes

Are scan results available in real time during scan?
Scan progress is available during real time, but the results are provided when the scan is completed.

Are scan results (even as a summary) available on-screen following a scan without having to run a separate report?
Yes

Advice on preventative/corrective action when vulnerabilities found?
Yes

Capability to auto-fix certain vulnerabilities? If so, is there an "interactive mode" and/or an undo facility?
Yes

Automatic alerting if severe vulnerabilities are found during a scan?
Yes, via email or SNMP

Integration with other scanning/IDS products?
Not currently supported

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
HackerShield provides a GUI environment with HTML based reports. No scripting is needed to generate different reports for management or administrators. Filtering can be adjusted on the fly via the GUI interface as well as the level of detail.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Is it possible to combine reports from several scanners?
No limitation on enterprise wide reporting other than license constraints. Version 3 supports the ability to combine reports.

Report management – archiving? Can historical scans be consolidated/compared for trend analysis/comparisons
HackerShield provides both the ability to archive historical scans and the ability to use baseline comparisons for the analysis of such historical data.

Can scans/reports be scheduled for automatic production? Can the results be e-mailed to administrators or published straight to a Web site?
HackerShield provides a built in scheduler to allow scans to be run unattended. Reports from those scans can be exported into numerous formats including ASCII, .mdb, .doc, and html.

Does the product incorporate IDS evasion techniques to test IDS effectiveness? If so, describe in detail how these are implemented.
No

How is it licensed? How is the license enforced?
HackerShield is licensed by the number of IP addresses that can be scanned for security holes. For example, a 200 IP address license will allow you to scan up to 200 IP devices (servers, workstations, routers, etc.) for security holes. Licensing is enforced at the scanning console.

End user pricing

Console + 1 IP address	$695.00
100 IP addresses	$1,995.00
500 IP addresses	$9,975.00
1,000 IP addresses	$19,950.00
Class C subnet	$3,995.00
Class B subnet	$32,000.00

Ongoing cost of maintenance/updates
Maintenance costs are 20% of purchase price

Console + 1 IP address	$139.00
100 IP addresses	$399.00
500 IP addresses	$1,995.00
1,000 IP addresses	$3,990.00
Class C subnet	$799.00
Class B subnet	$6,400.00

Network Associates CyberCop Scanner

Brief product description
CyberCop Scanner identifies security holes to prevent intruders from accessing data. It unveils weaknesses, validates policies and enforces corporate security strategies. It tests for vulnerabilities in Windows, Unix, and Novell machines, and performs perimeter audits of firewalls and routers.

Architecture – brief description
Scanner is a host-based solution for scanning the clients on a network. Management and reporting are configured via a Win32 based Security Management Interface (SMI) console.

Documentation
SMI Getting Started Guide (SMI10NGS.pdf) and CyberCop Scanner 5.5 Getting Started Guild (CSC55NGS.pdf) are available with the product or by contacting Network Associates Inc.

What are the minimum/recommended console OS and hardware requirements?
Windows NT 4.0 with Service Pack 4.0
Internet Explorer 4.0 SP1
266 MHz Pentium II processor
128 MB of RAM
200 MB of free disk space

On what platforms is this certified to run? Will it work on Windows 2000?
Windows NT 4.0, Windows 2000

At what layer of the protocol stack is the product working? Is a raw packet driver installed?
CyberCop Scanner runs at the application layer while its raw packet driver (ntbpf) operates at the network layer. The modules within the product scan for vulnerabilities in the application, presentation, session, transport and network layers.

Can multiple scanning engines be deployed and configured from a central console, i.e. define a single scanning policy centrally and deploy this to all scanners automatically?
The current version does not support distributed scanning agents.

Authentication between console and engines – Is it available? What algorithm/key lengths?
Authentication will be available with the distributed scanning engines. The current version does not place any agents on the hosts being scanned.

Secure logon for policy management?
At this time scanner does not have a logon process, if a user has logon rights to the box scanner is installed on, they can intern run the program.

How are policies distributed to scanners?
In the current version, policies are manually defined in a template. These templates can be shared between multiple scanners.

How are policy changes handled? Will the central console detect which scanning agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually? Can it be done once from a central location or do all scanners have to be updated individually?
In the current version, policies are manually defined in each scanner. The administrator must change policies and re-deploy them to each scanner individually.

How many attack signatures?
The CyberCop Scanner is updated regularly. The current vulnerability count is about 800.

Which platforms (i.e. NT, Windows 2000, Linux) and network resources (i.e. firewalls, routers, printers, Web/mail/FTP servers) are covered by the attack signatures?
CyberCop Scanner currently scans any device that has an IP address connected to the network. The specific operating systems and devices include: all versions of Windows, Free BSD, NetBSD, OpenBSD, BSDI, Linux, IRIX, HPUX, AIX, Solaris, SunOS, Novell, Cisco, Ascend, MacOS and HPLaserJet. It also includes specific utilities that test firewalls and intrusion detection systems and specific modules that test routers, Web servers and FTP servers for example.

Can it perform accurate OS detection?
CyberCop Scanner includes patent pending technology that detects the OS running on any network device. All of the vulnerability tests that are not relevant to the identified OS can be automatically deactivated. Since banner checks are prone to false positives, this feature uses an algorithm to ensure accuracy.

What types of port scans can be performed?
UDP, TCP, TCP SYN, TCP ACK, TCP FIN, RPC, FTP

Can the administrator define custom attack signatures?
CyberCop Scanner includes our exclusive Custom Audit Scripting Language (CASL). CASL is a C like language that enables the user the construct data packets from a graphical interface. These scripts can also be selected and deployed across the network like any of the vulnerabilities in the database. CyberCop Scanner also supports a VB Scripting engine for users that prefer to audit in a VB environment.

Can it perform true DoS attacks
CyberCop Scanner performs true DoS attacks. Each of these tests are not selected in the default testing templates and are clearly marked in the list of vulnerability tests because they should not be used in a production environment.

How are new attack signatures obtained and deployed?
Each month PGP Security posts vulnerability updates to a ftp server. CyberCop Scanner includes an AutoUpdate feature that automatically connects to the ftp server to download the new checks.

Frequency of updates? Provide dates of all updates in the last year.
Updates are posted on the 15th of every month.

Can one signature update file be downloaded to the local network and used to update all scanners from a central location, or is it necessary to initiate a live connection to the Internet download server for each scanner?
Updates can be downloaded to a local CyberCop Scanner workstation or can be downloaded and distributed from an internal/external ftp server.

Can signature updates be scheduled and fully automated?
The update procedure can be done manually, via automatic download or scheduled.

Are scan results available in real time during scan?
Yes. As a scan is running, the results of the scan can be easily viewed from the *Scan Results* window in the user interface.

Are scan results (even as a summary) available on-screen following a scan without having to run a separate report?
Yes. CyberCop Scanner's main screen identifies the number of nodes scanned, the number of vulnerabilities identified, the risk levels of the identified vulnerabilities and the time elapsed for the session.

Advice on preventative/corrective action when vulnerabilities found?
Security concerns and recommended fixes are provided for each identified vulnerability. Additional information includes risk factor for the vulnerability, complexity of the attack, ease of fix, root cause, popularity of the vulnerability and business impact. Each criteria is set with recommended values, but can be customized to meet the users corporate security policy.

Capability to auto-fix certain vulnerabilities? If so, is there an "interactive mode" and/or an undo facility?
CyberCop Scanner includes Fix-It Modules that enable the user to fix Windows registry and policy settings. Each of these modules are clearly marked with a "wrench icon" in the *Scan Results* window.

Automatic alerting if severe vulnerabilities are found during a scan?
Severe vulnerabilities are clearly labelled as such, but no alerting capabilities are included. A pre-defined report template ranks vulnerabilities by order of severity.

Integration with other scanning/IDS products?
Not supported at this time.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
CyberCop Scanner ships with Crystal Reports for both canned and customized reporting. This reporting engine allows one to create very granular reports for the security administrators and those that need to resolve the issues, up to the high-level reporting designed for the CIO and IT Manager within an organization. These reports include graphical, as well as detailed text outlining the vulnerability, resolution, risks and other options. Crystal Reports is known for it's ease of use in creating custom reports, but PGP has also included many "canned" reports so one can immediately start processing reports.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Is it possible to combine reports from several scanners?
CyberCop Scanner, with Crystal Reports, fully supports differential reporting to compare separate results databases. Users could also merge multiple results databases into a single larger database if desired. (Not supported as part of the product)

Report management – archiving? Can historical scans be consolidated/compared for trend analysis/comparisons
Differential reporting also allows a user to identify what has changed on a given range of nodes, since the last assessment. This allows a security administrator to identify new vulnerabilities that have been created or old vulnerabilities that have been resolved since the last assessment.

Can scans/reports be scheduled for automatic production? Can the results be e-mailed to administrators or published straight to a Web site?
The current version of CyberCop Scanner is not able to perform automated or scheduled scans, but this functionality will be returning in future versions. Results can be presented in various formats including HTML for web publishing.

Does the product incorporate IDS evasion techniques to test IDS effectiveness? If so, describe in detail how these are implemented.
Yes. CyberCop Scanner is one of the few assessment tools that includes full blown IDS auditing support. Scanner will leverage the power of the CASL engine to provide a full module set of checks, scans and probes to audit your IDS.

How is it licensed? How is the license enforced?
CyberCop Scanner is licensed on a per-node basis for full enterprise coverage, or per server if the customer only wishes to use the product for assessing their servers. We do not build any enforcement mechanisms into the product that might restrict or increase the difficulty of use in the product. The customer must identify how they plan to use the product, we will license it for that use. Any use beyond their license will be a license violation, but no mechanisms will prevent the use on systems not licensed to use the product. *[Editor's Note: This is the most flexible licensing policy we have encountered – excellent]*

End user pricing information
$48 / node at 250 node price point
$512 / server at 50 server price point

Ongoing cost of maintenance/updates
Standard Maintenance and Updates are included in the costs quoted above. Additional support contracts are also available.

Networks Vigilance NV e-secure

Brief product description
NV e-secure is a Network Vulnerability Assessment tool. It helps a company determine whether its networks and firewalls are vulnerable to attacks. A unique distributed architecture allows for enterprise-wide vulnerability assessment. It provides for remote segment vulnerability assessment as well as firewall security assessment.

Architecture – brief description
The main interface with the product is e-secure Console.
The user can manage all e-secure activities, including network security testing, firewall testing, remote segment network security testing via distributed test engines.
NV e-secure engine is our core technology. Basically, it plays what we call 'test cases'. The engine is able to inject packets on the network, receive answers from remote systems, check if they are still running and much more. A test case can be seen as the e-secure version of a hacker attack script.
Additionally, e-secure comes with 2 remote 'agents'. With e-secure Probe, the user is able to perform firewall security assessment. With e-secure Distributed Test Engine that installs on remote segments, the user can scan these segments from the same console, and get a single report consolidating vulnerabilities from local and remote networks

Documentation
A Getting started manual is provided. It is an on-line PDF file. We consider our e-secure WEB site a complementary information source as additional information including white-papers are available.

What are the minimum/recommended console OS and hardware requirements?
e-secure Console - Ethernet or Token Ring network adapter; 50MB of free disk space; and 64MB of RAM on Windows NT4, or 128MB of RAM on Windows 2000.

e-secure Distributed Engine - Ethernet or Token Ring network adapter; 30MB of free disk space; and 64MB of RAM on Windows NT4 or 128MB of RAM on Windows 2000.

e-secure Firewall Probe - Ethernet or Token Ring network adapter; 20MB of free disk space; and 64MB of RAM on Windows NT4 or 128MB of RAM on Windows 2000.

On what platforms is this certified to run? Will it work on Windows 2000?
Windows NT 4 SP3 and later
Windows 2000

At what layer of the protocol stack is the product working? Is a raw packet driver installed?
A raw packet driver is installed as part of the automated installation process.
It is used to inject "illegal" packets on the network as well as to perform network/service scans as efficiently as possible.
Other TCP/IP dialog uses the regular Windows Sockets Interface.

Can multiple scanning engines be deployed and configured from a central console, i.e. define a single scanning policy centrally and deploy this to all scanners automatically?
Yes. We have "Distributed Test Engines". They play test cases on their local segments, on behalf of the console and report results in real time using a secure channel. The Console keeps complete control on the scanning policy meaning it is not 'deployed' to remote scanners.

Authentication between console and engines – Is it available? What algorithm/key lengths?
There is no real authentication between console and engines yet. However, the information exchanged between console and engines are encrypted using the openssl 3.0 algorithm. The key in use is 1024 bytes length (RSA).

Secure logon for policy management?
Not needed. Administrator privileges are requested to run the product.

How are policies distributed to scanners?
At connection time, the entire policy settings (test cases configuration, policy parameters etc …) are sent to each connecting scanner.

How are policy changes handled? Will the central console detect which scanning agents are using a changed policy and redeploy automatically, or does the administrator have to do this manually? Can it be done once from a central location or do all scanners have to be updated individually?
Policies are managed centrally in the console. The policies are sent dynamically to the remote agents each time a session is run.

How many attack signatures?
At this time (Nov 6), 542 Test Cases are included in v 2.2.

Which platforms (i.e. NT, Windows 2000, Linux) and network resources (i.e. firewalls, routers, printers, Web/mail/FTP servers) are covered by the attack signatures?
Our Test Case database mainly includes scripts for Windows NT and Unix systems. However, a number of test cases for other network devices (routers, switches, printers) are also provided.

Can it perform accurate OS detection?
Yes. A network finger-printing capability is included. Accurate OS detection avoids playing test cases when inappropriate.

What types of port scans can be performed?
TCP and UDP port scans are available. Scanning ranges are configurable with a LowPort – HighPort interval.
As e-secure is an assessment tool, not an attack tool, port scanning does not do any attempt to conceal its activity.

Can the administrator define custom attack signatures?
No.

Can it perform true DoS attacks
It performs true DoS attacks. Some attacks may also crash the target system.

How are new attack signatures obtained and deployed?
Automatic product updates are part of the product. With its registration key, the user obtains a "login" on our e-secure web site. At each product start-up, the user has the opportunity to check for an update package. Installation of the available packages is completely automated.

Frequency of updates? Provide dates of all updates in the last year.
Between one and 2 updates every 2 weeks. "High urgency" updates can also been produced if required. No information for last year is applicable.

Can one signature update file be downloaded to the local network and used to update all scanners from a central location, or is it necessary to initiate a live connection to the Internet download server for each scanner?
Only the Console needs the Internet connection. The remote engine updates via the Console connection which acts as a sort of proxy. However, this process has to be repeated for each remote engine.

Can signature updates be scheduled and fully automated?
The console needs to be started in order to update. However the console can be configured to automatically check for updates with or without user confirmation. A fully automated web upgrade is planned in a future release.

Are scan results available in real time during scan?
No

Are scan results (even as a summary) available on-screen following a scan without having to run a separate report?
Yes. In fact, it is quite possible to do all the after-work inside the console GUI, without going through the generated reports *[Editor's Note: e-secure is one of the best products we have seen in this respect]*. Some users might find it easier to browse through.

Advice on preventative/corrective action when vulnerabilities found?
Advice is given on potential vulnerabilities. We usually direct the reader to relevant pages on vendor web sites.

Capability to auto-fix certain vulnerabilities? If so, is there an "interactive mode" and/or an undo facility?
No.

Automatic alerting if severe vulnerabilities are found during a scan?
A colour code warns about the follow-up urgency but no special alerting mechanism takes place.

Integration with other scanning/IDS products?
No.

Management reporting – range of reports/custom reports/how easy is it to filter and extract detail? Different reports for technicians and management/end users?
Manager reports give some factual information on the holes found and their follow-up urgencies. They are readable by non specialists.
Administrator reports provide all the technical details. Links to our e-secure WEB site guarantees that reference information (e.g. patch availability) is as up to date as possible.
Services reports contain similar information as administrator reports, although it is displayed service by service for easier security improvement planning.
Host reports document on open services (TCP, UDP, RPC).
Delta reports focus on new vulnerabilities (since previous job) only.
Historical reports display trends in numbers of vulnerabilities.
Furthermore, as previous job results are stored in a database, it is possible to re-generate reports at any time.

What are the limitations and restrictions on enterprise-wide alerting and reporting? Is it possible to combine reports from several scanners?
In our architecture, a single report can be obtained, consolidating vulnerability assessment from several test engines located remotely.

Report management – archiving? Can historical scans be consolidated/compared for trend analysis/comparisons
All job results, while in "Session mode", are automatically saved in a local database. Comparisons can be done easily with Delta reports and Historical reports, which can be generated at any time.

Can scans/reports be scheduled for automatic production? Can the results be e-mailed to administrators or published straight to a Web site?
Scans can be scheduled at a later time. The standard OS features (AT command) are used. An e-mail with attached generated report files can be sent to the requesting user. As reports are generated using standard HTML format they can be accessed locally or remotely using the local explorer. No publication on WEB site.

Does the product incorporate IDS evasion techniques to test IDS effectiveness? If so, describe in detail how these are implemented.
No.

How is it licensed? How is the license enforced?
Licenses are per "class C" (/24) network segment. Multi-segment licenses as well as site licenses are available. A "Class C" license gives the right to install 2 consoles and unlimited number of probe / distributed test engine. License information is stored in a binary file generated by Networks Vigilance or Cyrano.

End user pricing information

1st range	US$ 9,900
2nd range	US$ 9,000
3rd and +	US$ 5,000 per range
Site license	US$ 250,000

("range" means "class C" segment, maximum 254 addresses)

Ongoing cost of maintenance/updates
Yearly maintenance fee: 18 %

APPENDIX B – THE ADTECH AX/4000

About Adtech & Spirent

Located in Honolulu, Hawaii, Spirent Communications Adtech Division is a manufacturer of state-of-the-art telecommunications test systems.

Founded in 1967 by Dr. Ned Weldon, a professor of electrical engineering at the University of Hawaii, Adtech, Inc. provided electronics engineering services for over 20 years. In 1988, the company introduced a line of data-channel simulators and began to focus on products for the data communications market. In 1993, Adtech developed its first ATM test system.

In 1997, Adtech became a wholly-owned subsidiary of Bowthorpe, plc, the British technology company. In 2000, Bowthorpe began trading as Spirent plc, and Adtech is now a division of Spirent Communications.

Adtech's flagship product, the **AX/4000 Broadband Test System** (as used in NSS labs), is a modular, multi-port system that generates broadband test traffic, analyses full-rate traffic in real time, and simulates network induced delays and Quality of Service (QoS) impairments.

The Adtech AX/4000 Broadband Test System

The AX/4000 is a modular, multi-port system that can currently test four different transmission technologies (IP, ATM, Ethernet, and Frame Relay) simultaneously at speeds of up to 10 Gbps. Unlike software-based testing solutions, the AX/4000's FPGA hardware-based architecture is fast enough to provide more than one million full-rate measurements and statistics continuously and in real time.

Figure 78 - The Adtech AX/4000

The AX/4000 Generator and Generator/Analyser modules include tools for creating unlimited traffic variations and detail. Set-up "wizards" and logical functional blocks allow you to build complex traffic streams quickly and easily. When injected onto the network, these traffic streams can be "shaped" (to simulate constant or bursty traffic) and even introduce error conditions.

The controller software, available in both Windows and UNIX versions, has a very intuitive graphical user interface. Test set-up is logical and quick and when tests are running, the software displays real-time data and statistics that are thorough and easy to understand.

With an Ethernet control module installed in the AX/4000 chassis, the system can be connected to an Ethernet-based LAN for access by remote users.

Because every test module in the chassis has its own address on the network, users can access the modules they need and leave the remainder for others to use. This enables multiple users to access the same chassis simultaneously across a network.

The AX/4000 is available with a 16-slot mainframe or a four-slot portable chassis. Both are functionally identical except for the number of available slots, and all AX/4000 components will operate in either chassis.

Control modules provide the interface between the chassis and an external controller such as a PC or a workstation. Control modules are available with a high-speed IEEE-488 GPIB connector for direct cable connection to a controller or with a 10BaseT Ethernet connector for a network connection.

The actual broadband testing occurs inside the AX/4000 test modules. Each test module is essentially a single port tester that can operate independently or as part of a larger multi-port test set-up.

Figure 79 - The Adtech test modules

Adtech currently produces ten different test modules to support different test requirements and speeds. The AX/4000 uses plug-in port interfaces to provide the physical interface for test modules. These cards are interchangeable allowing a single test module to perform tests with a variety of physical connections and speeds. Over 30 port interfaces are available supporting a wide range of interface standards for ATM, Frame Relay, Ethernet, and IP.

In addition to creating an extremely wide range of packet and cell types, the AX/4000 allows you to program sequences of packets with looping, jumps, repeats, conditional branching and even error injection. Errors can be injected randomly or manually, and can be set to hit any byte or even certain bits within specific bytes.

It is also possible to simulate multiple classes of service by prioritising each traffic source. For example, you can assign a higher priority to constant bit rate (CBR) traffic and a lower priority to variable bit rate (VBR) traffic sources. After generating the traffic, you can use an AX/4000 analyser to check your device’s ability to maintain proper QoS levels.

In addition to providing live statistics, the analyser can also capture traffic at full rate for further analysis or protocol decoding. Captures can be triggered manually or automatically based on specific events or errors and can include packets or cells received before, after, or both before and after the trigger event.

The AX/4000 can maintain over 125,000 simultaneous QoS measurements per port at full rate and in real time. All statistics can be saved on disk for further analysis and for printing detailed test reports.