Network ICE™

BlackICE™ pro

User's Guide

Version 2.0

BlackICE User's Guide – Version 2.0

Author: Andrew Plato

Conventions Used in this Manual

Bold	The names of screen objects, such as menu choices, window names, field names, and items in lists.
Italics	Italics is used for emphasis or to highlight an important word or concept.
`Monospaced`	Pathnames, filenames, and code are shown in monospaced font.
`Monospaced Bold`	Values you must type in are shown in monospaced, bold font.
`Monospaced Italics`	Variables, such as a server name, are shown in monospaced, italic font. These are usually enclosed in angled brackets <*`servername`*> as well.
[Inside Brackets]	Keyboard keys, such as [ENTER] or [Page Up] are shown inside brackets.

CONTENTS

1 INTRODUCTION

Thank you for purchasing BlackICE Pro. BlackICE is a powerful way to detect, stop, and analyze the activities of people trying to hack into your network or computer. BlackICE was designed from the ground up to work with modern, switched networks to provide comprehensive protection against intruders.

BlackICE is a fully integrated component of the Network ICE *Collective Awareness*™ technology. Working in tandem with an ICEcap reporting and management console, BlackICE can protect your network from both internal and external threats.

WHAT IS A NETWORK INTRUSION?

In the past, it was relatively easy to stop hackers since most systems had few if any connections to other computers or networks. Older networks were simpler and thus easier to protect. Even as networking became common in the 1980s, systems were not connected to public networks, such as the Internet. Thus there were few hackers and few security incidents.

However with the rise of the Internet and ubiquity of corporate computer networks in the 1990s, hackers have more opportunity than ever to break into systems. Additionally, with many people using the internet for their daily financial and consumer activities, there is more sensitive information available.

Until now, most intrusion detection and protection was handled by expensive networking devices such as routers and firewalls. These devices are designed to block network traffic en mass. This often hinders the ability of legitimate users to access the Internet.

Hackers are clever individuals. As corporations implemented firewalls and other Internet protection measures, hackers found ways around these devices. The new targets for hackers are places few IT managers even perceive as threats. One of the most common ways to get into a network these days is to hijack a telecommuter's connection. Once inside the corporate firewall, a hacker can freely exploit internal servers and workstations.

BlackICE distributes powerful intrusion detection and protection throughout your network. The BlackICE Pro agent is small enough to run on all your workstations and servers, yet robust enough to identify and stop over 200 different attacks. When you deploy BlackICE to your corporate network, you're erecting an enterprise-wide web that can identify and stop hackers before they break into any system.

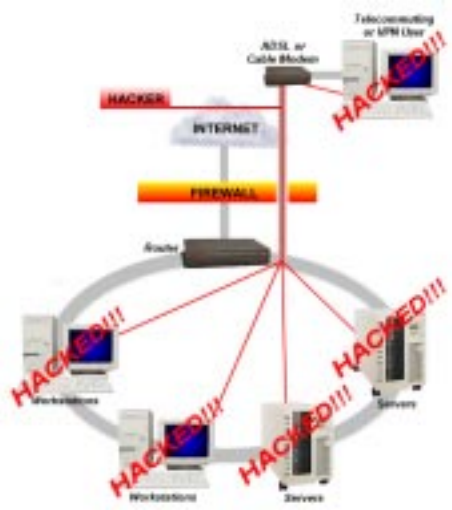


Figure 1 – Without BlackICE

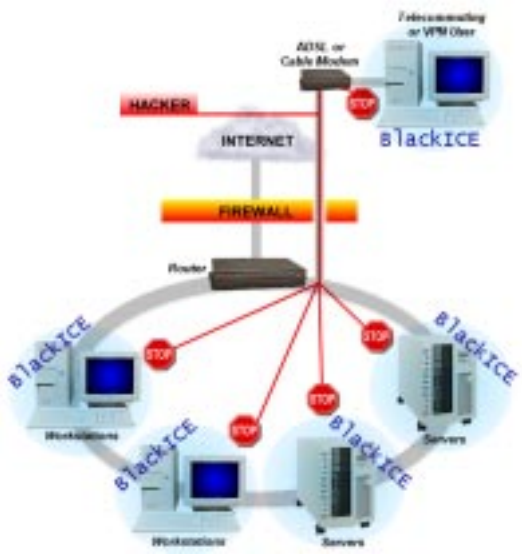


Figure 2 – With BlackICE.

The figure on the left illustrates a common corporate network. A firewall protects the network from external attackers. However, if a hacker is able to penetrate the firewall, which is not very difficult, he can easily gain access to the internal systems on the network. One of the most common ways hackers access networks is to hijack a VPN or dial up connection from a telecommuting user.

The figure on the right demonstrates how BlackICE intrusion countermeasures, can stop hackers even if they penetrate a firewall. BlackICE provides local, dynamic protection for each work station or server on the network.

BlackICE can also protect telecommuting and VPN users. Since these users are not protected from a corporate firewall, hackers can easily scan internet service providers to locate open connections. This is especially problematic for “always on” connections via DSL or cable modems.

How BlackICE Works

BlackICE consists of an extremely powerful detection and analysis engine that monitors numerous network ports and protocols for suspicious behavior. The BlackICE engine was coded specifically for modern high-speed networks. The application passively watches all traffic on the network connection without hindering or delaying traffic at all.

When suspicious behavior is detected, BlackICE springs into action and begins logging information about the event. BlackICE collects anything it can from the attack. Even the most sophisticated hackers cannot hide from BlackICE's evidence file collection and backtracing commands.

If BlackICE determines the attack poses an immediate threat to the system, it can block ALL network traffic from the attacking system. BlackICE blocks access at the network layer, therefore there is no way around the block.

If the BlackICE user interface is installed, information about attackers is displayed on the **Intruders** tab. Information about the type of attack the intruder attempted is displayed on the **Attacks** tab.

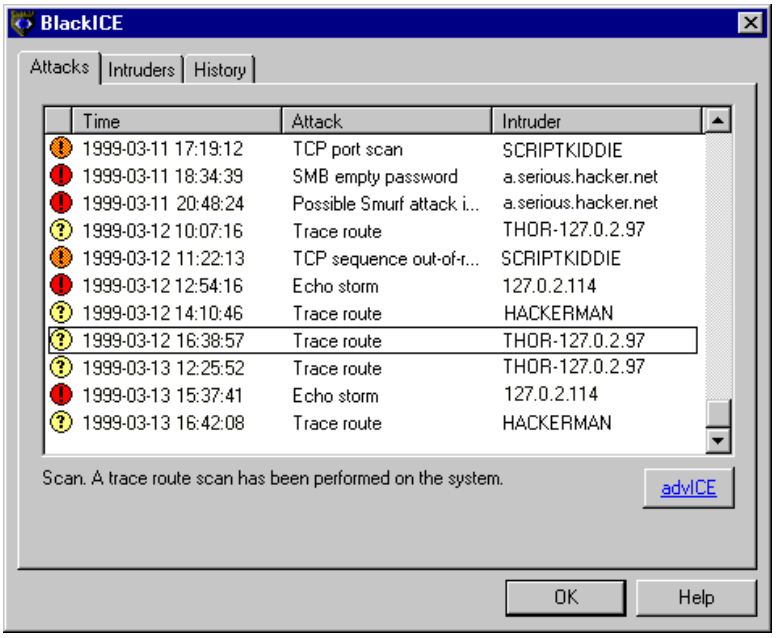


Figure 3 – The BlackICE Attacks tab.

Additionally, the **History** tab displays attacks and network traffic in colorful line graphs. This can help you spot trends and patterns in when hackers are trying to get into your computer.

ICECAP INTEGRATION

BlackICE Pro and Sentry are fully integrated components of the ICEcap management console. ICEcap is a server-based system that aggregates intrusion data from all the BlackICE agents on your network. ICEcap can also remotely install and manage BlackICE agents on the network.

Because ICEcap has an "enterprise-wide" view of network intrusions it can help identify "strategic" attacks and trends. Coupled with an ICEscan vulnerability scanner, ICEcap becomes a powerful intelligence center that can thwart hackers.

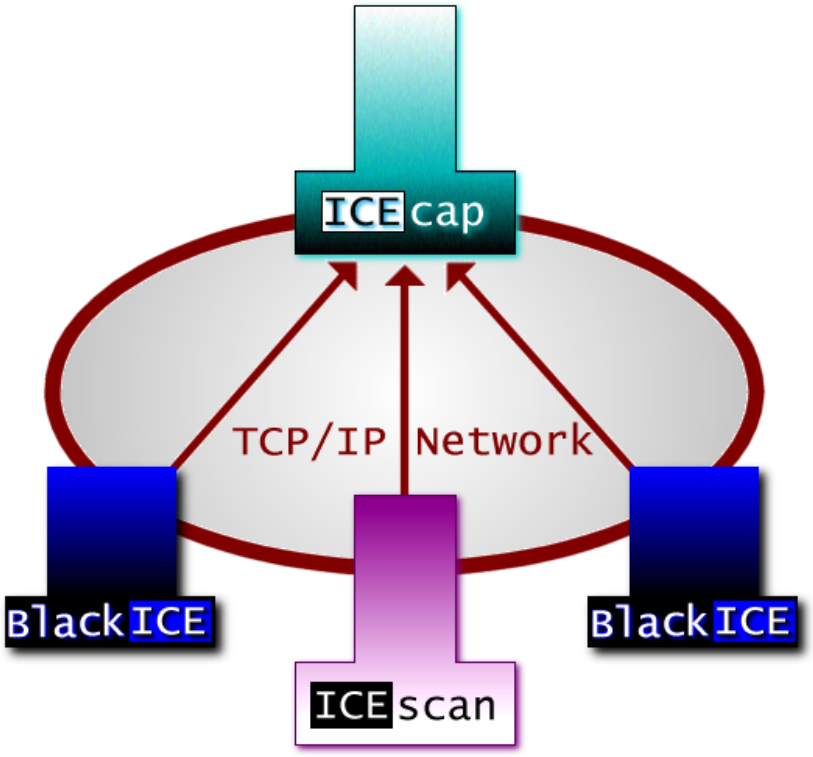


Figure 4 – On a network, BlackICE is used to defend each workstation and report events to an ICEcap server. The ICEcap server aggregates and reports the events that took place on each network workstation where BlackICE is installed.

Additionally, ICEcap can remotely install and manage all BlackICE installations on a network from a central location. Using the Agent Management features of ICEcap, you can install, update or uninstall BlackICE on any Windows-based system connected to the network. ICEcap can also issue downstream protection measures to all BlackICE agents.

ICEcap also provides a mechanism to install "silent" versions of BlackICE. These "silent" agents offer the exact same protection and detection of the regular BlackICE without the local user interface. Silent BlackICE agents are ideal for deployment to user workstations.

For additional information regarding deploying BlackICE via ICEcap, please refer to the *ICEcap Administration Guide* included with your copy of ICEcap.

TRAFFIC FILTERING

In addition to BlackICE's ability to automatically block intruders, you can also configure BlackICE to manually, trust, block, or ignore specific attacks or intruders.

Trusting Intruders

If your network has servers or devices that generate regular scans or probes of networked systems, you may want to trust these systems to ensure BlackICE does not inadvertently block them. For example, if you are using ICEscan from Network ICE to test for vulnerabilities, this system will generate false attacks on BlackICE systems, since it is executing many of the same attacks a hacker would. By trusting the ICEscan system, you can stop BlackICE from reporting ICEscan tests as attacks.

WARNING: When a system is trusted, BlackICE will ignore all attacks from that system. Since hackers often mask their true identity through "spoofed" IP addresses, a hacker could use your trusted addresses as a mechanism against you. Network ICE recommends trusting only those systems that regularly carry out scans.

If you need to issue enterprise-wide trusting measures using BlackICE, ICEcap from Network ICE can automatically distribute trusting instructions to all the BlackICE agents on your network. See the ICEcap Administration Guide for more information.

See page 26 for more information on how to trust an intruder.

Blocking Intruders

Under normal conditions, BlackICE will allow other systems to access your computer without hindering the network traffic in any way. Most "intrusions" on systems are innocuous port scans or ping sweeps. These intrusions are not dangerous and thus BlackICE does not automatically block these addresses. Furthermore, some internal systems may generate periodic port scans and ping sweeps to see if devices on your network are alive.

BlackICE only blocks intruders when they initiate an attack that is an immediate threat to the computer. For example, a LAND attack could cause a system to crash, as such BlackICE will block intruders attempting LAND attacks.

However, you can manually instruct BlackICE to block an intruder. BlackICE can only manually block addresses that have initiated an attack.

If you need to issue enterprise-wide protection measures using BlackICE, ICEcap from Network ICE can automatically distribute blocking instructions to all the BlackICE agents on your network. See the ICEcap Administration Guide for more information.

See page 25 for more information about Blocking Intruders. To modify the addresses BlackICE is currently blocking see page 37 for more information.

Ignoring Intruders

Since some intrusions on a network may be the result of automated port scans or other legitimate network tools, you may want to ignore specific attacks that keep reoccurring. For example, some Internet Service Providers carry out routine port scans to and ping sweeps to check the state of downstream clients.

BlackICE allows you to specify an attack or an attack by a specific intruder to ignore.

WARNING: When an entire attack is ignored, BlackICE will not log any information about that attack. Be careful which attacks you ignore, since some innocuous attacks could signal a prelude to a serious attack.

See page 27 for more information about how to ignore an attack.

SECURITY LEVELS

When BlackICE detects an attack, it can automatically block access from the hacker's system. However, not all suspicious network activity is an attack. What constitutes an attack vs. legitimate use of the network is not always easy to determine. Many Internet Service Providers execute regular and completely safe scans that BlackICE may detect as an attack.

Hackers often take advantage of legitimate Internet technologies to make their activities seem innocuous. One of the most common ways to hack computers is to exploit open "ports."

A *port* is a virtual "connection point" on a computer. When a computer is connected to a network (including the Internet), the computer communicates with other computers via virtual ports. For example, when you download e-mail, your computer establishes a connection on TCP port 110 to the mail server. Port 110 is the TCP port nearly all mail servers use. After sending logon information, the mail server responds and transmits your email to your computer.

Communication ports are divided into two categories: *System* and *Application*. The System Ports (ports 0 – 1023), or low-end ports, are used for services installed on a computer, such as e-mail or web browsing. The Application ports, or high-end ports (ports 1024 – 65536), are used by client applications such as chat programs or an Internet telephone.

It is generally harder to crack high-end ports since they are only open when specific applications are running. The lower ports are easier to crack since many of them are always open.

There are two categories of ports for Internet connections: TCP and UDP. TCP connections are the most common. They are used for web browsing, downloading files, etc. UDP ports are essentially the same as TCP. However, UDP connections do not have the error correction features that TCP has. UDP is used for streaming content like RealAudio.

BlackICE has four Security Levels that define how rigorously it blocks unsolicited traffic for ports and port type. Inbound traffic is blocked on the security level you select. The more restrictive the security level, the more likely BlackICE will block unsolicited inbound traffic. Outbound traffic is never blocked. This ensures that web browsing and other regular Internet functions remain unaffected.

There are four security levels for BlackICE: *Trusting*, *Cautious*, *Nervous*, and *Paranoid*. The following chart demonstrates the relative protection of these four levels.

Security Level	Port Type	Inbound Ports		Outbound Ports	
		System	Application	System	Application
Trusting	*UDP*	☑	☑	☑	☑
	TCP	☑	☑	☑	☑
Cautious	*UDP*	☒	☑	☑	☑
	TCP	☒	☑	☑	☑
Nervous	*UDP*	☒	☑	☑	☑
	TCP	☒	☒	☑	☑
Paranoid	*UDP*	☒	☒	☑	☑
	TCP	☒	☒	☑	☑

Security Level Descriptions

Trusting: When set to trusting, all ports remain open and unblocked. This setting is good to use if you have minimal threat of intrusions.

Cautious: The *Cautious* setting is good for regular use of the network. This setting only blocks inbound intrusions on System Port(s). All other ports remain unblocked and therefore should not interfere with normal network and Internet usage.

Nervous: This setting is preferable if you are experiencing repeated intrusions. For the *Nervous* setting, BlackICE blocks inbound intrusions on all the System ports and TCP Application ports. This setting may restrict some interactive content on web sites. Streaming media and other “application specific” Internet usage remains unaffected.

Paranoid: The *Paranoid* setting is very restrictive, but useful if your system is enduring repeated attacks. Under this setting BlackICE blocks all inbound intrusions. This setting may restrict some web browsing and interactive content.

For more information about setting security levels, see page 33.

EVIDENCE FILES

Evidence files are part of BlackICE's intrusion monitoring features. As a hacker is attempting to break into your system, BlackICE can capture all network traffic attributed to the hacker and place that information into an *evidence file*.

BlackICE evidence files are located in the <*installation directory*>/Network ICE/BlackICE folder. If you installed BlackICE to the Program Files directory on the C: drive (the default), for example, the evidence files would be located in C:/Program Files/Network ICE/BlackICE. Each file has an *.enc extension.

The number of evidence files BlackICE captures, the filename prefix, and the size of each evidence file are established on the Evidence Log tab for BlackICE configuration. See page 32 for more information.

To view the contents of an evidence file, you need a trace file decoding application. Many networking and security product companies produce such decoders. There are also some shareware decoders available on the Internet.

If you are running a Windows NT Server 4.0, you can install the Network Monitoring service. This service includes the trace file decoding application Network Monitor.

For more information about installing the Network Monitoring service or using the decoding tool, refer to the documentation included with your copy of Windows NT Server 4.0.

THE NETWORK ICE PRODUCT LINE

For superior detection and protection, BlackICE offers the power to stop hackers before they do any damage.

BlackICE Defender

BlackICE Defender is designed for home and small-business users. BlackICE Defender is ideal for “always on” Internet connections such as cable modems and DSL. BlackICE Defender can monitor and block any intrusions from any computer, anywhere on the Internet. Furthermore,

BlackICE Pro

Intended for workstations on corporate networks, BlackICE Pro features the same powerful detection and protection as BlackICE Defender. However, this version integrates with a ICEcap server for the ultimate network defense against intruders.

BlackICE Sentry

This version of BlackICE is specially tuned to monitor key subnets of a network and report any suspicious activity to an ICEcap server. BlackICE Sentry is ideal for monitoring devices not covered by other versions of BlackICE or that are connected to the network via shared media.

BlackICE Auditor

The Auditor series is designed for professional security consultants to perform short term (120 days or less) security audits on a company's network. Auditor versions of Network ICE products contain all the features of the full product, yet have a limited use license.

OTHER NETWORK ICE PRODUCTS

Network ICE offers these other products for use identifying and stopping intrusions and security breeches.

ICEscan

ICEscan is a security auditing program that scans the network for common network security vulnerabilities that hackers might exploit. ICEscan runs many of the same procedures hackers attempt and reports the success or failure of such attacks. ICEscan also includes an advanced scheduling and tracking system. The scheduling feature allows you to keep constant watch on the network even in the middle of the night. The tracking features look out for new systems added to the network. ICEscan integrates with ICEcap for centralized reporting and management of vulnerability data.

ICEcap

ICEcap is a centralized reporting and management system for BlackICE and ICEscan products. ICEcap can produce consolidated reports on the events and potential security breeches on a network. Using these reports, system administrators can, from one central location, review the security of all systems in a corporate enterprise. ICEcap can also identify attacks that single BlackICE installations would not detect as a serious intrusion. For example, ICEcap can detect that someone has performed a ping sweep on the network. An individual BlackICE system would not consider one ping an attack.

ICEcap is a powerful tool identifying and stopping internal hacking as well as external intrusions.

2 INSTALLING BLACKICE PRO

This section steps you through the process of installing the BlackICE application.

NOTE: These instructions describe how to manually install, remove and update BlackICE Pro on a system. If you wish to perform a centralized deployments of BlackICE agents via ICEcap or InstallPac, please refer to the documentation included with those products.

MINIMUM SYSTEM REQUIREMENTS

- **Operating Systems**[1]: Windows NT Workstation 4.0, Windows NT Server 4.0, Windows 95 OSR2, Windows 98.

  NOTE: BlackICE is not supported on systems using Windows 95 Retail configured for multiple users.

- **Processor**: Pentium or better.
- **Memory**: 16 MB or more.
- **Hard Drive Space**: 10 MB free.
- **Network Protocol**: TCP/IP
- **Network Connection**: 10/100 Ethernet LAN/WAN, cable modem, DSL router, ISDN router, or regular dial-up modem.

HOW TO INSTALL BLACKICE

1. Logon to the system where you are installing BlackICE with administrative privileges.
2. Locate the Setup Application: `BIsetup.EXE`. This program is available from Network ICE for download. If you have lost your original copy, contact Network ICE support at corpsupport@networkice.com to obtain a new copy. You can execute this application across a network.
3. Execute `BIsetup.EXE`. The system must unpack the files and verify them. When that is finished, the setup application begins.

☒ If setup detects and existing version of BlackICE, the setup prompts you to uninstall or continue to upgrade the previous version. See page 15 for more information about uninstalling BlackICE.

4. A welcome screen is displayed. Click **Next** to continue.
5. Review the **Licensing Agreement**. If you accept the agreement terms, click **Yes**. Otherwise, click **No** to exit the BlackICE setup application.

[1] Support for Windows 2000 will be included as part of a general release of BlackICE.

6. Verify the installation path for BlackICE. If you wish to change the path, click **Browse** and locate the path you wish to use. Click **Next** to continue.
7. Verify the folder where BlackICE shortcuts are located on the Windows Start menu. If you wish to use a different folder, select it from the list or enter a name in the **Program Folders** field. Do not place BlackICE shortcuts in the **Startup** folder. The setup application automatically places a shortcut in the Startup folder to launch the BlackICE user interface when the system is turned on. Click **Next** to continue.
8. Enter **the License Key** provided to you when you purchased BlackICE. If you have lost this key, contact Network ICE customer support at corpsupport@networkice.com to obtain a copy of your key.

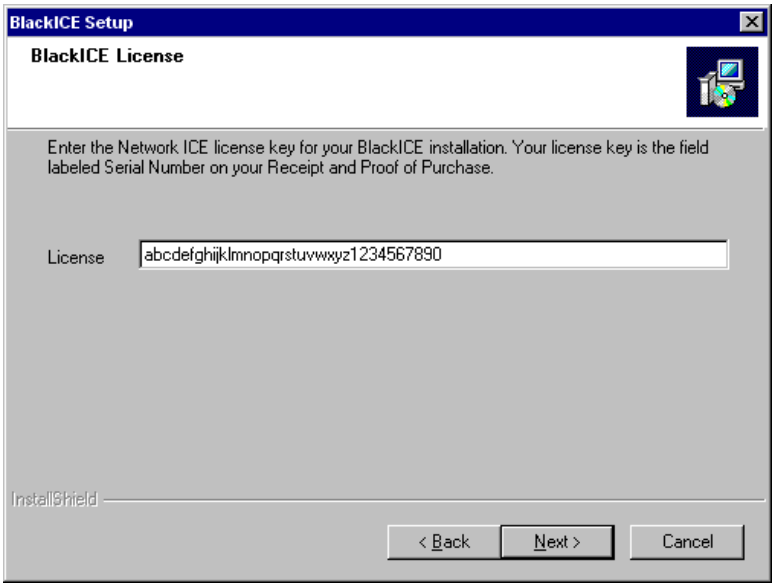


Figure 5 – Enter your license key.

9. The setup application asks if you are going to report events to an ICEcap server. If you do not have an ICEcap server on your network, click **No**. If you are using ICEcap click **Yes**, and complete the following **ICEcap configuration**.

NOTE: ICEcap settings can be modified later using the configuration features of BlackICE (see page 38 for more information). If you are not sure what the ICEcap settings are, click **No** and obtain ICEcap information from your system administrator. Also, before entering an account and password,

---

10. **ICEcap Configuration Steps**. Complete the following steps only if you are forwarding BlackICE event information to an ICEcap server.

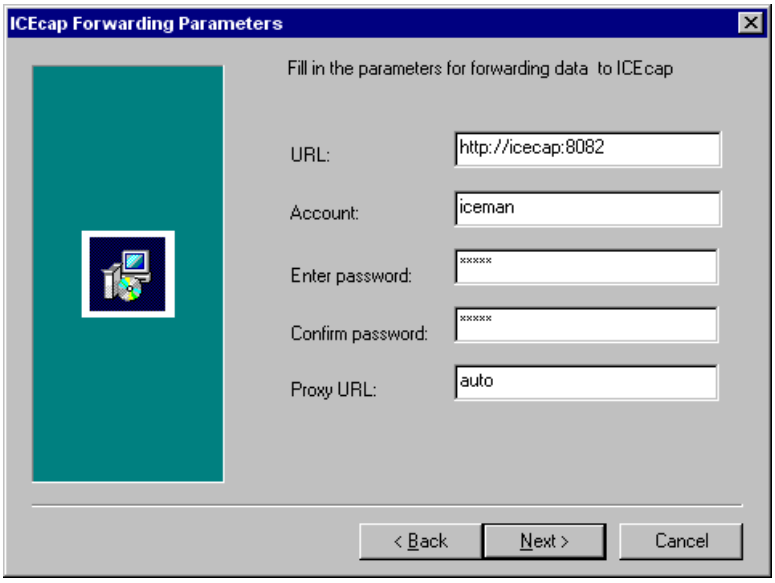


Figure 6 – The ICEcap parameters dialog box.

A. Enter the fully qualified **URL** for the ICEcap server. Make sure to append the TCP port the ICEcap server uses for event reporting.

B. Enter the ICEcap **Account** name and **Password** for that account in the provided fields. This is the account within ICEcap where this BlackICE agent will report agents. Retype the password in the **Confirm Password** field.

C. If the system must route through a proxy server to report events, enter the fully qualified address of the proxy server in the **Proxy URL** field.

D. Click **Next** to continue.

11. The next window summarizes all the selections you have made. If you need to change any of those parameters, click **Back** to retrace the previous steps.

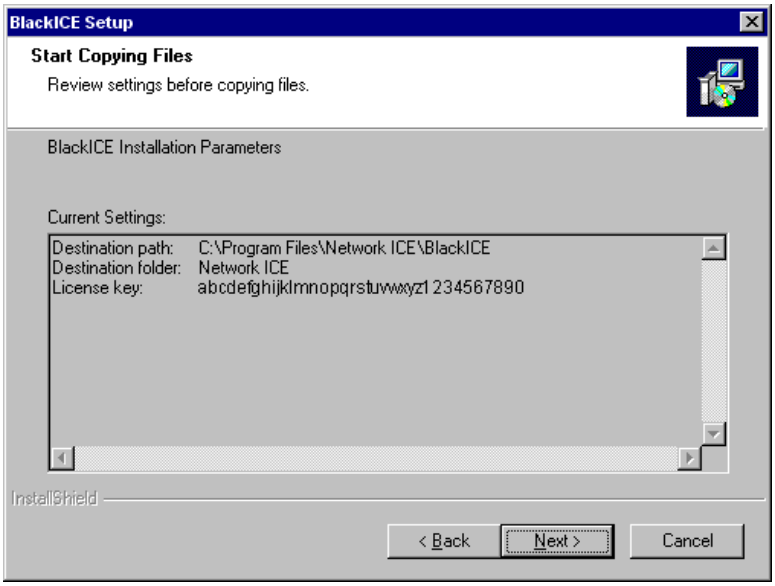


Figure 7 – BlackICE Installation Parameters window (this image does not show any ICEcap forwarding data.)

If the information is correct, click **Next**.

- The installation begins. When it is finished, the BlackICE service is started.

12. The system then prompts you to read the Release Notes. If this is your first time installing this version of BlackICE, it is good idea to review this information. To review the release notes, click **Yes**. Otherwise, click **No**.

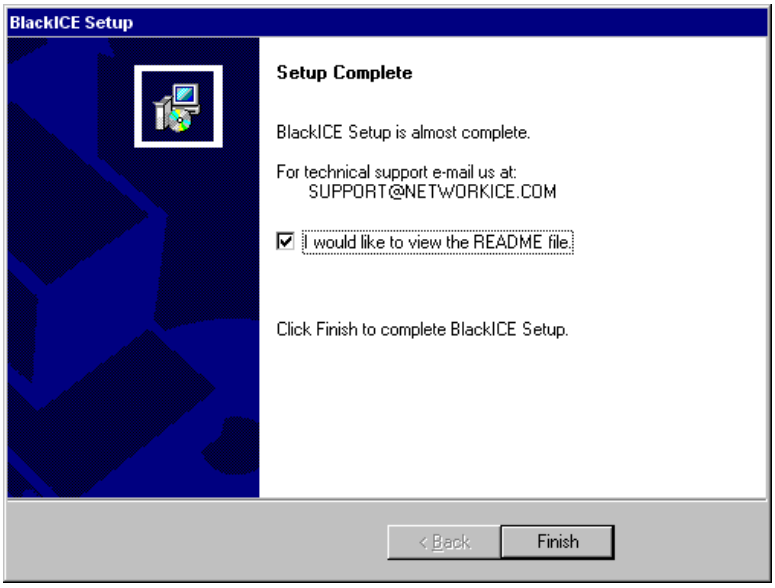


Figure 8 – Final setup screen.

- BlackICE setup is complete.

HOW TO UNINSTALL BLACKICE

To uninstall BlackICE follow these instructions. Once BlackICE is uninstalled, your system is no longer protected from intrusions.

1. From the **Start** menu, select **Settings**. The Control Panel is displayed.
2. Double-click **Add/Remove Programs**. The Add/Remove Programs Properties dialog box is displayed.

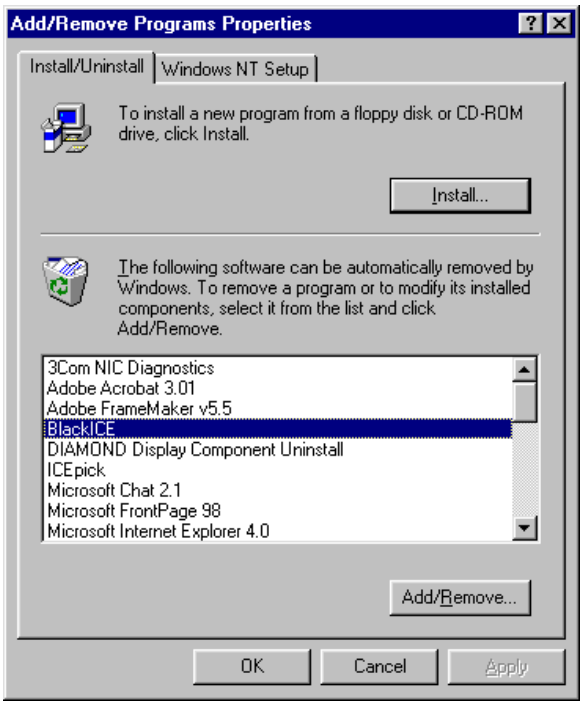


Figure 9 – The Add/Remove Programs dialog box.

3. Locate **BlackICE** in the list of programs.
4. Select **BlackICE** and click **Add/Remove**.
5. An introduction screen is displayed, click **Next** to continue.
6. An Setup window is displayed. **Select Remove BlackICE** <*version number*> and click **Next**.

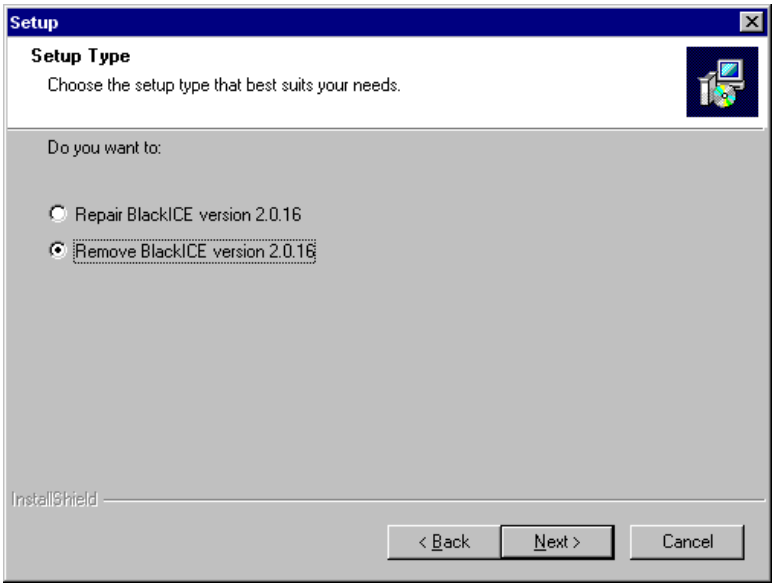


Figure 10 – Select Remove BlackICE.

7. You are prompted to confirm the removal of BlackICE. Click **Yes** to continue.
8. A status window is displayed. During the un-installation the application may prompt you regarding the state of read-only files. Click **Yes** to remove these read-only files. You may also be prompted regarding system files, click **Yes** to remove these files as well.

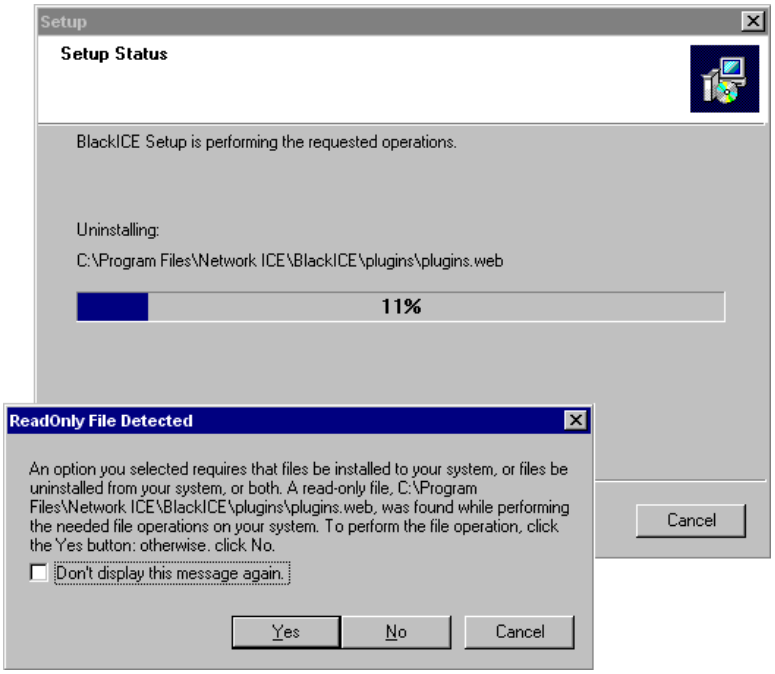


*Figure 11 – Click Yes to confirm the deletion of read-only files. Check the **Don't Display this message again** box to stop the setup program from prompting you about such files.*

9. Click **Finish** to conclude the removal.

HOW TO UPDATE BLACKICE

Network ICE issues regular updates to BlackICE to ensure it can detect and stop the latest attacks. The easiest way to update an existing installation of BlackICE is to use the **Download BlackICE Updates** option in the BlackICE menu.

1. From the BlackICE Summary application, click on the icon in the far left corner to display the main menu.
2. Select **BlackICE Utilities** and then select **Download BlackICE Update**.

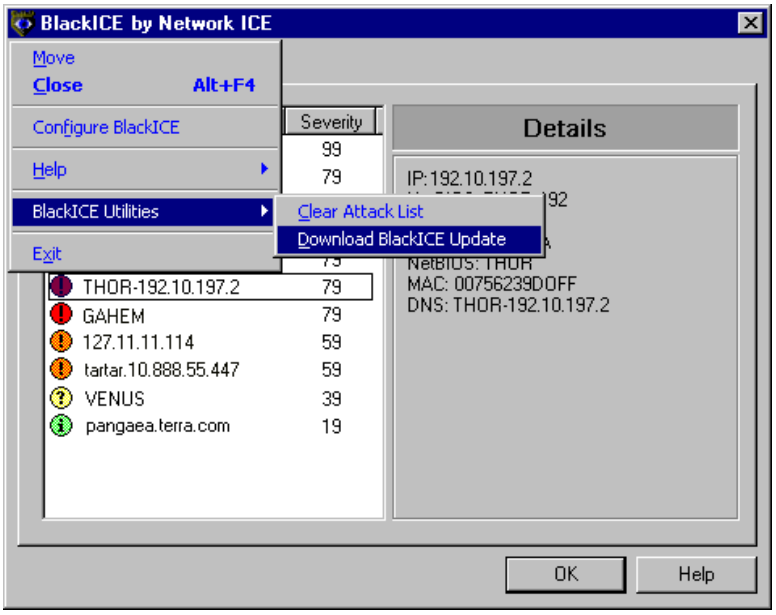


Figure 12 – Use the Download BlackICE Update feature to get the latest updates from Network ICE.

3. BlackICE checks the Network ICE web site for updates. If there are none available, a web page displays the installed version and license key values.

3 USING BLACKICE PRO

BlackICE consists of two main components: an invisible monitoring and protection engine and a summary application[2].

The monitoring and protection engine of BlackICE are always running when the computer is operating. This engine is "invisible" to ensure users do not accidentally or purposefully disable BlackICE.

The BlackICE summary application displays all the recent attacks on the system and intruders who made those attacks. It also includes a graph of all the recent network traffic and attacks.

The BlackICE summary application consists of three tabs reporting different information about the intrusions BlackICE has detected.

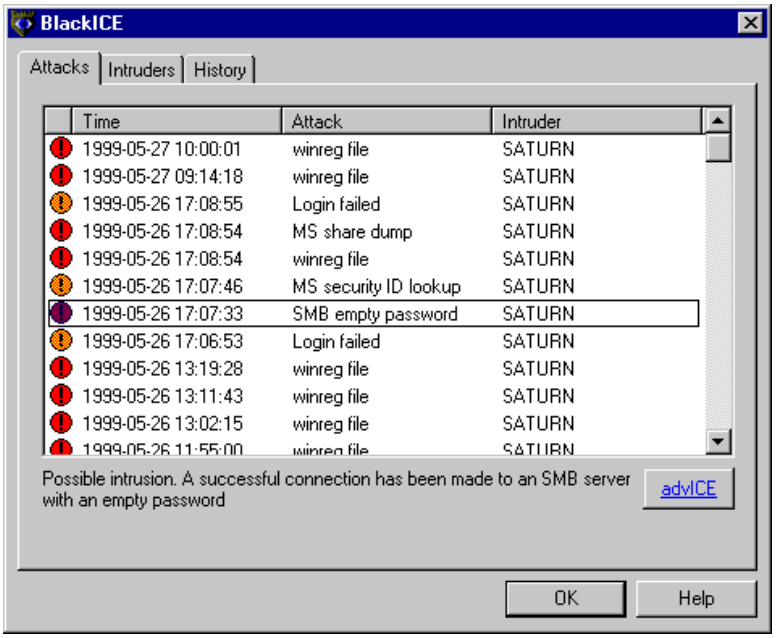


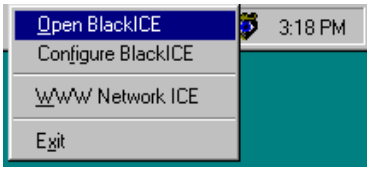
Figure 13 – The BlackICE application displaying the Attacks Tab.

This section describes how to use the BlackICE application as well as how to interpret the information displayed on each tab.

[2] The summary application is only available on systems where the BlackICE user interface is installed. "Silent" versions of BlackICE do not include the summary application.

HOW TO RUN THE BLACKICE SUMMARY APPLICATION

- If the BlackICE summary application has already been started, a small icon is displayed in the task-bar.



  - Right-click on the icon. A sub-menu of choices is displayed. Select **Open BlackICE**. You can also use this submenu to display the BlackICE Configuration features, access the Network ICE web site or Exit BlackICE.
  - A single regular click on the task-bar icon also opens the utility.
- If the tool is not already running, from the **Start** menu, select **Programs**, then select **Network ICE**, then select **BlackICE Utility**.

NOTE: Shutting down the BLACKICE.EXE application does not turn off the protection and detection engine of BlackICE. It merely closes the summary application. If you wish to completely disable BlackICE, please see page 41 for more information.

THE ATTACKS TAB

This tab summarizes all intrusion events on your system. The tab displays the time, type of event, and the intruder's name.

By default, the information in the Attacks tab is sorted first by time then by severity. Clicking a column header re-sorts the list by that column. Clicking the column header again toggles the sort order (ascending or descending).

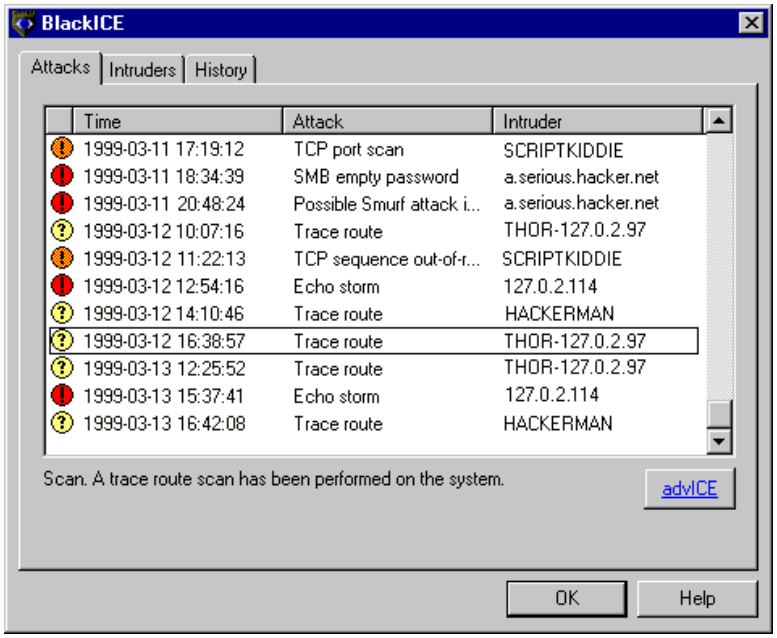


Figure 14 – Detected events are listed as critical, serious, suspicious, or informational on the Attacks tab.

Attack List Features

Indicator: Each event is indicated with one of four severity levels.

Icon	Severity	Description
	100 –75	**Critical event**: *Red exclamation point.* These are deliberate attacks on your system for the purpose of damaging data or crashing the system. Critical events always trigger protection measures.
	74 – 50	**Serious event**: *Orange exclamation point.* These are deliberate attempts to access information on your system, yet not directly damage anything. Some serious events trigger protection measures.
	49 – 25	**Suspicious event**: *Yellow question mark.* These are network activities that are not immediately threatening, but may indicate that someone is attempting to locate security vulnerabilities in your system. For example, hackers often scan the available ports or services on a system before attacking it. Suspicious events do not trigger protection measures.
	24 – 0	**Informational event**: *Green "i".* These indicate that a network event occurred that is not threatening but worthy of taking note. Informational events do not trigger protection measures.

Time: This is the time of the attack/event, listed in the format: `YYYY-MM-DD hh:mm:ss`. Time is in a 24-hour format for the time zone applicable to your system.

Attack: The name of the attack. For more information about a particular attack, select the attack in the list. A brief description of the attack is displayed at the bottom of the screen.

For a full description of an attack, as well as suggested remedies, see *Section 5: Handling Attacks* on page 45, or select the attack of interest and click the advICE button.

Intruder: The best name BlackICE can gather from the attacking system. This column displays the NetBIOS (WINS) name, DNS name, or IP address for the attacking system. If BlackICE cannot determine a name, it displays "unknown".

For more information about a particular intruder, double-click an event on the Attacks tab. The application displays the Intruders tab, which aggregates all known information about each intruder who has provoked an event on your system.

Ignore Attack: Right-click on any attack and select Ignore Attack from the pop-up menu to ignore a particular attack or a particular attack from a specific intruder. This is a useful way to stop BlackICE from reporting routine scans from ISPs or network probes.

Trust Intruder: Right-click on any attack and select **Trust** from the pop-up menu to trust the intruder. Once an intruder is trusted, all attacks from that intruder are totally ignored.

Clear Attack List: Right-click anywhere in the attack list and select **Clear Attack List** from the pop-up menu to remove all attacks from the attack list. Clearing the attack list does not change any blocked, trusted, or ignored intruders or attacks.

Other Attacks Tab Elements

Attack Description: Below the attack list, BlackICE displays a brief description of the selected attack. For additional information about the attack, click **advICE**.

advICE: Opens a browser session that accesses the advICE section of the Network ICE web site. Select the particular attack of interest and click the advICE button. Information about that specific intrusion is displayed.

OK: Closes the BlackICE summary application.

Help: Displays the on-line help for the Attacks tab.

THE INTRUDERS TAB

This tab aggregates information about all the intruders who have provoked events on your system. This tab is designed to help you determine the severity and location of each event.

By default, the information in the Intruders tab is sorted first by Intruder then by severity. Clicking a column header re-sorts the list by that column. Clicking the column header again toggles the sort order (ascending or descending).

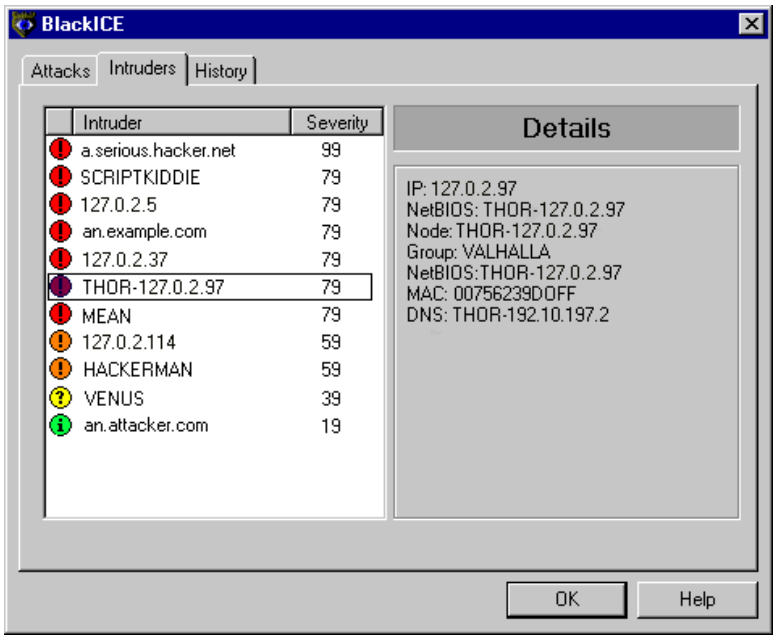


Figure 15 – Intruders tab.

Intruder List Elements

Indicator: Each entry is associated with one of four severity levels. The severity level reflects the most severe attack attributed to the Intruder.

Icon	Severity	Description
	100 –75	**Critical event**: *Red exclamation point.* These are deliberate attacks on your system for the purpose of damaging data or crashing the system. Critical events always trigger protection measures.
	74 – 50	**Serious event**: *Orange exclamation point.* These are deliberate attempts to access information on your system, yet not directly damage anything. Some serious events trigger protection measures.
	49 – 25	**Suspicious event**: *Yellow question mark.* These are network activities that are not immediately threatening, but may indicate that someone is attempting to locate security vulnerabilities in your system. For example, hackers often scan the available ports or services on a system before attacking it. Suspicious events do not trigger protection measures.
	24 – 0	**Informational event**: *Green "i".* These indicate that a network event occurred that is not threatening but worthy of taking note. Informational events do not trigger protection measures.

Intruder: The best name BlackICE can gather from the attacking system. This column displays the NetBIOS (WINS) name, DNS name, or IP address name for the attacking system. If BlackICE cannot determine a name, it displays *unknown*.

For more information on a particular intruder, select the intruder in the list. A description of all the information discovered about the intruder is displayed on the right side of the window.

Severity: The highest severity rating attributed to the intruder.

For more information about the activities of an intruder, double-click an entry on the screen. This takes you to the Attacks tab which displays all the attacks attributed to the selected intruder. The events are sorted first in alphabetic order by Intruder and then in descending order of severity.

Block Intruder: Right-click on any intruder and select Block from the pop-up menu to manually instruct BlackICE to block the intruder. A sub-menu lists choices for how long BlackICE should block the intruder: an *hour*, a *day*, a *month*, or *forever*.

Trust Intruder: Right-click on any intruder and select **Trust** from the pop-up menu to manually instruct BlackICE to trust all traffic from the system. Once an intruder is trusted, all attacks from that intruder are totally ignored.

Other Intruder Tab Elements

Details: Beside the Intruder List BlackICE displays all the back tracing information it has collected about the intruder. When BlackICE back traces an intruder it will attempt to gather the IP address, DNS name, NetBIOS name, Node Name, Group name and MAC address. Savvy hackers will likely block BlackICE from acquiring this information.

Back trace information is stored in standard text files in the Hosts folder in the directory where BlackICE is installed. Each file is prefixed with the intruder's IP address.

OK: Closes the BlackICE summary application.

Help: Displays the on-line help for the Intruders tab.

THE HISTORY TAB

This tab displays the recent activity on your system. These graphs are a good way to check for trends in hacking or scanning. For example, if many hacks are grouped together in the late hours of the night, there is a good chance that someone is trying to break into your system at that time.

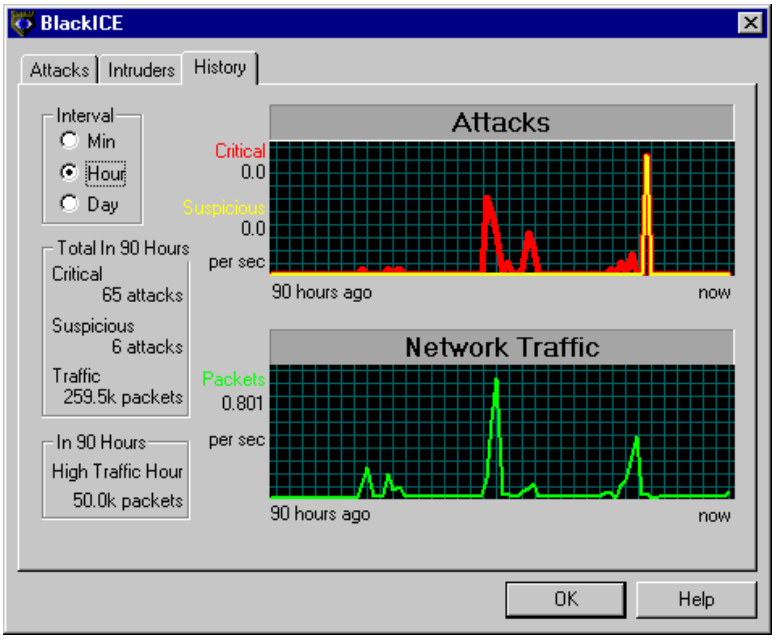


Figure 16 – The History tab is a good way to spot trends in intrusions.

History Tab Elements

Interval: Use these option buttons to select the interval for both graphs. **Min** displays the last 90 minutes of activity, **Hour** displays the last 90 hours of information, and so forth. BlackICE automatically displays the most informative interval.

Total Critical: The total number of events rated as *critical* for the selected interval. The events of this type are tracked on the Attacks graph with a red line.

Total Suspicious: The total number of events rated as *serious and suspicious* for the selected interval. The events of this type are tracked on the Attacks graph with a yellow line.

High Traffic: The highest amount of network traffic, measured in number of packets, for the selected interval. Traffic is tracked on the Network Traffic graph with a green line.

For more information about the attacks, single-click any point in either the **Attacks** or **Network Traffic** graphs. This takes you to the Attacks tab which displays the attacks in descending time order and focuses your attention on the attack which comes closest in time to the selected point in the graph. In a situation where a peak is displayed in the Attacks graph, you can click on the peak and zero in on what attacks occurred during that time.

OK: Closes the BlackICE summary application.

Help: Displays the on-line help for the History tab.

HOW TO BLOCK AN INTRUDER

BlackICE does not automatically block every intruder that attacks your computer. Only attacks that are a direct and immediate threat to the functioning of your system are block. However, you can manually block intruders.

WARNING: Be careful which systems you block. Nearly all Internet Service Providers (ISPs) conduct routine scans to check the state of connected clients. This is especially true of high-speed providers such as @Home and GTE. If you block your ISPs scans they might restrict your access or even terminate your account. For help identifying your ISPs systems, contact your ISP. Typically ISPs use DNS names that identify themselves as a member of the ISPs domain. For example, most @home systems have `.home.com` in their DNS name.

---

1. From the **Intruder** tab, right click on the intruder you wish to block.
2. From the pop-up menu, select **Block Intruder**.
3. A secondary menu pops up. Select the duration of the block: *For an Hour*, *For a Day*, *For a Month (30 days)*, or *Forever*.

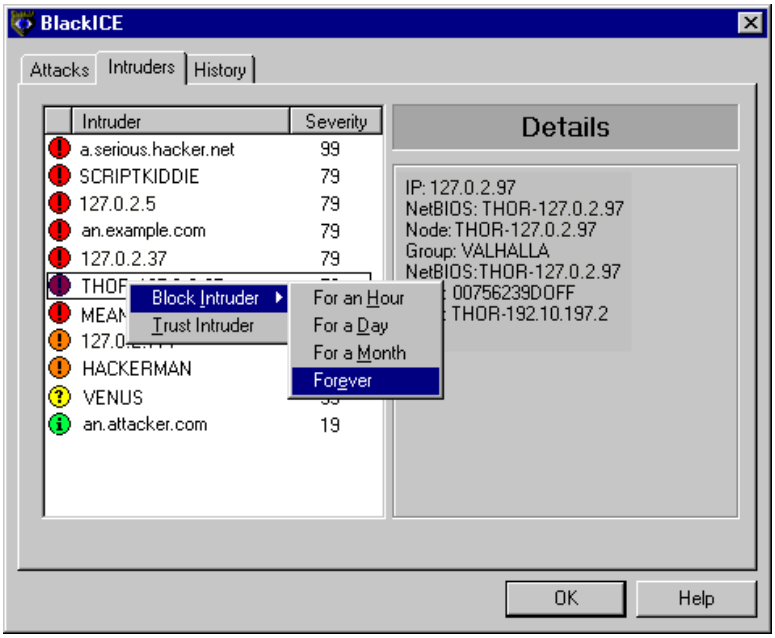


Figure 17 – You can use the Intruder's tab to manually block an intruder.

- BlackICE adds the intruder to the Blocked Addresses tab. To unblock an intruder see page 37 for more information.

HOW TO TRUST AN INTRUDER

Use this feature to instruct BlackICE to trust a system that has initiated an attack. Only trust those systems that you are certain are legitimately executing network scans such as servers from your ISP or an ICEscan server.

WARNING: Be careful which systems you trust since hackers can sometimes "spoof" legitimate addresses. Network ICE recommends only trusting those systems that are authorized to "hack" systems such as an ICEscan vulnerability scanner.

1. From the **Intruder** tab, right click on the intruder you wish to trust.
2. From the pop-up menu, select **Trust Intruder**.

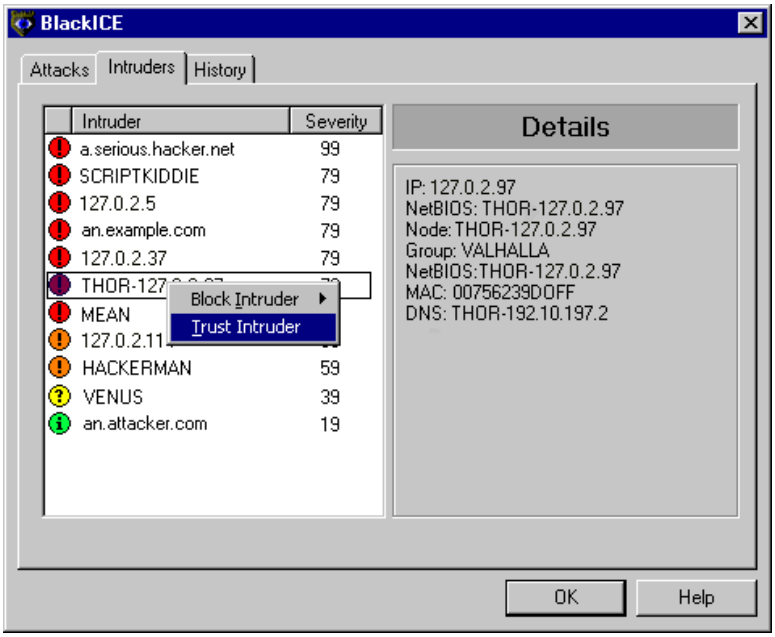


Figure 18 – Use the Intruder tab to manually trust an address.

- BlackICE adds the intruder to the Trusted Addresses tab. To "untrust" an intruder please see page 35 for more information.

How to Ignore an Attack

1. Use this feature to ignore an attack or an attack from a specific intruder. Be careful which attacks you ignore. See page 6 for more information about ignoring attacks.
2. From the **Attacks** tab, right click on the attack/intruder combination you wish to ignore.
3. From the pop-up menu, select **Ignore Attack**.
4. A sub-menu is display, select how you want BlackICE to ignore the attack.
   This Attack instructs BlackICE to ignore all future instances of the attack.
   This Attack by this Intruder instructs BlackICE to ignore all future instances by the referenced intruder. Other intruders for that attack will continue to be logged.

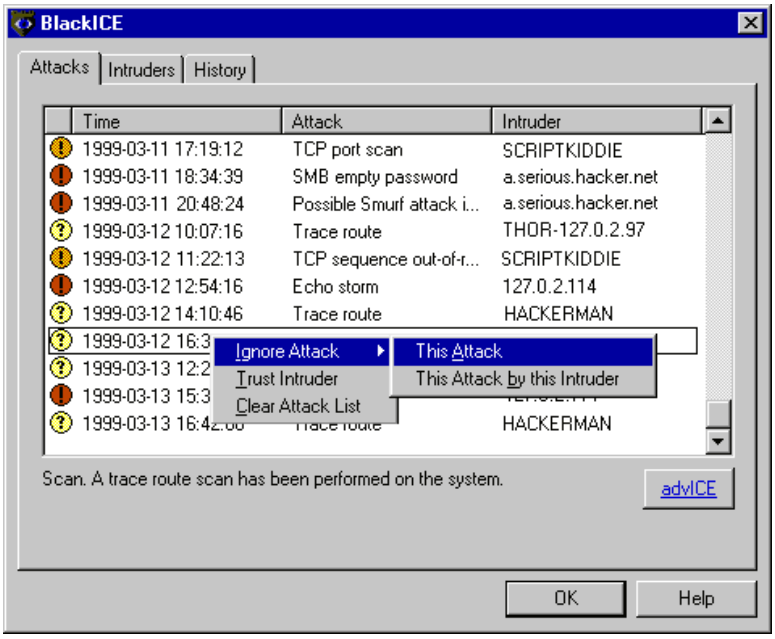


Figure 19 – Use the Attacks tab to ignore attacks.

- BlackICE begins ignoring the attack you selected immediately.

HOW TO CONFIGURE BLACKICE

This section describes how to customize the monitoring, detection, and use of BlackICE

You can access the Configuration dialog box two ways, from the Windows task bar or from the BlackICE summary application.

1. From the Windows Taskbar, right-click on the BlackICE icon.

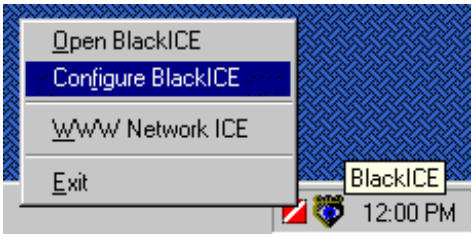


Figure 20 – From the desktop, right click on the BlackICE icon in the system tray.

OR, within the BlackICE Summary Application, click the BlackICE icon in the far left corner.

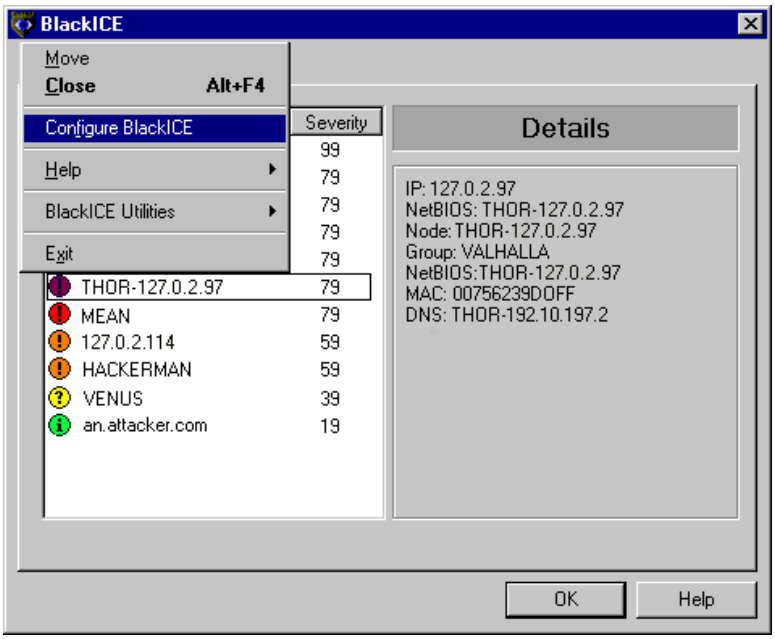


Figure 21 – Within the summary application, use the BlackICE icon in the far left corner.

2. Select BlackICE Configuration from the pop-up menu. The BlackICE Configuration window is displayed. The following sections detail each tab on this window.

Back Trace Tab

When BlackICE's monitoring engine detects a suspicious event, it immediately starts collecting information. One way BlackICE can locate an intruder is using a networking procedure called *backtracing*.

Backtracing is the process of tracing network connection back to its origin. When somebody connects to your computer via a network such as the Internet, your system and the intruder's system exchange packets. Before an intruder's packets reach your system, they travel through several routers. BlackICE can strip information off these packets and determine each router the intruder's packets had to travel or "hop" through. Eventually, BlackICE can "hop" all the way back to the intruder's system.

There are two ways that BlackICE can backtrace information: *directly* or *indirectly*.

An *indirect trace* uses protocols that do not make contact with the intruder's system, but collect information indirectly from other sources along the path to the intruder's system. On the other hand, a *direct trace* goes all the way back to the intruder's system to collect information. Direct traces generally gather more reliable information than indirect traces.

Hackers cannot detect any indirect tracing. However, direct traces can be detected an blocked by the hacker. Fortunately, most hackers are not experienced enough to block direct traces.

The Back Trace tab allows you to view and modify the configuration parameters that control the backtracing functions of BlackICE.

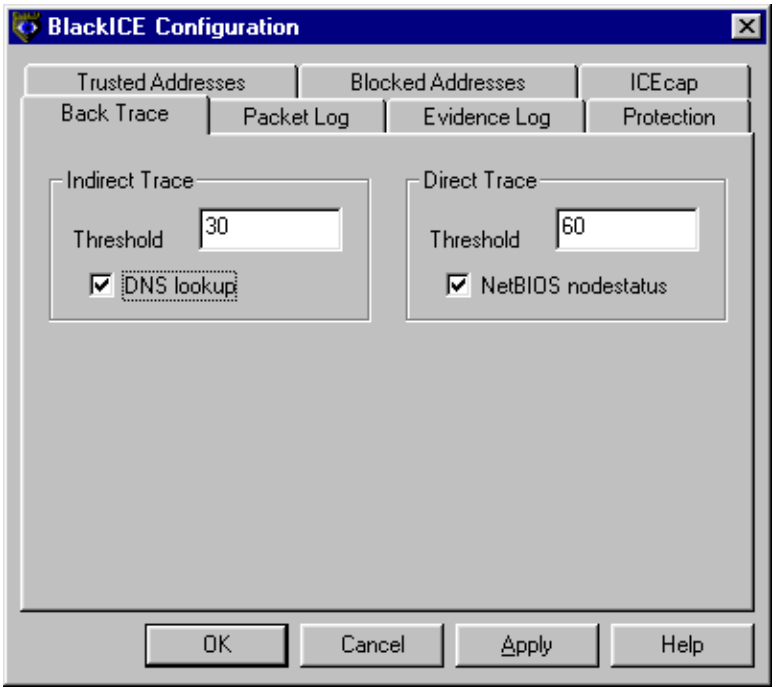


Figure 22 – Backtrace tab.

Indirect Trace

The Indirect Trace parameters establish how BlackICE executes indirect backtracing. Because indirect backtracing does not make contact with the intruder's system it does not acquire much information. Therefore, it is best for lower severity attacks.

Threshold: Indicates the attack severity level that will trigger an indirect trace of the attack.

Severity refers to the level of each attack. The following list summarizes how BlackICE categorizes severities. The default attack severity for the indirect trace threshold is 30.

Icon	Severity	Description
	100 –75	**Critical Event**: This is a deliberate attack on your system for the purpose of damaging data or crashing the system.
	74 – 50	**Serious Event**: This is a deliberate attempt to access information on your system, yet it does not directly damage anything. These events can trigger protection measures, if applicable.
	49 – 25	**Suspicious Event**: This is network activity that is not immediately threatening but may indicate that someone is attempting to locate security vulnerabilities in your system. For example, hackers often scan the available ports or services on a system before attacking it. Suspicious events do not trigger protection measures, and not all suspicious events are indicative of a true attack.
	24 – 0	**Informational Event**: This indicates that a network event occurred to your computer that is not threatening. Informational events do not trigger protection measures.

DNS LookUp: When checked, BlackICE queries available DNS (Domain Name Service) servers for information about the intruder. The DNS Lookup is enabled by default.

Direct Trace

The Direct Trace parameters establish how BlackICE executes direct backtracing. Because direct backtracing makes contact with the intruder's system it acquires a great deal of information. Therefore, it is best used for high severity attacks.

Threshold: The attack severity level that triggers a direct trace of the intruder. The default attack severity for the direct trace threshold is 60.

NetBIOS NodeStatus: When checked, BlackICE performs a NetBIOS lookup on the intruder's system. The NetBIOS Node Status is enabled by default.

Packet Log Tab

The Packet Log tab allows you to configure the packet logging features of BlackICE.

When packet logging is enabled, BlackICE records the system traffic into log files. Files are filled until a maximum size is reached. Then a new file is generated until the maximum files are used. Then BlackICE starts over replacing the first log file with a new file.

It is important to note that packet logging keeps track of ALL system traffic, not just intrusions. Therefore, packet logs can become very large and consume a great deal of system resources. However, if you are having repeated intrusions on a system, packet logging can help gather additional information about activity on the system.

Packet logs are encoded as "sniffer" style trace files. You will need a decoding application, such as Network Monitor included with Windows NT Server, to view the contents of these files. The file extension for all packet log files is `*.enc`.

BlackICE also captures network traffic specifically when an intrusion is detected in Evidence Files.

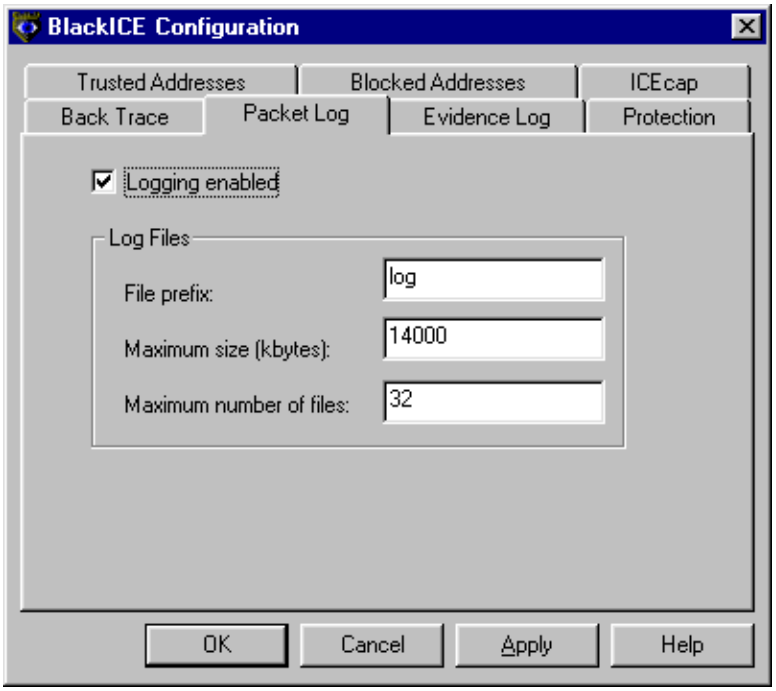


Figure 23 – The Packet Log tab.

Logging Enabled: When checked, BlackICE captures packet logs. Packet logging is disabled by default.

File Prefix: Specifies the prefix for the packet log file names. BlackICE automatically places an incremented counter in the filename. For example, if you enter `ABC` the file names will be `ABC0001.enc`, `ABC0002.enc`, etc. The default file prefix is `log`.

Maximum Size (kbytes): Specifies the maximum size, in kilobytes, for each log file. The default value is 1400 kilobytes.

Maximum Number of Files: Specifies the maximum number of log files to generate. The default value for the maximum number of files to log is 10.

Evidence Log Tab

When BlackICE detects suspicious activity it immediately begins collecting information about the event. This information is encoded into an evidence file. An evidence file is a raw dump of all network traffic relevant to a specific attack.

Evidence files are not the same as packet logs. The packet log is a summary of all inbound and outbound traffic on the system. An evidence file zeros in on the traffic associated with a specific attack.

BlackICE captures evidence files in a "round-robin" fashion. It collects files until the maximum number of files are used then recycles to the first file and replaces it with a new one.

Evidence files are encoded as "sniffer" style trace files. You will need a decoding application, such as Network Monitor included with Windows NT Server, to view the contents of these files. The file extension for all packet log files is `*.enc`.

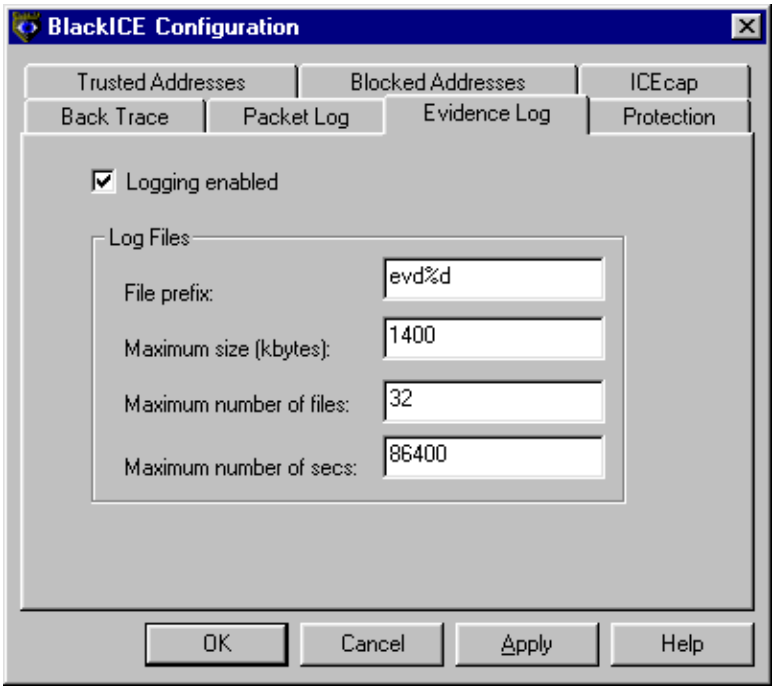


Figure 24 – The Evidence Log tab.

Logging Enabled: When checked, BlackICE collects evidence files for suspicious events. Evidence logging is enabled by default.

File Prefix: Specifies the prefix for the evidence file names. Use `%d` to place an incremented counter in the file name. For example, if you enter `XYZ%d` the file names will be `XYZ0001.enc`, `XYZ0002.enc`, etc. The default file prefix is `evd%d`.

Maximum Size (kbytes): Specifies the maximum size, in kilobytes, for each evidence file. The default is 1400 kilobytes.

Maximum Number of Files: Specifies the maximum number of evidence files to generate. When BlackICE reaches the maximum file, it recycles to the beginning of the file list. The default value for the maximum number of evidence files to log is 32.

Maximum Number of Secs: Specifies the maximum time period the evidence file reflects. For example, the default setting is 86400 seconds. This would result in a separate evidence file for each 24 hour period.

Protection Tab

The Protection tab establishes the Security Level BlackICE should enforce on the system. There are four pre-set security levels, as defined below.

Trusting: When set to *Trusting* all ports remain open and unblocked. This setting is good if there is minimal threat of intrusions.

Cautious: The *Cautious* setting is good for regular use of the Internet. This setting only blocks inbound intrusions on System Port(s). All other ports remain unblocked and therefore should not interfere with any Internet usage.

Nervous: This setting is preferable if you are experiencing repeated intrusions. For the *Nervous* setting, BlackICE blocks inbound intrusions on all the System ports and TCP Application ports. This setting may restrict some interactive content on web sites. Streaming media and other "application specific" Internet usage remains unaffected.

Paranoid: The *Paranoid* setting is very restrictive, but useful if your system has endured numerous attacks. Under this setting BlackICE blocks all inbound intrusions. This setting may restrict some web browsing and interactive content.

For more information about how security levels work, see page 6.

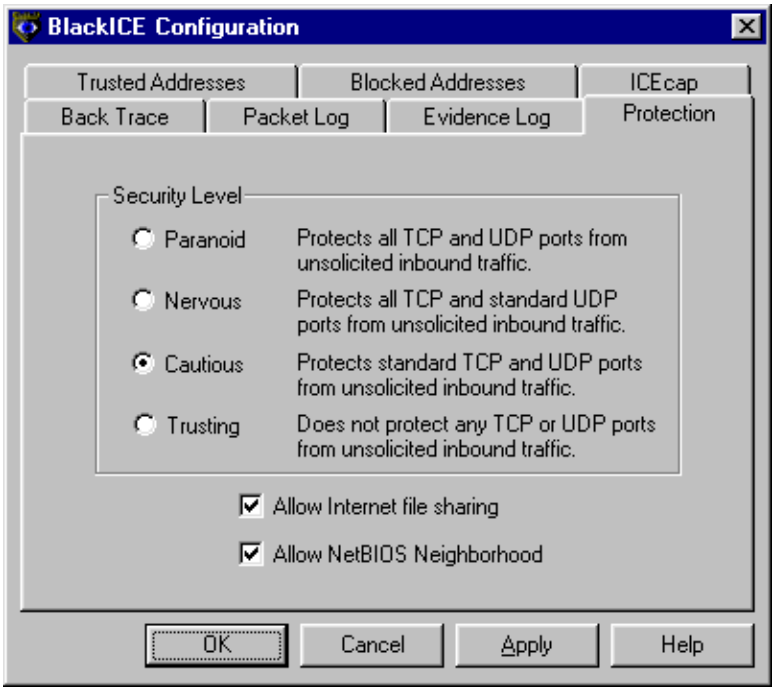


Figure 25 – The Protection Tab

Other Items

Allow Internet File Sharing: Uncheck this box to prevent systems from connecting to your system and accessing shares. By default this item is enabled.

WARNING: Disabling Internet file sharing may inhibit the ability of an ICEcap server to manage the remote BlackICE agent including issuing downstream protection measures. If you choose to disable this feature, make sure the ICEcap server uses a static IP address and that all BlackICE agents implicitly trust the ICEcap server's IP address. On an internal network it is preferable to leave file sharing enabled, but implement strong security passwords on those shares.

Allow NetBIOS Neighborhood: Check this box to report your system (NetBIOS) name to the Windows Network Neighborhood. Uncheck to hide your system name from this feature. If your network uses NetBIOS names to access file shares, you will need to keep this option enabled. Otherwise, you will have to use IP addresses to access the file shares. This option is enabled by default.

NOTE: If you enable the Internet file sharing but not the NetBIOS Neighborhood, you must use an IP address to remotely access your system.

Setting the Security Level

1. Select the **Security Level** you wish to use. The default Security Level is **Trusting**.
2. If you wish to disable file sharing over the Internet, uncheck the **Allow Internet File Sharing** box. Internet file sharing is enabled by default.
3. Check the **Allow NetBIOS Neighborhood** if you want your system to appear in the Network Neighborhood window. Uncheck the box to hide your system from browsing.
4. Click **Apply** to begin using the new security level.

Trusted Addresses Tab

The Trusted Addresses tab allows you to identify network addresses to exclude from all BlackICE monitoring and protection. When an address is trusted, BlackICE considers all network traffic from that address to be safe.

NOTE: Be very careful which systems you tell BlackICE to trust. A trusted system is completely free from any monitoring or protection.

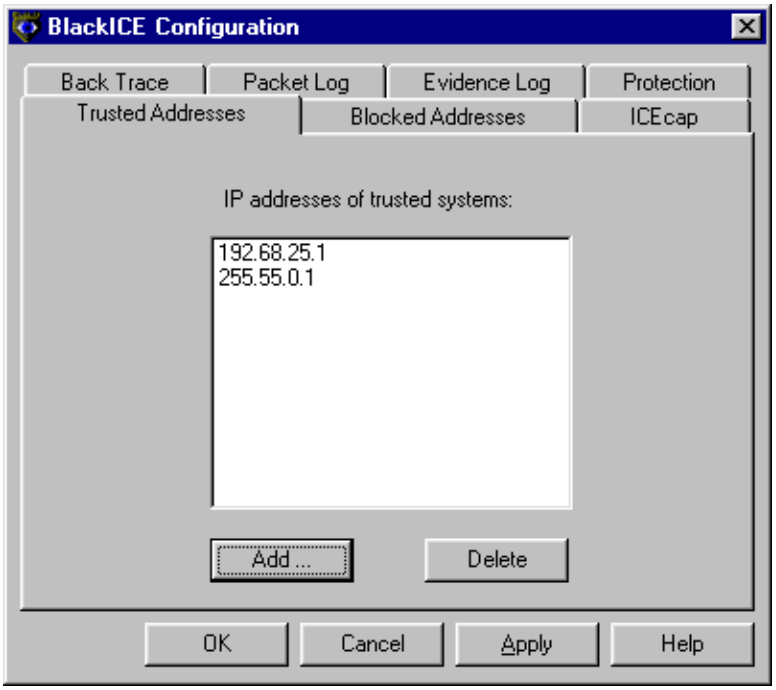


Figure 26 – Trusted Addresses tab.

IP addresses of trusted systems: Displays a list of the IP addresses of trusted systems. The default setting has no entries.

Add: Click to display the **Add** dialog box. Enter the IP address of the system you wish to exclude from all BlackICE monitoring and protection (the trusted system) and click **Add**.

Delete: Select an address in the list you wish to delete and click **Delete**. The address is deleted immediately from the trusted addresses list.

Adding a New Trusted Address

1. Click **Add** to place a new trusted address in the list. The IP Address to Trust dialog box is displayed.

Figure 27 -- IP Address to Trust dialog box.

2. Enter the **IP address** for the system you wish to trust.
3. Click **Add**. The new trusted address is added to the list.

Editing a Trusted Address

To change an address, delete the existing record and add a new one.

Deleting a Trusted Address

1. Click on the address entry you wish to delete.
2. Click **Delete**.

Blocked Addresses Tab

The Blocked Addresses tab shows you the network addresses that BlackICE is blocking. BlackICE rejects all network traffic from blocked IP addresses. This identifies the current hackers.

Blocked addresses have a specific end time, which can be a few minutes or a few days.

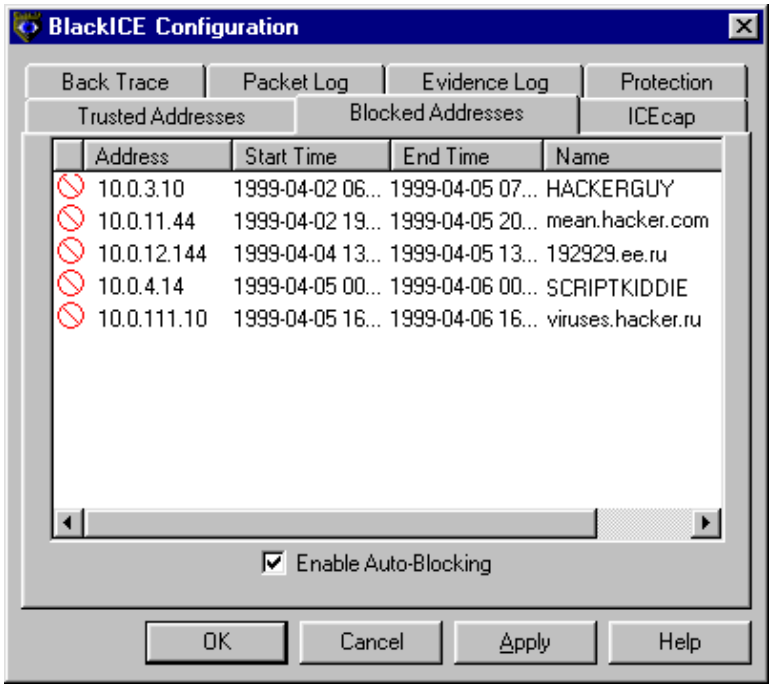


Figure 28 – Blocked Addresses tab.

- **Address**: The blocked address(es). The default setting has no entries.
- **Start Time**: The date and time the address was first blocked. The format is: `YYYY-MM-DD hh:mm:ss`. The time is in 24 hour format for the time zone applicable to your system.
- **End Time**: The date and time the address block will expire. The format is: `YYYY-MM-DD hh:mm:ss`. The time is in 24 hour format for the time zone applicable to your system.
- **Name**: The best name BlackICE discovered for the blocked system. This may be a DNS or NetBIOS (WINS) name. If BlackICE cannot determine the name of the system, the column is left blank.
- **Unblock and Trust**: Right-click on any blocked address to display a pop-up menu with the choice Unblock and Trust. This converts a blocked address to a trusted address.
- **Enable Auto-Blocking**: Leave this box checked to have BlackICE automatically block hackers when they attempt to break into your system. Unchecking this box disables auto-blocking. Attacks are still reported and logged, but not blocked.
- Clicking a column header sorts the block list by that column. Click again to toggle between ascending and descending sort orders.

Unblocking an Address and Changing it to a Trusted Address

This option is handy if BlackICE inadvertently blocks legitimate use of your system from another computer. However, you should only trust addresses that are from known systems. Advanced hackers can masquerade as a trusted address to crack into your system, so use this feature carefully.

1. Right-click on the blocked address entry you wish to change.
2. Select **Unblock and Trust** from the pop-up menu. The selected address is immediately removed from blocking, and then trusted. Note that once **Unblock and Trust** is selected, this action cannot be reversed. You can delete trusted addresses if necessary from the Trusted Addresses tab. See page 35 for more information.

ICEcap Tab

BlackICE Pro integrates with an ICEcap server for centralized reporting and analysis of network intrusions. ICEcap is intended for use on internal networks (or LANs) where more than one system is connected to the Internet. For more information about how BlackICE and ICEcap can help manage your network, download a copy of the ICEcap documentation from Network ICE at www.networkice.com.

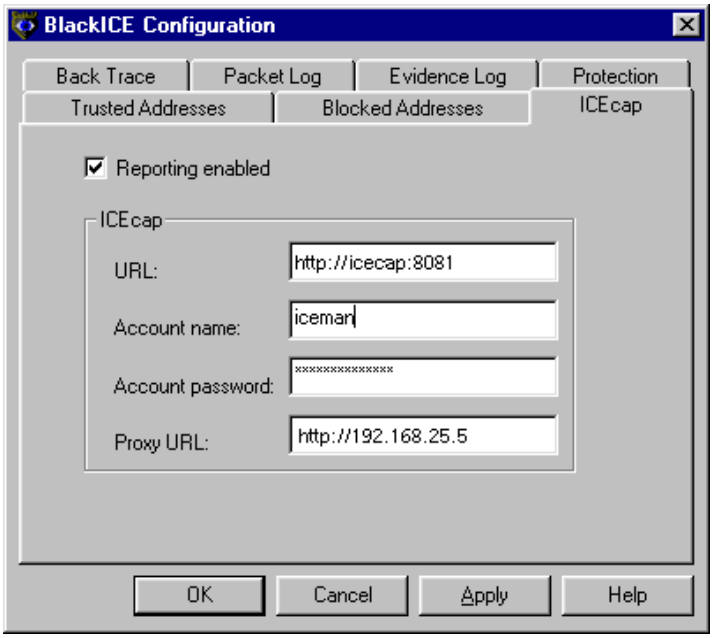


Figure 29 – ICEcap tab.

Reporting Enabled: Check this box to activate ICEcap reporting. Uncheck to turn off ICEcap reporting.

URL: The fully qualified URL for the ICEcap server in the format `http://<ICEcap server name>:<TCP port number>`. For example, if ICEcap was on a server named ICECAP using TCP port 8081, the entry would be: `http://ICECAP:8081` (the default).

Account Name: The ICEcap account name to use when uploading data. Refer to your ICEcap documentation for more information about account names. The default account name is "iceman".

Account Password: Enter the current password BlackICE is using to report information to ICEcap. Changing the password here does not change the account password in ICEcap. If BlackICE is not reporting any information to ICEcap, leave this field blank.

Proxy URL: If there is a proxy server between the BlackICE system and the ICEcap server, enter the fully qualified URL for the proxy server.

HOW TO CLEAR THE ATTACK LIST

After a while the attack list may become rather long. Use this feature to clear out the attack list.

NOTE: Clearing the attack list does not unblock or un-ignore any attacks or intruders.

1. From BlackICE Summary Application, click on BlackICE icon in the left corner.
2. From the pop-up menu, select **BlackICE Utilities**.
3. A sub-menu is displayed, select **Clear Attack List**.

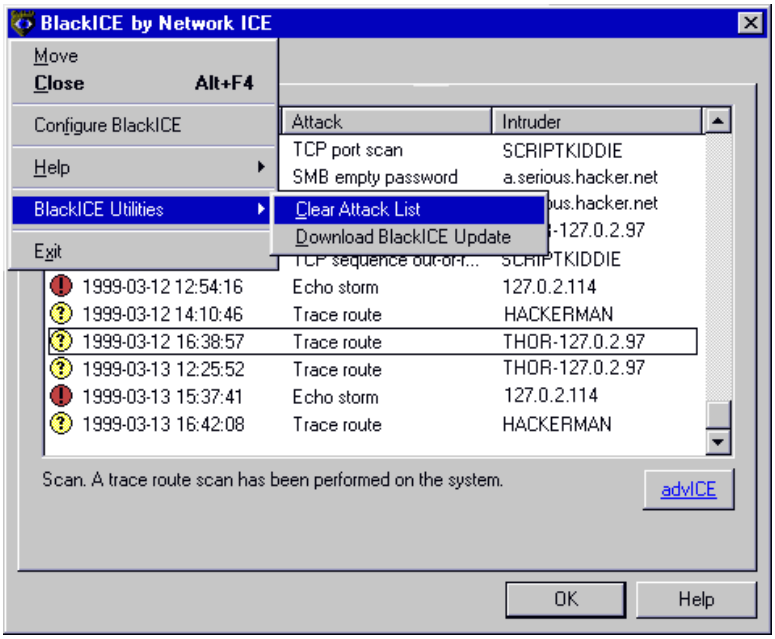


Figure 30 – Use the main menu to clear the attack list.

- BlackICE clears out the attack list. You can also right-click on any attack in the Attacks list and select Clear Attack List from the pop-up menu.

How to Update BlackICE

The BlackICE On-Line Update web page can automatically check your copy of BlackICE to see if you have the most recent version.

This utility downloads the latest BlackICE software (including intrusion detection files) from the Network ICE web site.

If you are using ICEcap to manage BlackICE agents, it is best to bulk deploy the updated files from the ICEcap management console. For more information about the bulk deployment features of ICEcap, refer to the ICEcap Administration Guide.

To Update BlackICE

1. Right-click on the BlackICE icon in the far, left corner of the BlackICE Summary Application.
2. Select **BlackICE Utilities**, then select **Download BlackICE Update** from the sub menu.

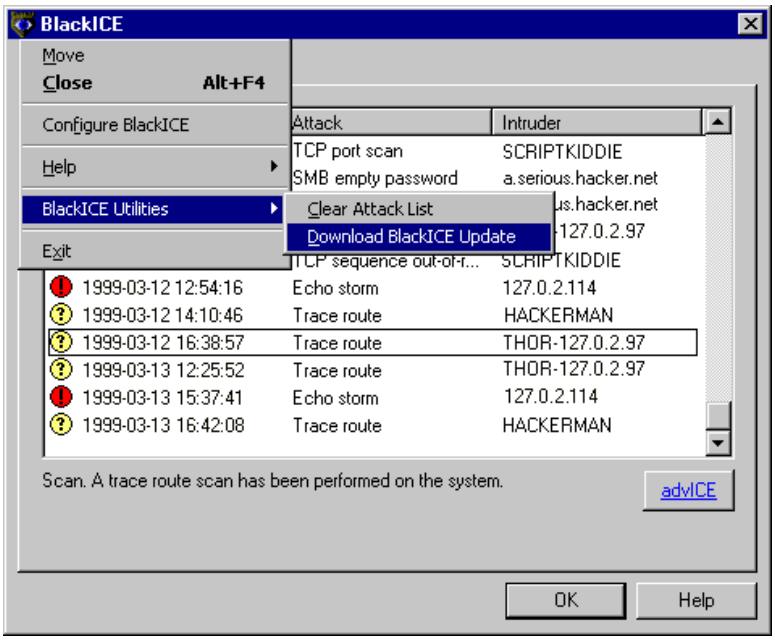


Figure 31 – Download BlackICE Update.

3. BlackICE opens a web browser session and connects to the Network ICE web site. The site checks your version against the Network ICE database. If there is a newer version available, a link is displayed to download the update. Click the link to download the update.

   If you have the latest version, the web page displays your version number and license key.

HOW TO DISABLE BLACKICE

Although it is not recommended, there may be special circumstances that require you to disable BlackICE on a system. When BlackICE is disabled, the system is not protected from any network intrusions.

To ensure that BlackICE is not disabled by a hacker, only a user sitting at a workstation or server can disable BlackICE on the system. The ICEcap management console cannot remotely disable BlackICE, although it can uninstall the software.

NOTE: Shutting down the BLACKICE.EXE application does not stop the BlackICE monitoring and protection engines. It merely exits the summary application.

If you wish to completely remove BlackICE from your system please see page 15 for more information.

For Windows NT Workstation or Server

1. From the **Start** menu, select **Settings**.
2. Double-click **Services** on the Control Panel. The Services dialog box is displayed.
3. Locate the **BlackICE** service and click **Stop**.

- Windows NT stops the service. BlackICE will restart when the system is rebooted or restarted from the Services dialog box.

For a Windows 95/98 System

1. Press [CTRL] [ALT] [DEL] keys simultaneously.
2. A Close Program dialog box is displayed.
3. Select **blackd.exe** in the list and click **End Task**.

- Windows 95/98 stops the BlackICE monitoring and protection engine, however BlackICE will restart when the system is rebooted.

4 BlackICE Features

The BlackICE product line consists of five specialized versions of BlackICE. Each version is suited for a different task. The following chart summarizes the features available in each version. The remainder of this chapter describes those features and how they can make your network and computer safe from hackers.

Feature → Version ↓	Attack Protection	ICEcap Integration	Wire Tapping
Defender	✓		
Pro / Auditor	✓	✓	
Sentry	✓	✓	✓

ICEcap Integration

Keeping track of hundreds of workstations is a difficult job. To help make this job easier, BlackICE Pro and Sentry feature ICEcap integration. ICEcap is a server-based Network ICE product that aggregates and compiles information from multiple BlackICE Pro and Sentry installations on a network.

Since many hackers will systematically sweep your network looking for holes, ICEcap affords you a strategic view of your network and what hackers are doing. For example, one of the most common ways to find holes in a network is to sweep through all the TCP ports open on each system. To an individual system, this is not considered a serious attack. But, when all the BlackICE installations in a subnet are suddenly reporting TCP port scans, something sinister may be afoot.

Only an ICEcap server can see these "network wide" trends and issues. ICEcap was designed from the ground up to work as a single information source. You can log-on to the server using a standard web browser and in minutes see all the attacks on all the systems on the network where BlackICE is installed. This information can be displayed for many different intervals, allowing you to spot trends. Are your systems getting hacked every Saturday night at 2:00 am? Are all the attacks coming from a particular domain? Information such as this can help you track down hackers and stop them cold.

ICEcap can also initiate down-stream protection on any BlackICE Pro or Sentry installation. Since ICEcap might detect an attack that each BlackICE installation missed, the protection features of BlackICE would not have blocked out the IP address of the attacker. ICEcap can order all BlackICE installations to stop any IP address.

Lastly, ICEcap uses standard technologies. The ICEcap database uses Microsoft SQL Server 6.5-7.0 or Microsoft Access 97 (or better). Access to reports and information is handled through any web browser such as Internet Explorer or Netscape Navigator. ICEcap also does not require a web server. The application includes its own web server specifically configured for BlackICE and ICEcap use only. This ensures that hackers do not submit false information to the ICEcap server to mask their activities.

DETECTION

BlackICE detection features comprise the core of the BlackICE product. It is available on all versions of BlackICE.

The BlackICE detection engine constantly monitors the ports and services on a system. If a suspicious event is detected, BlackICE analyzes the traffic using a series of advanced algorithms and dynamic filters to determine if the event is a serious attack or a legitimate use of the system. Depending on the configuration settings, BlackICE can also open an evidence file to collect all network traffic related to the intrusion.

The detection features of BlackICE are virtually undetectable to a hacker. BlackICE runs "silently" and "invisibly" on a system. It has a small memory footprint and is not easily disabled. Only a user physically located at the computer can disable BlackICE.

Lastly, if your network has an ICEcap server, the most important information is forwarded to the ICEcap server for analysis and reporting purposes.

PROTECTION

The BlackICE protection engine is composed of two parts: a *standard protection filter*, and a *dynamic protection filter*.

The *standard protection filter* stops many common attacks before they can ever get started. This includes stopping corrupt packets, badly fragmented packets, and many other potentially intrusive network traffic. The standard filters include configurable filters for IP addresses, TCP ports, and TCP SYN packets.

The dynamic protection filter works much like an IP address filter used on routers and other network devices. When an attack is detected, BlackICE adds the hackers IP address to a dynamic address filter table. Regardless of what the hacker does, any traffic from the hacker's IP address is rejected.

After 24 hours, if the attacker does not return, the IP address is removed from the filter. Since many hackers *spoof* legitimate IP addresses, this stops the hacker from getting into your system but does not permanently stop legitimate use of your system.

For example, your local network uses the IP address series 10.0.0.1 through 10.0.0.255. A hacker tries to attack a Windows NT Server with the IP address 10.0.0.10 using the spoofed IP address 10.0.0.66. Without BlackICE, the NT Server would consider the IP address 10.0.0.66 part of its subnet, and might let that system access resources on the server. However, since BlackICE determines that the packets from 10.0.0.66 are trying to break into the server, it automatically blocks all access from the 10.0.0.66 address for 24 hours. After 24 hours, the IP address is released, and the legitimate system assigned to the IP address 10.0.0.66 can resume using the resources on the NT Server.

If your copy of BlackICE is integrated with an ICEcap server, a detailed record of the attack is uploaded from BlackICE to the ICEcap database. Using the reports and tools included with ICEcap, a network administrator can see exactly what happened for this attack and any other attacks. Armed with the information ICEcap aggregated from all BlackICE installations, a network administrator can reconfigure the network routers or switches to stop packets coming in through a firewall or other connection.

Additionally, an ICEcap server can remotely initiate the protection filters on all BlackICE Pro installations. Since ICEcap can sometimes detect attacks that an individual BlackICE installation might miss, this feature allows network administrators the ability to manually invoke protection measures BlackICE overlooked.

WIRE TAPPING

A single workstation with BlackICE Pro monitors the traffic addressed specifically to that workstation. Since it is not possible to install BlackICE on all networked devices (such as printers or hubs) BlackICE Sentry was designed to actively monitor all traffic on a network segment. This "promiscuous" packet capture feature allows BlackICE Sentry to locate intrusions and scans on all devices within a monitored segment.

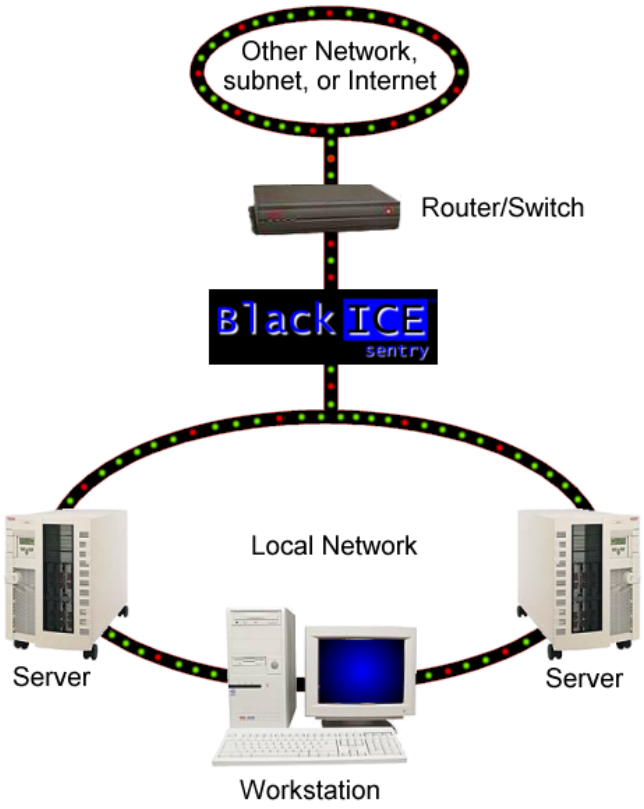


Figure 32 – BlackICE Sentry works like an advanced wire tap, monitoring all traffic on a subnet.

BlackICE Sentry is ideal for monitoring network traffic over slower Internet connections or firewalls. BlackICE Sentry can also be used as a "front-door" monitoring all packets that are going into or out of an important subnet. For example, if you had a large mainframe connected to your TCP/IP network you could install a BlackICE Sentry on the Mainframe's subnet and it would keep track of all the packets moving into and out of the mainframe.

When BlackICE Sentry detects a suspicious packet, it immediately captures as much information as possible about the intruder. This information is uploaded to an ICEcap server for reporting and analysis. With this information, you can configure filters, routers, and firewalls to stop the intruder.

To ensure that BlackICE Sentry does not slow down the network, it does not function as a packet filter. Therefore it cannot stop intrusive traffic like BlackICE Defender or Pro.

5 HANDLING ATTACKS

The Internet is a big place. Along with all the great web sites and information on the Internet, there are also people who are committed to causing trouble.

WHAT HACKERS CAN DO

Most hackers are inexperienced kids looking for fun. They merely want to show off to their friends that they could hack into a system. Unfortunately, even the most inexperienced hacker can cause severe damage.

Corporations have long known about the risks hackers present to their business. However, most home office and casual computer and Internet users are unaware what hackers can do. Hackers can render your computer totally unusable. They can steal or delete data. Hackers that are able to steal your digital identity can make financial transactions on your behalf, such as buying or selling securities or using your credit cards. A resourceful hacker can cause tremendous financial damage to anyone who uses the Internet.

In a 1997 report to a subcommittee of the United States Senate, Robert S. Litt, Deputy Assistant Attorney General stated, "Public reports have estimated that computer crime costs us between $500 million and $10 billion dollars per year. The Computer Security Institute has surveyed 428 information security specialists in Fortune 500 companies; 42% of the respondents indicated that there was an unauthorized use of their computer systems in the last year."

There are countless stories of hacker communities targeting companies and organizations for any number of personal and political reasons. In 1997 a London trading firm was forced to pay millions of dollars to an unknown group of foreign extortionists who demonstrated that they could wipe out entire systems at will. These extortionists were never captured and the trading firm learned an expensive lesson in network security.

Contrary to what the movies or "cyberpunk" books might depict, not all hackers are kids trying to deface web sites or steal credit card numbers. Many hackers are dedicated criminals and corporate spies trying to steal valuable information from companies and individuals. In the race to build faster and better networks, many companies forget to erect barriers to stop the hackers. Moreover, many home users are completely unaware of the threat of hackers and thus easy targets for hacking.

Of recent concern is *cyberterrorism*. What terrorists cannot accomplish with propaganda or cruise missiles, they sometimes can with computers. Many rogue states are or suspected to be engaged in terrorist activities designed specifically to disrupt or destroy the ability of a country and its corporations to function.

How They Do It

There are three basic attacks hackers can use to gain access to a system or network:

Internal Intrusions

An internal intrusion comes from within your corporation. It can be as simple as a curious employee or a serious attempt to hurt the company. Internal intrusions account for the most damage to companies because they come from people who already know the company, its security policies, and vulnerabilities. BlackICE can stop some internal intrusions.

External Intrusions

These include people trying to break into your systems from outside your company. These types of attacks are less common but almost always malicious in nature. BlackICE can stop external threats cold. Moreover, it can collect information about an external hacker to help you better defend yourself against that hacker in the future.

Social Intrusions

A social intrusion is when a hacker poses as an employee, authority figure, or friend in an attempt to get sensitive information about you and your systems. Perhaps the most common social intrusion is people posing as a system administrator asking for your password. Fortunately, social intrusions are pretty rare and easy to identify. Unfortunately, no software can stop a hacker armed with legitimate information he stole.

How to Respond to an Attack

BlackICE will protect your systems from any dangerous network intrusion. However, if you are experiencing a lot of attacks, you have some options for responding to the attacks.

Option 1 – Block the Attacker

Some hackers carry out repeated non-threatening attacks merely to be an annoyance. BlackICE only blocks intruders when they are directly threatening the operation of your system. For non-threading attacks, like port scans, BlackICE merely reports that the attack happened, but does not block the intruder.

BlackICE allows you to manually block intruder. Once an attacker is blocked, it cannot perform any more scans on your system.

See page 25 for more information about blocking an intruder.

NOTE: Do not block systems from your ISP or internal network. Most ISPs have automated scans to check the state of users' connections. Blocking your ISP's scans may cause your ISP to disconnect your Internet connection and may also be a violation of your usage agreement. Contact your ISP for help identifying the systems it uses to scan connections. Most ISP reveal the DNS address of their systems. This address usually contains the domain name of the ISP (e.g. *server.isp.com*).

Option 2 – Raise the Protection Level

If you are enduring numerous attacks, use the BlackICE security levels to protect your network ports. Raising the protection level may interfere with some Internet functions, especially multimedia content, however this is preferable to having to endure thousands of attacks.

See page 33 for more information about raising your BlackICE protection levels.

Option 3 – Go to the Source

Hackers have to get on the Internet somewhere. Most hackers are kids with standard accounts on ISPs or employees taking advantage of their company's high speed internet connection.

Most ISPs, corporations, and universities have strict rules regarding using their network to commit illegal activities. ISPs will usually terminate the accounts of users who attempt port scans or unauthorized access to systems. Likewise most corporations or universities will terminate employees or students who use their equipment for hacking activities.

Keep in mind that ISPs, corporations, and universities deal with hundreds possibly thousands of illegal use requests each day. Before you complain to the hacker's ISP, make sure you have adequate supporting evidence. This is where the backtracing and evidence logging features of BlackICE are a real asset.

Furthermore, reporting every system that scans your computer is probably more trouble than it is worth. Scans and probes are kicked off all the time on the Internet. Simply accessing a web site might kick off a scan. These are normal networking events and not always indicative of an attack.

It is best to report only those hackers that have carried out severe, repeated attacks on your system.

How to Report a Hacker

If BlackICE was able to get a DNS name from the hacker[3] use this to locate the origin of the hacker. For example, if BlackICE reported an attack from USER1.SAMPLEISP.COM, the hacker was obviously a user on the *Sample ISP*. Use an Internet search engine to locate the web site for the origin. Most ISPs, corporations, and universities will have a web site that lists how to contact them to report abuse. For most ISPs the mail address is *abuse@domainname.com*.

It is best to email the source rather than call. Most ISPs and corporations do not have the staff to handle individual abuse complains.

If you are unsure who owns the domain, use the Network Solutions WHOIS server at *http://www.networksolutions.com/cgi-bin/whois/whois/* to lookup a domain name.

When emailing the ISP, make sure to include the following information:

- Exact time the attack occurred.
- Your time zone.
- The type of attack.
- The Intruder's IP address, DNS address, NetBIOS address, and MAC Address, if available.
- Your name, email address, and ISP.
- Attach the following support files to your email. Make sure to explain that the evidence file is a "sniffer" type trace file. Most network administrators are familiar with this file format.
  - **Trace File**: Attach the BlackICE backtrace file for the intruder. These files are stored in the **C:\Program Files\Network ICE\BlackICE\Hosts** folder. The file names are the IP address and a .txt extension.
  - **Evidence File**: An evidence file is a raw dump of the network traffic related to the event. The file is encoded as a "sniffer" trace file. You will need a trace file decoding application to view the contents of this file. Windows NT Server includes the Network Monitor service and tools, which can decode such files. Other third party vendors supply such applications. Evidence files are stored in the **C:\Program Files/Network ICE/BlackICE** folder. By default, the file names are prefixed with the word "evd" and the date. This default can be changed in the Configure BlackICE features.

To manage space on your hard drive, BlackICE maintains a limited set of packet log and evidence files and cycles through the files in a "round robin" fashion. For example, if you set the maximum number of evidence files to 10, BlackICE will store 10 evidence files and then cycle back to the first file and overwrite it.

To determine which evidence file is correct for a particular attack, you may need to correlate the time of the attack with the timestamp on the file(s). If there are numerous files within the same time period, you will need to decode the file and locate the IP address of the attacker. Be careful not to send the wrong evidence file to the hacker's ISP.

If an attack is too old, BlackICE may have already overwritten the log or evidence file. To change the number of log and evidence keeps, see page 32 for information of evidence files and page 31 for information about packet log files.

---

[3] If you do not have a DNS name for the hacker it is probably best to just block the attacker and forget about it. Savvy hackers can hijack connections and spoof addresses, which makes it impossible to report them to anybody who could stop them.

Option 4 – Reconfigure Your Network Firewall

If your network is enduring numerous attacks from hackers, it may be a good time to review the configuration of your network firewall. Over time, many firewalls deteriorate and do not offer optimal protection. If you have a particularly malicious hacker you may want to filter out the hacker at the firewall thus offering another layer of protection.

Option 5 – Upgrade your Operating System

All the major operating systems regularly release updates to their software. The most current releases and service packs often patch known vulnerabilities. Your operating system vendor's web site is a good place to begin looking for updates.

GOOD SECURITY PRACTICES

You have already taken the first step toward stopping hackers with BlackICE. In addition to BlackICE you should consider the following good security practices:

- If you are on a corporate network, install Network ICE's ICEcap server. ICEcap is a powerful reporting and analysis server that aggregates data from BlackICE workstations all over the network. With this information, system administrators can spot trends and patterns in intrusions. This can be extremely helpful to stop hackers who are probing for a security breech.
- Install Network ICE's ICEscan. ICEscan can scan and analyze network devices and resources looking for common security breeches. When used in conjunction with an ICEcap server, system administrators can spot many security problems before hackers exploit them.
- Establish a good security plan. A good network takes into account what hackers can do and prepares for attacks. The best defense against hackers and crackers is information. Encourage your company or organization to develop a comprehensive security plan if you do not already have one.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc. to people without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection with a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
- Never reveal your IP address or other system networking information to people outside your company.
- Be very careful of files e-mailed to you, even those from people you know. One common way of getting BackOrifice and NetBus on a system is to embed the program into some cute dancing baby executable or other such program. While you are laughing at the antics of some on-screen cartoon, hackers are opening up your system and looking for files to steal.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers, and a symbol such as % or #.
- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.

- If you use “chat rooms” or IRC sessions, be careful with any information you reveal to strangers. Hackers are notorious for “address harvesting” from chat rooms and other interactive areas.
- If your system starts exhibiting odd behavior, contact your system administrator. Some hackers set off attacks that slowly cause your system to become unstable or unusable.
- If you are using Windows NT and your system suddenly displays a blue screen, write down the information at the top of the screen and contact your system administrator immediately. Some serious Windows errors are the result of hackers or viruses on a system.
- Always shred company phone books or network information before throwing it away. A dedicated hacker will dig through the trash of companies or individuals for information that might help them in a social intrusion.

RETALIATION HACKING

It is tempting to turn the tables on hackers and hack them back. **Network ICE strongly discourages any “retaliation hacking.”** It might feel good to attempt such revenge, but ultimately it is counterproductive.

First, hacking is most likely a violation of your ISP’s usage policies. Hacking is one of the quickest ways to get your Internet account cancelled. This includes corporate Internet connections.

Second, if you are getting hacked at work, retaliating against a hacker could merely incite the attacker to hack more. Most sophisticated hackers are diligent enough to protect their own systems. Therefore, if you attempt to hack them back this could encourage them. Less experienced hackers may find your retaliation as grounds to broadcast your company or account to various hacker forums. This could summon more experienced hackers to zero in on your company or systems. Inciting hackers to break into your company may be grounds for termination at your company.

Third, hacking really does not accomplish anything constructive. BlackICE and the rest of the Network ICE products will protect your systems from hackers. Retaliating will only waste time and resources and probably not stop the hacker. In the realm of networking countermeasures, the best offense is a solid defense.

A For More Help

For more help with your copy of BlackICE refer to these sources:

On-Line Help

The Online Help provides quick answers to many issues regarding BlackICE. To access the online help, follow one of these sets of directions:

From the BlackICE Application

- Click the BlackICE icon in the far left corner of the BlackICE Summary Application. A pop-up menu is displayed.
- Select **Help** and then **BlackICE Help Topics** from the submenu.

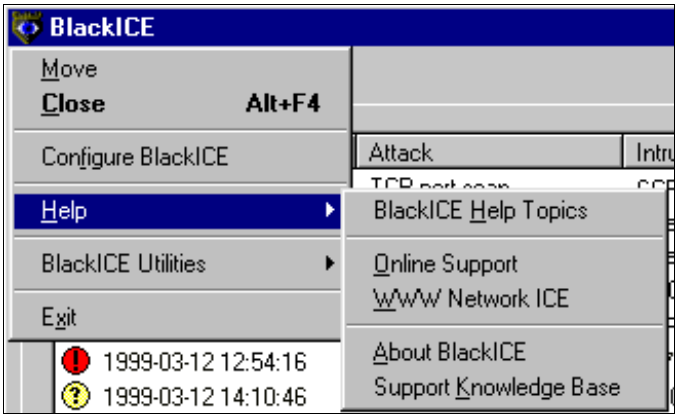


Figure 33 – Select BlackICE Help Topics to display the online help.

Network ICE Web Site

The Network ICE web site includes the latest information about BlackICE including FAQs, a support Knowledge Base, and the advICE library an extensive on-line resource for network security information.

Visit the site at www.networkice.com.

PRODUCT DOCUMENTATION

The latest product documentation is also available from the Network ICE web site at http://www.networkice.com/Support.

TECHNICAL SUPPORT

Web:	www.networkice.com/Support
Email:	corpsupport@networkice.com
Telephone:	(650) 532-4100 8:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday

For updates and upgrade information, please contact your sales representative or visit the Network ICE web site.

B GLOSSARY

ARP: Address **R**esolution **P**rotocol. a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

Authenticity: Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.

Back Door: A deliberately planned security breach in a program. Back doors allow special access to a computer or program. Sometimes back doors can be exploited and allow a cracker unauthorized access to data.

Back Orifice: Back Orifice is a remote administration tool which allows a user to control a computer across a TCP/IP connection using a simple console or GUI application. Back Orifice is a potentially disastrous Trojan horse since it can provide the user unlimited access to a system.

Blue Screen of Death (BSoD): When a Windows NT based system encounters a serious error, the entire operating system halts and displays a screen with information regarding the error. The name comes from the blue color of the error screen.

Brute Force Hacking: A technique used to find passwords or encryption keys. Brute Force Hacking involves trying every possible combination of letters, numbers, etc. until the code is broken.

Camping Out: Staying in a "safe" place once a hacker has broken into a system. The term can be used with a physical location, electronic reference, or an entry point for future attacks.

Cipher Text: Text that has been scrambled or encrypted so that it cannot be read without deciphering it. *See* Encryption

Cookie: A string of characters saved by a web browser on the user's hard disk. Many web pages send cookies to track specific user information. Cookies can be used to retain information as the user browses a web site. For example, cookies are used to 'remember' the items a shopper may have in a shopping cart.

Countermeasures: Techniques, programs, or other tools that can protect your computer against threats.

Cracker: Another term for hackers. Generally, the term cracker refers specifically to a person who maliciously attempts to break encryption, software locks, or network security.

Cracker Tools: Programs used to break into computers. Cracker tools are widely distributed on the Internet. They include *password crackers*, *Trojans*, *viruses*, *war-dialers*, and *worms*.

Cracking: The act of breaking into computers or cracking encryptions.

Cryptoanalysis: The act of analyzing (or breaking into) secure documents or systems that are protected with encryption.

Decryption: The act of restoring an encrypted file to its original state.

Denial of Service: Act of preventing customers, users, clients or other machines from accessing data on a computer. This is usually accomplished by interrupting or overwhelming the computer with bad or excessive information requests.

Digital Signature: Digital code that authenticates whomever signed the document or software. Software, messages, Email, and other electronic documents can be signed electronically so that they cannot be altered by anyone else. If someone alters a signed document, the signature is no longer valid. Digital signatures are created when someone generates a hash from a message, then encrypts and sends both the hash and the message to the intended recipient. The recipient decrypts the hash and original message, makes a new hash on the message itself, and compares the new hash with the old one. If the hashes are the same, the recipient knows that the message has not been changed. Also see *Public-key encryption* .

DNS: **D**omain **N**ame **S**ystem. A database of domain names and their IP addresses. DNS is the primary naming system for many distributed networks, including the Internet.

Encryption: The act of substituting numbers and characters in a file so that the file is unreadable until it is decrypted. Encryption is usually done using a mathematical formula which determines how the file is decrypted.

Event: BlackICE can detect numerous network activities. Some activities are direct attacks on your system, while others might be depending on the circumstances. Therefore, any activity, regardless of severity is called an event. An event may or may not be a direct attack on your system. BlackICE categorizes all events into four severity levels:

Icon	Severity	Description
	100 –75	**Critical Event**: This is a deliberate attack on your system for the purpose of damaging data or crashing the system.
	74 – 50	**Serious Event**: This is a deliberate attempt to access information on your system, yet it does not directly damage anything. These events can trigger protection measures, if applicable.
	49 – 25	**Suspicious Event**: This is network activity that is not immediately threatening but may indicate that someone is attempting to locate security vulnerabilities in your system. For example, hackers often scan the available ports or services on a system before attacking it. Suspicious events do not trigger protection measures, and not all suspicious events are indicative of a true attack.
	24 – 0	**Informational Event**: This indicates that a network event occurred to your computer that is not threatening. Informational events do not trigger protection measures.

Firewall: A hardware or software "wall" that restricts access in and out of a network. Firewalls are most often used to separate an internal LAN or WAN from the Internet. See Gateway.

FTP: **F**ile **T**ransfer **P**rotocol. A common protocol for exchanging files between two sites across a network. FTP is popular on the Internet because it allows for speedy transfer of large files between two systems. Like all networking protocols, it too has its share of vulnerabilities.

Gateway: A gateway is a system that provides access between two or more networks. Gateways are typically used to connect unalike networks together. A gateway can also serve as a firewall between two or more networks.

Hacker: Generally, a hacker is anyone who enjoys experimenting with technology including computers and networks. Not all hackers are criminals breaking into systems. Some are legitimate users and hobbyists. Nevertheless, some are dedicated criminals or vandals.

HTTP: Hyper **T**ext **T**ransfer **P**rotocol. The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certaint kinds of attacks.

Integrity: Proof that the data is the same as originally intended. Unauthorized software or people have not altered the original information.

Internet Worm: *See* Worm.

Intruder: Person or software interested in breaking computer security to access, modify, or damage data. *Also see* Cracker.

IP: **I**nternet **P**rotocol specifies the format of packets, also called *datagrams,* and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time. Current IP standards use 4 numbers between 0 and 255 separated by periods, such as 38.158.99.13.

IRC: Internet Relay Chat. IRC was developed in the late 1980s as a way for multiple users on a system to "chat" over the network. Today IRC is a very popular way to "talk" in real time with other people on the Internet. However, IRC is also one avenue hackers use to get information from you about your system and your company. Moreover, IRC sessions are prone to numerous attacks that while not dangerous can cause your system to crash.

Linux: A version of the UNIX operating system designed to run on IBM Compatible computers.

Logic Bomb: A virus that only activates itself when certain conditions are met. Logic bombs usually damage files or cause other serious problems when they are activated.

Name Resolution: The allocation of an IP address to a host name. *See* DNS

NetBIOS: **Net**work **B**asic **I**nput / **O**utput **S**ystem. NetBIOS is an extension of the DOS BIOS that enables a PC to connect to and communicate with a LAN.

NAT: **N**etwork **A**ddress **T**ranslation. An Internet standard that enables LAN, WAN, and MAN networks to use extended IP addresses for internal use by adding an extra number to the IP address. This standard translates internal IP addresses into external IP addresses and vice versa. In doing so, it generates a type of firewall by hiding internal IP addresses.

Packet Filter: A filter used in firewalls that scans packets and decides whether to let them through.

Password Cracker: A program that uses a dictionary of words, phrases, names, etc. to guess a password.

Password encryption: A system of encrypting electronic files using a single key or password. Anyone who knows the password can decrypt the file.

Password Shadowing: The storage of a user's username and password in a network administrator database.

Penetration: Gaining access to computers or networks by bypassing security programs and passwords.

Phreaking: Breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.

Ping Attack: An attack that slows down the network until it is unusable. The attacker sends a "ping" command to the network repeatedly to slow it down. See also Denial of Service.

Pirate: Someone who steals or distributes software without paying the legitimate owner for it. This category of computer criminal includes several different types of illegal activities:

- Making copies of software for others to use.
- Distributing pirated software over the Internet or a Bulletin Board System.
- Receiving or downloading illegal copies of software in any form.

Pirated Software: Software that has been illegally copied, or that is being used in violation of the software's licensing agreement. Pirated software is often distributed through pirate bulletin boards or on the Internet. In the internet underground it is known as Warez.

Plain Text: The opposite of Cipher Text, Plain Text is readable by anyone.

POP: **P**ost **O**ffice **P**rotocol. This is a common protocol used for sending, receiving, and delivering mail messages.

Port: A connection point where a computer communicates with other devices. Computers have hardware ports such as parallel ports for printers or USB ports for digital cameras. Networks use virtual ports for assigning a communications channel that the computer can control. For example, when browsing the web, most HTTP based communications take place using the TCP port 80. When a computer needs to access a web site, it opens a channel on TCP port 80, sends the packets through that port and then receives them back. There are two types of ports, TCP and UDP. UDP is the same as a TCP port except it lacks the error checking mechanism that TCP uses. There are over 131,000 ports available for use in a TCP/IP environment (64K TCP, 64K UDP). Most of these ports are unused, unassigned, or restricted. Some are very common ports, such as port 80. Others are used exclusively for a brand of software. For example, Quake games use TCP port 26000 (and others) for network games.

When hackers break into a system they typically exploit ports that are either accidentally or purposefully opened. For example, one of the easiest ways to see if the Trojan application Back Orifice is installed on a computer is to scan for activity on TCP port 54320. This is the TCP port Back Orifice uses when communicating with other systems.

Promiscuous Packet Capture: Actively capturing packet information from a network. Most computers only collect packets specifically addressed to them. Promiscuous packet capture acquires all network traffic it can regardless of where the packets are addressed.

Protocol: A "language" for communicating on a network. Protocols are sets of standards or rules used to define, format, and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.

Proxy Server: A server that performs network operations in lieu of other systems on the network. Proxy Servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server, via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system which originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.

Public Key Encryption: System of encrypting electronic files using a key pair. The key pair contains a public key used during encryption, and a corresponding private key used during decryption.

Reconnaissance: The finding and observation of potential targets for a cracker to attack.

Router: A device that connects two networks together. Routers monitor, direct, and filter information that passes between these networks. Because of their location, routers are a good place to install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.

SATAN: A UNIX program that gathers information on networks and stores it in databases. It is helpful in finding security flaws such as incorrect settings, software bugs and poor policy decisions. It shows network services that are running, the different types of hardware and software on the network, and other information. It was written to help users find security flaws in their network systems.

Shoulder Surfing: Looking over someone's shoulder to see the numbers they dial on a phone, or the information they enter into a computer.

Snooping: Passively watching a network for information that could be used to a hacker's advantage, such as passwords. Usually done while Camping Out.

SOCKS: A protocol that handles TCP traffic through proxy servers. SOCKS acts like a simple firewall because it checks incoming and outgoing packets and hides the IP addresses of client applications.

SPAM: Unwanted e-mail, usually in the form of advertisements.

Spoofing: To forge something, such as an IP address. IP Spoofing is a common way for hackers to hide their location and identity.

SSL (Secured Socket Layer): Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.

Telnet: A program that connects a computer to a server on a network. It allows a user to control some server functions and to communicate with other servers on the network. Telnet sessions generally require a valid username and password. Hackers commonly use Telnet to hack into corporate network systems.

Tempest: Illegal interception of data from computers and video signals.

Trojan or **Trojan Horse**: Like the fabled gift to the residents of Troy, a Trojan Horse is an application designed to look innocuous. Yet, when you run the program it installs a virus or memory resident application that can steal passwords, corrupt data, or provide hackers a back door into your computer. Trojan applications are particularly dangerous since they can often run exactly as expected without showing any visible signs of intrusion.

UNIX: A widely used operating system in large networks.

VPN: Virtual Private Network. These networks use public connections (such as the Internet) to transfer information. That information is usually encrypted for security purposes.

Vulnerability: Point where a system can be attacked.

War Dialer: A program that automatically dials phone numbers looking for computers on the other end. They catalog numbers so that hackers can call back and try to break in.

Warez: A term that describes Pirated Software on the Internet. Warez include cracked games or other programs that software pirates distribute on the Internet.

Wire Tapping: Connecting to a network and monitoring all traffic. Most wire tapping features can only monitor the traffic on their subnet.

Worm: A program that seeks access into other computers. Once a worm penetrates another computer it continues seeking access to other areas. Worms are often equipped with dictionary-based password crackers and other cracker tools which enable them to penetrate more systems. Worms often steal or vandalize computer data.