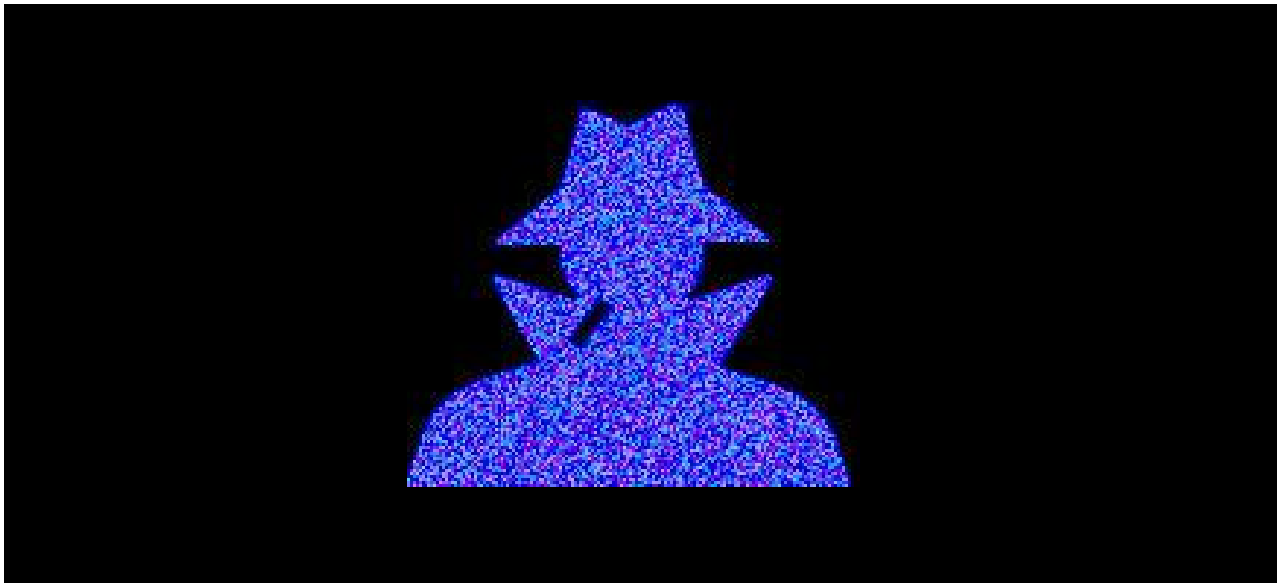
Network ICE

BlackICE defender



User's Guide

Version 1.0

BlackICE Defender User's Guide – Version 1.0

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 are 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 forpurchasing BlackICE Defender. BlackICE is a powerful way to detect, stop, and analyze the activities of people trying to hack into your computer. BlackICE was designed from the ground up to work seamlessly with Internet connections. BlackICE is ideal for any computer using a standard dial-up modem, cable modem, or DSL connection.

Overview

In the past, computer hacking presented very little threat to home or small-business computer users. Hackers spend most of their time attacking large corporate networks where there were valuable things to steal or vandalize. Most home computers of five to ten years ago held few if any files of interest to a hacker. Furthermore, Internet connections in the past were slow and extremely difficult to locate for even advanced hackers.

Today, the typical home or small-business computer presents numerous opportunities for hackers. Many home computers store credit card numbers, account numbers, and confidential information for on-line commerce, banking, or stock trading. Furthermore, home computers are easy targets. Most home computers have little, if any, protection from hackers. Exacerbating this problem is the rise of “always-on” Internet connections such as cable modems or DSL connections. The more people there are using the Internet, the more opportunities there are for hackers to steal things.

Until now, detecting and stopping hackers meant purchasing expensive hardware or mastering complex networking tools. BlackICE places on your home computer the same powerful intrusion detection and protection tools that big corporations use. Now you can stop hackers before they stop you.

What Can Hackers Do?

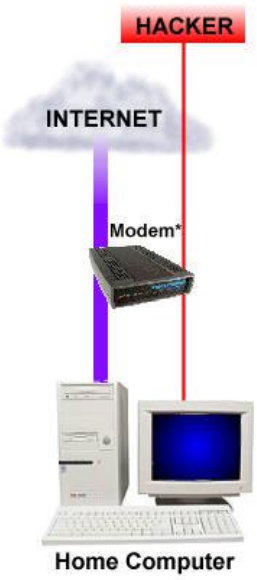
When you connect to the Internet your computer is a part of the huge global network. You can send data (outbound) and receive data (inbound). When you download photos on a web site, you send a request outbound to the web server, then the web server transmits the photo data back inbound to your computer.

Hackers, exploit the capability of your computer to communicate with other computers. A hacker can use widely available networking tools to connect to your computer and send it commands. For example, a hacker could connect to your system and download an encrypted file containing your credit card number. Then using a freely available decrypting program, the hacker cracks the file, gets the number, and goes on a buying spree at your expense.

While your link to the Internet is active, hackers can identify your system and break into it. This is why “always-on” Internet connections such as cable modems and DSL connections are particularly vulnerable. For a hacker to break into your system, he must first locate your computer. The more often your system is exposed to the Internet, the more likely a hacker will find it. Some hackers run continuous scans of certain areas of the Internet looking for home computers to break into.

Therefore, if your Internet connection is live 24 hours a day, a hacker has more opportunities to find your system. Dial-up connections are slightly safer, but still pose a significant opportunity to hackers. While you are chatting on-line with a friend over a dial-up connection, a hacker in Russia could have located your computer and begun hacking.

BlackICE operates like a persistent “traffic cop.” When BlackICE detects inappropriate access to your computer, it blocks access to the offending user. All other Internet access remains open and unaffected. Only the hacker is blocked, you can continue to browse the web, send email, and listen to Internet radio stations while BlackICE rejects the hackers.



** Regular modem, cable modem, or DSL connection*

Figure 1 – Without BlackICE

** Regular modem, cable modem, or DSL connection*

Figure 2 – With BlackICE.

The figure on the left illustrates a common home computer when connected to the Internet. While manyISPs have some protection from hacking, this protection only stops the most primitive attacks. Most novice hackers can easily break through your ISP’s protection measures. When they do, your computer is vulnerable to attack.

The figure on the right demonstrates a computer protected with BlackICE. If the hacker is able to locate your system, and break through your ISP, BlackICE stops the intrusion before any data is compromised.

How BlackICE Works

BlackICE consists of an extremely powerful detection and analysis engine that constantly monitors the inbound and outbound traffic between your computer and the Internet or any other computers on a network. When suspicious behavior is detected, BlackICE springs into action and begins logging information about the event. Information about the attacker is displayed on the Intruders tab. Information about the type of attack the intruder attempted is displayed on the Attacks tab.

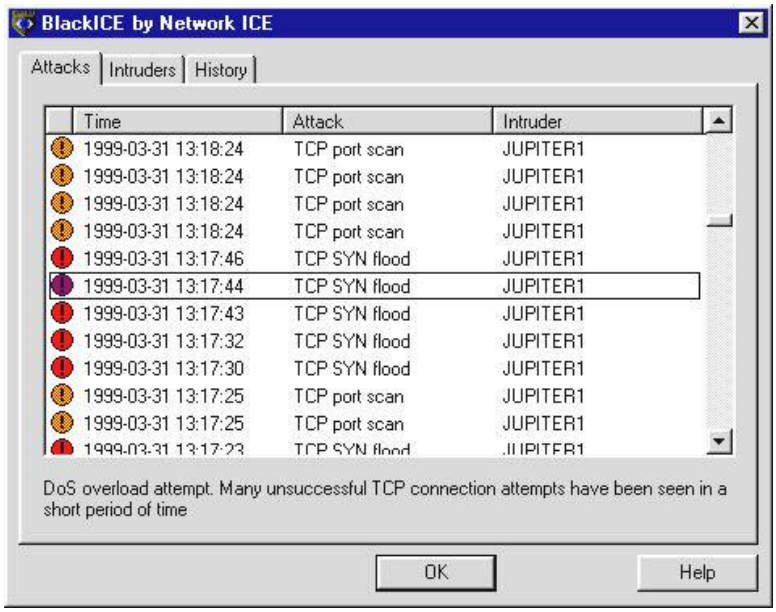


Figure 3 – The BlackICE Attacks tab.

The information BlackICE collects regarding an attack is analyzed with sophisticated networking algorithms. If the event is determined to be an intrusion, BlackICE automatically blocks any access from the hacker's machine (IP address). No matter how hard the hacker tries to crack your system, he cannot outrun BlackICE. BlackICE blocks the hacker's access at the packet level. In other words, any transmission the hacker sends to your computer is rejected before it ever gets inside the computer.

When BlackICE reports an attack, it not only tells you what the attack was but exactly who carried out the attack. BlackICE "backtraces" hackers when they try to break into your computer. Backtracing allows you to know exactly who is attacking you. In extreme cases, this information could be very valuable if you wish to pursue legal action against the hacker.

BlackICE also captures a complete record of the attack in Evidence files. These files contain all the data the hacker sent to your computer. In the hands of an experienced network engineer or Internet Service Provider, you can know exactly what the hacker was trying to do. See page 21 for more information about Evidence Files.

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.

If you are using BlackICE on your company LAN, you can also configure BlackICE to report events to an ICEcap server. ICEcap is a powerful reporting and management console for corporate networks. ICEcap can aggregate information from multiple computers running BlackICE. This helps identify more attacks and monitor intrusion information on an enterprise-wide level.

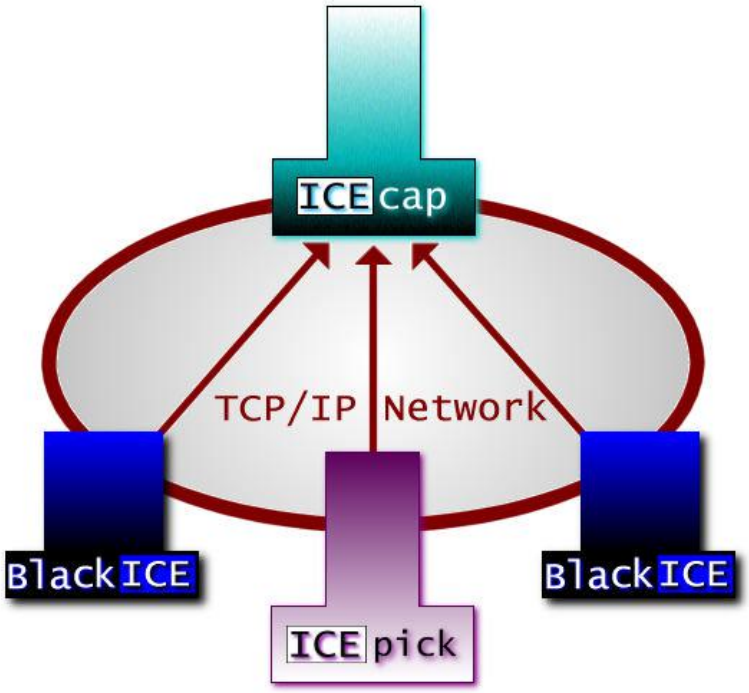


Figure 4 – On a corporate network, BlackICE is used to defend each workstation and report events to an ICEcap server. The ICEcap server aggregates and reports the events that took place on each network workstation where BlackICE is installed.

For proactive security assessment and monitoring, Network ICE's ICEpick can regularly scan your network for security problems. This information is also reported to the ICEcap server for analysis and review.

For more information about ICEpick and ICEcap, visit the Network ICE web site at www.networkice.com

Security Levels

When BlackICE detects an attack, it automatically blocks access from the hacker's system. However, not all Internet transmissions are attacks. What constitutes an attack vs. legitimate use of the Internet is not always easy to determine. Some legitimate Internet applications communicate with your computer in such a way that data is sent to you and then executed. For example, an on-line virus scanning tool may appear to BlackICE as an attack, since the web site is transmitting data directly to your computer and then executing it.

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

A port is a virtual "connection point" on your computer. When you are connected to the Internet, your computer communicates with other computers via virtual ports. For example, when you download your e-mail, your computer establishes a connection on TCP port 110 to your ISP's 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, 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, are used by client applications such as chat programs or the 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	þ *	þ	þ	þ
	TCP	þ	þ	þ	þ
Cautious	UDP	ý	þ	þ	þ
	TCP	ý	þ	þ	þ
Nervous	UDP	ý	þ	þ	þ
	TCP	ý	ý	þ	þ
Paranoid	UDP	ý	ý	þ	þ
	TCP	ý	ý	þ	þ

* – File Sharing is blocked, unless specifically turned on. See page 24 for more information.

Security Level Descriptions

Trusting: When set to Trusting, BlackICE only blocks file sharing over the Internet, unless Internet file sharing is specifically enabled on the Protection tab (See page 24 for more information). Blocking Internet file sharing ensures that hackers cannot download files off your computer. All other ports remain open and unblocked. Even though Internet file sharing is disabled, file sharing on an internal network remains unaffected. This setting is good to use if you have a slower Internet connection and little threat of attack.

Cautious: The Cautious setting is best 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 good 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 setting security levels, see page 24.

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 features the same powerful detection abilities as BlackICE Personal, however BlackICE Defender protects against intrusions. When attacks are detected, BlackICE Defender automatically blocks the attacker from gaining access to your system.

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 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 Probe 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 consultant to performshort 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.

ICEpick

ICEpick is a security auditing program. ICEpick scans the network for common network security vulnerabilities that hackers might exploit. ICEpick runs many of the same procedures hackers attempt and reports the success or failure of such attacks. ICEpick 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.

ICEcap

ICEcap is a centralized reporting system for BlackICE and ICEpick 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 may not detect as a series of 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

Installing BlackICE only takes a few minutes. This section steps you through the process of installing the BlackICE application.

Minimum System Requirements

- Operating Systems: Windows NT Workstation 4.0, Windows NT Server 4.0, Windows 95, Windows 98

NOTE: BlackICE has not been tested on Windows 2000 or Windows NT 5.0.

- Processor: Pentium or better.
- Memory: 16 MB or more.
- Hard Drive Space: 10 MB free.
- Network Connection: 10-BASE-T, ADSL, ISDN, cable modem, or regular modem connection using the TCP/IP protocol.

How to Install BlackICE

1. Locate the Setup Application.

   You must have the setup application to install BlackICE. There are a number of places to acquire this program.

   - If you have the BlackICEpac suite or a CD copy of BlackICE run Setup.EXE from the BlackICE folder.
   - If you are using BlackICEcap to distribute BlackICE, contact your system administrator about the correct internal web address where the setup application is located.
   - If you purchased BlackICE directly from Network ICE, you can download the latest version from www.networkice.com. Once you download the latest version, you can run BIsetup.EXE or you can chose to install across the net.

2. Run Setup.EXE or BIsetup.EXE. If you are running BIsetup.EXE, the application must unpack the setup files and verify them first. Once that is finished, Setup.EXE runs.

ý If setup detects and existing version of BlackICE, the setup prompts you to uninstall or continue to upgrade the previous version. See page 11 for more information about uninstalling BlackICE.

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

6. 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. BlackICE automatically places a shortcut here to start BlackICE when the system is first started. Click Next to continue.
7. Enter your license key. Your key was made available to you when you purchased BlackICE. If you have lost your key, please contact Network ICE Technical Support (see page 105.)
8. 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.

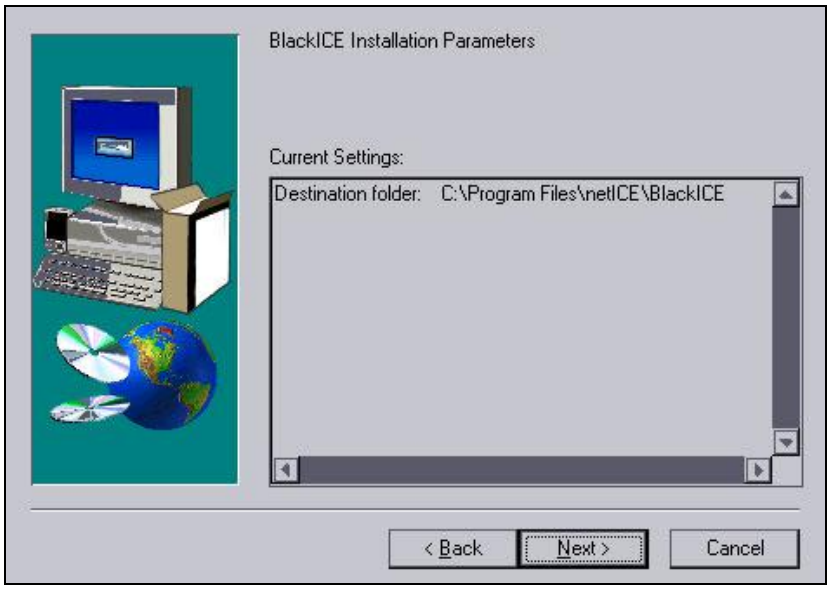


Figure 5 – BlackICE Installation Parameters window.

If the information is correct, click Next.

9. The installation begins. When it is finished, the BlackICE service is started.
10. 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.

- The BlackICE setup is complete.

Uninstalling 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 6 – The Add/Remove Programs dialog box.

3. Locate **BlackICE** in the list of programs.
4. Select **BlackICE** and click **Add/Remove**.
5. You are prompted to confirm the removal of BlackICE. Click **Yes** to continue.

6. An UNInstallShield application begins. This application will remove the BlackICE files, registry entries and other features.

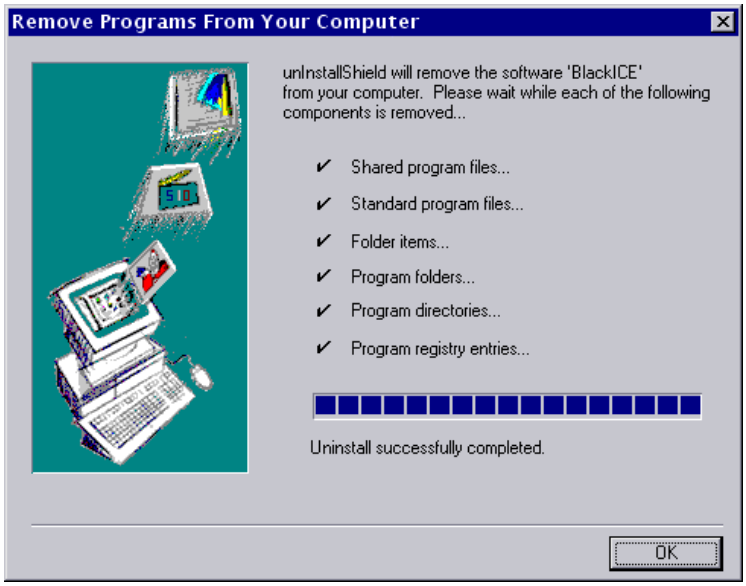


Figure 7 – UNInstallShield Application removing BlackICE.

7. When the application is completed, click OK.
8. If the uninstall encounters any errors or is unable to remove some components, a Details button is displayed. Click Details to display the uninstallation log. You may need to manually delete the ICEpick folders where you installed the application.

3 USING BLACKICE

BlackICE consists of two main components an invisible monitoring and detection engine and a summary application.

The monitoring and detection engines of BlackICE are always running when the computer is operating. These engines are “invisible” to anyone using the computer to ensure that they are not accidentally or purposefully disabled. Therefore, once BlackICE is installed, there is no need to worry about intrusion detection and monitoring. BlackICE works silently whenever the computer is operating.

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, each displaying a different aspect of the intrusion monitoring and detection.

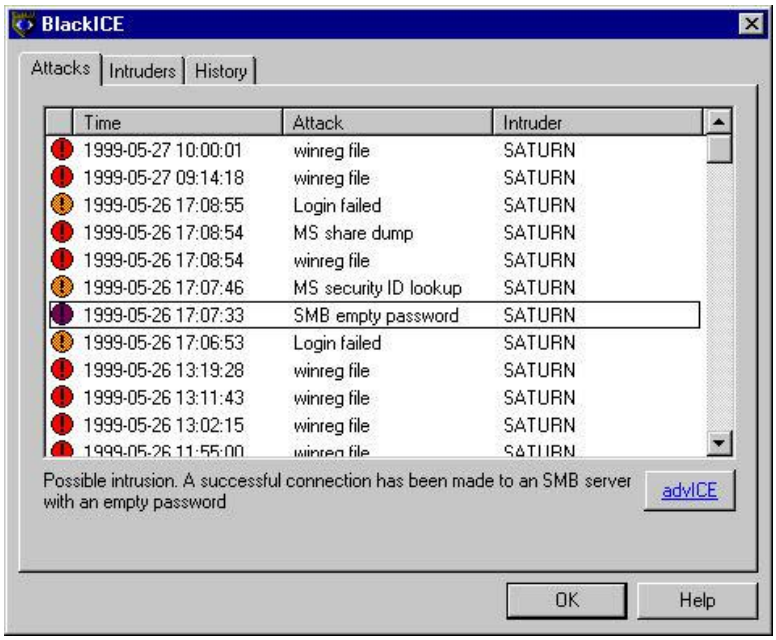
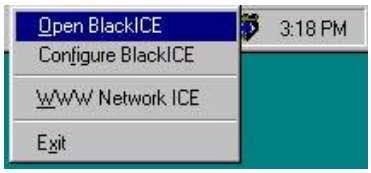


Figure 8 – The BlackICE application displaying the Attacks Tab.

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

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 access the Network ICE web site or Exit BlackICE.
  - A single regular click on the task-bar icon opens the utility as well.
- If the tool is not already running, from the Start menu, select Programs, then select Network ICE, then select BlackICE Utility.

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).

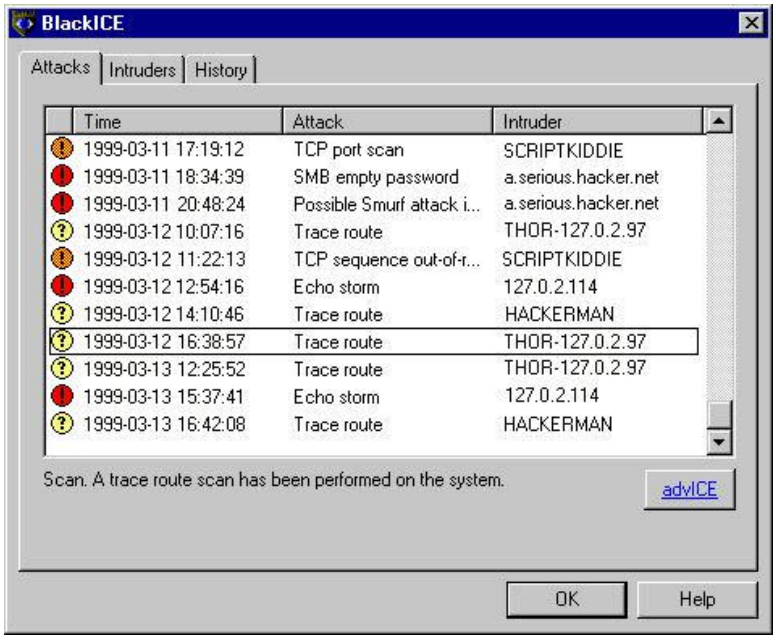


Figure 9 – Detected events are listed as critical, serious, suspicious, or informational on the Attacks tab.

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

- 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.
- 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.
- 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.

  Not all suspicious events are indicative of a true attack. For example, many Internet Service Providers have scanning programs installed on their servers to check if a connection is still valid. This is a completely safe and legitimate scan from your ISP, but BlackICE would still report it as a suspicious event. After a few weeks of information is collected, you may notice recurring scans from one location. Note the IP address(es) where the scans originate and contact your ISP. It is likely these scans are a standard part of your ISP's service and pose no threat to your system.

- 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 6: How to Handle Attacks on page 37, 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.

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.

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).

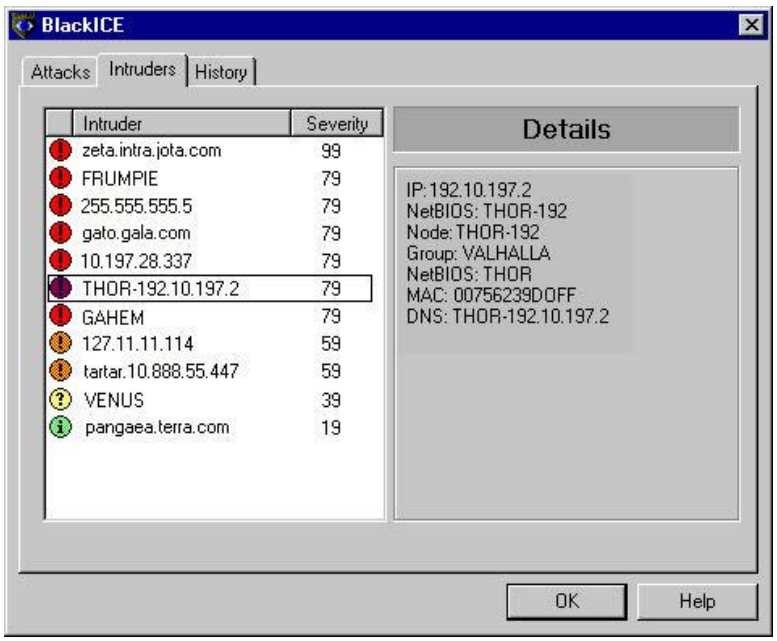


Figure 10 – Intruders tab.

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 –80	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.
	80 – 40	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.
	40 – 20	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.
	20 – 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.