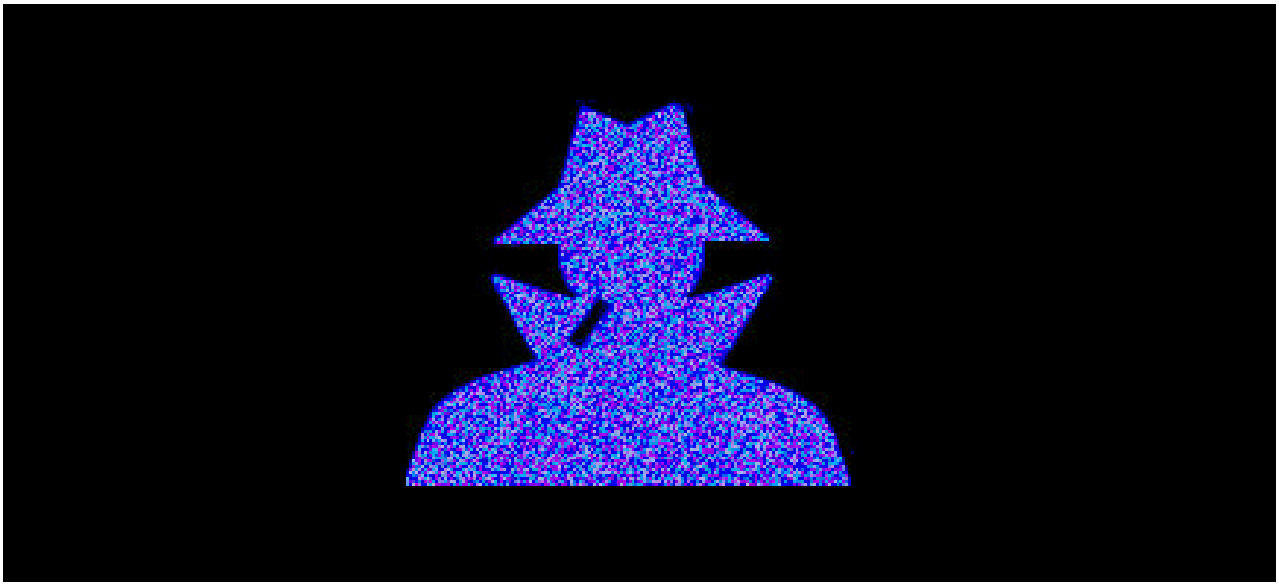
Network ICE

BlackICE defender



User's Guide

Version 1.0

BlackICE Defender User's Guide – Version 1.0

Copyright © 1999, Network ICE Corporation

All Rights Reserved

Author: Andrew Plato

The use and copying of this product is subject to a license agreement. Any other use is strictly prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form by any means without the prior written consent of Network ICE Corporation. Information in this user's guide is subject to change without notice and does not constitute any commitment on the part of Network ICE Corporation.

Network ICE Corporation may have patents or pending patent applications, trademarks, copyrights, and other intellectual property rights covering the subject matter of this user's guide. Furnishing of this document does not in any way grant you license to these patents, trademarks, copyrights, or any other intellectual property of the Network ICE Corporation.

BlackICE, ICEpick, ICEcap, ICEpac and the Network ICE logo are all trademarks of the Network ICE Corporation.

Windows® and Microsoft® are registered trademarks and Windows NT™, Windows 98™, SQL Server™, and Internet Explorer™ are all trademarks of the Microsoft Corporation.

Internet Security Systems (ISS) is a trademark of Internet Security Systems, Inc.

CyberCop is a trademark of Network Associates, Inc.

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

Section I: Introduction 1

Overview 1
What Can Hackers Do? 1
How BlackICE Works 3
Security Levels 4
Security Level Descriptions 6
The Network ICE Product Line 7
Other Network ICE Products 8

Section II: Installing BlackICE 9

Minimum System Requirements 9
How to Install BlackICE 9
Uninstalling BlackICE 11

Section III: Using BlackICE 13

How to Run the BlackICE Summary Application 14
The Attacks Tab 14
The Intruders Tab 16
The History Tab 18
Configuring BlackICE 19
Back Trace Tab 20
Packet Log Tab 22
Evidence Log Tab 23
Protection Tab 24
Trusted Addresses Tab 25
Blocked Addresses Tab 27
ICEcap Tab 28
Clearing the Attack List 29
Updating BlackICE 30
Evidence Files 31
Disabling BlackICE 32

Section IV: System Security 33

What Hackers Can Do 33
How They Do It 34
Stopping Hackers 34

Section V: How to Handle Attacks 37

Index of Attacks 37
BlackICE Attacks 40

Appendix A: For More Help 105

Online Help 105
Network ICE Web Site 105
Technical Support 105

Appendix B: Glossary 107

1 INTRODUCTION

Thank you for purchasing 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.

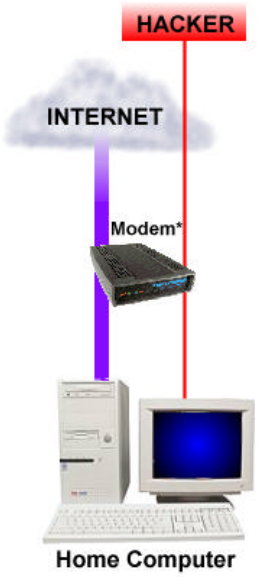


Figure 1 – Without BlackICE

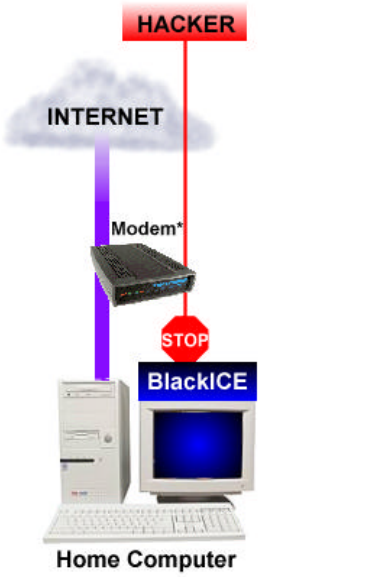


Figure 2 – With BlackICE.

The figure on the left illustrates a common home computer when connected to the Internet. While many ISPs 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.

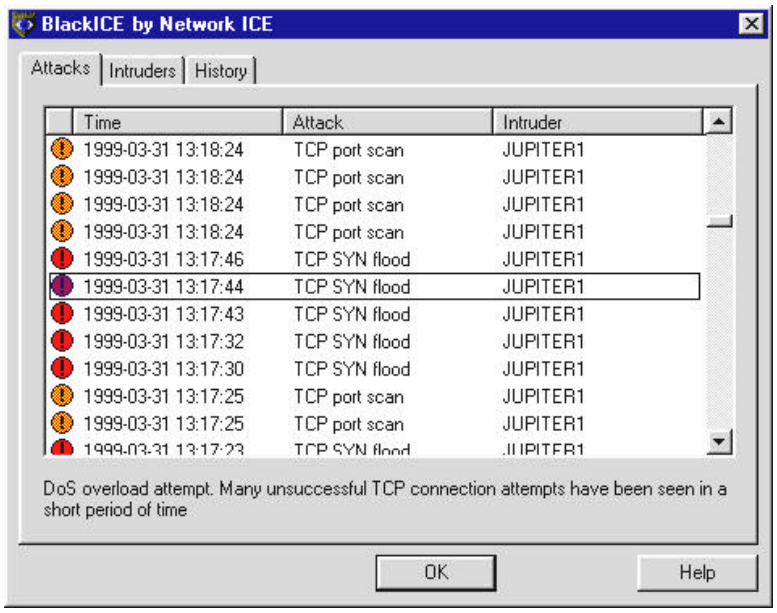


Figure 3 – The BlackICE Attacks tab.

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 31 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.

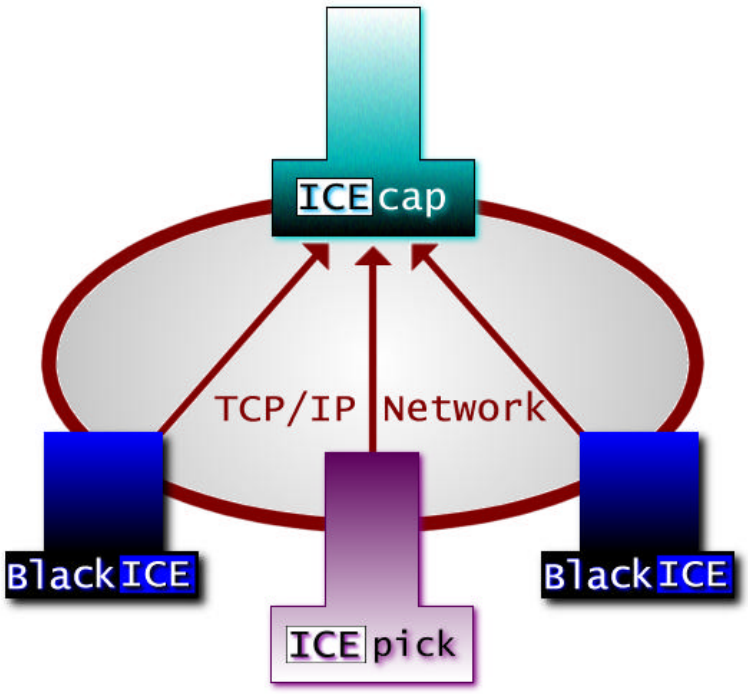


Figure 4 – On a corporate network, BlackICE is used to defend each workstation and report events to an ICEcap server. The ICEcap server aggregates and reports the events that took place on each network workstation where BlackICE is installed.

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*	☑*	☑	☑	☑
	TCP	☑	☑	☑	☑
Cautious	*UDP*	☒	☑	☑	☑
	TCP	☒	☑	☑	☑
Nervous	*UDP*	☒	☑	☑	☑
	TCP	☒	☒	☑	☑
Paranoid	*UDP*	☒	☒	☑	☑
	TCP	☒	☒	☑	☑

* – 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 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 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 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.

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 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

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 ICEpac suite or a CD copy of BlackICE run **`Setup.EXE`** from the **`BlackICE`** folder.
   - If you are using ICEcap 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.

☒ 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.

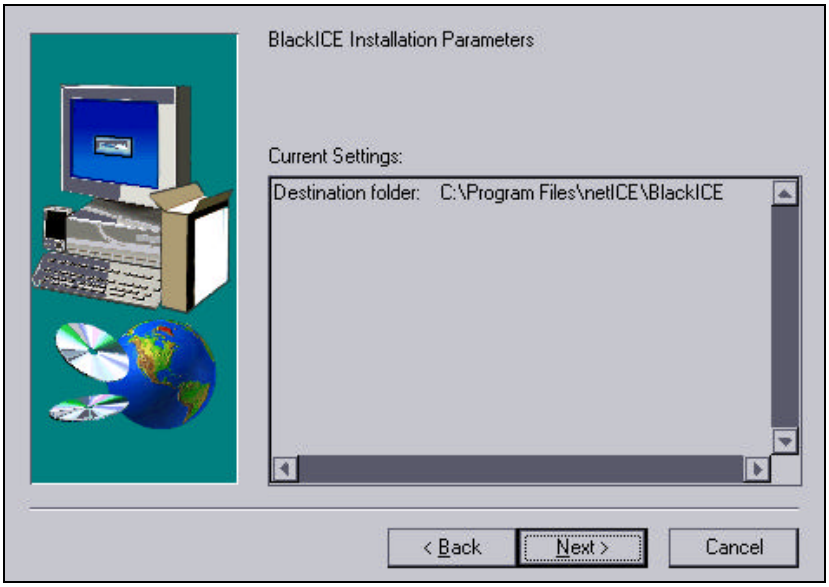


Figure 5 – BlackICE Installation Parameters window.

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.

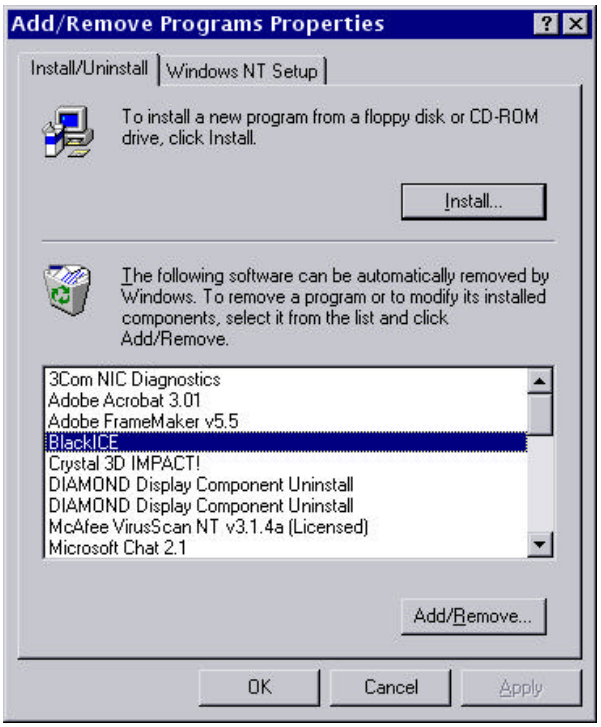


Figure 6 – The Add/Remove Programs dialog box.

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.

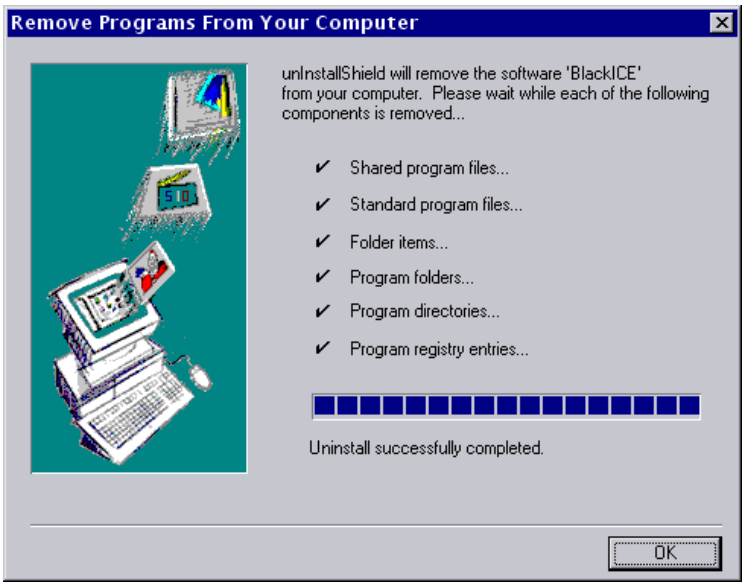


Figure 7 – UNInstallShield Application removing BlackICE.

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.

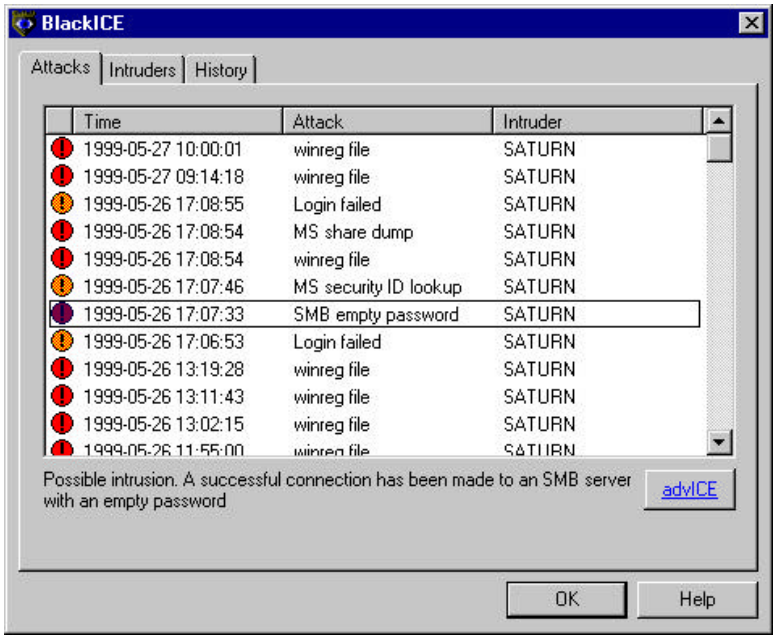
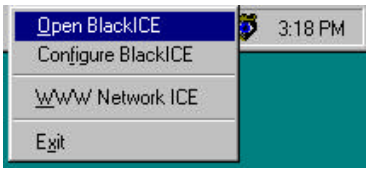


Figure 8 – The BlackICE application displaying the Attacks Tab.

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).

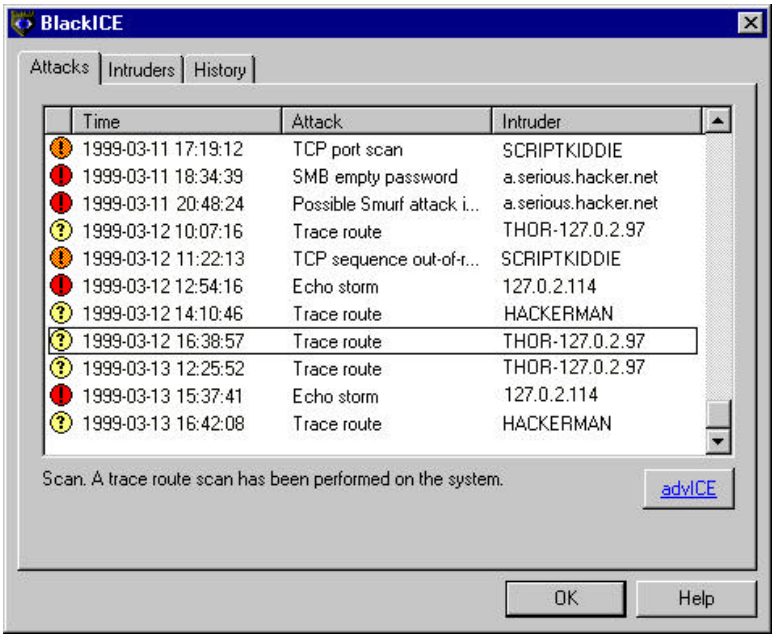


Figure 9 – Detected events are listed as critical, serious, suspicious, or informational on the Attacks tab.

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).

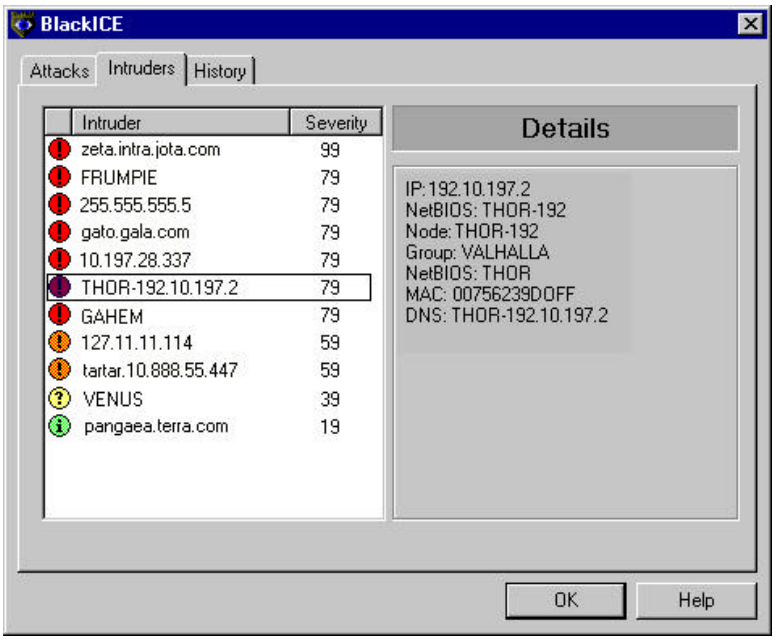


Figure 10 – Intruders tab.

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.

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.

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.

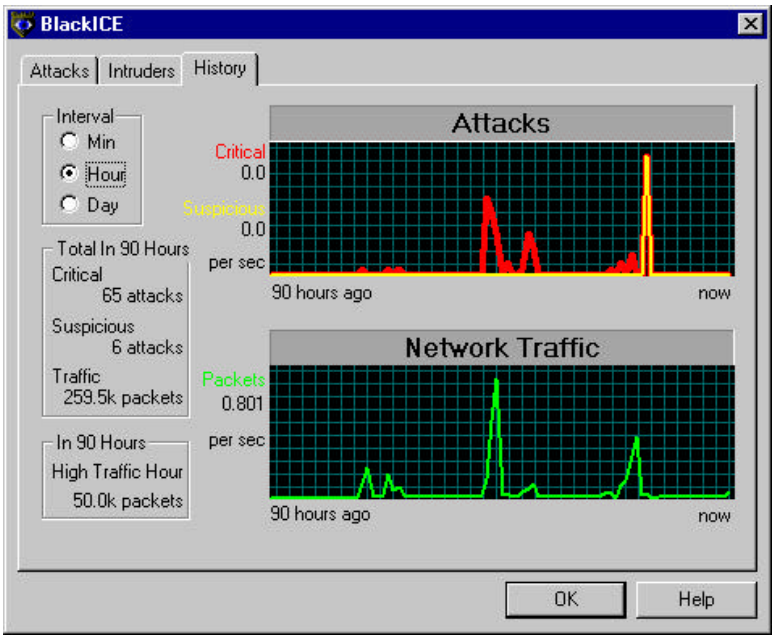


Figure 11 – The History tab is a good way to spot trends in intrusions.

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.

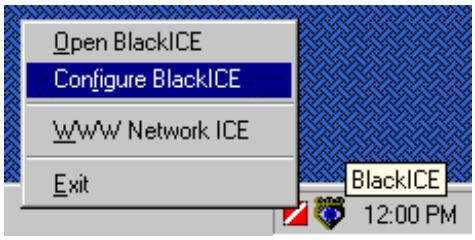
High Traffic: The highest amount of network traffic, measured in number of packets, for the selected interval. Traffic is tracked on the Network Traffic graph with a green line.

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.

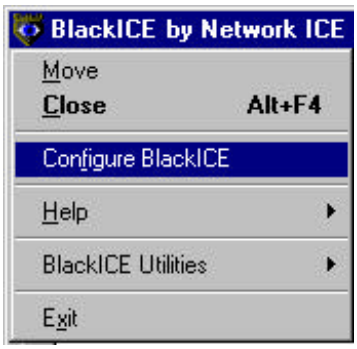
Configuring BlackICE

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.
2. Select BlackICE Configuration from the pop-up menu.



1. From the BlackICE Summary Application, right click on the BlackICE icon in the upper, left corner of the window.
2. Select BlackICE Configuration from the pop-up menu.

	100-80	**Critical Event**: This is a deliberate attack on your system for the purpose of damaging data or crashing the system.
	80-40	**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.
	40-20	**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.
	20-0	**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.

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

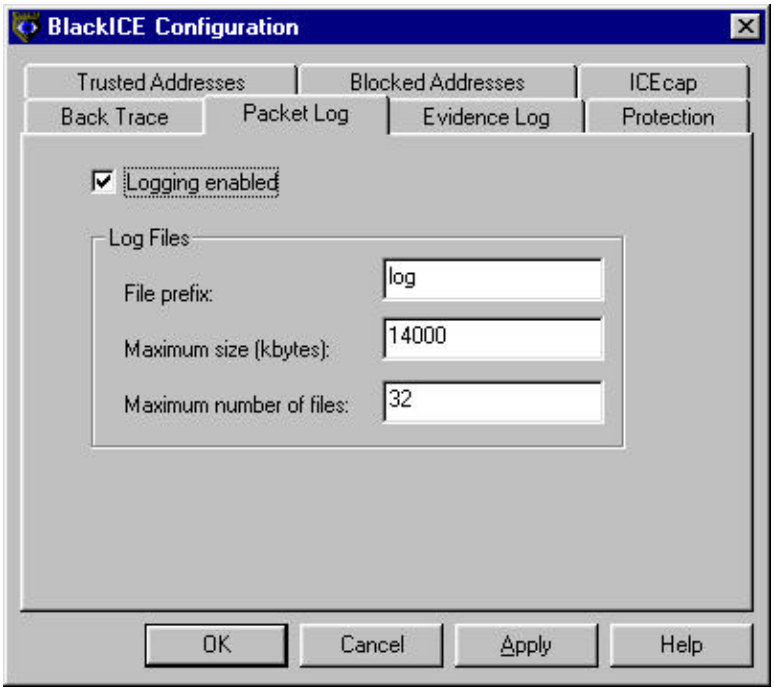


Figure 13 – The Packet Log tab.

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. Use **%d** to place an incremented counter in the file name. For example, if you enter ABC%d the file names will be ABC0001.log, ABC0002.log, etc. The default file prefix is "log".

Maximum Size (kbytes): Specifies the maximum size, in kilobytes, for each log file. The default value for the maximum log file size is 0.

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

BlackICE constantly monitors your system. When suspicious activity is detected, BlackICE immediately begins to collect information about the event. This information can be placed in Evidence Files. An evidence file is a raw dump of all network traffic from a suspected intruder.

Evidence files are not the same as Packet Logging. Evidence collection is performed for a specific event. Also an evidence file contains much more information than a packet log. A packet log is merely a report of all network traffic. For more information, see page 29 for more information.

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.

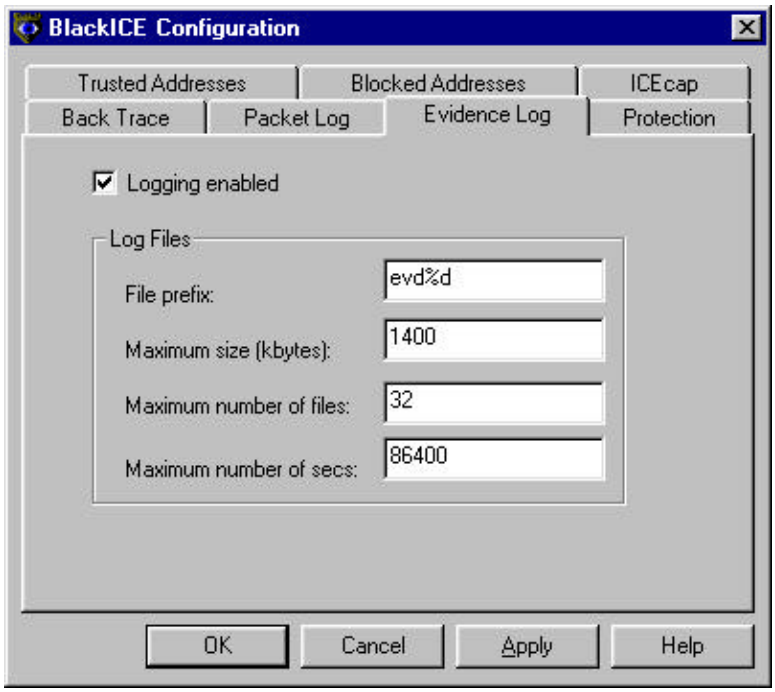


Figure 14 – The Evidence Log tab.

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 ABC%d the file names will be ABC0001.enc, ABC0002.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 kbytes.

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*, BlackICE only blocks file sharing over the Internet, unless Internet file sharing is specifically enabled on the Protection tab. Internet file sharing allows the user to share files on their disk with others across the Internet. Blocking Internet file sharing ensures that hackers cannot download files off your computer. All other ports remain open and unblocked. File sharing on an internal network remains unaffected even though Internet file sharing is disabled. 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 how security levels work, see page 4.

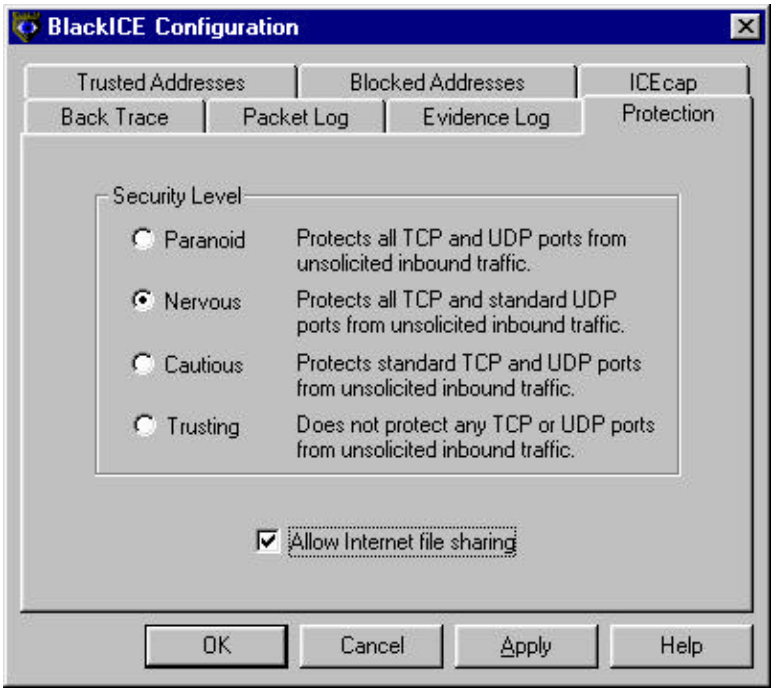


Figure 15 – The Protection Tab

Setting the Security Level

1. Select the **Security Level** you wish to use. The default Security Level is **Cautious**.
2. If you wish to enable file sharing over the Internet, check the appropriate box. Internet file sharing is disabled by default.

WARNING: Enabling Internet file sharing makes your computer very vulnerable to simple intrusions. However, when enabled, you can connect to your computer over the Internet and upload or download files. For example, if you want to transfer files from home to your work computer, this option must be enabled. Network ICE does not recommend leaving Internet file sharing enabled for extended periods of time.

3. 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. This should only be used for trusted ICEpick servers, network management servers, or other devices that may inadvertently trigger BlackICE events.

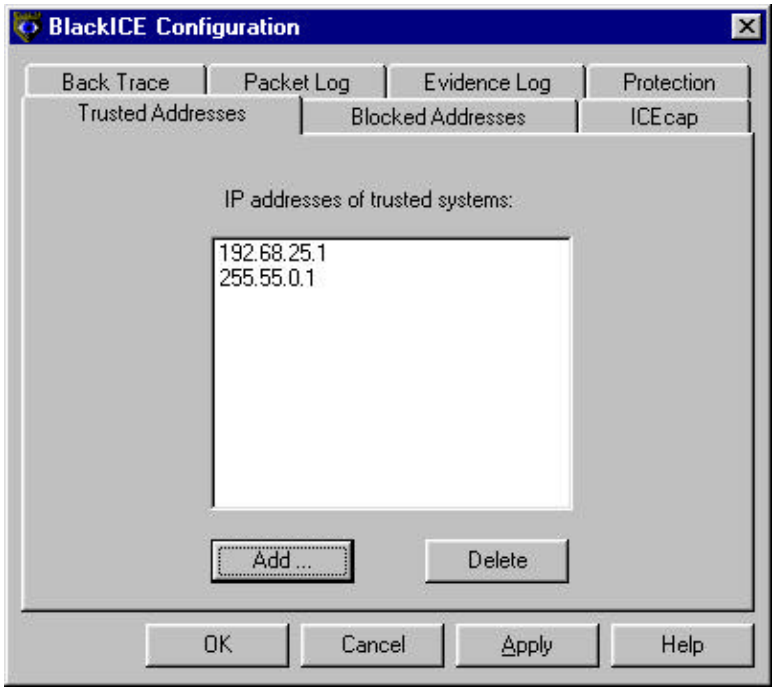


Figure 16 – Trusted Addresses tab.

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. This action cannot be reversed.

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 17 -- 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**.

NOTE: Deletion of an address from the trusted addresses list occurs immediately when you click **Delete**. This action cannot be reversed.

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.

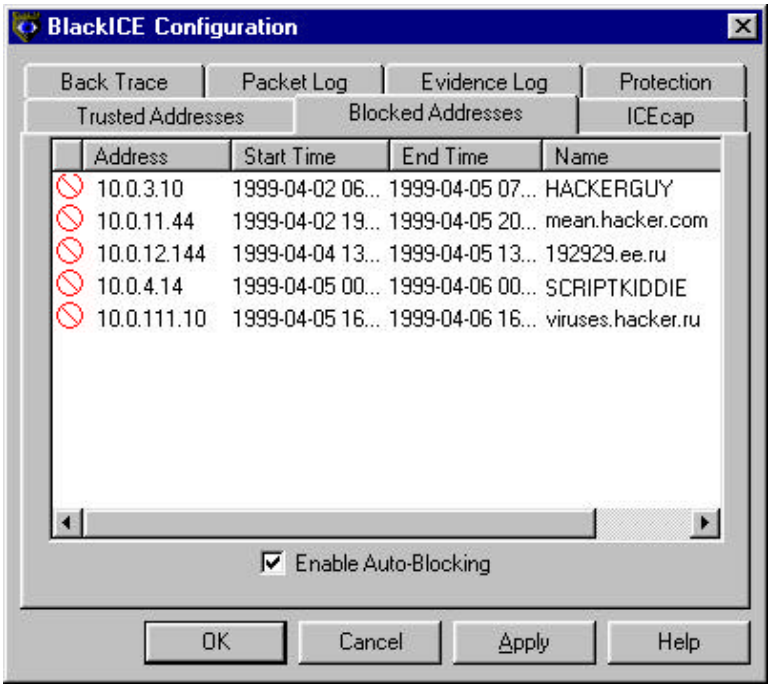


Figure 18 – Blocked Addresses tab.

- **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.
- **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 25 for more information.

ICEcap Tab

BlackICE can integrate 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

Depending on the features enabled in your license key, the ICEcap tab may be disabled. This tab allows you to establish the parameters for BlackICE to report events to an ICEcap server.

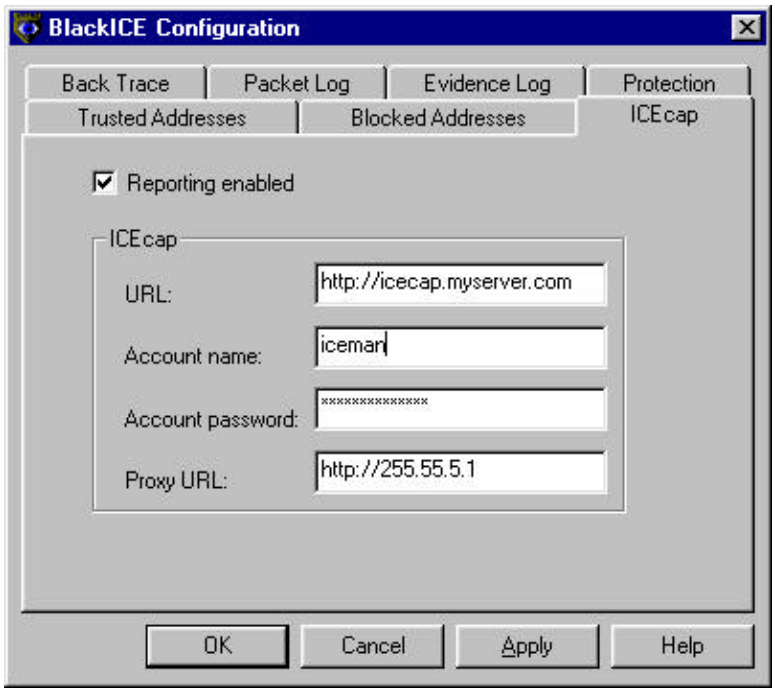


Figure 19 – ICEcap tab.

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 8082, the entry would be: `http://ICECAP:8082` (the default).

Account Name: The ICEcap account number to use when uploading data. Refer to your ICEcap documentation for more information about account numbers. The default account name is “default”.

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.

Clearing the Attack List

After a while, the attack list for BlackICE may become quite large. You can use the BlackICE Utilities to clear the attack list.

1. Right-click on the BlackICE icon within the BlackICE Summary Application.
2. Select **BlackICE Utilities**, then select **Clear Attack List** from the sub menu.

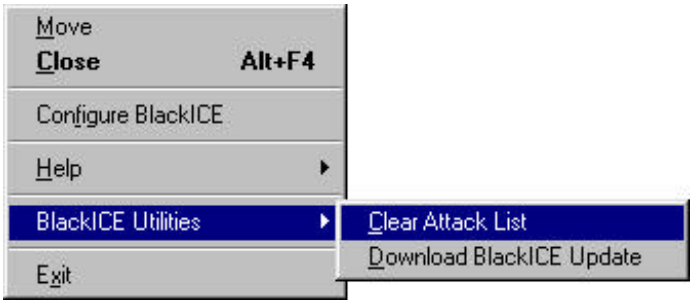


Figure 20 - Clearing the Attack List.

3. A confirmation dialog box is displayed. Click **OK** to confirm clearing the list.

Updating BlackICE

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

1. Right-click on the BlackICE icon within the BlackICE Summary Application.
2. Select **BlackICE Utilities**, then select **Download BlackICE Update** from the sub menu.

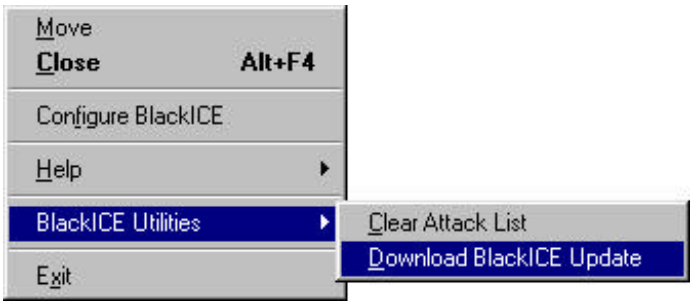


Figure 21 – Download BlackICE Update.

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. Download the new version and install it as instructed on the update web page.

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

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 23 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.

Disabling 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.

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 **BlackICE** in the list and click **End Task**.

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

4 SYSTEM SECURITY

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 of 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 Internet Service Providers (ISPs) forget to erect barriers to stop the hackers. Moreover, most home systems have no protection whatsoever from hackers.

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

External intrusions 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.

Stopping Hackers

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.
- If you have network, install Network ICE's ICEpick. ICEpick 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.
- If you have a DSL or cable modem connection, turn your computer off when not using it. These "always-on" connections are particularly vulnerable because they provide more opportunities for hackers to find your computer.
- 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 careful of files e-mailed to you from people you do not know. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- 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.
- Be careful with e-mail or web site that originate in foreign countries, especially Russia and the former Soviet states. Russia has a very active hacker subculture. Many hackers use off-shore accounts and connections to hack because it is more difficult to backtrace these accounts.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable. If this happens a lot, notify your ISP and reboot your machine. In extreme cases, hackers can damage the operating system on your computer, which would require re-installing the operating system.
- 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 ISP. Some serious Windows errors are the result of hackers or viruses on a system.
- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in a social intrusion.

5 How to Handle Attacks

This section describes all the attacks that BlackICE can detect as well as suggested ways to deal with those attacks. Please note, that these are merely suggested responses.

Index of Attacks

Use this index to quickly locate more information about an attack.

.

.bash.history URL · 40
.lnk URL type · 40
.url URL type · 40

A

Ascend attack · 41
Automount using rpc.statd · 41

B

Back Orifice ping · 41
Back Orifice response · 41
Back Orifice scan seen · 42
bat URL type · 42
Boink attack · 42
Bonk attack · 42

C

CGI aglimpse · 43
CGI anyform2 · 43
CGI bash · 43
CGI campas · 43
CGI convert.bas · 44
CGI csh. · 44
CGI faxsurvey · 44
CGI finger. · 44
CGI formmail · 45
CGI formmail.pl · 45
CGI glimpse · 45
CGI guestbook · 45
CGI guestbook.pl · 46
CGI handler · 46
CGI htmlscript · 46
CGI info2www · 46
CGI machineinfo · 47
CGI mlog.html · 47
CGI mylog.html · 47
CGI newdsn.exe · 47
CGI nph-test-cgi · 48
CGI perl · 48
CGI perl.exe · 48
CGI pfdispaly.cgi · 48
CGI phf · 49
CGI rguest.exe · 49
CGI rksh · 49
CGI sh · 49
CGI snork.bat · 50
CGI tcsh · 50
CGI test-cgi · 50
CGI test-cgi.tcl · 50
CGI uploader.exe · 51
CGI view-source · 51
CGI webdist.cgi · 51
CGI webgais · 51
CGI websendmail. · 52
CGI wguest.exe · 52
CGI win-c-sample.exe · 52
CGI wwwboard.pl · 52
cmd URL type · 53
Cold Fusion sample URL · 53
Cybercop FTP scan · 53

D

DNS cache corruption · 53
DNS Chaos lookup · 54
DNS HINFO query · 54
DNS Internet not 4 bytes · 55
DNS I-Query · 54
DNS I-Query exploit · 54
DNS malformed · 55
DNS name very long · 55
DNS non-Internet lookup · 55
DNS port probe · 56
DNS spoof attempt · 56
DNS spoof successful · 56
DNS zone transfer · 56
Duplicate IP address · 57

E

Echo storm · 57
ExploreZip virus · 57
EZMall data URL · 57

F

favico.ico bad format · 58
Finger · 58
Finger command · 58
Finger forwarding · 58
Finger forwarding very long · 59
FINGER port probe · 59
Fragment overlap · 59
FrontPage service.pwd · 59
FTP command line very long · 60
FTP CWD ~root command · 60
FTP CWD directory very long · 60
FTP file name very long · 60
FTP invalid PORT command · 61
FTP login failed · 61
FTP password very long · 61
FTP PORT bounce to other system · 61
FTP port probe · 62
FTP PORT restricted · 62
FTP SITE EXEC command · 62
FTP user name very long · 62

H

HP Remote watch · 63
HTTP asp with . appended · 63
HTTP cgi starting with php · 63
HTTP cgi with ~ appended · 63
HTTP GET data contains ../../../.. · 64
HTTP GET data very long · 64
HTTP GET data with repeated char · 64
HTTP login failed · 64
HTTP port probe · 65
HTTP URL contains ../../../.. · 65
HTTP URL has many slashes · 65
HTTP URL very long · 65
HTTP URL with $DATA appended · 66
HTTP URL with %81-%fe appended · 66
HTTP URL with blank appended · 66

I

ICMP subnet mask request · 66
ICMP unreachable storm · 67
IDENT port probe · 67
identd invalid response · 67
identd scan · 67
IGMP buffer overflow · 68
IIS data service query · 68
IIS malformed HTR request · 68
IIS password change · 68
IIS sample URL · 69
IMAP4 authentication very long · 69
IMAP4 command very long · 69
IMAP4 login failed · 69
IMAP4 password very long · 70
IMAP4 port probe · 70
IMAP4 user name very long · 70
IP source route · 70
IRC buffer overflow · 71
IRC port probe · 71
ISS scan · 71
ISS UDP scan · 71

L

Land attack · 72
Last fragment length changed · 72

M

Melissa virus · 72
MS domain dump · 72
MS malformed LSA request · 73
MS name lookup · 73
MS rpc dump · 73
MS security ID lookup · 73
MS share dump · 74
MSRPC port probe · 74

N

NETBIOS names query · 74
NETBIOS port probe · 74
NetBus seen · 75
NewTear attack · 75
NNTP name very long · 75
NNTP pipe seen · 75
NNTP port probe · 76

O

Order Form data URL · 76
Order Form v1.2 data URL · 76

P

Papa virus · 76
passwd file · 77
PCAnywhere login failed · 77
PCAnywhere ping · 77
PCANYWHERE port probe · 77
PICTURE.EXE virus · 78
Ping of death · 78
Ping sweep · 78
POP3 command very long · 78
POP3 login failed · 79
POP3 MIME file name very long · 79
POP3 password very long · 79
POP3 port probe · 79
POP3 user name very long · 80
Possible Fraggle attack initiated · 80
Possible Smurf attack initiated · 80
PPTP malformed · 80
PPTP port probe · 81
pwl file type · 81

Q

Quake backdoor · 81
QuikStore configuration URL · 81

R

Rlogin -froot backdoor · 82
RLogin login failed · 82
Rlogin login name very long · 82
Rlogin password very long · 82
RLOGIN port probe · 83
rpc nfs/lockd attack · 83
rpc.admind auth · 83
rpc.automountd overflow · 83
rpc.mountd overflow · 83
rpc.nfs mknod · 84
rpc.nfs uid is zero · 84
rpc.nisd long name · 84
rpc.pcnfs backdoor · 84
rpc.portmap dump · 85
rpc.portmap.set · 85
rpc.portmap.unset · 85
rpc.statd dotdot file create · 85
rpc.statd overflow · 86
rpc.tooltalkd overflow · 86
rpc.ypupdated command · 86
RWHO host name very long · 86

S

sam file · 87
Shopping cart order URL · 87
Site Server sample URL · 87
SMB empty password · 87
SMB file name very long · 88
SMB I/O using printer share · 88
SMB login failed · 88
SMB malformed · 88
SMB password very long · 89
SMB unencrypted password · 89
SMB Unicode file name very long · 89
SMTP command very long · 89
SMTP corrupted MAIL command · 90
SMTP corrupted RCPT command · 90
SMTP DEBUG command · 90
SMTP email name very long · 90
SMTP EXPN command · 91
SMTP login failed · 91
SMTP login name very long · 91
SMTP mail to decode alias · 91
SMTP mail to uudecode alias · 92
SMTP MIME file name very long · 92
SMTP pipe in mail address · 92
SMTP port probe · 92
SMTP relay attempt · 93
SMTP too many errors · 93
SMTP Too many recipients · 93
SMTP uucp-style recipient · 93
SMTP VRFY command · 94
SMTP WIZ command · 94
SNMP backdoor · 94
SNMP Corrupt · 94
SNMP Crack · 95
SNMP discovery broadcast · 95
Snork attack · 95
SOCKS port probe · 95
SoftCart password URL · 96
SQL login failed · 96
SQL port probe · 96
SUNRPC port probe · 96
SynDrop attack · 97

T

TCP port probe · 97
TCP port scan · 97
TCP sequence out-of-range · 97
TCP SYN flood · 98
Teardrop attack · 98
TearDrop2 attack · 98
Telnet abuse · 98
Telnet login failed · 99
Telnet login name very long · 99
Telnet password very long · 99
TELNET port probe · 99
Telnet terminal type very long · 100
TFTP file name very long · 100

TFTP file not found · 100
Too much fragmentation · 100
Trace route · 101
Trojan horse probe · 101

U

UDP port loopback · 101
UDP port scan · 101
Unknown IP protocol · 102

W

W97M.Marker.a virus · 102
WebStore admin URL · 102
WhatsUp scan · 102
win.ini file · 103
WinNuke attack · 103
winreg file · 103

X

XWINDOWS port probe · 103

BlackICE Attacks

This section lists all of the attacks BlackICE can detect. Attacks are broken out into six categories: *nuke attacks*, *scans*, *service hacks*, *Trojans/backdoors*, and *client attacks*. Alike attacks are grouped together under one entry.

.bash.history URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Patch Cobalt Qube/RaQ server.

Details: This file contains a history of shell commands some of which may contain confidential information.

Issue ID: 2002544

More Info: http://www.networkice.com/advice/Intrusions/2002544/default.htm

.lnk URL type

Impact: An intruder launches a program or an executable that could cause damage to a computer.

Defense Patch browser software.

Details: Attempt to access a lnk file which may cause access to privileged information on a client's system.

Issue ID: 2002546

More Info: http://www.networkice.com/advice/Intrusions/2002546/default.htm

.url URL type

Impact: An intruder launches a program or an executable that could cause damage to a computer.

Defense Patch browser software.

Details: Attempt to access a url file which may cause access to privileged information on the client system.

Issue ID: 2002545

More Info: http://www.networkice.com/advice/Intrusions/2002545/default.htm

Ascend attack

Impact: Older versions of Ascend routers may crash.

Defense Download and install patch from Ascend.

Details: Attacker sends a frame that can crash older versions of Ascend routers.

Issue ID: 2000204

More Info: http://www.networkice.com/advice/Intrusions/2000204/default.htm

Automount using rpc.statd

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: An attacker is using the statd service to execute an automount command on the local system.

Issue ID: 2001716

More Info: http://www.networkice.com/advice/Intrusions/2001716/default.htm

Back Orifice ping

Impact: Back Orifice can give an attacker full access to a system. If an attacker discovers a known Trojan on your system such as Backorifice he can use the application to break into your system and the network.

Defense Filter IP address from attacking source.

Details: Intruder attempts to see if you have BackOrifice installed.

Issue ID: 2001506

More Info: http://www.networkice.com/advice/Intrusions/2001506/default.htm

Back Orifice response

Impact: Intruder gains control of the system.

Defense Use anti-virus software to remove Back Orifice from system.

Details: An intruder is using BackOrifice to remotely control your system; it should be IMMEDIATELY removed from your system.

Issue ID: 2001505

More Info: http://www.networkice.com/advice/Intrusions/2001505/default.htm

Back Orifice scan seen

Impact: Attacker has full access to your machine.

Defense Never run programs given to you by untrustworthy people. Turn off file sharing when on the Internet.

Details: BackOrifice is a Trojan horse application that allows remote administration.

Issue ID: 2001501

More Info: http://www.networkice.com/advice/Intrusions/2001501/default.htm

bat URL type

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a bat file which may have been misplaced in the cgi-bin directory.

Issue ID: 2002501

More Info: http://www.networkice.com/advice/Intrusions/2002501/default.htm

Boink attack

Impact: System crash BSoD (Blue Screen of Death).

Defense Update operating system install filters.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000008

More Info: http://www.networkice.com/advice/Intrusions/2000008/default.htm

Bonk attack

Impact: System crash BSoD (Blue Screen of Death).

Defense Update operating system install filters.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000007

More Info: http://www.networkice.com/advice/Intrusions/2000007/default.htm

CGI aglimpse

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002503

More Info: http://www.networkice.com/advice/Intrusions/2002503/default.htm

CGI anyform2

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002504

More Info: http://www.networkice.com/advice/Intrusions/2002504/default.htm

CGI bash

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a Unix shell program; if successful the hacker gains unintended access to a server.

Issue ID: 2002505

More Info: http://www.networkice.com/advice/Intrusions/2002505/default.htm

CGI campas

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002506

More Info: http://www.networkice.com/advice/Intrusions/2002506/default.htm

CGI convert.bas

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002507

More Info: http://www.networkice.com/advice/Intrusions/2002507/default.htm

CGI csh.

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a Unix shell program; if successful the hacker gains unintended access to a server.

Issue ID: 2002508

More Info: http://www.networkice.com/advice/Intrusions/2002508/default.htm

CGI faxsurvey

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002509

More Info: http://www.networkice.com/advice/Intrusions/2002509/default.htm

CGI finger.

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute the finger program which may allow unintended access to a server.

Issue ID: 2002510

More Info: http://www.networkice.com/advice/Intrusions/2002510/default.htm

CGI formmail

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002511

More Info: http://www.networkice.com/advice/Intrusions/2002511/default.htm

CGI formmail.pl

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002512

More Info: http://www.networkice.com/advice/Intrusions/2002512/default.htm

CGI glimpse

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002513

More Info: http://www.networkice.com/advice/Intrusions/2002513/default.htm

CGI guestbook

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002514

More Info: http://www.networkice.com/advice/Intrusions/2002514/default.htm

CGI guestbook.pl

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002515

More Info: http://www.networkice.com/advice/Intrusions/2002515/default.htm

CGI handler

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002516

More Info: http://www.networkice.com/advice/Intrusions/2002516/default.htm

CGI htmlscript

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002517

More Info: http://www.networkice.com/advice/Intrusions/2002517/default.htm

CGI info2www

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002518

More Info: http://www.networkice.com/advice/Intrusions/2002518/default.htm

CGI machineinfo

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002519

More Info: http://www.networkice.com/advice/Intrusions/2002519/default.htm

CGI mlog.html

Impact: An intruder may read any arbitrary file on the system include password and host files.

Defense Update to a secure version of this file.

Details: Attempt to execute a CGI script with known weaknesses.

Issue ID: 2002539

More Info: http://www.networkice.com/advice/Intrusions/2002539/default.htm

CGI mylog.html

Impact: An intruder may read any arbitrary file on the system include password and host files.

Defense Update to a secure version of this file.

Details: Attempt to execute a CGI script with known weaknesses.

Issue ID: 2002540

More Info: http://www.networkice.com/advice/Intrusions/2002540/default.htm

CGI newdsn.exe

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002542

More Info: http://www.networkice.com/advice/Intrusions/2002542/default.htm

CGI nph-test-cgi

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002520

More Info: http://www.networkice.com/advice/Intrusions/2002520/default.htm

CGI perl

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute the perl program which may allow unintended access to a server.

Issue ID: 2002521

More Info: http://www.networkice.com/advice/Intrusions/2002521/default.htm

CGI perl.exe

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute the perl program which may allow unintended access to a server.

Issue ID: 2002522

More Info: http://www.networkice.com/advice/Intrusions/2002522/default.htm

CGI pfdispaly.cgi

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002523

More Info: http://www.networkice.com/advice/Intrusions/2002523/default.htm

CGI phf

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002524

More Info: http://www.networkice.com/advice/Intrusions/2002524/default.htm

CGI rguest.exe

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002525

More Info: http://www.networkice.com/advice/Intrusions/2002525/default.htm

CGI rksh

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a Unix shell program; if successful the hacker gains unintended access to a server.

Issue ID: 2002527

More Info: http://www.networkice.com/advice/Intrusions/2002527/default.htm

CGI sh

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a Unix shell program; if successful the hacker gains unintended access to a server.

Issue ID: 2002528

More Info: http://www.networkice.com/advice/Intrusions/2002528/default.htm

CGI snork.bat

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002541

More Info: http://www.networkice.com/advice/Intrusions/2002541/default.htm

CGI tcsh

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a Unix shell program; if successful the hacker gains unintended access to a server.

Issue ID: 2002529

More Info: http://www.networkice.com/advice/Intrusions/2002529/default.htm

CGI test-cgi

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002531

More Info: http://www.networkice.com/advice/Intrusions/2002531/default.htm

CGI test-cgi.tcl

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI script with known weaknesses.

Issue ID: 2002530

More Info: http://www.networkice.com/advice/Intrusions/2002530/default.htm

CGI uploader.exe

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002538

More Info: http://www.networkice.com/advice/Intrusions/2002538/default.htm

CGI view-source

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002532

More Info: http://www.networkice.com/advice/Intrusions/2002532/default.htm

CGI webdist.cgi

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI script with known weaknesses.

Issue ID: 2002533

More Info: http://www.networkice.com/advice/Intrusions/2002533/default.htm

CGI webgais

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002534

More Info: http://www.networkice.com/advice/Intrusions/2002534/default.htm

CGI websendmail.

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002535

More Info: http://www.networkice.com/advice/Intrusions/2002535/default.htm

CGI wguest.exe

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002526

More Info: http://www.networkice.com/advice/Intrusions/2002526/default.htm

CGI win-c-sample.exe

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002536

More Info: http://www.networkice.com/advice/Intrusions/2002536/default.htm

CGI wwwboard.pl

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002537

More Info: http://www.networkice.com/advice/Intrusions/2002537/default.htm

cmd URL type

Impact: Intruder gains access and may potentially crash system.

Defense Remove file if not necessary for operation. If necessary then update to a secure version.

Details: Attempt to execute a cmd file which may have been misplaced in the cgi-bin directory.

Issue ID: 2002502

More Info: http://www.networkice.com/advice/Intrusions/2002502/default.htm

Cold Fusion sample URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Remove ColdFusion documentation sample code example applications and tutorials from on production servers and secure access to these files on workstations.

Details: Attempt to access Cold Fusion sample file which may cause unintended access to data.

Issue ID: 2002554

More Info: http://www.networkice.com/advice/Intrusions/2002554/default.htm

Cybercop FTP scan

Impact: Attacker finds vulnerabilities that can be exploited.

Defense Install dynamic filters that can selectively stop these scans.

Details: An intruder is using the Network Associates Cybercop Scanner to probe your system for weaknesses.

Issue ID: 2001510

More Info: http://www.networkice.com/advice/Intrusions/2001510/default.htm

DNS cache corruption

Impact: Attacker uses one of a number of techniques to corrupt your DNS cache.

Defense Most DNS servers have no defense to some techniques.

Details: Attacker corrupts your DNS cache with his own entries; traffic can be redirected to another site.

Issue ID: 2000402

More Info: http://www.networkice.com/advice/Intrusions/2000402/default.htm

DNS Chaos lookup

Impact: Attacker retrieves version number of DNS server.

Defense Patch/upgrade DNS server.

Details: A DNS query includes a non-Internet address.

Issue ID: 2000411

More Info: http://www.networkice.com/advice/Intrusions/2000411/default.htm

DNS HINFO query

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Limit the information revealed on your DNS servers. Configure separate DNS servers for Internet and internal use.

Details: A DNS HINFO query was done; a hacker may be collecting information prior to launching an attack.

Issue ID: 2000407

More Info: http://www.networkice.com/advice/Intrusions/2000407/default.htm

DNS I-Query

Impact: This is an attempt to crash and compromise the DNS server.

Defense Patch/upgrade DNS server.

Details: System sees unusual DNS traffic; this most often indicates an intrusion attempt.

Issue ID: 2000409

More Info: http://www.networkice.com/advice/Intrusions/2000409/default.htm

DNS I-Query exploit

Impact: Intruder gains root access on your name server or disrupts normal operation of your name server.

Defense Disable inverse queries.

Details: Intruder is attempting to gain control of the DNS service via a well-known exploit.

Issue ID: 2000410

More Info: http://www.networkice.com/advice/Intrusions/2000410/default.htm

DNS Internet not 4 bytes

Impact: May crash the DNS server.

Defense Patch/upgrade DNS server.

Details: Attacker performs a DNS query with an Internet address that is not 4 bytes.

Issue ID: 2000406

More Info: http://www.networkice.com/advice/Intrusions/2000406/default.htm

DNS malformed

Impact: May crash the DNS server.

Defense Patch/upgrade DNS server.

Details: An ill-constructed DNS packet has been seen.

Issue ID: 2000405

More Info: http://www.networkice.com/advice/Intrusions/2000405/default.htm

DNS name very long

Impact: This is an attempt to crash and compromise the DNS server.

Defense Patch/upgrade DNS server.

Details: Attacker sends a DNS query that includes a very long system name; this may be an attempt to shutdown the DNS server.

Issue ID: 2000403

More Info: http://www.networkice.com/advice/Intrusions/2000403/default.htm

DNS non-Internet lookup

Impact: Attacker is prowling around your system.

Defense Patch/upgrade DNS server.

Details: This may be an attempt to corrupt a DNS server

Issue ID: 2000404

More Info: http://www.networkice.com/advice/Intrusions/2000404/default.htm

DNS port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003011

More Info: http://www.networkice.com/advice/Intrusions/2003011/default.htm

DNS spoof attempt

Impact: Subsequent attempts to redirect traffic to another site may be successful.

Defense Update DNS server.

Details: An attacker has attempted (unsuccessfully) to redirect traffic to another site.

Issue ID: 2000414

More Info: http://www.networkice.com/advice/Intrusions/2000414/default.htm

DNS spoof successful

Impact: The DNS cache has most likely been corrupted and subsequent Internet accesses may go to the wrong address.

Defense DNS service should be restarted.

Details: Attacker has succeeded in redirecting traffic to another site.

Issue ID: 2000408

More Info: http://www.networkice.com/advice/Intrusions/2000408/default.htm

DNS zone transfer

Impact: Attacker lists the systems in your network.

Defense Limit the information revealed on your DNS servers. Configure separate DNS servers for Internet and internal use.

Details: With a list of systems in your network the attacker can target obvious points of attack such as routers or file servers.

Issue ID: 2000401

More Info: http://www.networkice.com/advice/Intrusions/2000401/default.htm

Duplicate IP address

Impact: Someone is probing the system.

Defense Check configuration of systems reporting that IP address.

Details: A duplicate IP address was detected; a system may be misconfigured or an IP address has recently changed.

Issue ID: 2002301

More Info: http://www.networkice.com/advice/Intrusions/2002301/default.htm

Echo storm

Impact: System and network slow down.

Defense These services are used only in testing and should be disabled especially when connected to the Internet.

Details: A large number of ICMP echo frames have been sent to a single system; these may have resulted from a Smurf attack.

Issue ID: 2000102

More Info: http://www.networkice.com/advice/Intrusions/2000102/default.htm

ExploreZip virus

Impact: This email virus will damage your files if you execute it.

Defense Immediately rid your system of this virus.

Details: This virus has been received or sent via email.

Issue ID: 2002205

More Info: http://www.networkice.com/advice/Intrusions/2002205/default.htm

EZMall data URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Properly install shopping cart software.

Details: Attempt to access EZMall customer order directory.

Issue ID: 2002551

More Info: http://www.networkice.com/advice/Intrusions/2002551/default.htm

favico.ico bad format

Impact: Intruder gains access and may potentially crash system.

Defense Upgrade web browser Server.

Details: Downloaded ICON file is suspicious; it may be used to break into system on which the browser is executing.

Issue ID: 2002555

More Info: http://www.networkice.com/advice/Intrusions/2002555/default.htm

Finger

Impact: Attacker finds out who is logged on and information about users.

Defense Disable finger service.

Details: Attacker can see which users are connected; this information can be extremely useful for hacking into the system at a later time.

Issue ID: 2001101

More Info: http://www.networkice.com/advice/Intrusions/2001101/default.htm

Finger command

Impact: Attacker may collect information on users of the system.

Defense Upgrade operating system disable finger services.

Details: Attacker attempts to execute a remote command using a finger server.

Issue ID: 2001104

More Info: http://www.networkice.com/advice/Intrusions/2001104/default.htm

Finger forwarding

Impact: Attacker finds out who is logged on and information about users on another system.

Defense Disable finger service.

Details: Attacker attempts to use the finger service to forward a finger request to another system.

Issue ID: 2001102

More Info: http://www.networkice.com/advice/Intrusions/2001102/default.htm

Finger forwarding very long

Impact: Attacker overloads the system using finger commands.

Defense Upgrade operating system disable finger services.

Details: Attacker attempts to forward a very long finger command.

Issue ID: 2001103

More Info: http://www.networkice.com/advice/Intrusions/2001103/default.htm

FINGER port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003007

More Info: http://www.networkice.com/advice/Intrusions/2003007/default.htm

Fragment overlap

Impact: System crashes.

Defense Upgrade operating system to patch this vulnerability. Install filters to stop attacks.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000009

More Info: http://www.networkice.com/advice/Intrusions/2000009/default.htm

FrontPage service.pwd

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Upgrade Front Page Server.

Details: Attempt to execute a CGI program with known weaknesses.

Issue ID: 2002543

More Info: http://www.networkice.com/advice/Intrusions/2002543/default.htm

FTP command line very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade FTP server to patch this known bug.

Details: Attacker submits an unusually long command to attempt to break in or shutdown a server.

Issue ID: 2001310

More Info: http://www.networkice.com/advice/Intrusions/2001310/default.htm

FTP CWD ~root command

Impact: Exploits a bug in FTP servers that gains access to the entire FTP server.

Defense Upgrade FTP server to patch this known bug.

Details: Attacker has attempted to connect to the FTP server as the root user.

Issue ID: 2001304

More Info: http://www.networkice.com/advice/Intrusions/2001304/default.htm

FTP CWD directory very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade FTP server to patch this known bug.

Details: Buffer overflow attempt.

Issue ID: 2001308

More Info: http://www.networkice.com/advice/Intrusions/2001308/default.htm

FTP file name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade FTP server to patch this known bug.

Details: Buffer overflow attempt; this may be an intentional effort to overflow a buffer on a server.

Issue ID: 2001309

More Info: http://www.networkice.com/advice/Intrusions/2001309/default.htm

FTP invalid PORT command

Impact: An attacker is prowling around your system.

Defense No known defense.

Details: The FTP PORT command can't be recognized; this may indicate an attempt to crash or break in to the server.

Issue ID: 2001301

More Info: http://www.networkice.com/advice/Intrusions/2001301/default.htm

FTP login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple FTP login failures using bad user names and/or passwords.

Issue ID: 2001601

More Info: http://www.networkice.com/advice/Intrusions/2001601/default.htm

FTP password very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade FTP server to patch this known bug.

Details: Buffer overflow attempt.

Issue ID: 2001307

More Info: http://www.networkice.com/advice/Intrusions/2001307/default.htm

FTP PORT bounce to other system

Impact: An attacker establishes a connection between the FTP server machine and an arbitrary port on another system. This connection may be used to bypass access controls that would otherwise apply.

Defense Ensure that your FTP server software cannot establish connections to arbitrary machines.

Details: The FTP PORT command was used to setup an FTP transfer to another system.

Issue ID: 2001302

More Info: http://www.networkice.com/advice/Intrusions/2001302/default.htm

FTP port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003004

More Info: http://www.networkice.com/advice/Intrusions/2003004/default.htm

FTP PORT restricted

Impact: An attacker establishes a connection between the FTP server machine and a well-known port on another system. This connection may be used to bypass access controls that would otherwise apply.

Defense Ensure that your FTP server software cannot establish connections to arbitrary machines.

Details: The FTP PORT command has been used to setup an FTP transfer to a well-known port number.

Issue ID: 2001303

More Info: http://www.networkice.com/advice/Intrusions/2001303/default.htm

FTP SITE EXEC command

Impact: Exploits a bug in FTP servers that gains access to the entire FTP server.

Defense Upgrade FTP server to patch this known bug.

Details: Attacker has attempted to execute a command on the FTP server.

Issue ID: 2001305

More Info: http://www.networkice.com/advice/Intrusions/2001305/default.htm

FTP user name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade FTP server to patch this known bug.

Details: Buffer overflow attempt.

Issue ID: 2001306

More Info: http://www.networkice.com/advice/Intrusions/2001306/default.htm

HP Remote watch

Impact: Attacker can add or change privileged system files that then compromise system security and gain root access or destroy files.

Defense Remote Watch package is a system management tool whose capabilities have been largely incorporated in the System Administration Manager (SAM). These files can not be patched but should be removed as recommended by in HP Security Advisory #9610-039.

Details: An intruder attempts to connect to the HP Remote Watch program.

Issue ID: 2001504

More Info: http://www.networkice.com/advice/Intrusions/2001504/default.htm

HTTP asp with . appended

Impact: Attackers can access files which may contain user ids and passwords.

Defense Update HTTP server software.

Details: A specially constructed URL may allow access to Web page source code on the server.

Issue ID: 2000604

More Info: http://www.networkice.com/advice/Intrusions/2000604/default.htm

HTTP cgi starting with php

Impact: Attackers can execute commands on system.

Defense Update HTTP server software.

Details: A specially constructed URL starting with php and ending with cgi may allow undesirable access to the system.

Issue ID: 2000602

More Info: http://www.networkice.com/advice/Intrusions/2000602/default.htm

HTTP cgi with ~ appended

Impact: Attackers can access files and directories from the virtual web root.

Defense Update HTTP server software.

Details: An attempt has been made to access a backup of a cgi file.

Issue ID: 2000605

More Info: http://www.networkice.com/advice/Intrusions/2000605/default.htm

HTTP GET data contains ../../../..

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense No known defense. The data may be legitimate.

Details: The data passed to a URL has a suspicious pathname which might be used to access privileged files.

Issue ID: 2000609

More Info: http://www.networkice.com/advice/Intrusions/2000609/default.htm

HTTP GET data very long

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense No known defense. The URL may be legitimate.

Details: A URL containing a very long data string was detected; this may indicate an intrusion attempt.

Issue ID: 2000608

More Info: http://www.networkice.com/advice/Intrusions/2000608/default.htm

HTTP GET data with repeated char

Impact: Intruder may be attempting to break-in

Defense Attacker attempts to overflow a buffer on the server

Details: The data passed to a URL contains the same character repeated many times; this often signals a buffer overflow attempt

Issue ID: 2000611

More Info: http://www.networkice.com/advice/Intrusions/2000611/default.htm

HTTP login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple HTTP authentication failures using bad user names and/or passwords.

Issue ID: 2001602

More Info: http://www.networkice.com/advice/Intrusions/2001602/default.htm

HTTP port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003001

More Info: http://www.networkice.com/advice/Intrusions/2003001/default.htm

HTTP URL contains ../../../..

Impact: Attackers can access files and directories above the virtual web root.

Defense Update HTTP server software.

Details: An intruder may be attempting to access files in a directory which is not intended to be viewable.

Issue ID: 2000603

More Info: http://www.networkice.com/advice/Intrusions/2000603/default.htm

HTTP URL has many slashes

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Update HTTP server software.

Details: Attacker uses a URL containing large number of slashes; this is a probable attempt to crash a system.

Issue ID: 2000606

More Info: http://www.networkice.com/advice/Intrusions/2000606/default.htm

HTTP URL very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Update HTTP server software.

Details: Probable buffer overflow attempt on server URL.

Issue ID: 2000601

More Info: http://www.networkice.com/advice/Intrusions/2000601/default.htm

HTTP URL with %81-%fe appended

Impact: Attacker reads script source code.

Defense Upgrade server software

Details: This URL may allow the attacker to read the source code for server programs.

Issue ID: 2000612

More Info: http://www.networkice.com/advice/Intrusions/2000612/default.htm

HTTP URL with ::$DATA appended

Impact: Attacker reads script source code

Defense Upgrade server software review scripts to remove such hidden information.

Details: This URL may allow the attacker to read the source code for server programs.

Issue ID: 2000607

More Info: http://www.networkice.com/advice/Intrusions/2000607/default.htm

HTTP URL with blank appended

Impact: Attacker reads script source code

Defense Upgrade server software

Details: This URL may allow the attacker to read the source code for server programs.

Issue ID: 2000610

More Info: http://www.networkice.com/advice/Intrusions/2000610/default.htm

ICMP subnet mask request

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense No known defense.

Details: Attacker requests the value of the subnet mask; this provides knowledge about your network's configuration.

Issue ID: 2000105

More Info: http://www.networkice.com/advice/Intrusions/2000105/default.htm

ICMP unreachable storm

Impact: Slows down network connection.

Defense Update operating system.

Details: Attacker sends a large number of ICMP port-unreachable frames to a single IP address.

Issue ID: 2000104

More Info: http://www.networkice.com/advice/Intrusions/2000104/default.htm

IDENT port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003020

More Info: http://www.networkice.com/advice/Intrusions/2003020/default.htm

identd invalid response

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Hostile server is attempting to exploit identd client

Issue ID: 2001901

More Info: http://www.networkice.com/advice/Intrusions/2001901/default.htm

identd scan

Impact: An intruder may be gathering information which could be useful to setup a later attack..

Defense Uninstall identd.

Details: Intruder is scanning systems with identd looking for possible user information.

Issue ID: 2001902

More Info: http://www.networkice.com/advice/Intrusions/2001902/default.htm

IGMP buffer overflow

Impact: System crashes.

Defense Update operating system.

Details: A malformed frame was seen; some operating systems may fail unpredictably.

Issue ID: 2002902

More Info: http://www.networkice.com/advice/Intrusions/2002902/default.htm

IIS data service query

Impact: Intruder gains unauthorized access to server.

Defense Update Web server.

Details: Attempt to access Microsoft IIS remote data service

Issue ID: 2002560

More Info: http://www.networkice.com/advice/Intrusions/2002560/default.htm

IIS malformed HTR request

Impact: Intruder gains access and may break-in or crash system.

Defense Update Web server.

Details: A buffer overflow has been attempted against a well-known weaknesses in Microsoft's Internet Information Server.

Issue ID: 2002559

More Info: http://www.networkice.com/advice/Intrusions/2002559/default.htm

IIS password change

Impact: An intruder may be attempting to log onto a system.

Defense Remove remote-password change feature if not needed.

Details: A password change has been attempted using password change forms the directory IISADMPWD

Issue ID: 2002558

More Info: http://www.networkice.com/advice/Intrusions/2002558/default.htm

IIS sample URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Remove IIS sample files from server.

Details: Attempt to access Microsoft IIS sample file

Issue ID: 2002557

More Info: http://www.networkice.com/advice/Intrusions/2002557/default.htm

IMAP4 authentication very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Probable attempt to break-in using a buffer overflow.

Issue ID: 2000803

More Info: http://www.networkice.com/advice/Intrusions/2000803/default.htm

IMAP4 command very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Attacker submits an unusually long command to attempt to break in or shutdown a server.

Issue ID: 2000804

More Info: http://www.networkice.com/advice/Intrusions/2000804/default.htm

IMAP4 login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple IMAP4 login failures using bad user names and/or passwords.

Issue ID: 2001603

More Info: http://www.networkice.com/advice/Intrusions/2001603/default.htm

IMAP4 password very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Attempt to break in using a long password; this may be an intentional effort to overflow a buffer on a server.

Issue ID: 2000802

More Info: http://www.networkice.com/advice/Intrusions/2000802/default.htm

IMAP4 port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003005

More Info: http://www.networkice.com/advice/Intrusions/2003005/default.htm

IMAP4 user name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Attempt to break in using a long user name;this may be an intentional effort to overflow a buffer on a server.

Issue ID: 2000801

More Info: http://www.networkice.com/advice/Intrusions/2000801/default.htm

IP source route

Impact: Intruder gains unauthorized access to system.

Defense Install dynamic firewall.

Details: Attacker uses IP source routing that in some cases can go around firewalls.

Issue ID: 2000013

More Info: http://www.networkice.com/advice/Intrusions/2000013/default.htm

IRC buffer overflow

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Intruder attempts to compromise IRC service.

Issue ID: 2001801

More Info: http://www.networkice.com/advice/Intrusions/2001801/default.htm

IRC port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003019

More Info: http://www.networkice.com/advice/Intrusions/2003019/default.htm

ISS scan

Impact: Attacker finds vulnerabilities that can be exploited.

Defense Install dynamic filters that can selectively stop these scans.

Details: An intruder is using the ISS Internet Scanner to probe your system for weaknesses.

Issue ID: 2001508

More Info: http://www.networkice.com/advice/Intrusions/2001508/default.htm

ISS UDP scan

Impact: Attacker finds vulnerabilities that can be exploited.

Defense Install dynamic filters that can selectively stop these scans.

Details: An intruder is using the ISS Internet Scanner to probe your system for weaknesses.

Issue ID: 2001509

More Info: http://www.networkice.com/advice/Intrusions/2001509/default.htm

Land attack

Impact: System hangs slows down or crashes.

Defense Update operating system install filters.

Details: Attacker forges a TCP connection from your machine back to your machine causing an infinite loop.

Issue ID: 2000001

More Info: http://www.networkice.com/advice/Intrusions/2000001/default.htm

Last fragment length changed

Impact: System crashes.

Defense Upgrade operating system to patch this vulnerability. Install filters to stop attacks.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000010

More Info: http://www.networkice.com/advice/Intrusions/2000010/default.htm

Melissa virus

Impact: Indirectly this virus could cause a denial of service on your mail server.

Defense Immediately delete this email

Details: An email containing the Melissa virus has been received. You should immediately delete this email

Issue ID: 2002201

More Info: http://www.networkice.com/advice/Intrusions/2002201/default.htm

MS domain dump

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to service.

Details: Attempt to see what NT domains/user names are available.

Issue ID: 2002803

More Info: http://www.networkice.com/advice/Intrusions/2002803/default.htm

MS malformed LSA request

Impact: An intruder is attempting to crash the LSA service.

Defense Update operating system.

Details: A malformed frame was sent to the Security Authority of a Windows server; the server may fail.

Issue ID: 2002806

More Info: http://www.networkice.com/advice/Intrusions/2002806/default.htm

MS name lookup

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to service.

Details: Attempt to lookup an NT user name to see if it is valid.

Issue ID: 2002804

More Info: http://www.networkice.com/advice/Intrusions/2002804/default.htm

MS rpc dump

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to service.

Details: Attempt to see what MS RPC-based services are available.

Issue ID: 2002801

More Info: http://www.networkice.com/advice/Intrusions/2002801/default.htm

MS security ID lookup

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to service.

Details: Attempt to lookup an NT security ID to test its validity.

Issue ID: 2002805

More Info: http://www.networkice.com/advice/Intrusions/2002805/default.htm

MS share dump

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to service.

Details: Attempt to see what NT shares are available.

Issue ID: 2002802

More Info: http://www.networkice.com/advice/Intrusions/2002802/default.htm

MSRPC port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003014

More Info: http://www.networkice.com/advice/Intrusions/2003014/default.htm

NETBIOS names query

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense No known defense.

Details: A hacker may be collecting information prior to launching an attack.

Issue ID: 2000413

More Info: http://www.networkice.com/advice/Intrusions/2000413/default.htm

NETBIOS port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003009

More Info: http://www.networkice.com/advice/Intrusions/2003009/default.htm

NetBus seen

Impact: Attacker has full access to your machine.

Defense Never run programs given to you by untrustworthy people. Turn off file sharing when on the Internet.

Details: NetBus is a Trojan horse application that allows remote administration; it should be immediately removed from your system.

Issue ID: 2001502

More Info: http://www.networkice.com/advice/Intrusions/2001502/default.htm

NewTear attack

Impact: System crash BSoD (Blue Screen of Death).

Defense Update operating system install filters.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000004

More Info: http://www.networkice.com/advice/Intrusions/2000004/default.htm

NNTP name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Patch/upgrade NNTP services.

Details: The name field of a news posting is very long; this may indicate an attempt to overflow a buffer on the system.

Issue ID: 2002401

More Info: http://www.networkice.com/advice/Intrusions/2002401/default.htm

NNTP pipe seen

Impact: Attacker gains access to news server.

Defense Patch/upgrade NNTP services.

Details: A pipe symbol has been seen in an NNTP Control field; commands may be improperly executed on a server.

Issue ID: 2002402

More Info: http://www.networkice.com/advice/Intrusions/2002402/default.htm

NNTP port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003010

More Info: http://www.networkice.com/advice/Intrusions/2003010/default.htm

Order Form data URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Properly install shopping cart software.

Details: Attempt to access Order Form log file containing customer orders.

Issue ID: 2002550

More Info: http://www.networkice.com/advice/Intrusions/2002550/default.htm

Order Form v1.2 data URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Properly install shopping cart software.

Details: Attempt to access Order Form log file containing customer orders.

Issue ID: 2002549

More Info: http://www.networkice.com/advice/Intrusions/2002549/default.htm

Papa virus

Impact: Indirectly this virus could cause a denial of service on your mail server.

Defense Immediately delete this email.

Details: An email containing the Papa virus has been received. You should immediately delete this email.

Issue ID: 2002202

More Info: http://www.networkice.com/advice/Intrusions/2002202/default.htm

passwd file

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to file.

Details: Attempt to access the passwd file which contains encrypted Unix passwords.

Issue ID: 2002701

More Info: http://www.networkice.com/advice/Intrusions/2002701/default.htm

PCAnywhere login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple PCAnywhere login failures using bad user names and/or passwords.

Issue ID: 2001610

More Info: http://www.networkice.com/advice/Intrusions/2001610/default.htm

PCAnywhere ping

Impact: Someone is probing the system.

Defense Select a good password to prevent undesired access to your system.

Details: An intruder sends a special ping to the system to determine whether the PCAnywhere application is available.

Issue ID: 2001507

More Info: http://www.networkice.com/advice/Intrusions/2001507/default.htm

PCANYWHERE port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003012

More Info: http://www.networkice.com/advice/Intrusions/2003012/default.htm

PICTURE.EXE virus

Impact: This virus gathers password and other information and sends it to several e-mail addresses in China.

Defense Immediately delete this email

Details: This virus has sent an email; you should immediately rid your system of this virus.

Issue ID: 2002203

More Info: http://www.networkice.com/advice/Intrusions/2002203/default.htm

Ping of death

Impact: System crash BSoD (Blue Screen of Death).

Defense Filter out attacking IP address or update operating system to specifically stop this type of attack.

Details: Attacker sends illegal size ping packet (>64K) which networking software was not designed to handle.

Issue ID: 2000012

More Info: http://www.networkice.com/advice/Intrusions/2000012/default.htm

Ping sweep

Impact: Attacker locates systems that are available on a sub-network.

Defense Filter IP address pings at the router for the subnet.

Details: Attacker pings all machines within a subnet looking for those that are on-line.

Issue ID: 2000106

More Info: http://www.networkice.com/advice/Intrusions/2000106/default.htm

POP3 command very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Attacker submits an unusually long command to attempt to break in or shutdown a server.

Issue ID: 2000704

More Info: http://www.networkice.com/advice/Intrusions/2000704/default.htm

POP3 login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple POP3 login failures using bad user names and/or passwords.

Issue ID: 2001604

More Info: http://www.networkice.com/advice/Intrusions/2001604/default.htm

POP3 MIME file name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Attempt to exploit the MIME overflow bug; this may be an intentional effort to overflow a buffer on a server.

Issue ID: 2000703

More Info: http://www.networkice.com/advice/Intrusions/2000703/default.htm

POP3 password very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Attempt to break in using a long password; this may be an intentional effort to overflow a buffer on a server.

Issue ID: 2000702

More Info: http://www.networkice.com/advice/Intrusions/2000702/default.htm

POP3 port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003002

More Info: http://www.networkice.com/advice/Intrusions/2003002/default.htm

POP3 user name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: Attempt to break in using a long user name; this may be an intentional effort to overflow a buffer on a server.

Issue ID: 2000701

More Info: http://www.networkice.com/advice/Intrusions/2000701/default.htm

Possible Fraggle attack initiated

Impact: Slows down system.

Defense Upgrade system or install filters.

Details: A Echo Qotd or Chargen frame sent to broadcast address.

Issue ID: 2000205

More Info: http://www.networkice.com/advice/Intrusions/2000205/default.htm

Possible Smurf attack initiated

Impact: Slows down network connection.

Defense There is no defense for this attack because it is your connection that is being affected. Attacker is spoofing the IP address (specifically pretending to be you) so you cannot find out who the attacker is.

Details: Possible Smurf-amplifier attempt; an ICMP echo frame has been sent to a subnet address.

Issue ID: 2000103

More Info: http://www.networkice.com/advice/Intrusions/2000103/default.htm

PPTP malformed

Impact: System crashes.

Defense Update operating system.

Details: A malformed PPTP connection request has been seen; this may crash your server.

Issue ID: 2002901

More Info: http://www.networkice.com/advice/Intrusions/2002901/default.htm

PPTP port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003018

More Info: http://www.networkice.com/advice/Intrusions/2003018/default.htm

pwl file type

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to file.

Details: Attempt to access a Windows pwl file which contains encrypted Windows passwords.

Issue ID: 2002704

More Info: http://www.networkice.com/advice/Intrusions/2002704/default.htm

Quake backdoor

Impact: Intruder is able to execute his own code on the attacked system.

Defense Upgrade Quake to current version to patch this known bug.

Details: Attacker attempts to connect to a Quake server using a backdoor.

Issue ID: 2001503

More Info: http://www.networkice.com/advice/Intrusions/2001503/default.htm

QuikStore configuration URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Properly install shopping cart software.

Details: Attempt to access QuikStore configuration file.

Issue ID: 2002552

More Info: http://www.networkice.com/advice/Intrusions/2002552/default.htm

Rlogin -froot backdoor

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: The intruder tries to attack an older version of the Rlogin server which allows remote login as root without a password.

Issue ID: 2002101

More Info: http://www.networkice.com/advice/Intrusions/2002101/default.htm

RLogin login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple RLogin login failures using bad user names and/or passwords.

Issue ID: 2001605

More Info: http://www.networkice.com/advice/Intrusions/2001605/default.htm

Rlogin login name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Patch/upgrade Rlogin software.

Details: Attacker attempts to break in using buffer overflow against the login name field.

Issue ID: 2002102

More Info: http://www.networkice.com/advice/Intrusions/2002102/default.htm

Rlogin password very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Patch/upgrade Rlogin software.

Details: Attacker attempts to break into the system using buffer overflow against the password field.

Issue ID: 2002103

More Info: http://www.networkice.com/advice/Intrusions/2002103/default.htm

RLOGIN port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003008

More Info: http://www.networkice.com/advice/Intrusions/2003008/default.htm

rpc nfs/lockd attack

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Attempt to bypass NFS security by tunneling through lockd port 4045.

Issue ID: 2001707

More Info: http://www.networkice.com/advice/Intrusions/2001707/default.htm

rpc.admind auth

Impact: Scans for Solaris remote administration vulnerability.

Defense Update operating system.

Details: Remote administration of Solaris machines has been attempted without proper authentication

Issue ID: 2001704

More Info: http://www.networkice.com/advice/Intrusions/2001704/default.htm

rpc.automountd overflow

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Intruder is attempting to exploit the automountd buffer overflow.

Issue ID: 2001701

More Info: http://www.networkice.com/advice/Intrusions/2001701/default.htm

rpc.mountd overflow

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Intruder is attempting to exploit the mountd buffer overflow.

Issue ID: 2001706

More Info: http://www.networkice.com/advice/Intrusions/2001706/default.htm

rpc.nfs mknod

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Attacker attempts to execute mknod command on remote system.

Issue ID: 2001714

More Info: http://www.networkice.com/advice/Intrusions/2001714/default.htm

rpc.nfs uid is zero

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Attacker attempts to set the bottom 16 bits of a 32-bit user-id to zero so as to improperly login as root.

Issue ID: 2001713

More Info: http://www.networkice.com/advice/Intrusions/2001713/default.htm

rpc.nisd long name

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Attacker attempts to overflow an NIS+ buffer on a remote system.

Issue ID: 2001715

More Info: http://www.networkice.com/advice/Intrusions/2001715/default.htm

rpc.pcnfs backdoor

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Attacker attempts to use a backdoor in the PCNFS service to access remote files.

Issue ID: 2001710

More Info: http://www.networkice.com/advice/Intrusions/2001710/default.htm

rpc.portmap dump

Impact: Attacker finds older RPC-based programs that can be further exploited.

Defense Disable portmapper/rpcbind access from the Internet.

Details: Attacker scans the RPC service to determine which services are running and the version of those services.

Issue ID: 2001705

More Info: http://www.networkice.com/advice/Intrusions/2001705/default.htm

rpc.portmap.set

Impact: Attempts to send mountd commands to Portmap port.

Defense Patch/upgrade RPC services.

Details: Intruder is attempting to setup a service remotely which might be exploited at a later time.

Issue ID: 2001708

More Info: http://www.networkice.com/advice/Intrusions/2001708/default.htm

rpc.portmap.unset

Impact: An intruder may setting up the system for a later attack.

Defense Patch/upgrade RPC services.

Details: Intruder is attempting to reset a service remotely.

Issue ID: 2001709

More Info: http://www.networkice.com/advice/Intrusions/2001709/default.htm

rpc.statd dotdot file create

Impact: The attacker can read all files on the system.

Defense Install filters to stop this attack or upgrade systems to newer versions that specifically defend against this type of attack.

Details: Attacker attempts to access a privileged part of the file system.

Issue ID: 2001711

More Info: http://www.networkice.com/advice/Intrusions/2001711/default.htm

rpc.statd overflow

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Intruder is attempting to exploit the statd buffer overflow.

Issue ID: 2001702

More Info: http://www.networkice.com/advice/Intrusions/2001702/default.htm

rpc.tooltalkd overflow

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: Intruder is attempting to exploit the buffer overflow weakness in ToolTalk.

Issue ID: 2001703

More Info: http://www.networkice.com/advice/Intrusions/2001703/default.htm

rpc.ypupdated command

Impact: Intruder gains unauthorized access to system.

Defense The workaround is to disable rpc.ypupdated and contact the vendor for a patch.

Details: Attacker attempts to use the ypupdated command to execute arbitrary commands on the server.

Issue ID: 2001712

More Info: http://www.networkice.com/advice/Intrusions/2001712/default.htm

RWHO host name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade RWHO server to patch this known bug.

Details: Buffer overflow attempt; this may signal an intentional effort to overflow a buffer on a server.

Issue ID: 2001401

More Info: http://www.networkice.com/advice/Intrusions/2001401/default.htm

sam file

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to file.

Details: Attempt to access the sam file which contains privileged Windows information.

Issue ID: 2002702

More Info: http://www.networkice.com/advice/Intrusions/2002702/default.htm

Shopping cart order URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Properly install shopping cart software.

Details: Attempt to access Shopping cart order log file containing customer orders.

Issue ID: 2002548

More Info: http://www.networkice.com/advice/Intrusions/2002548/default.htm

Site Server sample URL

Impact: Intruder gains access and may potentially crash system.

Defense Remove sample files from server.

Details: Attempt to access site configuration file which was installed as a sample file for Microsoft Site Server.

Issue ID: 2002556

More Info: http://www.networkice.com/advice/Intrusions/2002556/default.htm

SMB empty password

Impact: Attackers can access the entire system.

Defense Patch/upgrade SMB server.

Details: Attacker makes a successful connection to a SMB server with an empty password.

Issue ID: 2000502

More Info: http://www.networkice.com/advice/Intrusions/2000502/default.htm

SMB file name very long

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: A file name is excessively long which may be an attempt to overflow a buffer and gain unauthorized access to a system.

Issue ID: 2000505

More Info: http://www.networkice.com/advice/Intrusions/2000505/default.htm

SMB I/O using printer share

Impact: Attackers can access the entire system.

Defense Disable printer sharing on all Windows 95 systems that are older than the OSR-2 release or upgrade to OSR-2 or Windows 98.

Details: Older versions of Windows 95 would allow an attacker to access an entire system if printer sharing was enabled.

Issue ID: 2000503

More Info: http://www.networkice.com/advice/Intrusions/2000503/default.htm

SMB login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple SMB login failures using bad user names and/or passwords.

Issue ID: 2001606

More Info: http://www.networkice.com/advice/Intrusions/2001606/default.htm

SMB malformed

Impact: System crashes.

Defense Update operating system.

Details: Attempt to crash the machine through the SMB service.

Issue ID: 2000501

More Info: http://www.networkice.com/advice/Intrusions/2000501/default.htm

SMB password very long

Impact: Attacker attempts to crash or break into a SMB server.

Defense Update operating system.

Details: Attacker attempts to break into the SMB server by using a very long password.

Issue ID: 2000504

More Info: http://www.networkice.com/advice/Intrusions/2000504/default.htm

SMB unencrypted password

Impact: Attacker retrieves user account and clear text password by sniffing wire.

Defense Upgrade OS software.

Details: An unencrypted password was transmitted to a server which requested the use of an encrypted password.

Issue ID: 2000507

More Info: http://www.networkice.com/advice/Intrusions/2000507/default.htm

SMB Unicode file name very long

Impact: Intruder gains unauthorized access to system.

Defense Update operating system.

Details: A file name is excessively long which may be an attempt to overflow a buffer and gain unauthorized access to a system.

Issue ID: 2000506

More Info: http://www.networkice.com/advice/Intrusions/2000506/default.htm

SMTP command very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade mail server to patch this known vulnerability.

Details: Attacker submits an unusually long command to attempt to break in or shutdown a server.

Issue ID: 2001012

More Info: http://www.networkice.com/advice/Intrusions/2001012/default.htm

SMTP corrupted MAIL command

Impact: Compromises mail servers.

Defense Upgrade mail server to patch this known vulnerability.

Details: Intruder is trying to hack the mail service by sending invalidly formatted commands.

Issue ID: 2001008

More Info: http://www.networkice.com/advice/Intrusions/2001008/default.htm

SMTP corrupted RCPT command

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade mail server to patch this known vulnerability.

Details: Intruder is attempting to gain control of the e-mail service through a buffer overflow in the RCPT TO command.

Issue ID: 2001010

More Info: http://www.networkice.com/advice/Intrusions/2001010/default.htm

SMTP DEBUG command

Impact: Compromises mail servers.

Defense Upgrade mail server to patch this known vulnerability.

Details: This was the hack used in the Morris Worm of 1988; it is unlikely that any system is vulnerable today.

Issue ID: 2001002

More Info: http://www.networkice.com/advice/Intrusions/2001002/default.htm

SMTP email name very long

Impact: Intruder gains unauthorized access to system.

Defense Update mail server software.

Details: Intruder is attempting to gain control of the e-mail service through a buffer overflow in the MAIL FROM command.

Issue ID: 2001009

More Info: http://www.networkice.com/advice/Intrusions/2001009/default.htm

SMTP EXPN command

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Reconfigure web server ignore EXPN command.

Details: The SMTP EXPN command provides information about users on a system; an intruder may use this to setup a later attack.

Issue ID: 2001004

More Info: http://www.networkice.com/advice/Intrusions/2001004/default.htm

SMTP login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple SMTP login failures using bad user names and/or passwords.

Issue ID: 2001609

More Info: http://www.networkice.com/advice/Intrusions/2001609/default.htm

SMTP login name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade mail server to patch this known vulnerability.

Details: Buffer overflow attempt; this may be an intentional effort to overflow a buffer on a server.

Issue ID: 2001003

More Info: http://www.networkice.com/advice/Intrusions/2001003/default.htm

SMTP mail to decode alias

Impact: In some systems this may be used to overwrite the /etc/passwd file or other critical files thus compromising the system.

Defense Disable the DECODE alias. then update mail server software.

Details: Intruder tries to execute code on the server using an old email alias.

Issue ID: 2001013

More Info: http://www.networkice.com/advice/Intrusions/2001013/default.htm

SMTP mail to uudecode alias

Impact: Intruder gains control of the system.

Defense Disable the UUDECODE alias then update mail server software.

Details: Intruder tries to execute code on the server using an old email alias.

Issue ID: 2001014

More Info: http://www.networkice.com/advice/Intrusions/2001014/default.htm

SMTP MIME file name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Install a patch from your vendor.

Details: This may be an intentional effort to overflow a buffer on a server.

Issue ID: 2001016

More Info: http://www.networkice.com/advice/Intrusions/2001016/default.htm

SMTP pipe in mail address

Impact: Compromises the mail server.

Defense Upgrade mail server to patch this known vulnerability.

Details: Attacker passes shell commands to the server via the e-mail handling service.

Issue ID: 2001001

More Info: http://www.networkice.com/advice/Intrusions/2001001/default.htm

SMTP port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003003

More Info: http://www.networkice.com/advice/Intrusions/2003003/default.htm

SMTP relay attempt

Impact: Relays spam through your e-mail server overloading your network connection and server as well as hiding the source of the spam behind your server.

Defense Turn off relaying.

Details: Attacker is trying to relay mail through your SMTP mail service.

Issue ID: 2001011

More Info: http://www.networkice.com/advice/Intrusions/2001011/default.htm

SMTP too many errors

Impact: Relays spam through your e-mail server overloading your network connection and server as well as hiding the source of the spam behind your server.

Defense No known defense.

Details: The SMTP server has issued too many error responses. This probably indicates that a spammer is trying to misuse the email system.

Issue ID: 2001015

More Info: http://www.networkice.com/advice/Intrusions/2001015/default.htm

SMTP Too many recipients

Impact: Relays spam through your e-mail server overloading your network connection and server.

Defense Update mail server software.

Details: A large number of recipients have been specified for a single email which may indicate a spammer.

Issue ID: 2001007

More Info: http://www.networkice.com/advice/Intrusions/2001007/default.htm

SMTP uucp-style recipient

Impact: Intruder may be attempting to bypass spam filters to send unauthorized email.

Defense Install a patch from your vendor.

Details: An old uucp-style mail recipient name (using %) has been seen.

Issue ID: 2001017

More Info: http://www.networkice.com/advice/Intrusions/2001017/default.htm

SMTP VRFY command

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Reconfigure web server ignore VRFY command.

Details: The SMTP VRFY command provides information about users on a system; an intruder may use this information to setup a later attack.

Issue ID: 2001005

More Info: http://www.networkice.com/advice/Intrusions/2001005/default.htm

SMTP WIZ command

Impact: Compromises mail servers.

Defense Upgrade mail server to patch this known vulnerability.

Details: This was the hack used in the Morris Worm of 1988; it is unlikely that any system is vulnerable today.

Issue ID: 2001006

More Info: http://www.networkice.com/advice/Intrusions/2001006/default.htm

SNMP backdoor

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Patch/upgrade SNMP services.

Details: Intruder attempts to exploit a default backdoor in the network equipment.

Issue ID: 2002003

More Info: http://www.networkice.com/advice/Intrusions/2002003/default.htm

SNMP Corrupt

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system or crashes system.

Defense Patch/upgrade SNMP software.

Details: Attacker sends corrupted SNMP traffic; this may be designed to compromise the system.

Issue ID: 2002001

More Info: http://www.networkice.com/advice/Intrusions/2002001/default.htm

SNMP Crack

Impact: Attacker attempts to crack the system password.

Defense Disable SNMP access enable IP address filtering.

Details: Attacker tries many different SNMP community strings (passwords) in an attempt to guess SNMP access passwords.

Issue ID: 2002002

More Info: http://www.networkice.com/advice/Intrusions/2002002/default.htm

SNMP discovery broadcast

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Patch/upgrade SNMP services.

Details: Intruder is scanning systems to see whether SNMP is supported.

Issue ID: 2002004

More Info: http://www.networkice.com/advice/Intrusions/2002004/default.htm

Snork attack

Impact: Slows down system.

Defense Upgrade system or install filters.

Details: Attacker sends an error packet to your system on port 135 and your system replies possibly resulting in an infinite loop.

Issue ID: 2000203

More Info: http://www.networkice.com/advice/Intrusions/2000203/default.htm

SOCKS port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003017

More Info: http://www.networkice.com/advice/Intrusions/2003017/default.htm

SoftCart password URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Properly install shopping cart software.

Details: Attempt to access SoftCart password file.

Issue ID: 2002553

More Info: http://www.networkice.com/advice/Intrusions/2002553/default.htm

SQL login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple SQL login failures using bad user names and/or passwords.

Issue ID: 2001607

More Info: http://www.networkice.com/advice/Intrusions/2001607/default.htm

SQL port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003013

More Info: http://www.networkice.com/advice/Intrusions/2003013/default.htm

SUNRPC port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003016

More Info: http://www.networkice.com/advice/Intrusions/2003016/default.htm

SynDrop attack

Impact: System crash BSoD (Blue Screen of Death).

Defense Update operating system install filters.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000005

More Info: http://www.networkice.com/advice/Intrusions/2000005/default.htm

TCP port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if a particular port is opened for remote access.

Issue ID: 2003102

More Info: http://www.networkice.com/advice/Intrusions/2003102/default.htm

TCP port scan

Impact: Locates open ports on a system.

Defense Filter IP address from attacking source.

Details: Attacker systematically scans through all possible ports on a system looking for those that are open.

Issue ID: 2000301

More Info: http://www.networkice.com/advice/Intrusions/2000301/default.htm

TCP sequence out-of-range

Impact: Subsequent attempts to hijack connections may be successful.

Defense No known defense.

Details: A TCP sequence number is out of the expected range; this may signal an attempt to hijack a TCP connection.

Issue ID: 2000304

More Info: http://www.networkice.com/advice/Intrusions/2000304/default.htm

TCP SYN flood

Impact: Slows down a system making it difficult or impossible for anyone to connect to it.

Defense "Upgrade system with "SYN cookies" install filters. "

Details: Attacker floods the system with TCP connection requests; real requests may not get through.

Issue ID: 2000302

More Info: http://www.networkice.com/advice/Intrusions/2000302/default.htm

Teardrop attack

Impact: System crash BSoD (Blue Screen of Death).

Defense Update operating system install filters.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000003

More Info: http://www.networkice.com/advice/Intrusions/2000003/default.htm

TearDrop2 attack

Impact: System crash BSoD (Blue Screen of Death).

Defense Update operating system install filters.

Details: The attacker overlaps fragments in a way designed to crash the machine.

Issue ID: 2000006

More Info: http://www.networkice.com/advice/Intrusions/2000006/default.htm

Telnet abuse

Impact: Locates and exploits holes in services. Hackers use Telnet to probe a system for weaknesses.

Defense None without an intrusion countermeasure system. An attacker using Telnet appears exactly as a legitimate connection except for the time between keystrokes. Normal services do not contain the advanced heuristics necessary to detect this activity.

Details: Attacker is probably using Telnet to directly connect to SMTP POP IMAP HTTP or FTP.

Issue ID: 2000901

More Info: http://www.networkice.com/advice/Intrusions/2000901/default.htm

Telnet login failed

Impact: An attacker is prowling around your system. Subsequent attempts may be successful.

Defense There is no defense for this type of intrusion.

Details: Multiple Telnet login failures using bad user names and/or passwords.

Issue ID: 2001608

More Info: http://www.networkice.com/advice/Intrusions/2001608/default.htm

Telnet login name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Patch/upgrade Telnet software.

Details: Attacker attempts to break in using a buffer overflow against the login name field.

Issue ID: 2000902

More Info: http://www.networkice.com/advice/Intrusions/2000902/default.htm

Telnet password very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Patch/upgrade Telnet software.

Details: Attacker attempts to break in using a buffer overflow against the password field.

Issue ID: 2000903

More Info: http://www.networkice.com/advice/Intrusions/2000903/default.htm

TELNET port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003006

More Info: http://www.networkice.com/advice/Intrusions/2003006/default.htm

Telnet terminal type very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Patch/upgrade Telnet software.

Details: Attempt to break in using a buffer overflow against the terminal-type Telnet option.

Issue ID: 2000904

More Info: http://www.networkice.com/advice/Intrusions/2000904/default.htm

TFTP file name very long

Impact: Intruder constructs data in a particular way and is able to execute his own code on the attacked system.

Defense Upgrade TFTP server.

Details: A TFTP file was very long; this indicates a possible attempt by a hacker to break-in to a server.

Issue ID: 2001202

More Info: http://www.networkice.com/advice/Intrusions/2001202/default.htm

TFTP file not found

Impact: An attacker is prowling around your system.

Defense Do not enable TFTP on system unless absolutely necessary.

Details: A TFTP file was not found; this may be a configuration problem or may indicate an illegitimate use of the TFTP command.

Issue ID: 2001201

More Info: http://www.networkice.com/advice/Intrusions/2001201/default.htm

Too much fragmentation

Impact: System and network slow down.

Defense Update operating system.

Details: The system received a large number of unprocessed fragments; this may be an attack or a simple spike in traffic.

Issue ID: 2000011

More Info: http://www.networkice.com/advice/Intrusions/2000011/default.htm

Trace route

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense No known defense.

Details: A trace route scan was performed on the system; this may be indicative of a future attempt to attack the system.

Issue ID: 2000101

More Info: http://www.networkice.com/advice/Intrusions/2000101/default.htm

Trojan horse probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if a trojan horse program is installed.

Issue ID: 2003101

More Info: http://www.networkice.com/advice/Intrusions/2003101/default.htm

UDP port loopback

Impact: Slows down system.

Defense Upgrade system or install filters.

Details: Attacker sends a UDP frame that has ports 7 (Echo) 17 (Quote of the Day) or 19 (Chargen) as source and destination.

Issue ID: 2000202

More Info: http://www.networkice.com/advice/Intrusions/2000202/default.htm

UDP port scan

Impact: Locates open ports on a system.

Defense Filter IP address from attacking source.

Details: Attacker systematically scans through all possible ports on a system looking for those that are open.

Issue ID: 2000201

More Info: http://www.networkice.com/advice/Intrusions/2000201/default.htm

Unknown IP protocol

Impact: Intruder may take advantage of security holes built into trojan horse to access files or crash system.

Defense Install or reconfigure port filters.

Details: A frame with an unknown IP protocol was detected.

Issue ID: 2000002

More Info: http://www.networkice.com/advice/Intrusions/2000002/default.htm

W97M.Marker.a virus

Impact: This macro virus will keep a log of the date/time of the infection and user information. When the payload in this virus activates on the 1st of the month it will upload this information to an FTP site

Defense Immediately rid your system of this virus.

Details: This virus has attempted an FTP transfer.

Issue ID: 2002204

More Info: http://www.networkice.com/advice/Intrusions/2002204/default.htm

WebStore admin URL

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Properly install shopping cart software.

Details: Attempt to access WebStore shopping cart administration directory.

Issue ID: 2002547

More Info: http://www.networkice.com/advice/Intrusions/2002547/default.htm

WhatsUp scan

Impact: Attacker find vulnerabilities that can be exploited.

Defense Install dynamic filters that can selectively stop these scan.

Details: An intruder is using the WhatsUp product by Ipswitch to probe your system for weaknesses.

Issue ID: 2001511

More Info: http://www.networkice.com/advice/Intrusions/2001511/default.htm

win.ini file

Impact: An intruder may be inserting a trojan horse.

Defense Examine file for corruption.

Details: Attempt to access system configuration information.

Issue ID: 2002705

More Info: http://www.networkice.com/advice/Intrusions/2002705/default.htm

WinNuke attack

Impact: System hang or BSoD (Blue Screen of Death).

Defense Filter out attacking IP address or update operating system to specifically stop this type of attack.

Details: Attacker sends out-of-band data to an open TCP connection; older versions of Windows can't handle this type of data.

Issue ID: 2000303

More Info: http://www.networkice.com/advice/Intrusions/2000303/default.htm

winreg file

Impact: An intruder may be gathering information which could be useful to setup a later attack.

Defense Close network path to file.

Details: Attempt to access the Windows registry.

Issue ID: 2002703

More Info: http://www.networkice.com/advice/Intrusions/2002703/default.htm

XWINDOWS port probe

Impact: Locates open port on a system.

Defense Filter IP address from attacking source.

Details: Attempt to see if this well-known service is available.

Issue ID: 2003015

More Info: http://www.networkice.com/advice/Intrusions/2003015/default.htm

A

FOR MORE HELP

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

Online 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 tool. A pop-up menu is displayed.
- Select **Help** and then **BlackICE Help Topics** from the submenu.

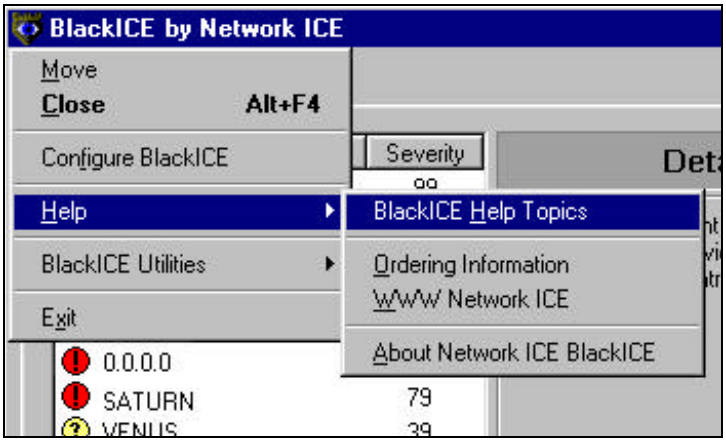


Figure 22 – Select BlackICE Help Topics to display the online help.

From the Windows Start Menu

- Select **BlackICE Help** from the **Programs**, **Network ICE**, **BlackICE** folder on your **Start** menu.

Network ICE Web Site

The Network ICE web site includes the latest information about BlackICE including FAQs, hints, and patches. There is also an extensive on-line library of information about computer and network security. Visit the site at www.networkice.com.

Technical Support

BlackICE technical support is available on the web at www.networkice.com. It is also available via email at support@networkice.com . There is currently no telephone support for BlackICE.

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.

BackOrifice: 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. BackOrifice 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
	100-80	**Critical Event**: This is a deliberate attack on your system for the purpose of damaging data or crashing the system.
	80-40	**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.
	40-20	**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.
	20-0	**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: An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software. Logical ports can be set up on networks for specific purposes like handling E-mail or HTTP data.

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.