Global Information Assurance Certification Paper

Case Study: Securing Windows XP Home Edition

Trevor Cuthbert
GSEC Practical Assignment
v.1.4b - Option 2
4-Feb-03

Table of Contents

Abstract

This document was written to outline the steps taken to secure a Windows XP Home Edition personal computer. It begins with a security assessment detailing the initial environment, usage, and risks. After the initial assessment, the paper explains the steps performed and tools used to increase the level of security. It then re-examines the state of the computer system to show an increased level of security. While these steps provide a strong level of security, there are additional procedures that can be implemented for further protection. It is up to the user to decide what level of security is acceptable on his/her computer system.

Initial State of Computer System – Before Section

Personal computers are becoming increasingly important as new services are offered on the Internet. While technology continues to advance at a rapid pace, many vulnerabilities and security holes are being introduced. There is a requirement to increase system security to protect the confidentiality, integrity, and availability of information and services.

Computer Environment

The computer I am securing is a stand alone system connected to the Internet through an ADSL modem. The computer is running Windows XP Home Edition with the latest operating system updates and patches. The operating system is a typical installation with the default services enabled. The BIOS and device drivers have been updated to current versions. Some of the applications are outdated and need to be upgraded. Internet Connection Firewall (ICF) is disabled and there is currently no firewall protection. The system is running Norton Antivirus 2002 for virus protection. It is configured to scan incoming/outgoing email and to use script blocking.

Computer Usage

I use my computer for many purposes. The main purposes are:

- Remote Access: I connect to my company's network using Cisco VPN and Citrix ICA clients.
- Online Banking: I perform personal banking transactions online such as bill payments, account transfers, and credit/loan applications.
- Online Gaming: I participate in playing games against other people over the Internet.
- Online Shopping: I purchase various merchandise from companies over the Internet.
- Communication: I communicate with people on the Internet using IRC, ICQ, and MSN Messenger. I also use my computer for personal email.
- Research: I research topics on the Internet and utilize various forums.

- File Storage: I store personal documents and files. Some of these files contain private information.

Computer Risks

There are various risks that can be associated with the computer usage above. Some of these are:

- Remote Access: The remote access connection established between my personal computer and my company's network can lead to security issues. A system compromise or virus/worm infection can cause serious problems that can propagate between these systems.
- Online Banking: There is risk of detailed financial information being accessed. This information could provide the ability to perform undesired transactions.
- Online Gaming: Fee based online gaming is a target among many hackers. Quite often attempts to compromise a system are made to steal game account passwords. The hijacked game accounts are generally emptied of possessions and deleted.
- Online Shopping: There is risk of credit card information being accessed and used for undesired purchases.
- Communication: Hackers can exploit various communication tools to either compromise a system or learn more information about them.
- Research: It is possible to load a webpage containing malicious code that can exploit weaknesses in Internet Explorer.
- File Storage: There is risk of private documents being accessed or deleted. The risk depends on the contents of the files.

The biggest risk is that the computer does not have firewall protection and is visible on the Internet. Any subnet sweep will quickly discover the computer and allow hackers to probe ports looking for specific weaknesses.

Steps Taken to Increase Security – During Section

Preparation

There were some precautionary steps I wanted to perform before attempting to secure Windows XP Home Edition.

Antivirus Scan

I verified that my antivirus program was using the most current virus definitions available. I performed a full system scan on all files to confirm that my system was free from infection before proceeding.

System Restore

System Restore is a built in feature that comes with Windows XP Home Edition. It takes snapshots of the system registry and allows the user to restore the computer to a previous state. I used system restore to create a restore point before making any configuration changes. This will allow the ability to undo changes that might affect the functionality of the computer. I used system restore throughout the hardening process. This prevents having to redo every change made if problems are encountered.

Test Application Functionality

I tested the applications on my computer to verify that they work as expected. I continued testing throughout the hardening process to ensure the steps performed did not affect the functionality of these programs. Testing the applications after every significant change would make it easier to determine which step(s) caused an application to lose functionality.

Personal Firewall

It is clear that the biggest security weakness of my computer is that it is not protected by a firewall. Windows XP Home Edition comes with a built in firewall called Internet Connection Firewall (ICF). I wanted to use a firewall that was more robust and configurable than ICF. I did some research and purchased ISS BlackICE PC Protection.

ISS BlackICE PC Protection

ISS BlackICE PC Protection has three main features:

- Personal Firewall – Allows the user to manually enter firewall rules allowing or denying access based on IP address, port, or both.
- Intrusion Detection – Built in Intrusion Detection system that detects attempts to probe or compromise a system. Intrusion events are logged and displayed. By right clicking an event it is possible to ignore the event, block an IP address, or trust an IP address. Selecting one of these options will automatically create the corresponding firewall rules.
- Application and Communication Control – Allows the user to create an inventory of files. The user can specify which file extensions to include in the inventory. The program creates a checksum database of these files. When a file is accessed, the program creates a new checksum and compares it to the checksum database. If the two checksums do not match, the program will alert the user that the file has changed. In addition, it will prevent the file from executing and from accessing the network. This prevents tampering with existing files and the installation of trojan programs.

The settings I used to configure the program can be found in Appendix A: ISS BlackICE PC Protection Settings.

These settings will automatically block all inbound TCP and UDP traffic originating from a remote source on ports 1 – 65535. After selecting this level of protection, I verified that all my applications were still functional.

To do more research on the product, I read through the ISS BlackICE PC Protection Knowledgebase.

By default, the intrusion detection system is set to trust 'SMB winreg file' events. This is due to the number of false positives associated with this attack. I decided that I would like the program to prevent against this attack. This can be done by editing the sigs.ini file located in the BlackICE folder. To disable the trust, place a semicolon (;) in front of the following line:

trust.issue = 2002703

Something to be aware of is that the product does not block ICMP traffic by default. You can configure BlackICE to block ICMP traffic by editing the firewall.ini file. I added the following three entries to my file:

[MANUAL ICMP ACCEPT]
REJECT, 8:0, ICMP, 2001-10-15 00:01:00, PERPETUAL, 1000, unknown
REJECT, 13:0, ICMP, 2001-10-15 00:01:00, PERPETUAL, 1000, unknown
REJECT, 17:0, ICMP, 2001-10-15 00:01:00, PERPETUAL, 1000, unknown

These three lines will block traffic for ICMP Echo, Timestamp, and Address Mask requests. You can block traffic for any ICMP message type. A list of ICMP message types can be found at http://www.spirit.com/Resources/icmp.html.

I downloaded the BlackICE Advanced Administration Guide which provides more technical detail for the advanced user.

Ethereal

BlackICE displays intrusion events but does not include software that allows you to view the evidence files. You are unable to examine specific information about the intrusion attempt, for example which port was accessed and what type of data was sent. To view the evidence files for forensic analysis, I downloaded the program Ethereal. This is a free network analyzer that can be used to view BlackICE evidence files.

Software Updates

Operating systems, applications, and device drivers are continuously being updated to add new functionality and/or address various issues. It is essential from a security point of view to keep your software at the current release levels.

Windows Update is the most convenient method to ensure you have the latest operating system updates and patches. I run Windows Update manually once a week. I install every patch unless I determine it isn't applicable or required.

After further inspection, I determined that both the BIOS and the device drivers are at the current release levels. I did find three applications that have been updated since I last checked, two of these are important from a security perspective.

I went to the respective vendors and upgraded:

- Cisco Systems VPN Client (used for remote access).
- Citrix ICA Client (used for remote access).
- Roxio Easy CD Creator (used for CD Burning).

While the Roxio software update doesn't have any security implications, it offers improved functionality and compatibility with Windows XP Home Edition. The Cisco and Citrix software provide remote access functionality. It is vital to keep these applications current as they are typically updated to address security issues.

SANS Top 20 Vulnerabilities

SANS keeps a list of the top 20 threats to computer systems. Since I am running Windows XP Home Edition, I was only concerned with the 10 that are applicable to Windows based systems. The entire list with detailed descriptions can be found at http://www.sans.org/top20/. At the end of the document there is a list of commonly exploited ports. Unless required, it is recommended to block these ports using a firewall. Since I have blocked incoming traffic to every port, I do not need to further customize my firewall.

Internet Information Services

Windows XP Home Edition does not come with Internet Information Services and I have no need to install this software on my computer. Therefore, this threat is not applicable to my computer.

Microsoft Data Access Components (MDAC)

Since I am running Windows XP Home Edition, I don't believe that my system is vulnerable. I did check the version of my msadcs.dll file. It is at version 2.71.9030.0 which is greater than 2.1. Therefore, it appears my version of MDAC is not vulnerable to this threat.

Microsoft SQL Server

I am not running Microsoft SQL Server. Therefore, this threat is not applicable to my computer.

NetBIOS

To test for vulnerability against this threat, I downloaded the Microsoft Baseline Security Analyzer. I do not have any shares, so I didn't expect the tool to report any vulnerability. After running the tool, it did not detect any NetBIOS vulnerabilities. It did question whether or not I had installed three security patches. I verified the installation of these patches by viewing Windows Update history.

Anonymous Logon

I am blocking all ports with the BlackICE firewall. Therefore, my computer is not vulnerable to this attack. However, to practice defense in depth and as an additional precaution, I modified the following registry key:

Key: HKLM/System/CurrentControlSet/Control/LSA
Name: RestrictAnonymous
Type: REG_DWORD
Value: 2

LAN Manager Authentication

My computer is vulnerable to this attack. To eliminate this vulnerability I modified the following two registry keys:

Key: HKLM/System/CurrentControlSet/Control/LSA
Name: LMCompatibilityLevel
Type: REG_DWORD
Value: 3

Key: HKLM/System/CurrentControlSet/Control/LSA
Name: NoLMHash
Type: REG_DWORD
Value: 1

General Windows Authentication

I use a very strong password on my Windows XP Home Edition computer. I feel the password is sufficiently strong and would require prolonged physical access to the computer to break it.

Internet Explorer

Since I run Windows Update once a week, I am not vulnerable from a patch level perspective. I ran the Microsoft Baseline Security Analyzer and it questioned my Internet Explorer zone settings. This is because I am using custom settings. Before I take a closer look at my zone settings, I wanted to run the free browser security check from Qualys that can be found at http://browsercheck.qualys.com/.

The browser check by Qualys identified that clipboard information could be read by the websites that I visit. This could allow private information to be viewed

remotely. To fix this, I changed the security zone setting for 'Allow paste operations via script' to Disable.

There are four different zones you can configure: Internet, Local Intranet, Trusted Sites, and Restricted Sites. Since my computer is a stand alone home computer, I only make use of the Internet zone. A good reference for setting up security zones can be found at http://www.microsoft.com/windows/ie/using/howto/security/setup.asp.

Using this information, I decided to use the following custom configuration on my computer for the Internet zone:

ActiveX Controls and Plug-Ins
- Download signed ActiveX controls - Prompt
- Download unsigned ActiveX controls - Disable
- Initialize and script ActiveX controls not marked as safe - Disable
- Run ActiveX controls and plug-ins - Enable
- Script ActiveX controls marked safe for scripting - Enable

Downloads
- File download - Enable
- Font download - Enable

Microsoft VM
- Java Permissions - High Safety

Miscellaneous
- Access data sources across domains - Disable
- Allow META REFRESH - Enable
- Display mixed content - Prompt
- Don't prompt for client certificate selection when no certificates or only one certificate exists - Disable
- Drag and drop or copy and paste files - Prompt
- Installation of desktop items - Prompt
- Launching programs and files in an IFRAME - Prompt
- Navigate sub-frames across different domains - Disable
- Software channel permissions – High Safety
- Submit nonencrypted form data - Enable
- Userdata persistence - Disable

Scripting
- Active scripting - Enable
- Allow paste operations via script - Disable
- Scripting of Java applets - Enable

User Authentication

- Logon - Prompt for user name and password

Remote Registry Access

I verified that the following registry key existed:

Key: HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
Name: Description
Type: REG_SZ
Value: Registry Server

The security permissions on the winreg subkey will allow only administrators and the LOCAL SERVICE account remote access. Therefore, this threat is not applicable to my computer.

Windows Scripting Host

Although I use an antivirus program to prevent malicious scripts from taking advantage of the Windows Scripting Host (WSH), I disabled this feature to prevent unknown scripts from executing. I downloaded a tool from Symantec to disable WSH. Instructions and a link to download the tool can be found at http://securityresponse.symantec.com/avcenter/venc/data/win.script.hosting.html.

Removing and Disabling Unnecessary Services

Local Area Connection Properties

In the Local Area Connection Properties tab I uninstalled the following three items:

- Client for Microsoft Networks
- File and Print Sharing for Microsoft Networks
- QoS Packet Scheduler

These components are not required by my computer and are no longer vulnerable to attack.

Services

By default, Windows XP Home Edition is configured to enable many services that are not required. These services utilize system resources and introduce unnecessary security threats. A good reference describing the function of Windows XP services can be found at the following location: http://www.uksecurityonline.com/husdg/windowsxp/disableservices.htm

Using this information I disabled services that I felt were unnecessary. Appendix B: Windows XP Services lists the service settings before and after I disabled them.

Below is a summary chart for comparison.

	Before	**After**
Number of Services	80	73
Set to Automatic	38	12
Set to Manual	40	3
Set to Disabled	2	58

Additional Hardening Procedures

An excellent source for additional hardening steps for Windows XP can be found at http://www.uksecurityonline.com/husdg/wxpp2.php. I used this list to implement additional security procedures that were applicable to my computer.

Raw Socket Permissions

I decided to lock down the raw socket permissions on my computer system as a precaution. A description of the possible problems with default socket permissions can be found at http://grc.com/dos/xpsummary.htm. The tools I used to test my socket permissions and to lock them down are found at http://grc.com/dos/sockettome1.htm.

Disable the Guest Account

I had previously disabled the Guest account on my computer system. I wanted to include this because it is extremely important to do so.

To disable the guest account:

- Go into 'User Accounts' which can be found in the Control Panel.
- Click on the Guest account icon.
- Click 'Turn off Guest Account'.

Replacing 'Everyone' Group with 'Authenticated Users' Group

I have always been a bit nervous with the way Microsoft implemented the 'Everyone' group. To alleviate my concerns I replaced all instances of the 'Everyone' group with a more secure 'Authenticated Users' group. While I do not use file sharing, I prefer the permissions on my files do not include the 'Everyone' group.

To replace the 'Everyone' group with 'Authenticated Users'

- Boot the computer in safe mode and log in using an administrator account.
- Open up Windows Explorer.
- There are three folders where we need to replace the 'Everyone' group with 'Authenticated Users'. These are:
    1. C:\
    2. C:\Documents and Settings
    3. C:\Documents and Settings\All Users

- For each folder listed above, right click the folder and select Properties. Select the Security tab and click the 'Advanced' button. Select the 'Everyone' group in the 'Permission entries' window. Click 'Edit'. Click 'Change'. Click 'Advanced'. Click 'Find Now'. In the search window locate and select the 'Authenticated Users' group. Click OK on each window that is open (5 in total).

Stop Port 445 from Listening

There are certain ports in Windows XP Home Edition that are continuously listening for traffic. To view which ports are listening on your computer, type 'netstat –an' at a Command Prompt. All ports that are listening will have a state that reflects this.

My firewall will prevent traffic from getting to this port but I decided to disable it. To stop port 445 from listening, edit the following registry key:

Key: HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
Name: TransportBindName
Type: REG_SZ
Value:

You'll notice there is nothing listed for value. The default value in this key is '\Device\'. Select the data within the string value and delete it.

Disabling DCOM

DCOM adds an addition level of risk when it is enabled. It is recommended to disable DCOM if it is not required. To disable DCOM, edit the following registry key:

Key: HKLM\SOFTWARE\Microsoft\Ole
Name: EnableDCOM
Type: REG_SZ
Value: N

Remove POSIX Subsystem

I do not use 16 bit applications and therefore do not require this subsystem. To remove the POSIX subsystem, I deleted the following registry key:

Key: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
Name: Posix
Type: REG_SZ
Value: %SystemRoot%\system32\psxss.exe

Disable Dump File Creation

When windows crashes it creates a dump file for troubleshooting purposes. The dump file can contain software passwords. Since my computer has been reliable, I decided dump files are more of a risk than a benefit. To disable dump files:

- Go to: Control Panel • System
- Select the Advanced tab.
- In the 'Startup and Recovery' section click 'Settings'.
- Set 'Write debugging information' to 'none'.

Clear Page File at Shutdown

It is possible for some applications to temporarily store passwords in memory which can get written into the page file. To prevent a password from being stored on the hard disk, I edited the following registry key:

Key: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Name: ClearPageFileAtShutdown
Type: REG_DWORD
Value: 1

Set .reg Files to Open with Notepad

To prevent accidental installation of .reg files, I associated this file type to open with notepad. To do this I edited the following registry key:

Key: HKLM\SOFTWARE\Classes\regfile\shell\open\command
Name: (Default)
Type: REG_SZ
Value: notepad.exe "%1"

Disable Internet Explorer Error Reporting

When a program crashes, Windows XP is configured to send debugging information to Microsoft via Internet Explorer. The debugging information contains a memory dump which may contain sensitive information. Since my computer has been reliable, I decided to disable this feature by editing the following registry key:

Key: HKLM\SOFTWARE\Microsoft\Internet Explorer\Main
Name: IEWatsonEnabled
Type: REG_DWORD
Value: 0

Harris STAT Scanner Professional Edition

To further enhance my security toolbox, I purchased the Harris STAT Scanner Professional Edition vulnerability assessment tool.

This tool was used to implement some of the hardening procedures in this document. It did a good job identifying many issues, but at the same time did produce some false positives.

Current State of Computer System – After Section

Online Penetration Tests

The best way to demonstrate the security of the system is to perform penetration tests similar to the scans performed by hackers. I tested my computer using the three sites listed below.

Symantec Security Check: Provides a free security scan of your computer. This scan checks for network vulnerability, NetBIOS availability, active trojans, antivirus product, antivirus definition, and browser privacy. The scan reported that all checks were safe with the exception of browser privacy. The warning for browser privacy stated that my browser releases history information to other web sites. This is a problem I will look into, but feel it is more of a privacy issue than a risk.

Broadband Reports.com: This scan reported a healthy setup. It could not detect a response from any port, TCP or UDP.

Shields UP!: There are two tests on this page. The first test checks to see if your computer is acting as an Internet server. This test could not detect port 139 or any NetBIOS running on my computer. The second test checks well known ports. This test could not detect any ports as all ports were given a stealth rating.

These results are promising. The BlackICE firewall not only blocks all inbound traffic, but it discards packets rather than sending a response. This allows my computer to appear invisible to remote users unless I establish a connection with their system.

Netstat and Fport

These are two command line utilities that display which ports are in use and which applications are using them. Netstat is a Windows utility and Fport is a utility created by Foundstone. It can be downloaded from http://www.foundstone.com/knowledge/proddesc/fport.html.

Typing 'netstat –an' at a Command Prompt listed TCP ports 135 and 1028 as listening. These are the ports we need to be concerned with since they are considered open and will accept traffic unless blocked by a firewall.

Running Fport from a Command Prompt associated port 135 with svchost.exe and port 1028 with navapw32.exe.

Svchosts.exe is a generic host process that allows services to run from dynamic-link libraries. A description of its functionality can be found at http://support.microsoft.com/default.aspx?scid=kb;en-us;314056. To find out which service was running under this host process, I used Fport to determine the process identifier (PID). Using Windows Task Manager, I shut down the corresponding process. I was immediately notified that the Remote Procedure Call (RPC) process had ended unexpectedly and that the computer was shutting down. The RPC process is critical to Windows XP and needs to be enabled. Therefore, I need to rely on my firewall to block traffic on port 135.

Navapw32.exe is the Norton Antivirus Auto-Protection application. It didn't make sense to me why this program would be listening on a port. I decided to use BlackICE communication control to block network access for this file. After I configured communication control to block network access, I rebooted the computer. When logging in I was notified that email antivirus protection was disabled. Apparently, Norton Antivirus requires a listening port for email scanning. I concluded it was a greater risk to have email antivirus protection disabled, than having a port listening. Therefore, I need to rely on my firewall to block traffic on this port.

These tools should be run occasionally to make sure that no additional ports are listening. A listening port can be evidence of the presence of a malicious program.

Computer Risks

I have added an additional layer of security by selecting and installing a personal firewall. All ports will not accept or respond to requests that do not originate from my computer. This renders my computer invisible to subnet scans. While the firewall prevents access, the intrusion detection system will log suspicious activity for analysis. This is useful for examining port traffic for malicious activity.

If a virus or trojan program gets installed on the computer, there are defenses that will help prevent damage from occurring. There was antivirus software installed before hardening the system. This acts as a first line of defense. BlackICE offers the addition of application protection and communication control. This will prevent unknown files from executing and accessing the network. This is a great feature but can be irritating if you make frequent updates to the system.

There is the risk of performing a baseline inventory of the system after a virus or trojan program has been installed. If this occurs, application protection and communication control will trust the malicious program and won't alert the user of its presence.

There are always risks associated with undiscovered vulnerabilities in operating systems, device drivers, and applications. It is essential to keep updating these programs frequently to minimize this risk.

There are risks associated with web browsing using Internet Explorer. I have lowered this risk by custom configuring my Internet security zone. While I could have secured these settings further, I tried to find a nice balance between security and operability.

Earlier I discussed the risks associated with remote access. This is still a concern but also applies to all third party applications that establish connections from my computer to the Internet. Once these connections are created, the firewall will no longer restrict access. This is where is becomes extremely important to have a defense in depth strategy. In this scenario, security becomes dependant on intrusion detection, application protection and communication control, antivirus software, and having the latest security patches installed.

In the case of complete system failure or compromise, I have created a backup image of my computer using Norton Ghost 2002. The image has been password protected and will allow the restoration of the system to a known good state.

There is no method that can guarantee complete security other than disconnecting the computer from the network. It is up to the user to decide what level of security is acceptable.

References

Internet Security Systems. “Knowledgebase”. URL:
https://iss.custhelp.com/cgi-bin/iss.cfg/php/enduser/std_alp.php?p_prod_lvl1=33
(21 Jan. 2003).

“ICMP Types and Codes”. URL:
http://www.spirit.com/Resources/icmp.html
(21 Jan. 2003).

“Ethereal Homepage”. URL:
http://www.ethereal.com/
(21 Jan. 2003).

SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts’ Consensus”. SANS/FBI Top 20 List. Version 3.21. 17 Oct. 2002. URL:
http://www.sans.org/top20/
(26 Jan. 2003).

Microsoft. “Microsoft Baseline Security Analyzer”. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp
(26 Jan. 2003).

Qualys. “Qualys Browser Checkup”. URL:
http://browsercheck.qualys.com/
(26 Jan. 2003).

Microsoft. “Setting Up Security Zones”. URL:
http://www.microsoft.com/windows/ie/using/howto/security/setup.asp
(26 Jan.2003).

Symantec. “How to disable or remove the Windows Scripting Host”. URL:
http://securityresponse.symantec.com/avcenter/venc/data/win.script.hosting.html
(26 Jan. 2003).

UKSecurityOnline. “Disabling unnecessary and potentially dangerous services”. URL:
http://www.uksecurityonline.com/husdg/windowsxp/disableservices.htm
(29 Jan. 2003).

UKsecurityOnline. “Windows XP - Home User Self-Defence”. URL:
http://www.uksecurityonline.com/husdg/wxpp2.php
(29 Jan. 2003).

Gibson Research Corporation. “A Brief Summary of My Position on the Denial of Service Windows XP Raw Socket Controversy”. 02 Aug. 2001. URL: http://grc.com/dos/xpsummary.htm
(29 Jan. 2003).

Gibson Research Corporation. “Introducing SocketToMe & SocketLock”. 24 Jan. 2002. URL:
http://grc.com/dos/sockettome1.htm
(29 Jan. 2003).

Harris. “Vulnerability Management – STAT Scanner”. 18 Dec. 2002. URL:
http://www.statonline.com/solutions/vuln_assess/index.asp
(29 Jan. 2003).

Symantec. “Symantec Security Check”. URL:
http://security.symantec.com/ssc/sc_ipcheck.asp?ax=0&langid=ie&venid=sym&plfid=23&pkj=MYBIPWFYJOKMFIDPMSV
(02 Feb. 2003).

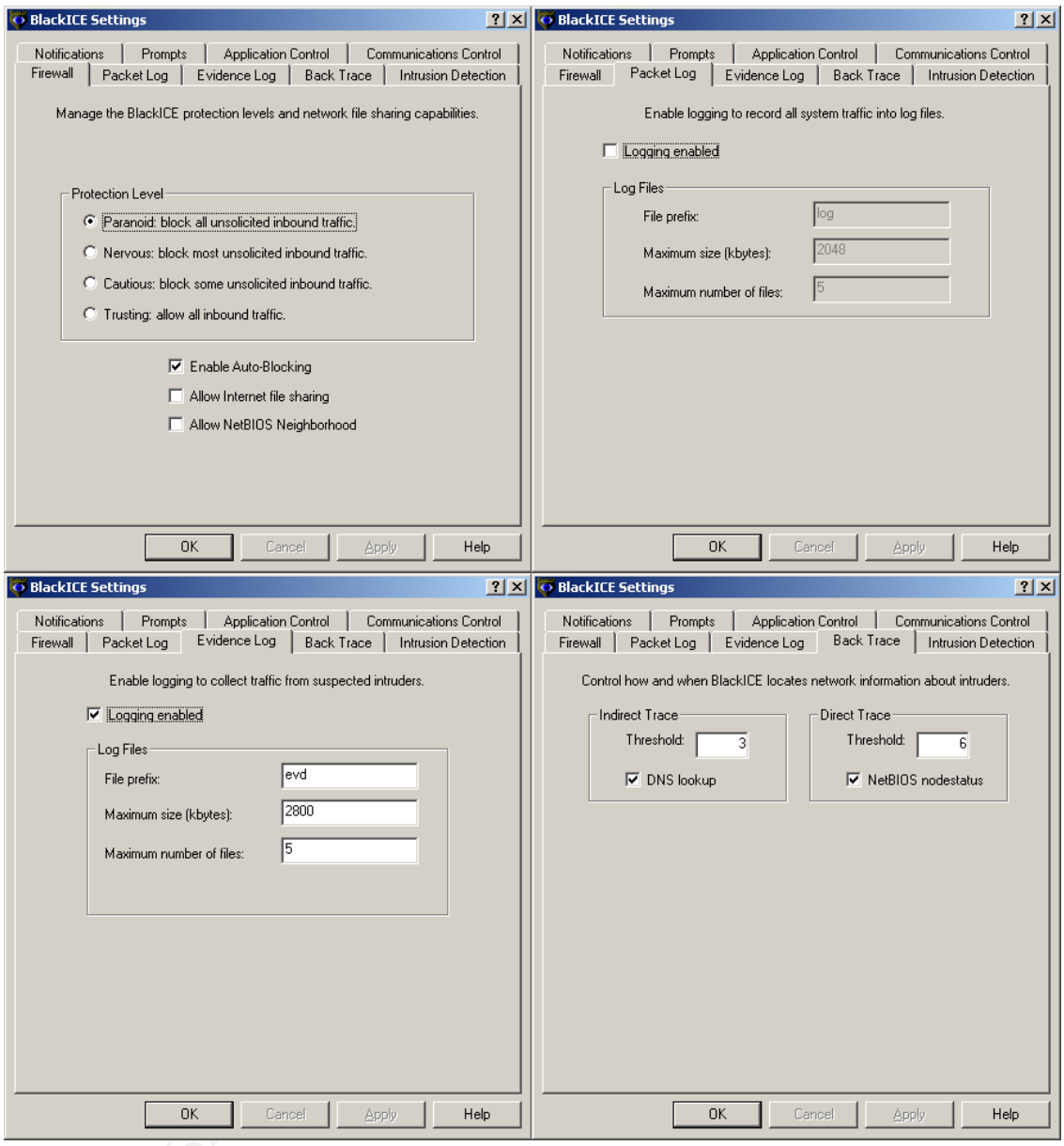
Broadband Reports.com. “Port scan..”. URL:
http://www.dslreports.com/scan
(02 Feb. 2003).

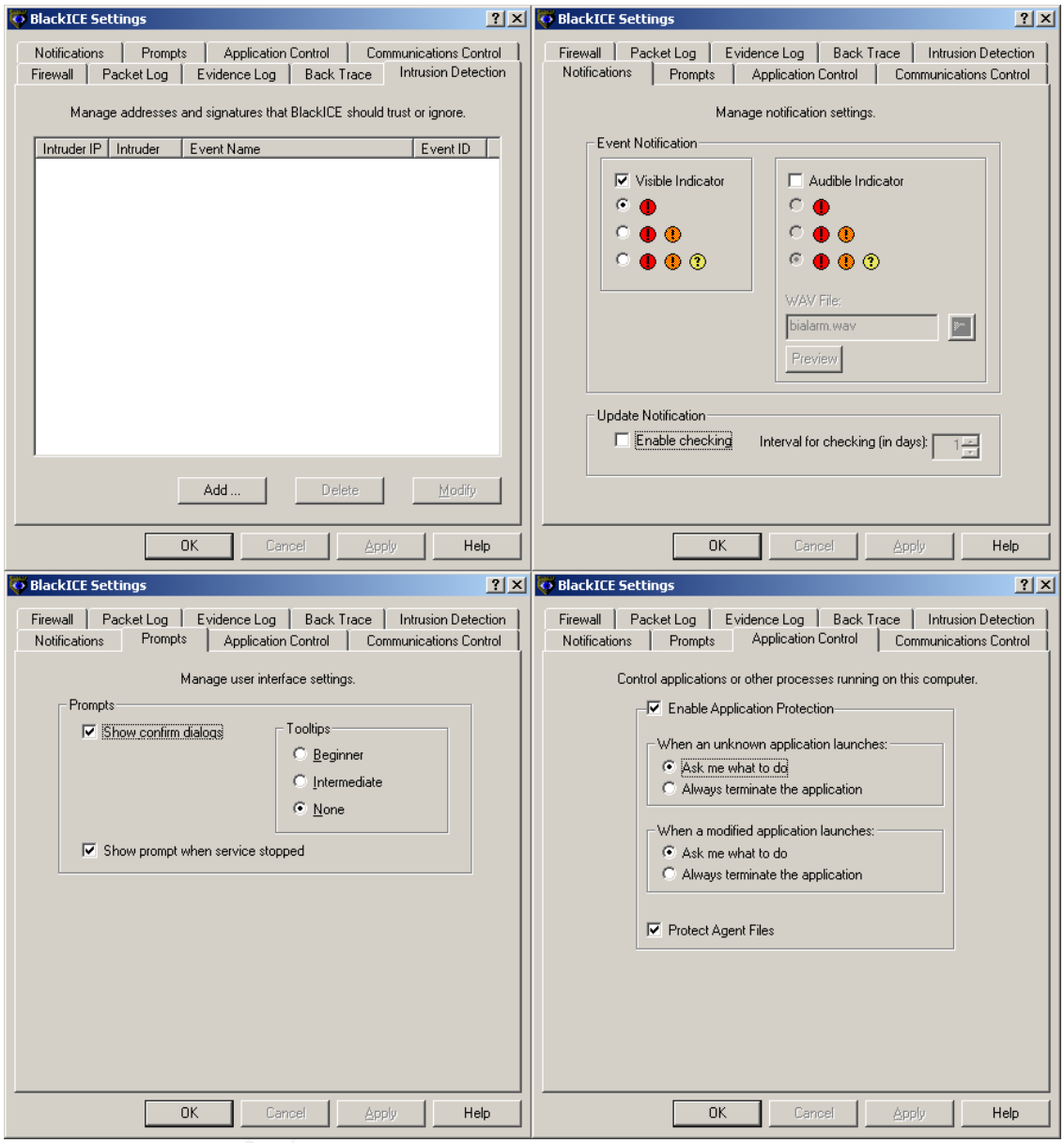
Gibson Research Corporation. “Shields Up!!”. URL:
https://grc.com/x/ne.dll?bh0bkyd2
(02 Feb. 2003).

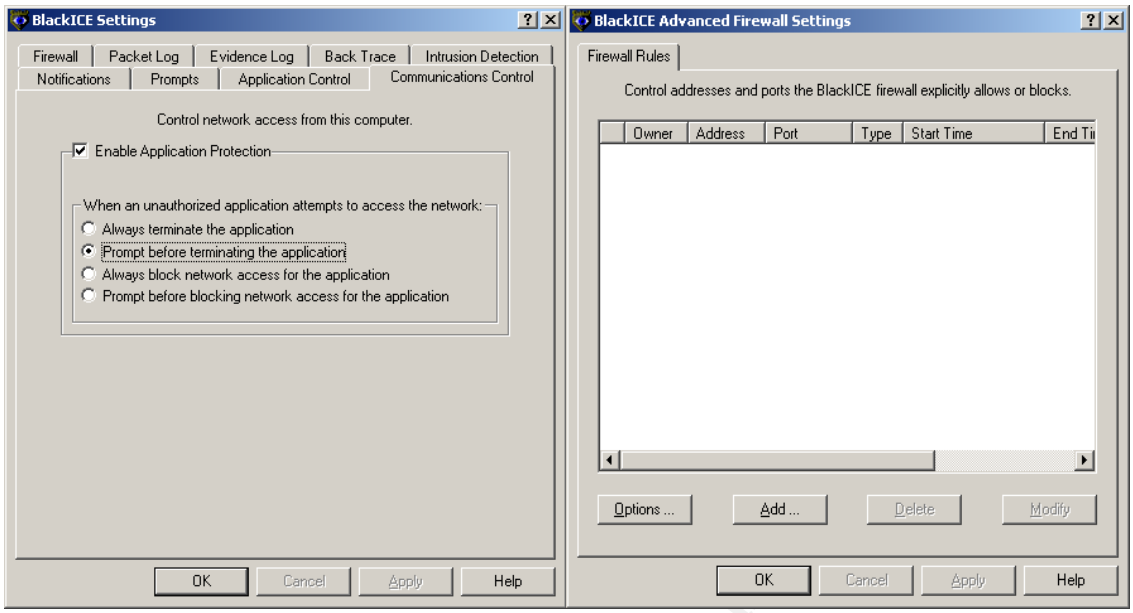
Foundstone. “Fport”. URL:
http://www.foundstone.com/knowledge/proddesc/fport.html
(02 Feb. 2003).

Microsoft. “A Description of Svchost.exe in Windows XP”. URL:
http://support.microsoft.com/default.aspx?scid=kb;en-us;314056
(04 Feb. 2003).

Appendix A: ISS BlackICE PC Protection Settings







Appendix B: Windows XP Services

Service Name	Original Settings (Before)	Current Settings (After)
Alerter	Manual	Not Installed
Application Layer Gateway Service	Manual	Disabled
Application Management	Manual	Disabled
Automatic Updates	Automatic	Disabled
Background Intelligent Transfer Service	Manual	Disabled
BlackICE	Automatic	Automatic
Cisco Systems, Inc. VPN Service	Automatic	Automatic
ClipBook	Manual	Disabled
COM+ Event System	Manual	Disabled
COM+ System Application	Manual	Disabled
Computer Browser	Automatic	Not Installed
Cryptographic Services	Automatic	Automatic
DHCP Client	Automatic	Automatic
Distributed Link Tracking Client	Automatic	Disabled
Distributed Transaction Coordinator	Manual	Disabled
DNS Client	Automatic	Disabled
Error Reporting Service	Automatic	Disabled
Event Log	Automatic	Automatic
Fast User Switching Compatibility	Manual	Disabled
Help and Support	Automatic	Disabled
Human Interface Device Access	Disabled	Disabled
IMAPI CD-Burning COM Service	Manual	Manual
Indexing Service	Manual	Disabled
Internet Connection Firewall (ICF/ICS)	Manual	Disabled
IPSEC Services	Automatic	Disabled
Logical Disk Manager	Automatic	Disabled
Logical Disk Manager Administrative Service	Manual	Disabled
Messenger	Automatic	Not Installed
MS Software Shadow Copy Provider	Manual	Disabled
NetMeeting Remote Desktop Sharing	Manual	Disabled
Network Connections	Manual	Manual
Network DDE	Manual	Disabled
Network DDE DSDM	Manual	Disabled
Network Location Awareness (NLA)	Manual	Disabled
Norton AntiVirus Auto Protect Service	Automatic	Automatic
Norton Unerase Protection	Disabled	Disabled

NVIDIA Driver Helper Service	Automatic	Disabled
NT LM Security Support Provider	Manual	Not Installed
Performance Logs and Alerts	Manual	Disabled
Plug and Play	Automatic	Automatic
Portable Media Serial Number Service	Automatic	Disabled
Print Spooler	Automatic	Automatic
Protected Storage	Automatic	Disabled
QoS RSVP	Manual	Disabled
RapApp	Automatic	Automatic
Remote Access Auto Connection Manager	Manual	Disabled
Remote Access Connection Manager	Manual	Disabled
Remote Desktop Help Session Manager	Manual	Disabled
Remote Procedure Call (RPC)	Automatic	Automatic
Remote Procedure Call (RPC) Locator	Manual	Not Installed
Removable Storage	Manual	Disabled
Routing and Remote Access	Manual	Disabled
ScriptBlocking Service	Automatic	Automatic
Secondary Logon	Automatic	Disabled
Security Accounts Manager	Automatic	Disabled
Server	Automatic	Not Installed
Shell Hardware Detection	Automatic	Disabled
Smart Card	Manual	Disabled
Smart Card Helper	Manual	Disabled
Speed Disk service	Manual	Disabled
SSDP Discovery Service	Manual	Disabled
System Event Notification	Automatic	Disabled
System Restore Service	Automatic	Disabled
Task Scheduler	Automatic	Disabled
TCP/IP NetBIOS Helper	Automatic	Disabled
Telephony	Manual	Disabled
Terminal Services	Manual	Disabled
Themes	Automatic	Disabled
Uninterruptible Power Supply	Manual	Disabled
Universal Plug and Play Device Host	Manual	Disabled
Upload Manager	Automatic	Disabled
Volume Shadow Copy	Manual	Disabled
WebClient	Automatic	Disabled
Windows Audio	Automatic	Automatic
Windows Image Acquisition (WIA)	Manual	Disabled
Windows Installer	Manual	Manual

Windows Management Instrumentation	Automatic	Automatic
Windows Time	Automatic	Disabled
Wireless Zero Configuration	Automatic	Disabled
WMI Performance Adapter	Manual	Disabled
Workstation	Automatic	Not Installed