



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gсна>

Auditing a Windows 2000 Web Server Running IIS 5.0

GIAC System and Network Auditor

Version 3.2

Option 1

Britt Savage

3/20/2005

Table of Contents

<u>Abstract</u>	4
<u>1 Research in Audit, Measurement Practice, and Control</u>	5
<u>1.1 System to be Audited</u>	5
<u>1.2 Risks to the System</u>	6
<u>1.2.1 Threats</u>	7
<u>1.2.2 Vulnerabilities</u>	7
<u>1.3 Current State of Practice</u>	9
<u>1.3.1 Nessus</u>	9
<u>1.3.2 Windows and IIS Hotfix Checking Tool</u>	9
<u>1.3.3 SurfersBeware.com Anti-Virus Checklist</u>	9
<u>1.3.4 Sean Heare's Data Center Physical Security Checklist</u>	10
<u>1.3.5 Leland Stanford Junior University IIS Security Checklist</u>	10
<u>1.3.6 Microsoft Corporation's Windows 2000 Security Hardening Guide</u>	10
<u>1.4 Scope</u>	10
<u>2 Audit Checklist</u>	11
<u>2.1 Physical Security</u>	11
<u>2.2 Server Hardening</u>	13
<u>2.2.1 Account Policy</u>	13
<u>2.2.2 Audit Policy</u>	14
<u>2.2.3 User Rights</u>	14
<u>2.2.4 Security Options</u>	16
<u>2.2.5 Unneeded Services</u>	18
<u>2.2.6 Removal of Unneeded Windows Components</u>	20
<u>2.2.7 Scan for Vulnerabilities</u>	21
<u>2.3 IIS Hardening</u>	23
<u>2.3.1 Removal of Default Installation Directories</u>	23
<u>2.3.2 Removal of Unnecessary ISAPI Filters</u>	24
<u>2.3.3 Removal of Unnecessary Extensions</u>	25
<u>2.3.4 File ACL's</u>	27
<u>2.4 Maintenance Procedures</u>	29
<u>2.4.1 Patch Level/Policy</u>	29
<u>2.4.2 Anti-Virus</u>	30
<u>2.4.3 Data/Configuration Backup</u>	31
<u>3 Audit Results</u>	33
<u>3.1 Physical Security</u>	33
<u>3.2 Server Hardening</u>	33
<u>3.2.1 Account Policy</u>	33
<u>3.2.2 Audit Policy</u>	35
<u>3.2.3 User Rights</u>	36
<u>3.2.4 Security Options</u>	36
<u>3.2.5 Unneeded Services</u>	39

<u>3.2.6</u>	<u>Removal of Unneeded Windows Components</u>	44
<u>3.2.7</u>	<u>Scan for Vulnerabilities</u>	45
<u>3.3</u>	<u>IIS Hardening</u>	45
<u>3.3.1</u>	<u>Removal of Default Installation Directories</u>	45
<u>3.3.2</u>	<u>Removal of Unnecessary ISAPI Filters</u>	46
<u>3.3.3</u>	<u>Removal of Unnecessary Extensions</u>	48
<u>3.3.4</u>	<u>File ACL's</u>	51
<u>3.4</u>	<u>Maintenance Procedures</u>	53
<u>3.4.1</u>	<u>Patch Level/Policy</u>	53
<u>3.4.2</u>	<u>Anti-Virus</u>	55
<u>3.4.3</u>	<u>Data/Configuration Backup</u>	55
<u>4</u>	<u>Audit Report</u>	57
<u>4.1</u>	<u>Executive Summary</u>	57
<u>4.2</u>	<u>Audit Findings and Recommendations</u>	57
<u>4.2.1</u>	<u>Positive Findings:</u>	57
<u>4.2.2</u>	<u>Negative Findings:</u>	60
	<u>References</u>	63
	<u>Appendix A – Nessus Scan Results</u>	64

Abstract

This paper is a security assessment of a Microsoft Windows 2000 server running IIS 5.0. The server is operated by XYZ, Inc., which is a small web based company that serves a small number of users. The web pages are dynamically created using ASP. The audit of this system is intended to assess the security of the operating system and the application which hosts its web pages, namely IIS. The results will be used by XYZ, Inc. to improve the security of the web server and mitigate any risks posed to it.

© SANS Institute 2000 - 2005, Author retains full rights.

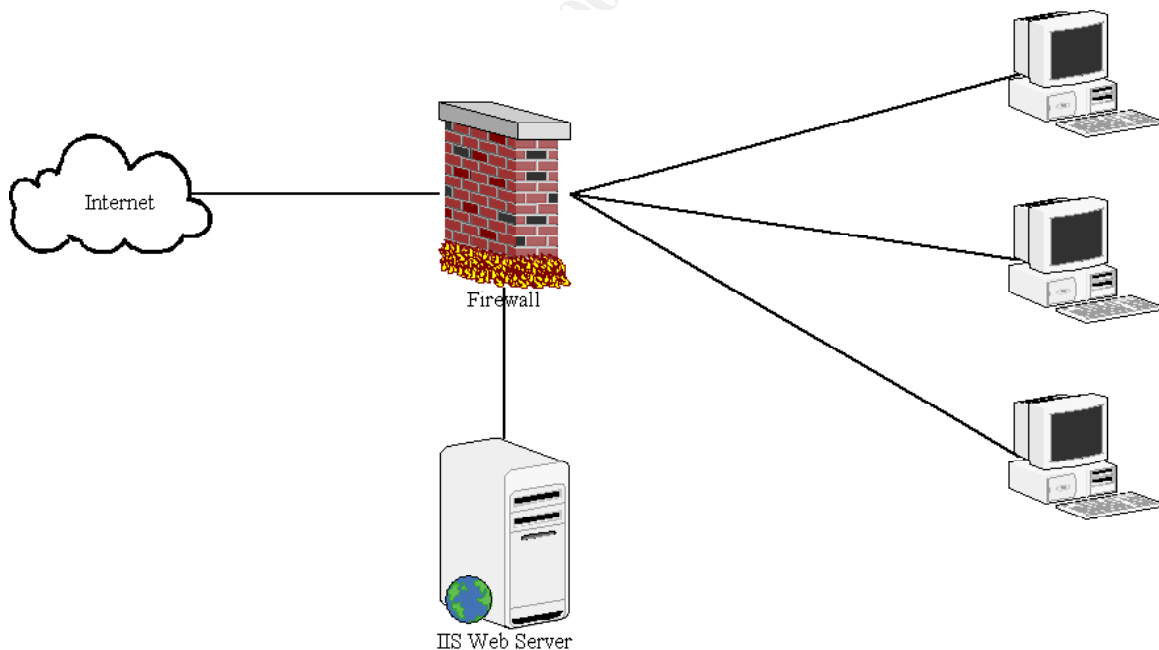
2 Research in Audit, Measurement Practice, and Control

2.1 System to be Audited

XYZ, Inc. is a very small web based company that provides users with a web site that serves dynamic web pages to a small set of customers. Each user must have a login in order to access the system. Although the server is accessible over the internet, only a few people can access the actual content of the web server.

The web server is running on a Dell PowerEdge 600sc with Windows 2000 Server. The users can only connect to the web site using http on the usual port 80. The web site uses Microsoft IIS to serve active server pages, and the backend database is running on the same server using a Microsoft Access ODBC to store information. A NetGear FR114P firewall/router creates a DMZ separating the server from the administrative network.

The network is a very simple setup, which I have illustrated below:



Here is the system information, which I have gathered using msinfo32.exe (the information in *Italics>* has been changed in order to hide that information):

Item	Value
OS Name	Microsoft Windows 2000 Server
Version	5.0.2195 Service Pack 4 Build 2195

OS Manufacturer	Microsoft Corporation
System Name	Web Server
System Manufacturer	Dell Computer Corporation
System Model	PowerEdge 600SC
System Type	X86-based PC
Processor	x86 Family 15 Model 2 Stepping 9 GenuineIntel ~2399 Mhz
BIOS Version	Phoenix ROM BIOS PLUS Version 1.10 A07
Windows Directory	C:\WINNT
System Directory	C:\WINNT\system32
Boot Device	\Device\Harddisk0\Partition1
Locale	United States
User Name	XXXXXXXXXXXXXXXXXXXX
Time Zone	Central Standard Time
Total Physical Memory	1,310,196 KB
Available Physical Memory	985,760 KB
Total Virtual Memory	2,862,448 KB
Available Virtual Memory	2,400,640 KB
Page File Space	1,552,252 KB
Page File	C:\pagefile.sys

2.2 Risks to the System

In evaluating the risks to a system, one must take into account two main factors:

- Threat – A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.¹ Examples of threats are malware, human error, and natural disasters.
- Vulnerability – A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.² Examples of vulnerabilities are unpatched systems, unlocked doors, and the lack of a redundant power supply.

Risks can be quantified by assigning a numeric value from one to ten to the threat, where one is the lowest probability that the threat will occur and ten is the highest probability. We likewise assign a value to the vulnerability using the same scale. We can then use the simple formula³:

¹ <http://www.sans.org/resources/glossary.php>

² <http://www.sans.org/resources/glossary.php>

³ Hoelzer, p. 2-34

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

This gives a quantifiable numeric value to the seriousness of the risk. We will use the following scale to rate the vulnerability as high, medium, or low:

Range	Seriousness
0-30	Low
31-70	Medium
71-100	High

2.2.1 Threats

Below is a table describing the possible threats to the system in question and a rating as described in section 1.2.

Threat	Probability	Capacity to Inflict Damage
Physical Threats	4	<ul style="list-style-type: none"> • Data and Hardware Theft • Data and Hardware Destruction • Loss of Availability (Denial of Service) • Disclosure of Private Information
Hackers	10	<ul style="list-style-type: none"> • Data Loss • Data Theft • Data Manipulation • Loss of Availability (Denial of Service) • Disclosure of Private Information
Malware and Viruses	10	<ul style="list-style-type: none"> • Data Loss • Data Theft • Data Manipulation • Loss of Availability (Denial of Service) • Disclosure of Private Information
Administrative and User Error	5	<ul style="list-style-type: none"> • Data Loss • Inadvertent Data Manipulation • Loss of Availability (Denial of Service) • Disclosure of Private Information

2.2.2 Vulnerabilities

Below is a table of possible vulnerabilities

Vulnerability	Likelihood of Exploit	Potential Impact
Unauthorized Physical Access	4	<p>Unauthorized physical access can lead to the following:</p> <ul style="list-style-type: none"> • Destruction of physical components • The loss, alteration, or theft of data. • Introduction of malware or viruses
Unauthorized Remote Access	10	<p>Unauthorized remote access can lead to the following:</p> <ul style="list-style-type: none"> • The loss, alteration, or theft of data. • Introduction of malware or viruses
Generic Accounts	6	<p>The use of default accounts and accounts with more privileges than necessary can lead to the following:</p> <ul style="list-style-type: none"> • Privilege escalation • Backdoor attacks • The loss, alteration, or theft of data. • Introduction of malware or viruses
Insufficient Auditing	5	<p>Insufficient auditing can lead to the following:</p> <ul style="list-style-type: none"> • Untraceable introduction of malware or viruses • Untraceable loss, alteration, or theft of data
Insufficient Access Controls	6	<p>Insufficient access controls can lead to the following:</p> <ul style="list-style-type: none"> • Privilege escalation • The loss, alteration, or theft of data. • Introduction of malware or viruses
Unnecessary Software or Services	6	<p>The presence of unnecessary software or services running on the system can lead to the following:</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • Backdoor attacks
Default Installation of IIS	8	<p>IIS being installed with the default configuration and settings can lead to the following:</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • The loss, alteration, or theft of data • Backdoor attacks

Known Vulnerabilities in Software	8	<p>Leaving known vulnerabilities in software unpatched can lead to the following</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • Backdoor attacks
Insufficient Anti-Virus Protection	4	<p>Having insufficient virus protection can lead to the following:</p> <ul style="list-style-type: none"> • Introduction of malware or viruses
Insufficient Backup Procedures	7	<p>The insufficient backup of data and software configurations can lead to the following when combined with any other disaster:</p> <ul style="list-style-type: none"> • The loss of data. • The loss of availability due to reconfiguration.

2.3 Current State of Practice

The following tools and references are used in this audit:

2.3.1 Nessus

<http://www.insecure.org>

Nessus is a vulnerability scanner. It is looked upon as one of the premier tools used by security professional. It will be run from a Fedora Core 2 Linux laptop, which will be connected to the DMZ.

2.3.2 Windows and IIS Hotfix Checking Tool

IIS:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=6c8afc1c-5008-4ac8-84e1-1632937dbd74&DisplayLang=en>

Windows 2000:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=25bd2e13-b437-4f1c-a36a-1bbf6e8ba288&DisplayLang=en>

Microsoft maintains a database of hotfixes that it has made available to the public. Microsoft has provided these tools, which compare the hotfixes installed on a system to this database.

2.3.3 SurfersBeware.com Anti-Virus Checklist

<http://viruses.surferbeware.com/antivirus-checklist.htm>

SurfersBeware.com has made available a checklist for configuring a generic Anti-Virus tool on any system.

2.3.4 Sean Heare's Data Center Physical Security Checklist

<http://sans.org/rr/whitepapers/awareness/416.php>

The SANS Institute has posted this white paper outlining guidelines for the physical security of a data center.

2.3.5 Leland Stanford Junior University IIS Security Checklist

<http://windows.stanford.edu/docs/IISsecchecklist.htm>

The trustees of Leland Stanford Junior University have posted this security checklist outlining detailed steps for securing Microsoft Internet Information Services.

2.3.6 Microsoft Corporation's Windows 2000 Security Hardening Guide

<http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en>

Microsoft has published a security hardening guide made available for download on their website. This guide has been geared more for a generic installation, and not all settings that it suggests are appropriate for a web server. It is still a good starting point for hardening a Windows 2000 host, though.

2.4 Scope

I have been asked to audit the system and its configuration. This will include the hardening of the operating system and IIS. I will not be auditing the network configuration or the configuration of the firewall. The scanning of any other system on the network, including the firewall, is strictly forbidden. I have only included the above network diagram as a reference to the operation of the

system. Procedures and policies that directly affect the security of the system will be taken into account in the assessment of the system.

© SANS Institute 2000 - 2005, Author retains full rights.

3 Audit Checklist

3.1 Physical Security

Reference	<p>Information Security Awareness and Education, http://www.security.umassp.edu/index.cfm?fuseaction=generic.506</p> <p>Data Center Physical Security Checklist, http://sans.org/rr/whitepapers/awareness/416.php</p>
Risk	<p>Physical security is a very important aspect of the overall security of a system that can be easily overlooked. Proper physical security helps deter people with bad intentions from gaining access to the system and prevents them from damaging data as well as hardware. Physical controls also help prevent people with good intentions from accidentally causing damage to physical components and data.</p> <p>Physical controls are not solely for preventing people from causing harm to a system. They also insure that, in the case of a natural disaster such as a fire or power outage, the system remains protected.</p> <ul style="list-style-type: none">• Introduction of malware or viruses• The loss, alteration, or theft of data• The loss, theft, or destruction of hardware• Loss of Availability

Testing Criteria / Compliance Criteria	<p>By inspection of the facility housing the system, verify the following:</p> <ul style="list-style-type: none"> • Are doors locked? • Are proper access controls in place? • Is an alarm system in place? • Is a usable fire extinguisher available? • Are proper smoke detectors in place? • Are the air temperature and humidity controlled? • Is a power backup in place? • Are the output devices protected from eavesdroppers at windows, etc?
Compliance	Pass / Fail
Test Nature	Subjective

© SANS Institute 2000 - 2005, 2006

3.2 Server Hardening

3.2.1 Account Policy

Reference	<p>Hardening Windows 2000, http://www.systemexperts.com/win2k/hardenW2K13.pdf</p> <p>Hadening Windows 2000 Server, http://www.whitehats.ca/main/members/Cerberus/cerberus_harden_w2k/cerberus_harden_w2k.html,</p> <p>Personal Experience</p>
Risk	<p>A weak account policy leaves the security of the system in the hands of each and every user. Proper account policies force the users to have strong passwords, change them on a regular basis, among other things. This helps in preventing hackers from gaining access to the system by being able to figure out a user's password.</p> <ul style="list-style-type: none">• Introduction of malware or viruses• The loss, alteration, or theft of data• Loss of Availability
Testing Criteria / Compliance Criteria	<p>Verify the system's account policy by using the Local Security Settings Tool. This can be brought up by clicking "Start" -> "Settings" -> "Control Panel" -> "Administrative Tools" -> "Local Security Policy." Verify that at a minimum the following is set:</p> <ul style="list-style-type: none">• Enforce password history: 5• Maximum password age: 60 days• Minimum password age: 5 days• Minimum password length: 8 characters• Passwords must meet complexity requirements: Enabled• Store password using reversible encryption for all users in the domain: Disabled• Account lockout duration: 15 days• Account lockout threshold: 3• Reset account lockout counter after: 30 minutes
Compliance	Pass / Fail

Test Nature	Objective
--------------------	-----------

3.2.2 Audit Policy

Reference	<p>Hardening Windows 2000, http://www.systemexperts.com/win2k/hardenW2K13.pdf</p> <p>Hardening Windows 2000 Server, http://www.whitehats.ca/main/members/Cerberus/cerberus_harden_w2k/cerberus_harden_w2k.html,</p> <p>Personal Experience</p>
Risk	<p>Although auditing is not a preventative security measure, it is essential to have when something goes wrong. If something happens on the system, such as loss of data, the best way to determine what happened is by reviewing the logs. Also, in a legal situation, it is very important to have sufficient logs to prove what happened.</p> <ul style="list-style-type: none"> • User Error • Unauthorized Access
Testing Criteria / Compliance Criteria	<p>Verify the system's audit policy by using the Local Security Settings Tool. This can be brought up by clicking "Start" -> "Settings" -> "Control Panel" -> "Administrative Tools" -> "Local Security Policy." Verify that at a minimum the following is set:</p> <ul style="list-style-type: none"> • Audit account logon events: success, failure • Audit account management: success, failure • Audit logon events: success, failure • Audit policy change: success, failure • Audit system events: success, failure
Compliance	Pass / Fail
Test Nature	Objective

3.2.3 User Rights

Reference	<p>Hardening Windows 2000, http://www.systemexperts.com/win2k/hardenW2K13.pdf</p> <p>Hadening Windows 2000 Server, http://www.whitehats.ca/main/members/Cerberus/cerberus_harden_w2k/cerberus_harden_w2k.html,</p> <p>Personal Experience</p>
Risk	<p>User rights are essential in practicing the policy of least privileged. This prevents users who should not be able to perform certain activities from making a mistake and causing the system or data harm. The policy of least privileged also prevent hackers that are able to gain access to the system through lower privileged accounts from causing more damage that would other wise be possible.</p> <ul style="list-style-type: none"> • User Error • Unauthorized Access • The loss, alteration, or theft of data • Loss of Availability

© SANS Institute 2000 - 2005

Testing Criteria / Compliance Criteria	<p>Verify the system's user rights assignment by using the Local Security Settings Tool. This can be brought up by clicking "Start" -> "Settings" -> "Control Panel" -> "Administrative Tools" -> "Local Security Policy." Verify that at a minimum the following is set:</p> <ul style="list-style-type: none"> • Act as part of the operating system: Administrator • Access this computer from the network: None • Backup files and directories: Administrator • Change the system time: Administrator • Create a token object: Administrator • Debug programs: Administrator • Deny access to this computer from the network: Everyone • Force Shutdown from a remote system: None • Increase scheduling priority: Administrator • Load and unload device drivers: Administrator • Manage auditing and security log: Administrator • Modify firmware environment variables: Administrator • Profile single processes: Administrator • Profile system performance: Administrator • Replace a process level token: Administrator • Restore files and directories: Administrator • Shut down the system: Administrator
Compliance	Pass / Fail
Test Nature	Objective

3.2.4 Security Options

Reference	<p>Hardening Windows 2000, http://www.systemexperts.com/win2k/hardenW2K13.pdf</p> <p>Hadening Windows 2000 Server, http://www.whitehats.ca/main/members/Cerberus/cerberus_harden_w2k/cerberus_harden_w2k.html,</p> <p>Personal Experience</p>
------------------	---

Risk	<p>Windows 2000 provides many options that further the security of the system. These options include mechanisms for discouraging people with physical access from performing illegal actions as well as preventing hackers, malware, and viruses from gaining access to the system. The risks to the system that are reduced by properly configuring the security settings in Windows include:</p> <ul style="list-style-type: none">• User Error• Unauthorized Access• The loss, alteration, or theft of data• Loss of Availability• Backdoor attacks
-------------	--

© SANS Institute 2000 - 2005, Author

Testing Criteria / Compliance Criteria	<p>Verify the system's security settings by using the Local Security Settings Tool. This can be brought up by clicking "Start" -> "Settings" -> "Control Panel" -> "Administrative Tools" -> "Local Security Policy." Verify that at a minimum the following is set:</p> <ul style="list-style-type: none"> • Additional restrictions for anonymous connections: No access without explicit anonymous permissions • Allow system to be shut down without having to log on: Disabled • Audit use of backup and restore privilege: Enabled • Clear virtual memory pagefile when system shuts down: Enabled • Digitally sign client communication (always): Enabled • Digitally sign server communication (always): Enabled • Disable CTRL+ALT+DEL requirement for logon: Disabled • Do not display last user name in logon screen: Enabled • LAN manager authentication level: Send NTLMv2 responses only/refuse LM & NTLM • Number of previous logons to cache (in case domain controller is not available): 0 • Prevent users from installing printer drivers: Enabled • Recovery console: allow automatic administrative logon: Disabled • Rename administrator account: Rename this to something other than "admin" or "administrator" • Restrict CD-ROM access to locally logged-on user only: Enabled • Restrict floppy access to locally logged-on user only: Enabled • Secure channel: digitally encrypt or sign secure channel data (Always): Enabled
---	--

Compliance	Pass / Fail
Test Nature	Objective

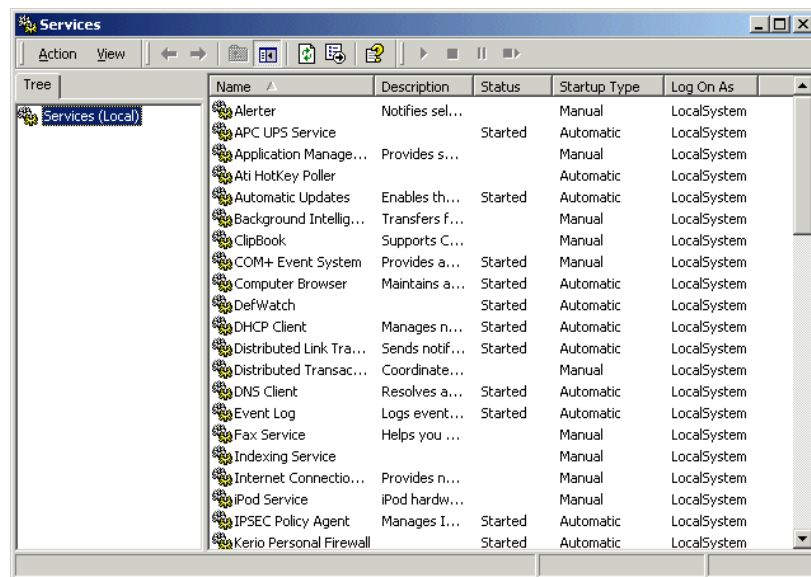
3.2.5 Unneeded Services

Reference	<p>Windows 2000 Services, http://www.sampublishing.com/articles/article.asp?p=25176&seqNum=3</p> <p>List of services that are needed to run a security-enhanced IIS computer, http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q189/2/71.ASP&NoWebContent=1</p> <p>Glossary of Windows 2000 Services, http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp</p>
Risk	<p>By default, Windows starts up many unneeded services, which can be disabled. These services can potentially contain security flaws, which can be exploited by viruses, hackers, and malware. It is good security practice to only have those services running on a system that are needed for the system to run as needed. If a service is definitely not needed it should be deleted.</p> <p>Windows has three options for the availability of its services:</p> <ul style="list-style-type: none"> • Disabled – The service cannot be used. • Manual – The service must be manually brought up. • Automatic – The services is started on system startup. <p>The following are security risks that can be reduced by disabling unneeded services:</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • The loss, alteration, or theft of data • Backdoor attacks • Loss of Availability

Testing Criteria / Compliance Criteria

Bring up the Services utility in Windows 2000. By inspection, verify that all services, which are enabled, are needed by the system.

The services utility can be brought up by clicking “Start” -> “Settings” -> “Control Panel” -> “Administrative Tools” -> “Services”



Here is a list of services required by Microsoft IIS.

Required:

- Event Log
- IIS Admin Services
- License Logging Service
- MSDTC
- Protected Storage
- Remote Procedure Call (RPC) Service
- Server
- Windows NT Server or Windows NT Workstation
- Windows NTLM Security Support Provider
- Workstation
- World Wide Web Publishing Service

May be required:

- Certificate Authority (required to issue certificates)
- Content Index (required if using Index Server)
- FTP Publishing Service (required if using FTP service; it's highly recommended that FTP and Web services run on different servers)
- NNTP Service (required if using NNTP Service)
- Plug and Play (recommended, but not required)
- Remote Access Services (required if you use dial-up access)
- RPC Locator (required if doing remote

Compliance	Pass / Fail
Test Nature	Objective and Subjective

Note: The above list of services is provided by Microsoft.⁴

3.2.6 Removal of Unneeded Windows Components

Reference	Personal Experience
Risk	<p>Windows components have much of the same security implications as Windows services. By having unnecessary components installed on a server, unnecessary security risks are taken. Windows components can have security flaws, which hackers, viruses, and malware can take advantage of to gain access to a system.</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • The loss, alteration, or theft of data • Backdoor attacks • Loss of Availability
Testing Criteria / Compliance Criteria	<p>To view the windows components installed on a system, click "Start" -> "Settings" -> "Control Panel" -> "Add/Remove Programs." Then click "Add/Remove Windows Components." Verify by inspection that only the necessary Windows components are installed.</p> <p>The following are the only components that are required by an IIS http server:</p> <ul style="list-style-type: none"> • IIS Common Files • IIS World Wide Web Server <p>Other components that may be necessary are:</p> <ul style="list-style-type: none"> • IIS Snap-In • Certificate Server
Compliance	Pass / Fail
Test Nature	Subjective

3.2.7 Scan for Vulnerabilities

Reference	Nessus Scanning on Windows Domain, http://www.nessus.org/documentation/nessus_domain_whitepaper.pdf Personal Experience
Risk	<p>Nessus is a security tool that scans for known vulnerabilities. It will determine the operating system and what is running on the system, along with the vulnerabilities associated with these things. By knowing what vulnerabilities exist on a system, this gives us an opportunity to patch them before they are exploited. By patching the vulnerabilities found by Nessus before a hacker, virus, or malware find them help reduce the following risks:</p> <ul style="list-style-type: none">• Introduction of malware or viruses• The loss, alteration, or theft of data• Backdoor attacks• Loss of Availability
Testing Criteria / Compliance Criteria	<p>Since a Nessus scan can have bad effects on the performance and possibly the availability of the server, I will perform the scan during a maintenance window in order to minimize these effects.</p> <p>I have been allowed to give Nessus access to the registry, as outlined in the paper by Sunil Vakharia, so I will scan with this access. To do this, I will create a "Nessus" user and give him only the required access as described by Mr. Vakharia. The following options will be set in the Scan:</p> <ul style="list-style-type: none">• Credentials – SMB Access is set to "Nessus"• Scan Options – Select "Safe checks"
Compliance	Pass / Fail
Test Nature	Subjective

3.3 IIS Hardening

3.3.1 Removal of Default Installation Directories

Reference	IIS Security Checklist, http://windows.stanford.edu/docs/IISsecchecklist.htm Personal Experience
Risk	<p>Having the default directories from an IIS installation can lead to exploits by hackers as well as robots that are looking for the holes associated with these directories. Also, by leaving the default directory structure for IIS, this gives an insight into the configuration to hackers, which can greatly simplify their attacks.</p> <ul style="list-style-type: none">• Introduction of malware or viruses• The loss, alteration, or theft of data• Backdoor attacks• Loss of Availability

Testing Criteria / Compliance Criteria	<p>Using Windows Explorer, check for the following content:</p> <ul style="list-style-type: none"> • %systemdirectory%\inetrv\iisadmin • %systemdirectory%\inetrv\iisadmpwd • inetpub\wwwroot (or \ftproot or \smtproot) • inetpub\scripts • inetpub\iissamples • inetpub\adminscripts • %systemroot%\help\iishelp\iis • %systemroot%\web\printers • %systemdrive%\program files\common files\system\msadc <p>In the Internet Services Manager check for the following virtual directories:</p> <ul style="list-style-type: none"> • iisadmin • iissamples • msadc. • iishelp • scripts • printers
Compliance	Pass / Fail
Test Nature	Objective

3.3.2 Removal of Unnecessary ISAPI Filters

Reference	<p>IIS Security Checklist, http://windows.stanford.edu/docs/IISsecchecklist.htm Personal Experience</p>
------------------	--

Risk	<p>As defined by Microsoft MSDN, ISAPI filters are DLL files that can be used to modify and enhance the functionality provided by IIS. ISAPI filters always run on an IIS server, filtering every request until they find one they need to process⁵. Hackers, viruses, and malware can use IIS ISAPI filters in much of the same way that the default IIS directory structure can be used. Known security flaws in the ISAPI filters can be used to gain access to the system, and execute malicious code.</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • The loss, alteration, or theft of data • Backdoor attacks • Loss of Availability
Testing Criteria / Compliance Criteria	<p>In the Internet Services Manager, select the ISAPI filter tab. Verify that no unnecessary filters are installed. Below is a list of common filters that may not be necessary:</p> <ul style="list-style-type: none"> • FrontPage • Digest Authentication • HTTP Authentication • SSL – SSL is a very good idea to use, but if it is not used, then it should be removed. <p>In Windows Explorer verify that the dll files associated with the ISAPI filters not being used are deleted:</p> <ul style="list-style-type: none"> • FrontPage: fpexdll.dll • Digest: md5filt.dll • Compression: compfilt.dll • SSL: sspifilt.dll
Compliance	Pass / Fail
Test Nature	Objective

⁵ Microsoft MSND, <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/html/e34a060c-6348-408c-9ce5-1b59f0cdebbs.asp>

3.3.3 Removal of Unnecessary Extensions

Reference	IIS Security Checklist, http://windows.stanford.edu/docs/IISsecchecklist.htm Personal Experience
Risk	<p>IIS extensions are used by IIS to verify specific types of files that can be executed by the web server to create dynamic web content. If code is introduced to the system containing these extensions, it could be used by hackers or malware to gain access to the system.</p> <ul style="list-style-type: none">• Introduction of malware or viruses• The loss, alteration, or theft of data• Backdoor attacks• Loss of Availability

© SANS Institute 2000 - 2005,

Testing Criteria / Compliance Criteria	<p>In the Internet Services Manager, go to the Home Directory Tab, and select Configuration. Verify that only the needed extensions are present. Here is a list of the default extensions:</p> <ul style="list-style-type: none"> • .htw • .ida • .idq • .asp • .cer • .cdx • .asa • .htr • .idc • .shtm • .shtml • .stm • .asax • .ascx • .ashx • .asmx • .aspx • .axd • .vsdisco • .rem • .soap • .config • .cs • .csproj • .vb • .vbproj • .webinfo • .licx • .resx • .resources
---	---

Compliance	Pass / Fail
Test Nature	Objective

3.3.4 File ACL's

Reference	<p>IIS Security Checklist, http://windows.stanford.edu/docs/IISsecchecklist.htm</p> <p>Personal Experience</p>
Risk	<p>IIS file access control lists are very important in the security of an IIS web server. By setting the acl's correctly, hacker and malware are prevented from being able to access parts of the web site that they are not intended to access. They will not be able to easily view sensitive data or execute code outside of the designated file system location.</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • The loss, alteration, or theft of data • Backdoor attacks

© SANS Institute 2000

Testing Criteria / Compliance Criteria	<p>In the Internet Services Manager, select “Properties” and the “Home Directory” tab. Verify that the permissions are set as stated below:</p> <ul style="list-style-type: none"> • Script Source Access – off • Read – on • Write – off • Directory Browsing – off • Index This Resource – off • Log Visits – on <p>Also in the “Home Directory” tab, click “Configuration.” Then click the “App Option” tab. Verify that the “Enable Parent Paths” option is disabled.</p> <p>In Windows Explorer, verify that the following permissions are set:</p> <ul style="list-style-type: none"> • IIS logs – System and Administrators only • Web root – Everyone read only • %systemroot% – Everyone read only • %systemroot%\system32 – Everyone read only • %systemroot%\system32\inetssrv – Everyone read only • %systemroot%\system32\inetssrv\asp – Everyone read only • %systemroot%\program files\common files\ – Everyone read only
Compliance	Pass / Fail
Test Nature	Objective

3.4 Maintenance Procedures

3.4.1 Patch Level/Policy

Reference	<p>IIS 5.0 Hotfix Checking Tool http://www.microsoft.com/downloads/details.aspx?FamilyID=6c8afc1c-5008-4ac8-84e1-1632937dbd74&DisplayLang=en</p> <p>Windows 2000 Hotfix Checking Tool: qfecheck.exe http://www.microsoft.com/downloads/details.aspx?FamilyID=25bd2e13-b437-4f1c-a36a-1bbf6e8ba288&DisplayLang=en</p> <p>Personal experience</p>
Risk	<p>Not having the latest patches and hotfixes installed in Windows or IIS can lead to hackers being able to access the system through known security flaws. It also allows for viruses, malware, and robots that scan for know holes in these components to find these holes and enter the system. They can then make the system part of a “zombie” network, used to attack other systems, run a denial of service attack, or harm or steal data off of the system. It usually takes less than a few days from the initial time that Microsoft releases information on known security flaws for hackers to create code that exploits these flaws.</p> <p>It is very important for administrators to have a good patching policy that they stick to in order to prevent this type of attack.</p> <ul style="list-style-type: none">• Introduction of malware or viruses• The loss, alteration, or theft of data• Loss of Availability

Testing Criteria / Compliance Criteria	<p>Inspect the administrator's patching policy for the following information:</p> <ul style="list-style-type: none"> • Schedule of applying patches • Testing procedure • Back-out procedures • Patch tracking procedures <p>Download and install the Windows 2000 Hotfix Checking Tool. Run this and verify that the patches and hotfixes that have not been installed are either not critical or have been noted as to why they have not been installed.</p> <p>Download and install the IIS Hotfix Checking Tool. Run this and verify that the patches and hotfixes that have not been installed are either not critical or have been noted as to why they have not been installed.</p>
Compliance	Pass / Fail
Test Nature	Objective and Subjective

3.4.2 Anti-Virus

Reference	<p>Anti-Virus Checklist, http://viruses.surferbeware.com/antivirus-checklist.htm</p> <p>Personal Experience</p>
Risk	<p>With the proper configuration anti-virus software scans all new files and data that are introduced to the system. If the anti-virus software has the latest virus definitions, the chance that a new virus will enter the system is greatly reduced. E-mail should not be configured on a web server such as this, but just to be on the safe side, the anti-virus software should be configured to scan all incoming email, as well as downloads.</p> <ul style="list-style-type: none"> • Introduction of malware or viruses • The loss, alteration, or theft of data • Loss of Availability

Testing Criteria / Compliance Criteria	<p>Verify that an anti-virus scanner has been installed on the server. Verify that the following settings have been enabled:</p> <ul style="list-style-type: none"> • Verify option I set to automatically scan e-mails. • Verify option is set to automatically scan downloads. • Verify option is set to run scan automatically. • Verify option is set to remove viruses automatically. • Verify option is set to automatically check for updates. • Full scans are scheduled to run daily.
Compliance	Pass / Fail
Test Nature	Objective

3.4.3 Data/Configuration Backup

Reference	<p>Microsoft Technet, http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/backuprest/br01.mspix</p>
------------------	--

Risk	<p>While backups do not prevent intrusions or provide any other first line defense mechanism, it is essential to have a good data and configuration backup policy. As I stated above, if a hacker, malware, or a virus was to bypass the other security measures in place and enter the system, they could alter or delete system critical files, data, or other software. This would be disastrous if backups of this information were not made on a regular basis.</p> <p>Another catastrophe that backups guard against is the physical threats. This includes, but is not limited to, the physical destruction of storage media by people, natural disasters, and hard disk failure.</p> <p>Microsoft Windows 2000 provides a backup utility that can be easily implemented. This is not the only way to automate backups, but I have been informed that this is the method used on this server. This checklist assumes this information to be correct and outlines the procedures to check the settings in Microsoft's backup utility.</p> <ul style="list-style-type: none">• The loss or alteration of data• Loss of Availability
-------------	---

© SANS Institute 2000 - 2005

Testing Criteria / Compliance Criteria	<p>Manually inspect the backup policy. Verify that the following items are explicitly defined:</p> <ul style="list-style-type: none"> • Backup Procedure • Backup Schedule <ul style="list-style-type: none"> ○ Full Backup Schedule ○ Incremental Backup Schedule • Restoration Procedure • Backup Media Storage • List of Critical Files to be Backed Up <p>Inspect the configuration of the Microsoft backup utility:</p> <ul style="list-style-type: none"> • Start the utility under “Start” -> “Programs” -> “Accessories” -> “System Tools” -> “Backup” • Select the “Scheduled Jobs” tab • Double click each job, select the “Backup details” tab, and verify the following: <ul style="list-style-type: none"> ○ Are all files listed in the list of critical files to be backed up listed with the correct schedule? ○ Is “Verify Data” selected?
Compliance	Pass / Fail
Test Nature	Objective and Subjective

© SANS INSTITUTE

4 Audit Results

4.1 Physical Security

Evidence:

Are doors locked? YES

Are proper access controls in place? NO

Is an alarm system in place? YES

Is a usable fire extinguisher available? YES

Are proper smoke detectors in place? YES

Are the air temperature and humidity controlled? YES

Is a power backup in place? YES

Are the output devices protected from eavesdroppers at windows, etc? NO

Findings and Items to be addressed:

Lack of an access log and insufficient surveillance can lead to unauthorized access by someone who is able to gain access to the facility and the security code. Also, the computer monitors were found to be facing the door, which has a small window in it. Since no video surveillance or security guard was present, this can lead to an eavesdropper gathering information by peering through the window.

4.2 Server Hardening

4.2.1 Account Policy

Evidence:

Enforce password history: 8

Maximum password age: 42 days

Minimum password age: 7 days

Minimum password length: 8 characters

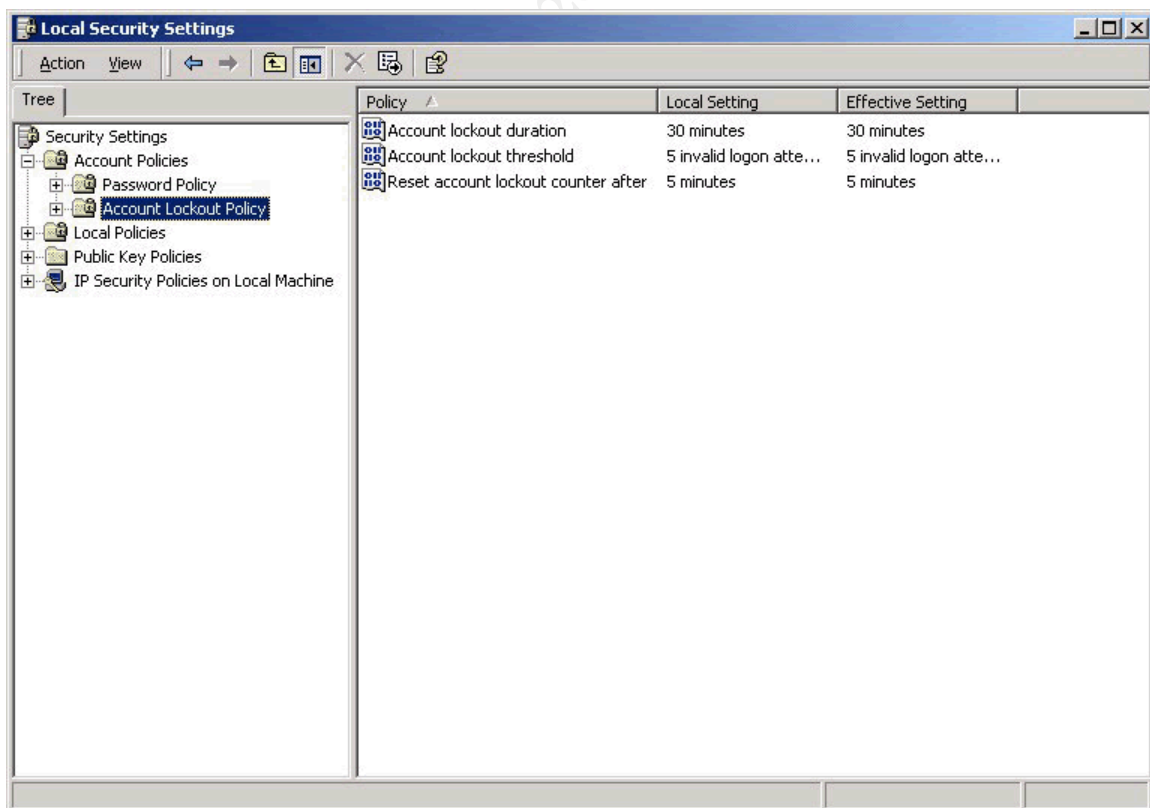
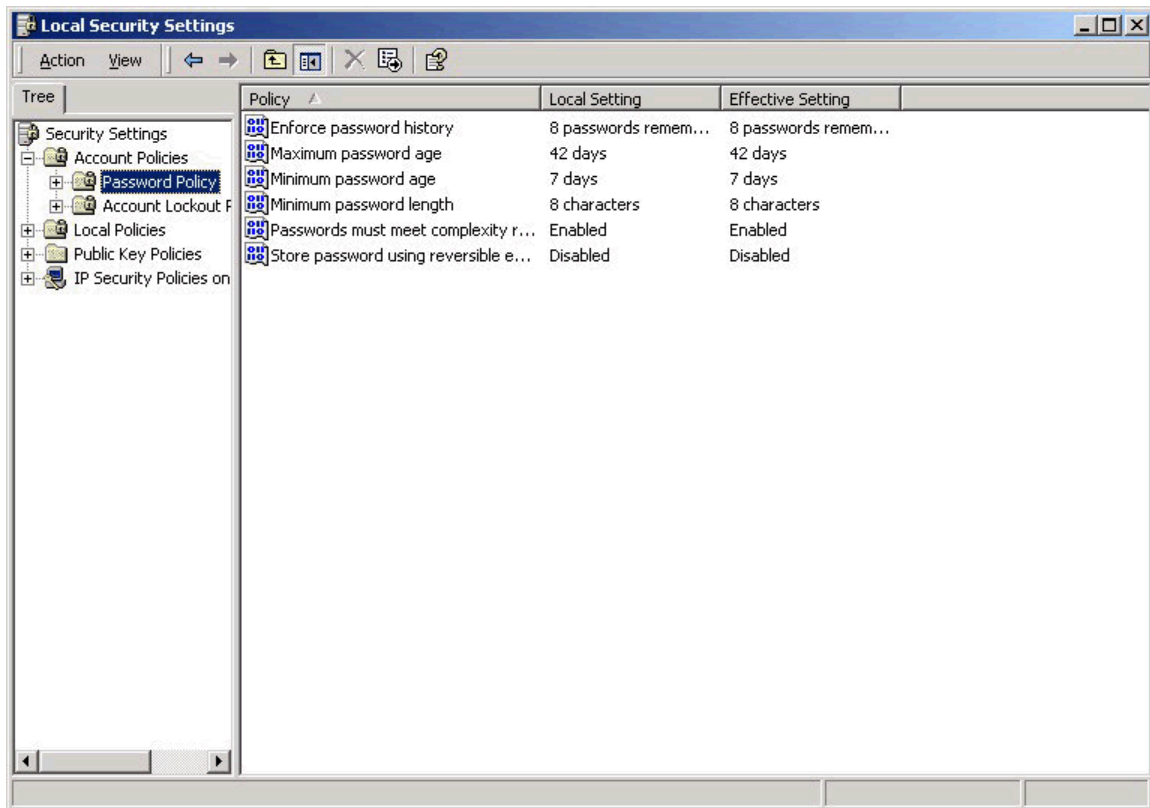
Passwords must meet complexity requirements: Enabled

Store password using reversible encryption for all users in the domain: Disabled

Account lockout duration: 30 Minutes

Account lockout threshold: 5

Reset account lockout counter after: 5 minutes



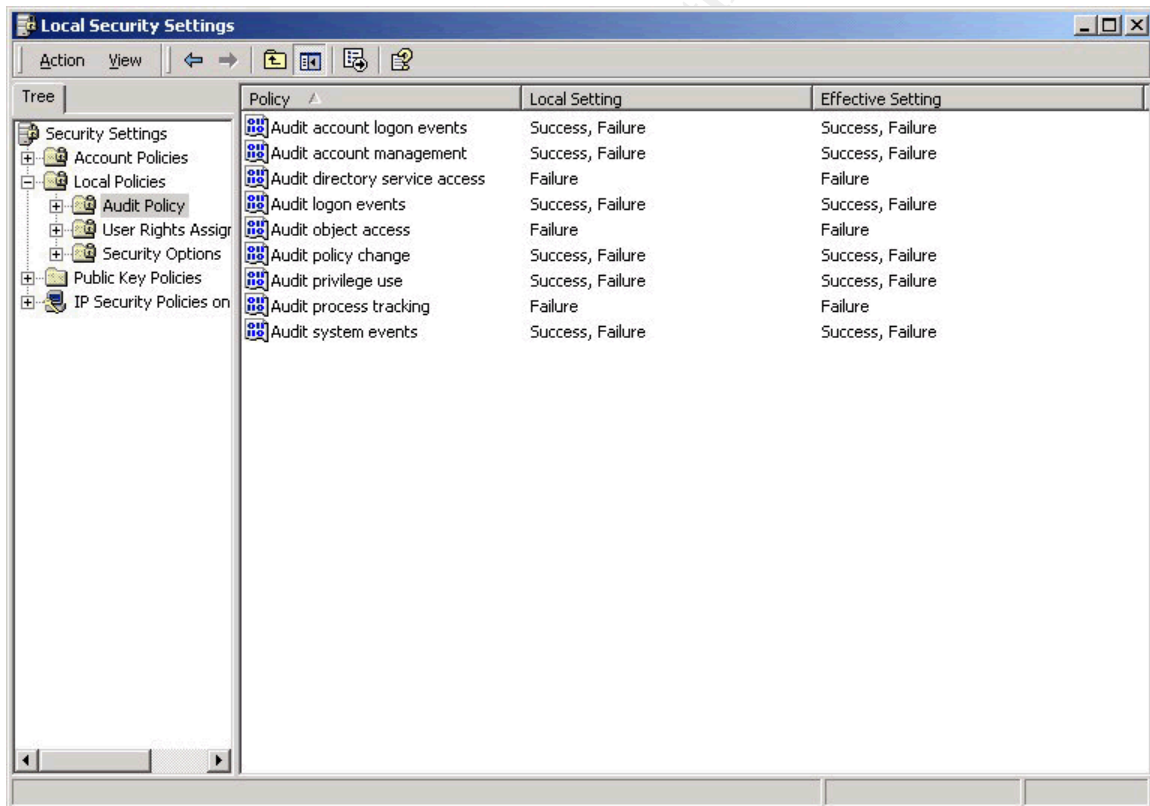
Findings & Items to be addressed:

The password policy is setup with the proper restrictions enabled, but the account lockout features failed to meet the minimum expected values. As stated above, these settings should be increased in order to prevent someone from trying to guess the password by brute force.

4.2.2 Audit Policy

Evidence:

Audit account logon events: success, failure
Audit account management: success, failure
Audit logon events: success, failure
Audit policy change: success, failure
Audit system events: success, failure



Findings & Items to be addressed:

All settings were met as expected and set to the proper configuration.

4.2.3 User Rights

Evidence:

Act as part of the operating system: None
Access this computer from the network: None
Backup files and directories: Administrators, Backup Operators
Change the system time: Administrators, Power Users
Create a token object: None
Debug programs: Administrators
Deny access to this computer from the network: Everyone
Force Shutdown from a remote system: None
Increase scheduling priority: Administrators
Load and unload device drivers: Administrators
Manage auditing and security log: Administrators
Modify firmware environment variables: Administrators
Profile single processes: Administrators, Power Users
Profile system performance: Administrators
Replace a process level token: None
Restore files and directories: Administrators, Backup Operators
Shut down the system: Administrators, Power Users, Users

Note: I have not included a screen shot of these settings due to the sensitivity of many of the settings.

Findings & Items to be addressed:

This biggest issue for the user rights is the values set for shutting down the system. The addition of power users and users to this list create the opportunity for anyone on the server to accidentally cause a denial of service by shutting down the system. Also, this allows for any hacker or Trojan that has gained access to the system to also cause a denial of service by shutting down the system. This setting should be set to administrators only in order to reduce these risks. As for the other four settings that have additional settings beyond what is recommended, I view these as lesser threats due to the fact that the power users and backup operators are very restricted groups as to the number of users in these groups. The backup operators only contains two users, which I was informed are operators who actually do backup the system. The power users is a group that I feel could be removed, though. There are four users in this group, but these users also belong to the administrators group. Therefore, I believe this group is not needed and should be removed.

4.2.4 Security Options

Evidence:

Additional restrictions for anonymous connections: No access without explicit

anonymous permissions

Allow system to be shut down without having to log on: Disabled

Audit use of backup and restore privilege: **Disabled**

Clear virtual memory pagefile when system shuts down: Enabled

Digitally sign client communication (always): **Disabled**

Digitally sign server communication (always): **Disabled**

Disable CTRL+ALT+DEL requirement for logon: Disabled

Do not display last user name in logon screen: Enabled

LAN manager authentication level: **Send LM & NTLM Responses**

Number of previous logons to cache (in case domain controller is not available):

0

Prevent users from installing printer drivers: Enabled

Recovery console: allow automatic administrative logon: Disabled

Rename administrator account: **Not Defined**

Restrict CD-ROM access to locally logged-on user only: **Disabled**

Restrict floppy access to locally logged-on user only: **Disabled**

Secure channel: digitally encrypt or sign secure channel data (Always): Enabled

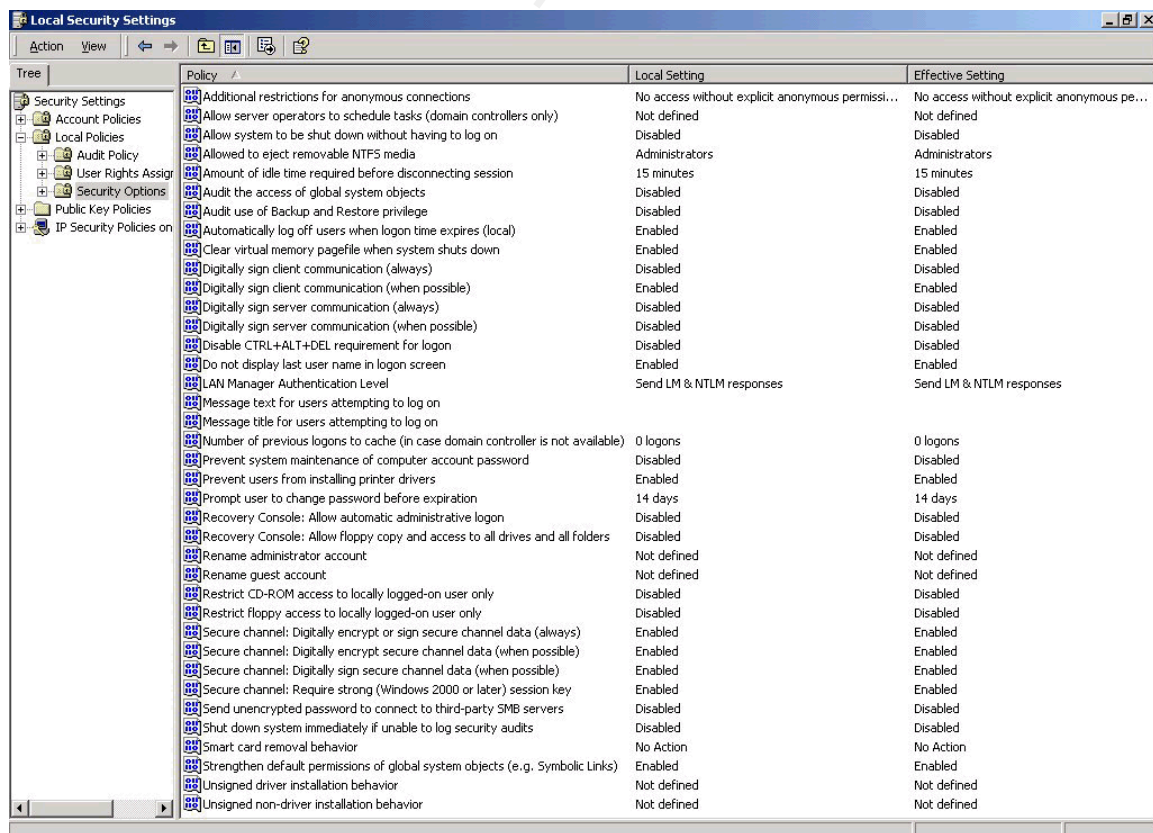
Secure channel: require strong (Windows 2000 or later) session key: Enabled

Send unencrypted password to connect to third-party SMB servers: Disabled

Strengthen default permissions of global system objects (e.g. Symbolic Links):
Enabled

Unsigned driver installation behavior: **Not Defined**

Unsigned non-driver installation behavior: **Not Defined**



Tree	Policy	Local Setting	Effective Setting
Security Settings	Additional restrictions for anonymous connections	No access without explicit anonymous permissi...	No access without explicit anonymous pe...
Account Policies	Allow server operators to schedule tasks (domain controllers only)	Not defined	Not defined
Local Policies	Allow system to be shut down without having to log on	Disabled	Disabled
Audit Policy	Allowed to eject removable NTFS media	Administrators	Administrators
User Rights Assign...	Amount of idle time required before disconnecting session	15 minutes	15 minutes
Security Options	Audit the access of global system objects	Disabled	Disabled
Public Key Policies	Audit use of Backup and Restore privilege	Disabled	Disabled
IP Security Policies on	Automatically log off users when logon time expires (local)	Enabled	Enabled
	Clear virtual memory pagefile when system shuts down	Enabled	Enabled
	Digitally sign client communication (always)	Disabled	Disabled
	Digitally sign client communication (when possible)	Enabled	Enabled
	Digitally sign server communication (always)	Disabled	Disabled
	Digitally sign server communication (when possible)	Disabled	Disabled
	Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
	Do not display last user name in logon screen	Enabled	Enabled
	LAN Manager Authentication Level	Send LM & NTLM responses	Send LM & NTLM responses
	Message text for users attempting to log on		
	Message title for users attempting to log on		
	Number of previous logons to cache (in case domain controller is not available)	0 logons	0 logons
	Prevent system maintenance of computer account password	Disabled	Disabled
	Prevent users from installing printer drivers	Enabled	Enabled
	Prompt user to change password before expiration	14 days	14 days
	Recovery Console: Allow automatic administrative logon	Disabled	Disabled
	Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled
	Rename administrator account	Not defined	Not defined
	Rename guest account	Not defined	Not defined
	Restrict CD-ROM access to locally logged-on user only	Disabled	Disabled
	Restrict floppy access to locally logged-on user only	Disabled	Disabled
	Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled	Enabled
	Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Enabled
	Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled
	Secure channel: Require strong (Windows 2000 or later) session key	Enabled	Enabled
	Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled
	Shut down system immediately if unable to log security audits	Disabled	Disabled
	Smart card removal behavior	No Action	No Action
	Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Enabled
	Unsigned driver installation behavior	Not defined	Not defined
	Unsigned non-driver installation behavior	Not defined	Not defined

Findings & Items to be addressed:

The following is a list of security options that were found to not match the security checklist created above, along with a description of the reasoning behind the recommended settings:

- Audit use of backup and restore privilege – By setting this to “Enable” it is ensured that a valid audit trail of all backup and restore user rights is created. This ensures that in the case that something goes wrong, it is possible to pinpoint the area of failure.
- Digitally sign client communication (always) and Digitally sign server communication (always). This ensures that the system will always digitally sign communication. This helps to prevent client and server spoofing, which is a way for unauthorized systems to intercept data that traverses the network.
- LAN manager authentication level – It has been proven that the Microsoft LanManger and NT LanManger version 1 hashing algorithms are weak. A password cracker easily breaks most passwords stored and transmitted in this manner. By allowing only NT LanManger version 2, passwords are more secure and it is less likely that an account can be hijacked.
- Rename administrator account – Many attacks on a Windows system try to find holes in the system that allows them to gain “Administrator” access. By renaming the administrator account to something other than “Administrator,” many of these attacks can be spoiled.
- Restrict Floppy and CD-ROM access to locally logged-on user only – By setting this to “Enabled,” anyone that is able to gain access to the system will not be able to access anything on the CD-ROM or floppy drive.
- Unsigned driver installation behavior and Unsigned non-driver installation behavior – By setting these security options to “Do Not Allow”, you are guaranteed that all drivers and software installed on the system are digitally signed and come from the original manufacturer. This prevents software that has been tampered with or infected from being introduced to the system.

4.2.5 Unneeded Services

Evidence:

The following is the output from the services utility (reformatted for clarity).

Name	Description	Status	Startup Type	Log On As
Alerter	Notifies selected users and computers of administrative alerts.	Started	Automatic	LocalSystem

Application Management	Provides software installation services such as Assign, Publish, and Remove.		Manual	LocalSystem
ASP.NET State Service	Provides support for out-of-process session states for ASP.NET. If this service is stopped, out-of-process requests will not be processed. If this service is disabled, any services that explicitly depend on it will fail to start.		Manual	LocalSystem
Automatic Updates	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.	Started	Automatic	LocalSystem
Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is disabled, then any functions that depend on BITS, such as Windows Update or MSN Explorer will be unable to automatically download programs and other information.		Manual	LocalSystem
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.		Manual	LocalSystem
COM+ Event System	Provides automatic distribution of events to subscribing COM components.	Started	Manual	LocalSystem
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	Started	Automatic	LocalSystem
DefWatch		Started	Automatic	LocalSystem
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Started	Automatic	LocalSystem
Distributed File System	Manages logical volumes distributed across a local or wide area network.	Started	Automatic	LocalSystem
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Started	Automatic	LocalSystem
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.		Manual	LocalSystem
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.	Started	Automatic	LocalSystem
DNS Client	Resolves and caches Domain Name System (DNS) names.	Started	Automatic	LocalSystem

Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.	Started	Automatic	LocalSystem
Fax Service	Helps you send and receive faxes		Disabled	LocalSystem
File Replication	Maintains file synchronization of file directory contents among multiple servers.		Manual	LocalSystem
IIS Admin Service	Allows administration of Web and FTP services through the Internet Information Services snap-in.	Started	Automatic	LocalSystem
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.		Manual	LocalSystem
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.		Disabled	LocalSystem
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.		Disabled	LocalSystem
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	Started	Automatic	LocalSystem
Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.		Disabled	LocalSystem
License Logging Service		Started	Automatic	LocalSystem
Logical Disk Manager	Logical Disk Manager Watchdog Service	Started	Automatic	LocalSystem
Logical Disk Manager Administrative Service	Administrative service for disk management requests		Manual	LocalSystem
Messenger	Sends and receives messages transmitted by administrators or by the Alert service.	Started	Automatic	LocalSystem
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.		Manual	LocalSystem
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.		Manual	LocalSystem

Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.	Started	Manual	LocalSystem
Network DDE	Provides network transport and security for dynamic data exchange (DDE).		Manual	LocalSystem
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE		Manual	LocalSystem
Norton AntiVirus Client		Started	Automatic	LocalSystem
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.		Manual	LocalSystem
Performance Logs and Alerts	Configures performance logs and alerts.		Manual	LocalSystem
Plug and Play	Manages device installation and configuration and notifies programs of device changes.	Started	Automatic	LocalSystem
Print Spooler	Loads files to memory for later printing.	Started	Automatic	LocalSystem
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.	Started	Automatic	LocalSystem
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.		Manual	LocalSystem
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.		Manual	LocalSystem
Remote Access Connection Manager	Creates a network connection.	Started	Manual	LocalSystem
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	Started	Automatic	LocalSystem
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.		Manual	LocalSystem
Remote Registry Service	Allows remote registry manipulation.		Disabled	LocalSystem
Removable Storage	Manages removable media, drives, and libraries.	Started	Automatic	LocalSystem

Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.		Disabled	LocalSystem
RunAs Service	Enables starting processes under alternate credentials		Disabled	LocalSystem
Security Accounts Manager	Stores security information for local user accounts.	Started	Automatic	LocalSystem
Server	Provides RPC support and file, print, and named pipe sharing.	Started	Automatic	LocalSystem
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.		Manual	LocalSystem
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.		Manual	LocalSystem
System Event Notification	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.	Started	Automatic	LocalSystem
Task Scheduler	Enables a program to run at a designated time.	Started	Automatic	LocalSystem
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.	Started	Automatic	LocalSystem
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service.	Started	Manual	LocalSystem
Telnet	Allows a remote user to log on to the system and run console programs using the command line.		Disabled	LocalSystem
Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.		Disabled	LocalSystem
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.		Manual	LocalSystem
Utility Manager	Starts and configures accessibility tools from one window		Disabled	LocalSystem
Windows Installer	Installs, repairs and removes software according to instructions contained in .MSI files.		Manual	LocalSystem

Windows Management Instrumentation	Provides system management information.	Started	Automatic	LocalSystem
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.	Started	Manual	LocalSystem
Windows Time	Sets the computer clock.		Manual	LocalSystem
Wireless Configuration	Provides authenticated network access control using IEEE 802.1x for wired and wireless Ethernet networks.		Manual	LocalSystem
Workstation	Provides network connections and communications.	Started	Automatic	LocalSystem
World Wide Web Publishing Service	Provides Web connectivity and administration through the Internet Information Services snap-in.	Started	Automatic	LocalSystem

Findings & Items to be addressed:

There are currently 67 services installed on this system. Below is a subset of these systems, which are not required by most configurations that are either started, in the automatic configuration or in the manual configuration. The system administrator must determine whether or not these services are required by the system. It is highly recommended that these services be disabled first and tested thoroughly before being completely removed from the system.

- Alerter
- ClipBook
- Computer Browser
- DHCP Client
- Distributed File System
- Distributed Link Tracking Client
- Distributed Link Tracking Server
- Distributed Transaction Coordinator
- File Replication
- Indexing Service
- Logical Disk Manager
- Logical Disk Manager Administrative Service
- Messenger
- Net Logon
- NetMeeting Remote Desktop Sharing
- Network DDE

- Network DDE SDSM
- NT LM Security Support Provider
- Performance Logs and Alerts
- Print Spooler
- QoS RSVP
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Procedure Call (RPC) Locator
- Smart Card
- Smart Card Helper
- TCP/IP NetBIOS Helper Service
- Telephony
- Uninterruptible Power Supply
- Windows Time
- Wireless Configuration

4.2.6 Removal of Unneeded Windows Components

Evidence:

The following Windows components were installed on this system:

IIS Common Files
 IIS World Wide Web Server
 Calculator
 WordPad
 IIS Snap-In

Findings & Items to be addressed:

The only two components that were installed on the system that are not included in the recommendations checklist are calculator and WordPad. There are no significant security issues with either of these components, so no action is recommended.

4.2.7 Scan for Vulnerabilities

Evidence:

A full report from the Nessus scan is listed in Appendix A

Findings & Items to be addressed:

The main finding from this report is the default shares still exist on this system.

The shares should be removed. There are many vulnerabilities, as stated in the Nessus report, which can be taken advantage of by hackers and malware. These services should be disabled in order to eliminate this vulnerability.

Other findings that should be addressed according to the Nessus report are:

- An old version of flash player is installed. Flash should actually not exist on this system. No web browsing that requires flash should ever be necessary from here.
- The HKLM\Software\Microsoft\Windows\CurrentVersion\Run key should be more restrictive.
- Microsoft Office should be upgraded to a more secure version.

4.3 IIS Hardening

4.3.1 Removal of Default Installation Directories

Evidence:

- C:\winnt\system32\inetrv\iisadmin – **Exists**
- C:\winnt\system32\inetrv\iisadmpwd – **Exists**
- inetpub\wwwroot (or \ftproot or \smtproot) – Removed
- inetpub\scripts – Removed
- inetpub\iissamples – Removed
- inetpub\adminscripts – Removed
- C:\winnt\help\iishelp\iis – **Exists**
- C:\winnt\web\printers – Removed
- C:\program files\common files\system\msadc – **Exists**

Findings & Items to be addressed:

The above directories that are shown to exist should be removed. Many attacks exist that take advantage of these directories being there. By removing them, the risk is reduced that a virus, malware, or a hacker will be able to exploit known vulnerabilities in these files.

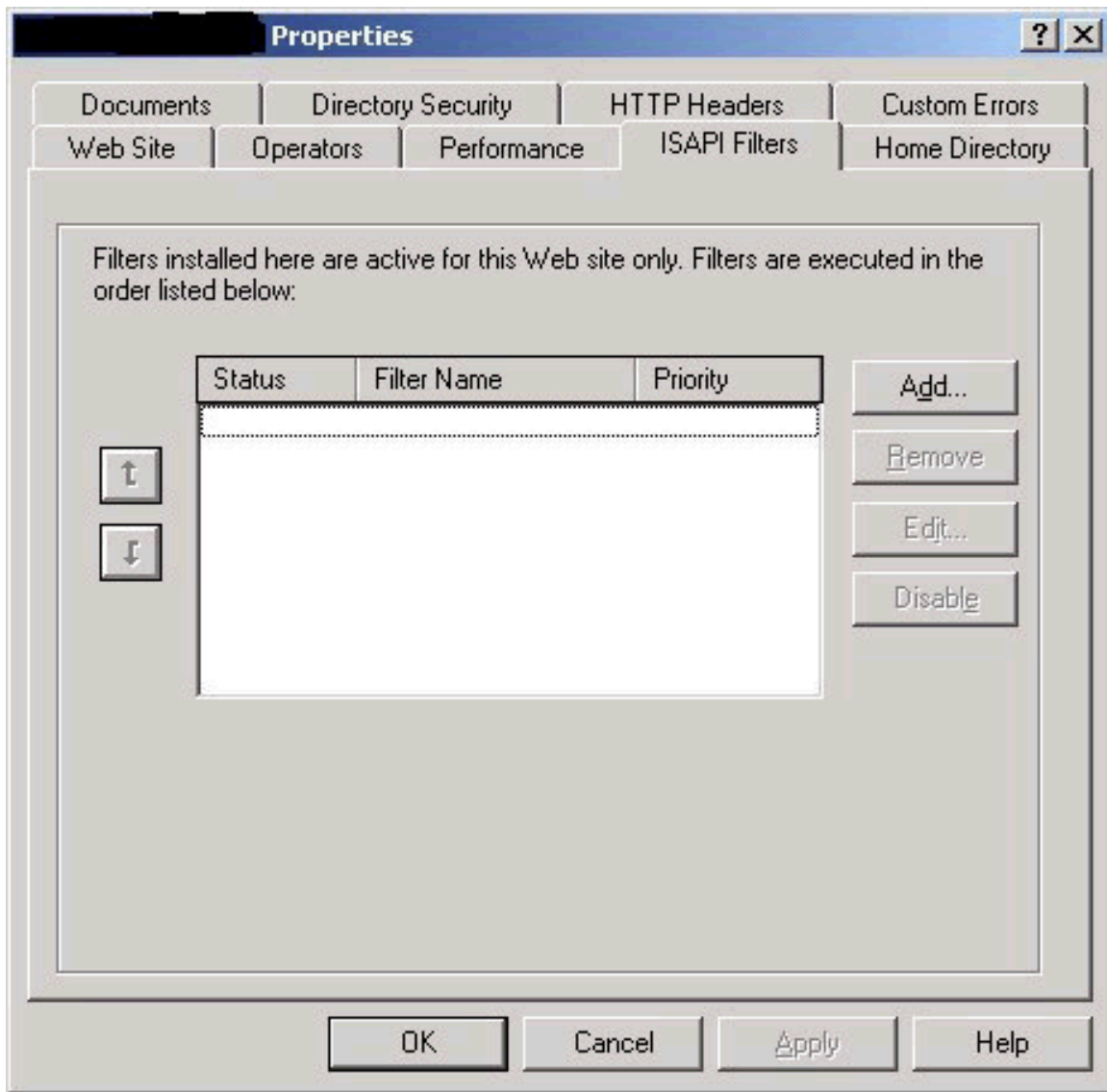
4.3.2 Removal of Unnecessary ISAPI Filters

Evidence:

ISAPI Filters:

- FrontPage – Removed
- Digest Authentication – Removed
- HTTP Authentication – Removed
- SSL – Removed

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute

Files associated with the filters:

- FrontPage: fpexdll.dll – Removed
- Digest: md5filt.dll – **Exists**
- Compression: compfilt.dll – **Exists**
- SSL: sspifilt.dll – **Exists**

Findings & Items to be addressed:

All of the above ISAPI filters were found to be removed from the Internet Services Manager, but not all of the files associated with these filters have been removed from the system. These files should be removed to ensure that exploits that exist in these filters are not taken advantage of. Since the filters are not being used it is not necessary to have these files.

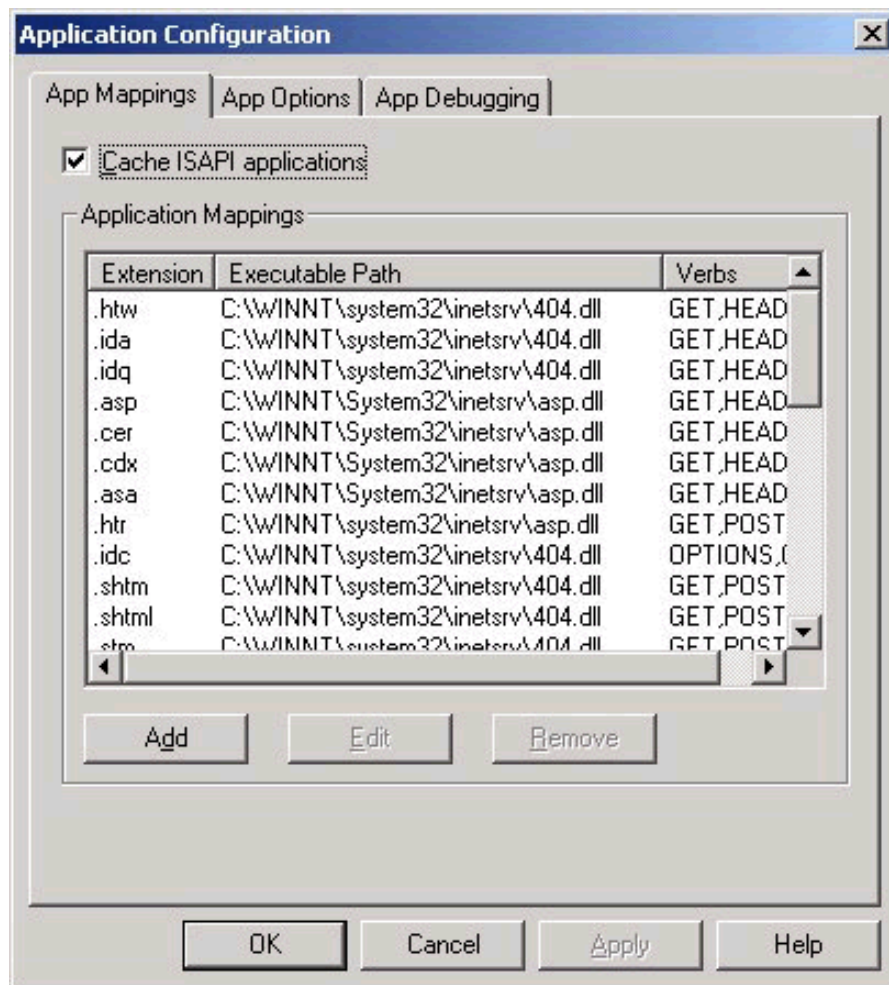
4.3.3 Removal of Unnecessary Extensions

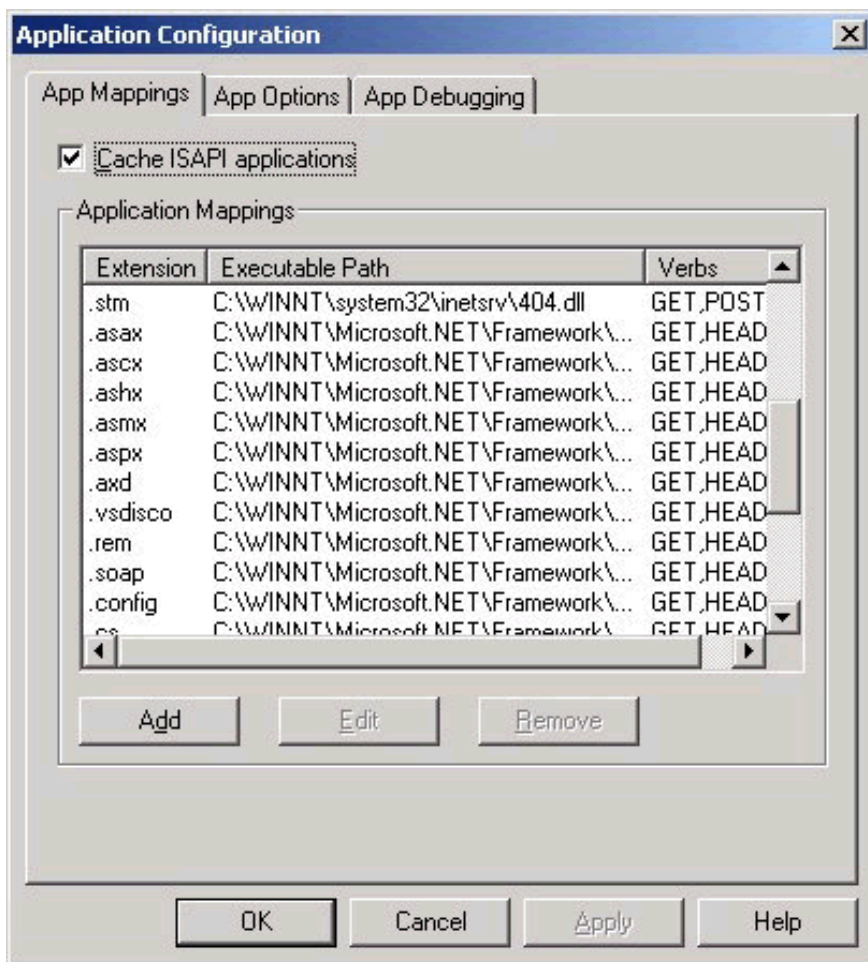
Evidence:

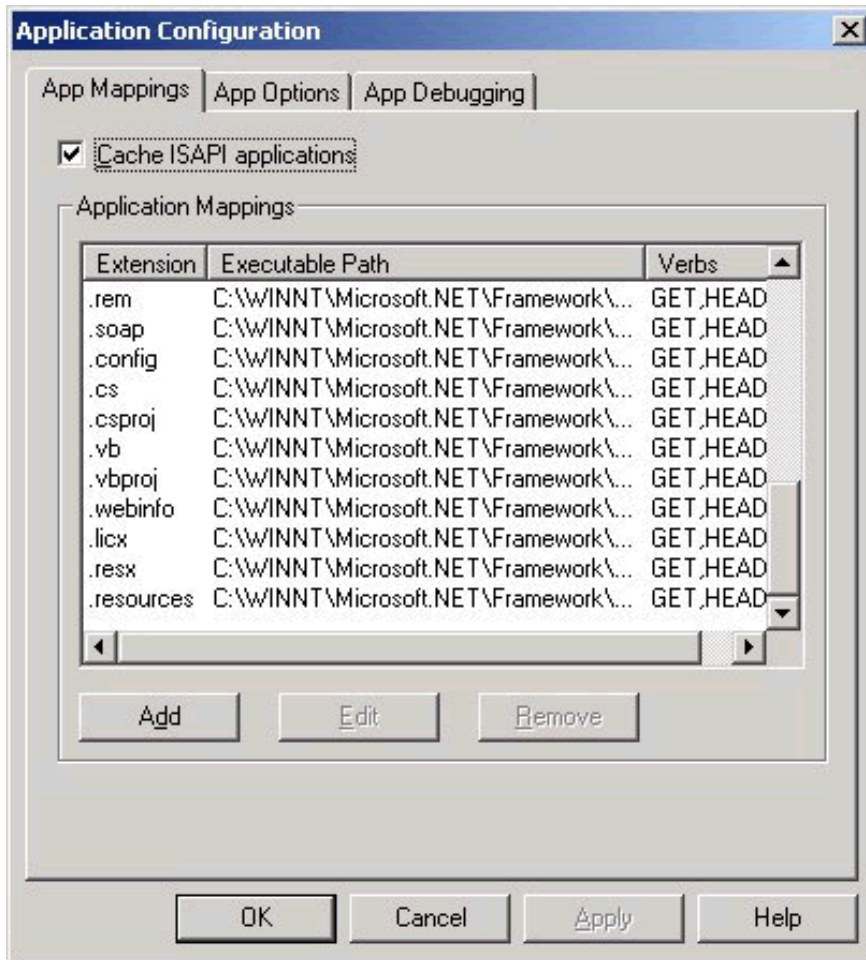
The following extensions were recognized by IIS on this system:

- .htw
- .ida
- .idq
- .asp
- .cer
- .cdx
- .asa
- .htr
- .idc
- .shtm
- .shtml
- .stm
- .asax
- .ascx
- .ashx
- .asmx
- .aspx
- .axd
- .vsdisco
- .rem
- .soap

- .config
- .cs
- .csproj
- .vb
- .vbproj
- .webinfo
- .licx
- .resx
- .resources







Files with the following extensions were found to be used on the system:

- .asp
- .asa

Findings & Items to be addressed:

All but the .asp and .asa file extensions are not being utilized on this system and, therefore, should be removed from IIS. This prevents any code that is introduced on the system with these extensions from being executed, causing damage or unauthorized access to the system.

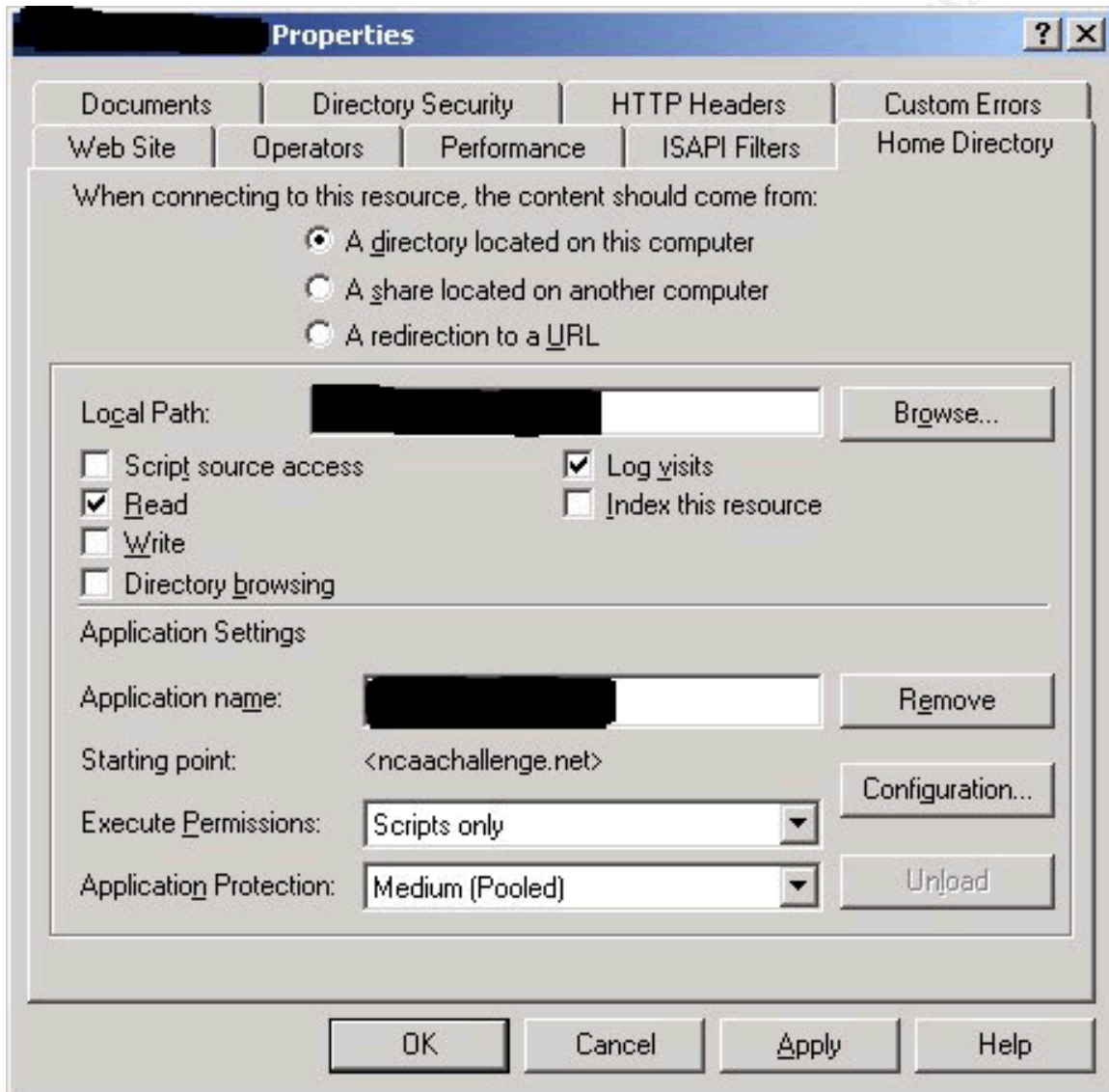
4.3.4 File ACL's

Evidence:

The following settings were set in the Internet Services Manager:

- Script Source Access – off

- Read – on
- Write – off
- Directory Browsing – off
- Index this Resource – off
- Log Visits – on
- Enable Parent Paths - off



The following ACL's exist on the system:

- IIS Logs – System and Administrators Full Control
- Web Root – Everyone Read Only
- C:\winnt – Everyone None, Users – Read and Execute
- C:\winnt\system32 – Everyone Read Only
- C:\winnt\system32\inetssrv – Everyone Read Only

- C:\winnt\system32\inet\asp – Does not exist
- C:\winnt\program files\common files\ - Everyone None

Findings & Items to be addressed:

All of the ACL's were found to be in accordance with the checklist.

4.4 Maintenance Procedures

4.4.1 Patch Level/Policy

Evidence:

Upon inspection of the administrator's patching policy, it was found that patches are downloaded and tested on a separate system with a similar configuration on a weekly basis. Upon successful testing, the patches are then installed on the production system. Patches and hotfixes that were installed on the operating system are then logged in a page in this document.

The output for the IIS Hotfix Checking Tools:

Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

```
-----
| HFCHECK Hotfix Check Script 1.00          |
| Thomas Deml (thomad@microsoft.com)       |
-----
```

No missing Hotfix found.

The output for the qfecheck Windows Hotfix Checking Tool:

Windows 2000 Hotfix Validation Report for \\XXXXX
Report Date: 3/5/2005 4:28pm

Current Service Pack Level: Service Pack 4

Hotfixes Identified:

Q282784: Current on system.
Q327194: Current on system.
KB329115: Current on system.
KB823182: Current on system.
KB823559: Current on system.
KB824105: Current on system.
KB824141: Current on system.
KB824146: Current on system.
KB824151: Current on system.
KB825119: Current on system.
KB826232: Current on system.
KB828028: Current on system.
KB828035: Current on system.
KB828741: Current on system.
KB828749: Current on system.
KB835732: Current on system.
KB837001: Current on system.
KB839643: Current on system.
KB839645: Current on system.
KB840315: Current on system.
KB840987: Current on system.
KB841356: Current on system.
KB841533: Current on system.
KB841872: Current on system.
KB841873: Current on system.
KB842526: Current on system.
KB871250: Current on system.
KB873333: Current on system.
KB885250: Current on system.
KB885834: Current on system.
KB885835: Current on system.
KB885836: Current on system.
KB888113: Current on system.
KB890047: Current on system.
KB890175: Current on system.
KB891711: Current on system.
KB891781: Current on system.

Note: I have been asked not to include a copy of any policies due to proprietary reasons.

Findings & Items to be addressed:

The policy does not explicitly define a way to back out the patches, though. Also, patches that do not pass the testing or that are backed out are not

recorded in the logs. A back out procedure should be defined in order to create a better process for removing patches that are found to cause problems on the system. As for missing hotfixes, none were currently found to not be installed.

4.4.2 Anti-Virus

Evidence:

Norton Anti-Virus Corporate Edition is installed on this server.

- Full scans are scheduled to run weekly.
- Norton is set to automatically scan all new and modified files on the system.
- It first will attempt to repair any infected file, and then quarantine it.
- It is configured to check for updated virus definitions on a weekly basis and download and install them automatically.

Findings & Items to be addressed:

All of the items in the checklist are configured correctly with the sole exception of the full scan section. This should be set to scan the entire system on a daily basis instead of a weekly basis in order to ensure that viruses are detected as soon as possible.

4.4.3 Data/Configuration Backup

Evidence:

Upon inspection of the administrator's backup policy, I have found the following information:

- All pages hosted by IIS are backed up on a weekly basis.
- The database is backed up nightly.
- These backups are done by Microsoft's backup utility.
- Backups are sent via ftp to a backend workstation, which are then burned to CD.
- Restoration is also done via Microsoft's backup utility.

Note: I have been asked not to include a copy of any policies due to proprietary reasons.

Inspection of Microsoft's backup utility's configuration show compliance with these procedures.

Findings & Items to be addressed:

Although all of the web pages and data related to the web pages are backed up on a regular interval, there is no backup of the entire system. This should be done in order to ensure a proper restore of the entire system in the event that it is compromised or configuration information is lost. I also found that the backup media (CD's) is stored in the same facility as the server. This media should be stored in a secure off-site facility. In the event of a natural disaster, this would prevent the loss of all data and its backups.

© SANS Institute 2000 - 2005, Author retains full rights.

5 Audit Report

5.1 Executive Summary

XYZ, Inc. has requested that a security audit be performed by an external entity on the Dell PowerEdge 600SC acting as a web server to provide services to their customers. This report has been prepared in order to convey the findings of this audit. The assessment here provides the measures which have already been taken in order to meet the industry's best practices as well as recommendations for meeting the standard that have not been met. The risks to this system have been taken into account in quantifying the severity of these findings.

5.2 Audit Findings and Recommendations

5.2.1 Positive Findings:

Note: These findings were overall positive, but some may have comments that need to be corrected by the system administrator.

Physical Security

Risk: Low

The facility housing the system has relatively good security. Many controls were found to be in place including a proper alarm system, adequate environment controls, and a power backup system.

Two areas that could be improved upon include proper access controls and protection from eavesdroppers. Both door locks and a security pad device were in place to facilitate access control, but I would recommend a monitoring system to help monitor those who access the server room. This could be a security guard manning the door or a surveillance system. Both require a significant investment in manpower. In order to keep someone from viewing information that is displayed on the screen while someone is working, I would recommend tilting the monitors away from the door, which has a small window in it. This would require almost no investment to correct.

Account Policy

Risk: Low

The account policy on the system was found to be adequate, although a couple of changes could be made in order to enhance the security of the system. Strong passwords, meaning a minimum length and minimum complexity requirements, were found to be enforced on this system. Also, passwords are forced to be changed on a regular basis.

The two things that could be changed on the system both involve the account lockout policy of the system. This means that accounts are locked after a number of unsuccessful login attempts are made. To change this, there are simply two policies that can be changed on the system. This would take a very insignificant investment in manpower to change.

Audit Policy

Risk: Low

Proper auditing of a system enforces accountability to all users. In the event that a mishap occurs on the system, auditing creates a means of finding out what events occurred that lead up to the mishap. This system was found to be in 100% compliance of the minimum security recommendations for a Windows 2000 Server.

Removal of Unneeded Windows Components

Risk: Low

Windows components are applications that come with Windows 2000 that improve the functionality of a computer. Many of these applications come with their share of security flaws, though, so only those components that are required to meet the functionality requirements of a system should be installed. This is definitely the case with this system. Only two components were found to be installed on this system that are not explicitly required to maintain its functionality. Both of these facilitate the maintenance of the computer and do not pose any serious security threats. I recommend that no action be taken here.

Removal of Unnecessary IIS ISAPI Filters

Risk: Low

ISAPI filters are libraries that can enhance the functionality of an IIS server. Some of these filters, such as the SSL ISAPI, can be beneficial to the security of a system if properly utilized, but, when they are not being used, they should be removed. ISAPI's are known to contain various security flaws, which can allow an attacker to cause a denial of service or even gain access to a system. One

well known example of this is the Code Red virus, which uses a known vulnerability in ISAPI's in order to gain access to a system.⁶

During the security assessment of this system it was found that all ISAPI filters have been removed from IIS. Going a step further, though, I found that some of the library files that provide the functionality of the ISAPI still existed on the system. Although, some security precautions have been taken to protect against vulnerabilities in ISAPI filters, these files should also be removed to ensure the security of this system. The removal of these filters only requires a minimal investment in manpower.

IIS File ACL's Security

Risk: Low

IIS uses its own file access control lists in order to determine what actions can be taken by a web user. Correct configuration of these ACL's prevents users from writing to directories, viewing source code, and viewing directory content, among other things. During this audit, I found that all of the ACL's were correctly set to industry best known practice, so no action is required.

Patch Level and Policy

Risk: Low

In assessing the patching policy, I took into consideration two factors. First, I looked at the current patch level of the system. I did this by using two tools provided by Microsoft, a Windows Hotfix checking tool and an IIS Hotfix checking tool, that check the current patches on a system against a database kept by them of all available patches. Then I looked at the actual written administrator's patch policy to determine if sufficient means were spelled out to apply patches and remove them if necessary.

I found that all known patches for this system have been applied while running the Hotfix checking tools. Inspection of the patching policy revealed adequate procedures for applying and tracking patches, but it did not provide means to remove patches that are found to cause problems on the system. This should be resolved, which would take a small amount of manpower.

Anti-Virus Policy

Risk: Low

Just as a desktop computer should be protected by anti-virus software, a web server should be protected in the same fashion. Proper configuration of the

⁶ CIADA Analysis of Code Red, <http://www.caida.org/analysis/security/code-red/>.

software will help prevent the introduction of malicious software to the system. I found Norton Anti-Virus to be installed on this server, and it was configured to meet industry best practices in all but one area. The software only scanned the full system on a weekly basis, but it is recommended that it be scanned on a daily basis. Changing the configuration to comply with this would only require an insignificant amount of manpower to correct.

5.2.2 Negative Findings:

Presence of Unused IIS Extensions

Risk: Medium

Microsoft IIS can be configured to only execute code with a known file extension. For every file extension listed in IIS, there is an interpreter that will execute that type of code. There exist known vulnerabilities where these file extensions can be used to gain access to the system by executing arbitrary code and by other means. By default IIS is configured to execute many different file extensions.

During this vulnerability assessment, I found that all of the default file extensions were still recognized by IIS. These should be removed in order to prevent an attacker from taking advantage of this. It is a very simple and fast task that would cost very little for the company to implement.

User Rights

Risk: Medium

User Rights define which users can take what actions on a system. On this system it was found that any user could shut down the system. This allows anyone with an account to be able to ultimately cause a period of unplanned down time either by accident or on purpose by completely shutting down the server. This can cause a significant loss of revenue if the system is shut down at an inopportune time or for a long period of time. To correct this would take a minimal investment in man power to change only one system setting, which would restrict everyone but administrators from taking down the system.

A second finding while auditing the user rights was that the group Power Users exists on the system. This group serves no purpose because all users belonging to the Power Users group also belong in the Administrators group, which has the same, and more, rights. Removing this group would have minimal security effects, but also only takes a minimal amount of effort to correct.

Presence of Default IIS Directories

Risk: Medium

When IIS is installed on a Windows 2000 server, many default directories and scripts are installed as well. These scripts and directories provide administrative capabilities and provide examples for use during development. On a production system, such as this, these directories and sample scripts are typically not ever used. Hackers, malware, and robots often look for these directories to be installed and use the known exploits in them to gain access to the system.

During this audit, I searched for these default directories and scripts and found that some were removed, while others were not. I would recommend the removal of these directories in order to prevent such exploits as described above. This would require a very small amount of manpower in order to remove and would not cost any additional investment by the company.

Data and Configuration Backup

Risk: Medium

One of the most overlooked aspects of information security is proper data and configuration backup. In the event of a catastrophic incident, proper backups can save a company millions of dollars in saved effort and data. I have inspected both the administrator's backup policy as well as compliance with this policy. I found that only partial backups are being made on a regular basis. The actual data used by the web application and the application itself are backed up on a nightly basis, but full system backups are never made. In the event of a system restore, a full backup can save a large amount of time and reduce the amount of downtime required to get the system back in operation. I also found that the media used to create the backups is not stored properly. It should be stored in a secure facility away from operational system so that it will not be lost at the same time as the system. Correcting this will cost a significant amount of money to use a secure storage facility.

Security Options

Risk: High

Windows 2000 has some built-in security options that are easily set to improve the security of the system. Many of these security options were correctly set but others were not. Risks that this system are vulnerable to with the current security settings include data theft, unauthorized access, and the introduction of malicious code to the system. I would recommend changing these settings to match or exceed the recommendations outlined above. This would require a minimal investment of labor to correct.

Presence of Unneeded Services

Risk: High

Windows services are applications that provide various functionalities to a system. Most of these services run on the system at all times and are known to have various security flaws associated with them. Others are only run when invoked, but can also contain security flaws that facilitate a hacker's job. A default installation of Windows 2000 installs numerous services that are not required for a system such as this. Not only do these services create serious security issues, but they also eat up valuable resources.

These unneeded services can easily be disabled and removed from the system. It is not always easy to tell which services are actually being used, though. Before the services are removed, it must be fully tested to ensure that the server maintains its functionality without the services running. Because of this, it will take a moderate amount of labor to safely remove them, but to ensure the security of this server it is highly recommended that this be done.

Presence of Windows Shares

Risk: High

Nessus is a vulnerability scanner that has a database of known vulnerabilities it compares a system against. This tool is used by both hackers and security professionals alike. To help assess the security of the system, I performed a Nessus scan to find some additional vulnerabilities. One of the most alarming findings while running the Nessus scan was the presence of Windows shares. Windows shares are used to access the content of one server by another computer. It contains some of the most widely exploited holes in a Windows environment. They can be used to allow a hacker to gain access to a system, introduce malware to a system, and steal or modify data that exists on a system.

By default, Windows creates a share for each drive. These are not required for the functionality of an IIS server and should be removed. This would take a minimal investment in time to be removed and is highly recommended.

References

<http://www.sans.org/resources/glossary.php>, The SANS Institute, 2005.

Amaris, Chris, Mark Burnett, Chris Doyle, L. J. Locher. Windows 2000 Services, Pearson Education, Sams Publishing, 2005.

Anti-Virus Checklist, <http://viruses.surferbeware.com/antivirus-checklist.htm>, SurfersBeware.com, 2004.

The CIADA Web Site, CIADA Analysis of Code Red, <http://www.caida.org/analysis/security/code-red/>.

Glossary of Windows 2000 Services, http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2k_services.asp, Microsoft Corporation, 2005.

Heare, Sean. Data Center Physical Security Checklist, <http://sans.org/rr/whitepapers/awareness/416.php>, The SANS Institute, 2003.

Hoelzer, David. *Advanced System and Network Auditing*, The SANS Institute, 2004.

IIS Security Checklist, <http://windows.stanford.edu/docs/IISsecchecklist.htm>, Trustees of the Leland Stanford Junior University, 2001.

Information Security Awareness and Education, <http://www.security.umassp.edu/index.cfm?fuseaction=generic.506>, University of Massachusetts.

Microsoft MSDN, <http://msdn.microsoft.com>, Microsoft Corporation, 2005.

Microsoft Technet, <http://www.microsoft.com/technet/default.mspx>, Microsoft Corporation, 2005.

Vakharia, Sunil, Nessus Scanning on Windows Domain, http://www.nessus.org/documentation/nessus_domain_whitepaper.pdf, November 4th, 2005.

Windows 2000 Security Hardening Guide, Version 1.3, <http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en>, Microsoft Corporation, May 15, 2003.

Appendix A – Nessus Scan Results

Note: Some information has been changed or deleted for security reasons.

10330 Informational http (80/tcp) The following directories were discovered:
/admin, /help, /include

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Nessus ID : [11032](#) Informational http (80/tcp) The following directories were discovered:
/admin, /help, /include

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Nessus ID : [11032](#) Informational http (80/tcp) The remote web server type is :
Microsoft-IIS/5.0

Solution : You can use urlscan to change reported server for IIS.
Nessus ID : [10107](#) Informational http (80/tcp) The remote IIS server *seems* to be Microsoft IIS 5 - SP3 or SP4

Nessus ID : [11874](#) Informational http (80/tcp) The remote IIS server *seems* to be Microsoft IIS 5 - SP3 or SP4

Nessus ID : [11874](#) Warning msrpc (135/tcp)
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Solution : filter incoming traffic to this port.

Risk factor : Low

Nessus ID : [10736](#) Informational netbios-ssn (139/tcp) An SMB server is running on this port

Nessus ID : [11011](#) **Vulnerability** microsoft-ds (445/tcp) The following shares can be accessed as administrator :

- C\$ - (readable?, writeable)
- + Content of this share :
- XXXX

- ADMIN\$ - (readable?, writeable)
- D\$ - (readable?, writeable)
- + Content of this share :
- XXXX

Solution : To restrict their access under WindowsNT, open the explorer, do a right click on each, go to the 'sharing' tab, and click on 'permissions'

Risk factor : High

CVE : [CAN-1999-0519](#), [CAN-1999-0520](#)

BID : [8026](#)

Nessus ID : [10396](#) **Vulnerability** microsoft-ds (445/tcp)

The remote host has an old version of the Flash Player plugin installed.

An attacker may use this flaw to construct a malicious web site which with a badly formed flash animation which will cause a buffer overflow on this host, and allow him to execute arbitrary code with the privileges of the user running internet explorer.

Solution : Upgrade to version 6.0.79.0 or newer.

See also : <http://www.macromedia.com/v1/handlers/index.cfm?ID=23821>

Risk factor : High

BID : [7005](#)

Nessus ID : [11323](#) **Vulnerability** microsoft-ds (445/tcp)

The remote host is running a version of flash player older than 7.0.19.0.

This version can be abused in conjunction with several flaws in the web browser to read local files on this system.

To exploit this flaw, an attacker would need to lure a user of this system into visiting a rogue website containing a malicious flash applet.

Solution : Upgrade to version 7.0.19.0 or newer.

See also : http://www.macromedia.com/devnet/security/security_zone/mpsb03-08.html

Risk factor : High

Nessus ID : [11952](#) **Vulnerability** microsoft-ds (445/tcp) The following registry keys are writeable by users who are not in the admin group :

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

These keys contain the name of the program that shall be started when the computer starts. The users who have the right to modify them can easily make the admin run a trojan program which will give them admin privileges.

Solution : use regedt32 and set the permissions of this key to :

- Admin group : Full Control
- System : Full Control
- Everyone : Read

Make sure that 'Power Users' do not have any special privilege for this key.

Risk factor : High

CVE : [CAN-1999-0589](#)

Nessus ID : [10430](#) **Vulnerability** microsoft-ds (445/tcp)

The remote host is running a version of Microsoft Office which contains a flaw in its WordPerfect converter, which might allow an attacker to execute arbitrary code on the remote host.

To exploit this flaw, an attacker would need to send a specially crafted file to a user on the remote host and wait for him to open it using Microsoft Office.

When opening the malformed file, Microsoft Office will encounter a buffer overflow which may be exploited to execute arbitrary code.

Solution : <http://www.microsoft.com/technet/security/bulletin/ms04-027.msp>

Risk factor : High

CVE : [CAN-2004-0573](#)

BID : [11172](#)

Nessus ID : [14732](#) Warning microsoft-ds (445/tcp)

The remote version of Windows contains a flaw which may allow an attacker to cause it to disclose information over the use of a named pipe through a NULL session.

An attacker may exploit this flaw to gain more knowledge about the remote host.

Solution : <http://www.microsoft.com/technet/security/bulletin/MS05-007.msp>

Risk factor : Low

CVE : [CAN-2005-0051](#)

BID : [12486](#)

Nessus ID : [16337](#) Warning microsoft-ds (445/tcp)

The remote registry can be accessed remotely using the login / password

combination used for the SMB tests.

Having the registry accessible to the world is not a good thing as it gives extra knowledge to a hacker.

Solution : Apply service pack 3 if not done already, and set the key HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg to restrict what can be browsed by non administrators.

In addition to this, you should consider filtering incoming packets to this port.

Risk factor : Low

CVE : [CAN-1999-0562](#)

BID : [6830](#)

Nessus ID : [10400](#) Warning microsoft-ds (445/tcp) Here is the list of the SMB shares of this host :

IPC\$ - Remote IPC

D\$ - Default share

ADMIN\$ - Remote Admin

C\$ - Default share

This is potentially dangerous as this may help the attack of a potential hacker.

Solution : filter incoming traffic to this port

Risk factor : Medium

Nessus ID : [10395](#) Warning microsoft-ds (445/tcp) The host Security Identifier (SID) can be obtained remotely. Its value is :

XXXX : XXXXXXXXXXXX

An attacker can use it to obtain the list of the local users of this host

Solution : filter the ports 137-139 and 445

Risk factor : Low

CVE : [CVE-2000-1200](#)

BID : [959](#)

Nessus ID : [10859](#) Warning microsoft-ds (445/tcp) The host SID could be used to enumerate the names of the local users of this host.

(we only enumerated users name whose ID is between 1000 and 1200 for performance reasons)

This gives extra knowledge to an attacker, which

is not a good thing :

- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TslnternetUser (id 1000)
- IUSR_XXXX (id 1001)
- IWAM_XXXX (id 1002)
- Web Anonymous Users (id 1003)
- Web Applications (id 1004)
- ASPNET (id 1005)

Risk factor : Medium

Solution : filter incoming connections this port

Nessus ID : [10916](#) Warning microsoft-ds (445/tcp) There are 36 services running on this host :

Alerter [Alerter]

Application Management [AppMgmt]

Computer Browser [Browser]

DefWatch [DefWatch]

Distributed File System [Dfs]

DHCP Client [Dhcp]

Logical Disk Manager [dmserver]

DNS Client [Dnscache]

Event Log [Eventlog]

COM+ Event System [EventSystem]

IIS Admin Service [IISADMIN]

Server [lanmanserver]

Workstation [lanmanworkstation]

License Logging Service [LicenseService]

TCP/IP NetBIOS Helper Service [LmHosts]

Messenger [Messenger]

Distributed Transaction Coordinator [MSDTC]

Network Connections [Netman]

Norton AntiVirus Client [Norton AntiVirus Server]

Removable Storage [NtmsSvc]

Plug and Play [PlugPlay]

IPSEC Policy Agent [PolicyAgent]

Protected Storage [ProtectedStorage]

Remote Access Connection Manager [RasMan]

Remote Registry Service [RemoteRegistry]

Remote Procedure Call (RPC) [RpcSs]

Security Accounts Manager [SamSs]

Task Scheduler [Schedule]

System Event Notification [SENS]

Print Spooler [Spooler]

Telephony [TapiSrv]

Distributed Link Tracking Client [TrkWks]
World Wide Web Publishing Service [W3SVC]
Windows Management Instrumentation [WinMgmt]
Windows Management Instrumentation Driver Extensions [Wmi]
Automatic Updates [wuauserv]

You should turn off the services you do not use.

This list is useful to an attacker, who can make his attack more silent by not portscanning this host.

Solution : To prevent the listing of the services for being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk factor : Low

Nessus ID : [10456](#) Warning microsoft-ds (445/tcp) The following local accounts have never logged in :

Guest

TsInternetUser

Unused accounts are very helpful to hacker

Solution : suppress these accounts

Risk factor : Medium

Nessus ID : [11457](#) Warning microsoft-ds (445/tcp) The following local accounts have never changed their password :

TsInternetUser

IUSR_XXXX

IWAM_XXXX

ASPNET

To minimize the risk of break-in, users should change their password regularly

Nessus ID : [10914](#) Warning microsoft-ds (445/tcp)

The remote ASP.NET installation might be vulnerable to a buffer overflow when an application enables StateServer mode.

An attacker may use it to cause a denial of service or run arbitrary code with the same privileges as the process being exploited (typically an unprivileged account).

Solution : See <http://www.microsoft.com/technet/security/bulletin/ms02-026.msp>

Risk factor : Medium

CVE : [CVE-2002-0369](#)

BID : [4958](#)

Nessus ID : [11306](#) Warning microsoft-ds (445/tcp)

The messenger service is running. This service allows NT users to send pop-ups messages to each others.

This service can be abused by who can trick valid users into doing some actions that may harm their accounts or your network (social engineering attack)

Solution : Disable this service.

Risk factor : Low

How to disable this service under NT 4 :

- open the 'Services' control panel
- select the 'messenger' service, and click 'Stop'
- click on 'Startup...' and change to radio button of the field 'Startup Type' from 'Automatic' to 'Disabled'

Under Windows 2000 :

- open the 'Administration tools' control panel
- open the 'Services' item in it
- double click on the 'messenger' service
- click on 'stop'
- change the drop-down menu value from the field 'Startup Type' from 'Automatic' to 'Disabled'

CVE : [CAN-1999-0630](#)

Nessus ID : [10458](#) Warning microsoft-ds (445/tcp) Here is the browse list of the remote host :

XXXX -
XXXX -
XXXX -
XXXX -

This is potentially dangerous as this may help the attack of a potential hacker by giving him extra targets to check for

Solution : filter incoming traffic to this port

Risk factor : Low

Nessus ID : [10397](#) Warning microsoft-ds (445/tcp)
The alerter service is running. This service allows NT users to send pop-ups messages to each others.

This service can be abused by an attacker who can trick valid users into doing some actions that may harm their accounts or your network (social engineering attack)

Solution : Disable this service.

Risk factor : Low

How to disable this service under NT 4 :

- open the 'Services' control panel
- select the 'Alerter' service, and click 'Stop'
- click on 'Startup...' and change to radio button of the field 'Startup Type' from 'Automatic' to 'Disabled'

Under Windows 2000 :

- open the 'Administration tools' control panel
- open the 'Services' item in it
- double click on the 'Alerter' service
- click on 'stop'
- change the drop-down menu value from the field 'Startup Type' from 'Automatic' to 'Disabled'

CVE : [CAN-1999-0630](#)

Nessus ID : [10457](#) Informational microsoft-ds (445/tcp) A CIFS server is running on this port

Nessus ID : [11011](#) Informational microsoft-ds (445/tcp)

It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000).

Note that this won't completely disable null sessions, but will prevent them from connecting to IPC\$

Please see <http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html>

All the smb tests will be done as 'Nessus'/'****' in domain XXXX

CVE : [CAN-1999-0504](#), [CAN-1999-0506](#), [CVE-2000-0222](#), [CAN-1999-0505](#), [CAN-2002-1117](#)

BID : [494](#), [990](#), [11199](#)

Nessus ID : [10394](#) Informational microsoft-ds (445/tcp) The remote native lan manager is : Windows 2000 LAN Manager
The remote Operating System is : Windows 5.0 Server
The remote SMB Domain Name is : XXXX

Nessus ID : [10785](#) Informational microsoft-ds (445/tcp) The following local accounts are disabled :

Guest

To minimize the risk of break-in, permanently disabled accounts should be deleted

Risk factor : Low

Nessus ID : [10913](#) Informational microsoft-ds (445/tcp)
The remote host has the Norton Antivirus installed. It has been fingerprinted as :

Norton/Symantec Antivirus
DAT version : 20050302

Risk factor : None

Nessus ID : [16193](#) Informational microsoft-ds (445/tcp)
The remote host does not have Windows Update enabled.

Enabling WindowsUpdate will ensure that the remote Windows host has all the latest Microsoft Patches installed.

Solution : Enable Windows Update on this host

See also : <http://www.microsoft.com/security/protect/>

Nessus ID : [12028](#) Informational NFS-or-IIS (1025/tcp) Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Here is the list of DCE services running on this port:

UUID: XXXX, version 1
Endpoint: XXXX: XXXX [1025]

UUID: XXXX, version 1
Endpoint: XXXX : XXXX [1025]

UUID: XXXX, version 1
Endpoint: XXXX: XXXX [1025]

UUID: XXXX, version 1
Endpoint: XXXX: XXXX [1025]

Solution : filter incoming traffic to this port.

Risk factor : Low

Nessus ID : [10736](#) Informational LSA-or-nterm (1026/tcp) Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Here is the list of DCE services running on this port:

UUID: XXXX, version 1
Endpoint: XXXX: XXXX [1026]
Named pipe : atsvc
Win32 service or process : mstask.exe
Description : Scheduler service

UUID: XXXX, version 1
Endpoint: XXXX: XXXX [1026]

Solution : filter incoming traffic to this port.

Risk factor : Low

Nessus ID : [10736](#) Informational ms-lsa (1029/tcp) Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Here is the list of DCE services running on this port:

UUID: XXXX, version 2
Endpoint: XXXX: XXXX [1029]

Solution : filter incoming traffic to this port.

Risk factor : Low

Nessus ID : [10736](#) Warning general/tcp

The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also : <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>
<http://www.kb.cert.org/vuls/id/464113>

Solution : Contact your vendor for a patch

Risk factor : Medium

BID : [7487](#)

Nessus ID : [11618](#) Warning general/tcp

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:

1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network.
2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.
3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

Solution : Contact your vendor for a patch

Risk factor : Low

Nessus ID : [10201](#) Warning general/tcp

The remote host accepts loose source routed IP packets.
The feature was designed for testing purpose.
An attacker may use it to circumvent poorly designed IP filtering
and exploit another flaw. However, it is not dangerous by itself.

Solution : drop source routed packets on this host or on other ingress
routers or firewalls.

Risk factor : Low

Nessus ID : [11834](#) Informational general/tcp The remote host is running
Microsoft Windows 2000 Server Service Pack 4 (English)

Nessus ID : [11936](#) Informational general/tcp The remote host has Symantec
Norton Antivirus version installed

Nessus ID : [14835](#) Warning general/icmp

The remote host answers to an ICMP timestamp request. This allows an
attacker
to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP
timestamp replies (14).

Risk factor : Low

CVE : [CAN-1999-0524](#)

Nessus ID : [10114](#) Informational general/udp For your information, here is the
traceroute to XXXX:

XXXX

XXXX

Nessus ID : [10287](#) Warning netbios-ns (137/udp) The following 9 NetBIOS
names have been gathered :

XXXX = This is the computer name registered for workstation services by a
WINS client.

XXXX = Computer name

XXXX = Workgroup / Domain name

XXXX = This is the current logged in user registered for this workstation.

XXXX = Workgroup / Domain name (part of the Browser elections)

XXXX = Workgroup / Domain name (Domain Controller)

XXXX

XXXX

__MSBROWSE__

The remote host has the following MAC address on its adapter :

XXXX

If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port.

Risk factor : Medium

CVE : [CAN-1999-0621](#)

Nessus ID : [10150](#)

This file was generated by [Nessus](#), the open-sourced security scanner.

© SANS Institute 2000 - 2005, Author retains full rights.