



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 IIS Microsoft Windows 2000 Server

Auditing Networks,
Perimeters, and Systems

GSNA Practical Assignment

Version 3.2

Option 1

Beverly Pfaff

November 11, 2004

Abstract

This paper provides details on an audit of a Microsoft Windows 2000 file server running Internet Information Services (IIS), a required component of Microsoft Software Update Service. The objective of the audit is to determine the level of security on this server and the degree of the threat exposure this server causes for the Agency XYZ computer environment by having IIS installed. Based on current events, a list of significant risks will be developed. The goal is to find out whether this box has been adequately secured against known threats and vulnerabilities. The goal is to determine whether security controls have been applied in accordance with current industry practices. The target audience for the findings from this audit is the server's system administrators and management.

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract.....	ii
Introduction	4
Part #1 -Research in Audit, Measurement, Practice, and Control	5
1.1 System to be Audited and its Role.....	5
1.1.1 Current Environment.....	5
1.1.2 Server Configuration.....	5
1.2 Significant Risks to the System.....	7
1.2.1 Threats.....	9
Affected Assets	10
1.2.2 Major Vulnerabilities.....	10
1.3 Current State of Practice.....	12
Part #2 – Audit Checklist.....	13
2.1 Check Security of Default Computer Accounts and Groups	13
2.2 Ensure the Guest Account is Disabled.....	14
2.3 Check for Unwanted Software	15
2.4 Are Any Trojans Listening on Open Ports?.....	16
2.5 Are Unneeded Services Running?.....	17
2.6 Cross Reference Processes to Ports and Services	18
2.7 Check for Virus Auto-Protection.....	19
2.8 Determine Whether Security Patching is Current	20
2.9 Analyze IIS for Vulnerabilities	21
2.10 Evaluate Other Installed Software Products for Vulnerabilities.....	22
Part #3 – Conduct the Audit Testing, Evidence and Findings	23
3.1 Evidence and Findings from 2.1 (Check Security of Default Computer Accounts and Groups).....	23
3.2 Evidence and Findings from 2.2 (Ensure Guest Account is Disabled).....	28
3.3 Evidence and Findings from 2.3 (Check for Unwanted Software).....	29
3.4 Evidence and Findings from 2.4 (Are Any Trojans Listening on Open Ports?).....	33
3.5 Evidence and Findings from 2.5 (Are Unneeded Services Running?).....	36
3.6 Evidence and Findings from 2.6 (Cross Reference Processes to Ports and Services	43
3.7 Evidence and Findings from 2.7 (Check for Virus Auto-Protection).....	52
3.8 Evidence and Findings from 2.8 (Determine Whether Security Patching is Current).....	53
3.9 Evidence and Findings from 2.9 (Analyze IIS for Vulnerabilities).....	60
3.10 Evidence and Findings from 2.10 (Evaluate Other Installed Software Products for Vulnerabilities).....	64
Part #4 – Audit Report.....	74
Executive Summary.....	74
Audit Findings.....	75
Audit Recommendations.....	82

List of Figures

Figure 1: Server Baseline.....	6
Figure 2: AgencyXYZ simplified network diagram-.....	7
Figure 3 – Addusers Listing.....	23
Figure 4 – Terminal Server Mode.....	25
Figure 5 – Microsoft Baseline Security Analysis of Guest.....	28
Figure 6 – List of Installed Software.....	30
Figure 7 – Installed Computer Components.....	30
Figure 8 – nMap Listing.....	33
Figure 9 – Netstat Listing	35
Figure 10 – Fport Listing	45
Figure 11 – Symantec Anti-virus Protection	52

List of Tables

Table 1 – Threat Likelihood.....	8
Table 2 – Threat Magnitude of Consequence	8
Table 3 – Risk Action Scale	9
Table 4 – Potential Threats	9
Table 5 – Assets.....	10
Table 6 – Major Vulnerabilities	12
Table 7 – Suggested List of Services to be Disabled	43
Table 8 – Cross Reference Chart – Process ID, Process, Port, Service.....	51
Table 9 – Nessus Report.....	57
Table 10 - Microsoft Baseline Security Analysis Results.....	58
Table 11 – Microsoft Baseline Security Analysis of IIS.....	60
Table 12 – Not/Maybe/Required IIS Services	63
Table 13 – Vulnerabilities in Other Install Software.....	73
Table 14 – Audit Findings.....	82

Introduction

The file server evaluated in this paper is owned by a government agency that will be called AgencyXYZ in order to not expose the name and business activities of the real organization. The server will be called AgencyXYZ server. AgencyXYZ server is a Microsoft Windows 2000 Server, Service Pack 4 that is running Internet Information Services (IIS) 5.0r to support a Microsoft Software Update Service (SUS) installation used for patch management in a medium-sized federal government organization. This server is not critical to the mission of Agency XYZ; however it makes a significant contribution to security within the Information Technology program. This server also hosts other significant systems such as the organization's managed enterprise anti-virus system and an Oracle database.

In the beginning Management and the system administrators were leery of IIS. But IIS was a necessary evil in order to have SUS. After they ran the Microsoft IIS Lockdown Tool against the box, I got the impression they mentally checked the security box—the box was secured. I remained some leery but more curious. When given the opportunity to audit something for this GIAC Practical, I chose the IIS box. I didn't find out until I was well into my audit that this server is more than just IIS. I had to contain the scope of my audit to ten areas that I wanted to test the security controls.

Security is very broad topic. My interest lies in the area that is currently disrupting the industry—the affect of malware on an organization. Malware is the emphasis point around which my project is developed.

Part #1 -Research in Audit, Measurement, Practice, and Control

1.1 System to be Audited and its Role

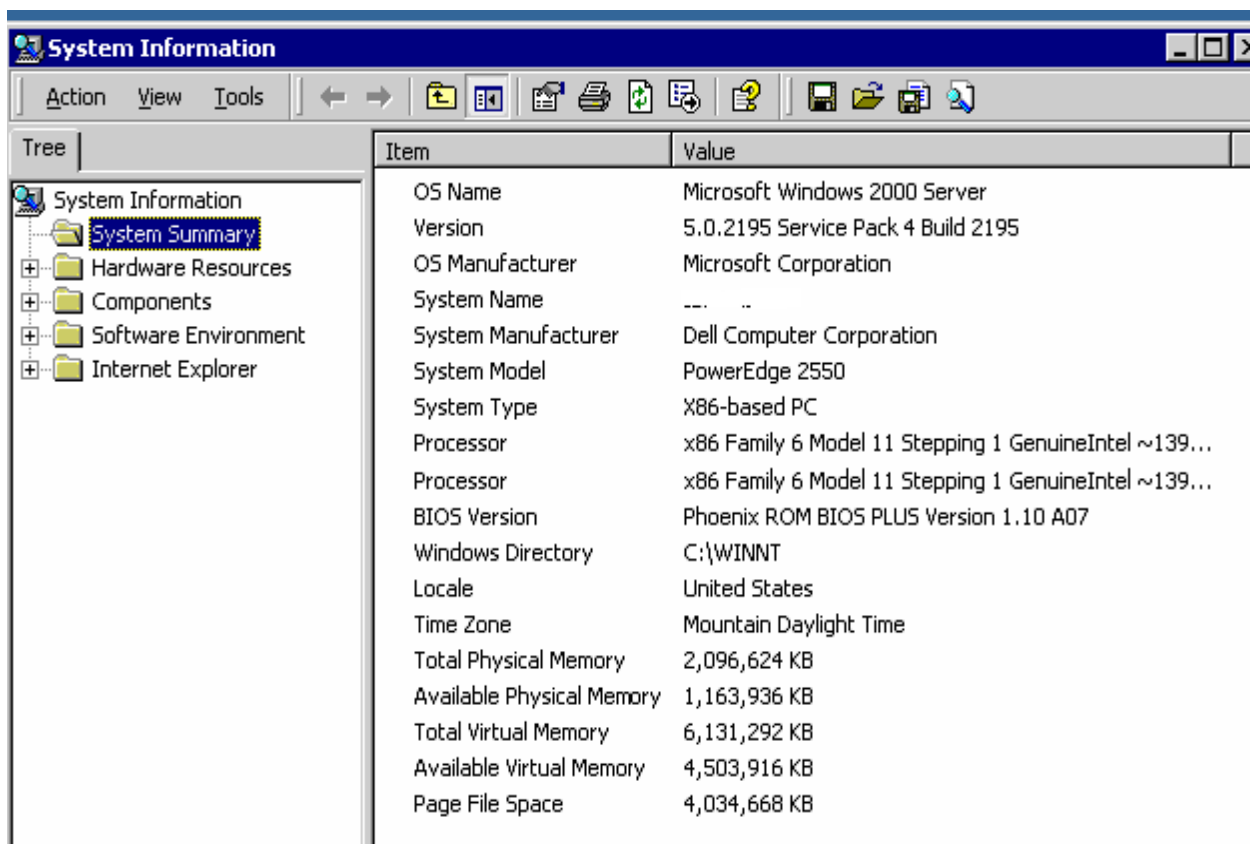
I am auditing a Microsoft Windows 2000 Server, Service Pack 4 that is running IIS 5.0 to support a Microsoft Software Update Service (SUS) installation used for patch management in a medium-sized federal government organization. The Microsoft servers and workstations exist in a Workgroup environment. This server plays a number of roles in the AgencyXYZ information technology (IT) organization. In addition to SUS, installed on this server are a Symantec Control Center that manages antivirus definition file updates on all Microsoft machines connected to the AgencyXYZ network and Oracle 9i web client/server applications. Because of the roles it plays, this server is accessible and interacts with all the Microsoft based systems connected to the AgencyXYZ network.

1.1.1 Current Environment

This server is located in an environmentally and physically controlled computer room. As displayed by Figure 2: AgencyXYZ simplified network diagram-, AgencyXYZ's computer network is protected by both Internet facing and inward-facing firewalls and an intrusion detection system (IDS) managed by personnel at the Headquarters Office. A security perimeter policy has been established within the AgencyXYZ organization. All data communication traffic is required to enter and exit through the Headquarters DMZ to the Internet. All external traffic is denied access to internal information technology resources except through approved avenues, i.e., vpn tunneling, and secure ftp. On the other hand, internal users have minimal restrictions when exiting and re-entering the AgencyXYZ firewalls, using web-based resources, accessible via the Internet. Internet Explorer security level is set to medium. ActiveX scripting and java applets are enabled. The Symantec antivirus shield is installed on all Microsoft machines on AgencyXYZ network. Internet email, funneled through the Headquarters DMZ virus/spam filters before distribution to user mailboxes is approximately 70 percent effective. There currently are no techniques employed to protect the user from hostile Internet links in email other than IT security awareness. The safeguards to encounters with malicious code in email or hostile web sites are patch management and the antivirus shield.

1.1.2 Server Configuration

The server hardware is a Dell PowerEdge 2550 with a single Pentium III 1.4 GHz processor and 2GB RAM, running Microsoft Windows 2000 Server version 5.0.2195 Service Pack 4. The utility *msinfo32.exe* was run to obtain a summary of the server system configuration:



The screenshot shows the 'System Information' window with the 'System Summary' tab selected. The left pane shows a tree view with 'System Information' expanded. The right pane displays a list of system items and their values.

Item	Value
OS Name	Microsoft Windows 2000 Server
Version	5.0.2195 Service Pack 4 Build 2195
OS Manufacturer	Microsoft Corporation
System Name	---
System Manufacturer	Dell Computer Corporation
System Model	PowerEdge 2550
System Type	X86-based PC
Processor	x86 Family 6 Model 11 Stepping 1 GenuineIntel ~139...
Processor	x86 Family 6 Model 11 Stepping 1 GenuineIntel ~139...
BIOS Version	Phoenix ROM BIOS PLUS Version 1.10 A07
Windows Directory	C:\WINNT
Locale	United States
Time Zone	Mountain Daylight Time
Total Physical Memory	2,096,624 KB
Available Physical Memory	1,163,936 KB
Total Virtual Memory	6,131,292 KB
Available Virtual Memory	4,503,916 KB
Page File Space	4,034,668 KB

Figure 1: Server Baseline

Below is a high level view of the AgencyXYZ network:

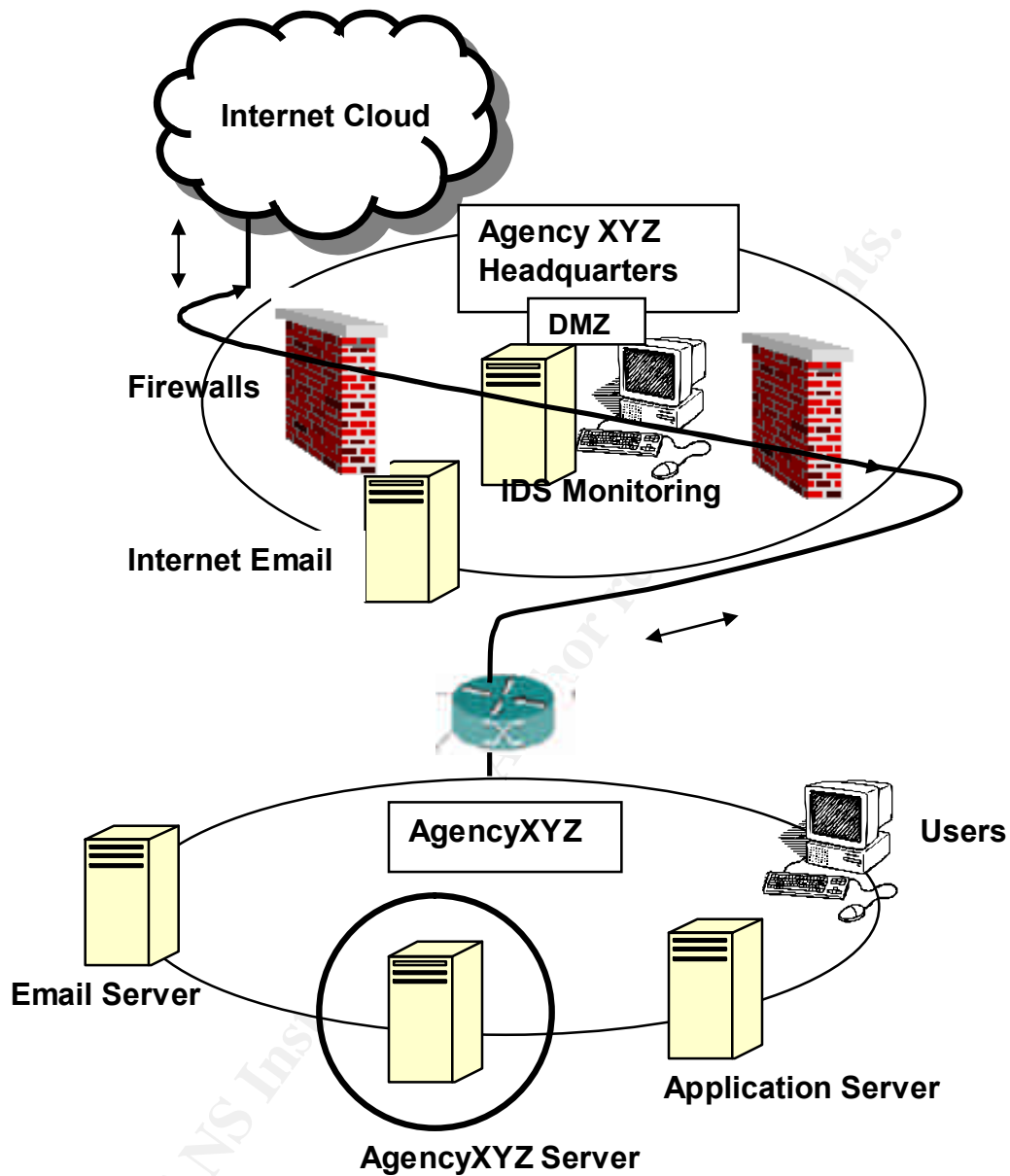


Figure 2: AgencyXYZ simplified network diagram-

1.2 Significant Risks to the System.

Before I could compile a list of risks that expose a Windows 2000 Server running IIS, I needed to first reacquaint myself with the definition of risk and how to determine the

level of risk in order to comply with the Global Information Assurance Certification assignment to evaluate the most significant risks.

According to the definition found at <http://www.atis.org/tg2k/risk.html> risk is the possibility that a particular threat will exploit a particular vulnerability of a data processing system.

How does one predict the possibility that a particular threat will exploit a particular vulnerability? NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002, provides an example threat likelihood table:¹

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Table 1 – Threat Likelihood

How does one determine the level of risk--by multiplying Threat Likelihood and Magnitude of Consequence? NIST SP 800-30 provides an example magnitude of consequence table if the threat is realized:

Magnitude of Consequence	Consequence Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Table 2 – Threat Magnitude of Consequence

¹ "NIST Special Publications". NIST Computer Security Resource Center web site. © 2000. URL: <http://csrc.nist.gov/publications/nistpubs/index.html>

Risk levels can be equated to a Risk Action Scale as provided in NIST SP 800-30:

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the DAA must determine whether corrective actions are still required or decide to accept the risk.

Table 3 – Risk Action Scale

1.2.1 Threats

A threat is any event that, if realized, can cause damage to a system, and create a loss of confidentiality, availability, or integrity.²

Potential Threats	Threat Examples
Hackers	Social engineering, intrusion attacks, port scanning, password cracking, exploiting known software weaknesses, network spoofing
Malicious Code	Viruses, Trojans, spyware
Human	User computing habits, with Internet usage and email, intentional and unintentional acts, negligence, errors, unauthorized access
Denial of Service	SoBig Mail bomb, Consuming server resources (MS-Blaster Worm), Saturating network resources (Ping floods).
Natural	Floods, earthquakes, tornadoes, electrical storms
Environmental	Long-term power failure, heat, water, fire
Physical	Internal theft, unrestricted access to the hardware in computer center, strangers/non-employees

Table 4 – Potential Threats

² Krutz, Ronald L. and Russell Dean Vines. The CISSP Prep Guide: Mastering the Ten Domains of Computer Security. Berkeley, California: McGraw-Hill/Osborne, 2001.

Affected Assets

Computer Hardware
Operating System
Applications
Company Data
User Data
Company Network
Company Productivity
Information Security Assurance
Timely Delivery of Services

Table 5 – Assets

1.2.2 Major Vulnerabilities

Vulnerability is a weakness in a system that can be exploited by a threat.³

Vulnerabilities	Likelihood of Exploitation	Magnitude of Consequence
Security flaws in software with published exploits.	High	<ul style="list-style-type: none"> May violate, harm, or impede an organization's mission, reputation, or interest. Denial of Service which could lead to lost productivity, public trust, or timely delivery of services. Introduction of malicious code, spam or spoofed email which could lead to lost productivity, public trust, or timely delivery of services.
No automated patch deployment process.	High	<ul style="list-style-type: none"> Disclosure of sensitive or restricted data could lead to company embarrassment and lost public trust, future system attacks, and exploitation of other systems on the network. Introduction of malicious code, spam or spoofed email which could lead to lost productivity, public trust, or timely delivery

³ Krutz, Ronald L. and Russell Dean Vines. The CISSP Prep Guide: Mastering the Ten Domains of Computer Security. Berkeley, California: McGraw-Hill/Osborne, 2001.

		of services.
No antivirus protection	High	<ul style="list-style-type: none"> • Introduction of malicious code, spam, or spoofed email which could lead to lost productivity, public trust, or timely delivery of services.
Breaching perimeter security	Low	<ul style="list-style-type: none"> • Hacker attack, system exploitation • Port scanning • Snooping.
Default permissions	Medium	<ul style="list-style-type: none"> • Data manipulation or theft. • Introduction of malicious code, spam, or spoofed email which could lead to lost productivity, public trust, or timely delivery of services. • System exploitation.
Generic Accounts	Medium	<ul style="list-style-type: none"> • Backdoor hack attacks. • Privilege escalation. http://www.microsoft.com/technet/itsolutions/techguide/msm/acctmgmt/acmarch/acmarch3.msp • Access to hidden shares. • Disclosure of sensitive or restricted data could lead to company embarrassment and lost public trust, future system attacks, and exploitation of other systems on the network.
Unnecessary services and open ports	Medium	<ul style="list-style-type: none"> • Introduction of malicious code, spam, or spoofed email which could lead to lost productivity, public trust, or timely delivery of services. • Backdoor hack attacks. • Unauthorized access leading to data manipulation or theft.
Default software installations	Medium	<ul style="list-style-type: none"> • Introduction of malicious code, spam, or spoofed email which could lead to lost productivity, public trust, or timely delivery of services. • Disclosure of sensitive or restricted data could lead to company embarrassment and lost public trust, future system attacks, and exploitation of other systems on the network.
A networked computer environment	High	<ul style="list-style-type: none"> • A blended threat for example could use malicious code to attack other systems on the network with unpatched O/S software vulnerabilities. The Nimda, Code Red, Netsky, or Blaster all take advantage of a networked environment to cause a denial of service which could lead to lost productivity, public trust, or timely delivery of services. • The systems on the network are probably homogeneous in regard to vulnerabilities.

Unrestricted ability to execute scripts and download files	Medium	<ul style="list-style-type: none">• Introduction of malicious code, spam or spoofed email which could lead to lost productivity, public trust, or timely delivery of services.• Unauthorized access leading to data manipulation or theft.• Sensitive, restricted, or Privacy Act data theft.• Stolen user identity.
--	--------	---

Table 6 – Major Vulnerabilities

1.3 Current State of Practice

I did extensive research using the Internet search engine Google (<http://www.google.com>) and Ask Jeeves (<http://www.ask.com>), for articles on threats, vulnerabilities, recent attacks, and IIS for starters. The Internet is a wonderful library of resource materials.

Through my entire Internet surfing and research, I'm sorry to say I never came across an entire audit system or package such as SANS has put together for its GSNA track. I can only conclude that it is a difficult thing to do. From personal experience, my organization has been the recipient of a computer security audit and it too, consisted of discordant pieces that looked at differing areas of the program.

What I did find, was that the information technology businesses are now approaching the distribution of their goods and services with a security bent. This paper is full of references to web sites containing documents discussing security vulnerabilities, vulnerability fixes, and ramifications if a person waits too long to apply a patch, etc. Microsoft is a perfect example. You will find that I have loaded this paper with footnote references to Microsoft web pages. For example, if I want to know what services are needed by IIS, so that I can audit my IIS box and determine what services are running that maybe shouldn't be, I found the paper Microsoft put together discussing that very topic.

As I said earlier, my intent is to center this paper on malware. So this paper is also full of references to experts in the security business who know the what, when, where, and how about an attack. I decided it made for good audit tools. I tried to keep all my reference materials within a 2003-2004 timeframe.

Part #2 – Audit Checklist

2.1 Check Security of Default Computer Accounts and Groups	
Reference	See footnotes.
Risk	Installing generic accounts, ⁴ taking the defaults such as well-known or null passwords and forgetting to go back afterward and make the account more secure, give the hacker an open door to walk through.
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> Run a native Windows tool, <i>addusers /d ckusracct.txt</i>, to generate a list of computer accounts associated to user groups⁵ List the default computer accounts/groups and determine whether they need to exist.⁶
Test Nature	Objective
Evidence	Place holder.
Findings	Place holder.

⁴ "TSInternetUser Password Is Changed Daily." Microsoft web site. © 2004. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;244057&sd=tech>

⁵ Implementing Windows Authentication for Oracle - Authenticate database users with Windows usernames and passwords, May 2004, by John Paul Cook." WindowsITPro web site. © 2004. URL: <http://www.winnetmag.com/Windows/Article/ArticleID/42280/42280.html>.

⁶ "Securing Exchange 2000 Servers Based on Role." Microsoft web site. © 2004. URL: <http://www.microsoft.com/technet/security/guidance/secmod43.msp>.

2.2 <i>Ensure the Guest Account is Disabled</i>	
Reference	See footnotes.
Risk	Accounts left in a default state may not have passwords ⁷ or the initial password is widely known.
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none">• Run Windows Baseline Analyzer to determine whether Guest is disabled.• Guest account is installed with a blank password by default.⁸ Determine whether the password was changed.
Test Nature	Objective
Evidence:	Place holder.
Findings:	Place holder.

⁷ "Windows 2000 Server Baseline Security Checklist." Microsoft web site. © 2004. URL: www.microsoft.com/technet/security/chklist/w2ksvrcl.mspx?pf=true

⁸ "Microsoft Windows Security 101, by Tony Bradley." About, Inc. web site. © 2004. URL: <http://netsecurity.about.com/cs/windowsxp/a/aa100903.htm>

2.3 Check for Unwanted Software	
Reference	See footnotes.
Risk	<p>The system administrator needs to be familiar with legitimately installed software. By tracking and validating installed software, strange programs will be easy to detect and can be checked for malicious code.⁹ The unwanted software may be as innocuous as a browser toolbar which interferes with viewing html files or as malicious as a backdoor Trojan bot connected to a zombie network.</p> <p>During software installations, other components may get installed by default unbeknownst to the system administrator.¹⁰ Default installs often have default passwords, ports, naming conventions, etc., which are well-known to the hacker community.</p>
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> • Go to Control Panel Add/RemovePrograms and take a screen shot of the installed software that is displayed. • Go to Control Panel/Administrative Tools/Component Services and make a screen shot of the displayed products. • Determine whether all software listed was legitimately installed by the system administrator.
Test Nature	Objective
Evidence:	Place holder.
Findings:	Place holder.

⁹ "Virus Rivalry Boosts Security Threats, July 26, 2004, by Stephen Lawson." ComputerWeekly web site. © 2004. URL: <http://www.computerweekly.com/print/ArticlePrinterPage.asp?liArtID=132259&liFlavou>

¹⁰ "Default Software Installs Are Not Secure, by R. Craig Peterson" Mainstream Security Services, LLC. © 2003. URL: http://www.mainstream.net/summary/default_software_installs_not_secure.shtml

2.4 Are Any Trojans Listening on Open Ports?	
Reference	See footnotes.
Risk	Trojans and worms commonly open ports to connect to web sites which are hosting a zombie network or master controller. Unless the system administrator knows which port should be open on a system, and is constantly comparing what should be open, to what is open, they may be infected and not know it. An anti-virus shield is good to have, but may not detect the most recent releases of malicious code.
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> • Run nMap.exe to get another listing of open ports in a different format.¹¹ • Run the native Windows command netstat -a to find out which ports are listening.¹² • Validate the open ports by comparing the two reports. • Look at open ports on the system I'm auditing and determine whether any are targets for Trojans.¹³ I have noticed that the Trojan port lists vary, so compare against several listings.⁽¹⁵⁾
Test Nature	Objective
Evidence	Place holder.
Findings	Place holder.

¹¹ "Nmap Security Scanner." Insecure.org web site. © 2004. URL: <http://www.insecure.org/>

¹² "Netstat." Microsoft web site. © 2004. URL: http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prmb_tol_jyv.asp

¹³ "Trojan Port List." G-Lock Software web site. © 2004. URL: http://www.glocksoft.com/trojan_port.htm

2.5 <i>Are Unneeded Services Running?</i>	
Reference	See footnotes.
Risk	Symantec advises its customers to turn off or remove unneeded services. A standard number of services are installed by default which aide hacker exploits, such as ftp, tftp, telnet, or IIS. Hackers count on the existence of these services in a running state in order to attack. The experts are saying this is one avenue for blended threats that if removed could lessen the impact of an attack. The system administrator has a better chance of quickly identifying rogue services if services are being managed. The point at which users are complaining about reboots and slow performance is not the time to go through the arduous process of determining what the purpose is for each service that is running.
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> • Run psservice.exe and pipe the results to a text file.¹⁴ • Look at the list of services generated by psservice. • Identify those services running. • Should any services that are running be disabled? • Should any services set to Manual be disabled?
Test Nature	Objective
Evidence	Place holder.
Findings	Place holder.

¹⁴ "PsTools, October 13, 2004, by Mark Russinovich and Bryce Cogswell." SysInternals web site. © 2004. URL: <http://www.sysinternals.com/ntw2k/freeware/pstools.shtml>

2.6 Cross Reference Processes to Ports and Services	
Reference	See footnotes.
Risk	Trojans tend to target certain ports. ¹⁵ Legitimate applications use some of these same ports. If the system administrator does not have a good understanding of the association of ports, processes, and services to applications, just by replacing a file or service and commandeering a port, a Trojan can disguise itself and pass itself off as a legitimate process for weeks, months, or years, until the hacker triggers a malicious event.
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> • From the Windows 2000 Resource Toolkit retrieve the file tlst.exe. Tlst.exe lets you list all the processes running on your machine and the associated task name and memory usage and pipe the results to a text file.. • Run fport.exe and pipe to a text file.¹⁶ • Cross-reference the Tasklist data to the fport. data to the services data. Note ports used by Trojans. Validate that processes running on these ports are legitimate installations.
Test Nature	Objective
Evidence	Place holder.
Findings	Place holder.

¹⁵ "Trojan & Worm Ports Information Center." DOSHelp.com web site. © 2004 URL:
<http://www.doshelp.com/trojanports.htm>

¹⁶ "Free Tools." Foundstone, Inc. web site. © 2004. URL:
<http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm>

2.7 Check for Virus Auto-Protection	
Reference	See footnotes.
Risk	<p>As firewalls and perimeter security cut off hackers access to organizations internal computer networks, they are turning to malware to carry on their work. In the Microsoft paper entitled, "The Anti-Virus Defense in Depth Guide", discusses the different avenues in which malware can enter an organization, i.e., Internet, guest clients, executables, email, removable media.¹⁷ A privacy firm called Webroot Software and ISP EarthLink did some research and discovered that one in three pcs has either spyware or a Trojan horse.¹⁸ When law enforcement shut down a web server in Russia on June 24, 2004, organizations running IIS 5.0 servers, did not know a lot about the Download.Ject Trojan horse and they did not know how their servers had become infected.¹⁹</p> <p>Microsoft released the patch on April 13, 2004, for the IE vulnerability that Download.Ject exploited. Symantec released a heuristic detection for a Microsoft Internet Explorer cross-zone scripting exploit called Bloodhound.Exploit.10 on June 10, 2004. There was two months reaction time with this vulnerability. But with the Blaster there was about 2 weeks (personal experience). The experts are saying that window is growing smaller each time an exploitable vulnerability is published. The key is real-time automation for patch management and virus file updates.</p>
Test Procedure/ Compliance Criteria	Find out whether this system has anti-virus software installed and is running a virus shield.
Test Nature	Objective
Evidence:	Place holder.
Findings:	Place holder.

¹⁷ "The Anti-Virus Defense in Depth Guide, dated May 20, 2004, updated August 25, 2004." Microsoft web site. © 2004. URL: http://www.microsoft.com/technet/security/guidance/avdind_0.mspx

¹⁸ "One in three PCs hosts spyware or Trojans, dated June 16, 2004, by Robert Jaques." Infomaticsonline, a United Kingdom web site. © 2004. URL: <http://www.infomaticsonline.co.uk/news/1155923>

¹⁹ "Email dated June 25, 2004, Russian IIS Hacks - yet another technique for spreading and installing "spamware, by Jan Reilink." Posted on Mailgate.org. © 2004. URL: <http://mailgate.supereva.it/be/be.comp.security/msg02227.html>

2.8 Determine Whether Security Patching is Current	
Reference	See footnotes.
Risk	Because most organizations employ perimeter security, the hacker can no longer walk in the front door. Most of the attacks today are executed through security weaknesses in installed software running on an internal system. Hackers are exploiting those organizations that have poor patch policies. If the hacker can gain entry to the internal network, usually through trickery--by sending the user email containing a hostile program or draw the user outside the perimeter to the Internet, they then have the opportunity to attack weakness in the software.
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> • Run nessus.exe, a Network Security Auditing Utility to see whether the latest patches are installed²⁰ • Run Windows Baseline Analyzer to generate a comparison list.²¹
Test Nature	Objective
Evidence	Place holder.
Findings	Place holder.

²⁰ "Nessus.org." Nessus web site. © 2004. URL:<http://www.nessus.org/index2.html>

²¹ "Microsoft Baseline Security Analyzer V1.2.1, August 16, 2004." Microsoft web site. © 2004. URL:
<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

2.9 Analyze IIS for Vulnerabilities	
Reference	See footnotes.
Risk	According to windowsecurity.com IIS is second in popularity after Apache. The reason IIS is so popular is because it is so easy to install. It is also easy to hack. The Microsoft Technical Security website lists 25 patches released between May 10, 2000 and October 12, 2004, that fix weaknesses in the IIS code. ²² Only one bulletin was released in 2004, MS04-030.
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> • Look at the results from running Microsoft Baseline Security Analyzer for weaknesses in IIS. • Look at the nessus.exe report for IIS weaknesses. • Determine what safeguards have been implemented to protect the IIS environment.
Test Nature	Objective
Evidence	Place holder.
Findings	Place holder.

22 "IIS LockDown Tool – Beyond the Basics, June 10, 2003, by Brett Hill". IISAnswers web site. © 2004.
 URL: http://www.iisanswers.com/articles/IIS_Lockdown/IISLockdown.htm

2.10 Evaluate Other Installed Software Products for Vulnerabilities	
Reference	See footnotes.
Risk	<p>When a really vulnerable software is installed on a system, e.g. IIS, the tendency is to narrow the range of vigilance to just that one piece of software. When other software products are installed on a system running IIS, 1) the subsequent installations may reverse security implemented by the IIS Lockdown tool, or 2) vulnerabilities in the OS or other products are overlooked.²³ In the case of the Download.Ject Trojan Horse, IIS was not the vulnerability that was exploited. It was used as the utility to propagate the infection. This time, Download.Ject exploited vulnerability in Internet Explorer concerning cross-zone scripting.</p> <p>Microsoft is not the only game in town. News alerts are released almost on a daily basis warning of vulnerabilities in many of the widely used software products. System administrator needs to treat all the vulnerabilities with the same priority.</p> <p>Frequently, software is installation-friendly by providing defaults which if not changed during or after the install could be exploited by malware later on. Sometimes additional components or services are installed or enabled that if not used should be disabled or uninstalled.</p>
Test Procedure/ Compliance Criteria	<ul style="list-style-type: none"> • Evaluate the installed software list, Figure, researching the security history of any product with which I am not familiar. • Use the Cross Reference Chart to familiarize myself with the association of processes, ports, and services. • Determine whether weaknesses have been published on any of the installed products. Start with the products that use the same ports as do Trojans. • Determine whether patches were applied.
Test Nature	Objective
Evidence	Place holder.
Findings	Place holder.

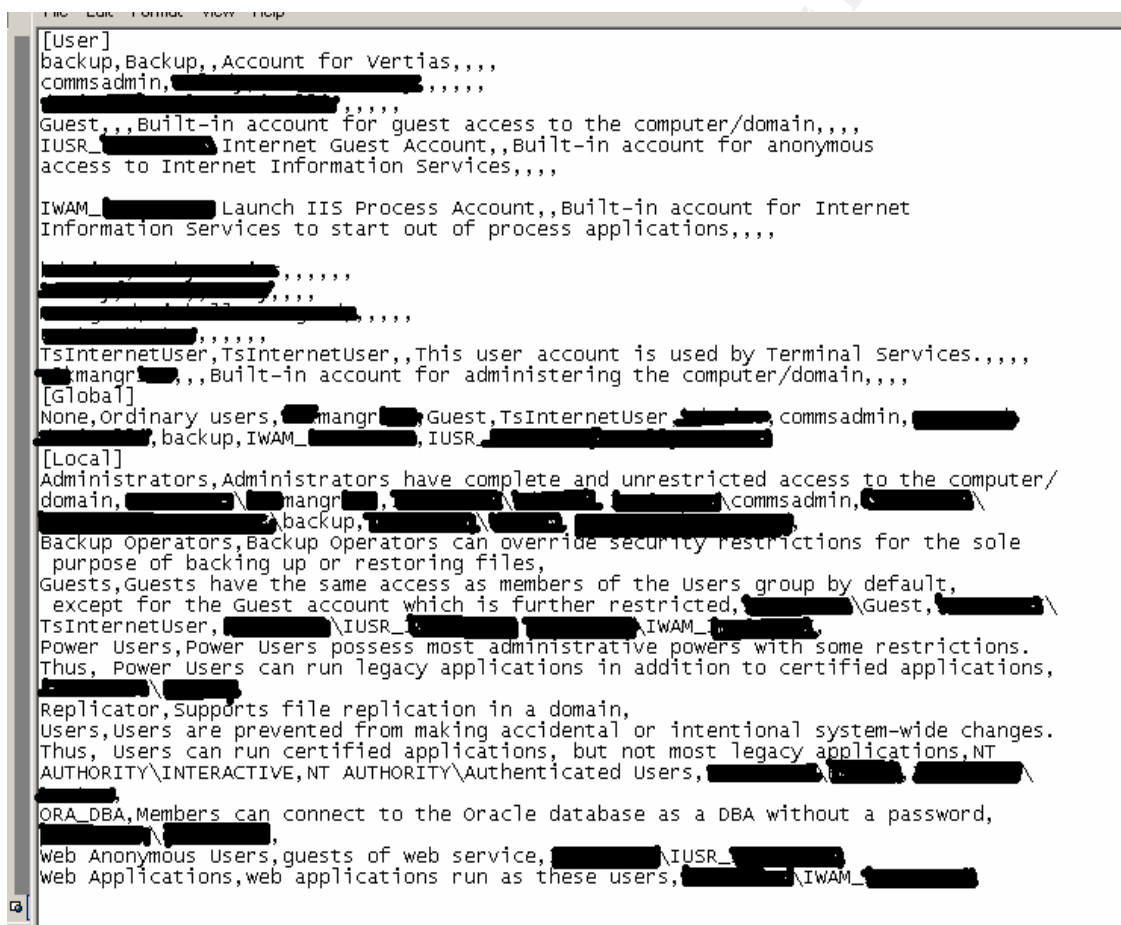
²³ "Microsoft Statement Regarding Configuration Change to Windows in Response to Download.Ject Security Issue, July 2, 2004." Microsoft web site. © 2004. URL: <http://www.microsoft.com/presspass/press/2004/jul04/07-02configchange.asp>

Part #3 – Conduct the Audit Testing, Evidence and Findings

3.1 Evidence and Findings from 2.1 (Check Security of Default Computer Accounts and Groups)

Evidence:

Addusers results:



```

[User]
backup,Backup,,Account for Vertias,,,
commsadmin,commsadmin,,Account for Vertias,,,
Guest,,Built-in account for guest access to the computer/domain,,,
IUSR,,Internet Guest Account,,Built-in account for anonymous
access to Internet Information Services,,,
IWAM,,Launch IIS Process Account,,Built-in account for Internet
Information Services to start out of process applications,,,
TsInternetUser,,This user account is used by Terminal Services,,,
mangr,,Built-in account for administering the computer/domain,,,
[Global]
None,Ordinary users,,Guest,TsInternetUser,commsadmin,
backup,IWAM,IUSR,
[Local]
Administrators,Administrators have complete and unrestricted access to the computer/
domain,,mangr,commsadmin,
Backup Operators,Backup Operators can override security restrictions for the sole
purpose of backing up or restoring files,
Guests,Guests have the same access as members of the Users group by default,
except for the Guest account which is further restricted,,Guest,
TsInternetUser,IUSR,IWAM,
Power Users,Power Users possess most administrative powers with some restrictions.
Thus, Power Users can run legacy applications in addition to certified applications,
Replicator,Supports file replication in a domain,
Users,Users are prevented from making accidental or intentional system-wide changes.
Thus, Users can run certified applications, but not most legacy applications,NT
AUTHORITY\INTERACTIVE,NT AUTHORITY\Authenticated Users,
ORA_DBA,Members can connect to the Oracle database as a DBA without a password,
web Anonymous Users,guests of web service,IUSR,
web Applications,web applications run as these users,IWAM,

```

Figure 3 – Addusers Listing

Findings:

Default accounts:

Guest – Microsoft guidance advises that the Guest account can't be renamed or deleted.

The Guest user account does show up on the listing generated by **adduser** for the AgencyXYZ server.

IUSR_AgencyXYZ – *This is a default anonymous Internet user account created during a IIS installation, which non-authenticated users access pages.*

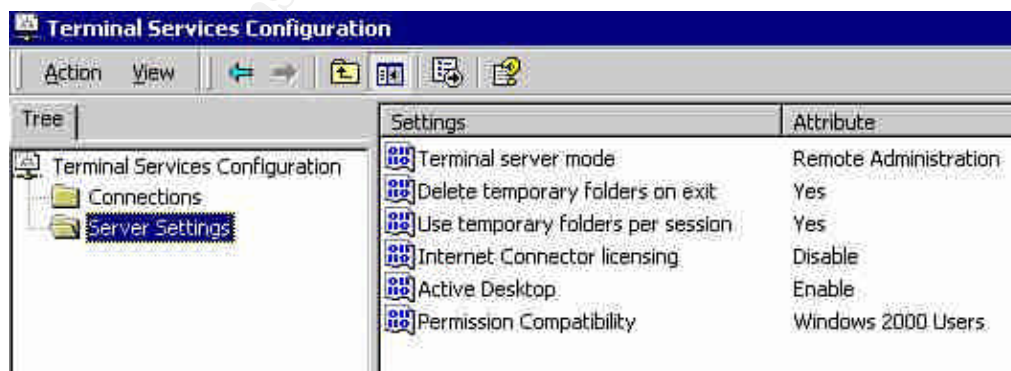
Some security experts advise renaming the IUSR_AgencyXYZ account. However Microsoft advises running the IIS Lockdown tool. The IUSR account is then made a member of the Web Anonymous Users group

IWAM_AgencyXYZ – *This is a default anonymous Internet user account created during the IIS installation, which allows non-authenticated users to start web applications. After the IIS Lockdown tool is run the IWAM user is added to the Web Applications Group.*

The IWAM_AgencyXYZ account does show up on the listing generated by **adduser** for the AgencyXYZ server which means IIS is installed on this server.

TSInternetUser – *Microsoft guidance advises that the TSInternetUser account is created at the time Terminal Services is installed. If Terminal Service Internet Connector License is not used, the TSInternetUser account should be disabled. This account is not automatically disabled by the security hardening templates. If Terminal Services is installed in application mode, Terminal Services Connector Licensing needs to be enabled. The Terminal Services Internet Connector Licensing uses the TSInternetUser account to automatically log users' onto the system.²⁴*

I had the system administrator go into the Terminal Services Manager to see what terminal server mode had been selected when Terminal Services was installed. The screenshot displays the fact that Terminal Services was installed in Remote Administration mode.



²⁴ "Terminal Services Internet Connector License and ASPs, October 21, 2003." Microsoft web site. © 2004. URL: <http://support.microsoft.com/default.aspx?scid=kb:en-us:288379&sd=tech>

Figure 4 – Terminal Server Mode

Because Terminal Services on this server has been configured for Remote Administration, the TSInternetUser account is probably not being used so should be disabled.

Default accounts which didn't show up (which is a good thing):

Administrator – *Microsoft security guidance recommends the Administrator account be renamed. The Administrator account can't be deleted.*

I noted that the Administrator account had been renamed in accordance with Microsoft security guidance.

Default groups with security issues to discuss:

Guests –

I note that user accounts IUSR_AgencyXYZ and IWAM_AgencyXYZ are associated to the default group Guests. The existence of these accounts means that IIS is installed on this system. The **addusers** utility noted that members of the Guests group have the same access privileges as the Users group by default.

The default user account TSInternetUser is also associated to the Guests group. The existence of the TSInternetUser account means Terminal Services have been installed on this server.

Administrators –

There are 12 user accounts on this server. General users do not have access to this server. All the user accounts on this system are either default, created by the products installed on this server or were created to administer the O/S or products such as Oracle, Symantec, IIS., SUS. Seven of the user accounts are associated to the Administrators group. This increases the element of risk for this system, because:

- 1) This system serves an important role in this organization's security program, and it would be unfortunate if it fell victim to an attack at the time it is suppose to be aiding the fight against an attack.
- 2) Malware that successfully exploits software includes taking control of the system by taking over the user's system profile and associated privileges. If the user has administrator privileges, the attacker could take control of the entire server. Malware could be introduced to the system if the user goes to the Internet, or reads email on this server (though it didn't appear that an email product was running on this server during my audit)(the organization has established a management practice that all email will be piped through one

system to the general purpose system that users log into.) The risk can be reduced if the system administrators avoid contact with malware, and that isn't always guaranteed even if we guard against the known threats, because the attackers always have the element of surprise to use to their advantage.

I recommend the system administrators that carry out the day-to-day administration of the system and who are familiar with the configuration of the system, look at the accounts that have administrator privilege and see if any accounts can be disabled or access to system areas removed. I'm surmising this situation has come about because of convenience and passing of time. I can say that because I am the functional administrator of the Symantec Enterprise Control Center that is installed on this server to manage the anti-virus file updates on servers and workstations in AgencyXYZ. Mine is not one of the seven administrator accounts on this system. I work through one of the day-to-day system administrator to manage the Symantec system. I find this practice commendable. Expecting this to be standard treatment for everyone, at the time I began my audit of this system, I was surprised to see who all had administrator privilege. The system administrators need to deal with the other software products administrators in this same manner as they dealt with me.

I also recommend that the system administrators create accounts associated to the Users group for the people who have to use the Internet to download patch files, etc. to reduce the risk of a successful exploit.

ORA_DBA – *When you install Oracle on a Windows server, the system creates an ORA_DBA Windows group and automatically adds to that group the Windows account used to install Oracle. Oracle9i uses Windows user login credentials to authenticate database users.²⁵ The Windows native authentication adapter is installed with Oracle Net Services and enables database user authentication in Windows 2000. ORA_DBA is considered a secure method for accessing Oracle databases.*

I noted that ORA_DBA on the **addusers** listing. I noted that the name of the data base administrator had been added to this group as the Oracle guidance suggests. I'm relying on Oracle's guidance that this is considered a secure method of authentication.

Web Anonymous Users - *This group is created by the IIS Lockdown tool. The IUSR_ServerName user account is added to this group when the IIS Lockdown script is run. The Web Anonymous Users group is assigned the Deny Write permission on Web content and the Deny Execute permission on selected administrative tools.*

I noted that the Web Anonymous Users group had been created, which meant the IIS Lockdown tool had been run on this server. The user account IUSR_AgencyXYZ had been added to this group.

²⁵ "Authenticating Database Users with Windows." Oracle web site. © 2004. URL: http://www.utexas.edu/its/unix/reference/oracledocs/v92/B10501_01/win.920/a95492/authen.htm

Web Applications – *This group is created by the IIS Lockdown tool. The IWAM_ServerName user account is added to this group when the IIS Lockdown script is run. This group is assigned the Deny Write permission on Web content and the Deny Full Control permission on selected administrative tools, if those options were enabled during the install.*

I noted that the Web Applications group had been created, which meant that the IIS Lockdown tool had been run on this server. The user account IWAM_AgencyXYZ has been added to this group.

Default groups which didn't show (could have strengthened security):

TelnetClients – *When the TelnetClients group exists, the Telnet service will allow only those users defined in the group to have access to the server.*

The group TelnetClients was not created on this server. The Telnet service is set to startup type **Manual** and is not currently running on this server. Port 23 is not open. Because the Telnet service could be started poses a degree of risk; therefore, the system administrator should either disable the Telnet service or create the TelnetClients group and add the names of the users that can use the service. The system administrators are using Terminal Services for remote administration. If Telnet is not used, it should be disabled.

3.2 Evidence and Findings from 2.2 (Ensure Guest Account is Disabled)

Evidence

Computer name:	WORKGROUP\		
IP address:			
Security report name:	WORKGROUP--\ (10-04-2004 2:55 PM)		
Scan date:	10/04/2004 2:55 PM		
Security update database version:	2004.9.14.0		
Security assessment:	Severe Risk (One or more critical checks failed.)		

Local Account Password Test	Some user accounts (1 of 12) have blank or simple passwords, or could not be analyzed.			
	User	Weak Password	Locked Out	Disabled
	Guest	Weak	-	Disabled
	IUSR_	-	-	-
	IWAM_	-	-	-
		-	-	-
	TsInternetUser	-	-	-
	backup	-	-	-
	commsadmin	-	-	-
		-	-	-
		-	-	-
		-	-	-
		-	-	-
	mangr	-	-	-

File System	All hard drives (2) are using the NTFS file system.		
	Drive Letter	File System	
	C:	NTFS	
	D:	NTFS	

Autologon	Autologon is not configured on this computer.
Guest Account	The Guest account is disabled on this computer.

Figure 5 – Microsoft Baseline Security Analysis of Guest

Findings:

The Guest Account is disabled. According to Microsoft, the Guest account is typically disabled at initial installation. Windows Baseline Security Analyzer determined the Guest account password to be “weak” which means it is no longer blank but is easily crackable. If a hacker was able to circumvent the perimeter security and gain access to the same subnet as the IIS server and run a password cracking tool, they could decipher the password in a short time.

I recommend that a system administrator enable the Guest account, change the password to something hard to guess, and disable the account again. Passwords should not be inserted into electronic documents stored on the system. Much of the

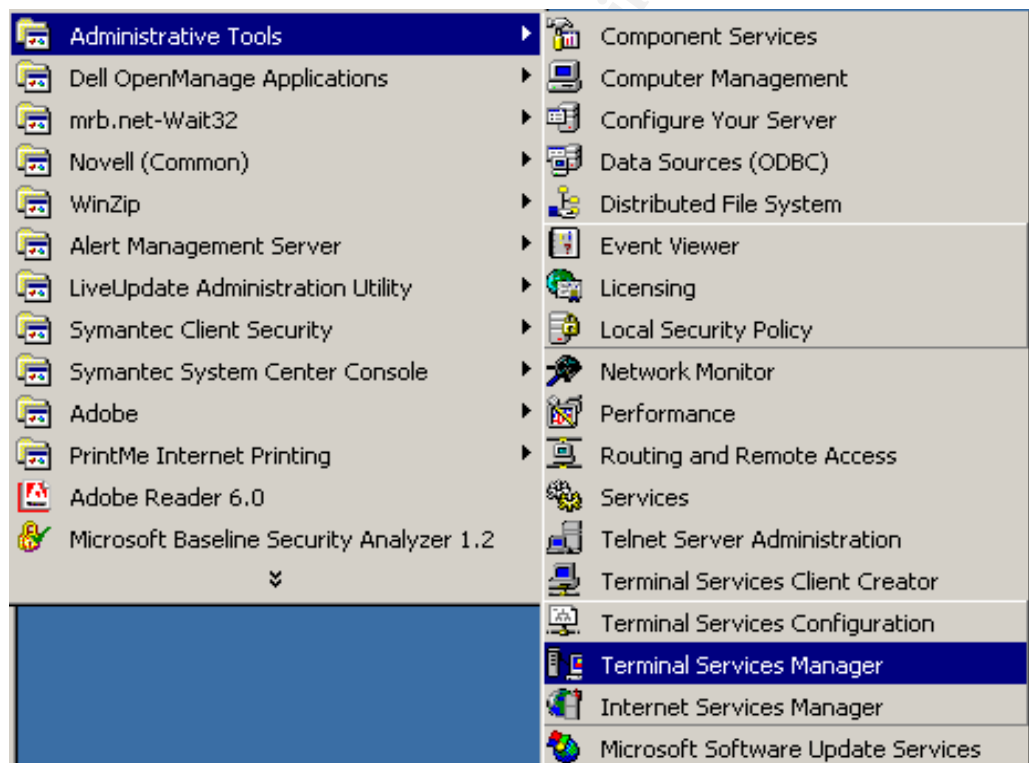
Trojan horse and zombie malware contains utilities that sift through information stored on the system, looking for confidential information to steal.

3.3 ***Evidence and Findings from 2.3 (Check for Unwanted Software)***

Evidence

List of installed software:



List of installed software (continued):**Figure 6 – List of Installed Software**List of installed computer components:**Figure 7 – Installed Computer Components****Findings:**

First, I marked the applications that I was familiar with:

From the Installed Software list:

- Adobe Acrobat Products – working with PDF files-

- Symantec - anti-virus protection.
- The IIS URLScan Tool is installed.
- VERITAS - backup utility.
- Microsoft Software Update Services (SUS) – Microsoft patch management.
- Outlook Express - email.
- Microsoft Baseline Security Analyzer – Test security controls.

From the Installed Components list

- Terminal Services
- Internet Information Services

I identified the applications that I was not familiar. I researched the following list of applications, familiarizing myself with their purpose:

From the Installed Software list:

- 3CDaemon – 3CDaemon is an FTP server developed by Dan Gill of 3Com. reportedly, it is possible to initiate a buffer overflow on a host running 3CDaemon. This is going to require further research to determine the extent of the vulnerability and if there is a patch available.²⁶
- AnswerWorks Runtime - AnswerWorks from Wextech Systems acquired by Vantage Software Technologies in September 2004, is a cross-lingual question and answering engine with an easy-to-use natural language interface that companies can add to "Help" systems and web-based knowledge repositories.²⁷ This interface allows users to search for and locate information by typing their requests in plain English. There don't seem to be any published security issues associated with the code.
- Mrb.net's Software – Wait32 - Wait32 is used in batch and command files to pause execution for the amount of time specified before executing the next line.²⁸ There don't seem to be any published security issues associated with the code.
- NICI (Shared) U.S./Worldwide (128 bit)(2.6.4-5) – Novell Cryptography Support Modules are implemented with the Novell International Cryptographic Infrastructure

²⁶ "3Com 3CDaemon Buffer Overflow Vulnerability, May 2, 2002, by Nikola Strahija." Xatrix Security web site. © 2004. URL: <http://www.xatrix.org/article.php?s=1453>.

²⁷ "Vantage Software Technologies Announces Acquisition of AnswerWorks™ Product Suite, September 15, 2004." Wextech web site. © 2004. URL: <http://www.wextech.com/awpr.htm>

²⁸ "Wait32, by Michael R. Bowler." mrb.net Software & Services web site. © 2004. URL: <http://www.mrb.net/software/free/wait32.html>.

(NICI) technology.²⁹ By downloading and installing the appropriate module, you enable NICI-based components (Novell Certificate Server, Novell SSL, Novell Single Sign-on, etc) to use an appropriate level of cryptography. This includes the use of unlimited strength cryptography or up to 56-bit DES/RC2/RC4 data encryption³⁰ and 1024-bit RSA* key management strength for worldwide users (where allowed by local law). There is a published OpenSSL security issue associated with NICI 2.6.1 and greater discussed under Item 2.10 "Evaluate Other Installed Software Products for Vulnerabilities."

From the Control Panel Configurable Components list

- PrintMe Internet Printing – This component is for wide area network printing and for wireless printing. Neither of which probably need to be performed from this server. However, this component is bundled with Adobe Acrobat 6 and gets installed by default. There is instruction out on the Internet to not install it, somewhat complex--the average system administrator is probably not going to bother. Acrobat has published security issues, but none are in regard to PrintMe.

²⁹ "NISCC vulnerability advisory on SSL (secure sockets layer) and TLS (transport layer security) protocols, August 3, 2004." Novell web site. © 2004. URL: <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087450.htm>.

³⁰ "NICI Encryption Modules." Novell web site. © 2004. URL: <http://www.novell.com/products/cryptography/>

3.4 Evidence and Findings from 2.4 (Are Any Trojans Listening on Open Ports?)

Evidence:

Results from *nMap.exe*:

```
# Nmap run completed at Fri Oct 08 15:48:11 2004 -- 1 IP address (1 host up) scanned in 52.906 seconds
# nmap 3.50 scan initiated Fri Oct 08 15:49:00 2004 as: nmap -sU -PT -PI -vv -T 3 -oN [REDACTED]7\acs.log
Interesting ports on [REDACTED]:
(The 1466 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
69/udp    open  tftp
137/udp    open  netbios-ns
138/udp    open  netbios-dgm
427/udp    open  svrloc
445/udp    open  microsoft-ds
500/udp    open  isakmp
514/udp    open  syslog
1028/udp   open  ms-lsa
2967/udp   open  symantec-av
3456/udp   open  iisrpc-or-vat
38037/udp  open  landesk-cba
38293/udp  open  landesk-cba

# nmap 3.50 scan initiated Fri Oct 08 15:50:41 2004 as: nmap -sR -PT -PI -vv -T 3 -oN [REDACTED]7\acs.log
Interesting ports on [REDACTED]:
(The 1640 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp
80/tcp    open  http
82/tcp    open  xfer
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
427/tcp   open  svrloc
443/tcp   open  https
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1030/tcp  open  iadl
1033/tcp  open  netinfo
3000/tcp  open  ppp
3001/tcp  open  nessusd
3372/tcp  open  msdtc
3389/tcp  open  ms-term-serv
4000/tcp  open  remoteanything
6003/tcp  open  X11:3
10000/tcp open  snet-sensor-mgmt
38292/tcp open  landesk-cba
```

Figure 8 – nMap Listing

Results from *netstat.exe /a*:

Active Connections

Proto	Local Address	Foreign Address	State
TCP	AgencyXYZ:ftp	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:http	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:82	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:epmap	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:https	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:microsoft-ds	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1025	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1030	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1033	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1046	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1063	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1067	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1070	AgencyXYZ:0	LISTENING

TCP	AgencyXYZ:1549	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1647	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1810	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1811	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1995	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:2402	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:2446	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:2453	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:2454	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:2542	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:2624	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3000	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3001	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3201	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3202	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3263	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3276	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3372	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3389	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3711	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4000	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4001	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4002	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4152	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4186	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4187	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4219	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4443	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4808	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4811	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:6003	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:6200	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:7777	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:7778	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:10000	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:12174	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:38292	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1039	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1067	AgencyXYZ:6100	ESTABLISHED
TCP	AgencyXYZ:2453	AgencyXYZ:6100	ESTABLISHED
TCP	AgencyXYZ:2454	AgencyXYZ:6100	ESTABLISHED
TCP	AgencyXYZ:2624	AgencyXYZ:6100	ESTABLISHED
TCP	AgencyXYZ:3101	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3102	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:4136	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4149	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4159	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4173	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4183	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4189	AgencyXYZ:microsoft-ds	TIME_WAIT
TCP	AgencyXYZ:4196	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4206	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4215	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:4227	AgencyXYZ:6100	TIME_WAIT
TCP	AgencyXYZ:6100	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:6100	AgencyXYZ:1067	ESTABLISHED
TCP	AgencyXYZ:6100	AgencyXYZ:2453	ESTABLISHED
TCP	AgencyXYZ:6100	AgencyXYZ:2454	ESTABLISHED
TCP	AgencyXYZ:6100	AgencyXYZ:2624	ESTABLISHED
TCP	AgencyXYZ:6100	AgencyXYZ:4137	TIME_WAIT
TCP	AgencyXYZ:6100	AgencyXYZ:4180	TIME_WAIT
TCP	AgencyXYZ:6100	AgencyXYZ:4218	TIME_WAIT
TCP	AgencyXYZ:netbios-ssn	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:427	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1046	AgencyXYZ:1748	ESTABLISHED
TCP	AgencyXYZ:1549	AgencyXYZ:524	ESTABLISHED
TCP	AgencyXYZ:1647	xxx.xx.xxx.xxx:http	ESTABLISHED
TCP	AgencyXYZ:1748	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1748	AgencyXYZ:1046	ESTABLISHED
TCP	AgencyXYZ:1754	AgencyXYZ:0	LISTENING

TCP	AgencyXYZ:1808	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1809	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:1995	AgencyXYZ:524	ESTABLISHED
TCP	AgencyXYZ:2402	AgencyXYZ:7778	CLOSE_WAIT
TCP	AgencyXYZ:2446	AgencyXYZ:7778	CLOSE_WAIT
TCP	AgencyXYZ:2542	AgencyXYZ:3000	ESTABLISHED
TCP	AgencyXYZ:3000	AgencyXYZ:2542	ESTABLISHED
TCP	AgencyXYZ:3001	AgencyXYZ:3263	ESTABLISHED
TCP	AgencyXYZ:3017	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3101	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3102	AgencyXYZ:0	LISTENING
TCP	AgencyXYZ:3263	AgencyXYZ:3001	ESTABLISHED
TCP	AgencyXYZ:3276	AgencyXYZ:524	ESTABLISHED
TCP	AgencyXYZ:3389	AgencyXYZ:1417	ESTABLISHED
TCP	AgencyXYZ:3711	AgencyXYZ:7778	CLOSE_WAIT
TCP	AgencyXYZ:4002	AgencyXYZ:4167	TIME_WAIT
TCP	AgencyXYZ:4002	AgencyXYZ:4168	TIME_WAIT
TCP	AgencyXYZ:4002	AgencyXYZ:4169	TIME_WAIT
TCP	AgencyXYZ:4002	AgencyXYZ:4170	TIME_WAIT
TCP	AgencyXYZ:4152	AgencyXYZ:7778	ESTABLISHED
TCP	AgencyXYZ:4186	AgencyXYZ:524	ESTABLISHED
TCP	AgencyXYZ:4187	AgencyXYZ:524	ESTABLISHED
TCP	AgencyXYZ:4203	AgencyABC:netbios-ssn	TIME_WAIT
TCP	AgencyXYZ:4219	AgencyXYZ:7778	ESTABLISHED
TCP	AgencyXYZ:4808	AgencyXYZ:7778	CLOSE_WAIT
TCP	AgencyXYZ:4811	AgencyXYZ:7778	CLOSE_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4140	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4141	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4155	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4156	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4164	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4165	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4178	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4179	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4192	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4193	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4201	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4202	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4211	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4212	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4222	TIME_WAIT
TCP	AgencyXYZ:6200	AgencyXYZ:4223	TIME_WAIT
TCP	AgencyXYZ:7778	AgencyXYZ:4081	TIME_WAIT
TCP	AgencyXYZ:7778	AgencyXYZ:4152	ESTABLISHED
TCP	AgencyXYZ:7778	AgencyXYZ:4219	ESTABLISHED
UDP	AgencyXYZ:tftp	*:*	
UDP	AgencyXYZ:microsoft-ds	*:*	
UDP	AgencyXYZ:syslog	*:*	
UDP	AgencyXYZ:1027	*:*	
UDP	AgencyXYZ:1028	*:*	
UDP	AgencyXYZ:1062	*:*	
UDP	AgencyXYZ:2148	*:*	
UDP	AgencyXYZ:2967	*:*	
UDP	AgencyXYZ:3456	*:*	
UDP	AgencyXYZ:38037	*:*	
UDP	AgencyXYZ:38293	*:*	
UDP	AgencyXYZ:netbios-ns	*:*	
UDP	AgencyXYZ:netbios-dgm	*:*	
UDP	AgencyXYZ:427	*:*	
UDP	AgencyXYZ:isakmp	*:*	
UDP	AgencyXYZ:1026	*:*	

Figure 9 – Netstat Listing

Findings:

When I compared the list of known Trojan ports to my open port list, the following ports matched: TCP - 21, 80, 135, 139, 445, 1025, 3000, 4000, 4001, 7777, 10000; UDP – 137, 138, 3456. The open ports which are frequently exploited by Trojan horses will require additional evaluation to make sure the reason for being open is legitimate. Under Item 3.6 I cross reference open ports to processes to services which will help determine the legitimacy of the software using these ports. Any questionable processes running on any of the identified ports will be identified under Item 3.6.

3.5 Evidence and Findings from 2.5 (Are Unneeded Services Running?)

Evidence:

PsService v2.12 - local and remote services viewer/controller
 Copyright (C) 2001-2004 Mark Russinovich
 Sysinternals - www.sysinternals.com

SERVICE_NAME: Alerter [3]
 DISPLAY_NAME: Alerter
 Notifies selected users and computers of administrative alerts.
 TYPE : 20 WIN32_SHARE_PROCESS
 STATE : 1 STOPPED
 (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
 WIN32_EXIT_CODE : 1077 (0x435)
 SERVICE_EXIT_CODE : 0 (0x0)
 CHECKPOINT : 0x0
 WAIT_HINT : 0x0

SERVICE_NAME: AppMgmt [2]
 DISPLAY_NAME: Application Management
 Provides software installation services such as Assign, Publish, and Remove.
 TYPE : 20 WIN32_SHARE_PROCESS
 STATE : 4 RUNNING
 (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
 WIN32_EXIT_CODE : 0 (0x0)
 SERVICE_EXIT_CODE : 0 (0x0)
 CHECKPOINT : 0x0
 WAIT_HINT : 0x0

SERVICE_NAME: Ati HotKey Poller [1]
 DISPLAY_NAME: Ati HotKey Poller
 (null)

(Note: Since the service details were not contributing to this paper, they were deleted to save space

SERVICE_NAME: BackupExecAgentAccelerator [1]
 DISPLAY_NAME: Backup Exec Remote Agent for Windows Servers
 Increases backup performance of remote Windows Servers systems by compressing the data to be backed up.

SERVICE_NAME: BITS [3]
 DISPLAY_NAME: 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.

SERVICE_NAME: Browser [1]
 DISPLAY_NAME: Computer Browser

Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.

SERVICE_NAME: cisvc [1]
DISPLAY_NAME: Indexing Service
Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.

SERVICE_NAME: ClipSrv [3]
DISPLAY_NAME: ClipBook
Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.

SERVICE_NAME: cusrv [1]
DISPLAY_NAME: Client Update Service for Novell
(null)

SERVICE_NAME: dcevt32 [1]
DISPLAY_NAME: Dell OpenManage Server Agent Event Monitor
(null)

SERVICE_NAME: dcstor32 [1]
DISPLAY_NAME: Dell OpenManage Server Agent
(null)

SERVICE_NAME: DefWatch [1]
DISPLAY_NAME: DefWatch
(null)

SERVICE_NAME: Dfs [1]
DISPLAY_NAME: Distributed File System
Manages logical volumes distributed across a local or wide area network.

SERVICE_NAME: Dhcp [1]
DISPLAY_NAME: DHCP Client
Manages network configuration by registering and updating IP addresses and DNS names.

SERVICE_NAME: Diskeeper [1]
DISPLAY_NAME: Diskeeper
Controls the Diskeeper Service

SERVICE_NAME: dmserver [5]
DISPLAY_NAME: Logical Disk Manager
Logical Disk Manager Watchdog Service

SERVICE_NAME: Dnscache [1]
DISPLAY_NAME: DNS Client
Resolves and caches Domain Name System (DNS) names.

SERVICE_NAME: Eventlog [1]
DISPLAY_NAME: 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.

SERVICE_NAME: EventSystem [2]
DISPLAY_NAME: COM+ Event System
Provides automatic distribution of events to subscribing COM components.

SERVICE_NAME: Fax [3]
DISPLAY_NAME: Fax Service
Helps you send and receive faxes

SERVICE_NAME: FLEXlm Service 1 [3]
DISPLAY_NAME: FLEXlm Service 1
(null)

SERVICE_NAME: IISADMIN [1]
DISPLAY_NAME: IIS Admin Service
Allows administration of Web and FTP services through the Internet Information Services snap-in.

SERVICE_NAME: Intel Alert Handler [1]

DISPLAY_NAME: Intel Alert Handler
(null)

SERVICE_NAME: Intel Alert Originator [1]
DISPLAY_NAME: Intel Alert Originator
(null)

SERVICE_NAME: Intel File Transfer [1]
DISPLAY_NAME: Intel File Transfer
(null)

SERVICE_NAME: Intel PDS [1]
DISPLAY_NAME: Intel PDS
(null)

SERVICE_NAME: IsmServ [5]
DISPLAY_NAME: Intersite Messaging
Allows sending and receiving messages between Windows Advanced Server sites.

SERVICE_NAME: kdc [5]
DISPLAY_NAME: Kerberos Key Distribution Center
Generates session keys and grants service tickets for mutual client/server authentication.

SERVICE_NAME: lanmanserver [1]
DISPLAY_NAME: Server
Provides RPC support and file, print, and named pipe sharing.

SERVICE_NAME: lanmanworkstation [1]
DISPLAY_NAME: Workstation
Provides network connections and communications.

SERVICE_NAME: LicenseService [1]
DISPLAY_NAME: License Logging Service
(null)

SERVICE_NAME: LmHosts [1]
DISPLAY_NAME: TCP/IP NetBIOS Helper Service
Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.

SERVICE_NAME: Messenger [1]
DISPLAY_NAME: Messenger
Sends and receives messages transmitted by administrators or by the Alerter service.

SERVICE_NAME: mnmsrvc [3]
DISPLAY_NAME: NetMeeting Remote Desktop Sharing
Allows authorized people to remotely access your Windows desktop using NetMeeting.

SERVICE_NAME: mr2kserv [1]
DISPLAY_NAME: mr2kserv
(null)

SERVICE_NAME: MSDTC [1]
DISPLAY_NAME: Distributed Transaction Coordinator
Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.

SERVICE_NAME: MSIInstaller [3]
DISPLAY_NAME: Windows Installer
Installs, repairs and removes software according to instructions contained in .MSI files.

SERVICE_NAME: NetDDE [3]
DISPLAY_NAME: Network DDE
Provides network transport and security for dynamic data exchange (DDE).

SERVICE_NAME: NetDDEdsdm [3]
DISPLAY_NAME: Network DDE DSDM
Manages shared dynamic data exchange and is used by Network DDE

SERVICE_NAME: Netlogon [3]
DISPLAY_NAME: Net Logon

Supports pass-through authentication of account logon events for computers in a domain.

SERVICE_NAME: Netman [2]

DISPLAY_NAME: Network Connections

Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.

SERVICE_NAME: Norton AntiVirus Server [1]

DISPLAY_NAME: Symantec AntiVirus Server

Provides real-time virus scanning, reporting, and management functionality for Symantec Client Security.

SERVICE_NAME: NSCTOP [1]

DISPLAY_NAME: Symantec System Center Discovery Service
(null)

SERVICE_NAME: NtFrs [3]

DISPLAY_NAME: File Replication

Maintains file synchronization of file directory contents among multiple servers.

SERVICE_NAME: NtLmSsp [3]

DISPLAY_NAME: NT LM Security Support Provider

Provides security to remote procedure call (RPC) programs that use transports other than named pipes.

SERVICE_NAME: NtmsSvc [3]

DISPLAY_NAME: Removable Storage

Manages removable media, drives, and libraries.

SERVICE_NAME: OracleOra9ias_homeAgent [1]

DISPLAY_NAME: OracleOra9ias_homeAgent
(null)

SERVICE_NAME: OracleOra9ias_homeEMWebsite [1]

DISPLAY_NAME: OracleOra9ias_homeEMWebsite
(null)

SERVICE_NAME: OracleOra9ias_homeProcessManager [1]

DISPLAY_NAME: OracleOra9ias_homeProcessManager
(null)

SERVICE_NAME: OracleOra9ias_homeWebCache [1]

DISPLAY_NAME: OracleOra9ias_homeWebCache
(null)

SERVICE_NAME: OracleOra9ias_homeWebCacheAdmin [4]

DISPLAY_NAME: OracleOra9ias_homeWebCacheAdmin
(null)

SERVICE_NAME: OracleOra9ias_homeWebCacheMon [3]

DISPLAY_NAME: OracleOra9ias_homeWebCacheMon
(null)

SERVICE_NAME: PlugPlay [1]

DISPLAY_NAME: Plug and Play

Manages device installation and configuration and notifies programs of device changes.

SERVICE_NAME: PolicyAgent [1]

DISPLAY_NAME: IPSEC Policy Agent

Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.

SERVICE_NAME: ProtectedStorage [1]

DISPLAY_NAME: Protected Storage

Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.

SERVICE_NAME: RasAuto [3]

DISPLAY_NAME: Remote Access Auto Connection Manager

Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.

SERVICE_NAME: RasMan [2]
DISPLAY_NAME: Remote Access Connection Manager
Creates a network connection.

SERVICE_NAME: RemoteAccess [5]
DISPLAY_NAME: Routing and Remote Access
Offers routing services to businesses in local area and wide area network environments.

SERVICE_NAME: RemoteRegistry [1]
DISPLAY_NAME: Remote Registry Service
Allows remote registry manipulation.

SERVICE_NAME: RpcLocator [3]
DISPLAY_NAME: Remote Procedure Call (RPC) Locator
Manages the RPC name service database.

SERVICE_NAME: RpcSs [1]
DISPLAY_NAME: Remote Procedure Call (RPC)
Provides the endpoint mapper and other miscellaneous RPC services.

SERVICE_NAME: RSVP [3]
DISPLAY_NAME: QoS RSVP
Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.

SERVICE_NAME: SamSs [1]
DISPLAY_NAME: Security Accounts Manager
Stores security information for local user accounts.

SERVICE_NAME: SCardDrv [3]
DISPLAY_NAME: Smart Card Helper
Provides support for legacy smart card readers attached to the computer.

SERVICE_NAME: SCardSvr [3]
DISPLAY_NAME: Smart Card
Manages and controls access to a smart card inserted into a smart card reader attached to the computer.

SERVICE_NAME: Schedule [1]
DISPLAY_NAME: Task Scheduler
Enables a program to run at a designated time.

SERVICE_NAME: seclogon [3]
DISPLAY_NAME: RunAs Service
Enables starting processes under alternate credentials

SERVICE_NAME: SENS [1]
DISPLAY_NAME: System Event Notification
Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.

SERVICE_NAME: Server Administrator [3]
DISPLAY_NAME: Server Administrator
(null)

SERVICE_NAME: SharedAccess [3]
DISPLAY_NAME: Internet Connection Sharing
Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.

SERVICE_NAME: SNMP [3]
DISPLAY_NAME: SNMP Service
Includes agents that monitor the activity in network devices and report to the network console workstation.

SERVICE_NAME: SNMPTRAP [3]
DISPLAY_NAME: SNMP Trap Service
Receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on this computer.

SERVICE_NAME: Spooler [1]

DISPLAY_NAME: Print Spooler
Loads files to memory for later printing.

SERVICE_NAME: SysmonLog [3]
DISPLAY_NAME: Performance Logs and Alerts
Configures performance logs and alerts.

SERVICE_NAME: TapiSrv [2]
DISPLAY_NAME: 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.

SERVICE_NAME: TermService [1]
DISPLAY_NAME: Terminal Services
Provides a multisection environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.

SERVICE_NAME: TlntSvr [3]
DISPLAY_NAME: Telnet
Allows a remote user to log on to the system and run console programs using the command line.

SERVICE_NAME: TrkSvr [3]
DISPLAY_NAME: Distributed Link Tracking Server
Stores information so that files moved between volumes can be tracked for each volume in the domain.

SERVICE_NAME: TrkWks [1]
DISPLAY_NAME: Distributed Link Tracking Client
Sends notifications of files moving between NTFS volumes in a network domain.

SERVICE_NAME: UPS [3]
DISPLAY_NAME: Uninterruptible Power Supply
Manages an uninterruptible power supply (UPS) connected to the computer.

SERVICE_NAME: UtilMan [3]
DISPLAY_NAME: Utility Manager
Starts and configures accessibility tools from one window

SERVICE_NAME: VxSvc [1]
DISPLAY_NAME: Disk Management Service
(null)

SERVICE_NAME: W32Time [3]
DISPLAY_NAME: Windows Time
Sets the computer clock.

SERVICE_NAME: W3SVC [1]
DISPLAY_NAME: World Wide Web Publishing Service
Provides Web connectivity and administration through the Internet Information Services snap-in.

SERVICE_NAME: WinMgmt [1]
DISPLAY_NAME: Windows Management Instrumentation
Provides system management information.

SERVICE_NAME: WMDM PMSP Service [1]
DISPLAY_NAME: WMDM PMSP Service
(null)

SERVICE_NAME: Wmi [2]
DISPLAY_NAME: Windows Management Instrumentation Driver Extensions
Provides systems management information to and from drivers.

SERVICE_NAME: wuauserv [1]
DISPLAY_NAME: 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.

SERVICE_NAME: WUSyncService [1]
DISPLAY_NAME: Software Update Services Synchronization Service

Enables Software Update Services to synchronize select content with the Microsoft Windows Update web site.

SERVICE_NAME: WZCSVC [3]

DISPLAY_NAME: Wireless Configuration

Provides authenticated network access control using IEEE 802.1x for wired and wireless Ethernet networks.

SERVICE_NAME: xsSmartAgent [3]

DISPLAY_NAME: Visibroker Smart Agent

(null)

Findings:

I prefer to use **psservice.exe** to cross reference the list that can be exported from the Services utility. because of the good description field. I determined which services were [1] running/automatic, [2] running/manual, [3] stopped/manual, [4] stopped/automatic and [5] disabled by this color scheme. Successful Trojan exploits now include hijacking the SYSTEM or Administrator account to gain the necessary access privileges to run malware that can start services that are in a Manual startup state. Services that are not being used should be disabled. This may become an inconvenience down the road, as the system administrator installs other software and receives errors until needed services are enabled. Guidance recommends that services be disabled, not deleted. I have put together a list of services below, I am recommending be disabled. There are 91 services on this **psservice.exe** listing. Only 4 are disabled. I recommend the system administrator review this list and consider disabling more services.³³ These recommendations are based on industry guidance.⁴⁴ The system administrator would need to determine whether any of the installed software products were dependent upon any of these services:

Services ³¹	Communications Protocols
Alerter	NetBIOS Interface
BITS	NWLink NetBIOS
ClipBook Server	NWLink IPX/SPX Compatible Transport
Computer Browser	Simple TCP/IP Services
DHCP Client	WINS Client (TCP/IP)
Distributed Link Tracking Client	
Fax Service	
Network DDE DSDM	
Performance Logs and Alerts	
Remote Access Services	
QOS RSVP	

³¹ "Glossary of Windows 2000 Services, July 31, 2001." Microsoft web site. © 2004. URL: <http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp>.

Services ³¹	Communications Protocols
Remote Registry Service	
Smart Card	
Smart Card Helper	
Spooler	
Telnet	
TCP/IP NetBIOS Helper	
Telephony Service	
Uninterruptible Power Supply	
Windows Time	
Wireless Configuration	

Table 7 – Suggested List of Services to be Disabled

3.6 Evidence and Findings from 2.6 (Cross Reference Processes to Ports and Services)

Evidence:

Results from the **tlist.exe** to list the running PID and Processes

0 System Process	496 mstask.exe	
8 System	1624 VxSvc.exe	
212 SMSS.EXE	1736 WinMgmt.exe	
232 CSRSS.EXE	1808 MsPMSPSV.exe	
228 WINLOGON.EXE	1824 svchost.exe	
284 SERVICES.EXE	1892 WUSyncSvc.exe	
296 LSASS.EXE	1336 java.exe	
404 termsrv.exe	1896 perl.exe	
492 svchost.exe	1976 beremote.exe	
588 spoolsv.exe	2140 dfssvc.exe	
616 msdtc.exe	2176 HNDLRVC.EXE	
736 ati2plxx.exe	2188 MSGSYS.EXE	
748 cisvc.exe	2260 IAO.EXE	
760 cusrv.exe	2280 XFR.EXE	
772 dcevt32.exe	800 svchost.exe	
788 dcstor32.exe	408 svchost.exe	
840 DefWatch.exe	1588 DLLHOST.EXE	
856 DKService.exe	3440 DLLHOST.EXE	
872 inetinfo.exe	3436 Apache.exe	
892 pds.exe	1044 3CDaemon.EXE	
944 LLSSRV.EXE	4676 Apache.exe	
976 mr2kserv.exe	1576 javaw.exe	
1056 Rtvscan.exe	2052 javaw.exe	
1100 NscTop.exe	4432 logon.scr	
1332 agntrsv.exe	3928 cidaemon.exe	
1348 nmentsrv.exe	3712 cidaemon.exe	
1360 opmn.exe	4180 CSRSS.EXE	
1372 CMD.EXE	3656 WINLOGON.EXE	NetDDE Agent
1388 opmn.exe	4292 rdpclip.exe	CB Monitor Window
1408 webcached.exe	4660 explorer.exe	Program Manager
1416 CMD.EXE	4024 nwtray.exe	NetWareProviderIcons
1432 dbnmp.exe	4640 dpmw32.exe	DPMW32.EXE Main
1468 webcached.exe	Window	
1484 regsvc.exe	2044 CMD.EXE	
12128 tlist.exe	C:\WINNT\system32\cmd.exe - tlist.exe	

Results from **fport.exe** which cross-reference process ID, process, and port:

FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
<http://www.foundstone.com>

Pid	Process	Port	Proto	Path
1044	3Cdaemon	-> 21	TCP	C:\PROGRA~1\3Com\3Cdaemon\3Cdaemon.EXE
872	inetinfo	-> 80	TCP	C:\WINNT\system32\inetrv\inetinfo.exe
872	inetinfo	-> 82	TCP	C:\WINNT\system32\inetrv\inetinfo.exe
492	svchost	-> 135	TCP	C:\WINNT\system32\svchost.exe
8	system	-> 139	TCP	
8	system	-> 427	TCP	
872	inetinfo	-> 443	TCP	C:\WINNT\system32\inetrv\inetinfo.exe
8	system	-> 445	TCP	
616	msdtc	-> 1025	TCP	C:\WINNT\system32\msdtc.exe
1496	MSTask	-> 1030	TCP	C:\WINNT\system32\MSTask.exe
872	inetinfo	-> 1033	TCP	C:\WINNT\system32\inetrv\inetinfo.exe
2280	xfr	-> 1039	TCP	C:\WINNT\system32\cba\xfr.exe
1332	agntsrvc	-> 1046	TCP	D:\ora9ias\bin\agntsrvc.exe
8	system	-> 1063	TCP	
1336	java	-> 1067	TCP	D:\ora9ias\jdk\bin\java.exe
1336	java	-> 1070	TCP	D:\ora9ias\jdk\bin\java.exe
8	system	-> 1549	TCP	
1892	wusyncSvc	-> 1647	TCP	D:\SUS\wusync\WUSyncSvc.exe
1432	dbnmp	-> 1748	TCP	D:\ora9ias\bin\dbnmp.exe
1432	dbnmp	-> 1754	TCP	D:\ora9ias\bin\dbnmp.exe
1432	dbnmp	-> 1808	TCP	D:\ora9ias\bin\dbnmp.exe
1432	dbnmp	-> 1809	TCP	D:\ora9ias\bin\dbnmp.exe
1336	java	-> 1810	TCP	D:\ora9ias\jdk\bin\java.exe
1336	java	-> 1811	TCP	D:\ora9ias\jdk\bin\java.exe
8	system	-> 1995	TCP	
1336	java	-> 2402	TCP	D:\ora9ias\jdk\bin\java.exe
1336	java	-> 2446	TCP	D:\ora9ias\jdk\bin\java.exe
1576	javaw	-> 2453	TCP	D:\ora9ias\jdk\bin\javaw.exe
2052	javaw	-> 2454	TCP	D:\ora9ias\jdk\bin\javaw.exe
4676	apache	-> 2542	TCP	D:\ora9ias\Apache\Apache\apache.exe
4676	apache	-> 2624	TCP	D:\ora9ias\Apache\Apache\apache.exe
1576	javaw	-> 3000	TCP	D:\ora9ias\jdk\bin\javaw.exe
2052	javaw	-> 3001	TCP	D:\ora9ias\jdk\bin\javaw.exe
4640	dpmw32	-> 3017	TCP	C:\WINNT\system32\dpmw32.exe
2052	javaw	-> 3101	TCP	D:\ora9ias\jdk\bin\javaw.exe
1576	javaw	-> 3102	TCP	D:\ora9ias\jdk\bin\javaw.exe
2052	javaw	-> 3201	TCP	D:\ora9ias\jdk\bin\javaw.exe
1576	javaw	-> 3202	TCP	D:\ora9ias\jdk\bin\javaw.exe
4676	apache	-> 3263	TCP	D:\ora9ias\Apache\Apache\apache.exe
8	system	-> 3276	TCP	

8	System	->	3276	TCP	
616	msdtc	->	3372	TCP	C:\WINNT\System32\msdtc.exe
404	termsrv	->	3389	TCP	C:\WINNT\System32\termsrv.exe
1408	webcached	->	3711	TCP	D:\ora9ias\bin\webcached.exe
1468	webcached	->	4000	TCP	D:\ora9ias\bin\webcached.exe
1408	webcached	->	4001	TCP	D:\ora9ias\bin\webcached.exe
1408	webcached	->	4002	TCP	D:\ora9ias\bin\webcached.exe
1388	opmn	->	4152	TCP	D:\ora9ias\opmn\bin\opmn.exe
8	System	->	4186	TCP	
8	System	->	4187	TCP	
1336	java	->	4311	TCP	D:\ora9ias\jdk\bin\java.exe
1408	webcached	->	4443	TCP	D:\ora9ias\bin\webcached.exe
1336	java	->	4808	TCP	D:\ora9ias\jdk\bin\java.exe
1336	java	->	4811	TCP	D:\ora9ias\jdk\bin\java.exe
1388	opmn	->	6003	TCP	D:\ora9ias\opmn\bin\opmn.exe
1388	opmn	->	6100	TCP	D:\ora9ias\opmn\bin\opmn.exe
1388	opmn	->	6200	TCP	D:\ora9ias\opmn\bin\opmn.exe
1408	webcached	->	7777	TCP	D:\ora9ias\bin\webcached.exe
4676	apache	->	7778	TCP	D:\ora9ias\Apache\Apache\apache.exe
1976	beremote	->	10000	TCP	C:\Program Files\VERITAS\Backup Exec\RANT\beremote.exe
2280	xfr	->	12174	TCP	C:\WINNT\system32\cba\xfr.exe
2188	MsgSys	->	38292	TCP	C:\WINNT\system32\MsgSys.EXE
1044	3CDaemon	->	69	UDP	C:\PROGRA~1\3Com\3CDaemon\3CDaemon.EXE
8	System	->	137	UDP	
8	System	->	138	UDP	
8	System	->	427	UDP	
8	System	->	445	UDP	
296	lsass	->	500	UDP	C:\WINNT\system32\lsass.exe
1044	3CDaemon	->	514	UDP	C:\PROGRA~1\3Com\3CDaemon\3CDaemon.EXE
8	System	->	1026	UDP	
1100	NSCTOP	->	1027	UDP	D:\PROGRA~1\Symantec\SYMANT~1\NSCTOP.EXE
1100	NSCTOP	->	1028	UDP	D:\PROGRA~1\Symantec\SYMANT~1\NSCTOP.EXE
588	spoolsv	->	1062	UDP	C:\WINNT\system32\spoolsv.exe
1624	vxsvc	->	2148	UDP	C:\Program Files\Dell\OpenManage\Array Manager\vxSvc.exe
1056	Rtvscan	->	2967	UDP	D:\PROGRA~1\sav\Rtvscan.exe
872	inetinfo	->	3456	UDP	C:\WINNT\system32\inetinfo.exe
2188	MsgSys	->	38037	UDP	C:\WINNT\system32\MsgSys.EXE
892	pds	->	38293	UDP	C:\WINNT\system32\cba\pds.exe

Figure 10 – Fport Listing

Findings:

I combined the data from the task listing, **fport** report, and services³² listing into a cross reference table (because there is no utility that will do this for me) to see if there are any correlations. Those port used by Trojans were marked. I validated the processes listening on those ports as legitimate software installations. This table proves to be a good diagram of the system.

³² "Port Requirements for Windows Systems." lair.moria.org web site. © 2004. URL: http://lair.moria.org/blog/Security/Port_Requirements_for_Microsoft_Windows_Server_System.htm

Cross Reference Chart Process ID, Process, Port, Service			
PID	Process	Port	Service ³³
8	System	137 UDP ³⁴ [Legit.]	[Service Name] Browser [Display Name] Computer Browser (svchost.exe) [Service Name] lanmanserver [Display Name] Server (svchost.exe)
		138 UDP [Legit.]	[Service Name] Browser [Display Name] Computer Browser (svchost.exe) [Service Name] Messenger [Display Name] Messenger (service.exe) [Service Name] lanmanserver [Display Name] Server (svchost.exe) [Service Name] Dfs [Display Name] Distributed File System (dfssvc.exe) [Service Name] LicenseService [Display Name] License Logging Service (llsrv.exe)
		139 TCP [Legit.]	[Service Name] Browser [Display Name] Computer Browser (svchost.exe) [Service Name] Spooler [Display Name] Print Spooler (spoolsv.exe) [Service Name] Server [Display Name] lanmanserver (svchost.exe) [Service Name] Dfs [Display Name] Distributed File System (dfssvc.exe) [Service Name] LicenseService

³³ "Black Viper's Windows 2000 Professional and Server Service Configurations". Black Viper web site. © 2004. URL: <http://www.blackviper.com/WIN2K/servicecfg.htm>

³⁴ "Window Networking/NetBIOS/SMB/CIFS." Keyfocus web site. © 2004. URL: http://www.keyfocus.net/kfsensor/help/AdminGuide/adm_NBT.php

Cross Reference Chart Process ID, Process, Port, Service			
PID	Process	Port	Service ³³
			[Display Name] License Logging Service (llssrv.exe)
		427 TCP 427 UDP	
		445 TCP [Legit.] 445 UDP	[Service Name] LicenseService [Display Name] License Logging Service (llssrv.exe) [Service Name] Spooler [Display Name] Print Spooler (spoolsv.exe) [Service Name] lanmanserver [Display Name] Server (svchost.exe) [Service Name] Dfs [Display Name] Distributed File System (dfssvc.exe)
		1026 UDP 1063 TCP 1549 TCP 1995 TCP 3276 TCP 4186 TCP 4187 TCP	
212	SMSS		[Service Name] SamSs [Display Name] Security Accounts Manager (lsass.exe)
228	WINLOGON		
232	CSRSS		
284	Services		[[Service Name] PlugPlay [Display Name] Plug and Play (services.exe)
296	lsass	500 UDP	[Service Name] Policy Agent [Display Name] IPSEC Policy (lsass.exe)
404	termsrv	3389 TCP	[Service Name] TermService [Display Name] Terminal Services (svchost.exe)
408	svchost		
492	svchost	135 TCP [Per IANA Port Listing, 135 is assigned to epmap. The <i>netstat</i> listing has the same assignment]	[Service Name] RpcSs [Display Name] Remote Procedure Call (svchost.exe) [Service Name] Dfs [Display Name] Distributed File System (dfssvc.exe) [Service Name] Eventlog

Cross Reference Chart Process ID, Process, Port, Service			
PID	Process	Port	Service ³³
			[Display Name] Event Log (services.exe)
588	spoolsv	1062 UDP	[Novell] (spoolsv.exe)
616	msdtc	1025 TCP ³⁵ [Legit.] 3372 TCP	[Service Name] MSDTC [Display Name] Distributed Transaction Coordinator (msdtc.exe)
736	ati2plxx		[Service Name] Ati HotKey Poller [Display Name] Ati Hotkey Poller (ati2plxx.exe)
748	cisvc		[Service Name] cisvc [Display Name] Indexing Service (cisvc.exe)
760	cusrv		[Service Name] cusrv [Display Name] Client Update Service for Novell (cusrv.exe)
772	Dcevt32		[Service Name] dcevt32 [Display Name] Dell OpenManage Server Agent Event Monitor (dcevt32.exe)
788	Dcstor32		[Service Name] dcstor32 [Display Name] Dell OpenManage Server Agent (dcstor32.exe)
800	svchost		
840	DefWatch		[Symantec] ³⁶ [Service Name] DefWatch [Display Name] DefWatch (DefWatch.exe)
856	DKService		[Service Name] Diskeeper [Display Name] Diskeeper (DKService.exe)
872	inetinfo		[IIS]
		80 TCP [Legit.]	[Service Name] W3SVC [Display Name] World Wide Web Publishing Service (inetinfo.exe)

³⁵ "What is msdtc.exe?" Neuber Software web site. © 2004. URL:
<http://www.neuber.com/taskmanager/process/msdtc.exe.html>.

³⁶ "Ports Used for Communication in Norton AntiVirus Corporate Edition." Symantec web site. ©2004
URL: <http://service1.symantec.com/SUPPORT/ent-security.nsf/pfdocs/2000101210181048>.

Cross Reference Chart Process ID, Process, Port, Service			
PID	Process	Port	Service ³⁷
		82 TCP 443 TCP 1033 TCP 3456 UDP ³⁷ [Legit.]	[Service Name] IISADMIN [Display Name] IIS Admin Service (inetinfo.exe)
892	pds	38292 TCP 38293 UDP	[Symantec] [Service Name] Intel PDS [Display Name] Intel PDS (pds.exe)
944	llssrv		[Service Name] LicenseService [Display Name] License Logging Service (llssrv.exe)
976	mr2kserv		[Dell Open Manage] [Service Name] mr2kserv [Display Name] mr2kserv (mr2kserv.exe)
1044	3CDaemon	21 TCP [Legit.] 69 UDP 514 UDP	(3CDaemon.exe)
1056	Rtvscan	2967 UDP	[Symantec] [Service Name] Norton AntiVirus Server [Display Name] Symantec AntiVirus Server (Rtvscan.exe)
1100	NSCTOP	1027 UDP 1028 UDP	[Symantec] [Service Name] NSCTOP [Display Name] Symantec System Center Discovery Service (NscTop.exe)
1332	agntsvr	1046 TCP	[Oracle] (agntsvr.exe)
1336	Java	1067 TCP 1070 TCP 1810 TCP 1811 TCP 2402 TCP 2446 TCP 4311 TCP 4808 TCP 4811 TCP	[Oracle] (java.exe)
1348	nmentsrv		[Oracle] (nmentsrv.exe)
1360	opmn		[Oracle] (opmn.exe)
1372	cmd		
1388	opmn	4152 TCP 6003 TCP	[Oracle] (opmn.exe)

³⁷ "Inetinfo Services Use Additional Ports Beyond Well-Known Ports, June 29, 2004." Microsoft web site.
© 2004. URL: <http://support.microsoft.com/default.aspx?scid=kb:en-us:327859>

Cross Reference Chart Process ID, Process, Port, Service			
PID	Process	Port	Service ³³
		6100 TCP 6200 TCP	
1408	Webcached	3711 TCP 4001 TCP [Legit.] 4002 TCP 4443 TCP 7777 TCP ³⁸ [Legit.]	[Oracle]
1416	cmd		
1432	dbsnmp	1748 TCP 1754 TCP 1808 TCP 1809 TCP	[Oracle] (dbsnmp.exe)
1468	webcached	4000 TCP [Legit.]	[Oracle] (webcached.exe)
1484	regsvc		[Service Name] RemoteRegistry [Display Name] Remote Registry Service (regsvc.exe)
1496	MSTask	1030 TCP	(mstask.exe)
1576	javaw	2453 TCP 3000 TCP [Legit.] 3102 TCP 3202 TCP	[Oracle] (javaw.exe)
1588	dllhost		[IIS]
1624	VxSvc	2148 UDP	[Dell Open Manager] [Service Name] VxSvc [Display Name] Disk Management Service (VxSvc.exe)
1736	winmgmt		
1808	mspmcsv		
1824	svchost		
1892	WUSyncSvc	1647 TCP	[Microsoft SUS] [Service Name] WUSyncService [Display Name] Software Update Services Synchronization Service
1896	perl		
1976	beremote	10000 TCP ³⁹	[Veritas]
2044	cmd		

³⁸ "Default Port Numbers and Port Ranges." Oracle web site. © 2004. URL:
<http://osi.oracle.com/CollaborationSuite9041/doc/install/ports.htm>.

³⁹ "Re: Port 10000, April 30, 2003." Email on a nessus.org server. © 2004. URL: "
<http://mail.nessus.org/pipermail/nessus/2003-April/msg00296.html>.

Cross Reference Chart Process ID, Process, Port, Service			
PID	Process	Port	Service ³³
2052	javaw	2454 TCP 3001 TCP 3101 TCP 3201 TCP	[Oracle]
2128	tlist		
2140	dfssvc		[Service Name] Dfs [Display Name] Distributed File System (dfssvc.exe)
2176	HNDLR SVC		
2188	MsgSys	38292 TCP 38037 UDP	[Symantec] (MSGSYS.EXE)
2260	IAO		
2280	xfr	1039 TCP 12174 TCP	[Symantec] (XFR.EXE)
3436	Apache		[Oracle] (Apache.exe)
3440	dllhost		[IIS]
3656	winlogon		(winlogon.exe)
3712	cidaemon		
3928	cidaemon		
4024	nwtray		[Novell]
4180	csrss		
4292	rdpclip		[Terminal Services]
4432	Logon.scr		
4640	dpmw32	3017 TCP	[Novell Print Services]
4660	explorer		
4676	apache	2542 TCP 2624 TCP 3263 TCP 7778 TCP	[Oracle]

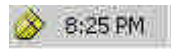
Green Color Scheme – Ports used by Trojans

Table 8 – Cross Reference Chart – Process ID, Process, Port, Service

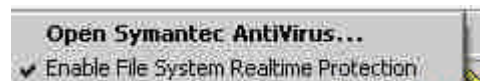
3.7 Evidence and Findings from 2.7 (Check for Virus Auto-Protection)

Evidence:

The server has the Symantec icon in the system tray which means an antivirus software is installed:



I also can tell if a virus shield is functioning in real-time mode by right-clicking on the Symantec icon and noting whether Enable File System Realtime Protection is checked.



Or I can go to the Symantec System Center and look at the File System Realtime Protection Status for this system:

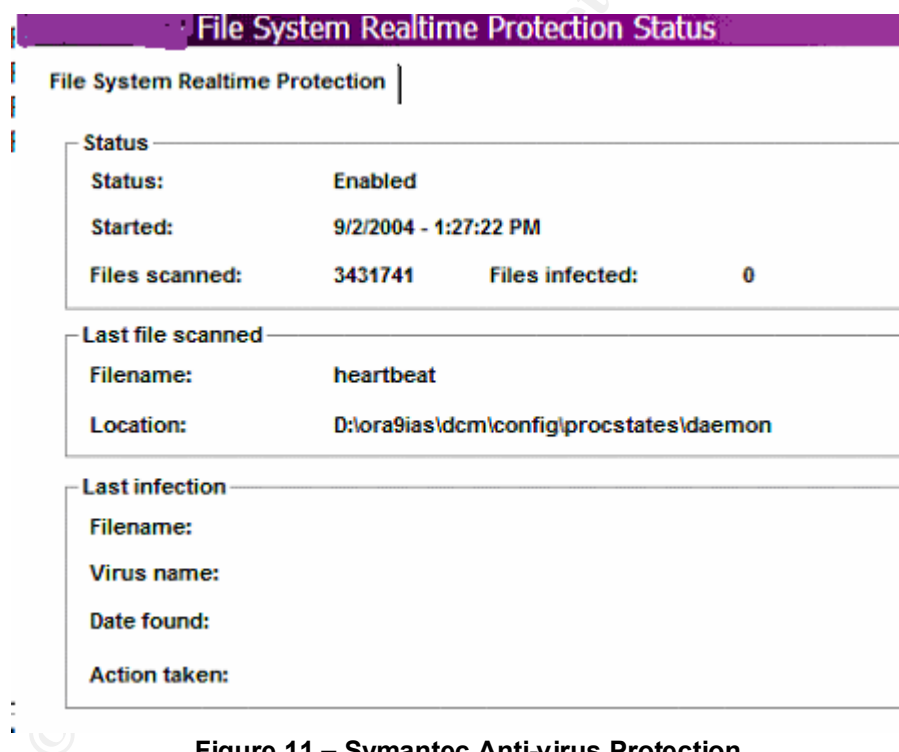


Figure 11 – Symantec Anti-virus Protection

Findings:

As display by the screenshots above, this system has Symantec Antivirus Server installed with realtime file system protection enabled. There are other ways to conclude this system is running Symantec: See Figure 6 – List of Installed Software, where we can see it is an installed program. Another example is to look at the Table 8 – Cross Reference Chart – Process ID, Process, Port, Service and note that open ports 1027

UDP, 1028 UDP, 1039 TCP, 2967 UDP, 12174 TCP, 38037 UDP, 38292 TCP, and 38293 UDP demonstrate that the program is running.⁴⁰

3.8 Evidence and Findings from 2.8 (Determine Whether Security Patching is Current)

Evidence:

Results from a **nessus.exe** port scan:

http (80/tcp)	Info	Service	Severity	Description
		microsoft-ds (445/tcp)	Info	Port is open
		NFS-or-IIS (1025/tcp)	Info	Port is open
		loc-srv (135/tcp)	Info	Port is open
		https (443/tcp)	Info	Port is open
		http (80/tcp)	Info	Port is open
		ftp (21/tcp)	Info	Port is open
		krb524 (4444/tcp)	Info	Port is open
		netbios-ssn (139/tcp)	Info	Port is open
		svrloc (427/tcp)	Info	Port is open
		microsoft-ds (445/tcp)	Low	<p>The host Security Identifier (SID) can be obtained remotely. Its value is :</p> <p>AGENCYXYZ : 5-21-854245398-1844823847-725345543</p> <p>An attacker can use it to obtain the list of the local users of this host</p> <p>Solution : filter the ports 137-139 and 445</p> <p>Risk factor : Low</p> <p>CVE : CVE-2000-1200</p> <p>BID : 959</p>
		loc-srv (135/tcp)	Low	<p>Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.</p>

			<p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Solution : filter incoming traffic to this port.</p> <p>Risk factor : Low</p>
		netbios-ns (137/udp)	<p>Low</p> <p>The following 7 NetBIOS names have been gathered : AGENCYXYZ = This is the computer name registered for workstation services by a WINS client. AGENCYXYZ = Computer name WORKGROUP = Workgroup / Domain name AGENCYXYZ = This is the current logged in user registered for this workstation. INet~Services = Workgroup / Domain name (Domain Controller) IS~AGENCYXYZ WORKGROUP = Workgroup / Domain name (part of the Browser elections) The remote host has the following MAC address on its adapter : 00:09:xx:3f:16:xx</p> <p>If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port.</p> <p>Risk factor : Medium CVE : CAN-1999-0621</p>
		microsoft-ds (445/tcp)	<p>Low</p> <p>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 :</p> <ul style="list-style-type: none"> - Administrator account name : mangr (id 500) - Guest account name : Guest (id 501) - TsInternetUser (id 1000) - (id 1001) - commsadmin (id 1002) - (id 1004) - backup (id 1005) - (id 1006) - ORA_DBA (id 1008) - IUSR_AgencyXYZ (id 1012) - IWAM_AgencyXYZ (id 1013) - Web Anonymous Users (id 1014) - Web Applications (id 1015)

⁴¹ "Netinfo" Freedownloads center web site. © 2004. URL:
http://www.freedownloadscenter.com/Network_and_Internet/Internet_Client_Suites/NetInfo.html.

			<ul style="list-style-type: none"> (id 1016) (id 1017) <p>Risk factor : Medium Solution : filter incoming connections this port</p> <p>CVE : CVE-2000-1200 BID : 959</p>
	microsoft-ds (445/tcp)	Info	<p>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 : Agencygroup</p>
	NFS-or-IIS (1025/tcp)	Info	<p>Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.</p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Here is the list of DCE services running on this port:</p> <p>UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:xxx.xxx.xx.xxx[1025]</p> <p>UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:xxx.xxx.xx.xxx[1025]</p> <p>UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:xxx.xxx.xx.xxx[1025]</p> <p>UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:xxx.xxx.xx.xxx[1025]</p> <p>Solution : filter incoming traffic to this port. Risk factor : Low</p>
	ftp (21/tcp)	Info	<p>Remote FTP server banner : 220 3Com 3C Daemon FTP Server Version 2.0r</p>
	netinfo ⁴¹ (1033/tcp)	Info	<p>Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.</p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Here is the list of DCE services running on this port:</p>

			<p>UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2 Endpoint: ncacn_ip_tcp:xxx.xxx.xx.xxx[1033]</p> <p>Solution : filter incoming traffic to this port. Risk factor : Low</p>
	krb524 (4444/tcp)	Info	<p>The following directories were discovered: /_pages, /cgi-bin, /demo, /fcgi-bin, /icons, /oprocmgr-service</p> <p>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</p>
	microsoft-ds (445/tcp)	Info	<p>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</p> <p>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</p> <p>All the smb tests will be done as "/" in domain WORKGROUP CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 BID : 494, 990</p>
	krb524 (4444/tcp)	Info	<p>The remote web server type is :</p> <p>Oracle9iAS/9.0.3.1 Oracle HTTP Server</p> <p>Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.</p>
	http (80/tcp)	Info	<p>The remote web server type is :</p> <p>Microsoft-IIS/5.0r</p> <p>Solution : You can use urlscan to change reported server for IIS.</p>
	http (80/tcp)	Info	The following directories were discovered:

		<p>/shared</p> <p>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</p>
iad1 (1030/tcp)	Info	<p>Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.</p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Here is the list of DCE services running on this port:</p> <p>UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1 Endpoint: ncacn_ip_tcp:xxx.xxx.xx.xxx[1030] Named pipe : atsvc Win32 service or process : mstask.exe Description : Scheduler service</p> <p>UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1 Endpoint: ncacn_ip_tcp:xxx.xxx.xx.xxx[1030]</p> <p>Solution : filter incoming traffic to this port. Risk factor : Low</p>
netbios-ssn (139/tcp)	Info	An SMB server is running on this port
microsoft-ds (445/tcp)	Info	A CIFS server is running on this port
ftp (21/tcp)	Info	<p>An FTP server is running on this port. Here is its banner :</p> <p>220 3Com 3CDaemon FTP Server Version 2.0r</p>
general/tcp	Info	The remote host is running Microsoft Windows 2000 Server
krb524 (4444/tcp)	Info	A SSLv3 server answered on this port
krb524 (4444/tcp)	Info	A web server is running on this port through SSL
https (443/tcp)	Info	<p>An unknown service is running on this port. It is usually reserved for HTTPS</p> <p>A web server is running on this port</p>

Table 9 – Nessus Report

Results from **Microsoft Baseline Security Analyzer**:

Score	Issue	Result												
Check failed (non-critical)	Windows Media Player Security Updates	1 security updates are out-of-date. <table> <tr> <th>Security Update</th><th>Description</th><th>Reason</th></tr> <tr> <td>MS02-032</td><td>Cumulative Patch for Windows Media Player (Q320920)</td><td>File version is greater than expected. [\\xxx.xxx.xx.xxx\C\$\WINNT\system32\msdxm.ocx, 6.4.9.1128 > 6.4.9.1124]</td></tr> </table>	Security Update	Description	Reason	MS02-032	Cumulative Patch for Windows Media Player (Q320920)	File version is greater than expected. [\\xxx.xxx.xx.xxx\C\$\WINNT\system32\msdxm.ocx, 6.4.9.1128 > 6.4.9.1124]						
Security Update	Description	Reason												
MS02-032	Cumulative Patch for Windows Media Player (Q320920)	File version is greater than expected. [\\xxx.xxx.xx.xxx\C\$\WINNT\system32\msdxm.ocx, 6.4.9.1128 > 6.4.9.1124]												
Check failed (non-critical)	MSXML Security Updates	1 security updates are out-of-date. <table> <tr> <th>Security Update</th><th>Description</th><th>Reason</th></tr> <tr> <td>MSXML 3.0</td><td>MSXML 3.0 SP3</td><td>The latest service pack for this product is not installed. Currently SP3 is installed. The latest service pack is SP4.</td></tr> </table>	Security Update	Description	Reason	MSXML 3.0	MSXML 3.0 SP3	The latest service pack for this product is not installed. Currently SP3 is installed. The latest service pack is SP4.						
Security Update	Description	Reason												
MSXML 3.0	MSXML 3.0 SP3	The latest service pack for this product is not installed. Currently SP3 is installed. The latest service pack is SP4.												
Best practice	Windows Security Updates	3 security updates could not be confirmed. <table> <tr> <th>Security Update</th><th>Description</th><th>Reason</th></tr> <tr> <td>MS03-030</td><td>Unchecked Buffer in DirectX Could Enable System Compromise (819696)</td><td>Please refer to 306460 for a detailed explanation.</td></tr> <tr> <td>MS04-016</td><td>Vulnerability in DirectPlay Could Allow Denial of Service (839643)</td><td>Please refer to 306460 for a detailed explanation.</td></tr> <tr> <td>MS04-028</td><td>Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)</td><td>Please refer to 306460 for a detailed explanation.</td></tr> </table>	Security Update	Description	Reason	MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.	MS04-016	Vulnerability in DirectPlay Could Allow Denial of Service (839643)	Please refer to 306460 for a detailed explanation.	MS04-028	Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)	Please refer to 306460 for a detailed explanation.
Security Update	Description	Reason												
MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.												
MS04-016	Vulnerability in DirectPlay Could Allow Denial of Service (839643)	Please refer to 306460 for a detailed explanation.												
MS04-028	Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)	Please refer to 306460 for a detailed explanation.												
Check passed	Microsoft VM Security Updates	No critical security updates are missing.												
Check passed	IIS Security Updates	No critical security updates are missing.												
Check passed	MDAC Security Updates	No critical security updates are missing.												
Check not performed	Office Security Updates	This scan can only be performed on a local machine.												

Table 10 - Microsoft Baseline Security Analysis Results

Findings:

The system administrator tells me that the notices of patches missing in the Baseline Security Analysis Report, MS03-030, MS04-016, and MS04-028, are false positives. I can agree because the **nessus.exe** report did not report these as being security vulnerabilities.

Taking the list of installed software compiled under Item 3.3, I compared it to the **nessus.exe** configuration file to determine whether the proper plug-ins were enabled that would test the software products for vulnerabilities. All of the Microsoft products were tested for vulnerabilities. Testing of the Oracle software products was hit and miss. Testing of the Novell products was hit and miss.

Conclusions I made from the **nessus.exe** report and the questions that came to mind that I needed to ask the system administrator:

- The vulnerable 3Com 3C Daemon FTP server was running on port 21. What is this ftp server used for? Is it possible to disguise its name or use something else?

From my Cross Reference Chart and the **netstat** listing, I noted that the Trivial File Transfer service associated with the 3C Daemon FTP server had UDP Port 69 open.

A system log associated with the 3C Daemon FTP server was holding UDP Port 514 open.

- **Nessus.exe** noted the processes running at ports 21/tcp, 135/tcp, 137/udp, 139/tcp, 445/tcp, 1025/tcp—ports mostly used by malware. Using the Cross Reference Chart, I concluded the services running at these ports are legitimate. The report reflected the fact that no attempt has been made to disguise the programs running on this system. On the other hand, this is an internal system protected by a security perimeter. Instead, a hacker will use malware to gain entry and hijack an account with administrator privilege.
- The krb524 (4444/tcp) service was noted as providing too much information. Interestingly, port 4444/tcp did not show up as open on the following month's **nessus.exe** scan. I also noted that the OracleOra9ias_homeWebCacheAdmin service (see the services list in section 3.5) was stopped even though the start mode on this service is "Automatic".
- The **nessus.exe** report did not display any critical vulnerabilities. Everything was either informational or low.

We need to add the **nessus.exe** plugins to the scan script for Oracle and Novell, to make sure the software has been patched for the vulnerabilities discussed under 3.10.

3.9 Evidence and Findings from 2.9 (Analyze IIS for Vulnerabilities)

Evidence:

Microsoft Baseline Security Analyzer Internet Information Services (IIS) Scan Results

Vulnerabilities

Score	Issue	Result
Check passed	IIS Lockdown Tool	The IIS Lockdown tool has been run on the machine.
Check passed	Sample Applications	IIS sample applications are not installed.
Check passed	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present.
Check passed	Parent Paths	Parent paths are not enabled.
Check passed	MSADC and Scripts Virtual Directories	The MSADC and Scripts virtual directories are not present.

Additional System Information

Score	Issue	Result				
Best practice	Domain Controller Test	IIS is not running on a domain controller.				
	IIS Logging Enabled	Some web or FTP sites are not using the recommended logging options.				
		<table><tr><th>Name</th><th>Protocol</th></tr><tr><td>Default Web Site</td><td>HTTP</td></tr></table>	Name	Protocol	Default Web Site	HTTP
Name	Protocol					
Default Web Site	HTTP					

Table 11 – Microsoft Baseline Security Analysis of IIS

Findings:

According to the **Microsoft Baseline Security Analyzer (MBSA)**, the Microsoft IIS Lockdown tool has been run on this system. MBSA also checked some of the security settings invoked by the IIS Lockdown tool to make sure a system administrator had not,

after the fact, changed the security settings to something less secure. This Windows 2000 server appears to be hardened as set by the IIS Lockdown tool.

According to MBSA patch history, all critical security updates for IIS have been installed, Table 11 – Microsoft Baseline Security Analysis of IIS.

The fact the IIS Lockdown tool has been run on this system can be confirmed by the fact that two groups exist, Web Anonymous Users and Web Applications.

Nessus.exe did not find any high severity problems with IIS.

The Install or Remove Programs list, Figure 6 – List of Installed Software shows that IIS UrlScan Tool 2.0 is installed. According to the Microsoft URLScan web site, the UrlScan security tool restricts the types of HTTP requests that Internet Information Services (IIS) will process. By blocking specific HTTP requests, the UrlScan security tool helps prevent potentially harmful requests from reaching the server.⁴²

Nessus.exe is recommending that the UrlScan.ini file be configured to hide the server header information. This will make it harder for a hacker to deduce this server is running IIS.⁴³ The Microsoft guidance for editing the UrlScan.ini:

1.	Stop the IISAdmin service, which will also stop all of the services that are dependent on it, such as the World Wide Web Publishing Service.
2.	In My Computer, locate the Urlscan folder. By default, this is located at %systemroot%\System32\Inetsrv\Urlscan.
3.	In Notepad or another text editor, open the Urlscan.ini file.
4.	Locate the following entry: RemoveServerHeader=0
5.	Modify this entry as follows: RemoveServerHeader=1
6.	Save the file.

⁴² "URLScan Security Tool." Microsoft web site. , © 2004. URL: <http://www.microsoft.com/technet/security/tools/urlscan.mspx>.

⁴³ "How to Mask IIS Version Information from Network Trace and Telnet." Microsoft web site. © 2004. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;317741>.

7. Restart the World Wide Web Publishing service and all of the other services that were stopped when the IISAdmin service was stopped. Starting a service that runs under the IISAdmin service also starts the IISAdmin service.

The server does not contain any user accounts other than the people who administer the system. Through organizational policy, these people have been asked to not surf the Internet from this system.

Microsoft recommends that in addition to using the IIS 5 Checklist, to apply the Windows 2000 Server Baseline Security Checklist

Services

Using Microsoft Knowledge Base Article 189271 as a general guide the following list is services that are required, may be required, and are not required.⁴⁴ Based on the listing produced by *pservice*, of the 91 services installed, 54 services are running. Some of these services may be running but serve no purpose. The system administrator needs to take the time to go through the list of services and determine whether some ports can be disable. In the future the system administrator should either run psservice or export the list of services from Administrator Tools after every new software install to be able to better associate services to software.

Required	May be Required	Not Required
Event Log	Certificate Authority (required to issue certificates)	Alerter*
IIS Admin Service	Content Index (required if using Index Server)	ClipBook Server*
License Logging Service	FTP Publishing Service (required if using FTP service; it's highly recommended that FTP and Web services run on different servers)	Computer Browser*
MSDTC	NNTP Service (required if using NNTP Service)	DHCP Client*
Protected Storage	Plug and Play	Messenger*
Remote Procedure Call (RPC) Service	RPC Locator (required if doing remote administration)	NetBIOS Interface
Server	Server Service (can be disabled, but required to run User Manager)	Net Logon*
Windows NTLM Security Support Provider		Network DDE*
Workstation		Network DDE DSDM*

⁴⁴ "List of services that are needed to run a security-enhanced IIS computer." Microsoft web site. © 2004
URL: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;189271>

Required	May be Required	Not Required
World Wide Web Publishing Service		Network Monitor Agent
		NWLink NetBIOS
		NWLink IPX/SPX Compatible Transport
		Simple TCP/IP Services
		Spooler*
		TCP/IP NetBIOS Helper*
		WINS Client (TCP/IP)
		Remote Access Services (required if you use dial-up access)*
		SMTP Service (required if using email service)
		Telephony Service (required if access is by dial-up connection)*
		Uninterruptible Power Supply (UPS) (optional; but it is recommended that you use a UPS)*

Services running on this system

* Installed services that could be disabled

Table 12 – Not/Maybe/Required IIS Services

Applications

IIS is installed on this system to support Microsoft Software Update Services. Software Update Services has three main components:⁴⁵

- Windows Update Synchronization Service which downloads the patches from the Microsoft web site.
- An Internet Information Services (IIS) web site that services update requests from clients configured to look to this server and Software Update Services for updates..
- A SUS administration Web page.

⁴⁵ "Software Update Services Deployment White Paper, page 7." Microsoft web site. © 2004. URL: <http://www.microsoft.com/windowsserversystem/sus/susdeployment.msp>

3.10 Evidence and Findings from 2.10 (Evaluate Other Installed Software Products for Vulnerabilities)

Evidence and Findings:

Software	Service/Port	Weakness	Findings
3Com 3CDaemon	21 TCP 69 UDP 514 UDP	Version 2.0, revision 10 has a buffer overflow vulnerability. Hackers may use this vulnerability to crash the server, which results in denial of service as well as executing arbitrary commands. The vulnerability was published in April 2002, CAN-2002-0606.	3CDaemon is a free TFTP, FTP, and Syslog daemon for Microsoft Windows platforms. I spent an hour+ conducting an Internet search for a patch. There doesn't appear to be a patch. There is no nessus plugin to test for this vulnerability either.
Adobe Acrobat		<p>CAN-2004-0629 - Buffer overflow in the ActiveX component (pdf.ocx) for Adobe Acrobat 5.0.5 and Acrobat Reader, and possibly other versions, allows remote attackers to execute arbitrary code via a URI for a PDF file with a null terminator (%00) followed by a long string.</p> <p>Can-2004-0632 - Adobe Reader 6.0 does not properly handle null characters when splitting a filename path into components, which allows remote attackers to execute arbitrary code via a file with a long extension that is not normally handled by Reader, triggering a buffer overflow.⁴⁶</p>	<p>Adobe has released a Reader 6.0.2 Update patch to fix CAN-2004-0629 (Adobe Acrobat ActiveX Control Buffer Overflow) and CAN-22004-0632 (Filename Handler Buffer Overflow).</p> <p>On the macromedia vulnerability, there is no patch. Instead, Adobe is suggesting we modify multimedia permission wetting for Macromedia Flash Player.</p>

⁴⁶ "Common Vulnerabilities and Exposures, - Adobe." CVE, MITRE web site. © 2004. URL: <http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=adobe>

Software	Service/Port	Weakness	Findings
		A vulnerability exists that could allow malicious code to access a user's computer when a malicious media file embedded in a PDF file is played by the Macromedia Flash Player on Windows.	
AMS Server			Symantec Alert Management System Server. AMS2 provides emergency management, and supports alerts from NetWare 5.0, and 6.0 servers, Windows NT servers and workstations, Windows 95/98 workstations, and Windows XP Pro workstation. Notifications can be sent through pagers, email, Network broadcast alerts, message boxes, and by executing a special program or SNMP trap. ⁴⁷
Answer Works Runtime		There don't seem to be any published security issues associated with the code.	AnswerWorks from Wextech Systems is a development tool that adds a natural-language interface to Windows and HTML online Help Systems. This interface allows users to search for and locate information by typing

⁴⁷ "Symantec AntiVirus Corporate Edition 8.x installation walk-through for administrators." Symantec web site. © 2004 URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002073014500548?OpenDocument&src=ent_hot&dtype=corp&prod=Symantec%20AntiVirus%20Corporate%20Edition&ver=8.x&tpre=

Software	Service/ Port	Weakness	Findings
			their requests in plain English. ⁴⁸
Intel PDS		There is no security vulnerability.	Symantec uses the Intel Ping Discovery Service (PDS), which is part of Intel's LANDesk Management Suite 6 and the Common Base Agent (CBA) - used for communicating between the core server and managed clients.
LSASS		Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows ⁴⁹	Local Security Authority Subsystem Service (LSASS) provides an interface for managing local security, domain authentication, and Active Directory processes. It handles authentication for the client and for the server. It also contains features that are used to support Active Directory utilities. Microsoft released a Security Bulletin and patch, MS04-011, on April 13, 2004, entitled Security Update for Microsoft Windows (835732), CAN-2004-0533
Mrb.net's Software – Wait32		There don't seem to be any published security issues associated with the code.	Mrb.net's Software – Wait32 - Wait32 is used in batch and command files to pause execution

⁴⁸ "Answerworks 3 FRQ." Delado web site. © 2004. URL: <http://www.delado.com/Wextech/prawfaq.htm>

⁴⁹ "CVE Cross Reverence 2003." Saint Corporation web site.. © 2004. URL: http://www.saintcorporation.com/demo/saint/cve_2003.html

Software	Service/Port	Weakness	Findings
			for the amount of time specified before executing the next line.
MSTask	Port 1030 lad1	MSTask is vulnerable to a remote code execution. The attacker could gain the same privilege as the user has on the machine.	<p>MSTask (Microsoft Task Scheduler) is an application that provides services for task scheduling⁵⁰. Microsoft released a Security Bulletin and patch, MS04-022, on July 13, 2004, entitled Vulnerability in Task Scheduler Could Allow Code Execution (841873), CAN-2004-0212⁵¹. The nessus plugin for the MSTask vulnerability is 13852. The nessus scan checked for this vulnerability and determined the patch had been applied as did the Microsoft Baseline Security Analyzer.</p> <p>My nessus scan has provided the information that MSTask is associated to the service iad1 on port 30. iad1 is the Bolt, Beranek and Newman (BBN) Interface Access Device (IAD) service. A dynamic</p>

⁵⁰ "Make sure you're protected on all sides." PC Flank web site. © 2004 URL: <http://www.pcflank.com/art20.htm>

⁵¹ "Microsoft Security Bulletin MS04-022, Vulnerability in Task Scheduler Could Allow Code Execution (841873)." Microsoft web site. © 2004 URL: <http://www.microsoft.com/technet/security/Bulletin/MS04-022.mspx?pf=true>

Software	Service/ Port	Weakness	Findings
			analyser from IBM giving information on run time performance and code utilisation. ⁵² This is tied to Microsoft's Remote Procedure Calls (RPC). The executable is svhost.exe
NICI (Shared) U.S./World wide (128 bit) (2.6.4- 5)		<p>A vulnerability in the way OpenSSL handles ASN.1 tags could allow a remote attacker to cause a denial of service. The U.K. National Infrastructure Security Co-ordination Centre (NISCC) (www.niscc.gov.uk) prepared a test suite to check the operation of SSL/TLS software when presented with a wide range of malformed client certificates.</p> <p>Dr Stephen Henson (steve@openssl.org) of the OpenSSL core team identified and prepared fixes for a number of vulnerabilities in the OpenSSL ASN1 code when running the test suite.</p> <p>A bug in OpenSSL's SSL/TLS protocol was also identified which causes OpenSSL to parse a client certificate from an SSL/TLS client when it should reject it as a protocol error⁵³.</p>	<p>OpenSSL implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols and includes a general purpose cryptographic library. SSL and TLS are commonly used to provide authentication, encryption, integrity, and non-repudiation services to network applications such as HTTP, IMAP, POP3, LDAP, and others. All versions of OpenSSL up to and including 0.9.6j and 0.9.7b and all versions of SSLeay are affected.</p> <p>Any application that makes use of OpenSSL's ASN1 library to parse untrusted data. This includes all SSL or TLS applications, using S/MIME (PKCS#7) or</p>

⁵² "Glossary of Computer Terms." Laynetworks web site. © 2004. URL: <http://www.laynetworks.com/glossary/i.htm>

⁵³ "OpenSSL Security Advisory [30 September 2003] Vulnerabilities in ASN.1 parsing." http://www.openssl.org/news/secadv_20030930.txt

Software	Service/Port	Weakness	Findings
		All versions of Novell eDirectory prior to 8.7.3 on all platforms are affected by the SSL/TLS ASN.1 decoder vulnerabilities ⁵⁴ . Vulnerabilities in the secure sockets layer (SSL) and transport layer security (TLS) protocols that use OpenSSL code.	<p>certificate generation routines. Recommendations -----</p> <p>Upgrade to OpenSSL 0.9.7c or 0.9.6k. Recompile any OpenSSL applications statically linked to OpenSSL libraries. CERT released vulnerability alerts CAN-2003-0543 (VU#255484), Can-2003-0544 (VU#380864), VU#686224, and VU#732952 . In response to the OpenSSL group's security alert, Novell released Security Update 5 (TID10087450), last modified August 3, 2004, fixing the vulnerabilities in its software that utilized SSL/TLS ASN.1.</p> <p>Microsoft products do not use the libraries in question.</p> <p>The <i>nessus</i> plugin 11875 does scan for this vulnerability. However, others such as 13811, 14808, 1530, and 15231 were not included in the scan script. These plug-</p>

⁵⁴ NISCC vulnerability advisory on SSL (secure sockets layer) and TLS (transport - TID10087450 (last modified 03AUG2004) “ <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087450.htm>

Software	Service/ Port	Weakness	Findings
			ins needed to be added to the <i>nessus script</i> for the next vulnerability scans.
Oracle9iAS HTTP Server 9.0.3.1	Krb524 (4444/tcp)	HTTP server SSL – A cryptographic weakness in version 4 of the Kerberos protocol allows an attacker to use a chosen-plaintext attack to impersonate any principal in a realm. Kerberos version 5 does not contain this cryptographic vulnerability. Sites are not vulnerable if they have Kerberos v4 completely disabled, including the disabling of any krb5 to krb4 translation services ⁵⁵ .	Alert #68 released on 9/24/04 – Oracle released patch.
Outlook Express		Outlook Express is vulnerable to a denial of service because of a lack of robust verification of malformed e-mail headers. exists that could allow an attacker to send a specially crafted e-mail message causing Outlook Express to fail.	Outlook Express is Microsoft's email client. Microsoft Security Bulletin MS04-018, CAN-2004-0215. http://www.microsoft.com/technet/security/Bulletin/MS04-018.mspx ⁵⁶ Cumulative Security Update for Outlook Express (823353), was released July 13, 2004, to patch If a user is running Outlook Express and receives a specially crafted e-mail message,

⁵⁵ "MIT krb5 Security Advisory 2003-004: Cryptographic weaknesses in Kerberos v4 protocol." MIT University web site. © 2004. URL: <http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-004-krb4.txt>

⁵⁶ "Microsoft Security Bulletin MS04-018 Cumulative Security Update for Outlook Express (823353)." Microsoft web site. © 2004. URL: <http://www.microsoft.com/technet/security/Bulletin/MS04-018.mspx>

Software	Service/ Port	Weakness	Findings
			<p>Outlook Express would fail. If the preview pane is enabled, the user would have to manually remove the message, and then restart Outlook Express to resume functionality.</p> <p>The system did not show a vulnerability to this weakness when scanned by nessus plugin #13643.</p>
Symantec System Center		<p>Symantec System Center vulnerability allows attacker to unlock server group without knowing password</p> <p>Symantec System Center is vulnerable to an attack that allows an attacker can unlock a server group without knowing the console password.</p>	Symantec AntiVirus and Symantec System Center were patched to protect against this attack.
Terminal Services	3389	<p>Two vulnerabilities: information disclosure, denial of service. The implementation of the Remote Data Protocol (RDP) in the terminal service in Windows NT 4.0 and Windows 2000 does not correctly handle a particular series of data packets.⁵⁷ If such a series of packets were received by an affected server, it would cause the server to fail. The server could be put back into normal service by rebooting it, but any</p>	<p>The system administrators use Terminal Services and Remote Desktop to perform administrative tasks remotely. Terminal Services is not installed by default.</p> <p>Microsoft Security Bulletin MS01-052, Invalid RDP Data can Cause Terminal Service Failure, originally posted</p>

⁵⁷ "Microsoft Windows Terminal Server Patch Unspecified Denial Of Service Vulnerability". SecurityFocus web site. © 2004. URL: <http://www.securityfocus.com/bid/10325>.

Software	Service/ Port	Weakness	Findings
		work in progress at the time of the attack would be lost.	on October 18, 2001 and updated on May 11, 2004. ⁵⁸ The nessus plugin 11146 is set to scan for this vulnerability, CAN-2002-0863.
VERITAS Backup Exec Remote Agent for Windows Servers		<p>Veritas Backup Exec contains a flaw that may lead to an unauthorized information disclosure. The issue is based on the requirement for the "RestrictAnonymous" registry key to be set to 0, creating a loss of confidentiality and allowing anonymous listing of the SAM database and all associated shared folders and files.⁵⁹</p> <p>VERITAS Technical Support has recently discovered that Backup Exec 9.0 servers may be susceptible to infection by the "W32.SQLEXP.Worm" (also known as "SQL Slammer" discovered 1/24/2003).⁶⁰</p>	<p>An enterprise backup system. This server contains a Veritas remote agent. The Veritas Backup Exec control center is installed on another server. Veritas Exec contains a Veritas client component. Upgrade to version 8.6 or higher, as it has been reported to fix this vulnerability. Post upgrade, ensure that the "RestrictAnonymous" registry key is set to 1.</p> <p>For the SQL Slammer download Veritas patches.</p>
Winlogon		A buffer overrun vulnerability exists in the Windows logon process (Winlogon). It does not check the size of a value used	The Windows logon process (Winlogon) is the component of the Windows operating

⁵⁸ "Microsoft Security Bulletin MS01-052, Invalid RDP Data can Cause Terminal Service Failure, October 18, 2001, updated May 11, 2004." Microsoft web site. © 2004. URL: <http://www.microsoft.com/technet/security/Bulletin/MS01-052.mspx>

⁵⁹ "Veritas Backup Exec Restrict Anonymous Requirement SAM Information Disclosure." Open Source Vulnerability Database web site. © 2004. URL: http://www.osvdb.org/displayvuln.php?osvdb_id=8230

⁶⁰ "W32.SQLEXP.Worm "SQL Slammer" (discovered on 1/24/2003) causes Microsoft Desktop Engine, included with VERITAS Backup Exec (tm) 9.0 for Windows Servers revision 4367 and VERITAS ExecView (tm) 3.1 revision 229, to flood the network and SQLSERVER.EXE may exhibit high CPU utilization." Net-security web site. © 2004. URL: <http://seer.support.veritas.com/docs/254244.htm>

Software	Service/Port	Weakness	Findings
		during the logon process before inserting it into the allocated buffer. The hacker who successfully exploits the buffer can take complete control of the machine.	system that provides interactive logon support. Winlogon.exe is the process that manages security-related user interactions in Windows. ⁶¹ Microsoft released a Security Bulletin and patch, MS04-011, on April 13, 2004, entitled Security Update for Microsoft Windows (835732), CAN-2003-0806 . ⁽⁶¹⁾ The nessus plugin for the MSTask vulnerability is 12209. The nessus scan checked for this vulnerability and determined the patch had been applied as did the Microsoft Baseline Security Analyzer .

Table 13 – Vulnerabilities in Other Install Software

⁶¹ "Microsoft Security Bulletin MS04-011 Security Update for Microsoft Windows (835732)" Microsoft web site. © 2004. URL: <http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx?pf=true>

Part #4 – Audit Report

Executive Summary

“Information is the world’s new currency,” was a statement made by W.Ralph Basham, director of the Secret Service. That statement is probably applicable to any organization in existence today. It’s no longer about the technology—it’s about the information. The bad guys are no longer targeting the technology—they have set their sites on the information. If you read the computer security news service commentaries today, i.e. Zdnet, News, Gartner, just to mention a few, you will find discussion about identity theft, credit card fraud, and social engineering. The experts that conduct the surveys and follow the trends are saying the attacks are serious and directed.

“Malicious software cases rose 22 percent in October, with Trojan horses accounting for nearly half,” according to TrendLabs. As long as people continue to open attachments in email, follow Internet links, or be socially engineered in other way, malware will continue to be the most successful means for a security breach.

How does this relate to AgencyXYZ server, which doesn’t contain the type of information the bad guys want, isn’t a public web server, and doesn’t directly support general users? The fact that AgencyXYZ is connected to the same network as are all the other workstations, printers, faxes, and servers in the AgencyXYZ organization and that network is directly connected to the Internet with no physical user restrictions either direction. One human miscalculation and one vulnerable system is all that is required for the bad guy to take up residence somewhere inside AgencyXYZ’s internal network.

The goal of this audit was to determine how secure a Microsoft Windows 2000 file server is, running IIS 5.0, a required component of Microsoft Software Update Service. The purpose of the tests conducted during the audit was to locate any vulnerability in the system software and processes. The conclusions taken from this audit will provide management with a better understanding of the level of threat exposure this server creates within the AgencyXYZ computer environment. The tests would reveal whether the security controls on this system are providing an adequate level of protection against threats such as malware, intrusions, and denial of service.

I believe the audit objectives were achieved. The audit did determine the level of security on AgencyXYZ server. The audit test results uncovered vulnerabilities in the system software and processes that need to be corrected—nothing severe. Human behavior does present a certain risk to the system. The information learned from this audit will give management a better understanding of the threat exposure this server causes for the Agency XYZ computer environment.

In conclusion, the user's workstation's probably pose a greater risk to the AgencyXYZ computer environment than does the AgencyXYZ IIS server. Because AgencyXYZ server is a IIS server, access controls are tighter on the server. The user can surf the Internet from the workstation and could encounter malware on a malicious web site, whereas the AgencyXYZ IIS doesn't have any general users who surf the Internet. Users receive Internet email at the workstation, whereas AgencyXYZ IIS server does not have an email process running. System Administrators connect directly to the Microsoft Windows Update web site to patch servers, whereas workstations are patched through Microsoft SUS which is sometimes hit and miss because of technical difficulties.

Audit Findings

Ten areas within the system operation, processing, or administrative functions were tested or evaluated. A description of the test and the test results are grouped by test number in the table below.

Item #	Item Description	Pass/ Fail
1	Check Security of Default Computer Accounts and Groups.	Fail
	Test: I used the Windows tool addusers.exe to generate a list of user accounts that showed the association to group accounts. I wanted to analyze the default accounts and determine whether any that were enabled should be disabled.	
	Test Results: IIS--The fact that IIS was installed on this server was validated by the existence of the IUSR_AgencyXYZ and IWAM_AgencyXYZ user accounts associated to the Guests group. I could tell that the Microsoft IIS Lockdown tool had been run because of the association of IUSR_AgencyXYZ guest account to the Web Anonymous Users group. Likewise, the guest account IWAM_AgencyXYZ was associated to the Web Applications group. Oracle—I could tell Oracle was installed on this server by the existence of the group ORA_DBA. From my research of the ORA_DBA group, I learned the process by which Oracle authenticated users was considered to be a secure method. I could validate that fact because Oracle had released patches for published vulnerabilities Telnet—I didn't see the existence of a group called TelnetClients. The Telnet service is not running; however, it is set to Manual. A malware program could easily start it.	

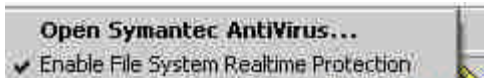
	<p>The Administrator user account has been renamed—an action recommended by the security experts.</p> <p>The TSInternetUser user account exists on the system, which means that Terminal Services has been installed. When Terminal Services has been installed in application mode, the Terminal Services Connector Licensing uses TSInternetUser account to automatically log user's onto the system. I looked at the Terminal Services configuration and determined it was installed in Remote Administration mode, Figure 4 – Terminal Server Mode. TSInternetUser account serves no purpose in the current configuration.</p> <p>Administrators - Because this is a utility server, general users do not have a reason to directly access this server. I counted 12 user accounts on this server. Seven of the 12 accounts belong to the Administrator group. I find this to be a bit excessive. We know all 7 are not day-to-day system administrators.</p>	
2	<p>Ensure the Guest Account is Disabled.</p> <p>Test: I ran Windows Baseline Security Analyzer to determine whether Guest is disabled. Guidance suggests that the Guest account is installed with a blank password by default.⁶² Part of the test was to determine whether the default password had been changed</p> <p>Test Results: According to the Windows Baseline Security Analysis, the Guest account is disabled. Windows Baseline Security Analyzer found the password to be weak. That presents a certain degree of risk because hackers have tools that can enable a disabled Guest account. If the hacker can crack the password, they are in.</p>	Fail

⁶² "Microsoft Windows Security 101, by Tony Bradley." About, Inc. web site. © 2004. URL: <http://netsecurity.about.com/cs/windowsxp/a/aa100903.htm>

3	<p>Check for Unwanted Software.</p> <p>Test: To check for unwanted software, first, I went to the Control Panel and Add Remove Programs and looked at what was listed, Figure 6 – List of Installed Software. Because there was software such as Terminal Services installed, I went into Control Panel, Administrative Tools, Component Services and looked at the processes listed. I opened Terminal Services Configuration to see what Terminal Server mode had been chosen during installation.</p> <p>Looking at the list of software under Add Remove Programs, I listed those products I wasn't familiar with, that required investigation. The objective was to determine whether all the software displayed was legitimately installed by the system administrator.</p> <p>Test Results: The software products that I was not familiar with and wanted to do more research on were: 3CDaemon, AnswerWorks Runtime, Mrb.net's Software – Wait32, NICI (Shared) U.S./Worldwide (128 bit)(2.6.4-5), and PrintMe Internet Printing. I found that none of these products were malware.</p> <p>PrintMe Internet Printing is a component of Adobe Acrobat 6 that is embedded into the Reader install—it is not easy to leave off if it is not wanted.</p> <p>3CDaemon looks like unwanted software, but the system administrators installed it because of the tftp component. My research pointed out security issues with 3CDaemon utility. I could not locate a patch.</p> <p>The NICI software had published security issues, but Novell produced patches to correct the problem. Nessus.exe would have been a good method to determine whether the patches had been applied. The organization needs to run another scan with the applicable plug-ins enabled.</p>	Pass
4	<p>Are Any Trojans Listening on Open Ports?</p> <p>Test: I ran nMap.exe because I wanted to see which ports were open. I ran netstat -a to get a second opinion on which ports are open but to also find out which ports are listening.</p> <p>The objective of this test was to determine whether Trojans were holding any of the ports open.</p>	Pass

	<p>Test Results:</p> <p>When I compared the list of known Trojan ports to my open port list, the following ports matched: TCP - 21, 80, 135, 139, 445, 1025, 3000, 4000, 4001, 7777, 10000; UDP – 137, 138, and 3456. I had to wait on finishing this test until I was able to put together my Cross Reference Chart (Test 6) to match software to processes, to ports and to services. The Cross Reference Chart displayed for me what owned each port. From the Chart I was able to determine that no Trojans were listening at any of the ports list above.</p>																							
5	<p>Are Unneeded Services Running?</p> <p>Test:</p> <p>Psservice.exe provided a descriptive listing of the services installed on the system. The system administrator was able to export the services listing for me this provided information on the service state (stopped or started), and startup mode,(manual, automatic or disabled). Between the two listings I have a very clear picture of services on this system.</p> <p>The objective of this test was to determine whether any services should be disabled.</p> <p>Test Results:</p> <p>The following table represents a list of services that I am recommending be looked at for possible disable. I am concerned that some of the services that are running should be disabled.(37)(44)(33) The following color scheme is yellow=started/automatic, blue=stopped/manual, green=started manual.</p> <table><tr><th>Services</th><th>Communications Protocols</th></tr><tr><td>Alerter</td><td>NetBIOS Interface</td></tr><tr><td>BITS</td><td>NWLink NetBIOS</td></tr><tr><td>ClipBook Server</td><td>NWLink IPX/SPX Compatible Transport</td></tr><tr><td>Computer Browser</td><td>Simple TCP/IP Services</td></tr><tr><td>DHCP Client</td><td>WINS Client (TCP/IP)</td></tr><tr><td>Distributed Link Tracking Client</td><td></td></tr><tr><td>Fax Service</td><td></td></tr><tr><td>Network DDE DSDM</td><td></td></tr><tr><td>Performance Logs and Alerts</td><td></td></tr><tr><td>Remote Access Services</td><td></td></tr></table>	Services	Communications Protocols	Alerter	NetBIOS Interface	BITS	NWLink NetBIOS	ClipBook Server	NWLink IPX/SPX Compatible Transport	Computer Browser	Simple TCP/IP Services	DHCP Client	WINS Client (TCP/IP)	Distributed Link Tracking Client		Fax Service		Network DDE DSDM		Performance Logs and Alerts		Remote Access Services		Fail
Services	Communications Protocols																							
Alerter	NetBIOS Interface																							
BITS	NWLink NetBIOS																							
ClipBook Server	NWLink IPX/SPX Compatible Transport																							
Computer Browser	Simple TCP/IP Services																							
DHCP Client	WINS Client (TCP/IP)																							
Distributed Link Tracking Client																								
Fax Service																								
Network DDE DSDM																								
Performance Logs and Alerts																								
Remote Access Services																								

	<table><tr><td>QOS RSVP</td><td></td></tr><tr><td>Remote Registry Service</td><td></td></tr><tr><td>Smart Card</td><td></td></tr><tr><td>Smart Card Helper</td><td></td></tr><tr><td>Spooler</td><td></td></tr><tr><td>Telnet</td><td></td></tr><tr><td>TCP/IP NetBIOS Helper</td><td></td></tr><tr><td>Telephony Service</td><td></td></tr><tr><td>Uninterruptible Power Supply</td><td></td></tr><tr><td>Windows Time</td><td></td></tr><tr><td>Wireless Configuration</td><td></td></tr></table>	QOS RSVP		Remote Registry Service		Smart Card		Smart Card Helper		Spooler		Telnet		TCP/IP NetBIOS Helper		Telephony Service		Uninterruptible Power Supply		Windows Time		Wireless Configuration		
QOS RSVP																								
Remote Registry Service																								
Smart Card																								
Smart Card Helper																								
Spooler																								
Telnet																								
TCP/IP NetBIOS Helper																								
Telephony Service																								
Uninterruptible Power Supply																								
Windows Time																								
Wireless Configuration																								
6	<p>Cross Reference Processes to Ports and Services.</p> <p>Test: I wanted to know what processes were running on this server. I retrieved and ran tlist.exe from the Windows 2000 Resource Toolkit to provide a listing. To gain an understanding of the processes associated to ports, I ran fport.exe.</p> <p>The objective of this exercise was to develop a Cross Reference Chart that would show me what software was associated to what processes and processes associated to ports and services to processes. I would be able to see if Trojans were installed as well as any unwanted software.</p> <p>Test Results: I developed a Cross Reference Chart, Table 8 – Cross Reference Chart – Process ID, Process, Port, Service. I was able to determine that no Trojans were running on this server. I was able to match all but a couple processes to software. I was able to associate services to software which would give a system administrator a better idea of which running services are really functional. I need to have this information in this chart available in order to finish Tests #4 and #5.</p>	Pass																						
7	<p>Check for Virus Auto-Protection.</p> <p>Test: The objective of this test was to determine whether this system has anti-virus software installed and is running a virus shield.</p>	Pass																						

	<p>Test Results: Yes, this server does have real-time anti-virus software installed. The image below with “Enable File System Realtime Protection” checked, is just one of a number of methods to determine this:</p>  <p>Another method could be to look for the open ports under Symantec in the Cross Reference Chart. Table 8 – Cross Reference Chart – Process ID, Process, Port, Service</p> <p>Another would be to look at running services. There are many ways to validate an anti-virus installation.</p>	
8	<p>Determine Whether Security Patching is Current.</p> <p>Test: I ran nessus.exe, a network security auditing utility to see whether the latest patches are installed. As a comparison I ran Windows Baseline Security Analyzer.</p> <p>Test Results: The Windows Baseline Security Analyzer noted three patches missing, which nessus.exe didn't. The system administrator said the Windows Baseline Security Analyzer notices were false positives. I could agree.</p> <p>It was during this test that I discovered that nessus.exe, using the default plug-in configuration file, does not scan all software for vulnerabilities. It is oriented to Microsoft and Unix (usually only the Top 20 exploits)⁶³ So if I based my conclusion solely on Windows Baseline Security Analyzer and nessus.exe in their current state, the software is patched. However, when I found out that nessus.exe plug-in were not installed or were not enabled to check for vulnerabilities in Oracle, Novell, Adobe Acrobat, and Veritas, I had to score the test a “Fail” while I really meant the results were inconclusive.</p>	Fail
9	Analyze IIS for Vulnerabilities.	Fail

⁶³ “The Twenty Most Critical Internet Security Vulnerabilities, October 8, 2004.” SANS web site. © 2004.
URL: <http://www.sans.org/top20/>

	<p>Test: I looked at the Microsoft Baseline Security Analysis of the AgencyXYZ server for weaknesses in IIS. I also looked at the nessus.exe report for IIS weaknesses.</p> <p>The objective of this test was to determine what safeguards have been implemented to protect the IIS environment.</p> <p>Test Results: The Microsoft Baseline Security Analysis concluded that AgencyXYZ server was secure. I noted that the Microsoft IIS Lockdown tool had been run on this server. In the list of installed software I could see that the URLScan tool was installed. Nessus.exe did not note any critical vulnerabilities. Based on these methods of testing vulnerability, IIS is very secure on this server.</p> <p>However, other areas of concern came to light during this test which is why there wasn't a "Pass" score, e.g. running Services, that the system administrator needs to evaluate before the score can be changed to "Pass". Another area of concern is the IIS server header. Nessus.exe recommends using the URLScan tool to change the server header name to disguise its identity.</p>	
10	<p>Evaluate Other Installed Software Products for Vulnerabilities.</p> <p>Test: Even though IIS is installed on this server, and Microsoft recommends that only IIS run on a server, a number of other significant utilities also run on this server. Using the list of installed software generated during Test 3, I researched the security history of any product. Considerable more time was spent on the software with which I was not familiar.</p> <p>My Cross Reference Chart served as a useful tool as I connected the software to processes, ports, and services.</p> <p>The objective of this test was 1) to determine whether there were security vulnerabilities in any of the software installed on this server and 2) determine whether proper patches had been applied.</p> <p>Test Results: As mentioned for Item 8 above, it was during this exercise that I learned that many of the installed software products have published security vulnerabilities. I also learned that nessus.exe was not configured to scan for security vulnerabilities in all the installed software products.</p>	Fail

	<p>The analysis to determine whether the installed software contained any security vulnerabilities was fairly straight forward. However, it was harder to determine whether these vulnerabilities had been patched, especially since tools such as nessus.exe were not thorough enough to be useful. The following software products contain security vulnerabilities that are going to require further action: 3CDaemon, Adobe Acrobat, NICI (Shared) U.S./Worldwide (128 bit) (2.6.4-5), Oracle9iAS HTTP Server 9.0.3.1, Veritas. The recommend action is discussed below at Item 10 of the Audit Recommendations Table.</p>	
--	---	--

Table 14 – Audit Findings

Audit Recommendations

Item #	Item Description
1	<p>Check Security of Default Computer Accounts and Groups.</p> <p>Recommendations:</p> <p>For the most part the level of security in this area is good. However, a couple of things can be done to make security better:</p> <ul style="list-style-type: none"> • Microsoft guidance recommends that if the Terminal Service Internet Connector License is not being used, the TSInternetUser should be disabled. • Adding the names of several system administrators to the TelnetClients group would reduce the risk of an Administrator's profile being hijacked. • Having seven system administrator accounts on this server seems a bit excessive. The day-to-day system administrators need to determine for what the seven accounts are being used, and arrive at solutions that do away with accounts that are enabled but inactive for months at a time. If for example a user account belongs to a program manager for occasional software maintenance, then the account can be enabled and disable or the person can work through the system administrator.

Item #	Item Description
	Cost: \$0
2	<p>Ensure the Guest Account is Disabled.</p> <p>Recommendations:</p> <p>Even though the Guest account is disabled, the password is weak. Hackers have tools that will enable the guest account if it is disabled. I recommend that the Guest account be enabled to change the password and disabled again.</p> <p>Microsoft recommends that passwords contain at least six characters, and the character string must contain at least three of these four character types: uppercase letters, lowercase letters, numerals, and nonalphanumeric characters (e.g., *, %, &, !).⁶⁴</p> <p>Cost: \$0</p>
3	<p>Check for Unwanted Software.</p> <p>Recommendations:</p> <p>None. There is no unwanted software on the server.</p> <p>Cost: \$0.</p>
4	<p>Are Any Trojans Listening on Open Ports?</p> <p>Recommendations:</p> <p>None. There are no Trojans listening at open ports.</p> <p>Cost: \$0.</p>
5	<p>Are Unneeded Services Running?</p> <p>Recommendations:</p> <p>The system administrator is going to have to determine if the services running actually support processes. I did not have direct access to the system to do a thorough analysis of the services installed on the</p>

⁶⁴ "Password Defense". Microsoft web site. © 2004. URL:
<http://www.microsoft.com/technet/Security/prodtech/win2000/pswddef.mspx>

Item #	Item Description
	<p>system. Any services not being used should be disabled. Microsoft had a bad habit of starting all the services by default in the older O/S's for the sake of convenience. Item 5 in the Test Results Table lists a number of services that Microsoft and other experts recommend be disabled on a IIS server. I recommend that the system administrator disable any unnecessary services. This is probably going to take some time to do the analysis.</p> <p>Cost: \$1,000.</p>
6	<p>Cross Reference Processes to Ports and Services.</p> <p>Recommendations:</p> <p>None. The software matched the processes and ports. There are no Trojans running on this server.</p> <p>Cost: \$0.</p>
7	<p>Check for Virus Auto-Protection.</p> <p>Recommendations:</p> <p>None. Virus Auto-protection is installed on this server.</p> <p>Cost: \$0.</p>
8	<p>Determine Whether Security Patching is Current.</p> <p>Recommendations:</p> <p>Before we can change the score on this test to "Pass" there would need to be additional vulnerability scans completed for Adobe Acrobat, Oracle, Novell, and Veritas.</p> <p>In addition, because there are no <i>nessus.exe</i> plug-ins to test for such vulnerabilities as 3CDaemon, Adobe Acrobat, and possibly Oracle, the system adminster would need to determine whether the proper patches have been applied. Typically the patch documentation includes information on how to verify that the patch actually installed.</p> <p>Cost: \$1,000.</p>

Item #	Item Description
9	<p>Analyze IIS for Vulnerabilities.</p> <p>Recommendations: IIS is secure on this server. But because this server contains other functions besides IIS, the system administrator needs to give all the processes running on this server equal consideration and make sure the changes made by the Lockdown tool remain in place.</p> <p>IIS is not going to be the weak link for the next exploit. It will be Oracle, or Acrobat or Internet Explorer or something else totally unexpected.</p> <p>Other areas of concern came to light during this test which is why there wasn't a "Pass" score, e.g. running Services that the system administrator needs to evaluate and determine what can be disabled, before the score can be changed to "Pass". Another area of concern is the IIS server header. Nessus.exe recommends using the URLScan tool to change the server header name to disguise its identity.</p> <p>Cost: \$0.</p>
10	<p>Evaluate Other Installed Software Products for Vulnerabilities.</p> <p>Recommendations: Of all the areas tested during the audit, it is apparent this is the area that received the least system administration attention. Follow-up analysis is required to deal with the following vulnerabilities:</p> <ul style="list-style-type: none"> • 3CDaemon – There is no patch. The system administrator/management need to decide whether to remove this utility or accept the risk. The level of risk is medium because this IIS server is not directly accessed by the internal users or the public. It is protected from the public by perimeter firewalls. • Adobe Acrobat – There are a number of published vulnerabilities. A determination still needs to be made as to whether the proper patches have been applied because nessus.exe did not scan for these vulnerabilities. In the case of the most recent vulnerability regarding Macromedia Flash Player, published in October, 2004, whether recommended changes to the multimedia permissions have been made will need to be validated. • NICI (Shared) U.S./Worldwide (128 bit) (2.6.4-5) - There are

Item #	Item Description
	<p>published vulnerabilities. Table 13 – Vulnerabilities in Other Install Software A determination still needs to be made as to whether the proper patches have been applied because nessus.exe did not scan for these vulnerabilities.</p> <ul style="list-style-type: none">• Oracle9iAS HTTP Server 9.0.3.1 - There are published vulnerabilities. Table 13 – Vulnerabilities in Other Install Software. A determination still needs to be made as to whether the proper patches have been applied because nessus.exe did not scan for these vulnerabilities.• VERITAS Backup Exec Remote Agent for Windows Servers - There are published vulnerabilities. Table 13 – Vulnerabilities in Other Install Software A determination still needs to be made as to whether the proper patches have been applied because nessus.exe did not scan for these vulnerabilities. <p>System administrators need to subscribe to organizations that distribute cyber alerts through email such as the Computer Emergency Readiness Team (CERT) to stay informed of security vulnerabilities in any of the widely used software products installed on AgencyXYZ.</p> <p>Cost: \$3,000.</p>