

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 permited without express written permission.

Secure Deployment of a Windows 2000 laptop using Nessus and the CIS benchmark tool

© SANS Institute 2004, Author retains full rights.

Jeffrey Bisko
GCWN Practical Assignment
Version 3.2 – Option 2
November 26, 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper discusses how Nessus Security Scanner and the Center for Internet Security (CIS) Benchmark Scoring Tool can be used to analyze and enhance the security of a Windows 2000 laptop. Nessus security scanner was used for the external assessment and the CIS benchmark security tool v.2.1.9 was used for the internal. The CIS tool was configured with NSA's(National Security Agency) Windows 2000 workstation (NSA_win2k_ workstation.inf) security template. The utilities were used to conduct a before and after lockdown analysis. The lockdown procedures are described in detail including an analysis of the NSA template to cover all lockdowns applied. Appendix A contains the initial Nessus test results and Appendix B contains the final CIS benchmark security tool Scan log.

Introduction

Windows 2000 Professional is an operating system designed for desktop and mobile computing with a business solution in mind. Over the last five years, mobile computing has taken the world by storm. Windows 2000 Professional deployed on a laptop computer gives users greater flexibility in being able to have access to a computer almost anywhere they go. Usually, the biggest concern with laptop computers is the risk of having information compromised. As reported by Kensington in the 2002 Computer Security Institute/FBI Computer Crime & Security Survey, the average financial loss resulting from a laptop theft grew by 44% from 2000 to 2001($62,000 to $89,000) (Kensington, Notebook Security). Although Windows 2000 Professional is an operating system that allows for computing on the go, security doesn't appear to be one of the main focuses behind its development. Also reported by Kensington, in a Search Security Newsletter dated April 4, 2002, 60% of all corporate data assets reside unprotected on PCs (Kensington, Notebook Security). In today's world where personal and business secrets are at stake, security is everything.

Since its release in February of 2000, many security books and articles have been written on the various security vulnerabilities discovered with the operating system. Entire web sites have been dedicated to the sole purpose of discussing the issue of lack of security. Periodically, Microsoft will post security patches and hotfixes that will fix recently discovered problems at http://www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=7. Trying to maintain a network with the latest hotfixes and service packs released by Microsoft can become a difficult task for administrators. But is that even enough? Patches and hotfixes are just software updates, they cannot make an operating configuration secure. What other measures should an administrator take into consideration besides just applying the latest updates?

Nessus security scanner and CIS's Windows Security Scoring Tool are two free-to-use utilities that have been developed to help administrators harden their systems beyond the basic patches released. According to the Nessus web site,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

"The "Nessus" Project aims to provide the internet community a free, powerful, up-to-date and easy to use remote security scanner."(Deraison, Introduction). Nessus is a great tool to use, but a little UNIX experience is required for installation. The CIS web site states that, "The CIS Scoring tool provides a quick and easy way to evaluate your host systems and compare their level of security against the Benchmarks."(CIS, Center for Internet…). Together, with Nessus taking an external approach and the CIS Scoring Tool taking an internal approach, the additional steps needed to analyze a system for hardening a Windows 2000 Professional laptop have become much easier.

NOTE Although the CIS benchmark security tools are free-to-use, special permission was granted by Bert Miuccio, Vice President of the Center for Internet Security, to reproduce screenshots and test results in this evaluation (reference: Miuccio e-mail).

This paper begins with taking a look at what Nessus can find on a Windows 2000 Professional laptop. Then, it continues with what the CIS Scoring Tool discovered. The Scoring Tool will be configured with the NSA security template and a detailed description of how the template is configured will follow. Then, the system will be locked down by taking into consideration the results from the previous scans. Then, the system will be reevaluated by running both Nessus and the Scoring Tool again.

Initial Systems Configurations

The following is a description of the hardware and software configurations of both the Windows 2000 Professional laptop and the Red Hat Linux laptop that was used as the remote security scanner.

*NOTE * Nessus actually has two components, a server and a client. It is possible to install both the client and server on a Unix system, or it is also possible to install only the server on the Unix box, and have a client reside on the target machine. A windows client has been developed called NessusWX that can be downloaded from http://nessuswx.nessus.org/. The Windows client was not used during this evaluation.

Hardware Configuration of Both Laptops

- Dell Latitude C640
- Mobile Pentium 4 1.8 GHz
- 128 MB Ram
- 20 GB Hard drive

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Software Configurations

- Windows target laptop

  - Windows 2000 Professional – all defaults accepted during the installation
  - Microsoft Office XP Professional with Microsoft Publisher Version 2002 – Complete Install
  - Win Zip 8.1 SR-1 – evaluation copy that can be downloaded for free from http://download.com.com/3002-2250-8132587.html?tag=dir
  - Windows 2000 Support Tools – installed from Support folder on the Windows 2000 Professional CD
  - ATI Video Drivers for Dell Latitude C640 – downloaded from http://support.dell.com/filelib/format.aspx?releaseid=r57447
  - DirectX 8.1b Runtime for Windows 2000(needed for ATI Video Drivers before drivers could be installed) – downloaded from http://www.microsoft.com/downloads/details.aspx?FamilyID=a2f63641-f038-43d1-94de-47a8306e4e1d&DisplayLang=en
  - Norton AntiVirus 2004 – evaluation copy downloaded from http://download.com.com/3001-2239-10223639.html
  - Internet Explorer 6 with Service Pack 1(needed for Norton Anti-Virus 2004 installation) – downloaded from http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/download.asp
  - Microsoft Windows Installer(also needed before install of Norton AntiVirus 2004) – it installed by itself during the Norton Anti-Virus installation

- Linux scanning laptop

  - Red Hat Linux 8.0
  - Nessus 2.0.7 – latest stable version can be downloaded from http://www.nessus.com/nessus_2_0.html - Downloaded on Oct. 16, 2003.

Windows Out of the Box

The evaluation begins by running Nessus against a Windows 2000 'Straight out-of-the-box' load. The 'Straight out-of-the-box' load was a default installation that did not have any additional service packs or hotfixes applied, apart from what software had been applied already. A few general software applications, listed above, had been added to simulate a typical user's personal laptop.

Nessus Configuration

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus can be configured in several different ways depending on the desired attacks an administrator would like to use against a network system or systems. Nessus has the capability to discover all open ports detected on a target system, and then has the ability to attack these ports. Nessus is especially resourceful because it will not only use common attacks against common ports. For instance, web servers generally use Port 80 for web pages, but it is possible to host these web pages on different ports like port 1000. Nessus is able to discover this and calls the capability Smart Service Recognition (Nessus, Features).

NOTE More information about Nessus can be found at the Nessus documentation site http://www.nessus.com/documentation.html. Another good site http://msgs.securepoint.com/nessus/ has a board where you can post questions and anyone can respond. Many times the project leader Renaud Deraison will even respond.

The following is a description of the settings used during this evaluation. In a nutshell, Nessus has been configured to not hold back and run all attack plug-ins. At times, slight deviations will be made from this original configuration and each will be addressed at that time. The Nessus GUI has eight functional tabs, but only the following three are significant for describing this configuration.

Plugins Tab (Figure 1)

Plugins are the Nessus term for the security tests (scripts) that are used to attack a network system(s). Some plugins are considered dangerous and may cause systems or services to crash. The plugins come listed under several groupings including Denial of Service, Backdoors, and Windows. With Nessus, it is possible to run one plugin at a time, or even disable all the dangerous plugins, but for this evaluation all plugins were enabled to try to find all possible vulnerabilities.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

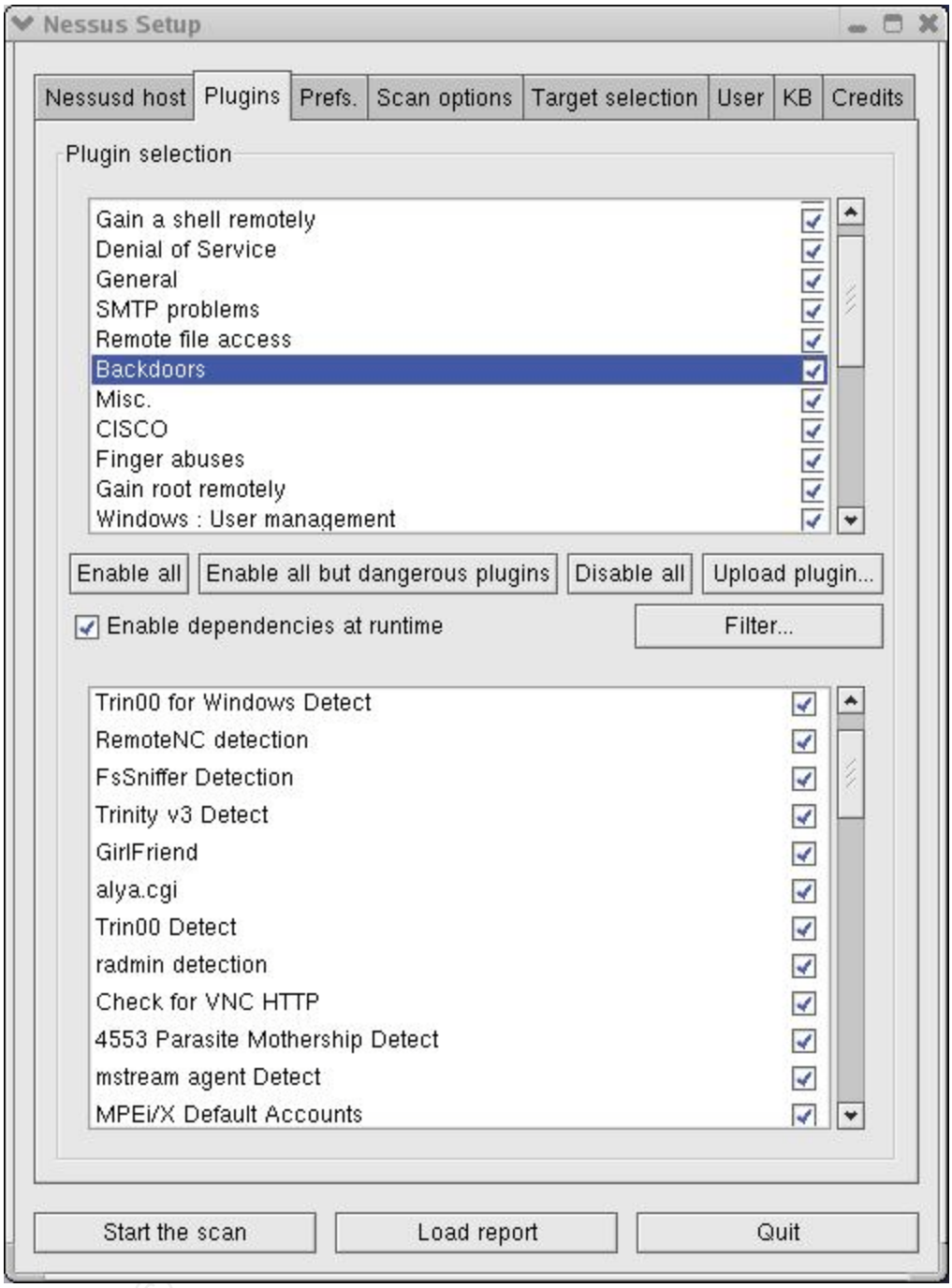

Figure 1(Plugins Tab)

Prefs. Tab (Preferences) (Figure 2)

The preferences tab contains options for setting the parameters on the different types of attacks. Some of the settings are irrelevant to this evaluation due to the simple design of the network configuration, i.e. no firewall and no IDS. For this evaluation, the Nessus scanning laptop was placed on the local network on the same subnet as the target system. Enabled settings of importance included:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- TCP Scanning technique will be Connect() – A TCP Connect() scan completes the three-way handshake.
- UDP port scan
- RPC port scan
- Identify the remote OS
- Use hidden option to identify the remote OS
- Port range will be User specified range(on Scan options tab below)
- Do not randomize the order in which ports are scanned
- SMB Scope will Request information about the domain

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

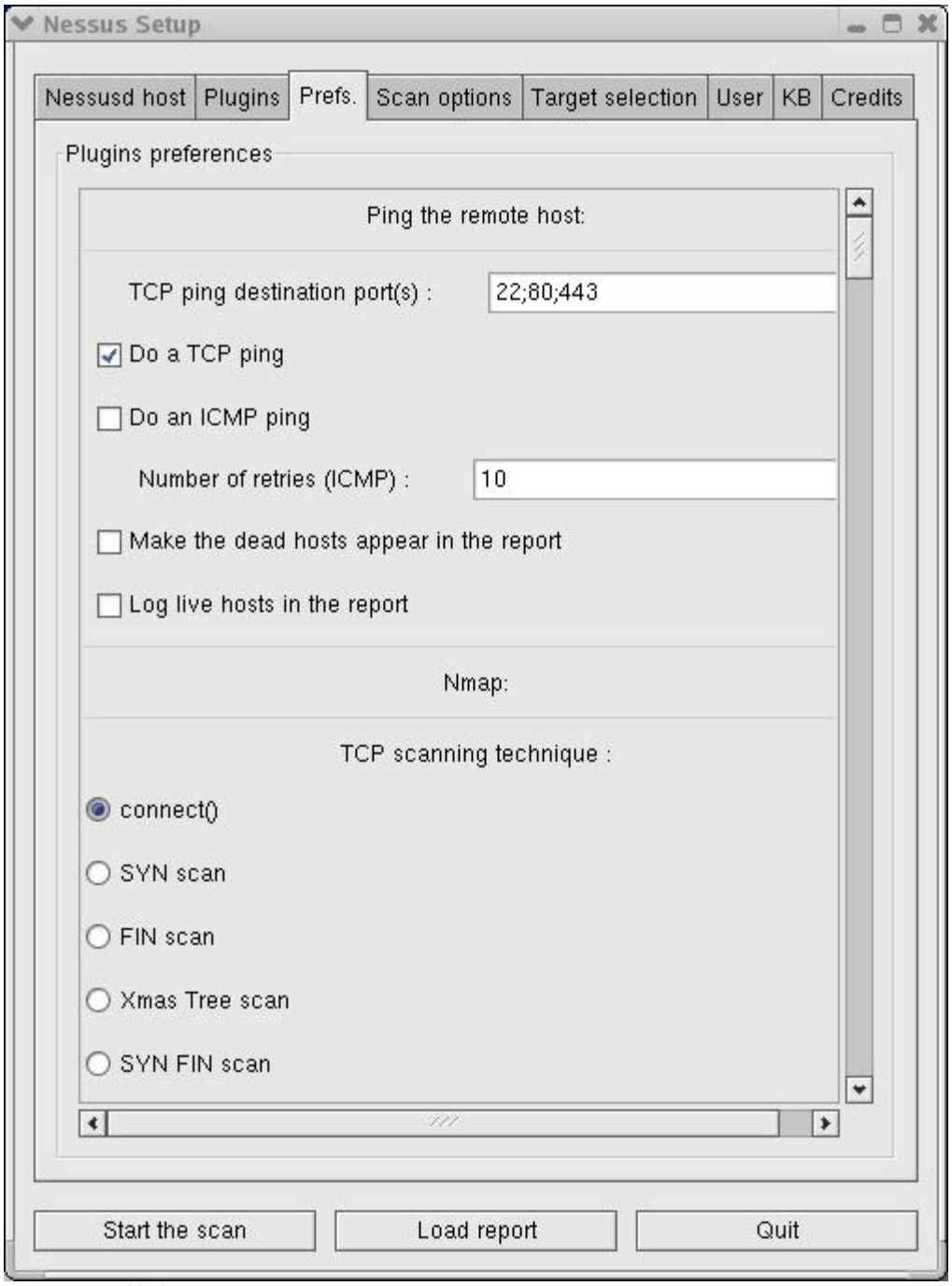

Figure 2(Prefs. Tab)

NOTE Nessus can be configured to run through a router and/or firewall even if it cannot connect to the target host with an ICMP packet(ping). After locking down a system or network down, it is an excellent practice to analyze it from all possible points of attack.

Scan options(Figure 3)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The scan options tab contains a few options to configure the port scanner. Under Port range, ports 1 – 65,535 were scanned. This refers to both UDP and TCP ports. Port scanner will have Ping the remote host, tcp connect() scan, Nmap, SYN scan, SNMP port scan, and scan for La Brea tarpitted hosts options all enabled to make sure that everything is enabled and tested.

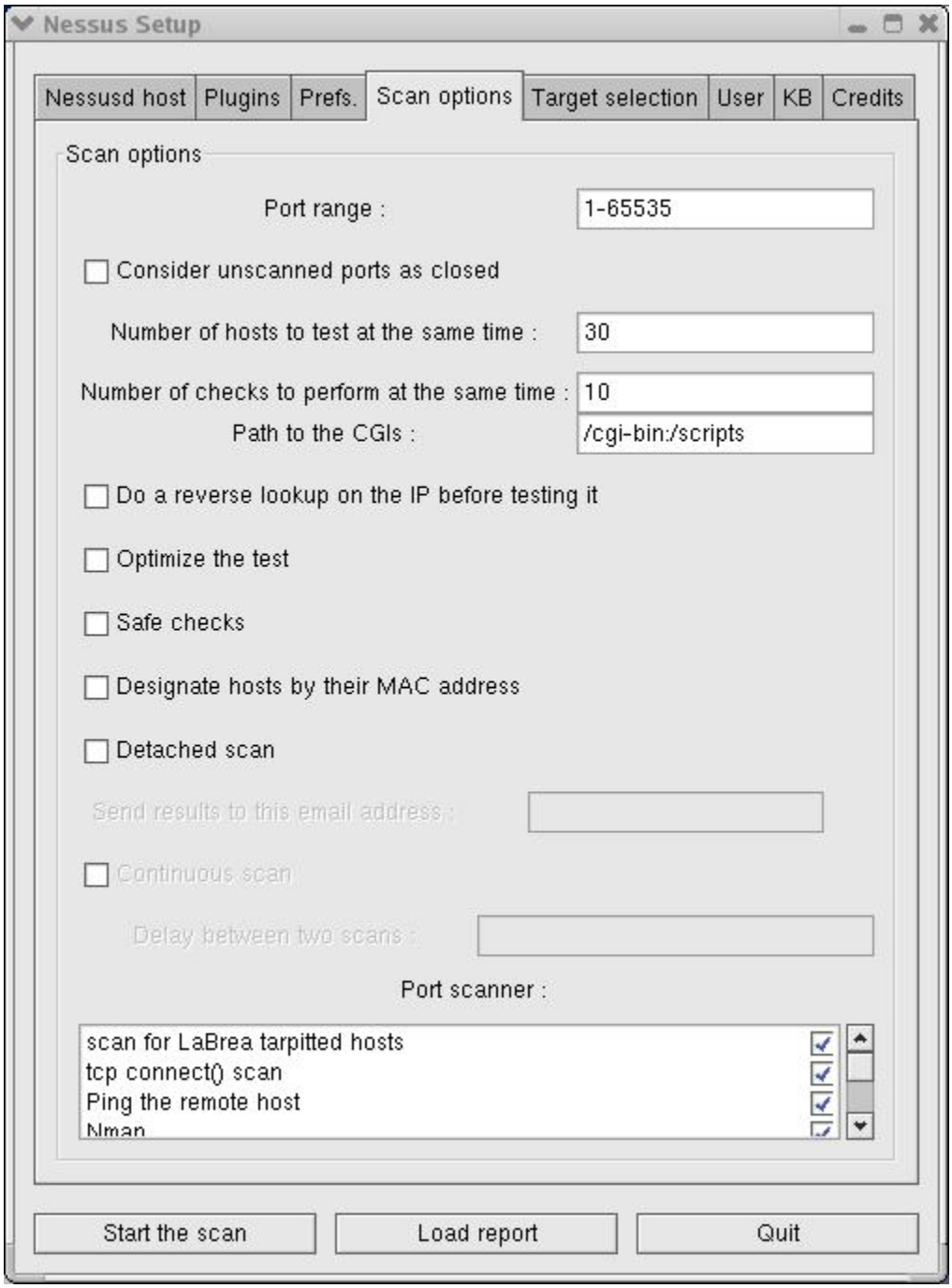

Figure 3(Scan options tab)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus Results
In an email from Renaud Deraison to William Heinbockel posted on http://www.rit.edu/~wjh3710/plugin_stats.html, Renaud explains the Nessus results in the following manner:

> Nessus classifies vulnerabilities into:
>
> 1. Security Notes
>   - information found about your system through scans/banners
> 2. Security Warnings
>   - the attack was a success but is not a great security problem
> 3. Security Holes
>   - the attack was a success and poses a great security risk
>
> These classifications can break-down further by risk:
>
> 1. None
>   - No inherant risk
> 2. Low
>   - The information found is useful to a cracker, but is not a threat in itself (ie. a banner with a version number)
> 3. Medium
>   - There is a security hole that can lead to priviledge escalation, but an attacker needs *something* to exploit it (ie. the ability to upload files, an acount on the remote host, ...)
> 4. High
>   - An attacker can gain a shell on the remote host (or execute arbitrary commands)
> 5. Serious
>   - The vulnerability leaks information that can be extremely useful to the cracker (ie. read any file as "nobody" on the remote host, get the source of a .asp script, and so on...)
> 6. Critical
>   - The remote host has already been compromised(Heinbockel, Nessus Analysis…)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

NOTE Nessus reports can be displayed as NBE, HTML, HTML with Pies and Graphs, XML, XML(old style – deprecated), NSR(deprecated), LaTeX, or ASCII text. The following results will be displayed in the HTML with Pies and Graphs format.

Nessus Report

The initial Nessus Results(Figure 4) reported 61 Security Holes(vulnerabilities), 21 Security Warnings(warnings), and 8 Security Notes(information). It further broke down these results down by assigning them into 47% High, 13% Serious, 27% Medium, and 14% Low.

Nessus Report

The Nessus Security Scanner was used to assess the security of 1 host

- **61 security holes have been found**
- **21 security warnings have been found**
- **8 security notes have been found**

Part I : Graphical Summary :

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

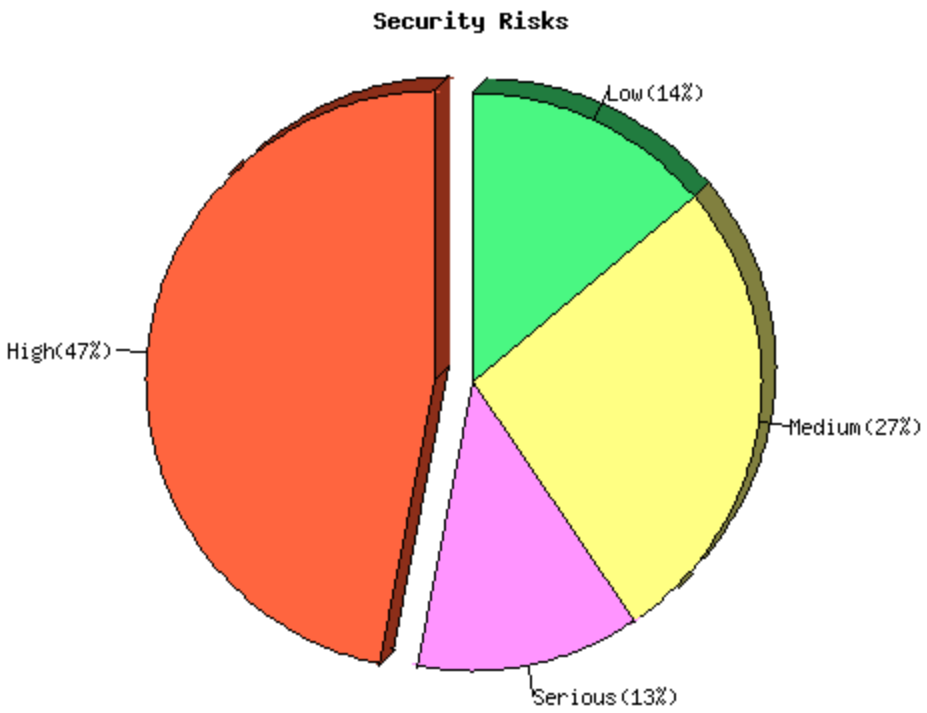

Figure 4

During this initial scan a Program Error popped up on the Windows desktop stating that svchost.exe had been crashed. This was later discovered to be RpcSs. Svchost.exe had the ability to be crashed by the plug-in RPC DCOM Interface DoS plugin. A few moments later, the Windows box experienced a Blue Screen of Death(BSoD) and then proceeded to reboot. SMB null param count DOS (SMB Die) was the plugin that caused the system to BSoD and reboot. After the system came back online, the system was configured to automatically login the administrator account. This was a default setting that was configured during the installation. After the system fully booted, svchost.exe was crashed. Once again it was found that RpcSs was the service that crashed. This time it was able to be crashed by MS RPC Services null pointer reference DoS. During the reboot of the Windows laptop, the Nessus scans continued to run, thus possibly missing vulnerabilities while the target system was offline. Due to the fact that three different plugins caused RpcSs to crash twice and a BSoD, the Nessus Scans were rerun with these three plugins disabled.

The results of the second scan yielded 57 Security Holes, 20 Security Warnings, and 8 Security Notes. This time, the machine did not BSoD and RpcSs was not crashed. Upon further analysis, it was determined that no additional findings were discovered on the second scan that weren't originally identified due to the system reboot. One discovered vulnerability turned out to be a false positive(Nessus ID : 10632) and one warning was listed twice(Nessus ID : 10201). The final results of the Nessus Scans produced 60 Holes, 20 Warnings, and 8 Notes.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus Analysis

Nessus discovered 88 total findings linked with Windows 2000 'straight out-of-the-box'. Nessus displays the results by listing the ports that were discovered as being open and then continues to break each port down by which plugin was able to exploit the finding. On this installation, the following ports were listed as being open. Some ports were listed as being open but were not successfully attacked by Nessus.

List of open ports :

- *loc-srv (135/tcp) (Security hole found)*
- *netbios-ssn (139/tcp) (Security notes found)*
- *microsoft-ds (445/tcp) (Security hole found)*
- *NFS-or-IIS (1025/tcp) (Security notes found)*
- *loc-srv (135/udp) (Security hole found)*
- *netbios-ns (137/udp) (Security warnings found)*
- *netbios-dgm (138/udp)*
- *microsoft-ds (445/udp)*
- *isakmp (500/udp)*
- *unknown (1026/udp) (Security notes found)*
- *unknown (1027/udp)*
- *general/tcp (Security warnings found)*
- *general/udp (Security notes found)*
- *general/icmp (Security warnings found)*
- *general/igmp (Security hole found)*

NOTE Nessus uses commonly used port names to associate the open ports but they are not always correct. TCPView (http://www.sysinternals.com/ntw2k/source/tcpview.shtml) and tlist.exe (from Windows 2000 Support Tools) were used in conjunction to correctly identify open ports and services/processes running on these ports listed. TCPView is freeware from Sysinternals. It is an excellent little program that displays both TCP and UDP endpoints in real-time. Permission was granted in an email by the developer Mark Russinovich for use with this paper(reference: Russinovich e-mail).

1. Loc-srv(135/tcp & udp) – The Microsoft Locator Service, also known as epmap for end-point mapper, is used by RPC(remote procedure call) as a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

mapping service and provides other RPC services. RPC services are assigned dynamically by the operating system. When they try to connect other services, they must go through this mapper to find where they are located. Services don't necessarily have to maintain the same port number on a system.

NOTE - The following list of Nessus ID numbers is a shortened version of the actual Nessus Results page with a brief description of the vulnerability. Each number is a link to the full Nessus Report in Appendix A. Nessus has a web site at http://cgi.nessus.org/plugins/search.html that allows you to manually search every plug-in.

Vulnerability found on port loc-srv (135/tcp)

Nessus ID : 11835 - Gain root remotely

Nessus ID : 11808 - Gain root remotely

Nessus ID : 11159 - Crash RpcSs

Nessus ID : 11133 - Gain root remotely

Warning found on port loc-srv (135/tcp)

Nessus ID : 10736 - Crash RpcSs

Vulnerability found on port loc-srv (135/udp)

Nessus ID : 11890 - run arbitrary code with Local System privileges

Five vulnerabilities and 1 warning were discovered on port 135(TCP and UDP) by Nessus. Port 135 was opened by svchost.exe. Two separate instances of svchost.exe were found running on the system. The first one was discovered to be running RpcSs. RpcSs is the RPC Service that provides port mapping for other RPC services. The other instance of svchost.exe was running EventSystem, Netman, NtmsSvc, SENS, and TapiSrv services.

Nessus was able to crash the RPC service twice. This was what led to the svchost.exe error that was displayed on the screen both before and after the system BSoD and rebooted. By crashing RpcSs, all services that depended on RpcSs were rendered useless. On this system, these services included COM+ Event System, Distributed Link Tracking Client, Distributed Transaction Coordinator, Fax Service, Indexing Service, IPSEC Policy Agent, Messenger, Network Connections, Norton AntiVirus Auto Protect Service, Print Spooler, Protected Storage, Removable Storage, Routing and Remote Access, Symantec Event Manager, Task Scheduler, Telephony, Telnet, Windows Installer, Windows Management Instrumentation, and XtreamLok License Manger.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus was also able to determine that it could remotely connect to the system and was able to gain root privileges. This would allow an attacker or worm to run code at the System level. MsBlater worm is one such worm.

Nessus was also able to discover that a DCE service was running on this port and that information could be released by sending it queries. This information could be used to gain a better understanding of the services/processes running on the system.

2. netbios-ns(137/udp) – Also known as nbname, the NetBIOS name service is a method for NetBIOS-enabled machines to identify each other either by broadcast or by using a name server(WINS).

Warning found on port netbios-ns (137/udp)

Nessus ID : 11830 - Extract Information from Memory

Nessus ID : 10150 - Gain system specific information(computer name, workgroup or domain, currently logged on user)

Two warnings were found on port 137. It was possible for Nessus to uncover NetBIOS information including the computer's name, the workgroup/domain name that the computer joined, the Administrator account was registered for the messenger service, and the MAC address. Once again, any information that an attacker can find can be turned right around and be used against the system.

Ports 137, 138, and 139 were also mentioned under a port 445 NetBIOS vulnerability (10859) that claimed that NetBIOS information can be found on this port and that ports 137, 138, and 139 should be filtered at a network router.

3. netbios-dgm(138/udp) –Also known as nbdatagram, the NetBIOS datagram service uses connectionless communication for unreliable and non-sequenced data exchange. Most commonly, port 138 is used to put information in Network Neighborhood. Port 138 was listed as an open port but Nessus didn't run any specific plugins to directly attack it.

4. netbios-ssn(139/tcp) – Also known as nbsession, the NetBIOS session uses connection-oriented(tcp) communication for dependable exchanges.

Information found on port netbios-ssn (139/tcp)

Nessus ID : 11011 - Gain access to shares or get a list of users on the system

Nessus was able to detect that an SMB server was running on this port. From that, it is possible to retrieve NetBIOS information.

5. Microsoft-ds(445/tcp & udp) – Microsoft CIFS(Common Internet File System) which supports file and printer sharing by using SMB(Server Message Block)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

over TCP. “This protocol was designed to replace the NetBIOS over TCP protocol used by older versions of Windows. “(Bott and Siechert. P.568). SMB over TCP eliminates the need for NetBT which will close the NetBIOS ports(137, 138, and 139) and eliminates the broadcasts that NetBT generates.

Port 445 was by far the most vulnerable port on this Windows 2000 laptop. 54 Vulnerabilities, 13 warnings, and 2 notes were detected by Nessus. Some of the vulnerabilities include being able to run code of choice, gain system privileges, buffer overflows, and crashing services. The warnings and information list that the system was willing to release specific information about the authenticated users, null sessions were possible, elevated privileges were possible, and that it was possible to crash services.

Vulnerability found on port microsoft-ds (445/tcp)

Nessus ID : 10394 - Found Administrator account without a password

Nessus ID : 10531 - Discovered system Service Pack(lack there of)

Nessus ID : 11307 - Run arbitrary code

Nessus ID : 11091 - Elevation of privileges

Nessus ID : 11191 - Gain complete control of system

Nessus ID : 11887 - Run arbitrary code
Nessus ID : 11413 - Gain system privileges
Nessus ID : 11145 - Identity spoofing

Nessus ID : 10866 - Remotely read files

Nessus ID : 11485 - Disable RPC remotely

Nessus ID : 11790 - Execute arbitrary code and gain System privileges

Nessus ID : 11423 - Execute code
Nessus ID : 10434 - Shutdown network browser and add false browser entries
Nessus ID : 11803 - Buffer overflow
Nessus ID : 10404 - Guessed administrator password(blank)
Nessus ID : 10396 - Access to shares as administrator

Nessus ID : 10396 - Access to shares as Administrator

Nessus ID : 10396 - Access to shares as local user

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus ID : 11541 - Gain elevated privileges

Nessus ID : 11878 - Run arbitrary code

Nessus ID : 11326 - Execute arbitrary code

Nessus ID : 10504 - Gain additional privileges

Nessus ID : 10430 - Users can modify certain registry keys

Nessus ID : 11528 - Execute code

Nessus ID : 10964 - Elevated privileges

Nessus ID : 10433 - Forces CPU to run at 100%

Nessus ID : 11789 - Gain additional privileges

Nessus ID : 11147 - Gain control of system

Nessus ID : 11888 - Execute arbitrary code

Nessus ID : 10632 - Execute arbitrary code – False positive – This is just checking to see if hotfix Q277873(Microsoft, MS Knowledge Base Article - 277873) has been installed. This hotfix is for IIS 4.0 or IIS 5.0 which neither of which was installed on the system.

Nessus ID : 10482 - SMB server failure

Nessus ID : 10499 - Security policy corruption

Nessus ID : 10519 - Obtain logon information

Nessus ID : 11144 - Delete digital certificates

Nessus ID : 11300 - Elevated privileges and crash system

Nessus ID : 10485 - Gain privileges

Nessus ID : 11886 - Elevated privileges

Nessus ID : 11787 - Corrupt memory

Nessus ID : 11885 - Elevated privileges

Nessus ID : 11832 - Buffer overflow

Nessus ID : 10668 - Execute arbitrary code

Nessus ID : 10865 - Run arbitrary code

Nessus ID : 10509 - RPC Denial of Service

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus ID : 10861 - Run arbitrary code

Nessus ID : 11177 - Gain control of system

Nessus ID : 11029 - Execute code as with System privileges

Nessus ID : 11212 - Execute arbitrary code

Nessus ID : 10486 - Execute code

Nessus ID : 10525 - Gain privileges

Nessus ID : 11366 - Gain privileges to domain

Nessus ID : 10555 - Attempt brute force password guessing

Nessus ID : 11178 - Corrupt kernel memory

Nessus ID : 10734 - Remote shutdown of system

Nessus ID : 11454 - Guessed administrator password

Nessus ID : 11110 - Crash system

Warning found on port microsoft-ds (445/tcp)

Nessus ID : 10400 - Remote access to registry

Nessus ID : 11301 - Execute arbitrary code

Nessus ID : 10395 - Null session

Nessus ID : 11325 - Execute arbitrary code

Nessus ID : 11215 - Disable digital signing

Nessus ID : 10859 - Get list of authenticated users

Nessus ID : 10860 - Get list of authenticated users

Nessus ID : 10915 - Get list of users that have never logged on

Nessus ID : 11777 - Found files through SMB share

Nessus ID : 10944 - System failure or Elevated privileges

Nessus ID : 11457 - Cached logons

Nessus ID : 11583 - Crash shlwapi.dll

Nessus ID : 10916 - Find accounts with non-expiring passwords

Information found on port microsoft-ds (445/tcp)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus ID : 11011 - Access SMB information

Nessus ID : 10913 - Finds disabled accounts

6. isakmp(500/udp) – Internet Security Association and Key Management Protocol is used to negotiate a security association between a client and a server used during encrypted communications by the IPSec driver. The client and server continue with the ISAKMP process by using IKE(Internet Key Exchange) protocol. Nessus was able to discover that port 500 was open, but it was not able to successfully attack it.

7. NFS-or-IIS(1025/tcp) – Ports 1024 and higher are dynamically assigned ports by the operating system. Nessus lists this port as being NFS or IIS but it was actually neither. On this system, port 1025 was actually opened by mstask.exe. Mstask.exe is Windows Task Scheduler and is used to launch programs at specified times. Mstask.exe launched automatically even though there weren't any applications configured.

Information found on port NFS-or-IIS (1025/tcp)

Nessus ID : 10736 – List DCE services

8. unknown(1026/udp) – Nessus was unable to identify the service listening on the port but it was later determined to be services.exe. "The Service Control Manager(services.exe) is an administrative tool provided in Windows 2000 that allows system services(Server, Workstation, Alerter, ClipBook, etc.) to be created or modified."(Microsoft. Microsoft Security Bulletin MS00-053). These services include Browser(Computer Browser), DHCP(DHCP Client), dmserver(Logical Disk manager), DNScache(DNS Client), Eventlog(Event Log), lanmanserver(Server), lanmandworkstation (Workstation), LmHosts(TCP/IP NetBIOS Helper Service), Messenger, PlugPlay(Plug and Play), Protected Storage, seclogon(RunAs Service), TrkWks(Distributed Link Tracking Client), and Wmi(Windows Management Instrumentation Driver Extensions). All of these services were configured to start automatically at system boot.

Information found on port unknown (1026/udp)

Nessus ID : 10736 – List DCE services

9. unknown(1027/upp) – Nessus was able to discover Port 1027 was open, but it was unable to identify what it was and how to attack it. It was actually opened by Spooler(Print Spooler) which was configured to start automatically at system start up.

10. general/tcp – Nessus discovered three warnings and 2 notes that deal with tcp in general as a protocol and not a specific port. TCP(Transmission

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Control Protocol) is a connection-oriented protocol that needs to establish a 'three-way handshake' before it will transmit data.

Warning found on port general/tcp

Nessus ID : 10201 - Non-random IP IDs

Nessus ID : 10201 – Non-random IP IDs

Nessus ID : 11618 - Does not discard TCP SYN packets

Information found on port general/tcp

Nessus ID : 10336 – Discovered Windows Operating System

Nessus ID : 11268 - Discovered Windows Operating System

It was possible to predict the next value of the IP_ID field of the IP packets sent by the host(this warning was listed twice but it was the same thing). This could leave the box open for man-in-the-middle attacks. It was possible to discover that the remote OS was Windows ME, Windows 2000, or Windows XP. Also, the workstation doesn't discard TCP SYN packets that have the FIN flag set. A packet was sent with the FIN flag set to the target host to close a tcp port. By doing this, it was possible to close a port even though it never created an open connection in the first place.

11. general/udp – UDP(User Datagram Protocol) is a connection-less protocol. This means that once a packet is sent, the sending host has no way to verify if the data was lost. Non-critical information uses UDP like video, where a few bytes of missing data won't necessarily ruin the entire package, just maybe a little blip in the display. Nessus discovered that it was possible to run a traceroute to the target system and have it respond with the correct data.

NOTE Traceroute and ping are two very important commands to a network administrator. Instead of blocking these ICMP packets altogether, it might be better to only block them from external sources by using a firewall or only allowing the replies back into a network by using a reflexive access control list on a router.

Information found on port general/udp

Nessus ID : 10287 – System responds to traceroute

Although this finding is not necessarily a vulnerability in itself, it could help an attacker map out the target network.

12. general/icmp – ICMP(Internet Control Message Protocol) is a protocol used to communicate status information between two host computers. Nessus discovered the target system answers to an ICMP timestamp request. This

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

could allow an attacker to learn the date and time set on the machine. This could help an attacker if any time-sensitive protocols are used. On Windows 2000, authentication protocols like Kerberos and NTLM are time-sensitive.

Warning found on port general/icmp

Nessus ID : 10114 – ICMP timestamp response

Nessus ID : 11834 - accepts loose source routed IP packets

13. general/igmp – IGMP(Internet Group Management Protocol) is a protocol that is used to report multicast group membership to adjacent routers.

Vulnerability found on port general/igmp

Nessus ID : 10179 - Pimp attack crashes system

CIS Scoring Tool Configuration

The CIS Scoring Tool utility was configured to compare the National Security Agency's (NSA) security template for Windows 2000 Professional, NSA-w2k_workstation.inf with the local system. The NSA template has been created as a means of incorporating the guidance recommended by the NSA SNAC(Systems and Network Attack Center) guides. These guides are recommendations published by the NSA in cooperation with several other agencies and companies on how to properly secure a windows 2000 network (http://www.nsa.gov/snac/win2k/download.htm). Several security templates come packaged with the CIS Scoring Tool utility including templates from NIST(National Institute of Standards and Technology), Microsoft, and CIS. This template can also be downloaded directly from the NSA web site at http://www.nsa.gov/snac/win2k/download.htm

CIS Scoring Tool Results

CIS Scoring Tool computes its Overall Score by grading areas on a 10 point scale. The higher the total, the more secure the system is. However, the higher the score the less functionality a system may have. An overall score of 10 might not be possible in a working domain environment. Each of the four areas (below) is capable of producing 2.5 points and partial points are not awarded. For example in the Registry and File Permissions field, having either 1 or 20,000 incorrect permissions set will result in a score of 0 out of a possible 0.625.

The Overall Score is broken down into 4 main areas. The areas are:

1. Service Packs and Hotfixes – CIS Scoring Tool v.2.1.9 uses HFNetChk v3.86 to verify that the latest service packs and hotfixes have been applied

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. Account and Audit Policies – this area verifies that no passwords are older than 90 days and that policies are event log settings match the security template used
3. Security Settings – verifies that Restrict Anonymous is configured and all the Security Options match the template
4. Additional Security Protection – checks the template against any services that are defined, user rights, NTFS permissions, and Registry and File Permissions, and NoLMHash

CIS Scoring Tool Analysis

After running CIS Scoring Tool against the freshly loaded system, the box received an Overall Score of only 2.1. The results are as follows:

Service Packs and Hotfixes: 0 points

Since the evaluated system was a default load of Windows 2000 without service packs or hotfixes installed, it was expected that 0 points would be received. The output was able to point out that Service Pack 4 is the latest service pack available for both Windows 2000 and also Service Pack 4 for Internet Explorer 5.01. It actually listed that 33 total hotfixes were missing including five for Internet Explorer 5.01.

Account and Audit Policies: 0.8333 points

- Password age received 0.8333 points because no passwords were over 90 days since last changed. The system that I used was freshly loaded a few days prior to running the tool. It was possible that this could be 0 points if the evaluated system had been in use for over 90 days.
- Policy Mismatches received a score of 0 points and had 12 mismatches out of a possible 15. Policy Mismatches actually cover three areas including Password Policy, Account Lockout Policy, and Audit Policy. (Table 1)

	Local Setting(Mismatch)	**Desired Template Setting**
Password Policy		
Enforce Password History	0 passwords remembered	24 passwords remembered
Maximum Password Age	42 days	90 days
Minimum Password Age	0 days	1 day
Minimum Password Length	0 characters	12 characters
Passwords Must Meet Complexity Requirements	Disabled	Enabled
Account Lockout Policy		
Account Lockout Threshold	0 invalid logon attempts	3 invalid logon attempts
Audit Policy		
Audit Account Management	No Auditing	Success, Failure
Audit Logon Events	No Auditing	Success, Failure
Audit Object Access	No Auditing	Failure
Audit Policy Change	No Auditing	Success, Failure

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit Privilege Use	No Auditing	Failure
Audit System Events	No Auditing	Success, Failure

Table 1

- Event Log Mismatches received a score of 0 points and had 10 mismatches out of a possible 11.(Table 2)

	Local Setting(Mismatch)	**Desired Template Setting**
Event Log Setting		
Maximum application log size	512 KB	4194250 KB
Maximum security log size	512 KB	4194250 KB
Maximum system log size	512 KB	4194250 KB
Restrict guest access to application log	Disabled	Enabled
Restrict guest access to security log	Disabled	Enabled
Restrict guest access to system log	Disabled	Enabled
Retention method for application log	By Days	Manual
Retention method for security log	By Days	Manual
Retention method for system log	By Days	Manual
Shut down the system when the security audit log is full	Disabled	Enabled

Table 2

Security Settings: 0 points

- Restrict Anonymous received 0 points. HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous was equal to 0.
- Security Options Mismatches received 0 points and had 16 mismatches out of a possible 40.(Table 3)

	Local Setting(Mismatch)	**Desired Template Setting**
Additional restrictions for anonymous connections	None. Rely on default permissions.	No access without explicit anonymous permissions.
Allow system to be shutdown without having to log on	Enabled	Disabled
Amount of idle time required before disconnecting session	15 minutes	30 minutes
Audit the access of global system objects	Disabled	Enabled
Audit use of Backup and Restore privilege	Disabled	Enabled
Clear virtual memory pagefile when system shuts down	Disabled	Enabled
Digitally sign server communications(when possible)	Disabled	Enabled

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Disable CTRL+ALT+DEL requirement for logon	Not Available	Disabled
Do not display last user name in logon screen	Disabled	Enabled
LAN Manager Authentication Level	Send LM & NTLM responses	Send NTLMv2 response only/ refuse LM & NTLM
Number of previous logons to cache	10 logons	0 logons
Prevent users from installing printer drivers	Disabled	Enabled
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Restrict floppy access to locally logged-on user only	Disabled	Enabled
Shut down system immediately if unable to log security audits	Disabled	Enabled
Smart card removal behavior	No Action	Lock Workstation
Unsigned non-driver installation behavior	Silently Succeed	Warn but allow installation

Table 3

Additional Security Protection: 1.25 points
- Available Services Mismatches received 0.625 points. Services are not configured in the NSA template.
- User Rights Mismatches received 0 points and had 11 mismatches out of a possible 35. (Table 4)

	Local Setting(Mismatch)	**Desired Template Setting**
User Rights Assignment		
Access this computer from the network	Everyone, Power Users, Backup Operators, Users, Administrators	Users, Administrators
Backup Files and Directories	Backup Operators, Administrators	Administrators
Bypass traverse checking	Everyone, Power Users, Backup Operators, Users, Administrators	Users
Change the system time	Power Users, Administrators	Administrators
Debug Programs	Administrators	
Log on as a batch job	Test1(a local admin account), SYSTEM	
Log on locally	Guest, Power Users, Backup Operators, Users, Administrators	Users, Administrators

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Profile Single Process	Power Users, Administrators	Administrators
Remove computer from the docking stations	Power Users, Users, Administrators	Users, Administrators
Restore files and directories	Backup Operators Administrators	Administrators
Shutdown the system	Power Users, Backup Operators, Users, Administrators	Users, Administrators

Table 4

- NoLMHash: No value. Registry entry has not been entered– this checks for the Registry setting HKLM\SYSTEM\CurrentControlSet\Control\Lsa\NoLMHash
- NTFS received 0.625 points because all the drives were loaded out with NTFS. This could very easily have been 0 points if the person who loaded out the box did not understand the difference between FAT and NTFS and loaded the system with FAT.
- Registry and File Permissions received 0 points and had 3854 mismatches. This can be a little misleading because the NSA template only has 31 registry settings and 57 file/folder permissions configured. What this 3854 mismatches is showing, is that by possibly configuring one file, folder, or registry key incorrectly, everything that falls below that entry is configured incorrectly also. For example, by giving a user too much access to Program Files folder, they not only have too much access to the folder, but to every program/file/folder that is in the folder which in this evaluation, actually led to 262 mismatches.

NSA Security Template

Security templates are configured in seven areas including Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry, and File System when viewing them with the Security Configuration and Analysis snap-in. When viewing the template in notepad, there is an eight section called Registry Values that will make changes to the registry entries. The NSA security template is configured as follows:

NOTE A lot of information can be found on the internet about the following information. Windows is the most documented operating system out there. The following settings are briefly described in the NSA SNAC guide *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set*. Each setting will be described in detail below.

Account Policies - Account Policies are broken down into three sections.

1. **Password Policy**(Haney, p.24-25)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

a. Enforce Password History – 24 passwords – This prevents users from using the same password over and over again. When a password change is enforced, a user has to use a password that hasn't been used for up to the last 24 passwords.
b. Maximum Password Age – 90 days – This forces a user to change their password at least every 90 days. A user can change their password more frequently, but it is not mandatory.
c. Minimum Password Age – 1 day – A user must maintain their newly changed passwords for a minimum of 1 full day. This will help prevent a user from changing their password 24 times in a row just to keep their original password.
d. Minimum Password Length – 12 characters – 12 character passwords are pretty difficult to guess for an attacker but they are fairly easy for password crackers to break.
e. Passwords Must Meet Complexity Requirements – enabled – This forces a password to use complex passwords by requiring that they have three of four password settings where the password must have an upper case character, a lower case character, a number, and/or a special character. Passwords must also not contain a portion of the user's login. Another requirement where passwords must be 6 characters in length is overridden by the previous setting.(12 characters)
f. Store passwords using reversible encryption for all users in the domain – Disabled –It is used for CHAP(Challenge Handshake Authentication Protocol) through remote access and for some applications. This is a pretty non-secure way of storing passwords.

2. **Account Lockout Policy**-(Haney, p.27)
   a. Account lockout duration – 15 minutes – After an account has been locked out, it will unlock itself after 15 minutes.
   b. Account lockout threshold – 3 invalid lockout attempts – After a user types in an invalid password 3 times, the account will become locked out and the user will not be able to login.
   c. Reset account lockout counter after – 15 minutes – For the 3 invalid login attempts to lock out an account, the 3 attempts must occur within 15 minutes of each other.

NOTE It may be better to configure passwords to be locked out until an administrator unlocks the account. In large companies, people get hired and fired very fast and accounts could remain after personnel have left. By allowing the account to unlock itself could leave a valid logon for someone to try and guess or for someone to use after they have left the company.

3. **Kerberos Policy** – The Kerberos Policy is not defined in the NSA security workstation template, because this area is configured for a Domain Security Policy on the Domain Controller. Kerberos is the default authentication used by Windows 2000.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Local Policies – Local Policies are broken down into three sections.

1. **Audit Policy** – (Haney, p.30)
   a. Audit account logon events – Success and Failure – An event is logged when a user tries to connect from another computer to the local computer and where the local computer is used to validate the account.
   b. Audit account management – Success and Failure – An event is logged anytime a user/group account is changed in any way, including creating or deleting an account.
   c. Audit directory service access – no auditing – No events are logged whenever a user tries to access a domain controller object. This setting is only relevant to domain controllers.
   d. Audit logon events – Success and Failure – An event is logged in the local security log when an attempt is made to log on or off the local system, including over the network and by services.
   e. Audit object access – Failure – An event is logged anytime a user tries to access a file, folder, etc. that they do not have permission to. If auditing is configured on individual files and folders, then this setting must also be enabled for events to be logged.
   f. Audit policy change – Success and Failure – An event is logged anytime a change is made to user rights, audit policies or trust policies.
   g. Audit privilege use – Failure – This will only generate an event when a user tries to use a right that they don't have. However, not all user rights are logged including "Bypass Traverse Checking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Back Up Files and Directories, and Restore Files and Directories."(Haney, p.30)
   h. Audit process tracking – no auditing – No events will be generated for tracking system processes like whenever an application is started or stopped.
   i. Audit system events – Success and Failure – An event is logged whenever something happens to the system(i.e. shutdown or restart).

2. **User Rights Assignments** – There are 34 different settings that can be configured for User Rights. The NSA template only defines the following 18: (Haney, p.32–37)
   a. Access this computer from the network(Users, Administrators) – This allows anyone in the Users and Administrators groups to connect to this computer remotely.
   b. Back up files and directories(Administrators) – This setting allows administrators to back up all files and folders regardless of the file/folder permissions present.
   c. Bypass traverse checking(Users) – This allows everyone in the Users group to go through a parent directory that they are blocked from to access files and folders that they are not specifically restricted from.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

d. Change the system time(Administrators) – Only administrators are permitted to change the time. A change in the system time will falsify audit logs.
e. Create a pagefile(Administrators) – When administrators are logged on, a pagefile can be created by an API(Application Programming Interface) to create extra virtual memory if physical memory is running low.
f. Force shutdown from a remote system(Administrators) – This will prevent malicious users from being able to shut down the system remotely by only allowing administrators this option.
g. Increase quotas(Administrators) – This allows a process to increase the processor quota for another process. This can only happen if administrators are logged on. It is possible to create a Denial of Service attack by misusing this right to allow one process to increase processor quota while another process may not have enough resources to run properly.
h. Increase scheduling priority(Administrators) – Similar to the Increase Quota right, this would allow an administrator to increase the priority of a process in Task Manager.
i. Load and unload device drivers(Administrators) – Only administrators are allowed to install or uninstall Plug and Play device drivers. This does not pertain to non-Plug and Play device drivers. Plug and Play drivers are considered 'trusted' by Microsoft and run at a higher privilege.
j. Log on locally(Users, Administrators) – Only users and administrators are allowed to log on to the local system. This setting will not prevent domain accounts from being aloud to logon to the domain controller from this workstation.
k. Manage auditing and security log(Administrators) – Unauthorized access to the audit logs could falsify them if data is modified. This right allows only administrators to clear the logs and allows only administrators to configure auditing on specific files, folders, etc.
l. Modify firmware environment values(Administrators) – This allows only administrators to modify firmware. On x86-based computers, the only firmware environment that can be modified is the Last Known Good Configuration.
m. Profile single process(Administrators) – Only administrators can use Windows performance monitoring tools on the system to monitor non-system processes.
n. Profile system performance(Administrators) – Only administrators can use Windows performance monitoring tools to monitor system processes.
o. Remove computer from docking station(Users, Administrators) – All Users and Administrators can undock a laptop from a docking station. This requires a user to be logged in although this does not prevent a malicious user from just ripping it out.
p. Restore files and directories(Administrators) – Only administrators can restore files and directories no matter what permissions are set on the original files and/or folders.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

q. Shut down the system(Users, Administrators) – All Users and Administrators can shut the system down. Once again this does not prevent a malicious user from just turning the power off.
r. Take ownership of files and other objects(Administrators) – This right will allow an administrator to take ownership of any object no matter what permissions have been set on it.

3. **Security Options** – Of the 40 configurable security options, 7 of them have a value of not defined and have been omitted below.(Haney, p.37-57)
   a. Additional restrictions for anonymous connections(No access without explicit anonymous permissions) – This will prevent anonymous users from listing domain user names and share names "by removing the "Everyone" and "Network" groups from the anonymous user token."(Haney, p.38)
   b. Allow system to be shut down without having to log on(Disabled) – This forces users to successfully logon before being able to properly shut down the system. Once again this will not prevent a hard boot of the system.
   c. Allowed to eject removable NTFS media(Administrators) – Only administrators are allowed to eject, format, or label NTFS media.
   d. Amount of idle time required before disconnecting session(30 minutes) – After 30 minutes of idle time in an SMB session, the session is disconnected.
   e. Audit the access of global system objects(Enabled) – Allows for the auditing of global system objects which include events and DOS devices. The audit object access audit policy must also be enabled which it is in this template.
   f. Audit the use of Backup and Restore privilege(Enabled) – This should actually be called 'Audit ALL privilege use'. When audit privilege use policy is enabled, not all uses of user rights are audited as stated above, with this setting enabled, they are.
   g. Automatically logoff users when logon time expires(local) (Enabled) – This will force a user to be disconnected from an SMB session if logon hours have expired.
   h. Clear virtual memory pagefile when system shuts down(Enabled) – This prevents any information that is in virtual memory from being available after the system has been shut down. It is possible to boot into a different operating system and access the hard drive where this information might be stored.
   i. Digitally sign client communication(always)(Disabled) – This will not force the client to digitally sign all SMB traffic. If enabled both client and server need to enabled for SMB signing to work
   j. Digitally sign client communication(when possible) (Enabled) – This will force SMB client to use SMB packet signing whenever the server has this option enabled.
   k. Digitally sign server communication(always)(Disabled) – This will not force the SMB server to always digitally sign SMB traffic.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

l. Digitally sign server communication(when possible) (Enabled) – This will force the SMB server to digitally sign its SMB traffic if the client also has SMB digital signing enabled.
m. Disable CTRL+ALT+DEL requirement for logon(Disabled) – This requires the user to press CTRL+ALT+DEL to log on to the system. By default, a windows system will automatically log in as an administrator.
n. Do not display last user name in logon screen(Enabled) – This will remove the last logged-on username from appearing in the logon box for the next user trying to logon. By leaving the last user name in the logon box, anyone with physical access to the workstation will know an authorized user account to the system or network.
o. LAN Manager Authentication level(Send NTLMv2 response only/refuse LM & NTLM) – NTLMv2 is the only accepted authentication method used for accessing pre-Windows 2000 systems. By default, Windows 2000 systems will authenticate using Kerberos if a Domain Controller is present. LM and NTLM have become extremely easy to crack with utilities like L0phtCrack(http://www.atstake.com/research/lc/download.html).
p. Number of previous logons to cache(0 logons) – This will prevent users from being able to logon if the domain is not available. However, a user can still log on locally if they have a local account created.
q. Prevent system maintenance of computer account password(Disabled) – This will not cause the operating system to change the computer account password on a weekly basis.
r. Prevent users from installing printer drivers(Enabled) – This will prevent users from being able to install printer drivers unless the drivers already reside on the local machine.
s. Prompt user to change password before expiration(14 days) – Currently, the NSA template forces a user to change their password every 90 days. 14 days prior, this setting will prompt a user for the change at logon.
t. Recovery Console: Allow automatic administrator logon(Disabled) – This will force a user to enter a username and password upon entering the Recovery Console.
u. Recovery Console: Allow floppy copy and access to all drives and all folders(Disabled) – This prevents the SET command from being used in the recovery console.
v. Restrict CD-ROM access to locally logged-on user only(Enabled) – Network access to the local CD-ROM is not allowed.
w. Restrict floppy access to locally logged-on user only(Enabled) – Network access to the local floppy disk drive is not allowed.
x. Secure Channel: Digitally encrypt or sign secure channel data(always)(Disabled) – This setting if enabled, would force a system to always send digitally encrypted or digitally signed channel data.
y. Secure Channel: Digitally encrypt secure channel data(when possible) (Enabled) – All secure channel data will be digitally encrypted whenever possible.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

z. Secure Channel: Digitally sign secure channel data(when possible) (Enabled) – All secure channel data will be digitally signed whenever possible.
aa. Secure Channel: Require Strong(Windows 2000 or later) session key(Disabled) – All secure channel data will not require the use of a strong encryption key(128-bit).
bb. Send unencrypted password to connect to third party SMB servers(Disabled) – This will prevent the system from sending SMB passwords in clear text for authentication to third-party SMB servers.
cc. Shut down system immediately if unable to log security audits(Enabled) – This will configure the local system to crash-on-audit-fail if the security log fills. Only then will an administrator be allowed to log on so that they can then clear the audit logs manually.
dd. Smart card removal behavior(Lock Workstation) – If a smart card is used for authentication, then the workstation will be locked out if the user removes their smart card from the reader.
ee. Strengthen default permissions of global system objects(e.g. Symbolic Links) (Enabled) – This will strengthen the permissions of shared system resources so that regular users only have read access to shared objects that they didn't create.
ff. Unsigned driver installation behavior(Warn but allow installation) – A warning message will be displayed on the screen when an unsigned driver(non-Windows certified) is about to be installed.
gg. Unsigned non-driver installation behavior(Warn but allow installation) – A warning message will be displayed on the screen when an unsigned non-driver is about to be installed.

Event Log – Settings for event logs(Haney, p.62)

a. Maximum application log size(4194240 kilobytes)
b. Maximum security log size(4194240 kilobytes)
c. Maximum system log size(4194240 kilobytes)

Log sizes are set at about 4 GB. If the logs are too small, the systems will shut down too frequently due to the Crash-on-audit-failure setting.

NOTE Event viewer may have a difficult time trying to open a log file if it gets too large.

d. Restrict guest access to application log(Enabled)
e. Restrict guest access to security log(Enabled)
f. Restrict guest access to system log(Enabled)

This will prevent guests and null users from being allowed to open any of the event logs. By default, only the security log is configured this way.

g. Retention method for application log(Manually)
h. Retention method for security log(Manually)
i. Retention method for system log(Manually)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Forces an administrator to manually clear all event logs and will prevent circular logging where the operating system overwrites previous logs once the log has reached maximum size. Careful, if logs are filled, new data will be discarded.

j. Shut down the computer when the security audit log is full(Enabled) - Crash-on-audit-failure will force an administrator to log on and manually clear the security log once it reaches maximum size.

Restricted Groups – The only restricted group is the Power Users group. By placing the Power Users group here without any accounts listed under it, no one can add themselves to this group and attain the permissions and rights of the Power Users group.

System Services – No system services are defined by default in the NSA template. In the Security Configuration Tool Set SNAC guide, it is recommended that all unnecessary services be disabled.(Haney, p.68) This will have to be conducted on a case-by-case basis.

Registry – Permissions have been set on specific registry keys to prevent non-administrators from gaining higher than needed access to important settings and data.(Haney, p.76-79) Permissions have been set on the following:

NOTE Several registry settings have been omitted from the descriptions below due to the key/subkey/entry not being present on a default Windows 2000 Professional installation.

a. Classes_Root – Contains the file associations for file extensions and their associated programs, and it also contains configuration data for COM(Common Object Model) objects.
b. Machine\software – Contains program variables that apply to all users of the computer.
c. Machine\software\microsoft\netdde – Contains settings for NetDDE (Network Dynamic Data Exchange). NetDDE allows applications like clipbook and MS Chat to exchange data.
d. Machine\software\microsoft\OS/2 Subsystem for NT – Contains basic software support information for the Microsoft OS/2 version 1.x subsystem.
e. Machine\software\microsoft\windows nt\CurrentVersion\AsrCommands – Contains ASR(Automatic Server Recovery) commands.(Haney, p.76)
f. Machine\software\microsoft\windows nt\CurrentVersion\Perflib – Contains settings for performance library. Performance library data is displayed by Performance Monitor.
g. Machine\software\microsoft\windows\CurrentVersion\Group Policy – Contains information for settings in Group Policy.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

h. Machine\software\microsoft\windows\CurrentVersion\Installer – Contains configuration information for Windows Installer service which makes installs and uninstalls of software easier to manage.
i. Machine\software\microsoft\windows\CurrentVersion\Policies – Contains several registry entries that Group Policy controls.
j. Machine\system – Contains current control sets and control sets used to start the system.
k. Machine\system\clone – Contains a temporary copy of the control set during system boot up. After a successful startup, this subkey will become the Last Known Good configuration.
l. Machine\system\controlset001(through 010) – Contains previous copies of control sets that can be used to boot the system.
m. Machine\system\CurrentControlSet\Control\SecurePipeServers\winreg – Contains permissions for accessing the registry remotely.
n. Machine\system\CurrentControlSet\Control\wmi\security – Contains settings for WMI(Windows Management Instrumentation).
o. Machine\system\CurrentControlSet\enum – Contains configuration information for hardware devices installed on the system.
p. Machine\System\CurrentControlSet\Hardware Profiles – Retains changes to the original hardware configuration.
q. Users\.default – Contains the profile that is used for the system prior to any users actually logging on.
r. Users\.default\software\microsoft\netdde – Contains setting for NetDDE(Network Dynamic Data Exchange). NetDDE allows applications like clipbook and MS Chat to exchange data.

File System – Permissions have been applied to system files and folders to prevent non-administrators with higher than needed access (Haney, p.88-94). Permissions have been set on the following:

NOTE Several file/folder settings have been omitted from the descriptions below due to the file/folder not being present on a default Windows 2000 Professional installation.

a. %Program Files% – Folder where all programs are installed by default.
b. %System Directory% - Contains many system files used for basic operation.
c. %System Directory%\appmgmt – "Contains application management files used for software installations."(Haney, p.88).
d. %System Directory%\config – Contains several hive files that are used to build the registry during boot up.
e. %System Directory%\DTCLog – Contains the "log file for MS Distributed Transaction Coordinator."(Haney, p.88)
f. %System Directory%\GroupPolicy – "Folder containing local Group Policy Objects.(Haney, p.88)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

g. %System Directory%\ias – Contains the databases used by IAS(Internet Authentication Service).
h. %System Directory%\Ntbackup.exe – Executable program to launch Backup.
i. %System Directory%\NtmsData – Folder that contains the databases for Removable Storage.
j. %System Directory%\rcp.exe – Executable for the remote copy command.
k. %System Directory%\regedt32.exe – Executable for launching the registry editing tool.
l. %System Directory%\ReinstallBackups – Contains original drivers that can be rolled back to if need be.
m. %System Directory%\rexec.exe – Executable that allows for executing programs on remote systems. Windows 2000 does not come with the REXEC service by default. It must be installed from the Windows 2000 Server Resource Kit.
n. %System Directory%\rsh.exe – Executable that allows for running commands on a remote computer. Windows 2000 does not come with the RSH service by default. It must be installed from the Windows 2000 Server Resource Kit.
o. %System Directory%\secedit.exe – Executable that will configure and/or compare the local system with a security template.
p. %System Directory%\Setup – Contains .dll files used for installation of certain applications.
q. %System Directory%\spool\printers – Contains printer spool which is the area on the local hard drive that is used to store information before it is sent to the printer.
r. %System Drive%\ - Contains the Windows 2000 operating system .
s. %System Drive%\autoexec.bat – A file used to launch automatically at boot up to launch DOS commands to set environment parameters. Comes with Windows 2000 for backward compatibility.
t. %System Drive%\boot.ini – File used to determine which operating system to boot into.
u. %System Drive%\config.sys – A file containing DOS commands used to describe device drivers that are loaded at boot up. Comes with Windows 2000 for backward compatibility.
v. %System Drive%\Documents and Settings – Folder that contains all profiles on the system.
w. %System Drive%\Documents and Settings\Administrator – Folder that contains the profile for the built-in administrator account.
x. %System Drive%\Documents and Settings\All Users – Folder that contains the profile that is common among all users.
y. %System Drive%\Documents and Settings\All Users\Documents\DrWatson – Folder that contains the DrWatson error log.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

z. %System Drive%\Documents and Settings\All Users \Documents\ DrWatson\drwtsn32.log – Log file for DrWatson errors generated by the system.
aa. %System Drive%\Documents and Settings\Default User – Folder that contains the profile used whenever a new user logs on.
bb. %SystemDrive%\IO.sys – Contains information needed to start the local system. Replaces config.sys and autoexec.bat.
cc. %SystemDrive%\MSDOS.sys – Works with IO.sys to help boot the system in a DOS environment.
dd. %SystemDrive%\ntdetect.com – Detects hardware during boot up in Windows 2000.
ee. %SystemDrive%\ntldr – Ntldr is what actually loads the operating system during boot up.
ff. %SystemDrive%\Temp – Folder that contains temporary files.
gg. %SystemRoot% - Folder where the Windows 2000 operating system is installed. By default it is the \winnt folder.
hh. %SystemRoot%\$NtServicePackUninstall$ - Contains files that would be reinstalled if a Service Pack uninstall is run.
ii. %SystemRoot%\debug – Folder that contains several system logs.
jj. %SystemRoot%\Debug\UserMode – Contains log files for applying group policy.
kk. %SystemRoot%\Offline Web Pages – Folder that stores downloaded web pages so that they can be viewed at a later time when internet access may be denied.
ll. %SystemRoot%\regedit.exe – Executable for launching registry editing tool.
mm. %SystemRoot%\Registration – Folder containing CLB(Component Load Balancing) registration files.(Haney, p.93)
nn. %SystemRoot%\repair – Folder that contains backups of important registry and system files that could be used during a system repair.
oo. %SystemRoot%\security – Contains security templates that ship with Windows 2000.
pp. %SystemRoot%\Tasks – Folder that contains tasks/jobs that can be run at specified times by Task Scheduler.
qq. %SystemRoot%\Temp – Folder that holds temporary files.

**The security template also include c:\autoexec.bat, c:\boot.ini, c:\config.sys, c:\ntdetect.com, and c:\ntldr listed at the end but they have all been covered previously. C:\ntbootdd.sys is also listed at the bottom but it covers permissions for SCSI drivers which is irrelevant on the current laptop.

Registry Values – There is a special section at the end of a security template that sometimes gets missed. When viewing a template with the Security Template snap-in, this section will not appear. The Registry Values section contains settings to modify registry entries and must be viewed in a text editor such as notepad.exe.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

NOTE most of the following registry entries have already been addressed in the NSA template in discussions above. These instances will reference the setting in the template that covers the registry setting.

a. MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1 – This is the same setting as Protect kernel object attributes from above.
b. MACHINE\System\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90 – This send a warning once the security log reaches 90% full.(*NOTE* Service Pack 3 or higher must be applied)
c. MACHINE\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset=4,1 – This helps protect a system from having its Browser service shut down.
d. MACHINE\System\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=4,1 – This helps protect against a denial-of-service attack against a WINS server.
e. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2 – This will disable IP source routing which helps protect against spoofing.
f. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0 – This prevents Dead Gateway Detect which could make a system use a different gateway.
g. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0 – This make ICMP traffic travel the shortest path to its destination.
h. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0 – This will disable the IRDP(Internet Router Discovery Protocol).
i. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,2 – This will help protect a system from a SYN flood attack.
j. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen=4,100 – Value used as a limit for Half-Open sessions before SynAttackProtect is implemented.
k. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired=4,80 - Value used as a limit for retired Half-Open sessions before SynAttackProtect is implemented.
l. MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000 – TCP will send a keep-alive packet after 5 minutes of being idle.(300000ms = 5 minutes)
m. MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255 – This will prevent all media from automatically launching when introduced to the system.
n. MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=4,0 – This will allow a system to log on with the Administrator account without requesting a logon a password.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

o. machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1 - Same setting as Secure channel: Digitally sign secret channel data(when possible) from above.
p. machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1 – Same setting as Secure channel: Digitally encrypt secure channel data(when possible) from above.
q. machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0 – Same setting as Secure channel: Require strong(Windows 2000 or later) session key from above.
r. machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0 – Same setting as Secure channel: Digitally encrypt or sign secure channel data(always) as above.
s. machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0 – Same setting as Prevent system maintenance of computer account password as above.
t. machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,0 – Same setting as Digitally sign client communication(always) from above.
u. machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1 – Same setting as Digitally sign client communication(when possible) from above.
v. machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0 – Same setting as Send unencrypted password to connect to third-party SMB servers as above.
w. machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,0 - Same setting as Digitally sign server communication(always) from above.
x. machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1 - Same setting as Digitally sign server communication(when possible) from above.
y. machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,1 – Same setting as Automatically log off users when logon time expires(local) as above.
z. machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30 – Same setting as Amount of idle time required before disconnecting session as above.
aa. machine\system\currentcontrolset\control\session manager\protectionmode=4,1 – Same setting as Strengthen default permissions of global system objects(e.g. Symbolic Links)
bb. machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1 – Same setting as Clear virtual memory pagefile when system shuts down as above.
cc. machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1 – Same setting as Prevent users from installing printer drivers as above.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

dd. machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2 – Same setting as Additional restrictions for anonymous connections as above.
ee. machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5 – Same setting as LAN Manager authentication level as above.
ff. machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1 – Same setting as Audit use of Backup and Restore privilege from above.
gg. machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1 - Same setting as Shut down system immediately if unable to log security audits as above.
hh. machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1 – Same as setting Audit the access of global system objects as above.
ii. machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0 – Same as setting Allow system to be shut down without having to log on as above.
jj. machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1 – Same as setting Do not display last user name in logon screen.
kk. machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0 – Same as setting Disable CTRL+ALT+DEL requirement for logon as above.
ll. machine\software\microsoft\windows nt\currentversion\winlogon\ scremoveoption=1,1 – Same as setting Smart Card removal behavior as above.
mm. machine\software\microsoft\windows nt\currentversion\winlogon\ passwordexpirywarning=4,14 – Same as setting Prompt user to change password before expiration as above.
nn. machine\software\microsoft\windows nt\currentversion\winlogon\ cachedlogonscount=1,0 – Same as setting Number of previous logons to cache(in case domain controller is not available) as above.
oo. machine\software\microsoft\windows nt\currentversion\winlogon\ allocatefloppies=1,1 – Same as setting Restrict floppy access to locally logged on user only as above.
pp. machine\software\microsoft\windows nt\currentversion\winlogon\ allocatedasd=1,0 – Same as setting Allowed to eject removable NTFS media as above.
qq. machine\software\microsoft\windows nt\currentversion\winlogon\ allocatecdroms=1,1 – Same as setting Restrict CD-ROM access to locally logged on user only as above.
rr. machine\software\microsoft\windows nt\currentversion\setup\ recoveryconsole\setcommand=4,0 – Same setting as Recovery Console: Allow floppy copy and access to all drives and folders as above.
ss. machine\software\microsoft\windows nt\currentversion\setup\ recoveryconsole\securitylevel=4,0 – Same setting as Recovery Console: Allow automatic administrative logon as above.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

tt. machine\software\microsoft\non-driver signing\policy=3,1 – Same setting as Unsigned non-driver installation behavior as above.
uu. machine\software\microsoft\driver signing\policy=3,1 – Same setting as Unsigned driver installation behavior as above.

Initial Scanning Conclusion

After running both the Nessus Security Scanner and CIS Scoring Tool, it is easy to see that a Windows 2000 'straight out-of-the-box' load is in rough shape. Nessus discovered 88 findings and CIS Scoring Tool produced a score of 2.1/10. The box is vulnerable to many attacks and it is capable of releasing and broadcasting information freely to the network. Valuable information about both the system and the users can be gained by using simple utilities that are free to download from the internet.

NOTE Although the system did score a 2.1/10, it was possible that it could have only received a score of 0.625/10 if the passwords were older than 90 days and if the system had been loaded out with FAT.

Lockdown Procedures

1. To bring the box up-to-date with the latest Microsoft downloads, Windows Update service was run (Oct 20, 2003). Windows Update had to be run several times. Each time, new results would pop up with different results. It took several system reboots to bring the system fully up-to-date. Also, Windows Office update was run http://office.microsoft.com/officeupdate/default.aspx (Microsoft, Windows Office Downloads). By just running the Windows Automatic updates, Office XP was not detected as needing security updates. With CIS Scoring Tool using HfNetChk, Office XP was detected needing several updates.
2. The NSA-w2k_workstation.inf security template was incorporated into the system by using Security Configuration and Analysis snap-in in the Microsoft Management Console(mmc.exe).
3. Renamed local Administrator account and changed all passwords to comply with new requirements enforced by the NSA template
4. Shutdown several unneeded services including Fax Service, Internet Connection Sharing, Messenger, Print Spooler was changed from Automatic to Manual, Task Scheduler, Telephony, and Wireless Configuration.
5. Disable NetBIOS over TCP/IP(Wins TAB of Local area connection)
6. Removed File and Printer Sharing for Microsoft Networks(Local area connection)

Reevaluation

CIS Scoring Tool Results(Figure 5)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

At this point the system was reevaluated. By applying the latest service packs and the NSA template, the box should have theoretically scored a perfect 10 when using CIS Scoring Tool. The final results can be viewed below and the final Scan log is in Appendix B.

2 flaws existed in the final report. Under Security Hofixes Missing, it was determined that one hotfix, MS03-037 (Microsoft, MS03-037…) was still missing. After going back and personally installing the hotfix (see below), the CIS Scoring Tool was still reporting that the hotfix was missing. (1.25 points were not given)

NOTE The Hotfix Report from the CIS Scoring Tool reported that MSO3-037(KB822150) was not installed. It gave the link http://support.microsoft.com/default.aspx?kbid=822150 as the website to download the hotfix. After downloading and successfully installing VBA64-*KB822150-X86-ENU.exe, the CIS Scoring Tool still reports that the patch for MS03-037 was still missing.

NOTE HfNetChk Pro 4 was downloaded from http://www.shavlik.com/downloads.aspx. This is the latest version. CIS Scoring Tool is using the older version v3.86. The missing hotfix was not detected as being missing on Pro 4 version. Also, by installing HfNetChk Pro 4, MDAC 2.7 with SP1 and MSXML 4.0 SP2 Parser and SDK also had to be installed. Windows Update then reported that an additional hotfix now had to be installed to bring the system up-to-date.

CIS Scoring Tool also reported that 11 Registry and File Permissions were mismatched resulting in a missed 0.625 points. These were all false positives. Three of these(marked with * below) are documented on the CIS web site at http://www.cisecurity.com/bench_win2000.html (CIS. Center for…) as being false positives on a default Windows 2000 installation for the NIST and Win2kProGold_R1.2.inf security templates, but they have also been generated as false positives here for the NSA template as well.

11 mismatches
1. - machine\software\Classes *
2. - machine\software\microsoft\windows\currentversion\group policy *
3. - machine\software\microsoft\windows nt\currentversion\perflib\009
4. - machine\system\controlset001 *
5. - machine\system\currentcontrolset\control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties
6. - machine\system\currentcontrolset\control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties
7. - machine\system\currentcontrolset\control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8. - machine\system\currentcontrolset\control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties
9. - machine\system\currentcontrolset\control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties
10. - machine\system\currentcontrolset\control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties
11.- machine\system\currentcontrolset\control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

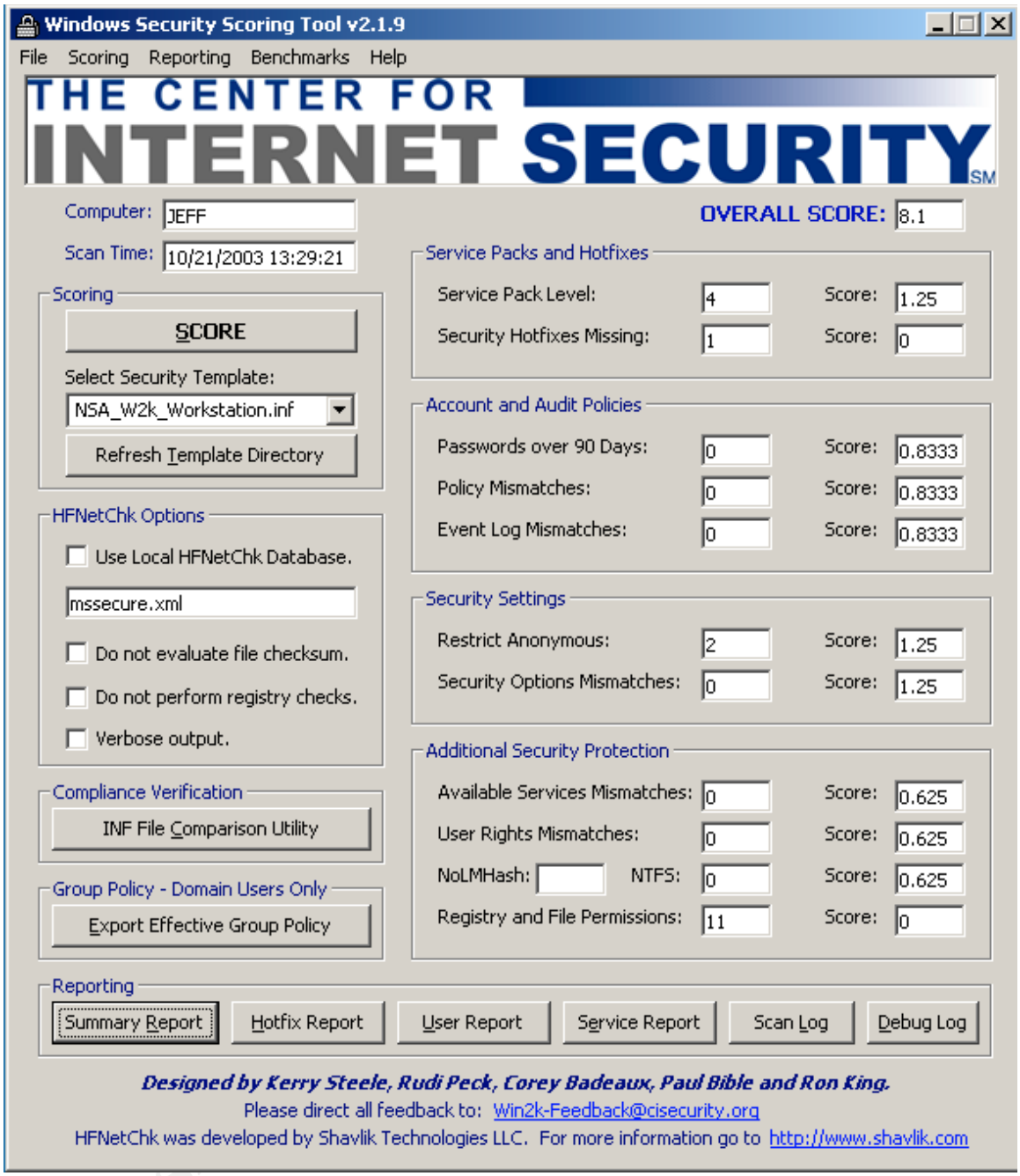

Figure 5

Nessus Results

Nessus was rerun against the system. This time, the Windows target laptop did not BSoD and svchost.exe did not crash. Remarkably, the system went from 60 Vulnerabilities to 0, 20 Warnings to 3, and 8 Notes to 3.

Warnings that remained:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Warning found on port general/tcp

Nessus ID : 10201 - Non-random IP IDs

NOTE This warning was once again listed twice but it is only counted as one warning found.

Nessus ID : 11618 - Does not discard TCP SYN packets

Warning found on port general/icmp

Nessus ID : 10114 – ICMP timestamp response

Information found:

Information found on port general/tcp

Nessus ID : 10336 – Discovered Windows Operating System

Nessus ID : 11268 - Discovered Windows Operating System

Information found on port general/udp

Nessus ID : 10287 – System responds to traceroute

Results After Lockdown

At this point, several vulnerabilities still exist.

a. The operating system generates non-random IP IDs. This is a function of the Windows operating system and would only be fixed by a Microsoft patch. At the present time, no such update is available.
b. The system does not discard TCP SYN packets when the FIN flag is set. This is not necessarily a vulnerability but more of a function of the TCP three-way handshake that could allow an attacker to identify open ports. A firewall can be configured to try and block this.
c. Several protocols use time-based authentication. The system responds to an ICMP timestamp request which could help an attacker to discover the time set on the system. ICMP Timestamp request(type 13) and ICMP Timestamp reply(type 14) should be blocked at a perimeter router.
d. Nmap and Nessus(by using Nmap)were able to figure out the operating system on the box remotely. Nmap will send special TCP/IP packets at a target and will analyze the results and compare it to a database that it has filled with expected results from different operating systems. Once a match is made, the remote operating system is then 'guessed'. http://www.insecure.org/nmap/data/nmap_manpage.html (Insecure.org, Nmap network…)
e. The system responds to a traceroute command. Traceroute(tracert.exe) is an important administration tool for discovering paths to remote systems. Traceroute can also be blocked at a router by not allowing ICMP Tracertoute(type 30) packets to pass.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusion

By default, Windows 2000 Professional deployed on a laptop is not secure and is extremely vulnerable to malicious attacks. Over the last few years, numerous vulnerabilities have been discovered. Microsoft is constantly trying to keep up with these by releasing hotfixes and patches. Too often they don't get applied to systems before a security incident has occurred. Nessus Security Scanner and the CIS Benchmark Security Tool are two free-to-use utilities that can help administrators examine many of these vulnerabilities and even take it a step beyond. There are many ways to lock down a Windows system, and there isn't a universally recognized best method. By analyzing the data from these two utilities, an administrator can have a good assessment of internal and external vulnerabilities. After applying the recommended lockdowns, it is possible to have a reasonably secure system, even with a Windows 2000 laptop.

© SANS Institute 2004, Author retains full rights.

References

@Stake. “Products.” URL: http://www.atstake.com/research/lc/download.html (4 Nov. 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Bott, Ed, and Carl Siechert. Microsoft Windows Security for Windows XP and Windows 2000 Inside and Out. Redmond: Microsoft Press, 2003.

CIS. "Center for Internet Security Benchmarks and Scoring Tool for Windows 2000 and Windows NT). February, 2003.
URL: http://www.cisecurity.org/bench_win2000.html (4 Nov. 2003)

CNET. "Win Zip 8.1". URL: http://download.com.com/3002-2250-8132587.html?tag=dir (4 Nov. 2003)

CNET. "Norton Antivirus 2004." URL: http://download.com.com/3001-2239-10223639.html (4 Nov. 2003)

Dell. "Downloads." URL:
http://support.dell.com/filelib/format.aspx?releaseid=r57447 (4 Nov. 2003)

Deriason, Renaud. "Introduction." URL: www.nessus.org/intro.html (4 Nov. 2003)

Heinbockel, William. "Nessus Analysis: NASL and Plugins." 20 Jan. 2003. URL:
http://www.rit.edu/~wjh3710/plugin_stats.html (4 Nov. 2003)

Haney, J. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. NSA. December 2000. Version 1.2.

Insecure.org. "Nmap network security scanner man page: URL:
http://www.insecure.org/nmap/data/nmap_manpage.html (4 Nov 2003)

Kensington. "Notebook Security". URL: www.pcsecurity.com/html/2178.html (4 Nov. 2003)

Microsoft. "DirectX 8.1b Runtime for Windows 2000." URL:
http://www.microsoft.com/downloads/details.aspx?FamilyID=a2f63641-f038-43d1-94de-47a8306e4e1d&DisplayLang=en (4 Nov. 2003)

Microsoft. "Internet Explorer 6 Service Pack 1." URL:
http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/default.asp (4 Nov. 2003)

Microsoft. "Microsoft Knowledge Base Article – 277873." 23 May, 2003. URL:
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q277/8/73.ASP&NoWebContent=1 (3 Nov 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft. "Microsoft Security Bulletin MS03-037." 3 Sep. 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-037.asp (4 Nov 2003)

Microsoft. "Microsoft Security Bulletin MS00-053." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-053.asp (4 Nov. 2003)

Microsoft. ":VBA: Availability of the Microsoft VBA Security Update MS03-037" 15 Sep. 2003. URL: http://support.microsoft.com/default.aspx?kbid=822150 (4 Nov 2003)

Microsoft. "Windows Office Downloads" URL: http://office.microsoft.com/officeupdate/default.aspx (4 Nov 2000)

Microsoft. "Windows(Security & Updates)." URL: http://www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=7 (4 Nov. 2003).

Miuccio, Bert. "gcwn paper." E-mail to the author. (3 Nov 2003)

Nessus. "Download the stable version of the Nessus Security Scanner for Unix-compatible system:". URL: http://www.nessus.com/nessus_2_0.html (16 Oct. 2003)

Nessus. "Documentation." URL: http://www.nessus.com/documentation.html (4 Nov 2003)

Nessus. "Features." 2000. URL: http://www.nessus.org/features.html (4 Nov 2003)

Nessus. "NessusWX – Nessus Client for Win32." 23 April, 2003. URL: http://nessuswx.nessus.org/ (4 Nov. 2003)

Nessus. "Plugins search" URL: http://cgi.nessus.org/plugins/search.html (4 Nov. 2003)

NSA. "National Security Agency Security Recommendation Guides." 5 Mar, 2003. URL: http://www.nsa.gov/snac/win2k/download.htm (4 Nov, 2003)

Russinovich, Mark. "tcp view." E-mail to the author. (9 Sep 2003)

Secure Point Technologies, Inc. "Nessus". URL: http://msgs.securepoint.com/nessus/ (4 Nov. 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Shavlik. “HFNetChkPro4.0” URL: http://www.shavlik.com/downloads.aspx (4 Nov 2003)

SysInternals. “TCPView.” 29 May 2003. URL: http://www.sysinternals.com/ntw2k/source/tcpview.shtml (4 Nov. 2003)

© SANS Institute 2004, Author retains full rights.

Appendix A

Vulnerability found on port loc-srv (135/tcp)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges.

An attacker or a worm could use it to gain the control of this host.

Note that this is NOT the same bug as the one described in MS03-026 which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.

Risk factor : High
Nessus ID : 11835

Vulnerability found on port loc-srv (135/tcp)

The remote host is running a version of Windows which has a flaw in its RPC interface which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. There is at least one Worm which is currently exploiting this vulnerability. Namely, the MsBlaster worm.

Risk factor : Serious
Nessus ID : 11808

Vulnerability found on port loc-srv (135/tcp)

MS Windows RPC service (RPCSS) crashes trying to dereference a null pointer when it receives a certain malformed request.
All MS RPC-based services (i.e. a large part of MS Windows 2000+) running on the target machine are rendered inoperable.

Solution : Block access to TCP port 135.
Risk factor : High
Nessus ID : 11159

Vulnerability found on port loc-srv (135/tcp)

The remote service is vulnerable to a format string attack
An attacker may use this flaw to execute arbitrary code on this host.

Solution : upgrade your software or contact your vendor and inform it of this vulnerability

Risk factor : High
Nessus ID : 11133

Warning found on port loc-srv (135/tcp)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

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

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

Information found on port netbios-ssn (139/tcp)

An SMB server is running on this port
Nessus ID : 11011

Vulnerability found on port microsoft-ds (445/tcp)

. It was possible to log into the remote host using the following login/password combinations :
'administrator'/''

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

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000).
Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$

. All the smb tests will be done as 'administrator'/'' in domain WORKGROUP

Nessus ID : 10394

Vulnerability found on port microsoft-ds (445/tcp)

The remote Windows 2000 does not have the Service Pack 4 applied.
(it uses instead)
You should apply it to be up-to-date
Risk factor : High

Nessus ID : 10531

Vulnerability found on port microsoft-ds (445/tcp)

The Windows shell of the remote host has an unchecked buffer which can be exploited by a local attacker to run arbitrary code on this host.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Affected Software:

Microsoft Windows NT 4.0
Microsoft Windows NT 4.0 Server, Terminal Server Edition
Microsoft Windows 2000

Recommendation: Users using any of the affected products should install the patch immediately.

Risk factor : Low
Nessus ID : 11307

Vulnerability found on port microsoft-ds (445/tcp)

A flaw in the Windows 2000 Network Connection Manager could enable privilege elevation.

Impact of vulnerability: Elevation of Privilege

Affected Software:

Microsoft Windows 2000

Recommendation: Users using any of the affected products should install the patch immediately.

Maximum Severity Rating: Critical

Risk factor : High

Nessus ID : 11091

Vulnerability found on port microsoft-ds (445/tcp)

A security issue has been identified in WM_TIMER that could allow an attacker to compromise a computer running Microsoft Windows and gain complete control over it.

Recommendation: Users using any of the affected products should install the patch immediately.

Maximum Severity Rating: Critical

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Affected Software:

Microsoft Windows NT 4.0
Microsoft Windows NT 4.0, Terminal Server Edition
Microsoft Windows 2000
Microsoft Windows XP

Risk factor : High
Nessus ID : 11191

Vulnerability found on port microsoft-ds (445/tcp)

A security vulnerability exists in the Microsoft Local Troubleshooter ActiveX control in
Windows 2000. The vulnerability exists because the ActiveX control (Tshoot.ocx) contains
a buffer overflow that could allow an attacker to run code of their choice on a user's system.
To exploit this vulnerability, the attacker would have to create a specially formed HTML based
e-mail and send it to the user.
Alternatively an attacker would have to host a malicious Web site that contained a Web page
designed to exploit this vulnerability.

Risk factor : High
Nessus ID : 11887

Vulnerability found on port microsoft-ds (445/tcp)

The remote host is vulnerable to a flaw in ntdll.dll
which may allow an attacker to gain system privileges,
by exploiting it thru, for instance, WebDAV in IIS5.0
(other services could be exploited, locally and/or remotely)

Note : On Win2000, this advisory is superceded by MS03-013

Risk factor : High
Nessus ID : 11413

Vulnerability found on port microsoft-ds (445/tcp)

Hotfix to fix Certificate Validation Flaw (Q329115)
is not installed.

The vulnerability could enable an attacker who had
a valid end-entity certificate to issue a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

subordinate certificate that, although bogus, would nevertheless pass validation. Because CryptoAPI is used by a wide range of applications, this could enable a variety of identity spoofing attacks.
Impact of vulnerability: Identity spoofing.

Maximum Severity Rating: Critical

Recommendation: Administrators should install the patch immediately.

Affected Software:

Microsoft Windows 98
Microsoft Windows 98 Second Edition
Microsoft Windows Me
Microsoft Windows NT 4.0
Microsoft Windows NT 4.0, Terminal Server Edition
Microsoft Windows 2000
Microsoft Windows XP
Microsoft Office for Mac
Microsoft Internet Explorer for Mac
Microsoft Outlook Express for Mac

Risk factor : High
Nessus ID : 11145

Vulnerability found on port microsoft-ds (445/tcp)

XMLHTTP Control Can Allow Access to Local Files.

A flaw exists in how the XMLHTTP control applies IE security zone settings to a redirected data stream returned in response to a request for data from a web site. A vulnerability results because an attacker could seek to exploit this flaw and specify a data source that is on the user's local system. The attacker could then use this to return information from the local system to the attacker's web site.

Impact of vulnerability: Attacker can read files on client system.

Affected Software:

Microsoft XML Core Services versions 2.6, 3.0, and 4.0.
An affected version of Microsoft XML Core Services also ships as part of the following products:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft Windows XP
Microsoft Internet Explorer 6.0
Microsoft SQL Server 2000

(note: versions earlier than 2.6 are not affected
files affected include msxml[2-4].dll and are found
in the system32 directory. This might be false
positive if you have earlier version)

Risk factor : High
Nessus ID : 10866

Vulnerability found on port microsoft-ds (445/tcp)

A flaw exists in the RPC endpoint mapper, which can be used by an attacker to disable it remotely.

An attacker may use this flaw to prevent this host from working properly

Affected Software:

Microsoft Windows NT 4
Microsoft Windows 2000
Microsoft Windows XP

There is no patch for NT4.

Microsoft strongly recommends that customers still using Windows NT 4.0 protect those systems by placing them behind a firewall which is filtering traffic on Port 135.

Risk factor : Serious
Nessus ID : 11485

Vulnerability found on port microsoft-ds (445/tcp)

The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges.

Risk factor : High

Nessus ID : 11790

Vulnerability found on port microsoft-ds (445/tcp)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The remote host is vulnerable to a flaw in the Windows Script Engine, which provides Windows with the ability to execute script code.

To exploit this flaw, an attacker would need to lure one user on this host to visit a rogue website or to send him an HTML e-mail with a malicious code in it.

Risk factor : Medium
Nessus ID : 11423

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'ResetBrowser Frame' and the 'HostAnnouncement flood' has not been applied.

The first of these vulnerabilities allows anyone to shut down the network browser of this host at will.

The second vulnerability allows an attacker to add thousands of bogus entries in the master browser, which will consume most of the network bandwidth as a side effect.

Risk factor : Medium

Nessus ID : 10434

Vulnerability found on port microsoft-ds (445/tcp)

The remote host is running a version of Windows with a version of DirectX which is vulnerable to a buffer overflow in the module which handles MIDI files.

To exploit this flaw, an attacker needs to craft a rogue MIDI file and send it to a user of this computer. When the user attempts to read the file, it will trigger the buffer overflow condition and the attacker may gain a shell on this host.

Risk factor : High

Nessus ID : 11803

Vulnerability found on port microsoft-ds (445/tcp)

. User 'ADMINISTRATOR' has NO password !
. User 'jeff1' has NO password !

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus ID : 10404

Vulnerability found on port microsoft-ds (445/tcp)

The following shares can be accessed as administrator :

- C$ - (readable, writeable)
+ Content of this share :
- arcldr.exe
- arcsetup.exe
- AUTOEXEC.BAT
- boot.ini
- CONFIG.SYS
- Dell
- Documents and Settings
- IO.SYS
- MSDOS.SYS
- NTDETECT.COM
- ntldr
- pagefile.sys
- Program Files
- RECYCLER
- System Volume Information

- ADMIN$ - (readable, writeable)

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

Nessus ID : 10396

Vulnerability found on port microsoft-ds (445/tcp)

The following shares can be accessed as ADMINISTRATOR :

- C$ - (readable, writeable)
+ Content of this share :
- arcldr.exe
- arcsetup.exe
- AUTOEXEC.BAT
- boot.ini
- CONFIG.SYS
- Dell
- Documents and Settings
- IO.SYS

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- MSDOS.SYS
- NTDETECT.COM
- ntldr
- pagefile.sys
- Program Files
- RECYCLER
- System Volume Information

- ADMIN$ - (readable, writeable)

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

Nessus ID : 10396

Vulnerability found on port microsoft-ds (445/tcp)

The following shares can be accessed as jeff1 :

- C$ - (readable, writeable)
+ Content of this share :
- arcldr.exe
- arcsetup.exe
- AUTOEXEC.BAT
- boot.ini
- CONFIG.SYS
- Dell
- Documents and Settings
- IO.SYS
- MSDOS.SYS
- NTDETECT.COM
- ntldr
- pagefile.sys
- Program Files
- RECYCLER
- System Volume Information

- ADMIN$ - (readable, writeable)

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

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus ID : 10396

Vulnerability found on port microsoft-ds (445/tcp)

The remote version of Windows has a flaw in the way the kernel passes error messages to a debugger. An attacker could exploit it to gain elevated privileges on this host.

To successfully exploit this vulnerability, an attacker would need a local account on this host.

Risk factor : High

Nessus ID : 11541

Vulnerability found on port microsoft-ds (445/tcp)

There is a flaw in the way the HTML converter for Microsoft Windows handles a conversion request during a cut-and-paste operation. This flaw causes a security vulnerability to exist. A specially crafted request to the HTML converter could cause the converter to fail in such a way that it could execute code in the context of the currently logged-in user. Because this functionality is used by Internet Explorer, an attacker could craft a specially formed Web page or HTML e-mail that would cause the HTML converter
to run arbitrary code on a user's system. A user visiting an attacker's Web site could allow the attacker to exploit the vulnerability without any other user action.

Risk factor : High

Nessus ID : 11878

Vulnerability found on port microsoft-ds (445/tcp)

The Microsoft VM is a virtual machine for the Win32 operating environment.

There are numerous security flaws in the remote Microsoft VM which could allow an attacker to execute arbitrary code on this host.

To exploit this flaw, an attacker would need to set up a malicious web site with a rogue Java applet and lure the user of this host to visit it. The java applet could then execute arbitrary commands on this host.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk factor : High

Nessus ID : 11326

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Still Image Service Privilege Escalation'
problem has not been applied.

This vulnerability allows a malicious user, who has the
right to log on this host locally, to gain additional privileges
on this host.

Risk factor : Medium

Nessus ID : 10504

Vulnerability found on port microsoft-ds (445/tcp)

The following registry keys are writeable by users who are not in
the admin group :

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

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

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

- admin group : Full Control
- system : Full Control
- everyone : Read

Risk factor : High

Nessus ID : 10430

Vulnerability found on port microsoft-ds (445/tcp)

The remote host is running a Microsoft VM machine which has a bug
in its bytecode verifier which may allow a remote attacker to execute
arbitrary code on this host, with the privileges of the user running the VM.

To exploit this vulnerability, an attacker would need to send a malformed

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

applet to a user on this host, and have him execute it. The malicious applet would then be able to execute code outside the sandbox of the VM.

Risk factor : High

Nessus ID : 11528

Vulnerability found on port microsoft-ds (445/tcp)

Authentication Flaw in Windows Debugger can Lead to Elevated Privileges (Q320206)

Impact of vulnerability: Elevation of Privilege

Affected Software:

Microsoft Windows NT 4.0
Microsoft Windows NT 4.0 Server, Terminal Server Edition
Microsoft Windows 2000

Recommendation: Users using any of the affected products should install the patch immediately.

Maximum Severity Rating: Critical (locally)

Risk factor : High

Nessus ID : 10964

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'IP Fragment Reassembly' vulnerability has not been applied on the remote Windows host.

This vulnerability allows an attacker to send malformed packets which will hog this computer CPU to 100%, making it nearly unusable for the legitimate users.

Risk factor : Serious

Nessus ID : 10433

Vulnerability found on port microsoft-ds (445/tcp)

The remote host runs a version of windows which has a flaw in the way the utility manager handles Windows messages. As a result, it is possible for a local user to gain additional privileges on this host.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk factor : Serious

Nessus ID : 11789

Vulnerability found on port microsoft-ds (445/tcp)

An unchecked buffer in Windows help could allow an attacker to could gain control over user's system.

Maximum Severity Rating: Critical

Recommendation: Customers should install the patch immediately.

Affected Software:

Microsoft Windows 98
Microsoft Windows 98 Second Edition
Microsoft Windows Millennium Edition
Microsoft Windows NT 4.0
Microsoft Windows NT 4.0, Terminal Server Edition
Microsoft Windows 2000
Microsoft Windows XP

Risk factor : High

Nessus ID : 11147

Vulnerability found on port microsoft-ds (445/tcp)

A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack.

This plugin determined by reading the remote registry that the patch MS03-043 has not been applied.

Risk factor : High

Nessus ID : 11888

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Webserver file request parsing' problem has not been applied.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This vulnerability can allow an attacker to make the
remote IIS server make execute arbitrary commands.

Risk factor : Serious

Nessus ID : 10632

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'NetBIOS Name Server Protocol Spoofing'
problem has not been applied.

This vulnerability allows a malicious user to make this
host think that its name has already been taken on the
network, thus preventing it to function properly as
a SMB server (or client).

Risk factor : Medium

Nessus ID : 10482

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Local Security Policy Corruption'
problem has not been applied.

This vulnerability allows a malicious user to corrupt parts of
a Windows 2000 system's local security policy, which may
prevent this host from communicating with other hosts
in this domain.

Risk factor : Medium

Nessus ID : 10499

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Telnet Client NTLM Authentication'
problem has not been applied.

This vulnerability may, under certain circumstances, allow a malicious
user to obtain cryptographically protected logon credentials from
another user.

Risk factor : Medium

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus ID : 10519

Vulnerability found on port microsoft-ds (445/tcp)

A vulnerability in the Certificate Enrollment
ActiveX Control in Microsoft Windows 98, Windows 98
Second Edition, Windows Millennium, Windows NT 4.0,
Windows 2000, and Windows XP allows remote attackers
to delete digital certificates on a user's system
via HTML.

Impact of vulnerability: Denial of service

Maximum Severity Rating: Critical

Recommendation: Customers should install the patch immediately

Affected Software:

Microsoft Windows 98
Microsoft Windows 98 Second Edition
Microsoft Windows Millennium
Microsoft Windows NT 4.0
Microsoft Windows 2000
Microsoft Windows XP

Risk factor : High

Nessus ID : 11144

Vulnerability found on port microsoft-ds (445/tcp)

The remote host is vulnerable to a denial of service attack,
which could allow an attacker to crash it by sending a specially
crafted SMB (Server Message Block) request to it.

Impact of vulnerability: Denial of Service / Elevation of Privilege

Maximum Severity Rating: Moderate

Risk factor : High
Nessus ID : 11300

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Service Control Manager Named Pipe Impersonation'

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

problem has not been applied.

This vulnerability allows a malicious user, who has the
right to log on this host locally, to gain additional privileges.

Risk factor : Medium

Nessus ID : 10485

Vulnerability found on port microsoft-ds (445/tcp)

There is a vulnerability in Authenticode that, under certain low memory conditions, could allow an ActiveX control to download and install without presenting the user with an approval dialog. To exploit this vulnerability, an attacker could host a malicious Web Site designed to exploit this vulnerability. If an attacker then persuaded a user to visit that site an ActiveX control could be installed and executed on the user's system. Alternatively, an attacker could create a specially formed HTML e-mail and i send it to the user.

Exploiting the vulnerability would grant the attacker with the same privileges as the user.

Risk factor : High

Nessus ID : 11886

Vulnerability found on port microsoft-ds (445/tcp)

The remote host is vulnerable to a flaw in its SMB stack which may allow an unauthenticated attacker to corrupt the memory of this host. This may result in execution of arbitrary code on this host, or an attacker may disable this host remotely.

Risk factor : Serious

Nessus ID : 11787

Vulnerability found on port microsoft-ds (445/tcp)

A vulnerability exists because the ListBox control and the ComboBox control both call a function, which is located in the User32.dll file, that contains a buffer overrun. An attacker who had the ability to log on to a system interactively could run a program that could send a specially-crafted Windows message to any applications that have implemented the ListBox control or the ComboBox control, causing the application to take any action an attacker specified. An attacker must have valid logon credentials to exploit the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

vulnerability. This vulnerability could not be exploited remotely.

Risk factor : Moderate

Nessus ID : 11885

Vulnerability found on port microsoft-ds (445/tcp)

The remote host is running a version of Microsoft Visual Basic for Applications which is vulnerable to a buffer overflow when handling malformed documents.

An attacker may exploit this flaw to execute arbitrary code on this host, by sending a malformed file to a user of the remote host.

Risk factor : High

Nessus ID : 11832

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Malformed request to index server' problem has not been applied.

This vulnerability can allow an attacker to execute arbitrary code on the remote host.

Risk factor : Serious

Nessus ID : 10668

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the Unchecked Buffer in SNMP Service has not been applied.

Impact of vulnerability: Run code of attacker's choice and denial of service attacks.

Recommendation: Customers should install the patch immediately or disable snmp (you should disable all unused services)

Risk factor : High

Nessus ID : 10865

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Malformed RPC Packet'

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

problem has not been applied.

This vulnerability allows a malicious user, to cause
a denial of service against this host.

Risk factor : Medium

Nessus ID : 10509

Vulnerability found on port microsoft-ds (445/tcp)

We were able to determine that you are running IE Version 6.0000
with these IE Hotfixes installed:;SP1;

But is missing security update(s) Q828750 (MS03-040)
Recommendation: Customers using Microsoft IE should install
this patch immediately.

Impact of vulnerability: Run code of attacker's choice.

Supersedes MS01-055, MS01-058, MS02-005, MS02-066, MS02-068, MS03-004, MS03-014,
MS03-015, MS03-020, MS03-032 and others

Risk factor : High

Nessus ID : 10861

Vulnerability found on port microsoft-ds (445/tcp)

Hotfix to fix Flaw in Microsoft VM
could Allow Code Execution (810030)

Impact of vulnerability: Three vulnerabilities, the most
serious of which could enable an attacker to gain complete
control over a user's system.

Maximum Severity Rating: Critical

Recommendation: Administrators should install the patch immediately.

Affected Software:

Versions of the Microsoft virtual machine (Microsoft VM) are
identified by build numbers, which can be determined using the
JVIEW tool as discussed in the FAQ. All builds of the Microsoft
VM up to and including build 5.0.3805 are affected by these
vulnerabilities.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Also Note: Requires full registry access (Administrator)
to run the test.

Risk factor : High
Nessus ID : 11177

Vulnerability found on port microsoft-ds (445/tcp)

An overflow in the RAS phonebook service allows a local user
to execute code on the system with the privileges of LocalSystem.

Impact of vulnerability: Elevation of Privilege

Affected Software:

Microsoft Windows NT 4.0
Microsoft Windows NT 4.0 Server, Terminal Server Edition
Microsoft Windows 2000
Microsoft Windows XP

Recommendation: Users using any of the affected
products should install the patch immediately.

Maximum Severity Rating: Critical (locally)

Risk factor : High

Nessus ID : 11029

Vulnerability found on port microsoft-ds (445/tcp)

The Microsoft Locate service is a name server that maps logical
names to network-specific names.

There is a security vulnerability in this server which allows
an attacker to execute arbitrary code in it by sending a specially
crafted packet to it.

Maximum Severity Rating: Critical

Recommendation: Administrators should install the patch immediately.

Affected Software:

Microsoft Windows NT 4.0
Microsoft Windows NT 4.0, Terminal Server Edition

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft Windows 2000
Microsoft Windows XP

Risk factor : High
Nessus ID : 11212

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'Relative Shell Path'
vulnerability has not been applied.

This vulnerability allows a malicious user
who can write to the remote system root
to cause the code of his choice to be executed by
the users who will interactively log into this
host.

Risk factor : Medium

Nessus ID : 10486

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the multiple LPC and LPC Ports vulnerabilities
has not been applied on the remote Windows host.

These vulnerabilities allows an attacker gain privileges on the
remote host, or to crash it remotely.

Risk factor : High

Nessus ID : 10525

Vulnerability found on port microsoft-ds (445/tcp)

Trust relationships are created between Windows NT or Windows 2000
domains to allow users in one domain to access resources in other domains
without requiring them to authenticate separately to each domain.
When a user in a trusted domain requests access to a resource in a trusting
domain, the trusted domain supplies authorization data in the form of a list
of Security Identifiers (SIDs) that indicate the user's identity and group
memberships. The trusting domain uses this data to determine whether to
grant the user's request.

A vulnerability exists because the trusting domain does not verify that
the trusted domain is actually authoritative for all the SIDs in the
authorization data. If one of the SIDs in the list identified a user

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

or security group that is not in the trusted domain, the trusting domain would accept the information and use it for subsequent access control decisions. If an attacker inserted SIDs of his choice into the authorization data at the trusted domain, he could elevate his privileges to those associated with any desired user or group, including the Domain Administrators group for the trusting domain. This would enable the attacker to gain full Domain Administrator access on computers in the trusting domain.

Risk factor : Medium

Nessus ID : 11366

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'domain account lockout' problem has not been applied.

This vulnerability allows a user to bypass the domain account lockout policy, and hence attempt to brute force a user account.

Risk factor : Medium

Nessus ID : 10555

Vulnerability found on port microsoft-ds (445/tcp)

Hotfix to fix Unchecked Buffer in PPTP Implementation (Q329834) is not installed.

A security vulnerability results in the Windows 2000 and Windows XP implementations because of an unchecked buffer in a section of code that processes the control data used to establish, maintain and tear down PPTP connections. By delivering specially malformed PPTP control data to an affected server, an attacker could corrupt kernel memory and cause the system to fail, disrupting any work in progress on the system.

Impact of vulnerability: Denial of service
Maximum Severity Rating: Critical

Recommendation: Administrators should install the patch immediately.

Affected Software:

Microsoft Windows 2000

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft Windows XP

Risk factor : High

Nessus ID : 11178

Vulnerability found on port microsoft-ds (445/tcp)

The hotfix for the 'IrDA access violation patch'
problem has not been applied.

This vulnerability can allow an attacker who is physically
near the W2K host to shut it down using a remote control.

Risk factor : Serious

Nessus ID : 10734

Vulnerability found on port microsoft-ds (445/tcp)

The account 'administrator'/'' is valid.
The worm W32/Deloder may use it to break into the remote host
and upload infected data in the remote shares

See also : CERT advisory CA-2003-08
Solution : Change your administrator password to a stronger one
Risk factor : High
Nessus ID : 11454

Vulnerability found on port microsoft-ds (445/tcp)

It seems that is was possible to crash the remote
windows remotely by sending a specially crafted packet.

An attacker may use this flaw to prevent this host from
working properly.

This attack is known as SMBDie.

Risk factor : High

Nessus ID : 11110

Warning found on port microsoft-ds (445/tcp)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The remote registry can be accessed remotely
using the login / password combination used
for the SMB tests.

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

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

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

Risk factor : Low

Nessus ID : 10400

Warning found on port microsoft-ds (445/tcp)

The remote Microsoft Data Access Component (MDAC) server
is vulnerable to a flaw which could allow an attacker to
execute arbitrary code on this host, provided he can
load and execute a database query on this server.

Impact of vulnerability: Elevation of Privilege

Affected Software:

MDAC version 2.5 Service Pack 2
MDAC version 2.5 Service Pack 3
MDAC version 2.6 Service Pack 2
MDAC version 2.7 RTM
MDAC version 2.7 Service Pack 1

Recommendation: Users using any of the affected
products should install the patch immediately.

Maximum Severity Rating: Moderate

Risk factor : Serious

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nessus ID : 11301

Warning found on port microsoft-ds (445/tcp)

Here is the list of the SMB shares of this host :

IPC$ - Remote IPC
ADMIN$ - Remote Admin
C$ - Default share

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

Solution : filter incoming traffic to this port
Risk factor : Medium
Nessus ID : 10395

Warning found on port microsoft-ds (445/tcp)

Outlook 2000 and 2002 provide the option to use Microsoft Word as the e-mail editor when creating and editing e-mail in RTF or HTML.

There is a flaw in some versions of Word which may allow an attacker to execute arbitrary code when the user replies to a specially formed message using Word.

An attacker may use this flaw to execute arbitrary code on this host.

Risk factor : Medium

Nessus ID : 11325

Warning found on port microsoft-ds (445/tcp)

The SMB signing capability in the Server Message Block protocol in Microsoft Windows 2000 and Windows XP allows attackers to disable the digital signing settings in an SMB session to force the data to be sent unsigned, then inject data into the session without detection, e.g. by modifying group policy information sent from a domain controller.

Maximum Severity Rating: Moderate

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Recommendation: Administrators should install the patch immediately.

Affected Software:

Microsoft Windows 2000
Microsoft Windows XP

Risk factor : Medium
Nessus ID : 11215

Warning found on port microsoft-ds (445/tcp)

The host Security Identifier (SID) can be obtained remotely. Its value is :

JEFF : 5-21-220523388-484763869-1060284298

An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137-139 and 445
Risk factor : Low

Nessus ID : 10859

Warning found on port microsoft-ds (445/tcp)

The host SID could be used to enumerate the names of the local users
of this host.
(we only enumerated users name whose ID is between 1000 and 1200
for performance reasons)
This gives extra knowledge to an attacker, which
is not a good thing :
- Administrator account name : ADMINISTRATOR (id 500)
- Guest account name : Guest (id 501)
- jeff1 (id 1000)
- Debugger Users (id 1001)

Risk factor : Medium
Solution : filter incoming connections this port

Nessus ID : 10860

Warning found on port microsoft-ds (445/tcp)

The following local accounts have never logged in :

Guest

Unused accounts are very helpful to hacker

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Solution : suppress these accounts
Risk factor : Medium
Nessus ID : 10915

Warning found on port microsoft-ds (445/tcp)

Here is a list of files which have been found on the remote SMB shares.
Some of these files may contain copyrighted materials, such as commercial movies or music files.

If any of this file actually contains copyrighted material and if they are freely swapped around, your organization might be held liable for copyright infrigement by associations such as the RIAA or the MPAA.

+ ADMIN$:

- \clock.avi

Solution : Delete all the copyrighted files
Nessus ID : 11777

Warning found on port microsoft-ds (445/tcp)

Buffer overflow in Multiple UNC Provider (MUP) in Microsoft Windows operating systems allows local users to cause a denial of service or possibly gain SYSTEM privileges via a long UNC request.

Affected Software:

Microsoft Windows NT 4.0 Workstation
Microsoft Windows NT 4.0 Server
Microsoft Windows NT 4.0 Server, Enterprise Edition
Microsoft Windows NT 4 Terminal Server Edition
Microsoft Windows 2000 Professional
Microsoft Windows 2000 Server
Microsoft Windows 2000 Advanced Server
Microsoft Windows XP Professional

Risk factor : Medium

Nessus ID : 10944

Warning found on port microsoft-ds (445/tcp)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The registry key
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount
is non-null. It means that the remote host locally caches the passwords of the users when they log in, in order to continue to allow the users to log in in the case of the failure of the PDC.

Solution : use regedt32 and set the value of this key to 0
Risk factor : Low
Nessus ID : 11457

Warning found on port microsoft-ds (445/tcp)

The remote host is running a version of the shlwapi.dll which crashes when processing a malformed HTML form.

An attacker may use this flaw to prevent the users of this host from working properly.

To exploit this flaw, an attacker would need to send a malformed HTML file to the remote user, either by e-mail or by making him visit a rogue web site.

Solution : None
Risk Factor : Low
Nessus ID : 11583

Warning found on port microsoft-ds (445/tcp)

The following local accounts have passwords which never expire :

ADMINISTRATOR
Guest
jeff1

Password should have a limited lifetime
Solution : disable password non-expiry
Risk factor : Medium
Nessus ID : 10916

Information found on port microsoft-ds (445/tcp)

A CIFS server is running on this port
Nessus ID : 11011

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Information found on port microsoft-ds (445/tcp)

The following local accounts are disabled :

Guest

To minimize the risk of break-in, permanently disabled accounts should be deleted
Risk factor : Low
Nessus ID : 10913

Information found on port NFS-or-IIS (1025/tcp)

Here is the list of DCE services running on this port:
UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
Endpoint: ncacn_ip_tcp:10.0.0.2[1025]

UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
Endpoint: ncacn_ip_tcp:10.0.0.2[1025]

Nessus ID : 10736

Vulnerability found on port loc-srv (135/udp)

A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack.

This plugin actually checked for the presence of this flaw.

Risk factor : High

Nessus ID : 11890

Warning found on port netbios-ns (137/udp)

The remote host is running a version of the NetBT name service which suffers from a memory disclosure problem.

An attacker may send a special packet to the remote NetBT name service, and the reply will contain random arbitrary data from the remote host memory. This arbitrary data may be a fragment from the web page the remote user is viewing, or something more serious like a POP password or anything else.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

An attacker may use this flaw to continuously 'poll' the content
of the memory of the remote host and might be able to obtain sensitive
information.

Risk Factor : Medium

Nessus ID : 11830

Warning found on port netbios-ns (137/udp)

. The following 8 NetBIOS names have been gathered :
JEFF = This is the computer name registered for workstation services by a WINS client.
WORKGROUP = Workgroup / Domain name
JEFF
JEFF = This is the current logged in user registered for this workstation.
WORKGROUP = Workgroup / Domain name (part of the Browser elections)
JEFF1 = This is the current logged in user registered for this workstation.
WORKGROUP
__MSBROWSE__
. The remote host has the following MAC address on its adapter :
0x00 0x08 0x74 0x98 0x04 0x1d

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

Risk factor : Medium

Nessus ID : 10150

Information found on port unknown (1026/udp)

Here is the list of DCE services running on this port:
UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
Endpoint: ncadg_ip_udp:10.0.0.2[1026]
Annotation: Messenger Service

Nessus ID : 10736

Warning found on port general/tcp

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

An attacker may use this feature to determine traffic patterns

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

within your network. A few examples (not at all exhaustive) are:

1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network.

2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.

3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

Solution : Contact your vendor for a patch
Risk factor : Low
Nessus ID : 10201

Warning found on port general/tcp

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

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

1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network.

2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.

3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

Solution : Contact your vendor for a patch

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk factor : Low
Nessus ID : 10201

Warning found on port general/tcp

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

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

Solution : Contact your vendor for a patch
Risk factor : Medium

Nessus ID : 11618

Information found on port general/tcp

Nmap found that this host is running Windows Millennium Edition (Me), Win 2000, or WinXP

Nessus ID : 10336

Information found on port general/tcp

Remote OS guess : Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP

Nessus ID : 11268

Information found on port general/udp

For your information, here is the traceroute to 10.0.0.2 :
10.0.0.59
10.0.0.2

Nessus ID : 10287

Warning found on port general/icmp

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

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

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

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk factor : Low

Nessus ID : 10114

Warning found on port general/icmp

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

Solution : drop source routed packets on this host or on the surrounding
routers or firewalls.
Risk factor : Low
Nessus ID : 11834

Vulnerability found on port general/igmp

It was possible to crash the remote host
using the 'pimp' attack. This flaw allows
an attacker to make this host crash at will,
thus preventing the legitimate users from
using it.

Solution : filter incoming IGMP traffic

Risk factor : Serious

Nessus ID : 10179

© SANS Institute 2004, Author retains full rights.

Appendix B

10/21/2003 12:51:04
----Analysis engine is initialized successfully.----

----Reading Configuration info...

----Analyze User Rights...

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
        Analyze SeNetworkLogonRight.
        Analyze SeTcbPrivilege.
        Analyze SeMachineAccountPrivilege.
        Analyze SeBackupPrivilege.
        Analyze SeChangeNotifyPrivilege.
        Analyze SeSystemtimePrivilege.
        Analyze SeCreatePagefilePrivilege.
        Analyze SeCreateTokenPrivilege.
        Analyze SeCreatePermanentPrivilege.
        Analyze SeDebugPrivilege.
        Analyze SeRemoteShutdownPrivilege.
        Analyze SeAuditPrivilege.
        Analyze SeIncreaseQuotaPrivilege.
        Analyze SeIncreaseBasePriorityPrivilege.
        Analyze SeLoadDriverPrivilege.
        Analyze SeLockMemoryPrivilege.
        Analyze SeBatchLogonRight.
        Analyze SeServiceLogonRight.
        Analyze SeInteractiveLogonRight.
        Analyze SeSecurityPrivilege.
        Analyze SeSystemEnvironmentPrivilege.
        Analyze SeProfileSingleProcessPrivilege.
        Analyze SeSystemProfilePrivilege.
        Analyze SeAssignPrimaryTokenPrivilege.
        Analyze SeRestorePrivilege.
        Analyze SeShutdownPrivilege.
        Analyze SeTakeOwnershipPrivilege.
        Analyze SeDenyNetworkLogonRight.
        Analyze SeDenyBatchLogonRight.
        Analyze SeDenyServiceLogonRight.
        Analyze SeDenyInteractiveLogonRight.
        Analyze SeUndockPrivilege.
        Analyze SeSyncAgentPrivilege.
        Analyze SeEnableDelegationPrivilege.
        Analyze SeImpersonatePrivilege.
Not Configured - SeImpersonatePrivilege.
        Analyze SeCreateGlobalPrivilege.
Not Configured - SeCreateGlobalPrivilege.

        User Rights analysis completed successfully.

----Reading Configuration info...


----Analyze Group Membership...
        Analyze Users.
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Not Configured - *S-1-5-32-545__Members.
        Analyze Replicator.
Not Configured - *S-1-5-32-552__Members.
        Analyze Guests.
Not Configured - *S-1-5-32-546__Members.
        Analyze Backup Operators.
Not Configured - *S-1-5-32-551__Members.
        Analyze Administrators.
Not Configured - *S-1-5-32-544__Members.
        Analyze Power Users.

        Group Membership analysis completed successfully.

----Reading Configuration info...


----Analyze Registry Keys...
Not Configured - users.
Not Configured - users\.default\software\microsoft\protected storage
system provider.
0 mismatches are found under users.
Not Configured - machine.
Mismatch      - machine\software\Classes.
Not Configured - machine\software\microsoft\protected storage system
provider.
Mismatch      - machine\software\microsoft\windows\currentversion\group
policy.
Mismatch      - machine\software\microsoft\windows
nt\currentversion\perflib\009.
Not Configured - machine\system\clone.
Mismatch      - machine\system\controlset001.
Warning 2: The system cannot find the file specified.
        Error querying security of machine\system\controlset003.
Not Available  - machine\system\controlset003.
Warning 2: The system cannot find the file specified.
        Error querying security of machine\system\controlset004.
Not Available  - machine\system\controlset004.
Warning 2: The system cannot find the file specified.
        Error querying security of machine\system\controlset005.
Not Available  - machine\system\controlset005.
Warning 2: The system cannot find the file specified.
        Error querying security of machine\system\controlset006.
Not Available  - machine\system\controlset006.
Warning 2: The system cannot find the file specified.
        Error querying security of machine\system\controlset007.
Not Available  - machine\system\controlset007.
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Warning 2: The system cannot find the file specified.
Error querying security of machine\system\controlset008.
Not Available - machine\system\controlset008.
Warning 2: The system cannot find the file specified.
Error querying security of machine\system\controlset009.
Not Available - machine\system\controlset009.
Warning 2: The system cannot find the file specified.
Error querying security of machine\system\controlset010.
Not Available - machine\system\controlset010.
Mismatch - machine\system\currentcontrolset\control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\currentcontrolset\control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.
Not Available - machine\system\currentcontrolset\control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.
Mismatch - machine\system\currentcontrolset\control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\currentcontrolset\control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.
Not Available - machine\system\currentcontrolset\control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.
Mismatch - machine\system\currentcontrolset\control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\currentcontrolset\control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.
Not Available - machine\system\currentcontrolset\control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.
Mismatch - machine\system\currentcontrolset\control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\currentcontrolset\control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not Available - machine\system\currentcontrolset\control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.
Mismatch - machine\system\currentcontrolset\control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\currentcontrolset\control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.
Not Available - machine\system\currentcontrolset\control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.
Mismatch - machine\system\currentcontrolset\control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\currentcontrolset\control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.
Not Available - machine\system\currentcontrolset\control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.
Mismatch - machine\system\currentcontrolset\control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\currentcontrolset\control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.
Not Available - machine\system\currentcontrolset\control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.
Not Configured - machine\system\currentcontrolset\enum.
Warning 2: The system cannot find the file specified.
Error querying security of machine\system\currentcontrolset\services\snmp.
Not Available - machine\system\currentcontrolset\services\snmp.
11 mismatches are found under machine.
0 mismatches are found under classes_root.

Registry keys analysis completed successfully.

----Reading Configuration info...

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
----Analyze File Security...
Warning 2: The system cannot find the file specified.
        Error querying security of c:\documents and settings\administrator.
Not Available  - c:\documents and settings\administrator.
Not Configured - c:\documents and settings\all users\documents.
Warning 2: The system cannot find the file specified.
        Error querying security of c:\my download files.
Not Available  - c:\my download files.
Warning 2: The system cannot find the file specified.
        Error querying security of c:\ntbootdd.sys.
Not Available  - c:\ntbootdd.sys.
Warning 2: The system cannot find the file specified.
        Error querying security of c:\program files\resource pro kit.
Not Available  - c:\program files\resource pro kit.
Not Configured - c:\system volume information.
Warning 2: The system cannot find the file specified.
        Error querying security of c:\temp.
Not Available  - c:\temp.
Not Configured - c:\winnt\offline web pages.
Warning 2: The system cannot find the file specified.
        Error querying security of c:\winnt\system32\appmgmt.
Not Available  - c:\winnt\system32\appmgmt.
Not Configured - c:\winnt\system32\reinstallbackups.
Warning 2: The system cannot find the file specified.
        Error querying security of c:\winnt\system32\repl.
Not Available  - c:\winnt\system32\repl.
Not Configured - c:\winnt\tasks.
0 mismatches are found under c:\.

        File security analysis completed successfully.


----Analyze General Service Settings...
        Analyze WZCSVC.
Not Configured - WZCSVC.
        Analyze wuauserv.
Not Configured - wuauserv.
        Analyze Wmi.
Not Configured - Wmi.
        Analyze WmdmPmSN.
Not Configured - WmdmPmSN.
        Analyze WinMgmt.
Not Configured - WinMgmt.
        Analyze W32Time.
Not Configured - W32Time.
        Analyze UtilMan.
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not Configured - UtilMan.
Analyze UPS.
Not Configured - UPS.
Analyze TrkWks.
Not Configured - TrkWks.
Analyze TlntSvr.
Not Configured - TlntSvr.
Analyze TapiSrv.
Not Configured - TapiSrv.
Analyze SysmonLog.
Not Configured - SysmonLog.
Analyze Symantec Core LC.
Not Configured - Symantec Core LC.
Analyze Spooler.
Not Configured - Spooler.
Analyze SharedAccess.
Not Configured - SharedAccess.
Analyze SENS.
Not Configured - SENS.
Analyze seclogon.
Not Configured - seclogon.
Analyze Schedule.
Not Configured - Schedule.
Analyze SCardSvr.
Not Configured - SCardSvr.
Analyze SCardDrv.
Not Configured - SCardDrv.
Analyze SBService.
Not Configured - SBService.
Analyze SAVScan.
Not Configured - SAVScan.
Analyze SamSs.
Not Configured - SamSs.
Analyze RSVP.
Not Configured - RSVP.
Analyze RpcSs.
Not Configured - RpcSs.
Analyze RpcLocator.
Not Configured - RpcLocator.
Analyze RemoteRegistry.
Not Configured - RemoteRegistry.
Analyze RemoteAccess.
Not Configured - RemoteAccess.
Analyze RasMan.
Not Configured - RasMan.
Analyze RasAuto.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not Configured - RasAuto.
Analyze ProtectedStorage.
Not Configured - ProtectedStorage.
Analyze PolicyAgent.
Not Configured - PolicyAgent.
Analyze PlugPlay.
Not Configured - PlugPlay.
Analyze NtmsSvc.
Not Configured - NtmsSvc.
Analyze NtLmSsp.
Not Configured - NtLmSsp.
Analyze Netman.
Not Configured - Netman.
Analyze Netlogon.
Not Configured - Netlogon.
Analyze NetDDEdsdm.
Not Configured - NetDDEdsdm.
Analyze NetDDE.
Not Configured - NetDDE.
Analyze navapsvc.
Not Configured - navapsvc.
Analyze MSIServer.
Not Configured - MSIServer.
Analyze MSDTC.
Not Configured - MSDTC.
Analyze mnmsrvc.
Not Configured - mnmsrvc.
Analyze Messenger.
Not Configured - Messenger.
Analyze MDM.
Not Configured - MDM.
Analyze LmHosts.
Not Configured - LmHosts.
Analyze lanmanworkstation.
Not Configured - lanmanworkstation.
Analyze lanmanserver.
Not Configured - lanmanserver.
Analyze Fax.
Not Configured - Fax.
Analyze EventSystem.
Not Configured - EventSystem.
Analyze Eventlog.
Not Configured - Eventlog.
Analyze Dnscache.
Not Configured - Dnscache.
Analyze dmserver.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not Configured - dmserver.
        Analyze dmadmin.
Not Configured - dmadmin.
        Analyze Dhcp.
Not Configured - Dhcp.
        Analyze ClipSrv.
Not Configured - ClipSrv.
        Analyze cisvc.
Not Configured - cisvc.
        Analyze ccSetMgr.
Not Configured - ccSetMgr.
        Analyze ccPwdSvc.
Not Configured - ccPwdSvc.
        Analyze ccEvtMgr.
Not Configured - ccEvtMgr.
        Analyze Browser.
Not Configured - Browser.
        Analyze BITS.
Not Configured - BITS.
        Analyze Ati HotKey Poller.
Not Configured - Ati HotKey Poller.
        Analyze aspnet_state.
Not Configured - aspnet_state.
        Analyze AppMgmt.
Not Configured - AppMgmt.
        Analyze Alerter.
Not Configured - Alerter.

        General Service analysis completed successfully.

----Analyze available attachment engines...
        Load attachment LanManServer.
LanManServer: Query configuration information

        Attachment engines analysis completed successfully.

----Reading Configuration info...

----Analyze Security Policy...
        Analyze password information.
        Analyze account lockout information.
Not Configured - NewAdministratorName.
Not Configured - NewGuestName.
        Analyze other policy settings.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

System Access analysis completed successfully.
Analyze log settings.
Analyze event audit settings.

Audit/Log analysis completed successfully.
Analyze machine\software\microsoft\driver signing\policy.
Analyze machine\software\microsoft\non-driver signing\policy.
Analyze machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel.
Analyze machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\autoadminlogon.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption.
Analyze machine\software\microsoft\windows\currentversion\policies\explorer\nodrivetypeautorun.
Analyze machine\software\microsoft\windows\currentversion\policies\system\disablecad.
Analyze machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername.
Analyze machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon.
Analyze machine\system\currentcontrolset\control\lsa\auditbaseobjects.
Analyze machine\system\currentcontrolset\control\lsa\crashonauditfail.
Analyze machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
Analyze machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Analyze machine\system\currentcontrolset\control\lsa\restrictanonymous.

Analyze machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers.

Analyze machine\system\currentcontrolset\control\session manager\enhancedsecuritylevel.

Analyze machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown.

Analyze machine\system\currentcontrolset\control\session manager\protectionmode.

Analyze machine\system\currentcontrolset\services\eventlog\security\warninglevel.

Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect.

Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff.

Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature.

Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature.

Analyze machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword.

Analyze machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature.

Analyze machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature.

Analyze machine\system\currentcontrolset\services\mrxsmb\parameters\refusereset.

Analyze machine\system\currentcontrolset\services\netbt\parameters\nonamereleaseondemand.

Analyze machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange.

Analyze machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Analyze machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey.

Analyze machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel.

Analyze machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\disableipsourcerouting.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\enabledeadgwdetect.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\enableicmpredirect.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\keepalivetime.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\performrouterdiscovery.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\synattackprotect.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxhalfopen.

Analyze machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxhalfopenretired.

Analyze MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl.
Not Available - MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl.

Analyze MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText.
Not Configured - MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText.

Analyze MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not Configured -
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption.

Registry values analysis completed successfully.

----Analyze available attachment engines...

Attachment engines analysis completed successfully.

----Un-initialize analysis engine...

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.