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.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

Evaluation of the Win2K Pro NSA Security Template for the Jump Kit Lap Top

© SANS Institute 2000 - 2002 Author retains full rights.

Peter Szczepankiewicz
GCNT Practical Assignment
Version 3.0
Option 2.0

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table Of Contents

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

I. Introduction

During my first on site incident handling, I had set my laptop to run an internal scan on the LAN. With the scan running, I walked away to work on another task. To my surprise, I saw my laptop computer name in the Windows NT Network Neighborhood. I ran back to the laptop and unbound NetBIOS from tcp and shut off the browser service. It was then that I saw a shared C$ folder on my jump kit laptop. So I shut off the server service. Then I noticed that the password for Administrator was the default password set in our shop. I unplugged from the network and did some back-pedaling. On a lighter note, there was no IIS installed.

Two hours prior, that laptop was handed to me as I ran out the door. I did not lock down this laptop before rushing to arrive on site. Generally, we're only given a few hours notice before going to a client site. The tools we take with us need to be secured ahead of time. We should assume the worst-case scenario. There is an insider with root access, and that insider is monitoring for visitors. This project evaluates a security template particularly useful for Windows 2000 Professional on a stand-alone laptop, to be used as a part of a jump kit for on site incident handling. This template should provide an easy and fast way to apply most of the security necessary to plug a laptop for an incident handler into a hostile environment. Assume that there is an insider lurking in a hostile network just waiting for an incident handler to arrive.

II. Checklist or Template.

Before selecting a template, it is important to baseline the system to find out what vulnerabilities exist in a default install of Windows 2000 professional. Then, some of the most prominent vulnerabilities will be identified.

Baseline System:

Windows 2000 Pro default install. I accepted all the defaults throughout the install process.

NTFS partition.

Administrator password is blank.

No Service Pack installed.

MS Office 97.

The following system information was gathered from winmsd from the Run… command. Select the actions menu to save the report window as a text file.

System Information report written at: 10/01/2001 06:13:34 AM

[System Summary]

Item	Value
OS Name	Microsoft Windows 2000 Professional
Version	5.0.2195 Build 2195
OS Manufacturer	Microsoft Corporation

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

System Name	W2K2
System Manufacturer	Dell Computer Corporation
System Model	Inspiron 8000
System Type	X86-based PC
Processor	x86 Family 6 Model 8 Stepping 6 Genuine Intel ~848 MHz
BIOS Version	Phoenix ROM BIOS PLUS Version 1.10 A04
Windows Directory	C:\W2KPRO2
System Directory	C:\W2KPRO2\System32
Boot Device	\Device\Harddisk0\Partition1
Locale	United States
User Name	W2K2\Administrator
Time Zone	Eastern Standard Time
Total Physical Memory	327,136 KB
Available Physical Memory	240,328 KB
Total Virtual Memory	1,122,120 KB
Available Virtual Memory	966,920 KB
Page File Space	794,984 KB
Page File	C:\pagefile.sys

The following software applications must be able to run on this laptop, as a minimum, for incident handling.

ISS Scanner 6.2
L0phtcrack 2.5
THC-scan for wardialing.

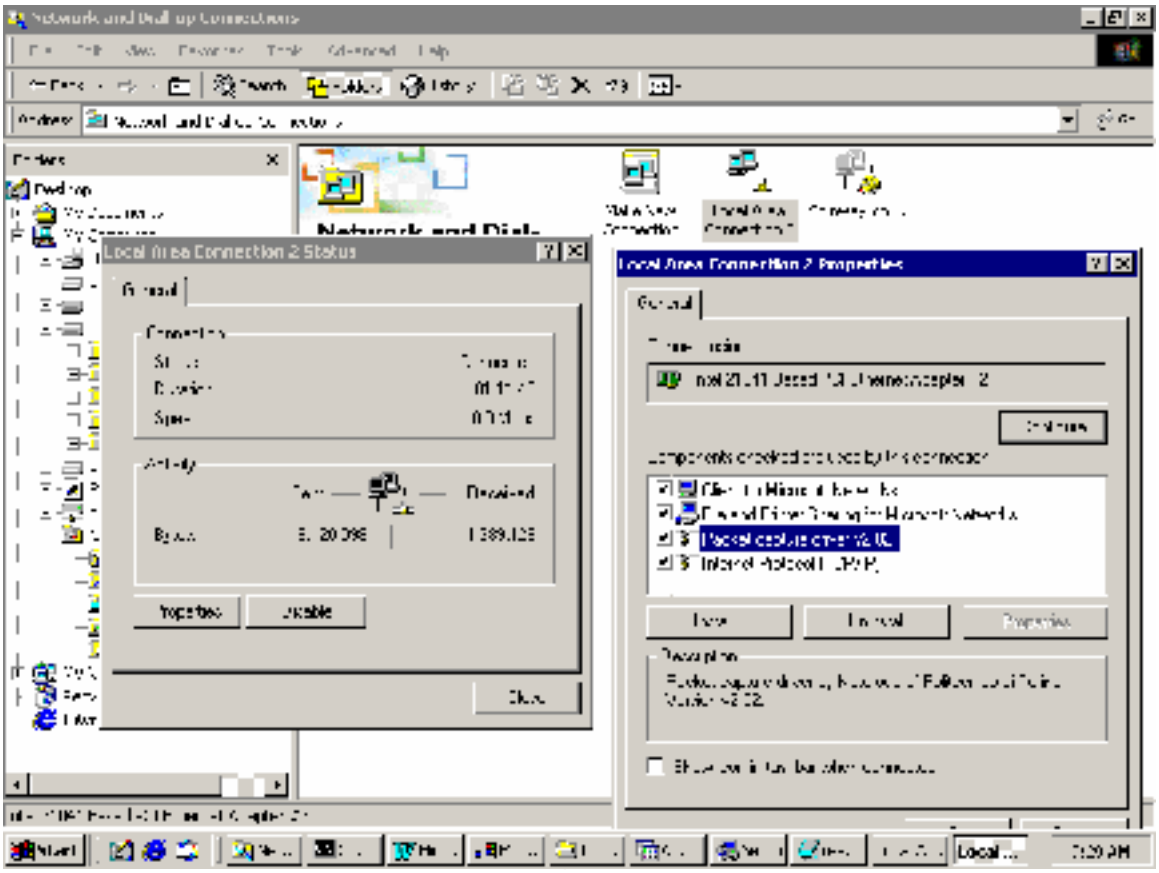
We need to know what are the vulnerabilities present in a default install of a stand-alone Windows 2000 Pro system. A few tools were used to baseline the system, including nmap, netstat, and ISS scanner.

First, I ran a baseline with NMAP and NETSTAT to see what ports were open. For this test, I used the Windows port of nmap downloaded from http://www.eEye.com. A new raw packet driver had to be installed to use nmapnt.

As mentioned in the readme file, this is how the packet driver is installed.

"Goto the properties for your network card.
You will want to install a new "protocol".
Click the browse button.
Now navigate to \Nmapnt\DRIVERS\PacketNT (NT4)
or to \Nmapnt\DRIVERS\Packet2K (Win2k)
Click ok a few times to back out of the network dialog boxes.
You will be asked to restart your computer, restart it.
Even if you are not asked to reboot, reboot otherwise the driver will not work correctly."

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



The ports open on the default install of Win2K Pro were found with NMAP and NETSTAT. First, an external scan of the computer was made with NMAP. Ports were found to be open. For the purposes of this test, only ports 1-1050 were scanned. In reality, ports 1-65535 should be scanned. The following are the results:

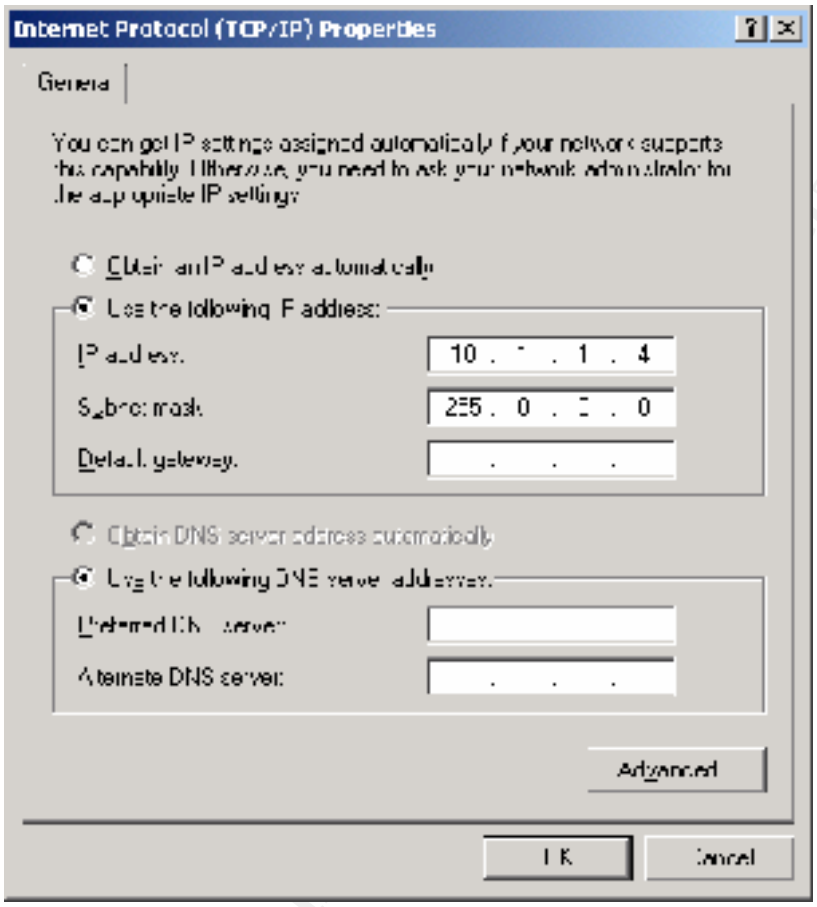
```
nmapnt -v -v -P0 -p 1-1050 10.1.1.4

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Initiating TCP connect() scan against W2K2 (10.1.1.4)
Adding TCP port 135 (state open).
Adding TCP port 445 (state open).
Adding TCP port 139 (state open).
Adding TCP port 1025 (state open).
The TCP connect scan took 27 seconds to scan 1050 ports.
Interesting ports on W2K2 (10.1.1.4):
(The 1046 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open listen

Nmap run completed -- 1 IP address (1 host up) scanned in 45 seconds

An IP address was assigned to the NIC. I added 10.1.1.4 to the NIC and rebooted.



C:\>ipconfig /all

Windows 2000 IP Configuration
Host Name . . . . . : W2k2
Primary DNS Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Xircom Cardbus Ethernet II 10/100

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Physical Address. . . . . : 00-10-A4-90-F2-41
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.1.1.4
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . :
DNS Servers . . . . . :

Then, netstat was run locally on the Win2K pro host. The following are the results.

netstat -a

Active Connections

Proto	Local Address	Foreign Address	State
TCP	w2k2:epmap	w2k2:0	LISTENING
TCP	w2k2:microsoft-ds	w2k2:0	LISTENING
TCP	w2k2:1025	w2k2:0	LISTENING
TCP	w2k2:1027	w2k2:0	LISTENING
TCP	w2k2:netbios-ssn	w2k2:0	LISTENING
UDP	w2k2:epmap	*:*	
UDP	w2k2:microsoft-ds	*:*	
UDP	w2k2:1026	*:*	
UDP	w2k2:netbios-ns	*:*	
UDP	w2k2:netbios-dgm	*:*	
UDP	w2k2:isakmp	*:*	

The open ports are shown below.
netstat -a -n

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	10.1.1.4:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	10.1.1.4:137	*:*	
UDP	10.1.1.4:138	*:*	
UDP	10.1.1.4:500	*:*	

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Windows 2000 dynamically opens port 139 when you physically plug in a live rj45 connected wire into the NIC. The open ports shown below are actually different from the open ports after assigning an IP address to the NIC. The Ethernet wire was removed from the NIC. Notice the missing ports. The same results occur when the NIC has no IP address assigned, but only has the internal loopback address 127.0.0.1.

netstat -a -n

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:1026	*:*	

The following are the ports that dynamically disappear when unplugging the wire, or on a NIC with only the loopback address.

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	10.1.1.4:139	0.0.0.0:0	LISTENING
UDP	10.1.1.4:137	*:*	
UDP	10.1.1.4:138	*:*	
UDP	10.1.1.4:500	*:*	

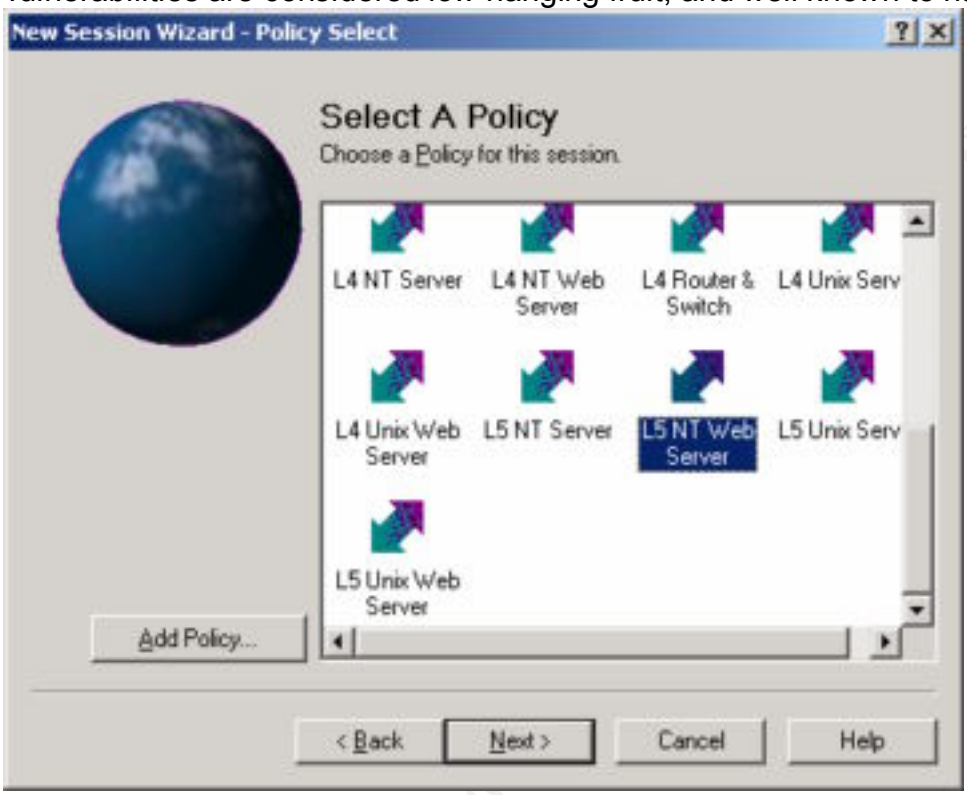
I installed ISS Scanner 6.2. The software was purchased separately. This is the actual ISS Scanner product, not the system scanner that comes with the Win2K resource Kit.

One unique thing I found was that NTFS is preferred before installing the system scanner from the win2K resource kit. When installing ISS Scanner from the Win2K Resource Kit, I received the following error when the disk system was FAT, and not yet NTFS.

FAT is the default install if one just keeps hitting return throughout the Win2K install process. However, for the purposes of this discussion, the laptop I am using already has NTFS.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

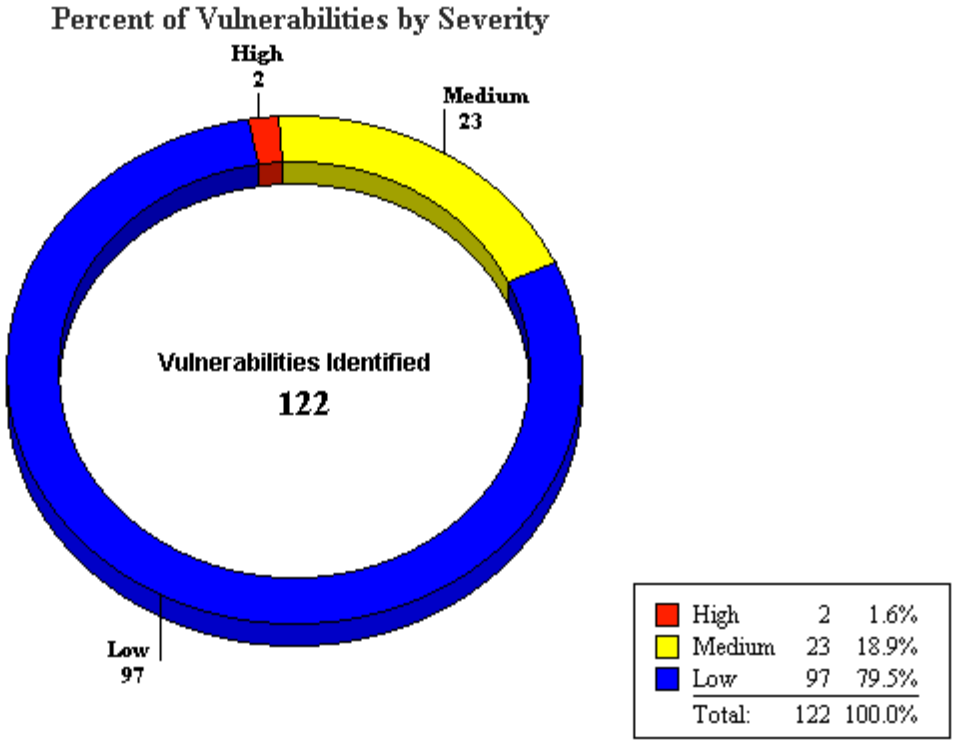
I used the L5 NT IIS profile for scanning throughout this project because I want to scan in depth, which is why I chose level 5. I also want to avoid IIS and all the code associated with it that has buffer overflow vulnerabilities. These vulnerabilities are considered low hanging fruit, and well known to hackers.



The system scanner took about 4 minutes to perform a scan. The real ISS Scanner took about 13 minutes to perform the scan.

The ISS Scan found many vulnerabilities in the default installation of Windows 2000 Professional. The graph below is taken from an executive summary report, generated by ISS Scanner.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



In total, 122 distinct vulnerabilities were found. Most these vulnerabilities found by ISS Scanner are mentioned in the Lab Mice Security Checklist. These two reports can be logically merged together to create a better security template. Some of the most relevant vulnerabilities include the following.

1. IisIsapiIdqBo: IIS idq.dll ISAPI extension buffer overflow (CAN-2001-0500)
2. IisIsapiPrinterBo: IIS 5.0 ISAPI Internet Printing Protocol extension buffer overflow
3. Critical Key Permissions: Critical key permissions incorrect. Run key in registry is writeable by non-administrators.
4. guestnopw: Guest account has no required password (CAN-1999-0504)
5. LM security: LAN Manager security
6. Posix Enabled: POSIX subsystem enabled (CAN-1999-0654)
7. pwlen: Minimum password length insufficient
8. regfile - permissions: Regfile associations can be changed by non-administrators
9. registry: Windows registry can be opened remotely
10. repair insecure: Repair directory readable
11. Win2kSp1: Windows 2000 without Service Pack 1 (CAN-1999-0662)
12. adminexists: The default Administrator account exists
13. Modem detected and active – should be there.
14. Auditing. Account management auditing was not enabled. File and object access auditing was not enabled.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

15. Last username appears at logon
16. Messenger service running

Four distinct checklists or templates were considered for locking down this system. They were:

1. LabMice Windows 2000 Installation Security Checklist.
2. NSA Windows 2000 Security Guide
3. Microsoft High Security for Stand Alone PC Template, located in systemroot\Security\Templates\hisecws.inf.
4. Jumes, et al. Windows MT4.0 Security, Audit and Control. There is a checklist for securing a system in the back of the book.

The Lab Mice checklist appeared to be pretty thorough. This checklist covered items that cannot be secured by a template. For example, physical security of the machine is considered. For a jump kit laptop, we cannot physically lock the laptop in my server room back at my office because, by definition, the laptop needs to come with me. But I can do things such as remove the floppy and CD ROM drives while I am not physically present with the laptop on sight. Another example of the depth of this checklist is that it mentions to use updated AntiVirus software. These are the basics that can easily go overlooked in a rush. In addition to that, I would add that at least one firewall application should be used. For this project, I chose Zone Alarm. Another example is that a BIOS password should be added to the laptop. One final example is the recommendation to use a biometrics device in addition to password authentication when accessing the laptop. For the purposes of this project, no biometrics device will be used, though they are beginning to become prolific out in the field. The final product of this project will include a security template the adjust all that can be done automatically, and a smaller checklist of items that need to be secured manually.

The template for high security from Microsoft was also considered.

The NSA Security Guide is downloadable form the NSA web site. It comes with a series of templates. I chose the template called W2K Workstation.INF. NSA has a good reputation when it comes to security, so I decided to evaluate this template. No template will cover all of my specific requirements, but the NSA template should cover some of them with high quality security.

For the purposes of this paper the NSA security template will be applied. First Service Pack 2 was installed on Win2K.

III. Security Settings.

My environment is a laptop in a hostile network. The laptop will be one of the main tools to handle an incident caused by a malicious system administrator who is still there. The security settings that are relevant for my environment are listed below, in order of importance. Each requirement will be explained.

1. No computer browser broadcasts running. The browser traffic lists all windows computers in network neighborhood. As an investigator, I want to

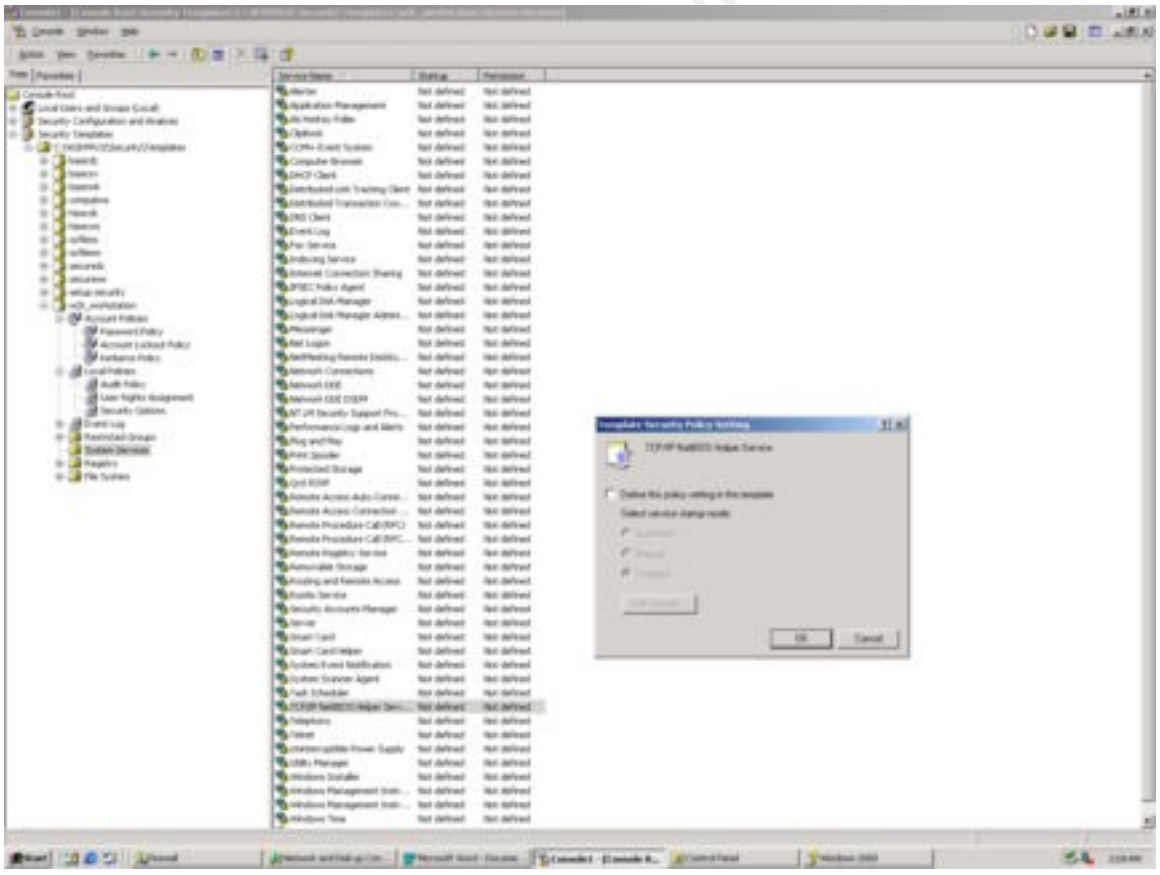
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

keep a low profile. There's no sense in broadcasting my presence in network neighborhood. It would be relatively easy for a non-skilled insider to know that my new computer was plugged into the net, just by seeing my computer's icon pop up in network neighborhood. Even after removing this feature, there are still other ways that the insider could easily find me. The NSA template does not shut off the computer browser service.

One item that should be performed is to unbind NetBIOS from tcp on the NIC bindings. This should prevent the NetBIOS traffic from leaving my laptop.

The computer browser service has a dependency on the server service. Shutting down the server service will shut down the browser service. If the server service is set to not startup upon reboot, then the computer browser service will fail to start and issue an event in the event viewer. To avoid this error, the computer browser service should also be disabled, or at least set to start up manually.

The NSA template does not perform these items. In the system services folder of the template, both the browser service and the TCP/IP NetBIOS helper are left run as always. These should be adjusted in the new template.



2. No IIS Server, or personal web server running. There is a saying that I heard in the field of computer security. "IIS = ROOT." The philosophies of principle of least privilege, and defense in depth are the basis of my assisting the customer to recover. It only makes sense to follow my own advice. There are

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

many buffer overflow vulnerabilities in IIS that allow a hacker to remotely execute code on the computer running IIS. For example, the MDAC exploit documented by Rain Forrest Puppy allows remote code execution, with System level privileges. The hacker does not even have to create a back door account to take advantage of MDAC. All that is needed is a web browser, and the hacker can root my computer. Another example of code with known vulnerabilities are the ISAPI components that are bundled with IIS.

Why would I even have IIS or personal web server (PWS) installed? I have witnessed examples of IIS being present on computers without the user knowingly installing it. What probably happened is that the user installed some other program that was bundled with IIS, or PWS.

One could run netstat –a –n at the command prompt to see if port 80 were open. If so, then I would need to shut down the web server and disable the service from starting at next boot up. I would like to delete files from the computer, but Windows 2000 has a feature where deleted files can be automatically replaced.

The NSA security template does not disable IIS or PWS.

3. Strong password. pwlen: Minimum password length insufficient. Laptops that are rapidly loaded are often given a default password. In the worst case, the password is blank for the Administrator. The password may be as easy as "password" or a known house password. It is important that the passwords on my laptop, especially the passwords of accounts in the Administrators group, be strong passwords.

The NSA template does satisfy this requirement. The NSA template requires a password of at least 12 characters in length. The password must contain three different types of characters, a small letter, a capital letter, and a numeric character. After installing the template, I tried to change my Administrator password to a long word without any numbers. I was not allowed to use that password. There is a pretty good password policy in the NSA template.

Policy Computer Setting
Store password using reversible encryption for all users in the domain Disabled
Passwords must meet complexity requirementsEnabled
Minimum password length 12 characters
Minimum password age 1 days
Maximum password age 90 days
Enforce password history 24 passwords remembered

If a hacker were able to capture my password hash, either via a dump from the SAM, copying the backup SAM from the repair directory, or sniffing the password hash from the wire, the hacker would try to crack the password. Using a strong password policy makes cracking the password more difficult and requires more time. One of the most popular windows password cracking tools, L0phtcrack, does not currently allow for brute force attempts with extended ASCII characters. One could use an extended ASCII character to escape brute force attempts that do not use extended ASCII characters.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. Password lockout screen saver when unattended. Physical security is important for this laptop. I will often be called away from my laptop to work on some other task, and I will not have the luxury to take my laptop everywhere I go. Physical security should not depend on me being present. If a hacker were to gain access to my keyboard while I am logged on with administrator access, the hacker could install a root kit on my computer to let my computer only see what the hacker wants me to see. He could hide in the network, and go totally unnoticed with such a root kit installed on the incident handler's computer.

The NSA template does enable this feature. However, I would like the laptop to lock the screen a little sooner. It should be adjusted in the new template. This setting is a little weak in the NSA template.

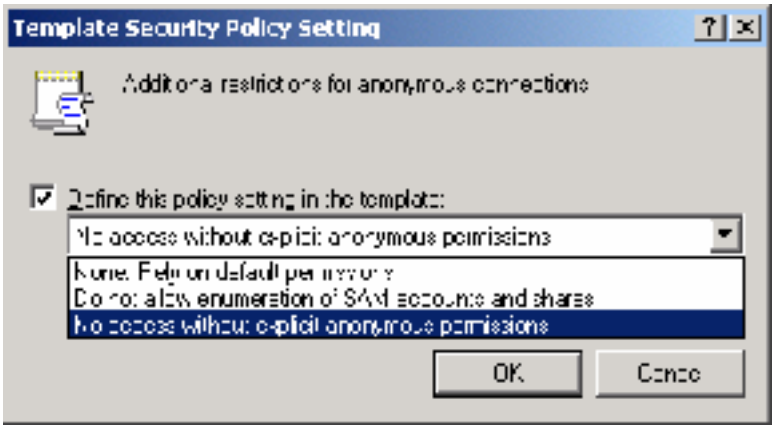
Along with password protected screen savers, the lab rat security check list suggested that a password be used in the system BIOS. In this manner, the laptop will not reboot without the BIOS password. This level of security cannot easily be scripted in a windows 2000 security template. Unfortunately, the best way is probably to manually set the BIOS password. Also, this password should be separate and distinct from the Windows account password. A BIOS password is a good example of defense in depth. The hacker would have to guess two passwords in order to successfully breach my laptop with keyboard access.

5. No last username to appear at logon. As mentioned above, there will be occasions where I am not present at this laptop. For example, early in the morning before work begins, it is possible that I set the laptop to boot up and leave it aside, and I could be called away. The default install of windows 2000 is to provide the last logged on user and ask only for the password. One half of the security is already breached. In an environment where the insider is looking for me, it would be best to not list my user name on this laptop.

The NSA template does enforce this policy.

6. No null sessions allowed. Windows NT was notorious for allowing unauthenticated access to conduct system level items, such as printing, domain queries during logon, etc. The null session is a connection over the network with no name and no password. A hacker will often take advantage of null sessions and use tools such as enum to list all the user account names on the computer. The hacker could also gather policy information on password settings, audit policy, etc. In general, too much information is available via a null session. Windows 2000 defaults for backward compatibility with Windows NT, and does allow for null sessions. Ideally, I would like to have no null sessions allowed to connect to my laptop. A lack of null sessions could affect the performance of older programs. This should not be a problem for my required programs to run, such as ISS Scanner, L0phtcrack, and THC.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



7. No server service. The computer server service allows other computers to use files and printers on my computer. A file server needs to run a server service. The server service is also a supporting service to the computer browser service, and to default administrative shares, such as the C$ share. Shutting off the server service is a very invasive security measure. For my requirements, the laptop does not need to be a file server to anyone. Shutting down the server service secures many inherent vulnerabilities in windows 2000.

The NSA template does not shut down the server service, and this should be added to a new template. Some cleanup will have to be performed after disabling the server service. Manually shutting down the server service will automatically force all the depending services to shut down, such as computer browser. However, the next time the computer reboots, the depending services may be set to automatically start up, but they cannot because the server service is disabled. These dependency services must be disabled also, or at least set to manually start. Automatic startups will cause errors.

8. Repair directory security. The repair directory must be secured because the repair directory stores a copy of the name and password database, in the sam file. By default, Windows 2000 sets the repair directory readable to accounts that are not in the administrators group. If a hacker were able to establish a null session, and climb up to a guest account access, the hacker would be able to copy that sam file. If the sam file was recently updated with the latest names and passwords, the hacker will now be able to crack my administrator password. The repair directory needs to be set to no access to all except for the Administrator.

The NSA template does support this requirement with the following line.

"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"

9. No remote viewing of registry. Windows registry cannot be opened remotely. As an incident handler in a hostile network, the hacker(s) could remotely view my registry. The registry contains everything about my computer, including meta data on how to implement security settings. The registry is often used to launch malicious code, for example. See MS knowledge base article Q185590 for an example. It is important that the registry be out of sight of the hacker.

The NSA template does not support this requirement, apparently. The

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ISS Scan that was performed after applying the template shows that the registry can still be viewed remotely.

10. Run key in registry is not writeable by non-administrators. Just as the file system has a startup folder to run code when a system boot up, so doe the registry have a run key to execute code upon system boot. More importantly, the run key executes code even before a user logs onto the computer. So a hacker would want to place malicious code to execute once from the run key and then delete itself to hide the tracks. All this could happen before logging on. By default, users can write to the run key in the registry in windows 2000. Access should be restricted to the run key down to No Access for all except for Administrators.

The NSA template does not support this requirement and it should be added to a new template.

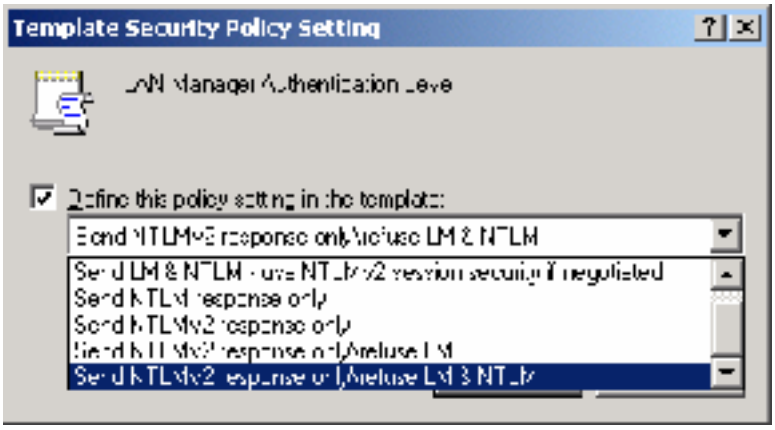
11. Guest account requires a password and is locked out. The default guest account is locked out on a fresh install of windows 2000. However, this account has no password. Complacency is the friend of the hacker. Physical access to this laptop will allow the insider to unlock the guest account and walk away. I would not be checking the guest account with great vigilance, and the backdoor would be wide open for the hacker to logon sometime later. Once guest access is granted, the hacker could try to escalate privileges later. In keeping with the philosophy of defense in depth, the guest account should be assigned a complex password, and should remain locked out.

The NSA template does not perform this function. Assigning passwords with a template is not a good idea. The password would be stored in plain text, no matter how complex. The paper template could become a source of information to a hacker who looks through the dumpster. Once the password is written in plain text, you lose a little control over who sees the password. I recommend that the Guest password be set manually.

12. Kerberos authentication required. Refuse LAN Manager challenges, including LMv2 challenges. LanManager version 1 (LMv1) was the default in Windows NT. LMv2 can only be enabled in later service packs for NT. In the world of LMv1, the password hash that travels over the wire can be sniffed, and cracked using tools such as L0phtcrack or smbrelay. Also, stored LM passwords are weaker by the nature of splitting the password into two parts of seven characters each. LanManager is only needed for backward compatibility concerning logons to windows 3.x and Windows 95. My laptop will never need to logon to another windows box. It is to my advantage to completely drop backward compatibility, and improve security in the process.

The NSA template is weak at enforcing this requirement.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Apparently, the highest setting available is NTLMv2 support. Unfortunately, this means that the LanMan passwords are still stored on my machine.

13. Disable extra subsystems, such as posix and OS/2. The principle of least privilege is deny all access and permit only what is needed by the user. In that way, excessive privileges are not granted by accident. There are no programs that I will run on windows 2000 that require posix, so posix support should be removed completely.

If there are basic tools that I would like to use in linux, such as nmap and tcpdump, then I can set up the laptop to dual boot, or run vmware. The posix subsystem in windows has not really gained much attention from the software market.

The NSA template does not support this requirement, so it should be added to a new template.

Good regfile permissions. If the hacker had logged into an account with write access to HKEY_LOCAL_MACHINE/Software/Classes/regfile/shell/open/command, then the hacker could execute malicious code. It is important to restrict write access to non-Administrators, for reasons already mentioned.

The NSA template does not enforce this requirement and it should be added to a new template if possible.

14. Install the latest Service Pack. As a general rule, it is a good idea to keep the laptop up to date with the latest service packs released form Microsoft. Older code may have bugs in it, such as buffer overflow vulnerabilities that are repaired in the service packs. This requirement cannot be contained in a template and must be done manually.

15. Secure the default administrator account. The default Administrator account in windows 2000 professional is called “Administrator.” That is a well-known default account with full privileges. The lab mice checklist suggests changing the default Administrator account to something else. I think it would be best to use a honey pot-like account called Administrator. It is important to note that the Default Admin account has to be copied and pasted to ensure that the comments field matches the real default account. Then the dummy account should be locked down with minimal rights in case it is broken into, and heavily audited, perhaps with some kind of alarm to notify me when someone attempts to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

log into the honey pot account.

The SID will still identify who is the real Administrator account and it does not take too much effort for a hacker to enumerate the SID. Still, this honey pot technique will make it that much more difficult.

If one were to just keep hitting the return key throughout a windows 2000 install, the Administrator account would have no password. As mentioned above, the password needs to be a strong one.

The NSA template only addresses the password policy. The NSA template does not change the name of the default administrator or create a honey pot account. This alone would be an interesting exercise to see if it could be made with a template. This should all be added to the new template if possible.

16. Modem active for wardialing. I require a modem in the laptop. Most computers on the network should never have a modem to ensure that all packets are routed through the firewall. In fact, once my laptop is plugged into the customer's network, the modem should be disabled manually, and the phone cord should be unplugged. There will be a need for the modem, to wardial the PBX of the customer. When the laptop is being used for wardialing, the NIC should be disabled, and the network cable should be unplugged. The laptop has the potential to act as a router around the firewall.

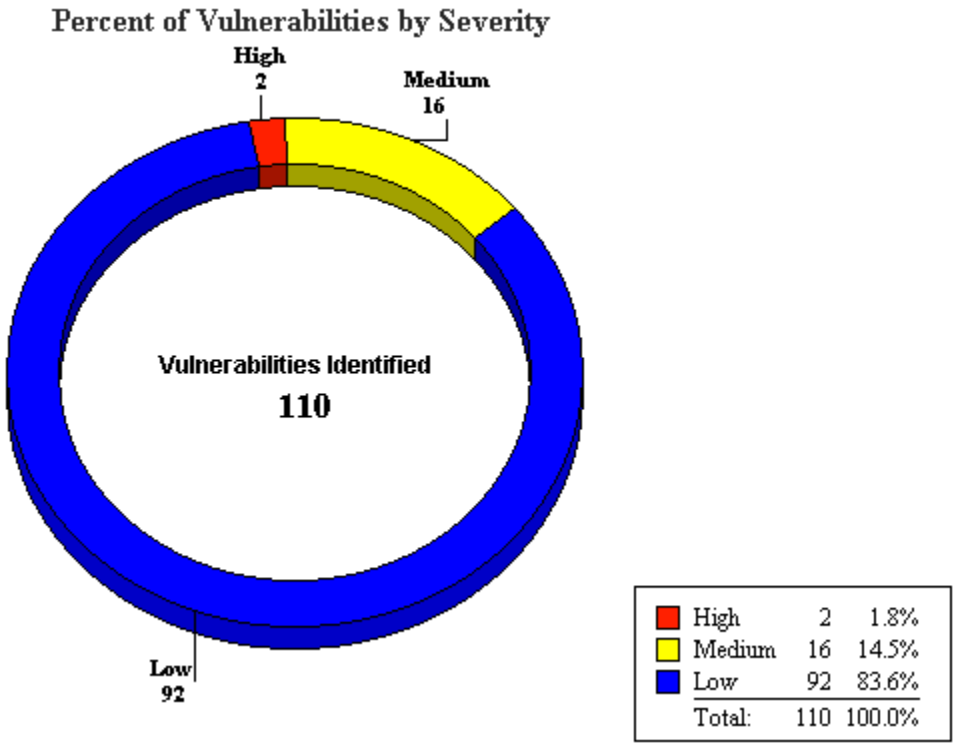
17. Auditing configured appropriately. Auditing is often considered the last line of defense. After all of my security measures have been breached, at least I should be able to see the hacker in the audit logs. Windows Event viewer logs are notorious for not reporting basic network information, such as the source IP address that attempted to logon as Administrator. At any rate, basic auditing should be turned on. Account management auditing must be enabled. This may allow me to see when a hacker attempts to create a backdoor account. File and object access auditing should be enabled. This setting will allow me to configure auditing on specific files and directories, such as the repair directory. There is almost never a valid reason for anyone to read the repair directory and potentially copy passwords.

18. Other software should be installed to increase the security of the laptop. The latest signature files of AntiVirus Software should be installed and maintained at least weekly, so that the laptops are always relatively up to date and read to go at a moments notice. A personal firewall, such as Zone Alarm, should be installed. A small sniffer program should be installed on the laptop, such as WinDump to detect and log any attacks at IP layer. A sniffer could also assist in basic network troubleshooting as needed. A traditional template cannot install any of this extra software. These files could be installed via a script and the template could launch the script. The process could be automated, but it would not be a simple template.

IV. Apply and test the template.

SP2 was installed on the system and ISS scanner was run. The following results were obtained.

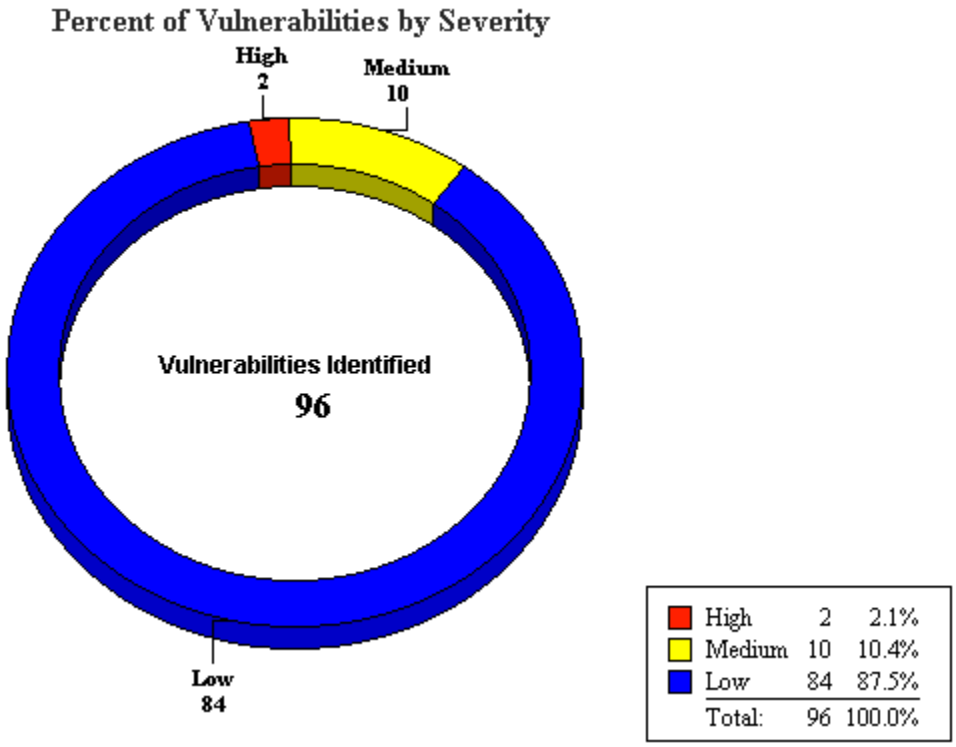
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



The next step was to import and apply the NSA template. I analyzed the template vs. the current computer settings. The Security Configuration and Analysis Tool showed that lots of changes were going to be made. Applying the NSA template took at least 5 minutes. The following results were obtained.

I wondered how much a reboot of the computer would affect the security settings. Changing the password policy to require complex passwords does not reset the existing weak passwords, for example. Rebooting should force the issue with many settings. Incidentally, I reset the password to comply with the security policy so as to not lock myself out. The following scan was run before rebooting.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



After rebooting the scan results were the same. It is possible that some settings were not in place before the reboot, but ISS Scanner just did not detect those settings.

Overall, we started with 122 vulnerabilities and we finished with 96. Applying PS2 and the NSA security template has decreased my number of vulnerabilities by 26.

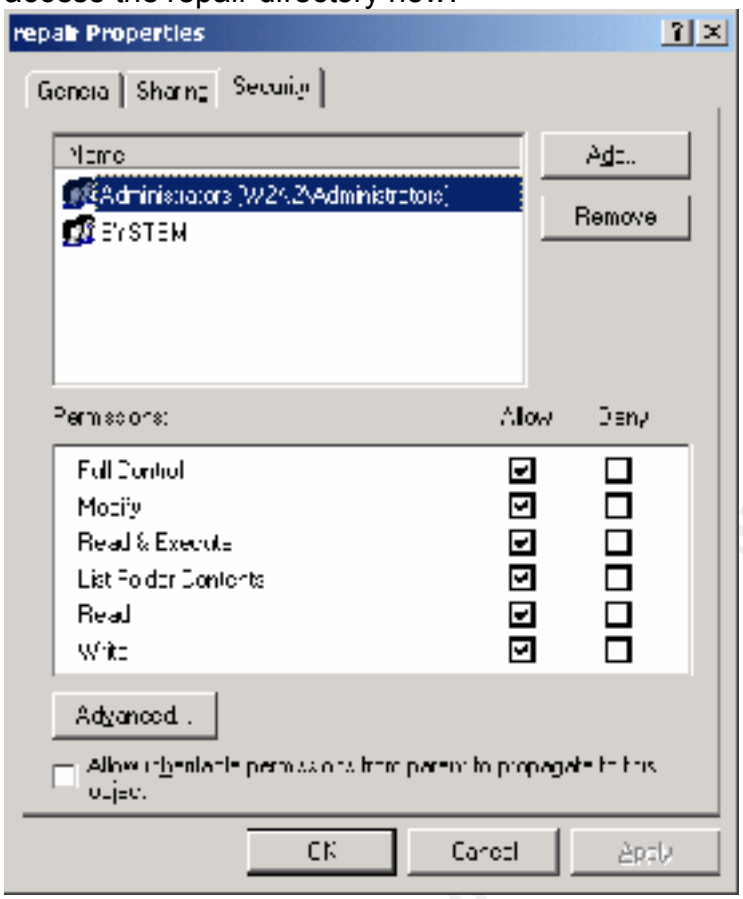
The NSA template could be applied to systems manually on each laptop as it is built with an image file. It is also possible to add this template to the Group Policy Object on a group called “Jump Kit Laptops.” Then the new laptops could just log into the Active Directory to force the application of the jump kit security template. More software would be needed to really secure these laptops than just the template, though. For example, the latest anti virus software and firewalls should be used. Installing software can be done through templates and scripts, but is beyond the scope of this paper.

The template was tested to ensure that items have been applied as expected. Security from this template is working properly. For example, when I reboot the computer and try to logon, there is no user listed in the user name space. This is basically a good thing because it prevents the hacker from seeing what my user name is. No user name could also backfire because it could allow the hacker to logon and I lose the benefit of seeing who was the last user to logon to my laptop.

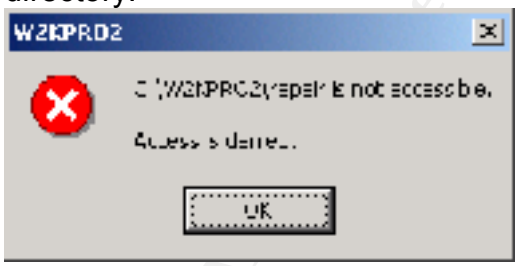
A second example of good security as a result of the NSA template is the repair directory permissions. When I log on as a different user who is not an administrator, I can see that the repair directory is inaccessible. The SAM file

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

stored there is now secure. Only the Administrators and the SYSTEM can access the repair directory now.



The guest account sees the following error when trying to open the repair directory.



The template does a very good job at applying a strong password policy. When I change the password and try to use the word “password,” the user is presented with the instructions as a reminder to use a good password, with explicit instructions. That is a nice feature.

The template did not "break" anything. I was able to perform regular tasks with my incident handling software toolset. ISS Scanner scanned another host over the network without a problem. The scan completed in about the same amount of time that the system took before the NSA security template was added. L0phtcrack 2.5 also runs without a problem. PWDUMP is able to dump passwords from the local computer, as well as over the network. The SMB packet capture feature also works. Finally, the war dialer THC-scan still

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

functions correctly. The issue here is really the modem, not THC-scan itself. The modem is still enabled and configured and was not broken by the security template.

I noticed that the Guest account password couldn't be changed by the Guest account. I do not know if this is a result of the template or not. As an administrator, I enabled the guest account and required the guest account to change the password at next logon. When the guest account logs on, the guest is not allowed to change its own password. This may be due to something within the template. A workaround could be to set the guest password from the administrator account through the MMC, or to change the guest account before applying the template.

L0phtcrack requires administrator access in order to run correctly. For that reason, I will most often be logged in as Administrator when using this laptop. There is really no need to test the tools when logged in as another user. I do have one more account setup as a backdoor, in case something happens to the Administrator account. All programs worked under that account as well, because that account is a member of the Administrators group. The only other account is Guest, which is disabled.

Netstat still displays all the same ports that were available at the original baseline. Shutting down the server service would probably change some of these ports.

V. Evaluate the template.

The default install of windows 2000 Professional is not very secure. I would not use leave it in default mode in a hostile network. Aside from obvious vulnerabilities such as a weak admin password, most of the vulnerabilities in the default install are caused backward compatibility functions. Null sessions and Lan Manager password vulnerabilities are a few examples of vestigial functions for backward compatibility. Any security would be better than the default install. The NSA security template addresses password strength and other issues that I may have in common with other computer network users. However, my requirements are relatively unique. As a standalone laptop, I will not ever need to log onto any Win2K Active Directory, NT Server, or even another windows machine. All I really need is the TCP/IP stack in order to run the ISS Scanner.

From the section of this paper entitled "III. Security Settings," the security provided by the NSA template is good in the following requirements: 3, 5, 8, 12, and 17. The security provided by the NSA template is weak in the following requirements: 1, 2, 4, 7, 10, 11, 13, 14, 15, 16, and 18. Concerning requirement 4, I would like the password protected screen saver to appear within 3 minutes of idle time. The current setting is too long, and exposes the laptop to undo risk. Concerning requirement 15, the default Administrator account is not renamed, and a honey pot created in its place. ISS Scanner reports describe how to do this in detail. Honey potting that account on the jump kit laptop is almost a must have. More skillful hackers will not try to logon as Administrator, but will go for SYSTEM level access instead. The best way for me to defend against that is to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

watch out for malicious code, and strange ports opened on my laptop. AntiVirus software and a personal firewall would help.

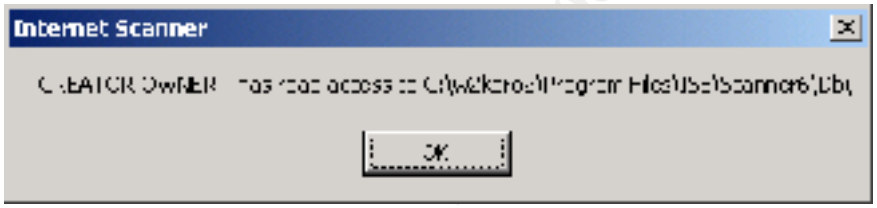
The reason that the NSA template is weak is that my requirements are for very high security. I am in a unique situation where I can trade away a lot of functionality that most other Windows users would need.

The NSA template is a good template for a general use Windows 2000 client on a LAN. One thing I would change would be to have the screen saver activate with password protection when the computer is unattended for some time. This small item would go a long way toward the overall network security posture.

The most notable changes that are unique in my particular environment are the very intrusive settings such as unbinding NetBIOS from tcp, shutting down the server service, and getting rid of Lan Manager passwords. Most of the other requirements are common to many other environments.

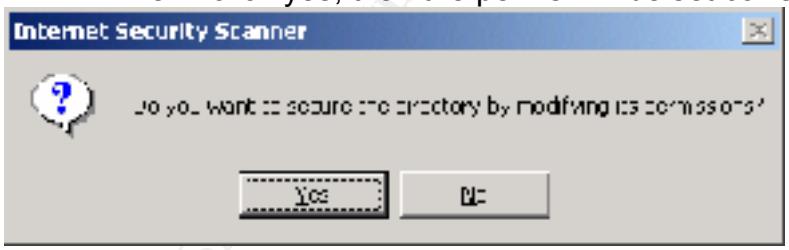
The NSA template does not adversely impact the applications I will use most often. Those applications are ISS Scanner, L0phtcrack, and a wardialer. MS Word will also be used to type up preliminary reports. Pwdump might be affected if null sessions could not be established outbound. However, I only require that null sessions cannot be established inbound to my laptop.

One minor error does occur for ISS Scanner but it is easy to overcome. Many of the directories are set with permissions for CREATOR OWNER. ISS



Scanner gives me a warning about that.

When I click yes, then the perms will be set correctly.



The only thing that truly requires special treatment to function is the modem. The modem should be software disabled by the template, so that I arrive on site with a more secure computer. Then I can manually enable to modem when I am read to wardial. This is important so that my laptop does not become a router to allow packets to route around the firewall established on site, assuming there is a firewall on site. In keeping with the theory of defense in depth, I would unplug the phone, remove the modem, and software disable the modem driver.

Further research could be done on combining OEM type templates such that the BIOS password could be set within the Windows 2000 template. It

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

seems to me that intricate knowledge would be required of the system BIOS, down to the register level. The operating system buffers the users from all these complexities. Still, it would be nice to be able to buy a vendor's laptop, and secure that laptop from start to finish all with one click on Go.

The security template could be improved by peer review from as many system administrators as possible. Adding new pieces to the security puzzle requires a sharing of ideas on a very large scale. There are many esoteric vulnerabilities. It is important that the good systems administrators benefit from the security "fix" before the vulnerability is exploited on their own systems.

I do not think that there are more efficient methods that could be used to secure and update jump kit systems. One could add the template to the GPO to automate security application when the laptop logs on to AD one time. From a business angle, we could contract out the work of building our jump kit laptops, but that brings with a whole new concern over computer security. We could ask a large computer distributor to configure jump kit laptops, but the same security concerns would arise. Ultimately, the best solution is the security template and a few more manual settings.

One final note I would like to add is that templates did not work very well in the world of Windows NT prior to service pack 4, and were especially flaky with Windows 95. I recall trying to build many clients on our LAN a few years back before image copying became widely used, and I was trying to use templates to configure all the clients the same. The hassle caused by the templates was not worth the final product. If and when the templates did apply without errors, we had to basically put our hands on every keyboard in the LAN. At one time that was only 400 people, but it quickly grew to 3,000 within a few years. We needed a central delivery mechanism, and something that would apply these templates at night when the users were not there. Windows2000 has come a long way from its predecessors concerning security templates.

A new template should be generated to fit my specific requirements. The following changes were made to the NSA template and my template is a work in progress below.

Disabled the server service.
Disabled the computer browser service.
Message text for users attempting to logon is set.
Renamed Administrator account.
Renamed Guest account.

New Jump Kit Laptop Security Template.
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Description=NSA Enhanced Security Settings for Windows 2000
Professional workstation
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 1
NewAdministratorName = "Duck"
NewGuestName = "Mickey"
ClearTextPassword = 0
[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 3
CrashOnAuditFull = 1
[Registry Values]
machine\system\currentcontrolset\services\netlogon\parameters\signsecur
echannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecur
echannel=4,1
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext=1,Loging on to this computer gives informed consent to monitoring.
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows\currentversion\policies\explorer\nodrivetypeautorun=4,255
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\autoadminlogon=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\driver signing\policy=3,1
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = *S-1-5-32-544
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-545
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege =
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-545,*S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-544
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = *S-1-5-32-545,*S-1-5-32-544
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
seshutdownprivilege = *S-1-5-32-545,*S-1-5-32-544
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege = *S-1-5-32-545,*S-1-5-32-544
[Registry Keys]
1="classes_root", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
2="machine\software", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
3="machine\software\microsoft\netdde", 2,
"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
4="machine\software\microsoft\os/2 subsystem for nt", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
5="machine\software\microsoft\protected storage system provider", 1,
"D:AR"
6="machine\software\microsoft\windows nt\currentversion\asrcommands",
2,
"D:PAR(A;CI;KA;;;BA)(A;CI;CCDCLCSWRPSDRC;;;BO)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
7="machine\software\microsoft\windows nt\currentversion\perflib", 2,
"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
8="machine\software\microsoft\windows\currentversion\group policy", 0,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
9="machine\software\microsoft\windows\currentversion\installer", 0,
"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
a="machine\software\microsoft\windows\currentversion\policies", 0,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
b="machine\system", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
c="machine\system\clone", 1, "D:AR"
d="machine\system\controlset001", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
e="machine\system\controlset002", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
f="machine\system\controlset003", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
10="machine\system\controlset004", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
11="machine\system\controlset005", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
12="machine\system\controlset006", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
        13="machine\system\controlset007", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
        14="machine\system\controlset008", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
        15="machine\system\controlset009", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
        16="machine\system\controlset010", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
        17="machine\system\currentcontrolset\control\securepipeservers\winreg",
2, "D:PAR(A;CI;KA;;;BA)(A;;KR;;;BO)(A;CI;KA;;;SY)"
        18="machine\system\currentcontrolset\control\wmi\security", 2,
"D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
        19="machine\system\currentcontrolset\enum", 1,
"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
        1a="machine\system\currentcontrolset\hardware profiles", 0,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
        1b="machine\system\currentcontrolset\services\snmp\parameters\permitte
dmanagers", 2, "D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
        1c="machine\system\currentcontrolset\services\snmp\parameters\validco
mmunities", 2, "D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
        1d="users\.default", 2,
"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
        1e="users\.default\software\microsoft\netdde", 2,
"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
        1f="users\.default\software\microsoft\protected storage system provider",
1, "D:AR"
        [File Security]
        1="c:\", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
        2="c:\autoexec.bat", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        3="c:\boot.ini", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
        4="c:\config.sys", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
        5="c:\documents and settings", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        6="c:\documents and settings\administrator", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        7="c:\documents and settings\all users", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        8="c:\documents and settings\all users\documents\drwatson", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICIIO;DCLCWP
;;;BU)(A;OICI;CCSWWPLORC;;;BU)"
        9="c:\documents and settings\all
users\documents\drwatson\drwtsn32.log", 2,
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1301bf;;;
BU)"
        a="c:\documents and settings\default user", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        b="c:\io.sys", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        c="c:\msdos.sys", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        d="c:\my download files", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1201bf;;;
BU)"
        e="c:\ntbootdd.sys", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
        f="c:\ntdetect.com", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
        10="c:\ntldr", 2, "D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
        11="c:\program files", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
        12="c:\program files\resource pro kit", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        13="c:\system volume information", 1, "D:PAR"
        14="c:\temp", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCWP;;;BU
)"
        15="c:\w2kpro2", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
        16="c:\w2kpro2\$ntservicepackuninstall$", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        17="c:\w2kpro2\csc", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        18="c:\w2kpro2\debug", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
        19="c:\w2kpro2\debug\usermode", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;;CCDCWP;;;BU)(A;OIIO;DCLC;;;BU)
"
        1a="c:\w2kpro2\offline web pages", 1, "D:(A;OICI;GA;;;WD)"
        1b="c:\w2kpro2\regedit.exe", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        1c="c:\w2kpro2\registration", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
        1d="c:\w2kpro2\repair", 2, "D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        1e="c:\w2kpro2\security", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
        1f="c:\w2kpro2\system32", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
        20="c:\w2kpro2\system32\appmgmt", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        21="c:\w2kpro2\system32\config", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        22="c:\w2kpro2\system32\dllcache", 2,
"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
        23="c:\w2kpro2\system32\dtclog", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
        24="c:\w2kpro2\system32\grouppolicy", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
        25="c:\w2kpro2\system32\ias", 2,
"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
        26="c:\w2kpro2\system32\ntbackup.exe", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        27="c:\w2kpro2\system32\ntmsdata", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        28="c:\w2kpro2\system32\rcp.exe", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        29="c:\w2kpro2\system32\regedt32.exe", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        2a="c:\w2kpro2\system32\reinstallbackups", 1,
"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(
A;OICI;GA;;;CO)"
        2b="c:\w2kpro2\system32\repl", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        2c="c:\w2kpro2\system32\repl\export", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200
a9;;;BU)"
        2d="c:\w2kpro2\system32\repl\import", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a
9;;;BU)"
        2e="c:\w2kpro2\system32\rexec.exe", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        2f="c:\w2kpro2\system32\rsh.exe", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        30="c:\w2kpro2\system32\secedit.exe", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
        31="c:\w2kpro2\system32\setup", 0,
"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
        32="c:\w2kpro2\system32\spool\printers", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCSWWPL
O;;;BU)"
        33="c:\w2kpro2\tasks", 1, "D:AR"
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

34="c:\w2kpro2\temp", 2,
"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU
)"
[Service General Setting]
1="browser", 4,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSW
RPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;
FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
2="lanmanserver", 4,
"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSW
RPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;
FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

VI. References

1. LabMice Windows 2000 Installation Security Checklist, Last updated October 25th 2001, www.labmice.net/articles/securingwin2000.htm
2. NSA Windows 2000 Security Guide, www.nsa.gov
3. Microsoft High Security for Stand Alone PC Template, Windows 2000 distribution CD
4. www.microsoft.com. Q185590. Guide To Windows NT 4.0 Profiles and Policies.
5. http://www.eEye.com for nmap ported to windows.
6. Jumes, et. Al. Windows NT4.0 Security, Audit, and Control. MS Press. 1999.

© SANS Institute 2000 - 2002, Author retains full rights

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: July 27th, 2017

Upcoming Training

SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC505: Securing Windows and PowerShell Automation	SEC505 - 201709,	Sep 18, 2017 - Nov 13, 2017	vLive
Secure DevOps Summit & Training	Denver, CO	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced