Microsoft Windows NT 4.0 Sp5 Enumeration: Through the Eyes of a Hacker

Adam Q. Steslicki

November 18, 2000

Introduction: “The best defense is a good offence”

What is the average hacker looking for on your NT systems? By attempting the same enumeration techniques and by using the same tools as the hackers are using, one can discover what information their NT systems are giving out to all whom are interested enough to look. The base installation of any NT system is, by default, giving out valuable information such as lists of users, last logon times, administrator user names, members of groups, and much more. In this paper we will uncover some of the more common methods of NT system enumeration, and best practices to be followed in order to prevent the flow of such information.

NOTE: The following presumes that an attacker has already acquired a set of NT 4.0 targets by completing the initial reconnaissance phase. The target machine used in the following examples and discussions will be:

Host name:	hackme.adamstez.com
NetBIOS name:	hackme
IP Address:	192.168.0.7

The attacking machine used in the following examples and discussions will be:

Host name:	2000srv.adamstez.com
NetBIOS name:	2000srv
IP Address:	192.168.0.1

Port Scanning: “What doors are open?”

Port scanning is the process of connecting to TCP and UDP ports on the target system to determine what services are running, or in a listening state. When port scanning a target system the hacker is looking to identify the services running on the target system, the specific application or version of that service, and possibly if not yet determined, the operating system of a given target.

SuperScan

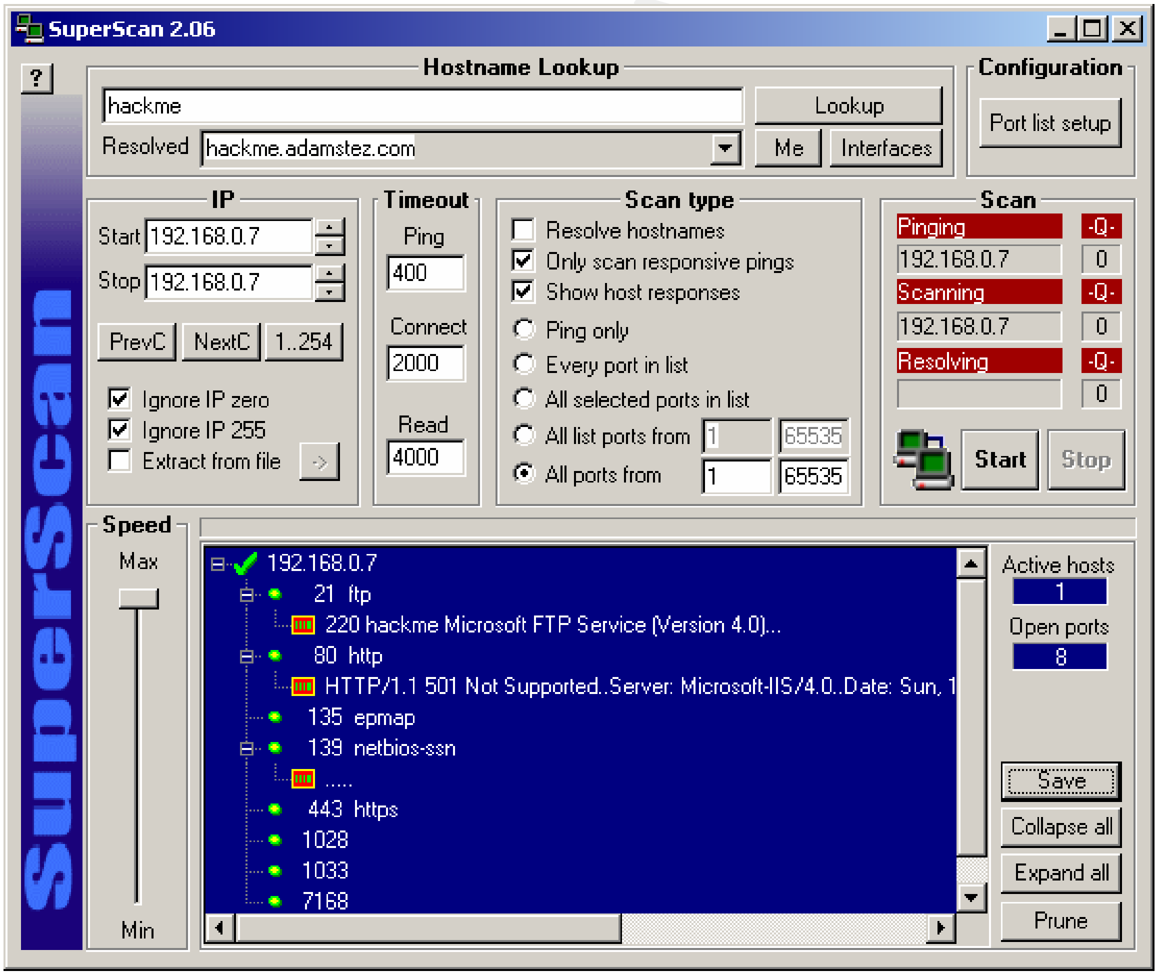
One common tool used to TCP port scan target systems is SuperScan by Rob Keir. As of this writing SuperScan is at version 2.06 and runs on all Microsoft Windows platforms. (Rob Keir). SuperScan can be found at http://packetstorm.securify.com/Win/scanner.zip

In order to use SuperScan, follow the steps below. We will perform a scan of our target host 192.168.0.7:

1. Download and extract the program files to your desired directory

2. Execute the scanner.exe file
3. SuperScan will open and present you with a GUI. See figure 1-1
4. Under the IP column enter the IP Address of the host you wish to scan. In our case this is our target machine 192.168.0.7
5. You can change various settings like the timeouts and the speed. Adjust them to your liking, or view the readme file for SuperScan for more information on the options
6. Change the Scan Type to "All ports from 1 to 65535" this will scan every TCP port on our target machine
7. Click on the "Start" button to initiate the TCP scan
8. Once the port scanning is complete you will see a screen like the one in Figure 1-1
9. You can save the results of your scan by selecting the "Save" Button on the lower right corner of the program for later analysis.
10. Once you are finished and have saved your results you may exit the program

Figure 1-1 SuperScan GUI



SuperScan 2.06

Hostname Lookup

hackme

Resolved hackme.adamstez.com

IP
Start 192.168.0.7
Stop 192.168.0.7

☑ Ignore IP zero
☑ Ignore IP 255
□ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
□ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 1 65535
● All ports from 1 65535

Scan
Pinging -Q-
192.168.0.7 0
Scanning -Q-
192.168.0.7 0
Resolving -Q-
0

Speed
Max
Min

```
192.168.0.7
    21  ftp
        220 hackme Microsoft FTP Service (Version 4.0)...
    80  http
        HTTP/1.1 501 Not Supported..Server: Microsoft-IIS/4.0..Date: Sun, 1
   135  epmap
   139  netbios-ssn
        .....
   443  https
  1028
  1033
  7168
```

Active hosts 1

Open ports 8

As you can see our target machine is offering a wide variety of services, which is the default Windows NT 4.0 install with service pack 5, applied. SuperScan is also able to tell us the NetBIOS name of the target machine, hackme, and the exact version of the software listening on those open ports. All of these TCP services are available for a remote attacker to exploit, but TCP is only one side of the story.

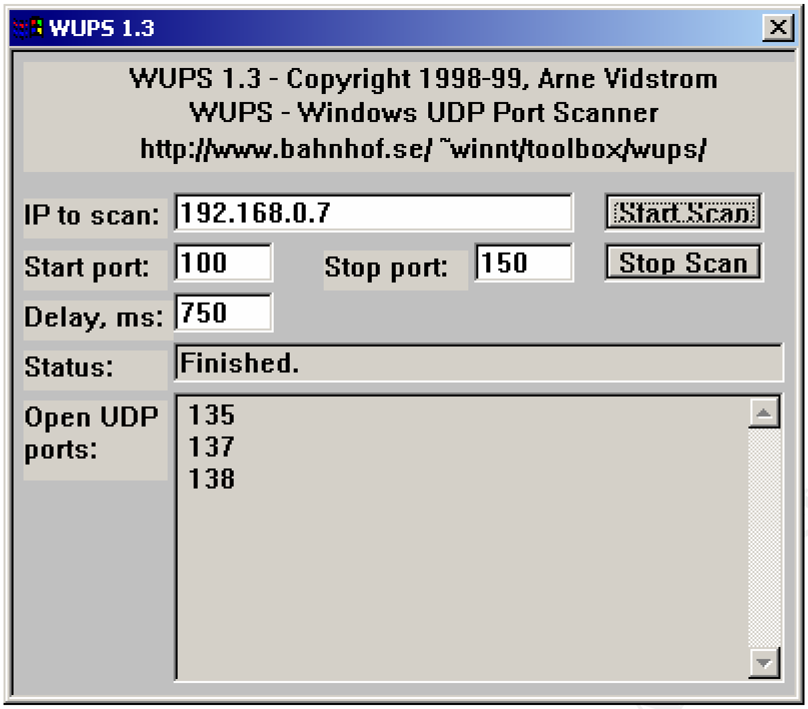
Wups

UDP port scanning is also an important factor that is often overlooked; many trojans listen on UDP ports as well as other exploitable services. On tool used by hackers to scan your UDP ports is the windows based Wups UDP scanner. (Arne Vidstrom). Wups can be downloaded from http://packetstorm.securify.com/NT/scanners/wups.exe

In order to use Wups follow the steps below, we will perform a scan of our target host 192.168.0.7:

1. Download the program and install
2. Start the Wups program
3. You will be presented with a screen similar to figure 2-1
4. Enter the target IP Address, in our example we will be scanning 192.168.0.7
5. Enter the desired range of ports to scan
6. Click on the "Start Scan" button to begin the UDP scan
7. Once the scanning is complete you will see a screen similar to figure 2-1

Figure 2-1 Wups GUI



WUPS 1.3 - Copyright 1998-99, Arne Vidstrom
WUPS - Windows UDP Port Scanner
http://www.bahnhof.se/ ~winnt/toolbox/wups/

IP to scan: 192.168.0.7

Start port: 100

Stop port: 150

Delay, ms: 750

Status: Finished.

Open UDP ports:

```
135
137
138
```

As you can see when Wups has finished you can see that UDP ports 135, 137, and 138 are open. The table below shows the services offered by these UDP ports: (Technotronic)

UDP Port Services

loc-srv	135/udp	Location Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/udp	NETBIOS Datagram Service

Countermeasures: "How do I protect against giving out Port information?"
Unfortunately it is difficult to prevent someone from port scanning you, however you can minimize your exposure by disabling unused services. This can be accomplished through the control panel services applet, and through the network applet. (Hacking Exposed). More of this will be discussed as we cover other specific NT countermeasures.

Another method of port scanning prevention would be detection via a host or network based intrusion detection system. Also most firewalls can be configured to detect and log port scans. Once again the best protection is still to disable unused services.

NT Banner Enumeration: "What version of IIS am I running?"

NT banner enumeration is the process of viewing the information returned by a particular system when an application connects and sends a request. (Mark Manasi). One can easily find out exactly what name and version of software you are running on a specific port by executing a simple telnet to the designated port. Below is the output of a telnet session to 192.0.0.7 on port 80, which we know to be open from our previous scans. After the initial telnet just hit enter a few times and this is what we get:

```
C:\>telnet 192.168.0.7 80

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Sun, 19 Nov 2000 00:53:12 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter
is incorrect. </body>
</html>

Connection to host lost.
```

The same thing goes for FTP:

```
C:\>telnet 192.168.0.7 21

220 hackme Microsoft FTP Service (Version 4.0).
221

Connection to host lost.
```

Now that NT has so kindly provided the hacker with the exact version of IIS running on the target machine, the hacker can now focus his efforts on finding an exploit that effects this particular machine. Banner grabbing can be applied to different systems and different ports, if a listening application provides an interesting response then that information can be used to specifically target your systems

Countermeasures: "How do I stop from giving out Banner information"

First you must research the correct way to disable the vendor specific presentation of version information in banners. Secondly audit yourself regularly with port scans and raw telnet connects to ports, to see how much information you are actually giving away.

Remember though that this is only a way to mask what type of FTP, Web server, or other application you are running. This is not a method of preventing an unauthorized user of discovering what operating system you are running those applications on top of. By disabling Microsoft's FTP server's banner you cloak the FTP server only, a determined individual will use other methods to discover exactly what operating system is running, namely remote operating system detection via TCP/IP stack finger printing which unfortunately is out of the scope of this document. (Insecure.org). If however you want more information it can be found at http://www.insecure.org/nmap/nmap-fingerprinting-article.html

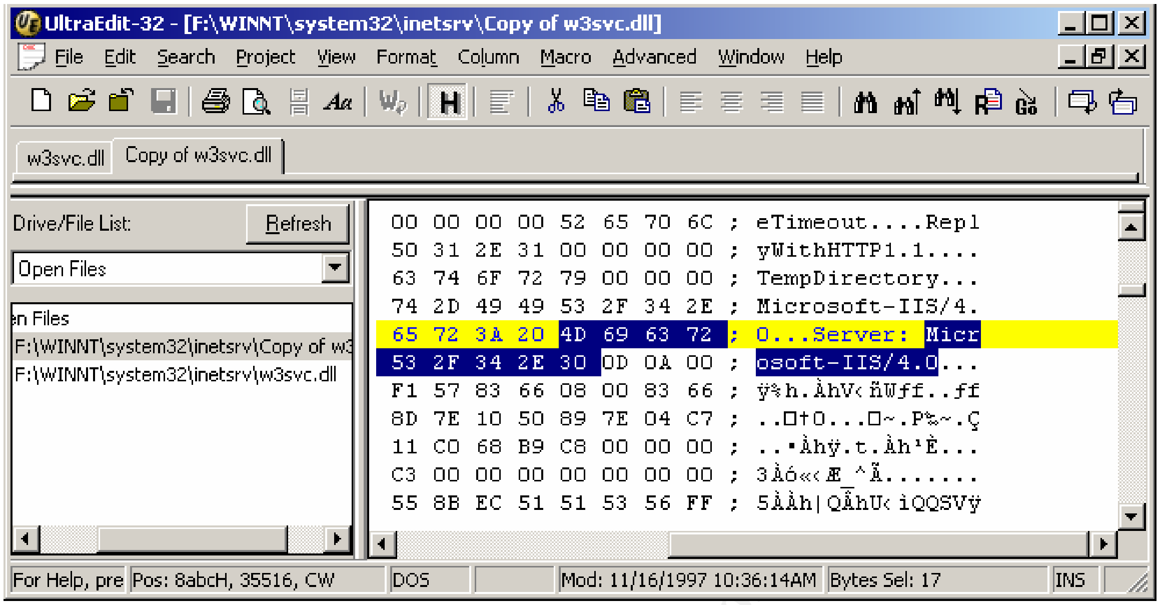
Removing Microsoft's IIS Banner

Here is an example of how to remove the banners from Microsoft NT IIS and FTP. First you will need to have access to a Hex Editor, UltraEdit by IDM Computer Solutions, is what will be used in this example. You can download an evaluation version of UltraEdit from ftp://ultraedit.com/uedit32.zip for the windows platform. The two files in question that hold the banner information for IIS and FTP are W3SVC.DLL and FTPSVC2.DLL respectively. (Júlio Falcão). Follow the steps below to remove the banners from Microsoft IIS and FTP:

Note: Be sure to make a back up copy of W3SVC.DLL and FTPSVC2.DLL before attempting the following steps.

1. Open the services applet in control panel
2. Stop the World Wide Web Publishing Service. This will give you access to edit the W3SVC.DLL file
3. Open your hex editor
4. Chose the file menu and then choose to open a file
5. Navigate to winnt\system32\inetsrv
6. To edit the IIS banner open the W3SVC.DLL file in your hex editor
7. Click on the Search menu and then click on the Find option
8. Search for the string "4.0". You are looking for this line "Server: Microsoft-IIS/4.0" in the hex editor. See figure 3-1
9. Move your cursor to the beginning of the "Microsoft-IIS/4.0" line
10. Begin to type the desired name of your new WWW server. You will see that your typing overwrites the text that is there. Be sure to replace the exact number of characters no more and no less, or you will not be able to restart IIS. See figure 3-2
11. Save the W3SVC.DLL file
12. Restart the World Wide Web Publishing Service for the changes to take effect

Figure 3-1 W3SVC.DLL in Hex Editor Unchanged

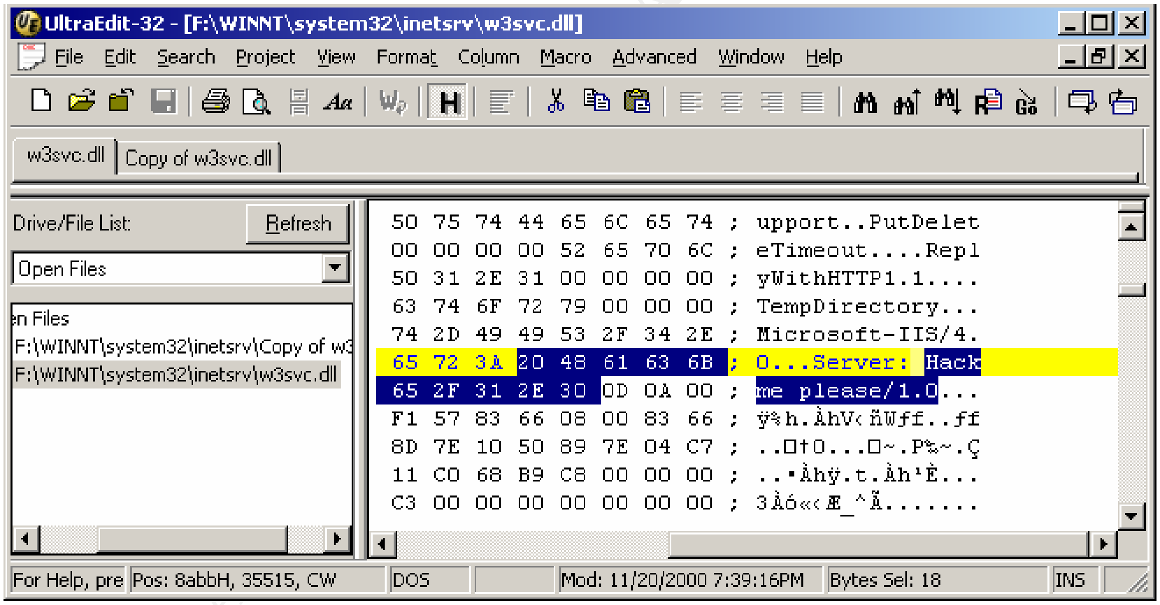

UltraEdit-32 - [F:\WINNT\system32\inetsrv\Copy of w3svc.dll]
File Edit Search Project View Format Column Macro Advanced Window Help
w3svc.dll
Copy of w3svc.dll
Drive/File List:
Refresh
Open Files

```
n Files
F:\WINNT\system32\inetsrv\Copy of w3
F:\WINNT\system32\inetsrv\w3svc.dll
```

```
00 00 00 00 52 65 70 6C ; eTimeout....Repl
50 31 2E 31 00 00 00 00 ; yWithHTTP1.1....
63 74 6F 72 79 00 00 00 ; TempDirectory...
74 2D 49 49 53 2F 34 2E ; Microsoft-IIS/4.
65 72 3A 20 4D 69 63 72 ; 0...Server: Micr
53 2F 34 2E 30 0D 0A 00 ; osoft-IIS/4.0...
F1 57 83 66 08 00 83 66 ; ÿ‰h.ÀhV‹ñWƒf..ƒf
8D 7E 10 50 89 7E 04 C7 ; ..□†0...□~.P‰~.Ç
11 C0 68 B9 C8 00 00 00 ; ..•Àhÿ.t.Àh¹È...
C3 00 00 00 00 00 00 00 ; 3Àó«‹Æ_^Ã.......
55 8B EC 51 51 53 56 FF ; 5ÀÀh|QÃhU‹iQQSVÿ
```

```
For Help, pre | Pos: 8abcH, 35516, CW | DOS | Mod: 11/16/1997 10:36:14AM | Bytes Sel: 17 | INS
```

Figure 3-2 W3SVC.DLL in Hex Editor Changed


UltraEdit-32 - [F:\WINNT\system32\inetsrv\w3svc.dll]
File Edit Search Project View Format Column Macro Advanced Window Help
w3svc.dll
Copy of w3svc.dll
Drive/File List:
Refresh
Open Files

```
n Files
F:\WINNT\system32\inetsrv\Copy of w3
F:\WINNT\system32\inetsrv\w3svc.dll
```

```
50 75 74 44 65 6C 65 74 ; upport..PutDelet
00 00 00 00 52 65 70 6C ; eTimeout....Repl
50 31 2E 31 00 00 00 00 ; yWithHTTP1.1....
63 74 6F 72 79 00 00 00 ; TempDirectory...
74 2D 49 49 53 2F 34 2E ; Microsoft-IIS/4.
65 72 3A 20 48 61 63 6B ; 0...Server: Hack
65 2F 31 2E 30 0D 0A 00 ; me please/1.0...
F1 57 83 66 08 00 83 66 ; ÿ‰h.ÀhV‹ñWƒf..ƒf
8D 7E 10 50 89 7E 04 C7 ; ..□†0...□~.P‰~.Ç
11 C0 68 B9 C8 00 00 00 ; ..•Àhÿ.t.Àh¹È...
C3 00 00 00 00 00 00 00 ; 3Àó«‹Æ_^Ã.......
```

```
For Help, pre | Pos: 8abbH, 35515, CW | DOS | Mod: 11/20/2000 7:39:16PM | Bytes Sel: 18 | INS
```

To prove that this actually works recall the output we received from our earlier telnet into 192.168.0.7 on port 80, show below for your convenience:

```
C:\>telnet 192.168.0.7 80

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Sun, 19 Nov 2000 00:53:12 GMT
Content-Type: text/html
Content-Length: 87
```

```
<html><head><title>Error</title></head><body>The parameter
is incorrect. </body>
</html>

Connection to host lost.
```

Now take a look at the output below from a new telnet into 192.168.0.7 on port 80 after our changes to the W3SVC.DLL file:

```
HTTP/1.1 400 Bad Request
Server: Hackme please/1.0
Date: Tue, 21 Nov 2000 00:39:34 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter
is incorrect. </body>
</html>

Connection to host lost.
```

Removing Microsoft's FTP Banner

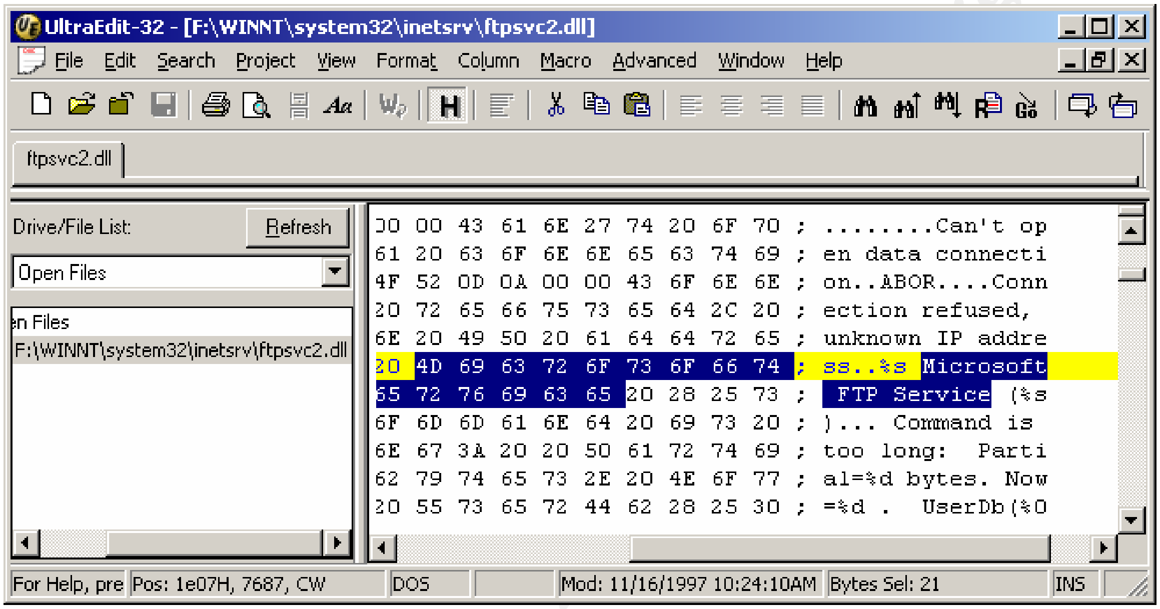
Making this change to Microsoft's FTP server is just as easy. Follow the steps below:

Note: Be sure to make a back up copy of W3SVC.DLL and FTPSVC2.DLL before attempting the following steps.

1. Open the services applet in control panel
2. Stop the FTP Publishing Service. This will give you access to edit the FTPSVC2.DLL file
3. Open your hex editor
4. Chose the file menu and then choose to open a file
5. Navigate to winnt\system32\inetsrv
6. To edit the FTP banner open the FTPSVC2.DLL file in your hex editor
7. Click on the Search menu and then click on the Find option
8. Search for the string "Microsoft FTP". You are looking for this line "Microsoft FTP Service" in the hex editor. See figure 3-3
9. Move your cursor to the beginning of the "Microsoft FTP Service" line
10. Begin to type the desired name of your new FTP server. You will see that your typing overwrites the text that is there. Be sure to replace the exact number of characters, no more and no less, or you will not be able to restart the FTP server. See figure 3-4
11. Next search for the string "Version 4"

12. Place your cursor over the beginning of the string and make the desired changes
13. Save the FTPSVC2.DLL file
14. Restart the FTP Publishing Service for the changes to take effect

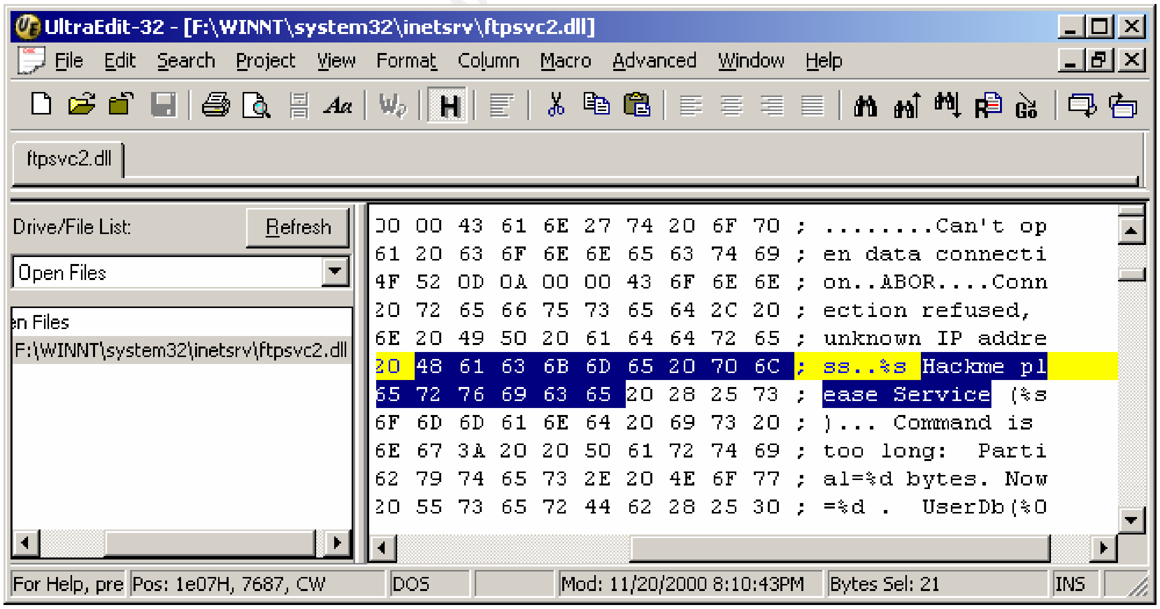
Figure 3-3 FTPSVC2.DLL in Hex Editor Unchanged


UltraEdit-32 - [F:\WINNT\system32\inetsrv\ftpsvc2.dll]
File Edit Search Project View Format Column Macro Advanced Window Help
ftpsvc2.dll
Drive/File List:
Refresh
Open Files
n Files
F:\WINNT\system32\inetsrv\ftpsvc2.dll

```
00 00 43 61 6E 27 74 20 6F 70 ; ........Can't op
61 20 63 6F 6E 6E 65 63 74 69 ; en data connecti
4F 52 0D 0A 00 00 43 6F 6E 6E ; on..ABOR....Conn
20 72 65 66 75 73 65 64 2C 20 ; ection refused,
6E 20 49 50 20 61 64 64 72 65 ; unknown IP addre
20 4D 69 63 72 6F 73 6F 66 74 ; ss..%s Microsoft
65 72 76 69 63 65 20 28 25 73 ;  FTP Service (%s
6F 6D 6D 61 6E 64 20 69 73 20 ; )... Command is
6E 67 3A 20 20 50 61 72 74 69 ; too long:  Parti
62 79 74 65 73 2E 20 4E 6F 77 ; al=%d bytes. Now
20 55 73 65 72 44 62 28 25 30 ; =%d .  UserDb(%0
```

For Help, pre | Pos: 1e07H, 7687, CW | DOS | Mod: 11/16/1997 10:24:10AM | Bytes Sel: 21 | INS

Figure 3-4 FTPSVC2.DLL in Hex Editor Changed


UltraEdit-32 - [F:\WINNT\system32\inetsrv\ftpsvc2.dll]
File Edit Search Project View Format Column Macro Advanced Window Help
ftpsvc2.dll
Drive/File List:
Refresh
Open Files
n Files
F:\WINNT\system32\inetsrv\ftpsvc2.dll

```
00 00 43 61 6E 27 74 20 6F 70 ; ........Can't op
61 20 63 6F 6E 6E 65 63 74 69 ; en data connecti
4F 52 0D 0A 00 00 43 6F 6E 6E ; on..ABOR....Conn
20 72 65 66 75 73 65 64 2C 20 ; ection refused,
6E 20 49 50 20 61 64 64 72 65 ; unknown IP addre
20 48 61 63 6B 6D 65 20 70 6C ; ss..%s Hackme pl
65 72 76 69 63 65 20 28 25 73 ; ease Service (%s
6F 6D 6D 61 6E 64 20 69 73 20 ; )... Command is
6E 67 3A 20 20 50 61 72 74 69 ; too long:  Parti
62 79 74 65 73 2E 20 4E 6F 77 ; al=%d bytes. Now
20 55 73 65 72 44 62 28 25 30 ; =%d .  UserDb(%0
```

For Help, pre | Pos: 1e07H, 7687, CW | DOS | Mod: 11/20/2000 8:10:43PM | Bytes Sel: 21 | INS

Again to prove that this has worked, recall our earlier telnet into 192.168.0.7 on port 21, shown below:

```
220 hackme Microsoft FTP Service (Version 4.0).
```

Now look at the results of a telnet to 192.168.0.1 on port 21, shown below:

```
220 hackme Hackme please Service (Victim  1.0).
```

This is an effective way to hide the version and vendor of your Microsoft FTP and WWW services, but remember this in no way hides your operating system. Also it is important to point out that this is security through obscurity, which everyone knows is not the greatest method of achieving secure systems. There are many other tell tale signs of Microsoft's WWW and FTP services, like custom error messages, but this will at least deter the average script kidde.

Simple NetBIOS enumeration: "This stuff is easy"

The process of gathering information about a targets NT systems is easy using the following tools and techniques. One should try the following techniques from inside and outside one's own network to see how much information you are giving away to internal and external users. (HappyHacker.org).

Net View

By using the built in NT net view command an attacker can find out much about the domain and computer structure of your network. Below a simple net view command is issued which shows the domains available to the attacking machine:

```
C:\>net view /domain
Domain

-------------------------------------------------------------
ADAMSTEZ
TESTDOM
The command completed successfully.
```

Also by selecting the domain one wishes to view we can see all of the computers in the domain:

```
C:\>net view /domain:testdom
Server Name            Remark

-------------------------------------------------------------
\\HACKME
The command completed successfully.
```

Nltest

Now to dig a little deeper we will use a tool from the NT Resource Kit called nltest. (Microsoft.com). Nltest is a tool that can identify the PDC and BDC of a network. Below is the output of nltest run on the domain testdom:

```
C:\>nltest /dclist:testdom
List of DCs in Domain testdom
    \\HACKME (PDC)
The command completed successfully
```

The Null Session

The following technique is arguably one of NT's most visible security failings, whether you have heard it called the "null session" or "anonymous logon" vulnerability, the fact remains that any anonymous user can connect to a target machine and enumerate certain resources without any logon credentials. (John Albright). The syntax of a null session connection is as follows:

```
C:\>net use \\192.168.0.7\IPC$ "" /user:""
The command completed successfully.
```

Now we have a null session connection to 192.168.0.7 which will allow us to pillage as much information as we desire about network information, shares, users, groups, registry keys, and so on. All of the following enumeration attacks use the null session vulnerability to gather information

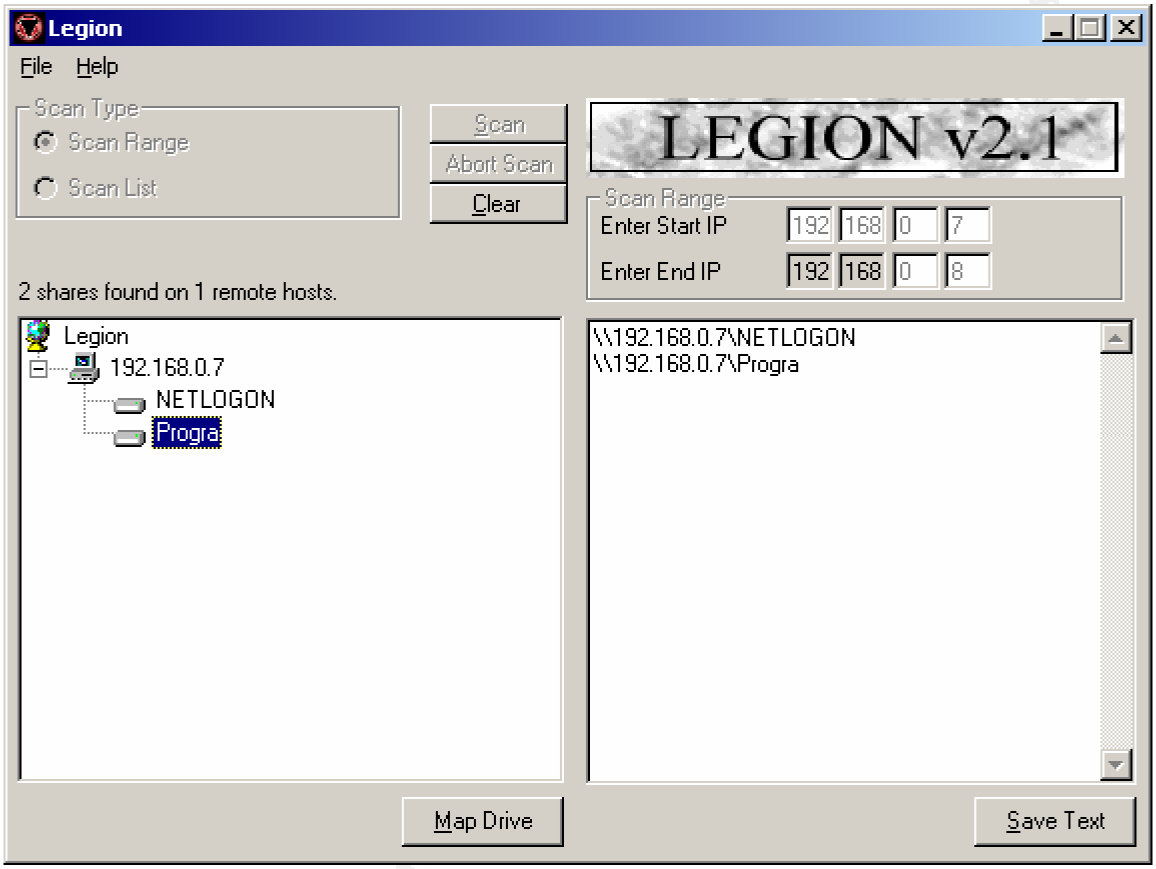
Legion

One tool that hackers use to enumerate shares on remote machines is Legion by Rhino9. Legion is a NetBIOS scanning tool that targets a group of machines or a specific machine looking for NetBIOS shares. Once a share has been found you can attempt to map a drive to the share. You can also attempt to brute force the username and password on the share to achieve unauthorized access, with the registered version only. (Rhino9). Legion can be downloaded from http://www.packetstorm.securify.com/groups/rhino9/legionv21.zip. In order to use Legion follow the steps below:

1. Download and install Legion to your desired directory
2. Start the Legion program
3. You will be presented with a screen similar to the one in figure 3-1
4. Enter a range of IP Address into the "Scan Range" section or you may elect to use a predetermined list of IP Addresses which can be selected by choosing the "Scan List" radio button
5. Click on the "Scan" button to initiate the NetBIOS share scan
6. Once Legion has finished you will see a screen similar to figure 3-1
7. If you would like to map a drive to the shares discovered click on the "Map Drive" button

8. If you would like to attempt to Brute Force attack the discovered shares you can click on the “Show BF Tool” button. Registered version only

Figure 3-1 Legion GUI



Scan Type
● Scan Range
○ Scan List

Scan Range
Enter Start IP 192 168 0 7
Enter End IP 192 168 0 8

2 shares found on 1 remote hosts.

```
Legion
  192.168.0.7
      NETLOGON
      Progra
```

```
\\192.168.0.7\NETLOGON
\\192.168.0.7\Progra
```

As you can see our target is offering two NetBIOS shares which we can attempt to make connections to using the built in brute force password cracking utility, registered version only.

Gnit

Another tool that checks for and interrogates the null session vulnerability and NetBIOS support is Gnit. Gnit was created by glitch of elicit.org and is freely available for download from http://packetstorm.securify.com/UNIX/scanners/gnit_rc1.zip. Gnit can discover remote NetBIOS name tables, all users, all groups, all shares, as well as giving detailed information about each user account. (Glitch). In order to use Gnit follow the steps below:

1. Download and extract Gnit
2. Open a command prompt
3. Change to the directory where Gnit was extracted

4. Type gnit followed by the IP Address of your target machine. Example: C:\> `gnit 192.168.0.7`
5. Gnit will initiate scanning. See figure 4-1
6. When finished Gnit will format a HTML report with the targets IP Address as the reports name, in Gnit's home directory
7. Open the HTML report in your web browser to view the results. See figure 4-2

Figure 4-1 Gnit command line output

```
J:\Programs\gnit>gnit 192.168.0.7
Starting scan of 192.168.0.7...
Connect checking port 139: NetBIOS...Open. Calling
netbios_scans
Connect checking port 80: HTTP...Open. Calling http_scans
Connect checking port 21: FTP...Open. Calling ftp_scans
Connect checking port 25: SMTP...Closed. Moving On...
Connect checking port 110: POP3...Closed. Moving On...
Connect checking port 23: Telnet...Closed. Moving On...
Connect checking port 42: WINS...Closed. Moving On...
Connect checking port 53: DNS...Closed. Moving On...
Connect checking port 119: NNTP...Closed. Moving On...
Connect checking port 389: LDAP...Closed. Moving On...
Connect checking port 1080: SOCKS...Closed. Moving On...
Connect checking port 1433: Microsoft SQL...Closed. Moving
On...
Connect checking port 5631: PC Anywhere...Closed. Moving
On...
Connect checking port 5800: VNC pPort...Closed. Moving
On...
Connect checking port 5900: VNC sPort...Closed. Moving
On...
Connect checking port 8010: WinGate LogFile
Service...Closed. Moving On...
Connect checking port 8080: Alt HTTP...Closed. Moving On...
Connect checking port 12345: Default NetBus...Closed.
Moving On...
Completed scan of 192.168.0.7.
```

As you can see Gnit provides a number of scans but for now the only scan results we are interested in are the NT system enumeration of accounts, groups, shares, and NetBIOS name table results.

Figure 4-2 Gnit HTML report

Results for 192.168.0.7

NBTStat Results	Details for Administrator
Intetrnal Segment: Node IpAddress: [192.168.0.1] Scope Id: [] NetBIOS Remote Machine Name Table Name Type Status --- HACKME <20> UNIQUE HACKME <00> UNIQUE TESTDOM <00> GROUP TESTDOM <1C> GROUP TESTDOM <1B> UNIQUE TESTDOM <1E> GROUP HACKME <03> UNIQUE INet~Services <1C> GROUP IS~HACKME......<00> UNIQUE TESTDOM <1D> UNIQUE ..__MSBROWSE__.<01> GROUP MAC Address = 00-60-08-C8-DB-7F \Device\NetBT_Tcpip_{8BF4FC44-9179-4B6E-A106-0F858C17F4F9}: Node IpAddress: [198.108.151.26] Scope Id: []	Global Group Membership: Domain Users Domain Admins Local Group Membership: Administrators Account Expires: Never Full Name: Bad Password Attempts: 22 Comments: Built-in account for administering the computer/domain Last Logon: Tue Oct 31 18:37:59 2000 Last Logoff: Wed Nov 8 18:53:53 2000 Logon Server: \\* Successful Logins: 0 Password Age: Mon Jan 19 21:46:23 1970 Primary Group ID: 513 Privilege: Admin RID: 500
NetView Results	Users and Groups
Shared resources at \\192.168.0.7 Share name Type Used as Comment --- NETLOGON Disk Logon server share Progra Disk The command completed successfully.	The groups are: Account Operators Administrators Backup Operators Guests Print Operators Replicator Server Operators Users MTS Trusted Impersonators Domain Admins Domain Guests Domain Users The list of user accounts are: Administrator Guest hackme IUSR_HACKME IWAM_HACKME

Note: Gnit HTML output was modified to save space

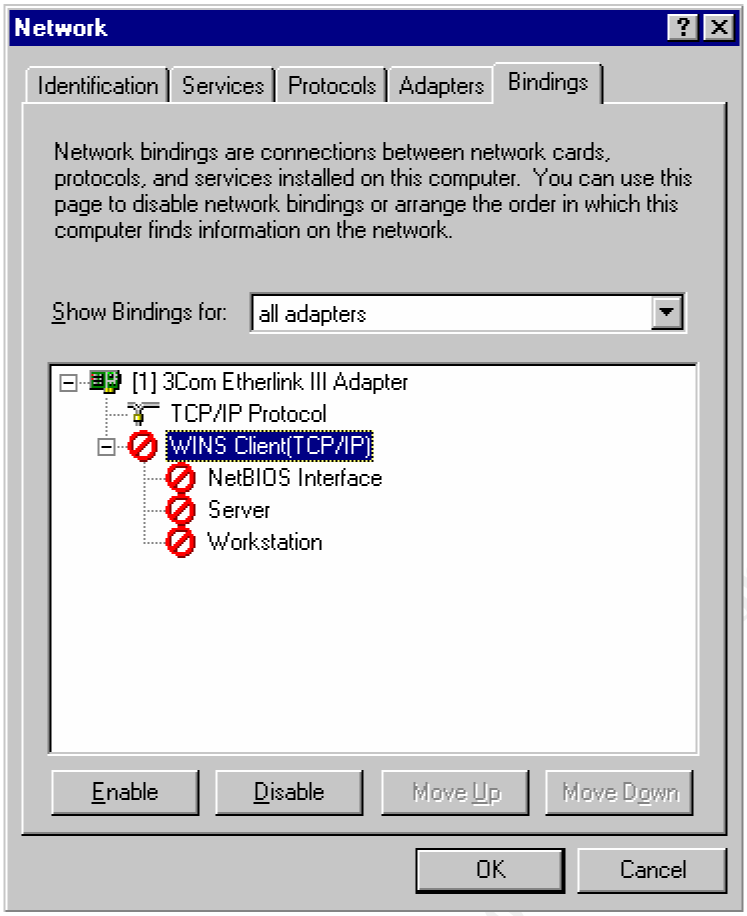
Not a bad amount of information, available to anyone who has the time to look. Gnit is a powerful tool but all of these results can be obtained from other various command line utilities provided either from the NT Resource Kit or freely available on the internet.

Countermeasures:

From the information provided by Gnit a hacker can launch a very detailed and precise attack on your systems, so how do you disable this kind of information from being handed out? All of the NetBIOS related enumeration techniques could be defeated in a number of easy steps. First disable TCP and UDP ports 135 through 139 at all external access devices. Disabling those ports can defeat nearly all of the techniques discussed above. For stand-alone systems on a DMZ or that are exposed to the Internet you can disable the NetBIOS bindings from the external interface using the network control panels bindings interface. (Mark Manasi). The steps to accomplish this are shown below:

1. From the NT systems desktop right click on the Network Neighborhood icon and select the properties option
2. Click on the Bindings tab
3. Select the external network adapter you wish to view the bindings for
4. Click on the + to expand the Interface tree
5. Click on the WINS Client (TCP/IP) so that it is highlighted
6. Click on the Disable button to disable the WINS Client binding for that adapter
7. You will see a screen similar to the screen in figure 5-1 when the WINS Client has been disabled
8. Restart your computer for the changes to take effect

Figure 5-1 Disabling WINS Client Bindings



Network bindings are connections between network cards, protocols, and services installed on this computer. You can use this page to disable network bindings or arrange the order in which this computer finds information on the network.

Show Bindings for: all adapters

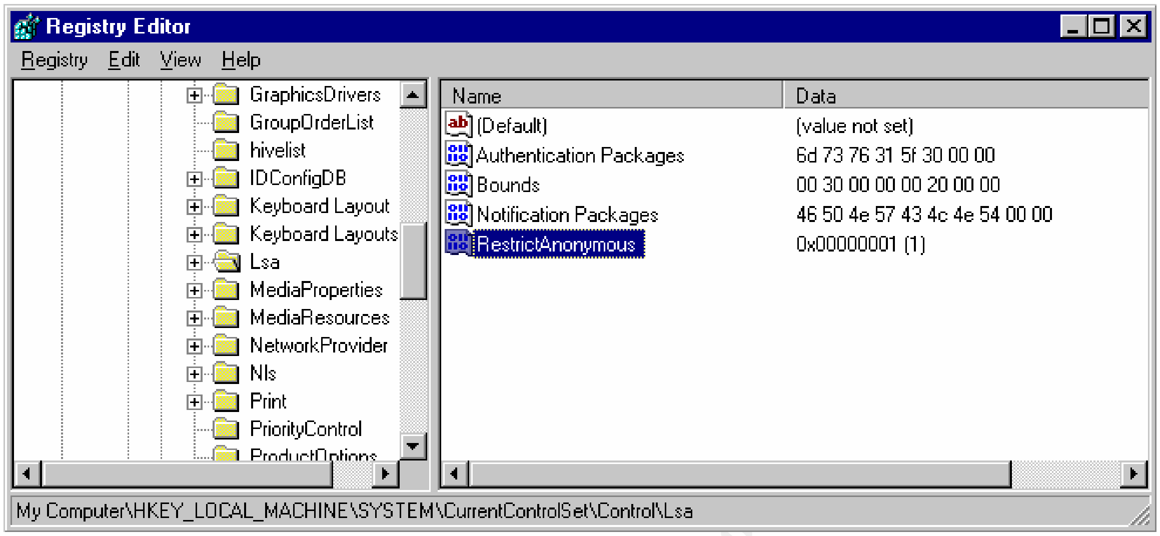
- [1] 3Com Etherlink III Adapter
  - TCP/IP Protocol
  - WINS Client(TCP/IP)
    - NetBIOS Interface
    - Server
    - Workstation

Once you see the screen in figure in 5-1 you can be assured that TCP and UDP ports 135 through 139 have been disabled. This will prevent any windows based service relying on NetBIOS from being exploited over the external interface.

Next you will need to disable the null session vulnerability. Following service pack 3 Microsoft has presented a mechanism used to disable null session information leaks. The mechanism is called RestrictAnonymous named after the registry key used to disable the null session. The steps to disable the null session connection are provided below:

1. Open your desired registry editor, in this example we will use regedit.exe
2. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa as seen in figure 5-2
3. Select the Edit menu | New | DWORD Value
4. Name the DWORD Value RestrictAnonymous
5. Double click the RestrictAnonymous DWORD
6. Enter a value of 1 to enable the DWORD
7. Exit the registry editor and restart the computer for the changes to take effect

Figure 5-2 RestrictAnonymous DWORD Value



Name	Data
(Default)	(value not set)
Authentication Packages	6d 73 76 31 5f 30 00 00
Bounds	00 30 00 00 00 20 00 00
Notification Packages	46 50 4e 57 43 4c 4e 54 00 00
RestrictAnonymous	0x00000001 (1)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Once the change has been made any attempts to connect to the target machine via a null session will fail.

Be sure to test this first in a development environment that duplicates your production servers. The null session method of access is used by some applications for information exchange and use.

Conclusion

All of the above methods are solid ways to perform a successful audit of your systems, and how to fix the holes when they are discovered. The paper also will help you to understand the techniques and tools hackers will use to infiltrate your systems and networks, and how to protect against them.

Bibliography

Reference #	Source	URL
1	Microsoft Knowledge Base article Q155363	http://support.microsoft.com/support/search
2	Bugtraq post	http://geek-girl.com/bugtraq/1997_2/0079.html
3	Hacking Exposed: Stuart McClure, Joel Scambray, George Kurtz	http://www.hackingexposed.com
4	Packetstorm	http://packetstorm.securify.com
5	Rob Keir	http://members.home.com/rkeir/
6	Arne Vidstrom	http://ntsecurity.nu/toolbox
7	Technotronic	http://www.technotronic.com/tcpudp.html
8	Mark Manasi	Mastering NT Server 4.0
9	Insecure.org	http://www.insecure.org
10	Júlio Falcão	[jfalcao@PROTEUS.COM.BR] from howto@LISTSERV.NTSECURITY.NET
11	HappyHacker.org	http://www.happyhacker.org/gtmhh/crackn t.shtml
12	Microsoft Resource Kit	http://www.microsoft.com/TechNet/subscription/masterlist/na/cd6.asp
13	John Albright	http://www.sans.org/y2k/practical/John_Albright.doc
14	Rhino9	http://packetstorm.securify.com/groups/rhino9/
15	Glitch	http://security.ellicit.org/