GIAC
CERTIFICATIONS

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
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Practical Assignment for SANS DC
Nathan J. Martz
Martz_sigala@hotmail.com or Nathan.martz@xacta.com

One of the most widely publicized Microsoft security vulnerability is that of shares. While Microsoft may have made their products easier to use, they have also made the out of the box configuration of their products wide open to exploitation. I have written this paper in order that I may better understand the technologies involved that allow Microsoft's products to be so easily exploited, and also to explain how this knowledge along with several easily available tools can be used to exploit Microsoft operating systems.

Any system running Microsoft networking may be vulnerable. Recent NT Service Packs limit this vulnerability if installed properly, but people using Windows 9.x are still vulnerable if they have enabled sharing.

NetBIOS and NetBEUI

NetBIOS was originally developed for IBM in the 1980s, and became widely used as Microsoft Windows for Workgroups and LAN Manager became more popular. IBM had it developed for its token ring products. Technically, NetBIOS is a session layer protocol, although it doesn't fully comply with the ISO OSI model. NetBIOS does not use an actual address for locating resources, but uses the NetBIOS name of the resource instead. Since it actually a session layer protocol, NetBEUI (NetBIOS Extended User Interface) is used for transport. NetBIOS over NetBEUI relies on broadcasting and while it is a fairly fast and small, it can eat up a lot of bandwidth especially as more workstations are added. The biggest drawback is that it is not routable.

On LANs using NetBIOS, each computer must have a unique name of 16 alphanumeric characters or less. (Microsoft's implementation allows for up to 15 characters with the 16th used as a NetBIOS suffix that specifies the function of the device or service.) These NetBIOS names identify network resources once they have registered their names on the network. A client advertises its name once it becomes active. If it is able to successfully advertise itself without another client claiming the same name, the registration is successful. Group names do not have to be unique - many unique names can together belong to a Group.

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

All processes that have the same Group name belong to the same Group.

(Neon Surge of Rhino9 has written a very good explanation of how NetBIOS and NetBEUI work (available by searching http://packetstorm.securify.com/ for "Neon Surge".) He points out that, "Port 137 is NetBIOS name UDP. Port 138 is NetBIOS datagram UDP. Port 139 is NetBIOS session TCP.")

Microsoft's answer to the problem of NetBIOS not being routable was support NetBIOS over TCP/IP. NetBIOS has to resolve the NetBIOS name into an IP address using a NetBIOS to TCP/UP interface before normal TCP/IP process can take place. There are several ways to do this. One way to do it is to have the interface broadcast the NetBIOS names to the TCP/IP network and wait for the response. This would be unworkable in a large network. Another way of doing it is to use an LMHOSTS file to associate NetBIOS names to an IP address. This has been a very popular way to solve the problem, but can be difficult to manage.

Microsoft's newer TCP/IP stacks allow for using the DNS service to resolve NetBIOS names. In order for this to work, the NetBIOS name must be the same as the DNS hostname. None of the three methods work with dynamically assigned IP addresses. Microsoft created the WINS service to help solve this problem. While this helps to resolve NetBIOS names, WINS still needs to be implemented with Microsoft's version of DNS in order to effectively resolve NetBIOS names to IP addresses. All of this sounds deceptively simple. I once worked at a large DOD facility where the network people planning the WINS implementation did not talk much with the people running the DNS servers. As planned migration to a different network operating system and different e-mail system began, the whole organization suffered through weeks of intermittent connectivity problems as the NT integrators did one thing while other network teams that controlled the DNS servers were involved with switching the backbone to ATM did another.

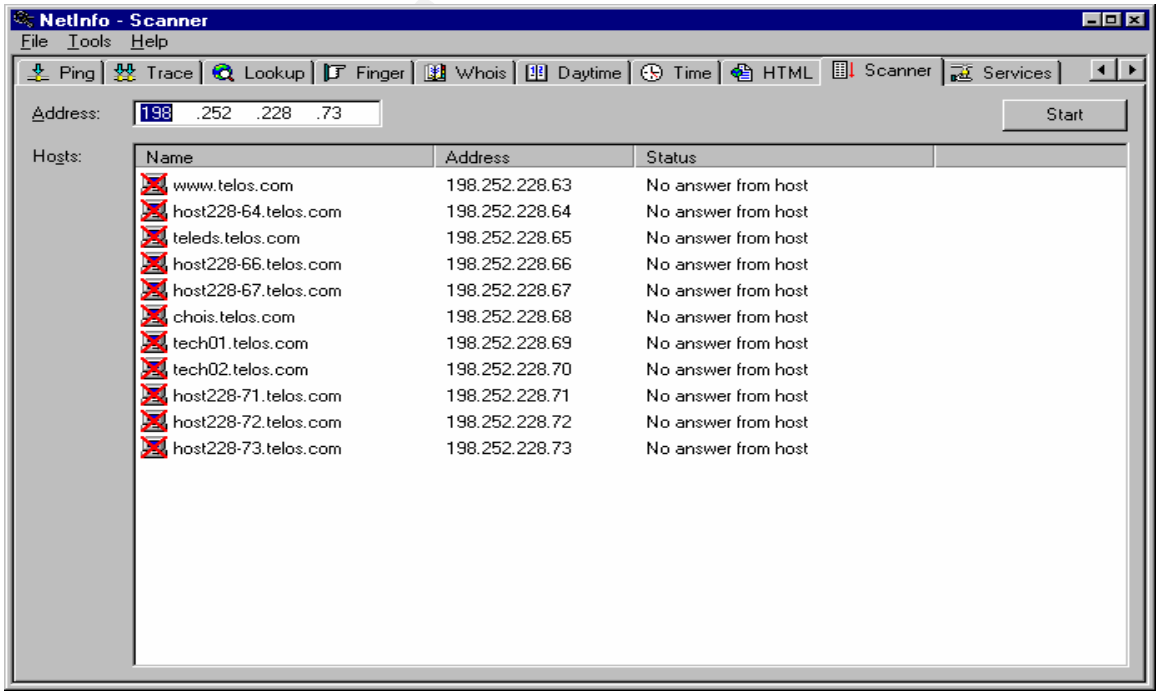
NetBIOS over NetBEUI is installed by default when you configure Windows 9.x/NT for networking. NetBEUI is also installed for Microsoft file and printer sharing. Microsoft also keeps these technologies around in order to provide backward compatibility with its old LAN Manager products. (I can understand that a company may want to

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

make a product backward compatible, but I have never actually seen or known anyone that has used LAN Manager in the last three years.)

Server Message Blocks (SMBs)
SMBs can be transported over NetBEUI, or NetBIOS over both IPX or TCP/IP and are used to communicate between Windows 3.X, Windows 9.X and Windows NT clients. SMBs allows for remote access to shared directories and files. Default installation of Microsoft File and Print sharing on Windows 3.x/9.x allow any user to share any directory or file on their computer. A system administrator with a couple of hundred Windows 9.x on his or her network will have a tough time preventing unauthorized file sharing unless each and every work station is locked down. Remote access to user-defined shares and to default operating system hidden shares (in the case of Windows NT) are made through ports 137, 138 and 139.

Attacks
So, given this background, how would an attacker go about trying to exploit a computer with a Microsoft operating system? The first step would be to find the IP and name of one first. There are a lot of different free tools out there, but the one I have occasionally used is called NetInfo, available at PacketStorm (http://packetstorm.securify.com/).



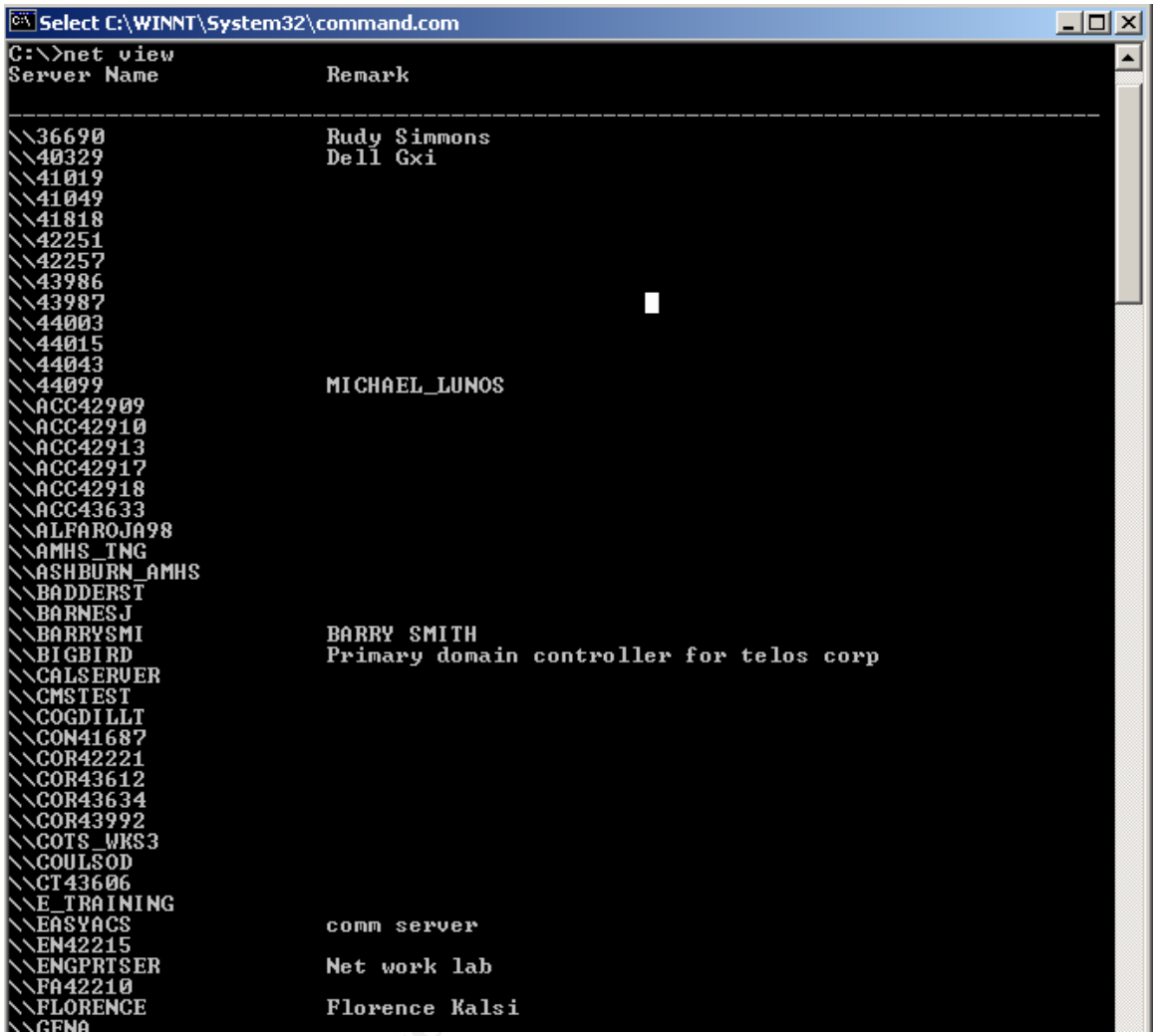
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The screen shot above is from NetInfo. I simply pinged my company's web server (www.telos.com), obtained its IP address, and then let NetInfo run a few seconds as it continued to ping IP numbers one-up from the web server. In this fashion, an attacker can pull out machine names and IP addresses.

Although there are numerous programs available to detect operating systems, such as nmap (www.insecure.org) and queso (www.apostols.org/projectz), often times the unwitting system administrator will make things easy by using a naming scheme such as "NTServer1" or "NT40WINS". These IPs and machines can be added to the attacker's LMHOSTS file in order to access these machines. (I am surprised at the number of computers that are named in this fashion, and some of the clients that I deal with would rather cross the ocean in a bathtub than rename the corporate servers.)

Once the attacker has added some likely suspects to the LMSHOST file, it is to rather simple to run the "net view" command from a DOS prompt to gather additional information. Net view can be run from any Microsoft operating system that has Microsoft networking installed, and will show all the computers running Microsoft networking. The following example comes my company's network, and you can see how much information is available from a simple "net view" command. Keeping in mind that the source of many compromises is internal, system administrators may want to keep comments in the "remarks" section to a minimum. Even with a naming scheme that doesn't give away the farm, some people still will make the mistake of adding something like "Primary Domain Controller" or "Exchange Server" to the remarks section.

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



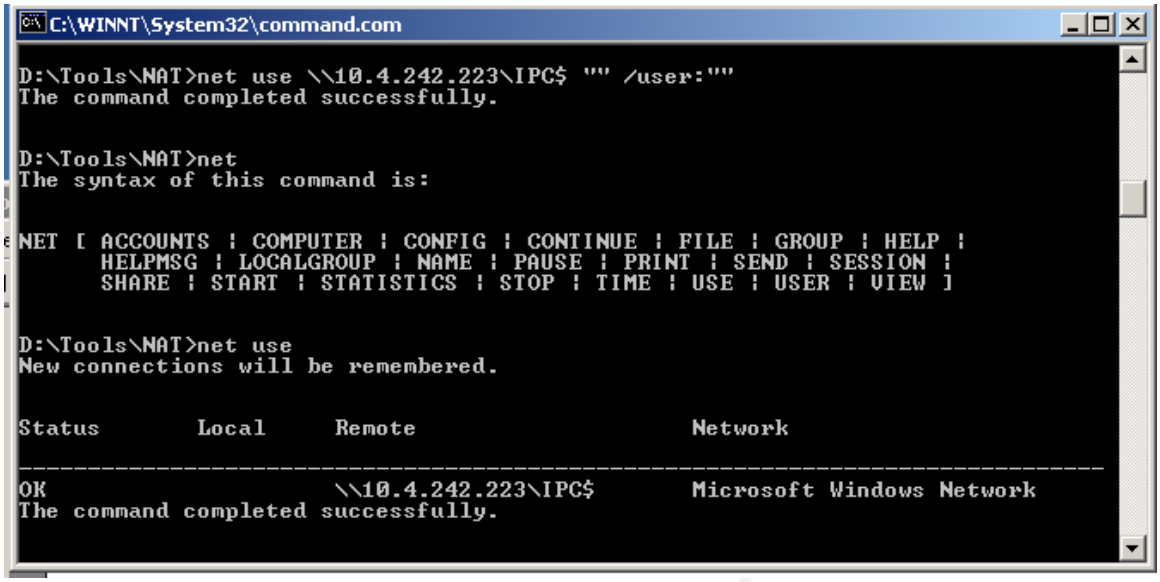
Information Gathering with Null Sessions

The next step is to establish a null session. Null sessions can be established with Windows 9.X/NT and Windows 2000. Again, there are numerous automated programs available to establish null sessions and to pull out as much additional information as possible, but in its most basic form, the null session can be established by using the "net use" command.

Net use \\xxx.xxx.xxx.xxx\IPC$ ""/user:""

It will look something like this:

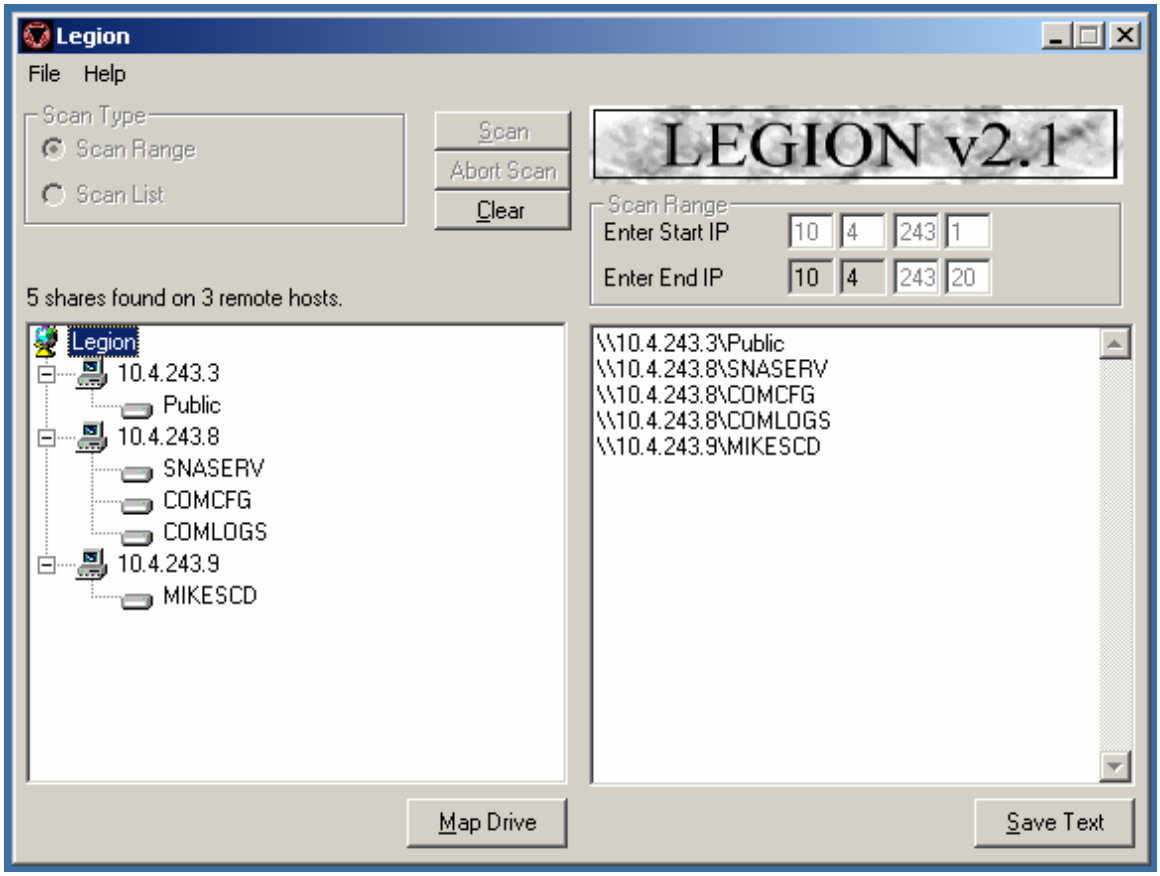
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



There are also automated tools that scan for NetBIOS shares. One popular tool, available at www.securityfocus.com as well as other sites, is Legion 2.1. Once shares are found, Legion will even map the share to a logical drive for you. The registered version also has an additional feature that will attempt to brute force a share password. A screen shot from Legion is shown below, and you can see that I found three machines in an IP range of 20 numbers that had shares. The second machine had three different shares.

© SANS Institute 2000 - 2002, Author

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



Null sessions can also be used to extract other useful information that makes the attacker's task easier. A popular freeware tool called Cerberus Internet Scanner (CIS)(www.cerberus-infosec.co.uk) written by David Litchfield is a very handy tool. It will check an IP address or machine name for shares, services and last, but not least, it will pull the user accounts from the machine and determine if any of the passwords are blank. It is a very nice tool to use against NT servers for a couple of reasons.

If an attacker is going to break into a system, he or she may try using a password cracker. Before going through the trouble of running some sort of brute force password cracker, they may try just guessing some of the passwords if they know the name of a valid user account. The Windows NT default configuration creates two accounts, Guest and Administrator, but many system administrators disable the Guest account and rename the Administrator account. CIS

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

will pull out the other valid user accounts, thus making guessing a lot easier. Here is a typical CIS report.

Cerberus Internet Scanner Results for knuckle_head
by David Litchfield
Cerberus Information Security

NetBIOS Share information

Share Name :NAIEventDB
Share Type :Disk
Comment :EventDatabase Share

Share Name :ADMIN$
Share Type :Default Disk Share
Comment :Remote Admin

Share Name :IPC$
Share Type :Default Pipe Share
Comment :Remote IPC

WARNING - Null session can be established to \\knuckle_head\IPC$

Share Name :C$ Share Type :Default Disk Share Comment :Default share
Share Name :SP5 Share Type :Disk Comment :
Share Name :D$ Share Type :Default Disk Share Comment :Default share
Share Name :E$ Share Type :Default Disk Share Comment :Default share
Share Name :F$ Share Type :Default Disk Share Comment :Default share

Account Information

Account Name :Administrator
The Administrator account is an ADMINISTRATOR, and the password was changed 7 days ago. This account has been used 28 times to logon. The default Administrator account has not been renamed. Consider renaming this account and removing most of its rights. Use a differnet account as the admin account. Comment :Built-in account for administering the computer/domain. ser Comment : Full name :

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

Account Name :Guest
The Guest account is a GUEST, and the password was changed 12 days ago. This account has been used 0 times to logon. The Guest account is DISABLED. Comment :Built-in account for guest access to the computer/domain User Comment : Full name :

Account Name :jason
The jason account is an ADMINISTRATOR, and the password was changed 4 days ago. This account has been used 0 times to logon. Comment : User Comment : Full name :

Account Name :Joe
The Joe account is a normal USER, and the password was changed 0 days ago. This account has been used 0 times to logon. Comment : User Comment : Full name :Joe User

Account Name :user
The user account is a normal USER, and the password was changed 3 days ago. This account has been used 0 times to logon. Comment : User Comment : Full name :

Account Name :User3
The User3 account is a normal USER, and the password was changed 0 days ago. This account has been used 0 times to logon. Comment : User Comment : Full name :User3

WARNING jason's password is blank
WARNING user's password is user

This program is small (108 KB), but really gives you a lot of good information quickly. I ran it against my Windows NT 4.0 Server, "Knuckle_head" and it warned me that null sessions can be established on the default admin share (IPC$). CIS then went on to pull out the user ids and tested for blank passwords. As shown above, CIS was able to discover that the account "Jason" has a blank password and to make matters worse, Jason is a member of the Administrator group. This really demonstrates the danger of creating accounts without passwords, and extra care should be taken to ensure that anyone in the Administrator's group be required to have a strong password. CIS saves the attacker from having to guess at legitimate user accounts and lets them get in to the

© SANS Institute 2000 - 2002 Author retains full rights.

business of breaking into the server. At a minimum, CIS is a nice tool to use for system administrators, or anyone that needs to do a quick check to ensure that no legitimate accounts have been set up with blank passwords. CIS also checks for the following services: ftp, Telnet, SMTP, WINS, DNS, finger, POP3, Portmapper, SLMail Remote Administration in addition to the share and user account information mentioned earlier. Again, it really does a nice job and is very small in size. Litchfield has come out with a newer GUI version, but I still like the old command line version better.

Wrap Up

Besides potentially giving away user information via null sessions, the potential loss of data from unsecured shares, and possible registry edits via null sessions, certain new viruses may also use shares to spread rapidly throughout a network.

The advice put forward on the SANS website is something that every Windows network administrator should follow (www.sans.org/topten.htm). Ensure only required directories are shared and are that these shares are protected with strong passwords. Prevent null sessions by restricting anonymous connections (Microsoft QB155363 at www.microsoft.com/support/search). Block inbound connections to ports 135 - 139 at the router. For stand alone NT machines connected to the Internet, disable NetBIOS bindings from the network interface. Since it is generally known that many security breaches come from the inside of an organization, care should be taken to limit file sharing all together. If possible, a system administrator should lock down any Windows 9.X machines on the network so that user cannot unilaterally enable sharing without the IT department's knowledge. The Windows 95 Policy Editor (poledit.exe) is a great tool for this.

Windows NT workstations are easier to secure, but the default configuration should be checked to make sure that the network is not vulnerable. On a NT-only network, it is possible to disable Lanman authentication by adding "LMCompatabilityLevel" Value with a Value Type "REG_DWORD=4" to the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA

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

This fix has been available since Service Pack 4 and is mentioned in Mclure, Scambray and Kurtz's Hacking Exposed, as well as on the Microsoft web site and other security sites.

The bottom line is that system administrators along with other persons tasked with security need to take security vulnerability warnings and advisories seriously. Although the Microsoft vulnerabilities related to NetBIOS and NetBEUI were made public several years ago, many organizations still have not made an effort to shore up their security infrastructure. Federal agencies have been forced to start doing so through such as Presidential Decision Directive (PDD) 63 and other efforts to secure the nation's critical infrastructure. Users need to be educated and held responsible when they deliberately weaken an organization's security posture. The Federal government is taking steps in the right direction, and the private sector would do well to follow if they haven't don so already.

Sources

Hacking Exposed: Network Security Secrets and Solutions, by Stuart McClure, Joel Scambray and George Kurtz. 1999, Osborne/McGraw-Hill, Berkeley, New York, etc.

NT 4 Server Unleashed!, by Jason Garms. 1996, SAMS Publishing, Indianapolis.

Networking Essentials, by Mark A. Sportack. 1998, SAMS Publishing, Indianapolis.

Understanding NetBIOS, by Neon Surge. Paper is currently posted at www.packetstorm.securify.com.

Understanding SMBs and Components, by Neon Surge, also posted at www.packetstorm.securify.com.

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