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
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

GIAC Level One Security Essentials Practical Assignment
NetBIOS and File Sharing Security in Windows
Mark Wade

Version 1.2f – August 13, 2001

Understanding NetBIOS 2
Figure One: NetBIOS Over IP 2
NetBIOS Names 3
Am I at Risk? 4
Scope ID 6
Fact VS Fiction 6
Conclusion 7
References and Works Cited 8

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

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

Overview

NetBIOS (Network Basic Input/Output System) is a program that allows different computers on the same local area network to communicate. NetBIOS frees these computers' applications from having to know the intricacies of the network and provides a means off creating a session between the two PCs. NetBIOS is not a protocol. This is a common mistake since NetBIOS does have base rules. For example, NetBIOS contains standard rules when involved in the naming of computers, workgroups, domains, users and other services utilizing NetBIOS.

The NetBIOS interface was first developed by Sytec Inc. (currently Hughes LAN Systems) for the International Business Machines Corporation (IBM) in 1983. It ran on a primitive IBM LAN that supported a maximum of 72 devices and utilized proprietary Sytec protocols to transport information. According to Microsoft, who has a long working history with IBM, NetBIOS was not originally designed to grow to support today's massively size networks. Later revisions in the mid-80s made NetBIOS the de facto when configuring networking system components and programs.

This paper focuses on NetBIOS when used over TCP/IP and the security questions about file sharing using the Operating Systems Windows 95, 98, and ME. When sharing file(s) and/or printer(s) on a LAN, and/or if one has enabled Microsoft Networking, then what is called shares may be exposed to the Internet. Shares are file and printer resources that have been enabled for sharing. A lot of times these shares are exposed without the owner of the machine realizing. They might lack a proper password (a proper password being a password meeting the criteria set by the level of security one desires on his network or machine) or possibly no password. If somebody gains access to these shares via the Internet, then they can access your computer and destroy and/or manipulate material located there within. Microsoft has posted a security bulletin and patch for this vulnerability at **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-072.asp** and the bugtraq has recorded the vulnerability as ID number **1780**.

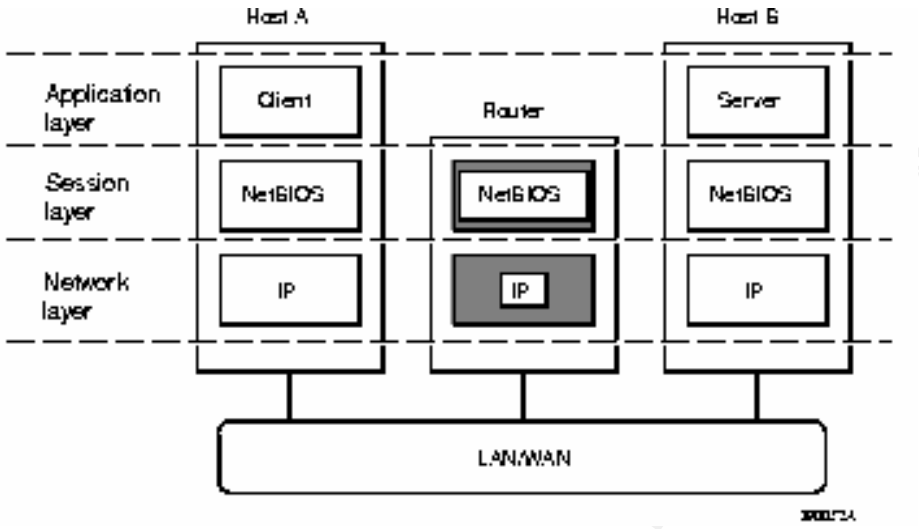
Understanding NetBIOS

A NetBIOS request is provided in the form of a Network Control Block (NCB). A NCB is a 64 bytes data structure and is required in every single command given by NetBIOS. NCBs specify the message location, name of destination, pointers to buffers, and various command codes. The NCB must be unaltered until the command is completed, so it cannot be used for other commands while the command is still processing. However, once a command has completed, the NCB can be altered, and reused for another command.

NetBIOS provides session and transport services. As seen in Figure One, NetBIOS is located in the OSI's (Open Systems Interconnection) session layer and has a hand in all network communication.

Figure One: NetBIOS Over IP (Anonymous)

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



However, it does not provide a standard frame or data format for transmission. A standard frame format is provided by a Transport protocol. The Transmission Control Protocol (TCP) will be focused on in this paper. One can also use NetBIOS Extended User Interface (Netbeui) instead of TCP. It is not necessary to expand on Netbeui in this paper, for more information on Netbeui, go to **http://hdallen.home.mindspring.com/netb.htm**.

NetBIOS provides the choice to choose between two communication modes, datagram or session. Datagram mode sends each message independently. This is referred to a connectionless communication. In this form of communication, all stations on the network are continually checking for datagrams. When a station finds a datagram addressed to its name, it receives the message. There is no form of acknowledgement that this machine received the message so you cannot guarantee safe passage of any messages you send. When utilizing datagrams you can either send messages to a specific workstation or broadcast to the entire network.

Session mode is connection oriented and lets two names (not two machines) establish a connection. A session connection only looks at names, meaning you could have a connection setup between two devices on the same machine. The session method allows larger messages to be handled, and provides error detection and recovery. If a message is not received successfully, an error is returned to the application.

NetBIOS Names

The purpose of NetBIOS names is to identify resources on a network. Applications use these names to start and end sessions. Most of the time these sessions will be between two machines but one can configure a single machine with multiple applications, each of which could have a unique NetBIOS name**.** Each station that supports an application also has a NetBIOS station name that is user defined. If it isn't user defined then NetBIOS derives the name by internal means.

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

16 aplhanumeric characters make up NetBIOS. Microsoft, however, limits these names to 15 characters and uses the 16th character as a NetBIOS suffix. The purpose of the NetBIOS suffix is to indentify the functionality installed or the registered device or service**.** The NetBIOS name space is flat, not hierarchical like DNS. For the NetBIOS name to be registered, the combination of characters must be unique within network. To gain a deeper understanding of NetBIOS, lets look at how it registers itself. When the client machine boots up, it broadcasts its NetBIOS information to every machine on the network. If another client on the network already has the name, it responds with a broadcast stating that it already has registered the NetBIOS name. At this point the new machine on the network stops trying to register. If not other machine on the network responds, the client finishes the registration process.

There are two types of names in a NetBIOS environment, unique and group. A unique name must not match any other name on the network. A group name does not have to be unique and all processes that have a given group name belong to the group. Each NetBIOS node maintains a table of all names currently owned by that node**.**

NetBIOS is what makes file sharing possible. When located within a workgroup or domain, you use NetBIOS to establish a connection when talking to shares located on other machines in your network. Some consider NetBIOS to be a dangerous convenience in the Windows Operating System. This paper discusses file sharing security but there are also many other risks associated with NetBIOS such as intelligence gathering using nbtstat.exe, allowing unwanted connections via command lines, and also allowing machines to be able to gain certain privileges you might not want them to have. These security holes can be plugged with the appropriate practices. This paper concentrates on enforcing file-sharing security but the above should also be considered when looking to see if your machine is at risk.

Am I at Risk?

There are several factors to take into consideration when figuring out whether or not you are at risk. First, check to see if file and printer sharing for Microsoft Networks is installed as a network component on your machine. Just double click the network icon in the control panel, select the configuration tab and click on File & Print Sharing. If the boxes on this screen are checked, then file sharing is enabled.

Also, check to see if file and printer sharing for Microsoft Networks is bound to TCP/IP on an adapter used for the Internet. Go back to the network icon located in the control panel and double click it. Highlight the TCP/IP protocol that is pointing to your Network Interface Card. Click on Properties and then on the Bindings tab. If Client for Microsoft Networks and File and printer sharing for Microsoft Networks are installed then your adapter has file sharing enabled.

If you want to disable the above file sharing, follow the following directions:

1. On the desktop, double-click on **My Computer**.
2. Double-click on **Control Panel**.
3. Double-click on **Network**.
4. From the Configuration tab, click on the **File & Print Sharing** button.

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

5. Turn off file sharing and print sharing by clicking each box to remove the check marks.
6. Click on the **OK** button.
7. Select the TCP/IP protocol that is pointing to your Ethernet card or USB cable modem.
8. Click on the **Properties** button and click on the **Bindings** tab.
9. Click to uncheck the boxes next to "Client for Microsoft Networks" and "File and printer sharing for Microsoft Networks". NOTE: If there is more than one listing of TCP/IP, steps 7-9 should be repeated.

Click the **OK** button twice and restart your computer.

Also check to see if Share(s) have actually been configured for file(s) and printer(s). Check to see if options for files and printers are checked under File and Print Sharing. A big area of vulnerability involved with file sharing is the use of easily cracked passwords. A NetBIOS password that provides good security is one that is at least 8 characters long, a mixture of alphabetic letters and numeric digits, not a recognizable word or phrase, not something associated with you, different from your other previous passwords, and still something you can remember.

There is no risk if you do not have files shared. Some administrators don't want their users to be able to create file shares. To uninstall NetBEUI from a machine follow these directions as taken from **http://cable-dsl.home.att.net/index.htm#CaseB**:

1. Open Control Panel - **Network**.
2. If **NetBEUI** is **not** installed in the **Configuration** list:
    a. Click **Add**.
    b. Select **Protocol**.
    c. Click **Add**.
    d. Select **Microsoft** as the **Manufacturer**, and then **NetBEUI** as the **Network Protocol**.
    e. Click **OK** twice to close the Network windows.
    f. **Restart** your computer if prompted to do so, and then reopen **Network**.
3. If you **do** want to share files or printers on a local area network, enable **File and Print Sharing**:
    a. Click on **File and Print Sharing**.
    b. **Check** (enable) the desired options for files and/or printer(s).
    c. Click **OK** twice to close the **Network** windows.
4. **Restart** your computer if prompted to do so, and then reopen **Network**.
5. Unless you normally logon to Microsoft Networks (*e.g.,* Windows NT/2000/XP servers), **Primary Network Logon** should be set to **Windows Logon**.
6. **UN**-bind **TCP/IP** from Microsoft Networking for ***all* instances of TCP/IP that point to a network adapter** (including **Dial-Up Adapter**):
    a. Open **TCP/IP Properties** by double-clicking on the **TCP/IP** entry in the **Configuration** list that points to a network adapter. If you get the long message starting "You have asked to change TCP/IP properties for a dial-up adapter...", click **OK**.
    b. Click on the **Bindings** tab.

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

c. **UN**-check the option **File and Printer Sharing for Microsoft Networks**
d. **UN**-check the option **Client for Microsoft Networks**.
e. Click **OK** twice to close the **Network** windows. If you get the message "You have not selected any drivers to bind with. Would you like to select one now?", click **No**.

7. **Restart** your computer if prompted to do so, and then reopen **Network**.
8. Make sure that **NetBIOS** is **not** enabled on ***all* instances of TCP/IP that point to a network adapter** (including **Dial-Up Adapter**):
   a. Open **TCP/IP Properties** by double-clicking on the **TCP/IP** entry in the **Configuration** list that points to a network adapter. If you get the long message starting "You have asked to change TCP/IP properties for a dial-up adapter...", click **OK**.
   b. Click on the **NetBIOS** tab.
   c. **UN**-check (if checked) the option **I want to enable NetBIOS over TCP/IP**.
   d. Click **OK** twice to close the **Network** windows.
9. **Restart** your computer if prompted to do so.
10. Close Control Panel.

Scope ID

A NetBIOS Scope ID provides an extended naming service for the NetBIOS over TCP/IP (known as NBT) module**.** The primary purpose of a NetBIOS scope ID is to isolate NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID. The NetBIOS scope ID is a character string that is appended to the NetBIOS name**.** The NetBIOS scope ID on two hosts must match, or the two hosts will not be able to communicate**.** It also allows computers to use the same computer name if they have different scope IDs. The Scope ID becomes a part of the NetBIOS name, making the name unique**.** A strong Scope ID is a good way to protect against outside intrusion. This is because computers running NetBIOS over TCP/IP with Scope ID are invisible to other computers that do not have the same Scope ID. By default, the Scope ID is not set so normally such computers utilizing NetBIOS of TCP/IP is visible to everyone. By initiating the Scope ID, one basically locks out outside users trying to connect to your NetBIOS session. For Windows 95 and 98, WINS must be enabled on the machine.

Fact VS Fiction

Before jumping the gun and spending unnecessary time in locking down your system, here are some things to keep in mind about file sharing. Your machine is not automatically threatened because File and Printer Sharing is enabled. It is only vulnerable if you have created unsafe file shares, which the above section can help you identify. Using strong passwords following the above rule set helps limit the chance of somebody cracking your share. Also, keep in mind removing Client for Microsoft Networks does not protect ones machine. The larger risk comes from the server component (i.e. File and Printer Sharing for Microsoft Networks) not the client component (i.e. Client for Microsoft Networks). If you remove Client for Microsoft Networks, you remove your ability to save passwords, so think about which one you

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

remove before you press that remove button. Finally, keep in mind that if you had unsafe file sharing enabled on your computer and you fixed the problem, you still might have been compromised. Run a virus checker to see if anybody has installed a virus or Trojan on your machine.

Conclusion

So file sharing in Windows 95, 98, and ME can carry a lot of risks, but it also brings a lot of rewards. Utilizing this document can help you secure file sharing. You also have a deeper understanding on how file sharing occurs through NetBIOS and windows networking. NetBIOS and file sharing have changed drastically since the late 80s and networking technology is heading to new places. But these operating systems will always be around and newer interfaces will be based on the old ones. Keeping up with the past will prepare you for the future.

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

References and Works Cited

Allen, Doug. Doug's Networking Pages. 1/6/01.
URL: **http://hdallen.home.mindspring.com/netb.htm**

Anonymous. NETBIOS Overview. 9/27/97
URL:
http://support.baynetworks.com/library/tpubs/html/router/soft1200/117358AA/B_39.HTM

Beal, Melissa. Definition of NetBIOS. 7/27/01.
URL: **http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci212633,00.html**

Bugtraq. Microsft Windows 9x/Me Share Level Password Byp. 10/10/00.
URL: **http://www.securityfocus.com/bid/1780**

Lirik. NT NetBIOS Hacking. 3/31/99.
URL: **http://www.seclabs.org/netbios/netbios.htm**

Microsoft. Security Bulletin MS00-72. 02/16/00.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-072.asp

Microsoft. Using and Troubleshooting the TCP/IP Scope ID. 8/8/01.
URL: **http://support.microsoft.com/default.aspx?scid=kb;EN-US;q138449**

Navas, John. Cable Modem / DSL Tuning Guide. 9/26/99.
URL: **http://cable-dsl.home.att.net/index.htm#CaseB**

Navas, John. The Navas Group Home Page. 12/7/01.
URL: **http://cable-dsl.home.att.net/netbios.htm#Risk**

NeonSurge. Understanding NetBIOS. 01/29/01.
URL: **http://www.ladysharrow.ndirect.co.uk/NT/understanding_netbios.htm**

Winston, Gavin. NetBIOS Specification. 1999.
URL: **http://members.tripod.com/~Gavin_Winston/NETBIOS.HTM**

© SANS Institute 2000 - 2002 Author retains full rights.