Global Information Assurance Certification Paper

How safe is file sharing?
Microsoft, the Freedom to Share
Loyal A. Moses

File sharing in today's network environments is a necessity that could cost you more than it is worth. The ability to spread vast amounts of information across small and large corporate networks while providing convenience, ease of management and accountability is an asset we take for granted. Convenience is not without cost, cost to individuals, to families, corporations, governments and even countries. This price is obviously something that can be averted; the dangers left by convenience can easily be managed by the understanding and implementation of practical security procedures and precautions. Security is a state of mind, it is the methods and processes that one follows that make a situation secure. Picture a bank vault, and ask yourself if this vault is secure. Is the vault secure only because it is a vault and it was built intentionally to be strong? Or is it secure because there is an armed guard in the bank, or because there is an alarm that is triggered by un-authorized access? Security is neither in the device nor the individual it is the process that binds all of this together into one fail-safe mechanism. Our networks are filled with numerous security related issues, from an email containing a customer list found in the in-box of a competitor to strategic corporate espionage. Trust in data sharing is possibly one of our most exploitable habits. Creating a file folder share on your home-business computer so a friend could take a look at vacation pictures. This sounding harmless enough is the perfect scenario for the thousands of computer crimes committed daily around the world. Now visualize an employee at work following the same practice, they shared the folder so someone in another department could access the new game they downloaded from tucows.com. The folder share meant only to make pictures of your family or the new game available to friends has now given an attacker a potential entry point into your computer system. How is this possible?

The operating systems of yesterday were based primarily on convenience and security as an afterthought. One of the most dangerous conveniences in networked computers today is NetBIOS. NetBIOS (**N**etwork **B**asic **I**nput/**O**utput **S**ystem) provides applications with a programming interface for sharing services and information across a variety of lower-layer network protocols, including IP. NetBIOS is primarily used in the sharing of folders/directories and printers. These simple concepts can spell disaster in the hands of an experienced attacker.

This document will demonstrate the security aspect of NetBIOS as well as some of the tools used in compiling information from a target system and gaining un-authorized access. The following information is intended for educational purposes only; all excessive and unnecessary information has been removed.

nbtstat.exe – This diagnostic command displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP). This command is only available if the TCP/IP protocol has been installed. If TCP/IP ports 137,138 and 139 are available on the target machine, then the command 'nbtstat.exe –A *ipaddress'* will display the active user, services running, nt domain name, machine name and the ethernet hardware address. This can give an attacker the information needed to begin a potential hack on the target system. Once it is known that the protocol exists and is installed correctly then it is just a matter of exploitation. For instance, the machine name is valuable for attacking the target using multiple vulnerabilities (e.g., msadc.pl – an exploit written by Rain Forest Puppy to demonstrate the insecurity of msadcs.dll). The machine name is also a valuable asset for this example.

The NULL IPC$ Connection - IPC stands for Interprocess Communication, this is the way programs (such as the browser service) communicate with each other. IPC$ is a share created on each Windows NT computer through which interprocess communication can take place. A NULL session (as apposed to a validated session) is used because browsing shares via NetBIOS can occur without a valid trust relationship. The original purpose of a NULL session is to allow unauthenticated hosts to obtain browse lists from NT servers and participate in MS networking. The problem occurs where a NULL session becomes part of the everyone group and now has access to resources in which they were not authenticated. Originally, 'everyone' did not mean 'anyone'. A logon was still needed for you to participate in the everyone group. However, NULL sessions are the once case 'everyone' could mean 'anyone' and you can then gain access to unauthorized information. This is the reason behind the **New** 'Authenticated Users' group as this does not include NULL sessions and so can never mean 'anyone'. To exploit the NULL session vulnerability the following command can be issued once the target systems name and ip

have been entered into your lmhosts file.

net use \\targetmachinename\ipc$ "" /user:""

If succesfull you have just created a connection with the target system via a NULL session, and can now view the browse list for shares and data. It is also possible if the target has not been secured to access the targets registry as well as the user manager and other NT features remotely.

An AT&T website quotes *"… hysteria related to NetBIOS over TCP/IP is unwarranted. Some Internet sites are making matters worse spreading bad advice …*"

Thought and preparation are key points in the creation of a secure environment. An unmanaged NetBIOS could lead to disaster. Here are a few examples and precautions one can take:

- Remove NetBIOS from all production systems
- Remove the 'everyone' group from all data of importance
- Utilize IP Filtering on the OS to block ports or install a secure firewall
- Remove the administrative shares on all production systems
- In the case that NetBIOS shares are needed, the use of strong passwords is recommended

Clearly NetBIOS has its advantages and its disadvantages. From the two basic examples provided in this document it is suggested that the protocol be handled with extreme caution. NetBIOS is a convenience to our networked world as well as a breeding ground for new and potentially very harmful exploits. Firewalls and intrusion detection systems have come a long way in the last decade and are now able to prevent nearly all of these attacks. In conclusion, something foreseen to be simple and basic, is the one thing that will end up plaguing networks in the end. Everything no matter the size or functionality should be audited with caution and scrutiny to determine the level of danger it will bring with its convenience.

'Now… lets all get along play fairly and share nicely.'

Microsoft "Nbtstat" Nbtstat.
URL: http://windowsupdate.microsoft.com/nt5help/Server /en/nbtstat.htm (10 April 2000).

The Navas Group "File and Printer Sharing (NetBIOS) Fact and Fiction" File and Printer Sharing (NetBIOS) Fact and Fiction. 5 April 2000.
URL: http://navasgrp.home.att.net/tech/netbios.htm (10 April 2000).

Webopedia "NetBIOS" NetBIOS.
URL: http://webopedia.internet.com/TERM/N/NetBIOS.html (10 April 2000).