# Global Information Assurance Certification Paper

Glen Sharlun
Incident Handling and Hacker Exploits
Washington DC, July 2000

# INAPPROPRIATE INFORMATION SHARING VIA WINDOWS NT PORTS 135->139 AND USING LEGION TO EXPLOIT IT

## Exploit Details:

Name: Legion v2.1 (shareware) By Rhino9
**http://packetstorm.securify.com/groups/rhino9/**

Variants: SMBscanner, Cerberus Information Security, NBTdump, Cain 2.0, GNIT NT Vulnerability Scanner, Share Finder, Cain & Abel (Just the tip of the iceberg of tools that exploit MS share "feature".)

Operating System: All Microsoft operating systems. Unix and Macintosh have their variants of this vulnerability. (NFS exports and Web sharing or AppleShare/IP, respectively)

Protocols/Services: NetBIOS (Network Basic Input/Output System)

Brief Description: Legion automates the locating and connecting of Windows-based shares. The software depends on the user NOT protecting their shares with passwords BEFORE connecting to the Internet. The software also has a brute-force password cracking plug-in that can be used to find passwords for shares that are protected (Commercial version).

## Protocol Description:

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (Error, invalid term). It was created by IBM for its early PC Network, was adopted by Microsoft, and has since become a de facto industry standard. NetBIOS is used in Ethernet, token ring, and Windows NT networks. It does not in itself support a routing mechanism so applications communicating on a wide area network (WAN) must use another "transport mechanism" (such as TCP) rather than or in addition to NetBIOS.

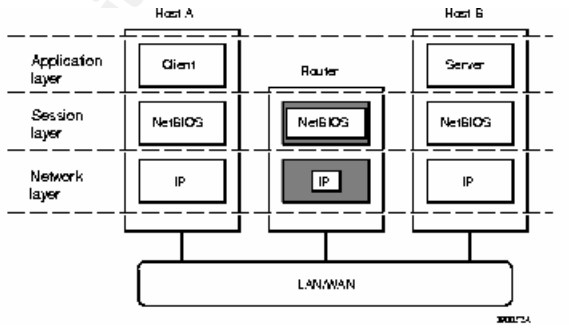
NetBIOS frees the application from having to understand the details of the network, including error

recovery (in session mode). A NetBIOS request is provided in the form of a Network Control Block (NCB) which, among other things, specifies a message location and the name of a destination.

It offers network applications a set of "hooks" to carry out inter-application communication and data transfer. In a basic sense, NetBIOS allows applications to talk to the network. Its intention is to isolate application programs from and type of hardward dependancies. It also spares software developers the task of developing network error recovery and low level message addressing or routing. The use of the NetBIOS interface does a lot of this work for them.

NetBIOS provides the session and transport services described in the Open Systems Interconnection (OSI) model. However, it does not provide a standard frame or data format for transmission. A standard frame format is provided in the NetBIOS Extended User Interface (NetBUI).

NetBIOS provides two communication modes: session or datagram. Session mode lets two computers establish a connection for a "conversation," allows larger messages to be handled, and provides error detection and recovery. Datagram mode is "connectionless" (each message is sent independently), messages must be smaller, and the application is responsible for error detection and recovery. Datagram mode also supports the broadcast of a message to every computer on the LAN.




NetBIOS over IP

**Description of variants:**

There are not necessarily direct relations between the following variants and Rhino9's Legion, but the NetBIOS exploit is used. (Largely based on timelines of

development, Legion (as a concept) is likely in the bloodline of most of the variants below).

Getsvrinfo 1.0 by AbuseLabs:
A little program coded for Windows NT that obtains the parameters of a remote Windows NT server, parameters include NetBIOS name, NetBIOS domain/workgroup, amount of users currently logged in, and remote operating system version.

GNITvse rc1: GNIT Vulnerability Scanning Engine by glitch of ellicit.org
A vulnerability scanner which scans for the following: NBTStat Scan; Null IPC Session Establishment; Net View Scan; Enumerates all Global Groups; Enumerates all Local Groups; Enumerates all User Accounts;

NB4 by Craig at freenet.de
This is a NBTSTAT scanner, its written in Batch language and scans from xxx.xxx.xxx.1 to xxx.xxx.xxx.255 for NetBIOS hosts

NBName by Sir Dystic at CDC
NBName decodes and displays all NetBIOS name packets it receives on UDP port 137. Using the /DENY * command line option it will respond negatively to all NetBIOS name registration packets it receives. Using the /CONFLICT command line option it will send a name release request for each name that is not already in conflict to machines it receives an adapter status response from. The /FINDALL command line option causes a wildcard name query request to be broadcast at startup and each machine that responds to the name query is sent an adapter status request. The /ASTAT command line option causes an adapter status request to be sent to the specified IP address, which doesn't have to be on your local network. Using /FINDALL /CONFLICT /DENY * will disable your entire local NetBIOS network and prevent machines from rejoining it.

Net Fizz 0.1 by Zorkeres
Net Fizz is a multithreaded net share scanner for Windows NT only. It is fast and has the capability of showing hidden shares.

NetBIOS Auditing Tool (NT) 1.0 by Secure Networks Inc.
The intention of this package is to perform various security checks on remote servers running NetBIOS file

sharing services. In the grand scheme of NetBIOS and Windows NT security, NAT is fairly small. It is, without question a step in the right direction but it like any other software, needs further development.

NTInfoScan 4.2.2 by David Litchfield
NTInfoScan is a security scanner designed specifically for the Windows NT 4.0 operating system. It's simple to use - you run it from a command line - and when the scan is finished it produces an HTML based report of security issues found with hyper-text links to vendor patches and further information. NTInfoScan is currently at version 4.2.2. It tests a number of services such as ftp, telnet, web service, for security problems. Added to this NTInfoScan will check NetBIOS share security and User account security.

Winfingerprint 2.2.6 by Kriby Kuehl at technotronic.com
Advanced remote windows OS detection. Current Features: Determine OS using SMB Queries, PDC (Primary Domain Controller), BDC (Backup Domain Controller), NT MEMBER SERVER, NT WORKSTATION, SQLSERVER, NOVELL NETWARE SERVER, WINDOWS FOR WORKGROUPS, WINDOWS 9X, Enumerate Servers, Enumerate Shares including Administrative ($), Enumerate Global Groups, Enumerate Users, Displays Active Services, Ability to Scan Network Neighborhood, Ability to establish NULL IPC$ session with host, Ability to Query Registry (currently determines Service Pack Level & Applied Hotfixes. Changes: Enumerates Transports, Retrieves Date & Time.

Winfo 1.4 by Arne Vidstrom
Winfo uses null sessions to remotely retrieve a list of user accounts, workstation trust accounts, interdomain trust accounts, server trust accounts, and shares, from Windows NT. It also identifies the built-in Administrator and Guest accounts, even if their names have been changed. Of course winfo will show all hidden shares. One of the features is the -n switch, which activates null session mode. Without this switch, winfo can be used to retrieve the information mentioned, but using an already established connection to the other computer. For example, if null sessions have been restricted, but you have a valid user account, you can connect first and then use winfo to retrieve the information you need.

**How the exploit works:**

Windows 95/98 makes it easy for desktop users to share their files and printers with other users. In the past, this was useful only in office settings, where PC's were routinely networked. However, with computers and network equipment getting cheaper, more and more people are setting up small local area networks (LAN's) at home. Once networked, Windows 9x makes it very easy for users to create shared folders and allow others to access their files.

As useful as shared resources might be, opening up data for others creates a potential security issue. While sharing computers among household members may not be much of a risk, the proliferation of Internet access from the home has led many to unknowingly expose their hard drive to outsiders.

The main reason why so many people inadvertently open themselves up to intrusion is that there is almost no documentation for the average user that talks about their exposure on the Internet. There are no warning signs that someone is intruding, and no indication that the user is actually offering shared folders to the outside. Microsoft's Network Neighborhood tool misleads users into believing that they are isolated, simply because they cannot see outside computers while on the Internet. While others cannot see the user's PC in their Network Neighborhood window either, that does not mean that someone cannot find the user's shared folders.

There are only two obstacles that deter the potential intruder. First, the intruder has to locate a vulnerable Windows 9x machine. Second, the intruder has to guess the password.

Rhino9's Legion, which polls wide ranges of IP addresses to see if any computers have available shared folders. The application broadcasts a NetBIOS request to find all computers that have NetBIOS services. The application then searches each earmarked computer for available shares, and displays the results. (I believe that Legion simply issues nbtstat commands to get its results.) Once these shares are known, there is no way to detect or deter brute force password guessing.

**Diagram:**

There is nothing worth diagramming here. The scanner simply sends TCP NetBIOS packets at the hosts in the scanning range and waits for a response.

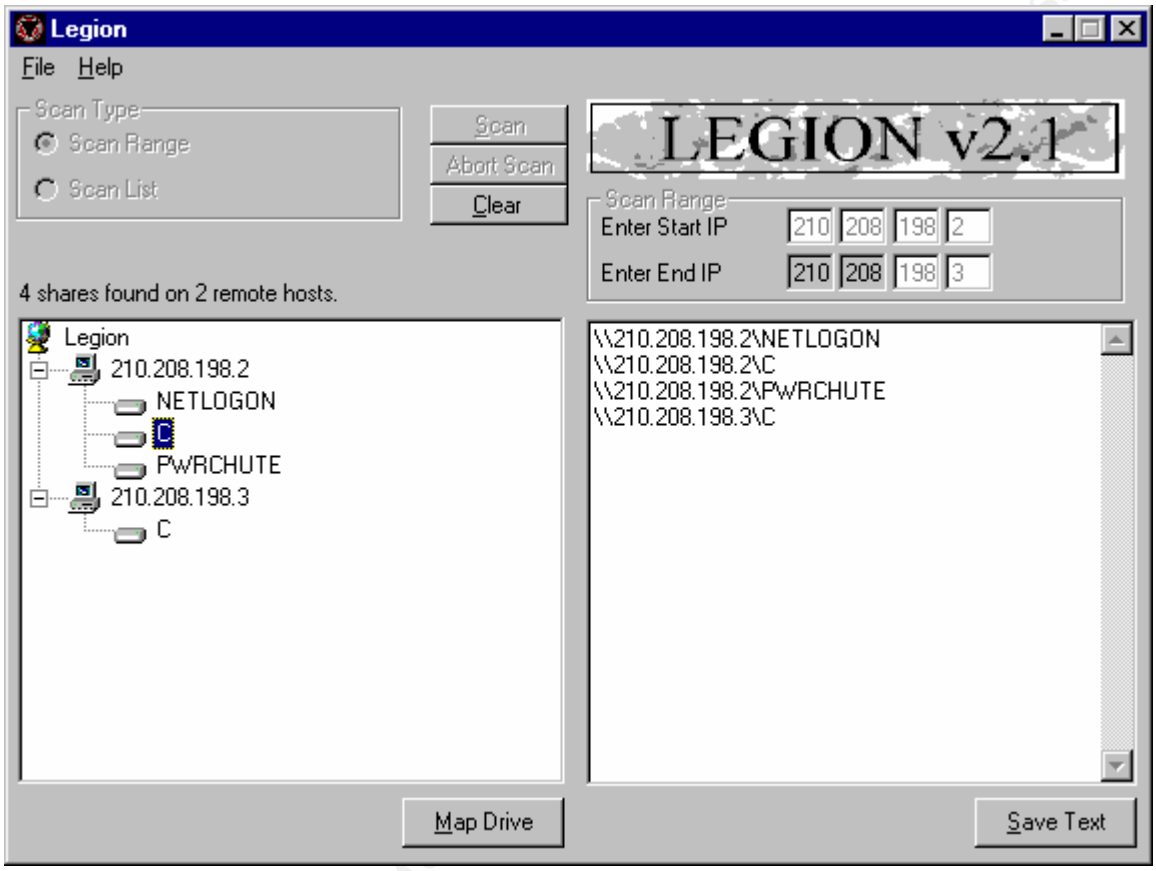
If there is a response, it is almost as simple as it asking "who are you, and what do you have available for me to look at"?

**How to use it?**

Legion can be downloaded from any number of sites (just put its name in any search engine ie. Dogpile, google,…) and will be a zipped file. Install it in normal windows fashion and it should look something like this:


It would be very difficult for it to be any easier. Simply click on the appropriate connection speed, put in the IP range, and hit scan.

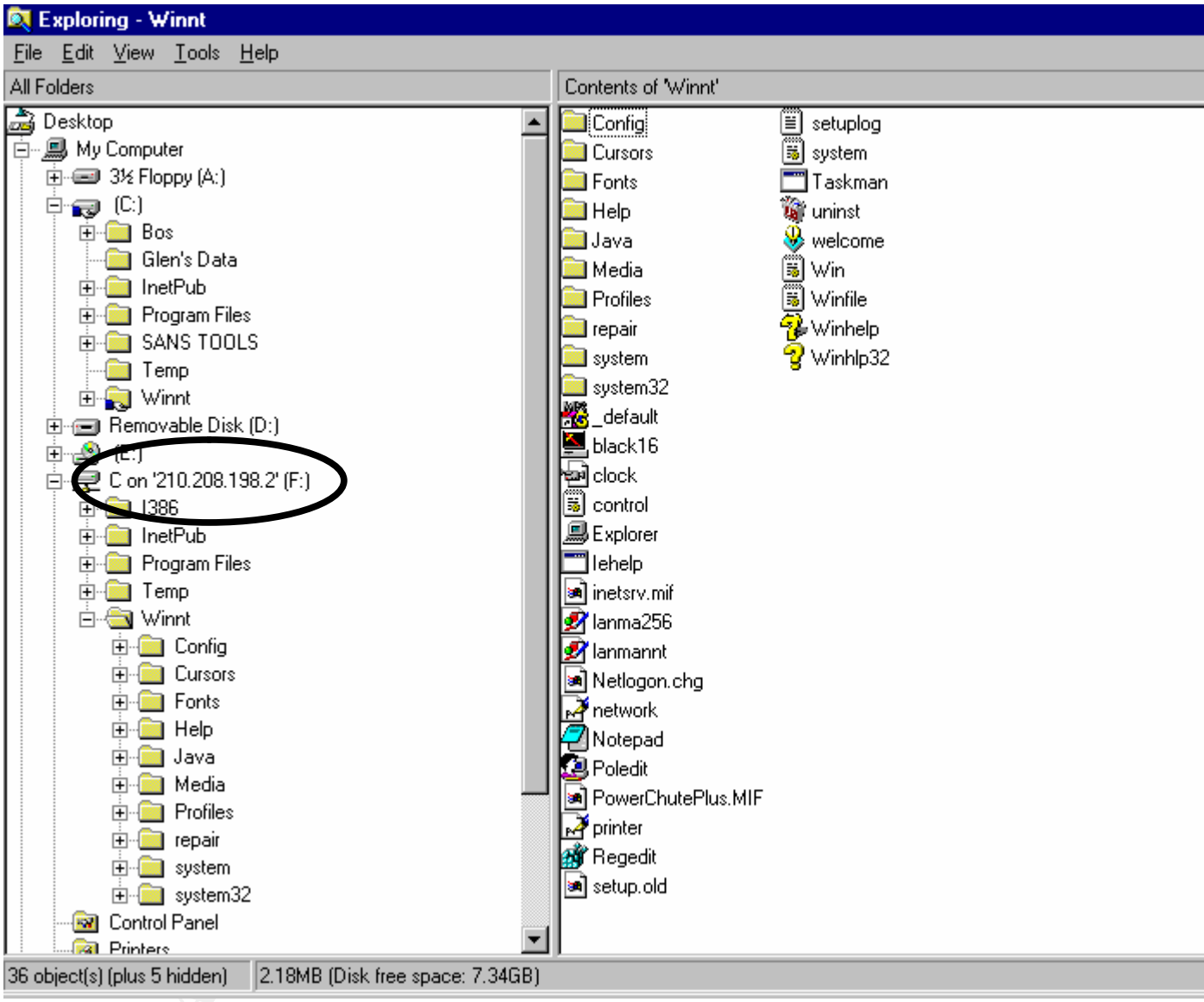
(The quality of the screen capture degrades significantly if the image is made smaller so I have opted for inefficient clarity vice space efficient, "fuzzy-ness".)




This scan of a LABORATORY NETWORK (I know, should use unrouteable IP's, but it is air-gapped and we are always taking it down and re-building it).

This scan only took about 40 seconds and resulted in the identification of 4 shared shares on 2 remote hosts. The "C" drive of course looks the most inviting so we will map it to our network explorer simply by clicking on 'Map Drive'.

If this was the commercial version of Legion, there would be an option to brute force crack any shares that were identified as shared, but password protected. (This is the shareware version.) These shares are not password protected.




Note the circled area above. The victims "C" drive is now mapped to my network explorer and I can read, write, delete files, as I desire. This would definitely be one of the easiest ways to install a Trojan server.

**Signature of the attack:**

This is the packet capture of the scan of the 2 hosts (share.open.2 & .3). Legion.scanner is the scanning machine with Legion. All of the other IP addresses listed are Legion invoking the others systems to speak-up (with the arp requests).

| Time | Source IP | Port | Dest IP | Port | Size | Protocol |
|---|---|---|---|---|---|---|
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.8LEGION.SCANNER | IP-4831 | | SHARES.OPEN.2 | IP-139 | | 64TCP NetBIOS |
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.800:D0:B7:4A:0A:16 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.8SHARES.OPEN.2 | IP-139 | | LEGION.SCANNER | IP-4831 | | 64TCP NetBIOS |
| 21:00.800:50:04:BE:AC:56 | | | 00:D0:B7:4A:0A:16 | | | 64ARP Rsp |
| 21:00.800:50:DA:10:79:AE | | | 00:50:04:BE:AC:56 | | | 64ARP Rsp |
| 21:00.8LEGION.SCANNER | IP-4832 | | SHARES.OPEN.3 | IP-139 | | 64TCP NetBIOS |
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.800:50:DA:10:78:D0 | | | 00:50:04:BE:AC:56 | | | 64ARP Rsp |
| 21:00.8SHARES.OPEN.3 | IP-139 | | LEGION.SCANNER | IP-4832 | | 64TCP NetBIOS |
| 21:00.8LEGION.SCANNER | IP-4831 | | SHARES.OPEN.2 | IP-139 | | 64TCP NB SessMsg |
| 21:00.8LEGION.SCANNER | IP-4833 | | JUST.TALKIN.6 | IP-139 | | 64TCP NetBIOS |
| 21:00.800:D0:B7:4A:0A:16 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.8SHARES.OPEN.3 | IP-139 | | LEGION.SCANNER | IP-4832 | | 64TCP NetBIOS |
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.800:50:DA:10:79:AE | | | 00:D0:B7:4A:0A:16 | | | 64ARP Rsp |
| 21:00.8JUST.TALKIN.6 | IP-139 | | LEGION.SCANNER | IP-4833 | | 64TCP NetBIOS |
| 21:00.800:50:DA:10:79:9D | | | 00:50:04:BE:AC:56 | | | 64ARP Rsp |
| 21:00.8SHARES.OPEN.2 | | | SHARES.OPEN.3 | | | 74ICMP Redir |
| 21:00.8LEGION.SCANNER | IP-4834 | | JUST.TALKIN.5 | IP-139 | | 64TCP NetBIOS |
| 21:00.800:D0:B7:4A:0A:16 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.8JUST.TALKIN.6 | IP-139 | | LEGION.SCANNER | IP-4833 | | 64TCP NetBIOS |
| 21:00.8LEGION.SCANNER | IP-4832 | | SHARES.OPEN.3 | IP-139 | | 64TCP NB SessMsg |
| 21:00.800:50:DA:10:78:D0 | | | 00:D0:B7:4A:0A:16 | | | 64ARP Rsp |
| 21:00.800:50:DA:10:79:9D | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.8JUST.TALKIN.5 | IP-139 | | LEGION.SCANNER | IP-4834 | | 64TCP NB SessMsg |
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.800:50:DA:28:29:AC | | | 00:50:04:BE:AC:56 | | | 46ARP Rsp |
| 21:00.8LEGION.SCANNER | IP-4833 | | JUST.TALKIN.6 | IP-139 | | 64TCP NB SessMsg |
| 21:00.8SHARES.OPEN.2 | | | JUST.TALKIN.6 | | | 74ICMP Redir |
| 21:00.800:D0:B7:4A:0A:16 | | | 00:50:DA:10:79:9D | | | 64ARP Rsp |
| 21:00.8SHARES.OPEN.2 | | | JUST.TALKIN.5 | | | 74ICMP Redir |
| 21:00.8JUST.TALKIN.5 | IP-139 | | LEGION.SCANNER | IP-4834 | | 64TCP NB SessMsg |
| 21:00.8LEGION.SCANNER | IP-4836 | | JUST.TALKIN.7 | IP-139 | | 64TCP NetBIOS |
| 21:00.8JUST.TALKIN.7 | IP-139 | | LEGION.SCANNER | IP-4836 | | 62TCP NetBIOS |
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |
| 21:00.800:50:04:BE:AC:56 | | | Ethernet Broadcast | | | 64ARP Req |

| | | | | |
|---|---|---|---|---|
| 21:00.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:00.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:00.8SHARES.OPEN.2 | | JUST.TALKIN.7 | | 74ICMP Redir |
| 21:00.8JUST.TALKIN.7 | IP-139 | LEGION.SCANNER | IP-4836 | 64TCP NetBIOS |
| 21:00.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:00.8LEGION.SCANNER | IP-4836 | JUST.TALKIN.7 | IP-139 | 64TCP NB SessMsg |
| 21:00.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:00.8LEGION.SCANNER | IP-4844 | JUST.TALKIN.15 | IP-139 | 64TCP NetBIOS |
| 21:00.800:30:C1:8E:DF:98 | | 00:50:04:BE:AC:56 | | 64ARP Rsp |
| 21:00.8LEGION.SCANNER | IP-4841 | JUST.TALKIN.12 | IP-139 | 64TCP NetBIOS |
| 21:00.8JUST.TALKIN.12 | IP-139 | LEGION.SCANNER | IP-4841 | 64TCP NB SessMsg |
| 21:01.3LEGION.SCANNER | IP-4834 | JUST.TALKIN.5 | IP-139 | 64TCP NetBIOS |
| 21:01.3LEGION.SCANNER | IP-4841 | JUST.TALKIN.12 | IP-139 | 64TCP NetBIOS |
| 21:01.3JUST.TALKIN.5 | IP-139 | LEGION.SCANNER | IP-4834 | 64TCP NB SessMsg |
| 21:01.3JUST.TALKIN.12 | IP-139 | LEGION.SCANNER | IP-4841 | 64TCP NB SessMsg |
| 21:01.8LEGION.SCANNER | IP-4834 | JUST.TALKIN.5 | IP-139 | 64TCP NetBIOS |
| 21:01.8LEGION.SCANNER | IP-4841 | JUST.TALKIN.12 | IP-139 | 64TCP NetBIOS |
| 21:01.8JUST.TALKIN.5 | IP-139 | LEGION.SCANNER | IP-4834 | 64TCP NB SessMsg |
| 21:01.8JUST.TALKIN.12 | IP-139 | LEGION.SCANNER | IP-4841 | 64TCP NB SessMsg |
| 21:02.3LEGION.SCANNER | IP-4834 | JUST.TALKIN.5 | IP-139 | 64TCP NetBIOS |
| 21:02.3LEGION.SCANNER | IP-4841 | JUST.TALKIN.12 | IP-139 | 64TCP NetBIOS |
| 21:02.3JUST.TALKIN.5 | IP-139 | LEGION.SCANNER | IP-4834 | 64TCP NB SessMsg |
| 21:02.3JUST.TALKIN.12 | IP-139 | LEGION.SCANNER | IP-4841 | 64TCP NB SessMsg |
| 21:03.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:03.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:03.8LEGION.SCANNER | IP-4844 | JUST.TALKIN.15 | IP-139 | 64TCP NetBIOS |
| 21:03.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:03.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:03.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:03.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:03.800:50:04:BE:AC:56 | | Ethernet Broadcast | | 64ARP Req |
| 21:04.8LEGION.SCANNER | IP-4831 | SHARES.OPEN.2 | IP-139 | 64TCP NB SessMsg |
| 21:04.8LEGION.SCANNER | IP-4832 | SHARES.OPEN.3 | IP-139 | 64TCP NB SessMsg |
| 21:04.8SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-4831 | 64TCP NB SessMsg |
| 21:04.8SHARES.OPEN.3 | IP-139 | LEGION.SCANNER | IP-4832 | 64TCP NB SessMsg |
| 21:04.8LEGION.SCANNER | IP-4833 | JUST.TALKIN.6 | IP-139 | 64TCP NB SessMsg |
| 21:04.8JUST.TALKIN.6 | IP-139 | LEGION.SCANNER | IP-4833 | 64TCP NB SessMsg |
| 21:04.8LEGION.SCANNER | IP-4831 | SHARES.OPEN.2 | IP-139 | 64TCP NB SessMsg |
| 21:04.8LEGION.SCANNER | IP-4832 | SHARES.OPEN.3 | IP-139 | 64TCP NB SessMsg |
| 21:04.8LEGION.SCANNER | IP-4833 | JUST.TALKIN.6 | IP-139 | 64TCP NB SessMsg |
| 21:04.8LEGION.SCANNER | IP-4836 | JUST.TALKIN.7 | IP-139 | 64TCP NB SessMsg |
| 21:04.8JUST.TALKIN.7 | IP-139 | LEGION.SCANNER | IP-4836 | 58TCP NB SessMsg |
| | | | | |
| 21:04.8LEGION.SCANNER | IP-4836 | JUST.TALKIN.7 | IP-139 | 64TCP NB SessMsg |
| 21:33.3LEGION.SCANNER | IP-137 | SHARES.OPEN.2 | IP-137 | 96UDP NB NamSvc |
| 21:33.3SHARES.OPEN.2 | IP-137 | LEGION.SCANNER | IP-137 | 365UDP NB NamSvc |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 64TCP NetBIOS |
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 64TCP NetBIOS |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 64TCP NB SessMsg |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 130TCP NB SessReq |

| | | | | |
|---|---|---|---|---|
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 64TCP NB PSesRsp |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 232SMB NegP |
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 153SMB NegP |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 340SMB SLgO |
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 202SMB SLgO |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 162TCP NB SMB |
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 165TCP NB SMB |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 218SMB NBIO |
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 186SMB NBIO |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 246SMB NBIO |
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 778SMB NBIO |
| 21:33.3LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 104SMB CloF |
| 21:33.3SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 97SMB CloF |
| 21:33.4LEGION.SCANNER | IP-137 | SHARES.OPEN.3 | IP-137 | 96UDP NB NamSvc |
| 21:33.4SHARES.OPEN.3 | IP-137 | LEGION.SCANNER | IP-137 | 257UDP NB NamSvc |
| 21:33.4LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 64TCP NetBIOS |
| 21:33.4SHARES.OPEN.3 | IP-139 | LEGION.SCANNER | IP-1114 | 64TCP NetBIOS |
| 21:33.4LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 64TCP NB SessMsg |
| 21:33.4LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 130TCP NB SessReq |
| 21:33.4SHARES.OPEN.3 | IP-139 | LEGION.SCANNER | IP-1114 | 64TCP NB PSesRsp |
| 21:33.4LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 232SMB NegP |
| 21:33.4SHARES.OPEN.3 | IP-139 | LEGION.SCANNER | IP-1114 | 139SMB NegP |
| 21:33.4LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 218SMB SLgO |
| 21:33.4SHARES.OPEN.3 | IP-139 | LEGION.SCANNER | IP-1114 | 114SMB SLgO |
| 21:33.4LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 140SMB OpnX |
| 21:33.4SHARES.OPEN.3 | IP-139 | LEGION.SCANNER | IP-1114 | 97SMB OpnX |
| 21:33.5LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 161SMB NBIO |
| 21:33.5SHARES.OPEN.3 | IP-139 | LEGION.SCANNER | IP-1114 | 202SMB NBIO |
| 21:33.5LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 64TCP NB SessMsg |
| 21:33.6LEGION.SCANNER | IP-1114 | SHARES.OPEN.3 | IP-139 | 64TCP NB SessMsg |

This is the mapping of drive 'C' to the scanners system.

| Time | Source IP | Port | Dest IP | Port | Size | Protocol |
|---|---|---|---|---|---|---|
| 31:28.9 | LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 194 | SMB SLgO |
| 31:28.9 | SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 186 | SMB SLgO |
| 31:28.9 | LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 145 | SMB TrCX |
| 31:28.9 | SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 116 | SMB TrCX |
| | | | | | | |
| 31:29.1 | LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 64 | TCP NB SessMsg |
| 31:31.3 | LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 132 | SMB X2IO |
| 31:31.3 | SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 138 | SMB X2IO |
| 31:31.3 | LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 140 | SMB X2IO |
| 31:31.3 | SHARES.OPEN.2 | IP-139 | LEGION.SCANNER | IP-1112 | 162 | SMB X2IO |
| 31:31.5 | LEGION.SCANNER | IP-1112 | SHARES.OPEN.2 | IP-139 | 64 | TCP NB SessMsg |

Really the only signature profile that is evident is all the "banging" on port 139, but that does not mean that it is hostile. This is also the beauty (from the scanners standpoint) of this scan; it can really blend in with the noise.

**How to protect against it?**

The only way a user can prevent unwanted intruders is to make sure that File and Print Sharing is disabled or to disable the NetBIOS over the Internet service in network properties (These each have there own consequences.).

ALWAYS password protect your Windows-based shares - AND - if you're on an NT network, highly consider enabling User--Level protection. User-Level protection causes share connections to be authenticated by the NT Server instead of a simple user-defined password.

If you must use share-level protection (simple per-share passwords), then definitely employ complex and long passwords that include a wide variety of characters, such as a mixture of "!@#$%^&*()_+=-[]}{\\":';?><,./", numbers, and up/lower case letters. While passwords ARE in fact crackable by brute force over time, creating complex passwords helps to make brute force cracking attempts long and painful, and usually not worth the effort to the potential intruder.

When sharing mounted drives, ensure only required directories are shared.

For added security, allow sharing only to specific IP addresses because DNS names can be spoofed.

For Windows NT systems, prevent anonymous enumeration of users, groups, system configuration and registry keys via the "null session" connection.

Block inbound connections to the NetBIOS Session Service (tcp 139) at the router or the NT host.

Consider implementing the RestrictAnonymous registry key for Internet-connected hosts in standalone or non-trusted domain environments:

NT4:
http://support.microsoft.com/support/kb/articles/Q143/4/74.asp

Win2000:
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

**Source code/Pseudo code:**

Rhino9 (and all of the other sites that carry his(?) work) do not distribute the source code

**Additional information:**

How To Eliminate The Ten Most Critical Internet Security Threats:
http://sans.org/topten.htm

NetBIOS exploit tools:
http://www.securityfocus.com/
Tools/auditing/network/netbios

NetBIOS Overview:
http://support.baynetworks.com/library/tpubs/html/router/soft1200/117358AA/B_39.HTM

Rhino9:
http://www.technotronic.com/rhino9/

The Windows NT Wardoc: A study in remote NT penetration by NeonSurge and the Rhino9 team:
http://home.cyberarmy.com/tcu/wardoc.htm

Last Updated: July 21st, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Security Awareness Summit & Training 2017 | Nashville, TN | Jul 31, 2017 - Aug 09, 2017 | Live Event |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| Community SANS Memphis SEC504 | Memphis, TN | Aug 21, 2017 - Aug 26, 2017 | Community SANS |
| Mentor Session AW - SEC504 | Milwaukee, WI | Aug 23, 2017 - Sep 29, 2017 | Mentor |
| Mentor Session AW - SEC504 | New York, NY | Aug 24, 2017 - Sep 08, 2017 | Mentor |
| Mentor Session - SEC504 | Denver, CO | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling | SEC504 - 201709, | Sep 05, 2017 - Oct 12, 2017 | vLive |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| SANS Dublin 2017 | Dublin, Ireland | Sep 11, 2017 - Sep 16, 2017 | Live Event |
| Mentor AW - SEC504 | Santa Clara, CA | Sep 11, 2017 - Sep 22, 2017 | Mentor |
| Mentor Session - SEC504 | Arlington, VA | Sep 20, 2017 - Nov 01, 2017 | Mentor |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS SEC504 at Cyber Security Week 2017 | The Hague, Netherlands | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Columbia SEC504 | Columbia, MD | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Mentor Session - SEC504 | Boston, MA | Sep 26, 2017 - Nov 07, 2017 | Mentor |
| Mentor Session AW - SEC504 | Houston, TX | Oct 02, 2017 - Dec 11, 2017 | Mentor |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Mentor Session - SEC504 | Columbia, SC | Oct 03, 2017 - Nov 14, 2017 | Mentor |
| Community SANS Chicago SEC504 | Chicago, IL | Oct 09, 2017 - Oct 14, 2017 | Community SANS |
| SANS Phoenix-Mesa 2017 | Mesa, AZ | Oct 09, 2017 - Oct 14, 2017 | Live Event |