Global Information Assurance Certification Paper

W32 Deloder Worm: The Building of an Army

By Vance Stone

GCIH Practical Assignment

Version 2.1 (revised August 8, 2002)

Option 2: Cyber Defense Initiative

Table of Contents

Introduction

The recent rash of Internet worms has produced an army of hundreds of thousands of compromised machines that could ultimately be used to launch a massive distributed-denial-of-service attack at any time. These worms allow intruders to remotely control infected computers from one central computer.

Officials at the CERT® Coordination Center said the organization is monitoring at least five large networks of compromised machines installed with so-called bots. The bots connect compromised PCs or servers to Internet Relay Chat servers, which attackers commonly use to execute commands on the remote systems.

At least one of these networks is an army of more than 100,000 machines and there are indications that these networks are being used for attacks. Whether the army is used today or held in reserve to be used at some future date for an attack doesn't really matter. The potential is there for them to cause serious long-term damage.

In addition to the IRC Trojan, computers compromised by the Deloder worm have an additional backdoor which is typically used for network administration. This tool allows the attacker to remotely control the compromised system or spy on every single keystroke. Deloder installs the administration tool with the same password for all systems so that amateur attackers can utilize these compromised systems.

Contributing to the overall problem is the poor security posture of many computer owners with shared resources and broadband Internet access. Deloder and many other recent worms spread by exploiting weak or null passwords used to protect shared network drives and folders.

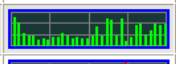
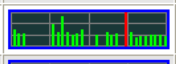
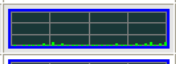
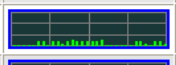
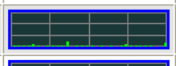
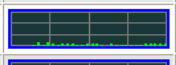
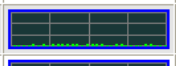
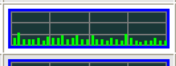
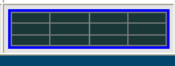
This paper is a review of the Deloder worm and discusses the vulnerabilities associated with port 445/tcp (Microsoft-ds). The paper has suggestions on how to prevent being a victim of this attack and discusses some techniques for detecting attacks associated with port 445/tcp.

Port Selection / Frequency of Attacks

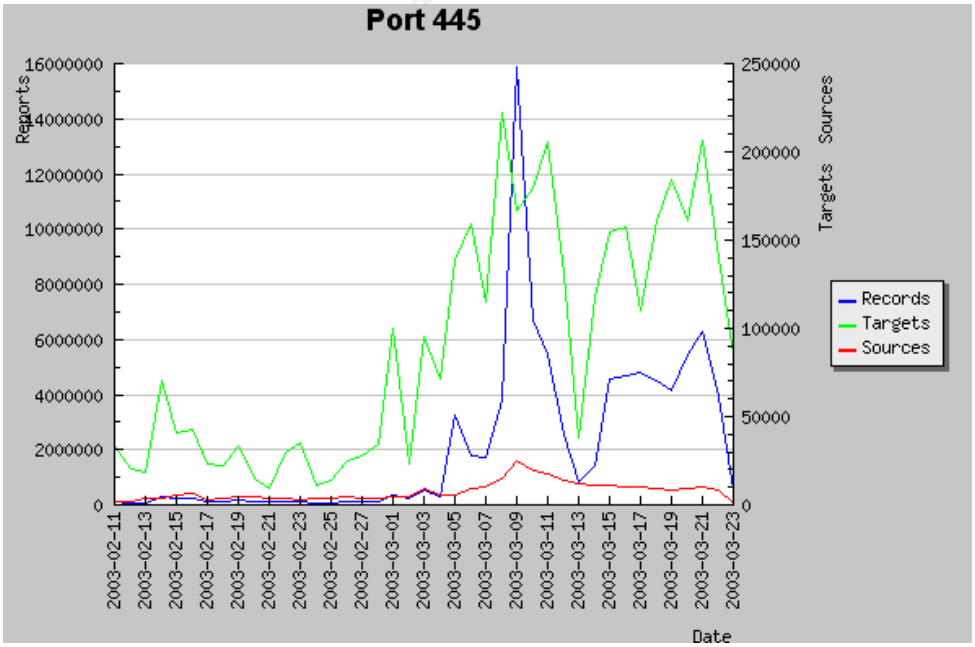
According to IANA, Port 445 is registered as Microsoft-ds. A registered port is one whose purpose has been listed by IANA for the convenience of the Internet community. According to Microsoft port 445 tcp/udp is used for Microsoft CIFS, also known as SMB. For the past few months port 445 has been steadily in the Top 10 attacked ports as listed on the incidents.org website. The current chart of the Top 10 Ports is available from http://isc.incidents.org/top10.html . A snapshot of the chart from March 23, 2003 is shown below.

Last update March 23, 2003 03:01 am GMT (59 minutes ago)

Top 10 Ports

Service Name	Port Number	30 day history	Explanation
netbios-ns	137		NETBIOS Name Service
www	80		World Wide Web HTTP
ms-sql-m	1434		Microsoft-SQL-Monitor
microsoft-ds	445		Win2k+ Server Message Block
ident	113		
gnutella-svc	6346		gnutella-svc
smtp	25		Simple Mail Transfer
netbios-ssn	139		NETBIOS Session Service
eDonkey2000	4662		eDonkey2000 Server Default Port
aicc-cmi	3316		AICC CMI

Other interesting information on the incidents.org website displays that there was a large insurgence on March 7, 2003 when the Deloder Worm was released. The antivirus companies were quick to issue new virus definitions to combat the attack. Because there was much media attention the number of systems compromised was minimized.



After several months of this steady pattern, one can only conclude that many system administrators do not understand the potential for future disaster and should be taking system security more seriously.

Description of Service

Although file sharing is CIFS's primary purpose, there are other functions with which CIFS is commonly associated. Most CIFS implementations are also capable of determining other servers on the network (browsing), printing, and even complicated authentication techniques.

CIFS defines a series of commands used to pass information between networked computers. Requests can be sent over a network to remote devices. CIFS can also make requests to the protocol stack of the local computer. The messages can be broadly classified as follows:

- Connection establishment messages consist of commands that start and end a connection to a shared resource at the server.
- Namespace and File Manipulation messages are used to gain access to files at the server and to read and write them.
- Printer messages are used to send data to a print queue at a server and to get status information about the print queue.
- Miscellaneous messages are used to write to mailslots and named pipes.

Some of the platforms that CIFS supports are:

- Microsoft Windows 2000, Microsoft® Windows NT®, Microsoft® Windows® 98, Microsoft® Windows® 95
- Microsoft® OS/2 LAN Manager
- Microsoft® Windows® for Workgroups
- UNIX
- VMS
- Macintosh
- IBM LAN Server
- DEC PATHWORKS
- Microsoft® LAN Manager for UNIX
- 3Com 3+Open
- MS-Net

Protocol

The Common Internet File System (CIFS) is a network protocol whose most common use is sharing files on a Local Area Network (LAN). It is a native file-sharing protocol in Windows 2000 and Windows XP. The protocol allows a client to manipulate files just as if they were on the local computer. Operations such as read, write, create, delete, and rename are all supported – the only difference

being that the files are *not* on the local computer and are actually on a remote server.

The Common Internet File System protocol runs over TCP/IP and is an enhanced version of the open, cross-platform protocol for distributed file sharing called Server Message Block (SMB). The SMB protocol is the standard way that millions of PC users already share files across corporate intranets and is the native file-sharing protocol in Windows 95, Windows NT and OS/2.

The CIFS protocol works by sending packets from the client to the server. Each packet is typically a basic request of some kind, such as open file, close file, or read file. The server then receives the packet, checks to see if the request is legal, verifies the client has the appropriate file permissions, and finally executes the request and returns a response packet to the client. The client then parses the response packet and can determine whether or not the initial request was successful.

CIFS is a fairly high-level network protocol. In the OSI model, it is probably best described at the Application/Presentation layer. This means CIFS relies on other protocols for transport. While NetBIOS over TCP (NBT) was at one time the de-facto standard transport protocol, Windows 2000 and Windows XP allow it to be transported directly over TCP directly utilizing port 445.

Vulnerabilities

The Deloder worm attempts to logon to a computer by utilizing a dictionary of simple passwords. A system with no password or a weak password for the Administrator account allows the worm complete access to any resource and administrative privileges. Despite this threat, accounts with bad or empty passwords remain extremely common, and organizations with good password policy far too rare. The best and most appropriate defense against these is a strong password policy which includes thorough instructions for good password habits and proactive checking of password integrity.

The Common Vulnerabilities and Exposures (CVE) list is a dictionary that provides common names for publicly known information security vulnerabilities and exposures. It is accepted by many as the central listing for vulnerabilities and exposures. It contains one name and one description for each vulnerability or exposure. The CVE is hosted by the Mitre Corporation.

The CVE contains an entry for port 445 as follows:

CVE-2002-0597

Description: LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service (CPU/memory exhaustion) via a stream of malformed data to microsoft-ds port 445.

Reference: BUGTRAQ:20020417 KPMG-2002011: Windows 2000 microsoft-ds Denial of Service
Reference: VULNWATCH:20020417 [VulnWatch] KPMG-2002011: Windows 2000 microsoft-ds Denial of Service
Reference: Microsoft Knowledge Base:Q320751
Reference: XF:win2k-lanman-dos(8867)
Reference: BID:4532

The CVE also has a candidate for inclusion in the list of approved entries. This candidate is in the process of being reviewed before it can be included in the list. The entry is as follows:

CAN-2002-0283

Phase: Proposed (20020502)
Description: Windows XP with port 445 open allows remote attackers to cause a denial of service (CPU consumption) via a flood of TCP SYN packets containing possibly malformed data

Reference: BUGTRAQ:20020215 Windows XP Remote DOS attacks with SYN Flag. Make CPU 100%
Reference:
URL:http://marc.theaimsgroup.com/?l=bugtraq&m=101408718030099&w=2.

In addition to the registered vulnerabilities associated with port 445, the paper "CIFS: Common Insecurities Fail Scrutiny" discusses protocol and administrative vulnerabilities associated with CIFS. Such vulnerabilities include:

- A CIFS compliant server can not enforce the use of password encryption; it is the client that chooses the password encryption. Thus allowing attackers the ability to use plaintext passwords in brute-force guessing.
- Login successes and failures must be enabled on a Windows 2000/XP system; logging is not enabled with the factory defaults. And even when logging is enabled only the name given by the connecting client is saved, not the IP address.
- Based on the timing of error responses from a Windows CIFS server, it is easy to remotely determine if an account has been temporarily locked out.

The paper also mentions that other attacks may be possible, such as:

- Man-in-the-middle attacks against the authentication protocol
- Desynchronizing an existing session between two hosts and taking over the connection.

Exploit Details

- Name: W32/Deloder-A [Sophos], WORM_DELODER.A [Trendmicro], Win32.Deloder Worm [ComputerAssociates], W32/Deloder.worm [McAfee], W32.HLLW.Deloder[Symantec]
- Cert® Advisory CA-2003-08, CVE-2002-0597, CAN-2002-0283
- Operating System: Windows 2000 and Windows XP
- Protocols/Services: Microsoft-ds (port 445/tcp) / Applications utilizing shared drives
- Description: W32.HLLW.Deloder is a network-aware worm that attempts to connect to a target host, using port 445/tcp. If the worm makes a successful connection, it copies files to the victim computer. Then it attempts to launch several remote services, which:
  - Copies and executes the backdoor Trojan
  - Copies and executes the worm
  - Deletes the default shares

Description of Variants

Deloder scans for other systems listening on port 445/tcp and when a system is discovered, the worm connects to the $IPC share using a set of pre-programmed usernames and passwords, it copies itself to the victim and runs its payload.

To date two variants of Deloder have been discovered, one on March 9, 2003 and one on April 11, 2003. They both have the same techniques for automated scanning and exploitation but their backdoor Trojans differ somewhat.

The version of Deloder discovered on March 9, 2003, utilizes VNC (Virtual Network Computing), an open-source remote display tool from AT&T. The worm drops the server component of the tool on the compromised system. When the VNC tool executes it listens on port 5800/tcp or 5900/tcp for instructions from clients. And if a VNC client requests a connection to the compromised system plus provides the correct password, the user of the VNC client is granted full access to the system. The client can remotely control the compromised system, or simply spy on every keystroke and mouse move on the compromised system. The version of Deloder discovered on April 11, 2003, performs the same attack as the first version by scanning for other systems listening on port 445/tcp. And attempting to crack the Administrator password and running its payload.

However the April 11,2003 version utilizes a remote administration tool called Remote Administrator rather than VNC as a backdoor. Remote Administrator is a popular remote administration tool for Windows systems from Famatech. The worm drops the server component of the popular tool and runs it as a service on the remote XP/2000 computer. The tool listens on port 4899 for commands. And once the service is running, a user using a client program can see the remote computer's screen. Mouse movements and key presses are transferred to the remote computer.

Table 1 Files dropped by Deloder variant discovered on March 9, 2003

File name	File Size	Type
Dvldr32.exe	745,984 bytes	the worm
inst.exe	684,562 bytes	trojan dropper
rundll32.exe	29,336 bytes	IRC bot
cygwin1.dll	944,968 bytes	file used by IRC bot
explorer.exe	212,992 bytes	VNC application
omnithread_rt.dll	57,344 bytes	part of VNC application
VNCHooks.dll	32,768 bytes	part of VNC application
psexec.exe	36,352 bytes	Remote Process Launch application

Table 2 Files dropped by Deloder variant discovered on April 11, 2000

File name	File Size	Type
Dvldr32.exe	802,824 bytes	the worm
inst.exe	684,562 bytes	trojan dropper
hypertrm.exe	241,664 bytes	Remote Administration tool
AdmDll.dll	90,112 bytes	file used by Remote Administration
raddrv.dll	29,408 bytes	file used by Remote Administration
psexec.exe	36,352 bytes	Remote Process Launch application

The payload for the variant discovered on March 9, 2003, contains an IRC bot Trojan. When this bot joins its IRC network, a remote intruder controlling the IRC channel can issue arbitrary commands on the compromised computer, including launching denial-of-service attacks.

At the time of this writing there is not much public information about the variant discovered on April 11, 2003. According to McAfee, the two IRC files, rundll32.exe and cygwin1.dll, are not dropped by this variant as shown in the tables above. Therefore the fate of the IRC component is indeterminate for this version. And other sources have not yet updated their information.

Another similar IRC bot worm is the W32/Slackor.worm. The worm scans the local network (via sweeping contiguous IP addresses) for machines present on the network. Once a system is found, the worm tries to connect to the 'IPC$' and/or 'C$' and/or 'C' shares on that machine (variant dependant) using usernames and passwords that it carries. If successful the worm copies its components to the system folders on the compromised computer.

Variants of this worm consisted of a dropper which dropped and executed various other components. These included a batch script (for connecting to remote machines), an application to launch processes on remote machines, and an IRC bot. The batch script drives propagation, attempting to connect to remote

shares using various usernames and passwords. However the W32/Slackdor.worm does not contain a remote administration tool as the Deloder worm.

Protocol Description

Much of this section was derived from the CIFS Technical Reference and the paper CIFS Explained.

The CIFS (SMB over TCP) architecture is based upon a client sending requests and a server replying to each request sent. The only exception to the request-response is one case in which the server must send an unsolicited request to the client when the server must break an oplock it has established with the client.

Servers make file systems and other resources (printers, mail slots, named pipes, APIs) available to clients on the network. Client computers may have their own hard disks, but they also want access to the shared file systems and printers on the servers.

Clients connect to servers using TCP/IP in this case. Once they have established a connection, clients can then send commands (SMBs) to the server that allow them to access shares, open files, read and write files, and generally do all the sort of things that they want to do with a file system. However, in the case of SMB, these things are done over the network.

Protocol dialects/negotiation: There have been many versions of the CIFS protocol since its inception in the 1980's. The initial dialects offered the basic file services however as more complex services were desired newer protocol versions were required. When a client wishes to access files on a remote server, the first CIFS packet that is sent is a negotiate protocol packet. In this CIFS packet, the client lists all of the dialect strings that it is capable of understanding. In the response packet, the server indicates which dialect it wishes to communicate in, or indicates that the server understood no dialects. In this way, the client and server can negotiate which dialect to use for a particular CIFS session.

Security: A share is a server entity (typically a file folder or printer) that is available to clients for network sharing. Access to the share is restricted in one of two ways:

1. *Share level*: Protection is applied at the share level on a server. Each share can have a password, and a client only needs that password to access all files under that share. This was the first security model that SMB had and is the only security model used in Windows 95 and 98.

2. *User level*: Indicates that a client wishing to access the share must provide a username and a password for access. This provides the server

administrator fine grain control over who has access to what share. This type of security is used in Windows NT and Windows 2000.

Authentication: User authentication is based on the shared knowledge of the user's password. There are two styles of user authentication. The first involves the client sending passwords in plain text to the server. And since plain text passwords expose the user's password, this form of authentication is discouraged and by default should be disabled.

The second involves a challenge/response protocol whereby the server sends a "challenge" to the client. The client responds to the challenge in a way that proves it knows the user's password. A "response" is created from the challenge by encrypting it with a 168 bit "session key" computed from the user's password. 'The response is then returned to the server, which can validate the response by performing the same computation.

Command batching: Many CIFS packets are capable of piggybacking other CIFS packets in order to reduce response latency and better utilize network bandwidth. This technique is referred to as ANDX batching.

Opportunistic locking: When a CIFS packet specifies to open a file, an opportunistic lock (oplock) can be requested. If granted by the server, the oplock indicates to the client that no other entities are accessing the file. This allows the client to make any modifications to the file that it wants and not have to write them all to the server immediately.

When operating CIFS over TCP, connections are established to port 445/tcp and each message is framed as follows:

<table>
<tr><td>byte 0</td><td>byte 1</td><td>byte 2</td><td>byte 3</td></tr>
<tr><td>zero</td><td colspan="3">length</td></tr>
<tr><td>0xFF</td><td>"S"</td><td>"M"</td><td>"B"</td></tr>
<tr><td>Command</td><td>Error Class</td><td>Must be zero</td><td>Error Code</td></tr>
<tr><td>Error Code (cont.)</td><td>Flags</td><td colspan="2">Flags2</td></tr>
<tr><td colspan="4">Pad or security signature - typically pad and therefore must be zero</td></tr>
<tr><td colspan="2">Tree ID (TID)</td><td colspan="2">Process ID (PID)</td></tr>
<tr><td colspan="2">User ID (UID)</td><td colspan="2">Multiplex ID (MID)</td></tr>
<tr><td>Word Count</td><td colspan="3"></td></tr>
<tr><td colspan="4">Parameter Words[Word Count] - the number of words in this variable size section is specified by the Word Count variable.</td></tr>
<tr><td colspan="2">Byte Count</td><td colspan="2"></td></tr>
<tr><td colspan="4">Buffer[Byte Count] - the number of bytes in this variable size section is specified by the Byte Count variable.</td></tr>
</table>

Each CIFS over TCP request starts with a 4 byte field encoded as above: a byte of zero, followed by three bytes of length; after that follows the body of the request.

Header: Every CIFS packet contains a 4-byte header. The first byte is 0xFF, followed by the ASCII representation of the letters “S”, “M”, and “B”.

Command: The command field contains the operation code that this SMB is requesting or responding to. Refer to the CIFS1.0 section 5.1 for the list of approximately a hundred command possibilities.

Error class: A server indicates whether or not a given request was successful with the error class field. If the field is zero, the request has been successful. If the field is non-zero, the field indicates which of the following classes the error code is from:

- ERRDOS – Error is from the core DOS operating system set
- ERRSRV – Error is generated by the server network file manager
- ERRHRD – Hardware error
- ERRCMD – Command was not in the “SMB” format

Error code: This field indicates the type of error that has occurred. It is typically set to zero, indicating no error. If set, this number in conjunction with the error class above can give full error descriptions. The full error descriptions can be looked up in the CIFS1.0 draft. As with the error class, this field is set only by servers in response to a previous request.

Flags: This field contains 8 individual flags, numbered from least significant bit to most significant bit. Flags that are not defined MUST be set to zero by clients and MUST be ignored by servers. The only bit of note in this field is bit 3. When bit 3 is set to ‘1’, all pathnames in this particular packet must be treated as caseless. When bit 3 is set to ‘0’, all pathnames are case sensitive.

Flags2: This field contains nine individual flags, numbered from least significant bit to most significant bit. Flags that are not defined MUST be set to zero by clients and MUST be ignored by servers. Bits that are useful:

- Bit 0, if set, indicates that the server may return long file names in the response.
- Bit 6, if set, indicates that any pathname in the request is a long file name.
- Bit 16, if set, indicates strings in the packet are encoded as UNICODE.

Pad/security signature: This field is typically set to zero.

Tree ID (TID): The TID is identifies to which resource (disk share or printer, typically) this particular CIFS packet is referring. When packets are exchanged which do not have anything to do with a resource, this number is meaningless and ignored.

If a client wishes to gain access to a resource, the client sends a CIFS packet with the command field set to SMB_COM_TREE_CONNECT_ANDX. In this packet, the share or printer name is specified (i.e. \\SERVER\DIR). The server then verifies that the resource exists and the client has access, then sends back a response indicating success. In this response packet, the server will set the TID to any number that it pleases. From then on, if the client wishes to make requests specific to that resource, it will set the TID to the number it was given.

Process ID (PID): The PID identifies which process is issuing the CIFS request on the client. The server uses this number to check for concurrency issues (typically to guarantee that files will not be corrupted by competing client processes).

User ID (UID): The UID identifies the user who is issuing CIFS requests on the client side. The client must obtain the UID from the server by sending a CIFS session setup request containing a username and a password. Upon verifying the username/password, the server responds to the session setup and includes a generated UID. The client then uses the assigned UID in all future CIFS requests. If any of these client requests require file/printer permissions to be checked, the server will verify that the UID in the request has the necessary permissions to perform the operation. Other sessions could potentially be using an identical UID that the server correlates with a different user. Note: if a server is operating in share level security mode, the UID is meaningless and ignored.

Multiplex ID (MID): The value is used along with the PID to allow multiplexing the single client and server connection among the client's multiple processes, threads, and requests per thread. Clients may have many outstanding requests at one time. Servers MAY respond to requests in any order, but a response message MUST always contain the same MID and PID values as the corresponding request message. The client MUST NOT have multiple outstanding requests to a server with the same MID and PID.

Word Count and parameter words: CIFS packets use these two fields to hold command-specific data. The CIFS packet header template above cannot hold every possible data type for every possible CIFS packet. To remedy this, the parameter words field was created with a variable length. The word count specifies how many 16-bit words the parameter words field will actually contain. In this way, each CIFS packet can adjust to the size needed to carry its own command-specific data.

The word count for each packet type is typically constant and defined in the CIFS1.0 draft. There are two word counts defined for every single command; one word count for the client request and another for the server response. Two counts are needed because the amount of data necessary to make a request is not necessarily the same amount needed to issue a reply.

Byte Count and buffer: These fields are very similar to the word count and parameter words fields above; they hold a variable amount of data that is specified on a per packet basis. The byte count indicates how many bytes of data will exist in the buffer field that follows.

The major difference between the parameter data section above and the buffer is what type of data they store. The parameter words data section typically holds a small number of packet options, while the buffer data section typically holds large amounts of raw data (e.g. file data).

How the Exploit Works

The activities of Deloder break down into the categories of attack and await further instructions. The worm attacks other systems converting them into bots. As bots the victim computers are forced into attacking other systems and listening for further commands.

The attack and convert procedures are performed by the following files:

- Dvldr32.exe – the self-propagating malicious code written in MS VC 6.0
- Psexec.exe – the Remote Process Launch application from Sysinternals
- Inst.exe – a Trojan installer

The victim computers listen for commands via two back doors:

1. the victim attempts to connect to one of a number of pre-configured IRC servers utilizing the following files:

    - rundll32.exe – the IRC-Pitchfork bot application
    - cygwinl.dll – IRC-Pitchfork dependency file

2. The victim executes a copy of VNC (Virtual Network Computing), an open-source remote display tool from AT&T. The tool listens on port 5800/tcp or 5900/tcp for commands. The tool is comprised of the following files:

    - explorer.exe – a renamed copy of the VNC application
    - omnithread_rt.dll – a VNC dependency file
    - VNCHooks.dll – a VNC dependency file

The Attack

Deloder scans random addresses and attempts to connect to Windows 2000/XP shares, via port 445/tcp. If it can connect then it utilizes a brute-force dictionary password crack routine to log on to the remote system. The dictionary of passwords may vary depending on the variant. However the most common variant includes 85 passwords which are listed in Appendix A.

If the logon attempt is successful it connects as the administrator of a system and can launch processes as it wishes. It copies itself, Dvldr32.exe, and Trojan installer, inst.exe, to the system Windows directory on the remote computer. It creates the following registry entry so that the worm is run automatically each time Windows is started:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ messnger = <pathname of worm>

When Dvldr32.exe is executed for the first time, it drops the files, psexec.exe in the current folders and inst.exe in the following startup folders:

- C$\WINNT\All Users\Start Menu\Programs\Startup\
- C\WINDOWS\Start Menu\Programs\Startup\
- C$\Documents and Settings\All Users\Start Menu\Programs\Startup\

Dropping the file, inst.exe, in these folders ensures that the backdoor component is executed at startup. And to prevent multiple instances of itself from executing, Deloder creates a unique mutex named "testXserv".

According to Sophos, the attacking worm uses psexec to set the file attributes for inst.exe and Dvldr32.exe to read-only, attempts to launch inst.exe and Dlvdr32.exe, and attempts to disable the network shares C$, D$, E$, F$, IPC$ and ADMIN$.

Once the machine is restarted psexec.exe is executed and the victim computer picks random addresses and attempts to compromise other systems.

When executed, inst.exe drops the two Trojan backdoors into the system. One backdoor the IRC bot Trojan uses the following files:

- %windir%\Fonts\rundll32.exe
- %sysdir%\cygwin1.dll

and the other backdoor a VNC server is composed of the following files:

- %windir%\Fonts\explorer.exe
- %windir%\Fonts\omnithread_rt.dll
- %windir%\Fonts\VNCHooks.dll

Where "%windir%" is Windows root directory and "%sysdir%" is the Windows System directory.

The worm creates two keys in the Windows Registry, so that the Trojan backdoor components will be run next time Windows starts.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
"TaskMan" = "%windir%\Fonts\rundll32.exe"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
"Explorer" = "%windir%\Fonts\explorer.exe"

When the worm launches rundll32.exe the IRC Trojan connects utilizing port 6667/tcp to an IRC server. According to McAfee the list of IRC servers is as follows:

cocket.nailed.org
cocket.mooo.com
cocket.bounceme.net
cocket.phathookups.com
cocket.gotdns.com
cocket.ma.cx
cocket.orgdns.org
cocket.minidns.net
cocket.dyn.nicolas.cx
cocket.dynup.net
cocket.pokemonfan.org
cocket.staticcling.org
cocket.getmyip.com

Once the Trojan connects to one of the IRC servers, it listens on a channel for commands.

When the worm launches "explorer.exe" the VNC server is initiated listening on 5800/tcp or 5900/tcp.

Diagram

The following diagram illustrates an attacker scanning a group of target systems looking for the open port TCP/445. If the port is open the worm will connect and attempt to login to the Administrator utilizing a brute-force password crack routine. If the worm is successful, the system will be infected and will begin the vicious cycle of scanning other targets to compromise.

Figure 1 Deloder Worm Exploit

How to Use the Exploit

Once connected to an IRC Server the system would be controlled by the Bot Master. The compromised system would be monitoring the channel for certain trigger words and would perform actions accordingly.

The bot can easily be requested to send most any information about itself up the channel such as CPU speed, available RAM, logical drives, available disk space, and any data contained on the logical drives.

Additionally the IRC channel can be used by the Bot Master to send attack commands. And commands sent over the IRC channel are sent to all of the bots at the same time. Therefore if there are hundreds of bots on a channel and the Bot Master sends out an attack command, then several hundred systems will be performing the attack. The following is a list of a few of the Distributed Denial of Service(DDOS) attack possibilities:

- ICMP ping flood attacks – this sends a ping flood of size and amount which has been defined by the Bot Master to a target IP address. This form of attack is considered a bandwidth saturation attack because it stops any useful data from getting in or out of a network.
- IGMP packet flood attack – this sends malicious fragmented IGMP packets to a targeted computer. Fragmented IGMP packets will often cause un-patched Windows 98 systems to BSoD(Blue Screen of Death) or in some cases cause the system to force a reboot. This form of attack is also considered a bandwidth saturation attack.
- UDP packet of Death - this sends a UDP packet of size and amount which has been defined by the Bot Master to a target IP address on random ports between 1000 and 6669.

As stated earlier, VNC is a remote display tool which can be used to view the computer screen and take over the keyboard and mouse control of a compromised system. The intruder would have the same capabilities over the system as if he were sitting in front of the compromised system. Once a system has been compromised by the Deloder, only three steps would be required for an intruder to dominate a compromised system:

- The intruder would need to locate the system by scanning for systems with ports 5800/tcp and 5900/tcp open.
- The intruder would need to connect to the remote system
- The intruder would need to enter the password “strict” as stated by KLC Consulting.

After that point, an intruder would have access to any data stored on the local computer and all logical drives. The intruder would also have access to any data that passes through the computer such as account numbers that are entered for an Internet transaction, even though they were not stored. The Internet part of the transaction might have been encrypted but the account data could be captured before it was encrypted since keystrokes can be monitored.

Since the worm performs a number of different tasks a combination of existing programs would be required to exploit this vulnerability. And a manual exploit could be performed in the event that no automated tools were available. You may recall that the worm performs the following steps:

1) Scan for open Windows shares utilizing port 445/tcp
2) Perform a brute-force dictionary attack
3) Copy worm, IRC Trojan, and VNC applications to victim computer and setting file attributes.
4) Set Registry keys
5) Execute worm, IRC Trojan, and VNC applications on victim computer
6) Repeat

In order to perform the above tasks the following programs could be used:

1) Scan for systems with port 445 open by using a tool such as SuperScan which was developed by Foundstone, Inc.

   SuperScan is a powerful connect-based TCP port scanner, pinger and hostname resolver. Its multithreaded and asynchronous techniques make this program extremely fast and versatile. It can perform ping scans and port scans using any IP range or extract addresses from a specific text file. It can resolve and reverse-lookup any IP address or range. Modify the port list and port descriptions using the built in editor. Connect to any discovered open port using user-specified "helper" applications (e.g. Telnet, Web browser,

FTP) and assign a custom helper application to any port. Save the scan list to a text file. And it has a user friendly interface.

The following figure is an example of using SuperScan to scan a range of /16 addresses for systems with port 445 active.

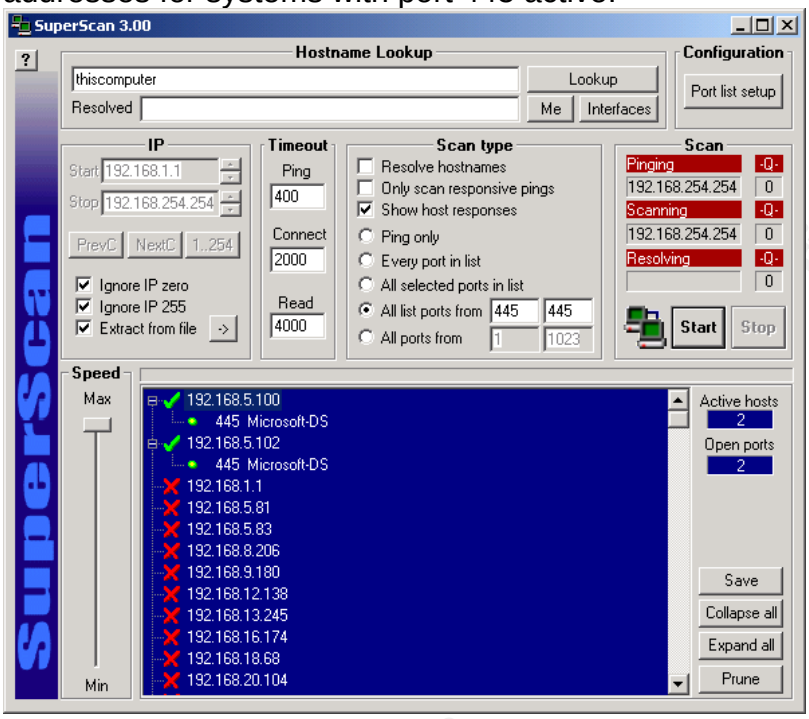


Figure 2 Example of Scanning for Vulnerable Systems

Note: To simulate the worm, the IP addresses were randomized over the range of 192.168.X.X and stored into a text file. The text file was then selected as the input to SuperScan however SuperScan displayed the systems alphabetically with the active ones first.

2) A brute force dictionary attack could be performed using enum to determine the Administrator password.

Enum is a console-based Win32 information enumeration utility written by Jordan Ritter. Using null sessions, enum can retrieve userlists, machine lists, sharelists, namelists, group and member lists, password and LSA policy information. Enum is also capable of a rudimentary brute-force dictionary attack on individual accounts.

Once the dictionary file has been created with the desired list of possible passwords, then enum can be used to determine the password for any given that the password is in the dictionary. For example if the passwords were entered into the file dictfile.txt the following enum command would determine

which of the passwords was the correct one for the account named *any_account.*

enum –D –u *any_account* –f dictfile.txt *target_host_IP_address*

With *target_host_IP_address* being the IP address of the remote computer. An example which simulates the Deloder worm's password crack is given in Appendix B.

3) Once the administrative password is known, CIFS protocol would allow the attacker to copy, create, delete, and set the attributes of files just as the files were on the attacking compute. While CIFS protocol is most often used on Windows operating systems, many other operating systems are capable of utilizing it as previously discussed.

4) Since Deloder was written in Microsoft Visual C, a MS VC routine would be required to creating a registry key. The creator could write one himself or many examples are available from sources. Such an example routine is included in Appendix C as written by David Overton.

5) In order to remotely execute applications the Remote Process Launch application, psexec.exe, could be utilized.

   PsExec developed by Mark Russinovich is a tiny quick routine that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools that otherwise do not have the ability to show information about remote systems.

   The command format is as follows:

   psexec \\computer [-u username [-p password]][-s][-i][-c[-f]][-d] program[arguments]

-u	Specifies optional user name for login to remote computer.
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
-s	Run remote process in the System account .
-i	Run the program so that it interacts with the desktop on the remote system.
-c	Copy the specified program to the remote system for execution. If you omit this option then the application must be in the system's path on the remote system.
-f	Copy the specified program to the remote system even if the file already exists on the remote system.
-d	Don't wait for application to terminate. Only use this option for non-interactive applications.
program	Name of the program to execute.

arguments Arguments to pass (note that file paths must be absolute paths on the target system)

For example in order for Deloder to execute Dvldr32.exe on a victim computer the command could look something like the following:

psexec *victim_address* –u Administrator –p *password* –s –d %windir%dvldr32.exe

where *victim_address* is the IP address of the victim's computer and the password is the Administrative password as discovered above and the %windir% is the folder where the dvldr32.exe is located.

6) By returning to step one, one would simulate the steps taken by the Deloder worm.

Signature of the Attack

The Windows 2000/XP security log can indicate a possible attack by the Deloder worm. An audit entry of a security event such as a logon attempt can be recorded in the security log. If the security log is examined regularly it is possible to detect this type of attacks.

Appendix D contains a summary listing of the security log after a password attack was performed on a test network. Upon examining the security log it is easy to note that therein lays a listing of a hundred or so logon failures within a time interval of a minute or two. This type of activity of quick logon/logoff failures indicates an automated password crack attempt.

Once the detail is examined the security log shows an entry like the following for each incorrect password attempt:

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 5/4/2003
Time: 6:31:30 PM
User: NT AUTHORITY\SYSTEM
Computer: *victim_ID*
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: Administrator
Domain: *attacker_ID*
Logon Type: 3
Logon Process: NtLmSsp

Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: *attacker_ID*

The above detailed entry shows the date, time, the attacker_ID, the victim_ID, and that the attacker was attempting to logon to the Administrator account. This entry also shows that the attempt failed because of "Unknown user name or bad password".

The remaining entries in the security log are similar repeats of the above entry with the different passwords from the Deloder worm being attempted.

It should be noted that by default security auditing is not enabled on Windows 2000/XP, so there will likely be no events in the security log. Security auditing can be enabled by an administrator. The administrator would need to perform the following steps:

1. Open Local Security Policy from Administrative Tools in Control Panel
2. In the left pane open Local Policies and select Audit Policy
3. In the right pane right-click on Audit Logon Events and select Failure

Of course if this computer is a member of a domain and the network administrator has configured a Group Policy then the Group Policy overrides the Local Security Policy.

Additionally numerous login failures via Microsoft-ds for a system can indicate an attack. An example of such a suspected attack attempt was captured by Ethereal and is included in Appendix E.

Ethereal is a free network protocol analyzer for Unix and Windows. It allows one to examine data from a live network or from a capture file on disk. One can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.

This attack was unsuccessful because the Administrator password was a strong one. It is suspected that this was an actual Deloder attack because the symptoms of utilizing port 445/tcp and performing approximately 85 attack attempts are consistent with the worm. The full frame summaries are located in Appendix E with the IP addresses having been sanitized so the attacker was assigned (10.1.1.10) and the target being assigned (10.1.1.4).

An explanation of the most pertinent 11 frames captured are as follows:

Frames 80 – 82 shows the scan taking place where the attacker is determining if the target utilizes SMB on port 445 (Microsoft-ds). Since the target responded with an [ACK] to the attackers [SYN] the target confirms this fact.

The two systems follow through with the connection utilizing the TCP three-way handshake.

No.	Time	Source	Destination	Prot	Info
80	2260.4404	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [SYN] Seq=1516704752 Ack=0 Win=16384 Len=0
81	2260.4942	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [SYN, ACK] Seq=3198658100 Ack=1516704753 Win=17520 Len=0
82	2260.5603	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516704753 Ack=3198658101 Win=17520 Len=0

Frames 83 - 84 show the two systems negotiating the dialect of SMB that they will use.

No.	Time	Source	Destination	Prot	Info
83	2260.5662	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
84	2260.5674	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response

Frames 85 shows the attacker requesting to be allowed access to a resource utilizing the SMB AndX command.

No.	Time	Source	Destination	Prot	Info
85	2260.6361	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE

Frame 86 shows that the target has ExtendedSecurity enabled and therefore it is requesting logon information from the attacker.

No.	Time	Source	Destination	Prot	Info
86	2260.6376	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED

Frame 87 shows the attacker sending logon credentials.

No.	Time	Source	Destination	Prot	Info

87	2260.6736	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH

Frame 88 shows the target rejecting the attacker's logon credentials with an error response.

No.	Time	Source	Destination	Prot	Info
88	2260.6783	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE

Frame 89 shows the attacker attempting to close the SMB session.

No.	Time	Source	Destination	Prot	Info
89	2260.7058	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request

Frame 90 shows the SMB session being dismantled and the target returning an error: "Bad userid" since no UID was ever created.

No.	Time	Source	Destination	Prot	Info
90	2260.7060	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid

The majority of the remaining frames captured are groups of frames like those above where the attacker is attempting to logon utilizing different passwords. When required the attacker will recreate the TCP three-way handshake and SMB dialect negotiation. But if the TCP connection is still valid, the attacker will omit these steps and proceed with the SMB logon attempt.

The final few frames captured terminate the TCP session with a [FIN,ACK] and [ACK] being exchanged between both systems.

808	2277.6043	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [FIN, ACK] Seq=1525277392 Ack=3202736317 Win=17075 Len=0
809	2277.6045	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1349 [FIN, ACK] Seq=3202736317 Ack=1525277393 Win=17477 Len=0
810	2277.6251	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525277393 Ack=3202736318 Win=17075 Len=0

Other ways to detect an attack by the Deloder worm include using anti-virus software created or updated since March 9, 2003. Since the version of

psexec.exe included with Deloder is UPX packed, some versions of anti-virus software such as McAfee will detect this component as IRC/Flood.i.

Other indications of a possible attack by the Deloder worm include widespread scanning for 445/tcp. These can be detected by observing firewall logs and selecting port 445/tcp.

Additionally, if the worm were successful in compromising a host, it may also be detected because:

- it may have unauthorized connections to IRC servers (typically on port 6667/tcp, although ports may vary)
- the VNC package installed will typically listen on ports 5800/tcp or 5900/tcp
- if a compromised system is used in a DDoS attack on another site, large volumes of IP traffic (ICMP, UDP, or TCP) may be detected emanating from the compromised system.

How to Protect Against the Attack

Defense in Depth is practical strategy for protecting information systems in today's networked environments. The application of defense techniques should be based on the Protect, Detect, and React paradigm. This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks.

The defense posture should be designed around a layered approach such that there are multiple defense mechanisms which present unique obstacles between the adversary and the target. Each of these mechanisms should include both protection and detection measures to increase the risk for the attacker. The defense plan should force the attacker to penetrate the outer perimeter, such as the local and wide area network before even reaching a host.

Defend the network and infrastructure

For example, ACLs should be deployed on the border routers and should provide logging capabilities. Additionally, a firewall should be deployed with more granularity and logging capabilities. In some situations, these products may be able to alert users to the fact that their machine has been compromised. Furthermore, they should have the ability to block intruders from accessing backdoors over the network. Note that no firewall can detect or stop all attacks, so it is important to continue to follow safe computing practices.

In the case of the intruder activity described above, blocking connections to port 445/tcp from entering or leaving a network reduces the risk of external infected systems attacking hosts inside a network or vice-versa. Of course this assumes that that file shares being accessible to/from the Internet or other networks is not a requirement. If SMB shares across the Internet are required, added protection

would be provided if a port 445/tcp filter was customized such that the SMB could be exchanged only between specific IP addresses. Even further protection would be provided if a Virtual Private Network were provided between the two sites.
Ingress filtering manages the flow of traffic as it enters a network under administrative control. In the network usage policy of many sites, external hosts are only permitted to initiate inbound traffic to machines that provide public services on specific ports. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services. If this is not possible, a port 5800/tcp filter should be installed to block any possible inbound VNC connections.
Egress filtering manages the flow of traffic as it leaves a network under administrative control. There is typically limited need for internal systems to access SMB shares across the Internet, therefore port 445/tcp should be blocked. Additionally, in order to block the IRC backdoor, a port 6667/tcp egress filter should be put in place.

Firewall and router logs should be maintained and monitored for signs of a threat. Any suspicious activity such as high traffic on port 445/tcp should be examined. Additionally any traffic on ports 6667/tcp, 5800/tcp, and 5900/tcp should be carefully investigated.

Some routers/firewalls are capable of taking advantage of a technique called Network Address Translation. NAT is defined as the translation of an IP address known within one network to a different IP address known within another network. By using NAT, systems on an inside network appear as one system to an outside network. This technique still enables the inside systems to have full access to the outside network.

NAT hides the internal network IP addresses through translation so a high level of protection is automatic without any special setup. As a result of the internal addresses being hidden, NAT only allows connections that originate in the inside network, effectively blocking external connections.

Properly written address translators require a person on the outside to first compromise the NAT device before being able to mount an attack against an inside host. Therefore a NAT device should be used as just another layer in the security suite.

Defend the servers and hosts

Keep the Operating System software and applications software up-to-date
If only one thing is done to help protect the safety of a computing environment, software updates should always be promptly installed. Failure to apply "fixes" in a prompt manner can leave a computer exposed unnecessarily to loss or damage of personal files and data. These updates address known exploitable flaws or introduce additional security features.

The automatic update feature offered by many packages should be used to keep the system up-to-date.

Run and maintain an anti-virus product
The malicious code being distributed in these attacks is under continuous development by intruders, but most anti-virus software vendors release frequently updated information, tools, or virus databases to help detect and recover from the malicious code involved in this activity. Therefore, it is important that users keep their anti-virus software up to date.

Again, the automatic update feature offered by many anti-virus packages should be used to keep the anti-virus system up-to-date.

Disable or secure file shares
If a given computer is not intended to be a server (i.e., share files or printers with others), then "File and Printer Sharing for Microsoft Networks" should be disabled.

If “File and Printer Sharing for Microsoft Networks” is required the user authentication should also be required and each account should have a well-chosen password. As stated above, a firewall should be considered to control which computer can access these shares.

Passwords
Implementation of stringent validation criteria such a strong passwords can help keep the Deloder worm from infecting systems. A strong password should have the following characteristics:

- Contain at least seven characters
- Include upper and lower case letters, numerals, and symbols
- Have at least one symbol character in the second through sixth position
- Have at least four different characters in the password (no repeats)
- Look like a sequence of random letters and numbers

Some don’ts for creating strong passwords:

- Don't use ANY PART of the logon name for the password
- Don't use any actual word or name in ANY language
- Don't use numbers in place of similar letters
- Don't reuse any portion of your old password
- Don't use consecutive letters or numbers like "abcdefg" or "234567"
- Don't use adjacent keys on your keyboard like "qwerty"

Account lockout policy

An account lockout policy should be used to help detect and block an automated password attack. The policy would disable an account after a set number of failed logon attempts. The account could be automatically reset after a certain amount of time or could remain disabled until an administrator manually resets it. This feature is disabled by default; therefore to enable this feature one should launch Local Security Policy and proceed to Computer\Configurations\Windows Settings\Security Settings\Account Policies\Account Lockout Policy.

There are three items that must be configured in order to enable this option:

1. Account lockout threshold – the number of failed logon attempts before the user account is locked out.
2. Account lockout duration – the number of minutes of how long the account is locked out. A value of zero says that the account is locked out until an administrator unlocks it.
3. Reset account lockout counter after – the number of minutes that must elapse after a failed logon attempt before the counter resets to 0 the counter for failed attempts. This must be less than or equal to the account lockout duration.

Typically a lockout threshold of 5 attempts and 30 minutes for lockout duration and reset time is sufficient to defend against automated password crack attempts.

Programs of unknown origin

Programs of unknown origin should not be executed unless the author(s) of a program is known or trusted, a program should never be downloaded, installed, or executed. Users of IRC, Instant Messaging (IM), and file-sharing services should be particularly wary of executing software sent to them by other users or following links sent to them, as this is a common method for intruders to attempt to infiltrate systems.

Security Logs

On the Windows 2000/XP systems, logon failure auditing should be enabled and the security log file should be examined periodically for unsuccessful logon attempts. Numerous logon failures could represent a possible attack and should be examined further.

What could the vendor do to fix the vulnerability?

- Require complex passwords for all remote logins
- Require a lockout policy.
- Require logging of logon failures. And build in an intrusion detection system that alerts an administrator whenever there are a large number of logon failures within a short amount of time. When logging is enabled the IP address of the client should also be recorded.

- Require that all passwords passed between client and server be encrypted.

- Manage the error responses from a Windows 2000/XP system, so that it is difficult to remotely determine if an account has been temporarily locked out.
- Correct the Denial of Service attack which is possible by sending a string of packets with the [SYN] flag set to a Windows 2000/XP computer with port 445/tcp enabled.

Source Code/Pseudo Code

The source code for the open-source VNC application (edition 3.3.3.9) can be found at the URL: http://www.uk.research.att.com/vnc/download.html .

VNCHooks.dll – VNC Server component

omnithread_rt.dll – VNC Server component

explorer.exe – the renamed VNC server

Psexec.exe is a freeware remote process execution utility by SysInternals. At the time of this writing the source code for it was unavailable.

After searching a number of sites including:
http://www.ussrback.com,
http://www.packetstormsecurity.org,
http://www.resonantcoderz.com/
http://www.virusexchange.org
http://www.coderz.com
and several web search engines, it was determined that the source code and pseudo code for the following main Deloder routines were unobtainable at the time of this writing:

rundll32.exe – IRC client

cygwin1.dll – a component required by rundll32.exe the IRC client

inst.exe – backdoor Trojan installer

dvldr32.exe – Worm/Trojan package file

Additional Information

Storage Networking Industry Association. Internet Engineering Task Force (IETF). “The Common Internet File System (CIFS) Technical Reference.” Revision 1.0. March 2002, http://www.snia.org/tech_activities/CIFS/CIFS-TR-1p00_FINAL.pdf (25 Mar. 2003)

Hobbit, “CIFS: Common Insecurities Fail Scrutiny.” Avain Research. Jan. 1997. URL: http://web.textfiles.com/hacking/cifs.txt (5 Apr. 2003)

Klevin, John. “CIFS Explained.” CodeFX. 2001. URL: http://www.codefx.com/CIFS_Explained.pdf (25 Mar. 2003)

Overton, David. “Get Easy Registry Access.” 16 Aug. 2000, URL: http://planet-source-code.com (24 Apr. 2003)

Richard Sharpe, “Just what is SMB ?”. V1.2 . 8 Oct. 2002. URL: http://samba.anu.edu.au/cifs/docs/what-is-smb.html (25 Mar. 2003)

Russinovich, Mark. “PsExec.” “Sysinternals Freeware – Utilities for Windows NT and Windows 2000.” Sysinternals. 26 Apr. 2002. URL: http://www.sysinternals.com/ntw2k/freeware/psexec.shtml (21 Apr. 2003)

Lai, Kyle. “Deloder Worm/Trojan Analysis (Deloder-A).” version 1.1. KLC Consulting, Inc. 11 Mar. 2003. URL: http://www.klcconsulting.net/deloder_worm.html (12 Mar. 2003)

Lai, Kyle. “Deloder worm loads VNC and its password, watch out…” KLC Consulting, Inc. 27 Mar. 2003. URL: http://www.klcconsulting.net/articles/deloder/deloder_loads_vnc_password.pdf (10 May. 2003)

McAfee Security. “W32/Deloder.worm.” “Virus Information Library.” 9 Mar. 2003. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=100127.htm (11 Apr. 2003)

McAfee Security. “IRC-Pitchfork.” “AVERT Research Center.” 12 Mar. 2003. URL: http://vil.nai.com/vil/content/v_100129.htm (17 Mar. 2003)

McAfee Security. “BackDoor-ARG.” “AVERT Research Center.” 12 Mar. 2003. URL: http://vil.nai.com/vil/content/v_100128.htm (17 Mar. 2003)

McAfee Security. “RemoteAdmin.svr application.” “AVERT Research Center.” 11 Apr. 2003. URL: http://vil.nai.com/vil/content/v_100246.htm (21 Apr. 2003)

TrendMicro. “WORM_DELODER.A.” “Virus Encyclopedia.” 9 Mar. 2003. URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DELODER.A&VSect=T (17 Mar. 2003)

F-Secure, “Deloder.” “F-Secure Computer Virus Information Pages.” URL: http://www.f-secure.com/v-descs/deloader.shtml (16 Apr. 2003)

Symantec, “W32.HLLW.Deloder.” “Symantec Security Response.” URL: http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.hllw.deloder.html (17 Mar. 2003)

Sensible Security Solutions. “W32.HLLW.Deloder Virus Information.” URL: http://www.sss.ca/sensible/home.nsf/docbyid/C2E6210F37A759FC85256CE40064B094?OpenDocument (22 Apr. 2003)

FRISK Software International. “W32/HLLW.Deloder.” URL: http://www.f-prot.com/virusinfo/descriptions/hllw_deloder_A.html (22 Apr. 2003)

SOPHOS. “W32/Deloder-A.” URL: http://www.sophos.com/virusinfo/analyses/w32delodera.html (14 Apr. 2003)

Carnegie Mellon Software Engineering Institute. “CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares.” 11 Mar. 2003. URL: http://www.cert.org/advisories/CA-2003-08.html (26 Mar. 2003)

Microsoft Corporation, Inc. “Checklist: Create Strong Passwords.” 2 Apr. 2002. URL: http://www.microsoft.com/security/articles/password.asp (10 Apr 2003)

Harbin Institute of Technology & Antiy Labs, “Worm.Dvldr analysis report.” 9 Mar. 2003. URL: http://www.antiy.net/cert/a030308a.htm (16 Apr. 2003)

The Mitre Corporation. “CAN-2002-0283 (under review)”, 02 May 2002, URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0283 (10 Apr. 2003)

The Mitre Corporation. “CVE-2002-0597”, 02 Apr. 2003, URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0597 (10 Apr. 2003)

APPENDIX A Password List

- <no password>
- 0
- 000000
- 00000000
- 007
- 1
- 110
- 111
- 111111
- 11111111
- 12
- 121212
- 123
- 123123
- 1234
- 12345
- 123456
- 1234567
- 12345678
- 123456789
- 1234qwer
- 123abc
- 123asd
- 123qwe
- 2002
- 2003
- 2600
- 54321
- 654321
- 88888888
- a
- aaa
- abc
- abc123
- abcd
- Admin
- admin
- admin123
- administrator
- alpha
- asdf
- computer
- database
- enable

- foobar
- god
- godblessyou
- home
- ihavenopass
- Internet
- Login
- login
- love
- mypass
- mypass123
- mypc
- mypc123
- oracle
- owner
- pass
- passwd
- Password
- password
- pat
- patrick
- pc
- pw
- pw123
- pwd
- qwer
- root
- secret
- server
- sex
- super
- sybase
- temp
- temp123
- test
- test123
- win
- xp
- xxx
- yxcv
- zxcv

APPENDIX B Enum Example

This is an illustration which demonstrates enum as a brute-force dictionary password crack. For this example the password for the Administrator account on the Windows 2000 system was set to "*admin".* The 85 passwords from the Deloder worm's password list were entered into the dictionary file dictfile.txt. The following command could be used to perform the dictionary attack:

enum –D –u Administrator –f dictfile.txt *target_host_IP_address*

And the output would look like the following:

username: Administrator
dictfile: dictfile.txt
server: *target_host_IP_address*
connected as VSLAPTOP-2K\Administrator, disconnecting... success.

(1) Administrator |
return 1326, Logon failure: unknown user name or bad password.

(2) Administrator | 0
return 1326, Logon failure: unknown user name or bad password.

(3) Administrator | 000000
return 1326, Logon failure: unknown user name or bad password.

(4) Administrator | 00000000
return 1326, Logon failure: unknown user name or bad password.

(5) Administrator | 007
return 1326, Logon failure: unknown user name or bad password.

(6) Administrator | 1
return 1326, Logon failure: unknown user name or bad password.

(7) Administrator | 110
return 1326, Logon failure: unknown user name or bad password.

(8) Administrator | 111
return 1326, Logon failure: unknown user name or bad password.

(9) Administrator | 111111
return 1326, Logon failure: unknown user name or bad password.

(10) Administrator | 11111111
return 1326, Logon failure: unknown user name or bad password.

(11) Administrator | 12
return 1326, Logon failure: unknown user name or bad password.

(12) Administrator | 121212
return 1326, Logon failure: unknown user name or bad password.

(13) Administrator | 123
return 1326, Logon failure: unknown user name or bad password.

(14) Administrator | 123123
return 1326, Logon failure: unknown user name or bad password.

(15) Administrator | 1234
return 1326, Logon failure: unknown user name or bad password.

(16) Administrator | 12345

return 1326, Logon failure: unknown user name or bad password.

(17) Administrator | 123456
return 1326, Logon failure: unknown user name or bad password.

(18) Administrator | 1234567
return 1326, Logon failure: unknown user name or bad password.

(19) Administrator | 12345678
return 1326, Logon failure: unknown user name or bad password.

(20) Administrator | 123456789
return 1326, Logon failure: unknown user name or bad password.

(21) Administrator | 1234qwer
return 1326, Logon failure: unknown user name or bad password.

(22) Administrator | 123abc
return 1326, Logon failure: unknown user name or bad password.

(23) Administrator | 123asd
return 1326, Logon failure: unknown user name or bad password.

(24) Administrator | 123qwe
return 1326, Logon failure: unknown user name or bad password.

(25) Administrator | 2002
return 1326, Logon failure: unknown user name or bad password.

(26) Administrator | 2003
return 1326, Logon failure: unknown user name or bad password.

(27) Administrator | 2600
return 1326, Logon failure: unknown user name or bad password.

(28) Administrator | 54321
return 1326, Logon failure: unknown user name or bad password.

(29) Administrator | 654321
return 1326, Logon failure: unknown user name or bad password.

(30) Administrator | 88888888
return 1326, Logon failure: unknown user name or bad password.

(31) Administrator | a
return 1326, Logon failure: unknown user name or bad password.

(32) Administrator | aaa
return 1326, Logon failure: unknown user name or bad password.

(33) Administrator | abc
return 1326, Logon failure: unknown user name or bad password.

(34) Administrator | abc123
return 1326, Logon failure: unknown user name or bad password.

(35) Administrator | abcd
return 1326, Logon failure: unknown user name or bad password.

(36) Administrator | Admin
return 1326, Logon failure: unknown user name or bad password.

(37) Administrator | admin
password found: admin

APPENDIX C Example MS Visual C++ Routine

This routine was obtained from http://www.planet-source-code.com and was submitted by David Overton. It is a subroutine which will create a registry key and is written in C.

```
// Creates a key specified by pszSubKey - you can't create
// keys directly under HKEY_LOCAL_MACHINE in Windows NT or 2000
// just for an extra bit of info.
bool CRegistry::CreateKey(HKEY hKeyRoot, LPCTSTR pszSubKey)
{
   HKEY hKey;
   DWORD dwFunc;
   LONG  lRet;

   lRet = RegCreateKeyEx(
      hKeyRoot,
      pszSubKey,
      0,
      (LPTSTR)NULL,
      REG_OPTION_NON_VOLATILE,
      KEY_WRITE,
      (LPSECURITY_ATTRIBUTES)NULL,
      &hKey,
      &dwFunc
   );

   if(lRet==ERROR_SUCCESS) {

      RegCloseKey(hKey);
      hKey = (HKEY)NULL;

      return true;
   }

   SetLastError((DWORD)lRet);
   return false;
}
```

APPENDIX D Security Log Listing

This table is the Security Log from a Windows 2000 system after logon failures had been enabled. An automated password attack was performed on a test network using a brute-force password crack program. Upon examining the security log it is easy to note that therein lies a listing of a hundred or so logon failures within a time interval of a minute or two. This type of activity of quick logon/logoff failures indicates an automated password crack attempt. Note that the client name of the computer performing the attack is given.

Type	Date	Time	Source	Category	Event	User	Computer
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:30 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id

Audit							
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id

Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:29 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id

Audit							
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id
Failure Audit	5/4/2003	6:31:28 PM	Security	Logon/Logoff	529	SYSTEM	victim_id

APPENDIX E Sample Attack Attempt Logs

This log was recorded on 4/13/03 by Ethereal on a Windows 2000 system. The attacker was 10.1.1.10 and the target was 10.1.1.4. The data was copied into Excel for formatting purposes.

No.	Time	Source	Destination	Prot	Info
80	2260.4404	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [SYN] Seq=1516704752 Ack=0 Win=16384 Len=0
81	2260.4942	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [SYN, ACK] Seq=3198658100 Ack=1516704753 Win=17520 Len=0
82	2260.5603	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516704753 Ack=3198658101 Win=17520 Len=0
83	2260.5662	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
84	2260.5674	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
85	2260.6361	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
86	2260.6376	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
87	2260.6736	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
88	2260.6783	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
89	2260.7058	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
90	2260.7060	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
91	2260.7149	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
92	2260.7160	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
93	2260.7428	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516705619 Ack=3198658846 Win=16775 Len=0
94	2260.7552	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
95	2260.7857	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
96	2260.8487	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
97	2260.8489	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
98	2260.8534	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
99	2260.8546	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
100	2260.9410	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516706180 Ack=3198659213 Win=16408 Len=0
101	2260.9463	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
102	2260.9486	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE

103	2260.9874	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
104	2260.9876	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
105	2260.9951	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
106	2260.9962	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
107	2261.0611	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516706741 Ack=3198659580 Win=17520 Len=0
108	2261.0734	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
109	2261.1051	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
110	2261.1242	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
111	2261.1244	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
112	2261.1349	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
113	2261.1360	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
114	2261.1624	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516707302 Ack=3198659947 Win=17153 Len=0
115	2261.1674	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
116	2261.1696	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
117	2261.2309	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
118	2261.2310	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
119	2261.2359	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
120	2261.2370	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
121	2261.2609	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516707863 Ack=3198660314 Win=16786 Len=0
122	2261.2660	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
123	2261.2682	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
124	2261.2966	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
125	2261.2967	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
126	2261.3132	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
127	2261.3143	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
128	2261.3539	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516708424 Ack=3198660681 Win=16419 Len=0
129	2261.3667	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
130	2261.4239	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
131	2261.4459	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request

132	2261.4461	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
133	2261.4571	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
134	2261.4583	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
135	2261.4809	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516708985 Ack=3198661048 Win=17520 Len=0
136	2261.4885	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
137	2261.4908	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
138	2261.5706	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
139	2261.5708	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
140	2261.5817	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
141	2261.5828	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
142	2261.6328	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516709546 Ack=3198661415 Win=17153 Len=0
143	2261.6425	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
144	2261.6448	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
145	2261.7008	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
146	2261.7121	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
147	2261.7123	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [ACK] Seq=3198661454 Ack=1516710107 Win=17309 Len=0
148	2261.7130	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
149	2261.7145	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
150	2261.7393	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516710107 Ack=3198661782 Win=16786 Len=0
151	2261.7486	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
152	2261.7511	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
153	2261.8223	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
154	2261.8225	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
155	2261.8276	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
156	2261.8288	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
157	2261.8487	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516710668 Ack=3198662149 Win=16419 Len=0
158	2261.8697	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
159	2261.8720	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE

160	2261.9487	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
161	2261.9489	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
162	2261.9598	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
163	2261.9922	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
164	2262.0376	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516711229 Ack=3198662516 Win=17520 Len=0
165	2262.0429	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
166	2262.0457	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
167	2262.0719	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
168	2262.0722	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
169	2262.0770	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
170	2262.0783	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
171	2262.1567	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516711790 Ack=3198662883 Win=17153 Len=0
172	2262.1649	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
173	2262.1672	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
174	2262.1949	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
175	2262.1951	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
176	2262.2108	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
177	2262.2119	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
178	2262.2582	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516712351 Ack=3198663250 Win=16786 Len=0
179	2262.2682	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
180	2262.2705	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
181	2262.2904	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
182	2262.2906	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
183	2262.3039	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
184	2262.3672	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
185	2262.3966	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516712912 Ack=3198663617 Win=16419 Len=0
186	2262.4021	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
187	2262.4047	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
188	2262.4715	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request

189	2262.4717	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
190	2262.4778	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
191	2262.4790	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
192	2262.5009	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516713473 Ack=3198663984 Win=17520 Len=0
193	2262.5192	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
194	2262.5214	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
195	2262.5622	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
196	2262.5624	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
197	2262.5669	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
198	2262.5680	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
199	2262.6132	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516714034 Ack=3198664351 Win=17153 Len=0
200	2262.6349	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
201	2262.6747	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
202	2262.7330	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
203	2262.7332	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
204	2262.7380	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
205	2262.7393	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
206	2262.7629	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516714595 Ack=3198664718 Win=16786 Len=0
207	2262.7751	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
208	2262.7775	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
209	2262.8410	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
210	2262.8412	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
211	2262.8612	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
212	2262.8624	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
213	2262.8821	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516715156 Ack=3198665085 Win=16419 Len=0
214	2262.8931	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
215	2262.8954	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
216	2262.9345	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request

217	2262.9388	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
218	2262.9389	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [ACK] Seq=3198665124 Ack=1516715717 Win=16748 Len=0
219	2262.9608	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
220	2262.9622	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
221	2263.0454	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516715717 Ack=3198665452 Win=17520 Len=0
222	2263.0584	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
223	2263.0610	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
224	2263.1401	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
225	2263.1403	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
226	2263.1525	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
227	2263.1538	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
228	2263.1738	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516716278 Ack=3198665819 Win=17153 Len=0
229	2263.1876	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
230	2263.1899	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
231	2263.2644	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
232	2263.2733	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
233	2263.2810	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
234	2263.2946	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
235	2263.3120	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516716839 Ack=3198666186 Win=16786 Len=0
236	2263.3583	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
237	2263.3607	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
238	2263.3870	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
239	2263.3872	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
240	2263.4198	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
241	2263.4209	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
242	2263.4687	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
243	2263.4710	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
244	2263.5199	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
245	2263.5201	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid

246	2263.5462	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
247	2263.5870	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
248	2263.6171	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516717961 Ack=3198666920 Win=17520 Len=0
249	2263.6673	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
250	2263.6699	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
251	2263.7606	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
252	2263.7608	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
253	2263.7657	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
254	2263.7669	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
255	2263.7866	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516718522 Ack=3198667287 Win=17153 Len=0
256	2263.8225	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
257	2263.8248	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
258	2263.8622	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
259	2263.8671	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
260	2263.8700	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
261	2263.8715	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
262	2263.9647	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516719083 Ack=3198667654 Win=16786 Len=0
263	2263.9813	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
264	2263.9839	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
265	2264.0732	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
266	2264.0734	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
267	2264.0854	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
268	2264.0867	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
269	2264.1132	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516719644 Ack=3198668021 Win=16419 Len=0
270	2264.1216	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
271	2264.1821	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
272	2264.2412	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
273	2264.2415	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid

274	2264.2520	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
275	2264.2534	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
276	2264.3102	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516720205 Ack=3198668388 Win=17520 Len=0
277	2264.3191	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
278	2264.3216	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
279	2264.3845	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
280	2264.3847	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
281	2264.4068	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
282	2264.4079	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
283	2264.4388	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516720766 Ack=3198668755 Win=17153 Len=0
284	2264.4477	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
285	2264.4769	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
286	2264.5046	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
287	2264.5049	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
288	2264.5244	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
289	2264.5255	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
290	2264.5829	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516721327 Ack=3198669122 Win=16786 Len=0
291	2264.6184	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
292	2264.6206	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
293	2264.7248	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
294	2264.7421	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
295	2264.7708	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
296	2264.7723	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
297	2264.8113	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
298	2264.8139	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
299	2264.9149	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
300	2264.9151	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
301	2264.9201	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE

302	2264.9212	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
303	2264.9467	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516722449 Ack=3198669856 Win=17520 Len=0
304	2264.9566	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
305	2264.9588	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
306	2265.0165	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
307	2265.0233	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
308	2265.0344	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
309	2265.0559	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
310	2265.0737	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516723010 Ack=3198670223 Win=17153 Len=0
311	2265.0820	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
312	2265.0846	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
313	2265.1164	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
314	2265.1166	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
315	2265.1289	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
316	2265.1301	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
317	2265.1687	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516723571 Ack=3198670590 Win=16786 Len=0
318	2265.1796	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
319	2265.1820	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
320	2265.2143	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
321	2265.2144	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
322	2265.2239	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
323	2265.2249	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
324	2265.2506	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516724132 Ack=3198670957 Win=16419 Len=0
325	2265.2907	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
326	2265.2929	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
327	2265.3228	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
328	2265.3303	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
329	2265.3305	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [ACK] Seq=3198670996 Ack=1516724693 Win=16187 Len=0

330	2265.3358	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
331	2265.3683	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
332	2265.4102	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516724693 Ack=3198671324 Win=17520 Len=0
333	2265.4153	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
334	2265.4179	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
335	2265.4406	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
336	2265.4407	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
337	2265.4467	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
338	2265.4478	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
339	2265.4920	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516725254 Ack=3198671691 Win=17153 Len=0
340	2265.5022	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
341	2265.5044	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
342	2265.5257	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
343	2265.5259	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
344	2265.5435	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
345	2265.5446	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
346	2265.5669	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516725815 Ack=3198672058 Win=16786 Len=0
347	2265.5778	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
348	2265.5800	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
349	2265.6152	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
350	2265.6154	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
351	2265.6249	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
352	2265.6259	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
353	2265.6494	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516726376 Ack=3198672425 Win=16419 Len=0
354	2265.6542	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
355	2265.6822	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
356	2265.7122	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
357	2265.7125	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
358	2265.7170	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE

359	2265.7185	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
360	2265.7735	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516726937 Ack=3198672792 Win=17520 Len=0
361	2265.7830	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
362	2265.7856	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
363	2265.8111	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
364	2265.8112	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
365	2265.8266	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
366	2265.8277	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
367	2265.8525	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516727498 Ack=3198673159 Win=17153 Len=0
368	2265.8636	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
369	2265.8659	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
370	2265.9090	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
371	2265.9092	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
372	2265.9312	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
373	2265.9323	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
374	2265.9523	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516728059 Ack=3198673526 Win=16786 Len=0
375	2265.9644	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
376	2265.9666	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
377	2266.0023	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
378	2266.0076	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
379	2266.0078	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [ACK] Seq=3198673565 Ack=1516728620 Win=17309 Len=0
380	2266.0234	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
381	2266.0248	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
382	2266.1010	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516728620 Ack=3198673893 Win=16419 Len=0
383	2266.1129	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
384	2266.1155	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
385	2266.1563	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
386	2266.1565	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid

387	2266.1624	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
388	2266.1636	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
389	2266.1925	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516729181 Ack=3198674260 Win=17520 Len=0
390	2266.1984	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
391	2266.2007	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
392	2266.2467	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
393	2266.2469	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
394	2266.2523	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
395	2266.2534	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
396	2266.3603	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516729742 Ack=3198674299 Win=17481 Len=0
397	2266.6171	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
398	2266.6615	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
399	2266.6643	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
400	2266.6971	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
401	2266.6973	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
402	2266.7074	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
403	2266.7086	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
404	2266.7459	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516730303 Ack=3198674994 Win=16786 Len=0
405	2266.7582	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
406	2266.7605	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
407	2266.8254	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
408	2266.8255	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
409	2266.8301	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
410	2266.8312	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
411	2266.8625	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516730864 Ack=3198675361 Win=16419 Len=0
412	2266.8751	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
413	2266.8773	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE

414	2266.9146	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
415	2266.9149	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
416	2266.9252	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
417	2266.9466	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
418	2266.9640	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516731425 Ack=3198675728 Win=17520 Len=0
419	2267.0450	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
420	2267.0477	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
421	2267.1109	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
422	2267.1111	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
423	2267.1157	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
424	2267.1169	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
425	2267.2221	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516731986 Ack=3198676095 Win=17153 Len=0
426	2267.2297	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
427	2267.2698	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
428	2267.2934	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
429	2267.2936	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
430	2267.3036	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
431	2267.3049	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
432	2267.3223	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516732547 Ack=3198676462 Win=16786 Len=0
433	2267.3337	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
434	2267.3360	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
435	2267.4287	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
436	2267.4288	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
437	2267.4395	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
438	2267.4406	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
439	2267.4608	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516733108 Ack=3198676829 Win=16419 Len=0
440	2267.4720	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
441	2267.4742	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
442	2267.5178	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request

443	2267.5250	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
444	2267.5252	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [ACK] Seq=3198676868 Ack=1516733669 Win=17309 Len=0
445	2267.5390	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
446	2267.5633	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
447	2267.5958	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516733669 Ack=3198677196 Win=17520 Len=0
448	2267.6312	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
449	2267.6340	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
450	2267.7012	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
451	2267.7013	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
452	2267.7636	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
453	2267.7648	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
454	2267.8279	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
455	2267.8496	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
456	2267.9688	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
457	2267.9690	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
458	2268.0252	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
459	2268.0264	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
460	2268.0994	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
461	2268.1402	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
462	2268.3496	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516735141 Ack=3198677969 Win=16747 Len=0
463	2268.4640	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
464	2268.4642	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [ACK] Seq=3198677969 Ack=1516735141 Win=17520 Len=0
465	2268.7535	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
466	2268.7539	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
467	2268.7553	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
468	2268.8262	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516735352 Ack=3198678297 Win=16419 Len=0
469	2268.8315	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH

470	2268.8340	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
471	2268.8580	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
472	2268.8581	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
473	2268.8641	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
474	2268.8652	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
475	2268.8866	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516735913 Ack=3198678664 Win=17520 Len=0
476	2268.8938	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
477	2268.9210	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
478	2268.9404	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
479	2268.9407	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
480	2268.9498	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
481	2268.9511	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
482	2268.9824	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516736474 Ack=3198679031 Win=17153 Len=0
483	2268.9884	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
484	2268.9908	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
485	2269.0817	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
486	2269.0819	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
487	2269.0867	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
488	2269.0880	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
489	2269.1139	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516737035 Ack=3198679398 Win=16786 Len=0
490	2269.1191	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
491	2269.1214	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
492	2269.1453	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
493	2269.1455	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
494	2269.1778	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
495	2269.2278	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
496	2269.2486	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516737596 Ack=3198679765 Win=16419 Len=0
497	2269.2541	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH

498	2269.2590	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
499	2269.3311	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
500	2269.3314	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
501	2269.3371	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
502	2269.3384	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
503	2269.3788	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516738157 Ack=3198680132 Win=17520 Len=0
504	2269.3858	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
505	2269.3882	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
506	2269.4141	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
507	2269.4143	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
508	2269.4185	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
509	2269.4196	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
510	2269.4523	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516738718 Ack=3198680499 Win=17153 Len=0
511	2269.4590	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
512	2269.4614	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
513	2269.5061	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
514	2269.5063	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
515	2269.5129	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
516	2269.5716	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
517	2269.6326	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516739279 Ack=3198680866 Win=16786 Len=0
518	2269.6448	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
519	2269.6475	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
520	2269.7186	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
521	2269.7188	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
522	2269.7253	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
523	2269.7266	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
524	2269.8045	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516739840 Ack=3198681233 Win=16419 Len=0
525	2269.8087	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH

526	2269.8111	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
527	2269.8982	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
528	2269.8986	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
529	2269.9154	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
530	2269.9167	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
531	2269.9377	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516740401 Ack=3198681600 Win=17520 Len=0
532	2269.9497	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
533	2269.9521	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
534	2269.9947	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
535	2269.9949	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
536	2270.0060	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
537	2270.0071	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
538	2270.0268	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516740962 Ack=3198681967 Win=17153 Len=0
539	2270.0611	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
540	2270.0636	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
541	2270.0942	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
542	2270.0944	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
543	2270.1403	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
544	2270.1654	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
545	2270.2029	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
546	2270.2056	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
547	2270.2770	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
548	2270.2771	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
549	2270.3010	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [FIN, ACK] Seq=1516741916 Ack=3198682412 Win=16708 Len=0
550	2270.3012	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1267 [FIN, ACK] Seq=3198682412 Ack=1516741917 Win=17477 Len=0
551	2270.3385	10.1.1.10	10.1.1.4	TCP	1267 > microsoft-ds [ACK] Seq=1516741917 Ack=3198682413 Win=16708 Len=0
552	2270.3467	10.1.1.10	10.1.1.4	TCP	1279 > microsoft-ds [SYN] Seq=1520479930 Ack=0 Win=16384 Len=0

553	2270.3469	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1279 [SYN, ACK] Seq=3200967252 Ack=1520479931 Win=17520 Len=0
554	2270.3952	10.1.1.10	10.1.1.4	TCP	1279 > microsoft-ds [ACK] Seq=1520479931 Ack=3200967253 Win=17520 Len=0
555	2270.4117	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
556	2270.4127	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
557	2270.4483	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
558	2270.4778	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
559	2270.5307	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
560	2270.5333	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
561	2270.5727	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
562	2270.5729	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
563	2270.6235	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
564	2270.6247	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
565	2270.6659	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
566	2270.6696	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
567	2270.7575	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
568	2270.7579	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
569	2270.8419	10.1.1.10	10.1.1.4	TCP	1279 > microsoft-ds [FIN, ACK] Seq=1520481190 Ack=3200968076 Win=16697 Len=0
570	2270.8422	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1279 [FIN, ACK] Seq=3200968076 Ack=1520481191 Win=16261 Len=0
571	2270.8941	10.1.1.10	10.1.1.4	TCP	1279 > microsoft-ds [ACK] Seq=1520481191 Ack=3200968077 Win=16697 Len=0
572	2271.1269	10.1.1.10	10.1.1.4	TCP	1286 > microsoft-ds [SYN] Seq=1521051270 Ack=0 Win=16384 Len=0
573	2271.1272	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1286 [SYN, ACK] Seq=3201177750 Ack=1521051271 Win=17520 Len=0
574	2271.1893	10.1.1.10	10.1.1.4	TCP	1286 > microsoft-ds [ACK] Seq=1521051271 Ack=3201177751 Win=17520 Len=0
575	2271.2329	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
576	2271.2340	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
577	2271.2654	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
578	2271.2667	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED

579	2271.3033	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
580	2271.3337	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
581	2271.3663	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
582	2271.3665	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
583	2271.3968	10.1.1.10	10.1.1.4	TCP	1286 > microsoft-ds [FIN, ACK] Seq=1521051969 Ack=3201178207 Win=17064 Len=0
584	2271.3970	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1286 [FIN, ACK] Seq=3201178207 Ack=1521051970 Win=16822 Len=0
585	2271.4148	10.1.1.10	10.1.1.4	TCP	1286 > microsoft-ds [ACK] Seq=1521051970 Ack=3201178208 Win=17064 Len=0
586	2271.5548	10.1.1.10	10.1.1.4	TCP	1293 > microsoft-ds [SYN] Seq=1521457339 Ack=0 Win=16384 Len=0
587	2271.5550	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1293 [SYN, ACK] Seq=3201340208 Ack=1521457340 Win=17520 Len=0
588	2271.6135	10.1.1.10	10.1.1.4	TCP	1293 > microsoft-ds [ACK] Seq=1521457340 Ack=3201340209 Win=17520 Len=0
589	2271.6346	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
590	2271.6358	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
591	2271.6586	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
592	2271.6598	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
593	2271.6993	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
594	2271.7017	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
595	2271.7605	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
596	2271.7606	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
597	2271.8071	10.1.1.10	10.1.1.4	TCP	1293 > microsoft-ds [FIN, ACK] Seq=1521458038 Ack=3201340665 Win=17064 Len=0
598	2271.8073	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1293 [FIN, ACK] Seq=3201340665 Ack=1521458039 Win=16822 Len=0
599	2271.8227	10.1.1.10	10.1.1.4	TCP	1293 > microsoft-ds [ACK] Seq=1521458039 Ack=3201340666 Win=17064 Len=0
600	2271.8325	10.1.1.10	10.1.1.4	TCP	1297 > microsoft-ds [SYN] Seq=1521740326 Ack=0 Win=16384 Len=0
601	2271.8328	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1297 [SYN, ACK] Seq=3201436741 Ack=1521740327 Win=17520 Len=0
602	2271.8508	10.1.1.10	10.1.1.4	TCP	1297 > microsoft-ds [ACK] Seq=1521740327 Ack=3201436742 Win=17520 Len=0
603	2271.8741	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
604	2271.8839	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response

605	2271.9503	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
606	2271.9518	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
607	2271.9851	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
608	2271.9875	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
609	2272.0292	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
610	2272.0294	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
611	2272.0751	10.1.1.10	10.1.1.4	TCP	1297 > microsoft-ds [FIN, ACK] Seq=1521741025 Ack=3201437198 Win=17064 Len=0
612	2272.0753	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1297 [FIN, ACK] Seq=3201437198 Ack=1521741026 Win=16822 Len=0
613	2272.0804	10.1.1.10	10.1.1.4	TCP	1301 > microsoft-ds [SYN] Seq=1521971538 Ack=0 Win=16384 Len=0
614	2272.0806	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1301 [SYN, ACK] Seq=3201524266 Ack=1521971539 Win=17520 Len=0
615	2272.0929	10.1.1.10	10.1.1.4	TCP	1297 > microsoft-ds [ACK] Seq=1521741026 Ack=3201437199 Win=17064 Len=0
616	2272.0981	10.1.1.10	10.1.1.4	TCP	1301 > microsoft-ds [ACK] Seq=1521971539 Ack=3201524267 Win=17520 Len=0
617	2272.1110	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
618	2272.1121	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
619	2272.1376	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
620	2272.1967	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
621	2272.2908	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
622	2272.2935	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
623	2272.3911	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
624	2272.3913	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
625	2272.4138	10.1.1.10	10.1.1.4	TCP	1301 > microsoft-ds [FIN, ACK] Seq=1521972237 Ack=3201524723 Win=17064 Len=0
626	2272.4140	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1301 [FIN, ACK] Seq=3201524723 Ack=1521972238 Win=16822 Len=0
627	2272.4652	10.1.1.10	10.1.1.4	TCP	1301 > microsoft-ds [ACK] Seq=1521972238 Ack=3201524724 Win=17064 Len=0
628	2272.4738	10.1.1.10	10.1.1.4	TCP	1305 > microsoft-ds [SYN] Seq=1522283999 Ack=0 Win=16384 Len=0

629	2272.4740	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1305 [SYN, ACK] Seq=3201668050 Ack=1522284000 Win=17520 Len=0
630	2272.4925	10.1.1.10	10.1.1.4	TCP	1305 > microsoft-ds [ACK] Seq=1522284000 Ack=3201668051 Win=17520 Len=0
631	2272.4992	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
632	2272.5089	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
633	2272.5381	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
634	2272.5396	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
635	2272.5977	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
636	2272.6001	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
637	2272.6260	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
638	2272.6261	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
639	2272.6679	10.1.1.10	10.1.1.4	TCP	1305 > microsoft-ds [FIN, ACK] Seq=1522284698 Ack=3201668507 Win=17064 Len=0
640	2272.6681	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1305 [FIN, ACK] Seq=3201668507 Ack=1522284699 Win=16822 Len=0
641	2272.6840	10.1.1.10	10.1.1.4	TCP	1305 > microsoft-ds [ACK] Seq=1522284699 Ack=3201668508 Win=17064 Len=0
642	2272.7492	10.1.1.10	10.1.1.4	TCP	1309 > microsoft-ds [SYN] Seq=1522529945 Ack=0 Win=16384 Len=0
643	2272.7495	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1309 [SYN, ACK] Seq=3201778979 Ack=1522529946 Win=17520 Len=0
644	2272.7669	10.1.1.10	10.1.1.4	TCP	1309 > microsoft-ds [ACK] Seq=1522529946 Ack=3201778980 Win=17520 Len=0
645	2272.7875	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
646	2272.8068	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
647	2272.8773	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
648	2272.8786	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
649	2272.9268	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
650	2272.9292	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
651	2272.9617	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
652	2272.9618	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
653	2272.9891	10.1.1.10	10.1.1.4	TCP	1309 > microsoft-ds [FIN, ACK] Seq=1522530644 Ack=3201779436 Win=17064 Len=0

654	2272.9893	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1309 [FIN, ACK] Seq=3201779436 Ack=1522530645 Win=16822 Len=0
655	2272.9971	10.1.1.10	10.1.1.4	TCP	1313 > microsoft-ds [SYN] Seq=1522809643 Ack=0 Win=16384 Len=0
656	2272.9974	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1313 [SYN, ACK] Seq=3201864911 Ack=1522809644 Win=17520 Len=0
657	2273.0439	10.1.1.10	10.1.1.4	TCP	1309 > microsoft-ds [ACK] Seq=1522530645 Ack=3201779437 Win=17064 Len=0
658	2273.0565	10.1.1.10	10.1.1.4	TCP	1313 > microsoft-ds [ACK] Seq=1522809644 Ack=3201864912 Win=17520 Len=0
659	2273.0667	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
660	2273.1025	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
661	2273.1409	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
662	2273.1424	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
663	2273.1672	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
664	2273.1696	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
665	2273.2151	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
666	2273.2152	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
667	2273.2445	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
668	2273.2456	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
669	2273.2748	10.1.1.10	10.1.1.4	TCP	1313 > microsoft-ds [ACK] Seq=1522810510 Ack=3201865657 Win=16775 Len=0
670	2273.2822	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
671	2273.2844	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
672	2273.3207	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
673	2273.3209	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
674	2273.3656	10.1.1.10	10.1.1.4	TCP	1313 > microsoft-ds [FIN, ACK] Seq=1522810903 Ack=3201865735 Win=16697 Len=0
675	2273.3658	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1313 [FIN, ACK] Seq=3201865735 Ack=1522810904 Win=16261 Len=0
676	2273.3752	10.1.1.10	10.1.1.4	TCP	1319 > microsoft-ds [SYN] Seq=1523165547 Ack=0 Win=16384 Len=0
677	2273.3754	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1319 [SYN, ACK] Seq=3201985781 Ack=1523165548 Win=17520 Len=0
678	2273.3862	10.1.1.10	10.1.1.4	TCP	1313 > microsoft-ds [ACK] Seq=1522810904 Ack=3201865736 Win=16697 Len=0

679	2273.3978	10.1.1.10	10.1.1.4	TCP	1319 > microsoft-ds [ACK] Seq=1523165548 Ack=3201985782 Win=17520 Len=0
680	2273.4028	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
681	2273.4151	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
682	2273.4650	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
683	2273.4665	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
684	2273.4996	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
685	2273.5020	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
686	2273.5374	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
687	2273.5376	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
688	2273.5751	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
689	2273.5762	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
690	2273.6178	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
691	2273.6202	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
692	2273.6567	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
693	2273.6569	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
694	2273.7007	10.1.1.10	10.1.1.4	TCP	1319 > microsoft-ds [FIN, ACK] Seq=1523166807 Ack=3201986605 Win=16697 Len=0
695	2273.7010	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1319 [FIN, ACK] Seq=3201986605 Ack=1523166808 Win=16261 Len=0
696	2273.7217	10.1.1.10	10.1.1.4	TCP	1319 > microsoft-ds [ACK] Seq=1523166808 Ack=3201986606 Win=16697 Len=0
697	2273.7342	10.1.1.10	10.1.1.4	TCP	1323 > microsoft-ds [SYN] Seq=1523416546 Ack=0 Win=16384 Len=0
698	2273.7346	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1323 [SYN, ACK] Seq=3202129387 Ack=1523416547 Win=17520 Len=0
699	2273.7579	10.1.1.10	10.1.1.4	TCP	1323 > microsoft-ds [ACK] Seq=1523416547 Ack=3202129388 Win=17520 Len=0
700	2273.7624	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
701	2273.7636	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
702	2273.7871	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
703	2273.7883	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
704	2273.8298	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
705	2273.8323	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE

706	2273.8580	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
707	2273.8582	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
708	2273.8900	10.1.1.10	10.1.1.4	TCP	1323 > microsoft-ds [FIN, ACK] Seq=1523417245 Ack=3202129844 Win=17064 Len=0
709	2273.8901	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1323 [FIN, ACK] Seq=3202129844 Ack=1523417246 Win=16822 Len=0
710	2273.9328	10.1.1.10	10.1.1.4	TCP	1323 > microsoft-ds [ACK] Seq=1523417246 Ack=3202129845 Win=17064 Len=0
711	2274.0067	10.1.1.10	10.1.1.4	TCP	1327 > microsoft-ds [SYN] Seq=1523679502 Ack=0 Win=16384 Len=0
712	2274.0071	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1327 [SYN, ACK] Seq=3202218200 Ack=1523679503 Win=17520 Len=0
713	2274.0268	10.1.1.10	10.1.1.4	TCP	1327 > microsoft-ds [ACK] Seq=1523679503 Ack=3202218201 Win=17520 Len=0
714	2274.0316	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
715	2274.0717	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
716	2274.1424	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
717	2274.1438	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
718	2274.1713	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
719	2274.1738	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
720	2274.2144	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
721	2274.2146	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
722	2274.2331	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
723	2274.2342	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
724	2274.2741	10.1.1.10	10.1.1.4	TCP	1327 > microsoft-ds [ACK] Seq=1523680369 Ack=3202218946 Win=16775 Len=0
725	2274.2795	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
726	2274.2818	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
727	2275.5668	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
728	2275.5669	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1327 [ACK] Seq=3202218985 Ack=1523680719 Win=16304 Len=0
729	2275.6954	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
730	2275.7457	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
731	2275.7459	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
732	2275.7893	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE

733	2275.7906	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
734	2275.8223	10.1.1.10	10.1.1.4	TCP	1327 > microsoft-ds [ACK] Seq=1523680930 Ack=3202219313 Win=16408 Len=0
735	2275.8378	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
736	2275.8402	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
737	2275.9409	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
738	2275.9454	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
739	2275.9745	10.1.1.10	10.1.1.4	TCP	1327 > microsoft-ds [FIN, ACK] Seq=1523681323 Ack=3202219391 Win=16330 Len=0
740	2275.9748	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1327 [FIN, ACK] Seq=3202219391 Ack=1523681324 Win=17477 Len=0
741	2275.9957	10.1.1.10	10.1.1.4	TCP	1327 > microsoft-ds [ACK] Seq=1523681324 Ack=3202219392 Win=16330 Len=0
742	2276.0895	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [SYN] Seq=1525272253 Ack=0 Win=16384 Len=0
743	2276.0897	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1349 [SYN, ACK] Seq=3202732924 Ack=1525272254 Win=17520 Len=0
744	2276.1122	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525272254 Ack=3202732925 Win=17520 Len=0
745	2276.1612	10.1.1.10	10.1.1.4	SMB	Negotiate Protocol Request
746	2276.1623	10.1.1.4	10.1.1.10	SMB	Negotiate Protocol Response
747	2276.2573	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
748	2276.2588	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
749	2276.3066	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
750	2276.3090	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
751	2276.4300	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
752	2276.4302	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
753	2276.4704	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
754	2276.4715	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
755	2276.4952	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525273120 Ack=3202733670 Win=16775 Len=0
756	2276.5278	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
757	2276.5304	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
758	2276.6012	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
759	2276.6014	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid

760	2276.6061	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
761	2276.6073	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
762	2276.6552	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525273681 Ack=3202734037 Win=16408 Len=0
763	2276.6616	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
764	2276.6639	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
765	2276.7667	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
766	2276.7772	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
767	2276.7789	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
768	2276.7803	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
769	2276.8584	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525274242 Ack=3202734404 Win=17520 Len=0
770	2276.8661	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
771	2276.8692	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
772	2276.9831	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
773	2276.9832	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
774	2276.9883	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
775	2276.9894	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
776	2277.0081	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525274803 Ack=3202734771 Win=17153 Len=0
777	2277.0157	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
778	2277.0189	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
779	2277.0692	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
780	2277.0705	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
781	2277.0908	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
782	2277.0923	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
783	2277.1450	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525275348 Ack=3202735138 Win=16786 Len=0
784	2277.1554	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
785	2277.1582	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
786	2277.1908	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
787	2277.1910	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid

788	2277.2170	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
789	2277.2182	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
790	2277.2616	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525275893 Ack=3202735505 Win=16419 Len=0
791	2277.2716	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
792	2277.2746	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
793	2277.3060	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
794	2277.3062	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
795	2277.3417	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
796	2277.3428	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
797	2277.3948	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
798	2277.4155	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
799	2277.4485	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
800	2277.4487	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
801	2277.4624	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
802	2277.4635	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
803	2277.5147	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525276999 Ack=3202736239 Win=17153 Len=0
804	2277.5271	10.1.1.10	10.1.1.4	SMB	Session Setup AndX Request, NTLMSSP_AUTH
805	2277.5294	10.1.1.4	10.1.1.10	SMB	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
806	2277.5816	10.1.1.10	10.1.1.4	SMB	Logoff AndX Request
807	2277.5818	10.1.1.4	10.1.1.10	SMB	Logoff AndX Response, Error: Bad userid
808	2277.6043	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [FIN, ACK] Seq=1525277392 Ack=3202736317 Win=17075 Len=0
809	2277.6045	10.1.1.4	10.1.1.10	TCP	microsoft-ds > 1349 [FIN, ACK] Seq=3202736317 Ack=1525277393 Win=17477 Len=0
810	2277.6251	10.1.1.10	10.1.1.4	TCP	1349 > microsoft-ds [ACK] Seq=1525277393 Ack=3202736318 Win=17075 Len=0