



The University of Texas at San Antonio™

ISCS 3523-003 Intrusion Detection and Incident Response

**Lab #04 Attack Analysis
The SimSpace Cyber Range**

Student:

Dillen Dela Cruz, odv464

*Prepared for Intrusion Detection and Incident Response
04/18/2024
Professor: Shawn Zumwalt*

Contents

Images.....	8
Citations:.....	21

In my initial investigation, I started with the Application log, where I noticed a series of entries related to LoadPerf which stated that description of Event ID 1000 could not be found (figure 1). LoadPerf is for managing performance counters on Windows systems, crucial for monitoring CPU usage, memory usage, disk activity, and network traffic. Additionally, within the same logs, I observed mentions of other services such as RSVP, QoS RSVP, PSched, Remote Access Routing, Routing and Remote Access, TermService, Terminal Services, MSDTC, and WmiApRpl (figure 2). Outside research revealed that if these services are either missing or corrupted, it can lead to significant implications. Network connectivity issues may arise, with disruptions to remote resource access or network service utilization due to problems with services like Remote Access Routing, Routing and Remote Access, or WmiAPRpl. Moreover, performance decline may occur, as critical services responsible for managing network traffic and ensuring quality of service, such as RSVP, PSched, QoS RSVP, and WmiAPRpl, may be compromised or absent, resulting in slower data transfer speeds and increased latency. Additionally, security risks may come up if essential networking, remote access, or management services fail to operate properly, potentially exposing the system to vulnerabilities. Attackers could exploit vulnerabilities to gain unauthorized access, intercept sensitive data, or execute malicious commands remotely. The absence of proper management and monitoring capabilities, particularly from services like WmiAPRpl, could make it challenging to effectively detect and respond to security incidents, furthering the system's vulnerability. In addition, I noticed that descriptions of both Event ID 5603, related to WinManagement, and Event ID 1800 (figure 3), linked to SecurityCenter (figure 4), were also absent in the logs. Similar to what I observed with LoadPerf, other services like RSOP Planning Mode Provider and root/RSOP were mentioned in the WinManagement logs. However, the Security Center logs did not list any additional services. WinMgmt typically refers to the Windows Management Instrumentation service, responsible for managing and controlling Windows operating systems and components. Security Center refers to the Windows Security Center service, which monitors the system's security status, including antivirus software and firewall protection (University Information Technology Services). Entries related to Security Center in the Application log might signal security-related events or issues, such as updates to security settings or alerts about security breaches or vulnerabilities. Finally, another occurrence of this is from Event ID 7, 2, 4, and 1 which the description from source crypt32 cannot be found, which the component that raises this event could be either not be installed on the local computer or the installation is corrupted (figure 7). This suggests that the component responsible for generating these events may either not be installed on the local computer or the installation could be corrupted. Crypt32.dll is a module bundled with Windows and Windows Server operating systems, tasked with implementing numerous cryptographic messaging and certificate functions within the CryptoAPI (Microsoft).

Frequently appearing logs, not just those above, also include those related to Network Configuration, indicating instances of both restoring and not restoring network configurations for adapters, specifically one with the MAC address 00:0C:29:7F:D7:02 (as shown in figure 5). Additionally, there were logs detailing the startup of the database engine, the creation of new

instances, the subsequent stopping of those instances, and ultimately the shutdown of the database engine (as depicted in figure 6).

These observations offer clues that could indicate a compromised system. The absence of event descriptions, particularly for critical services like LoadPerf and SecurityCenter, might signal unauthorized manipulation of event logs by an attacker, aimed at concealing their actions and evading detection by system administrators or security monitoring tools. Additionally, the mention of crypt32.dll, a crucial component responsible for cryptographic functions within the Windows operating system, heightens concern. The lack of event descriptions related to crypt32 raises the possibility of underlying issues with cryptographic operations or security-related events, essential for maintaining data integrity and confidentiality. Potential implications of missing or corrupted services, such as network connectivity issues, performance degradation, and security risks, increase concern about the overall system health and security posture. These issues could potentially expose the system to unauthorized access, data breaches, or other malicious activities organized by attackers.

Next my investigation moves on to the analysis of the Security logs. In the Security log we see the same pattern of description of Events from different sources cannot be found. Here we have it from EventLog, SRService, Setup, W32Time and Print (figure 8). Considering the services currently running, it's recommended that the Simple Service Discovery Protocol (SSDP) should be disabled. SSDP is a network protocol responsible for discovering and advertising network services utilizing the UPnP (Universal Plug n Play) architecture. UPnP presents a security risk due to its capability for automatic discovery and attachment to network devices (Tenable). In a security-conscious environment, it's not recommended for workstations to automatically discover and connect to networked services. As noted by Skyway West, attackers can exploit this vulnerability to launch Denial of Service attacks, overwhelming a victim's server by flooding it with requests. Given this information, let's turn our attention to another service that follows this sequence, the Print Spooler service. It's an important part of the Windows operating system, designed to temporarily store print jobs in the computer's memory until they're ready to be printed (EPSON). If the Print Spooler service is active, it could indicate the presence of a network-connected printer. Additionally, noticing the lack of descriptions for events from the "Print" source in our earlier discussion suggests potential issues with the component responsible for generating these events, either it's missing from the local computer or it's corrupted. Reflecting on our previous conversation about how attackers might exploit this situation to hide their actions and avoid detection by system administrators or security monitoring tools, this printer could potentially serve as an access point for the attacker. the fact that SSDP is typically enabled by default on many systems is potentially exposing them to these risks without users' awareness.

One thing I also found during the security logs are constant Events from the source Tcpip stating that a network adapter was connected to the network and had initiated normal operations (figure 10). This may give us a clue as to when the attacker had gotten into the system and what he has been doing ever since the infiltration. By analyzing the timestamps of these Tcpip events, we can establish a timeline (starting at 7/8/2017) of the attacker's activities, including the initial compromise, movement within the network, and any malicious actions taken on compromised

systems. Considering that W32Time was also affected, experiencing similar issues with events initiated and sourced by that service but lacking descriptions, it's important to be cautious about relying on the accuracy of time synchronization on the compromised system.

Lastly, in the Security log, I came across a warning that TCP/IP had reached the security limit for concurrent TCP connect attempts. This suggests that the system might be facing an unusually high number of TCP connection attempts in a short time frame, possibly hinting malicious activity like network-based attacks, port scanning, or reconnaissance by an attacker. Going over the security limit for TCP connect attempts could affect the availability and performance of network services since legitimate connection requests might be delayed or denied. This limit is in place to safeguard against certain types of network attacks, like SYN flood attacks or other forms of resource exhaustion attacks. In addition to this warning, the logs showed that shortly afterward, an unknown user login was detected, which was the event discussed earlier regarding the network adapter being connected to the network. This sequence of events raises concerns that the attacker may have exploited the network congestion caused by the excessive TCP connection attempts to gain unauthorized access to the system.

After analyzing both the Application and Security logs, I proceeded to examine the network architecture using Network Miner. From the host results in Network Miner, it was evident that the IP address 192.168.134.129 stood out as the potential malicious host, primarily because it was running a Linux OS, which is uncommon in a professional environment (figure 12). Upon further investigation into this IP address, it was found to have one incoming session and six outgoing sessions. The incoming session indicated a significant volume of data being sent, with the network connection initiated by the victim computer, identified as APLOVERS computer, aligning with the time of the warning from the Security Log regarding the TCP/IP reaching the security limit for concurrent TCP connect attempts on 7/8/2017 (figure 13). For the outgoing sessions, four ports were identified: 445, 1000, 135, and 139. Notably, the majority of the packets were sent over a single port, 445 (figure 13). Looking deeper into this I looked at the "Parameters" tab and filtered out the Linux IP (figure 14). The result was many different type of SMB messages. From frame 34-38 we see a lot of SMB Native LAN Manager and SMB Native OS which both are indicates the operating system of the SMB client or server. It seems that the Linux IP is likely performing a port scan to identify potential targets and gather information about their systems. The fact that responses are received suggests that port 445 is open on the target system, which could be the entry point for the attacker. This is further supported by the SMB commands observed in frames 40-102, specifically "Tree Connect AndX Request 23793" and "NT Create AndX Request 23793" (as shown in figure 14). The "Tree Connect" command is used to establish connections to shared resources like folders or printers, while "NT Create" is a request to create or open a file, directory, or device on the remote server, according to Microsoft. Examining the parameter values such as "\\192.168.134.132\\IPC\$", "\\SRVSVC", "\\BROWSER", and "\\SPOOLS", it's likely that these correspond to specific pipes used in the Server Message Block (SMB) protocol. Named pipes, like these, can be helpful for monitoring SMB activity and lateral movement. "\\SRVSVC" is probably linked to the SRVSVC pipe, facilitating communication for server services in SMB. "\\BROWSER" might represent the BROWSER pipe, managing browser service communication and network resource lists (MSRC). Lastly,

"\SPOOLS" may refer to the SPOOLS pipe, which handles print job management and communication between clients and print servers within SMB. A noteworthy point is the value "IPC\$" associated with the first parameter, which, according to Microsoft Learn, is a share created by the Windows Server service, enabling anonymous users to perform certain activities. Another interesting observation is that all these services, except the first one, were running on the compromised computer. Moreover, it was noted that the services SRVSVC and SPOOLS had missing log descriptions. Overall, the findings suggest a potentially successful reconnaissance and exploitation effort targeting the network.






After reviewing my previous discoveries, I turn to Wireshark to inspect the network traffic further. One of my first steps is to analyze the I/O graph for any irregularities, particularly spikes in packet activity. I notice significant increases in packets labeled 711, 1437, and 2211, all within the same TCP stream. Upon closer examination, the data appears to be gibberish or garbage data (figure 16), but a particular phrase catches my attention, "This program cannot be run in DOS mode." This phrase is commonly found in the header of binary executable files on Windows systems. Its presence in the TCP packet data suggests that the packets may contain executable code, hinting at a potential attempt to execute a program or inject code. Given that these packets originate from the previously identified malicious Linux machine, I speculate that it might be running a Buffer Overflow program. Inspecting more of the random strings, I found the words "METERPRETER" (figure 17). Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code (Double Octopus). In addition to the buffer overflow program, I was speculating earlier could also contain instructions to download and execute the Meterpreter payload from an attacker-controlled server.

Next, I examined the Expert Information section for any significant summaries (figure 18). The output revealed the presence of malformed packets originating from a printer. This serves as initial evidence regarding the source of the attack. Upon further investigation of frame 87, two key points emerged. Firstly, the summary indicates "EnumPrinters," suggesting an attempt at enumeration to map out the victim's network and identify vulnerabilities. Secondly, it utilizes the SPOOLS protocol for printer interactions. However, upon closer inspection of figures 19 and 20, it becomes evident that the source is indeed a printer. The TCP frame information clearly identifies the device as the local printer connected to the host computer named APLOVERS. This printer is likely either physically connected to the machine or part of a local network automatically authenticated to the printer. Frame 2310 is the same information that was found in frame 87.

The attacker's strategy involved targeting the printer through an open port (445) on the network, successfully exploiting this entry point to penetrate the system. Leveraging vulnerabilities within the printer's SMB service, they executed a program capable of initiating a buffer overflow and deploying Meterpreter, a potent tool providing an interactive shell for further exploration and code execution within the target machine. Evidence of the attacker's exploitation efforts is reflected in the security logs, where successful login attempts associated with Meterpreter usage were recorded. Additionally, the attacker utilized SMB for various name pipes to facilitate file sharing and establish connections between the compromised printer and

the host computer, as evidenced by parameters extracted from Network Miner, specifically noting SMB Tree and SMB Create. The attacker's success in infiltrating the printer was facilitated by the victim computer's SSDP, which automatically established connections with the printer, potentially without the user's awareness. Once inside the victim's computer, the attacker leveraged higher-priority access to different services, potentially exploiting vulnerabilities and obscuring their actions by manipulating logs, as indicated by the absence of log descriptions. Further analysis of the data stream containing the executable code and references to "METERPRETER" revealed the use of encryption methods like RSA and SHA, suggesting potential data exfiltration activities. The presence of such encryption methods indicates the handling of important data in a specialized manner, potentially involving the extraction and transmission of sensitive information from the compromised system. This could be the reason why crypt32 was tampered with. In conclusion, the attacker's multi-faceted approach, targeting the printer as an entry point and leveraging vulnerabilities within SMB and Meterpreter, underscores the sophistication of their tactics. Through a combination of exploitation, lateral movement, and potential data exfiltration, the attacker posed a significant threat to the victim's security posture. It's clear that the attacker's strategies went beyond simply exploiting vulnerabilities. They demonstrated a deep understanding of system architecture and employed sophisticated methods to infiltrate and manipulate critical components. This high level of sophistication suggests a well-equipped and highly skilled threat actor, possibly operating with specific objectives in mind. Furthermore, their deliberate targeting of system processes and establishment of covert communication channels underscores a strategic approach aimed at long term persistence and data theft.

Images

Level	Date and Time	Source	Event ID	Task Category
 Information	8/6/2016 4:05:15 PM	LoadPerf	1000	None
 Information	8/6/2016 4:05:38 PM	LoadPerf	1000	None
 Information	8/6/2016 4:05:40 PM	LoadPerf	1000	None
 Information	8/6/2016 4:06:54 PM	LoadPerf	1000	None
 Information	8/6/2016 4:06:56 PM	LoadPerf	1000	None

1.

2.

The description for Event ID 1000 from source LoadPerf cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

#SvcP
Root:RSVP

The following information was included with the event:

PSched
PSched

The following information was included with the event:

RemoteAccess
Routing and Remote Access

The following information was included with the event:

TermService
Terminal Services

The following information was included with the event:

MSDTC
MSDTC

The following information was included with the event:

WmiApRpl
WmiApRpl

3.

Event 5803, WmiAgent

General Details

The description for Event ID 5803 from source WmiAgent cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

WmiAgent
root:WMI

The message resource is present but the message was not found in the message table

Log Name: \\.\C:\WINDOWS\system32\WmiAgent\WmiAgent-Application Log.vml
Source: WmiAgent
Event ID: 5803
Level: Warning
User: SYSTEM
OpCode: Info
Log Date: 8/6/2016 4:08:56 PM
Task Category: None
Keywords: Classic
Computer: APLOVERS-769932

4.

The description for Event ID 1000 from source SecurityCenter cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be scraped with the event.

The following information was included with the event:

The message resource is present but the message was not found in the message table

Log Name:	\\SCS-FILE\sharedfiles\Maybe Hacked Box--Application Log.ev		
Source:	SecurityCenter	Logged:	8/8/2016 4:11:52 PM
Event ID:	1000	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	APLOVERS-765952
OpCode:	Info		

More Information: [Event Log Online Help](#)

5.

Event 270, VMUpgradeHelper

General Details

Not restoring network configuration for adapter with MAC address 00:0C:29:7F:D7:02. The device ID for this adapter is unchanged.

Log Name:	\\SCS-FILE\sharedfiles\Maybe Hacked Box--Application Log.ev		
Source:	VMUpgradeHelper	Logged:	8/8/2016 6:04:13 PM
Event ID:	270	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	APLOVERS-765952
OpCode:	Info		

More Information: [Event Log Online Help](#)

wuauctl (1588) The database engine 5.01.2600.5512 started.

6.

Event 102, ESENT

General Details

wuaueng.dll (1588) SUS20ClientDataStore: The database engine (%5,%6,%7,%8) is starting a new instance (%4).

Event 103, ESENT

General Details

wuaueng.dll (1588) SUS20ClientDataStore: The database engine stopped the instance (0).

Dirty Shutdown: %6

Internal Timing Sequence: %5

Event 101, ESENT

General Details

wuauctl (1588) The database engine stopped.

Icon	Time	Source	Level	Category	Task	Keywords	Path
Information	8/6/2016 4:12:47 PM	crypt32	7	None			
Information	8/6/2016 4:12:47 PM	crypt32	2	None			
Information	8/6/2016 4:12:47 PM	crypt32	4	None			
Information	8/6/2016 4:12:47 PM	crypt32	1	None			
Warning	8/6/2016 4:13:15 PM	WinMg...	5603	None			
Warning	8/6/2016 4:13:15 PM	WinMg...	5603	None			
Warning	8/6/2016 4:13:15 PM	WinMg...	5603	None			
Information	8/6/2016 4:13:40 PM	VMTools	105	None			
Information	8/6/2016 4:13:40 PM	LoadPerf	1001	None			

Event 2: crypt32

General Details

The description for Event ID 2 from source crypt32 cannot be found. Other the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

<http://www.microsoft.com/message/00000000-0000-0000-0000-000000000000>

The locale specific resource for the desired message is not present.

Log Name:	\\USCIS-FILE\sharedfiles\Maybe-Hacked-Box--Application Log-ent		
Source:	crypt32	Logged:	8/6/2016 4:12:47 PM
Event ID:	2	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	APR/COVERS-763952
OpCode:	N/A		

More Information: [Event Log Online Help](#)

Event 6011: EventLog

GeneralDetails

The description for Event ID 6011 from source EventLog cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

MACHINENAME
APLOVERS-769952

The message resource is present but the message was not found in the message table

Log Name:	\\SOS-FLEP\sharedfiles\Mayke-Hacked-Rox-Security-Log.txt	
Source:	EventLog	Logged: 8/6/2016 4:05:54 PM
Event ID:	6011	Task Category: None
Level:	Information	Keywords: Classic
User:	N/A	Computer: APLOVERS-769952
OpCode:	Info	

More information: [Event Log Online Help](#)

Event 325: SRService

GeneralDetails

The description for Event ID 325 from source SRService cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

The message-specific resource for the event was not found.

Log Name:	\\SOS-FLEP\sharedfiles\Mayke-Hacked-Rox-Security-Log.txt	
Source:	SRService	Logged: 8/5/2016 4:11:43 PM
Event ID:	325	Task Category: None
Level:	Information	Keywords: Classic
User:	N/A	Computer: APLOVERS-769952
OpCode:	Info	

More information: [Event Log Online Help](#)

Event 20, Print

GeneralDetails

The description for Event ID 20 from source Print cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

TP Output Gateway PS
Windows NT x86
Version 3
PSCRIPT5.DLL, P5SU.DLL, TRPS.PPD, PSCRIPT.HLP, PSCRIPT.MTE, TRPSJNL, TRPS.DLL

The message resource is present but the message was not found in the message table

Log Name: \\SCS-FILE\sharedfiles\Maybe Hacked Box--Security Log.vnt

Source: Print

Event ID: 20

Level: Warning

User: SYSTEM

OpCode: Info

Logged: 8/6/2016 4:13:14 PM

Task Category: None

Keywords: Classic

Computer: APLOVERS-765952

Event 8004, Setup

GeneralDetails

The description for Event ID 8004 from source Setup cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

2600

The locale specific resource for the desired message is not present.

Log Name: \\SCS-FILE\sharedfiles\Maybe Hacked Box--Security Log.vnt

Source: Setup

Event ID: 8004

Level: Information

User: N/A

OpCode: Info

Logged: 8/6/2016 4:10:55 PM

Task Category: None

Keywords: Classic

Computer: APLOVERS-765952

Event 36, W32Time

GeneralDetails

The description for Event ID 36 from source W32Time cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

40152

The message resource is present but the message was not found in the message table

Log Name: \\SCS-FILE\sharedfiles\Maybe Hacked Box--Security Log.vnt

Source: W32Time

Event ID: 36

Level: Warning

User: N/A

OpCode: Info

Logged: 8/7/2016 5:54:14 AM

Task Category: None

Keywords: Classic

Computer: APLOVERS-765952

More Information: [Event Log Online Help](#)

Event 7035, Service Control Manager

GeneralDetails

The SSDP Discovery Service service was successfully sent a start control.

9.

Maybe Hacked Box--Security Log Page 1

Next Page Back to Top

To make this Analytic, Debug or Classic event log easier to navigate and manipulate, first save it in

Level	Date and Time	Source	Event ID	Task Ca...
Information	7/8/2017 1:37:22 PM	EventL...	6009	None
Information	7/8/2017 1:37:22 PM	EventL...	6005	None
Information	7/8/2017 1:37:23 PM	Tcpip	4201	None
Information	7/8/2017 1:37:51 PM	Service...	7035	None
Information	7/8/2017 1:37:51 PM	Service...	7036	None
Information	7/8/2017 1:37:51 PM	Service...	7036	None
Information	7/8/2017 1:37:51 PM	Service...	7035	None

Event 4201, Tcpip

General Details

The system detected that network adapter \DEVICE\TCPIP_{E47E5BF4-CB18-4823-8386-69FDBB9322CA} was connected to the network, and has initiated normal operation.

Log Name: \\ISCS-FILE\sharedfiles\Maybe Hacked Box--Security Log.evt

Source: Tcpip Logged: 7/8/2017 1:37:23 PM

Event ID: 4201 Task Category: None

Level: Information Keywords: Classic

User: N/A Computer: APLOVERS-765952

OpCode: Info

More Information: [Event Log Online Help](#)

10.

Maybe Hacked Box--Security Log Page 1

Next Page Back to T

To make this Analytic, Debug or Classic event log easier to navigate and manipulate, first save

Level	Date and Time	Source	Event ID	Task Ca...
Information	7/8/2017 1:37:51 PM	Service...	7035	None
Information	7/8/2017 1:37:51 PM	Service...	7035	None
Information	7/8/2017 1:37:52 PM	Service...	7036	None
Information	7/8/2017 1:37:57 PM	Service...	7036	None
Information	7/8/2017 1:38:43 PM	Service...	7035	None
Information	7/8/2017 1:38:43 PM	Service...	7036	None
Warning	7/8/2017 2:56:46 PM	Tcpip	4226	None

Event 4226, Tcpip

General Details

TCP/IP has reached the security limit imposed on the number of concurrent TCP connect attempts.

Log Name: \\ISCS-FILE\sharedfiles\Maybe Hacked Box--Security Log.evt

Source: Tcpip Logged: 7/8/2017 2:56:46 PM

Event ID: 4226 Task Category: None

Level: Warning Keywords: Classic

User: N/A Computer: APLOVERS-765952

OpCode: Info

More Information: [Event Log Online Help](#)

11.

-- Select a network adapter in the list --

Hosts (16) Files Images Messages Credentials Sessions (6) DNS (14) Parameters (65) Keywords Anomalies

Sort Hosts On: MAC Address (ascending)

fd3e:4f5a:5b81::1 [dns.msftncsi.com]
 131.107.255.255 [dns.msftncsi.com]
 192.168.134.129 [1NSQhr0LMwH8ZEh3] [bdI4kHD5f5kAzksc] (Linux)
 IP: 192.168.134.129
 MAC: 000C293F2031
 NIC Vendor: VMware, Inc.
 MAC Age: 1/21/2003
 Hostname: 1NSQhr0LMwH8ZEh3, bdI4kHD5f5kAzksc
 OS: Linux
 TTL: 64 (distance: 0)
 Open TCP Ports: 29922
 Sent: 1573 packets (1,712,909 Bytes), 0.00% cleartext (0 of 0 Bytes)
 Received: 585 packets (156,369 Bytes), 0.00% cleartext (0 of 0 Bytes)
 Incoming sessions: 1
 Outgoing sessions: 6
 Host Details
 192.168.134.132 [APLOVERS-765952] (Windows)
 fe80::9431:7662:5ecc:c92f
 192.168.134.158 [WIN-Q10910JGOSC]
 192.168.134.1 [STUDENT28<20>] [STUDENT28]
 65.55.158.118 [onpremy2.ipv6.microsoft.com.akadns.net] [onpremywindows.ipv6.microsoft.com.akadns.net]
 192.168.134.2
 224.0.0.22
 224.0.0.252
 239.255.255.250
 ff02::16
 ff02::1:2
 ff02::1:3
 192.168.134.255

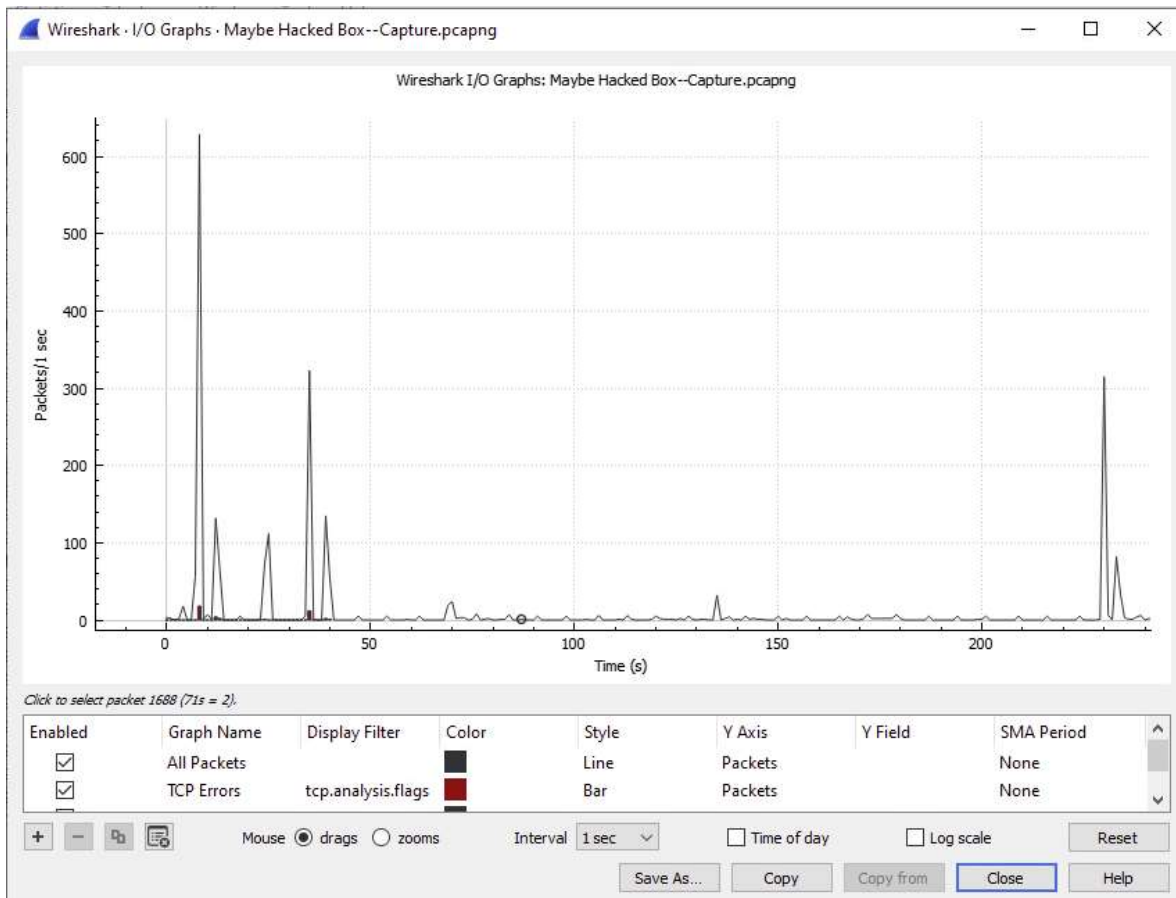
12.

13.

192.168.134.129 [1NSQhr0LMwH8ZEh3] [bdI4kHD5f5kAzksc] (Linux)
 IP: 192.168.134.129
 MAC: 000C293F2031
 NIC Vendor: VMware, Inc.
 MAC Age: 1/21/2003
 Hostname: 1NSQhr0LMwH8ZEh3, bdI4kHD5f5kAzksc
 OS: Linux
 Ethernet: Linux Ethernet (100.00%)
 aB (Packets): Linux 2.6 (kernel: 10) (possibly: 0/0) (100.00%)
 Data: TCP: 1573 packets (1,712,909 Bytes), 0.00% cleartext (0 of 0 Bytes)
 Received: 585 packets (156,369 Bytes), 0.00% cleartext (0 of 0 Bytes)
 Incoming sessions: 1
 Server: 192.168.134.129 [1NSQhr0LMwH8ZEh3] [bdI4kHD5f5kAzksc] (Linux) TCP 29922
 Server: 192.168.134.129 [1NSQhr0LMwH8ZEh3] [bdI4kHD5f5kAzksc] (Linux) TCP 29922 (153041 data bytes sent, Client: 192.168.134.132 [APLOVERS-765952] (Windows) TCP 1241 (120673 data bytes sent), Session start: 2017-07-08 19:29:40 UTC, Session end: 2017-07-08 19:30:40 UTC)
 Outgoing sessions: 6
 Server: 192.168.134.132 [APLOVERS-765952] (Windows) TCP 445
 Server: 192.168.134.132 [APLOVERS-765952] (Windows) TCP 445 (5641 data bytes sent, Client: 192.168.134.129 [1NSQhr0LMwH8ZEh3] [bdI4kHD5f5kAzksc] (Linux) TCP 41254 (8163 data bytes sent), Session start: 2017-07-08 19:09:40 UTC, Session end: 2017-07-08 19:09:40 UTC
 Server: 192.168.134.132 [APLOVERS-765952] (Windows) TCP 445 (5 data bytes sent, Client: 192.168.134.129 [1NSQhr0LMwH8ZEh3] [bdI4kHD5f5kAzksc] (Linux) TCP 90952 (5 data bytes sent), Session start: 2017-07-08 19:13:22 UTC, Session end: 2017-07-08 19:13:22 UTC
 Server: 192.168.134.132 [APLOVERS-765952] (Windows) TCP 445 (5079 data bytes sent, Client: 192.168.134.129 [1NSQhr0LMwH8ZEh3] [bdI4kHD5f5kAzksc] (Linux) TCP 57967 (8595 data bytes sent), Session start: 2017-07-08 19:13:26 UTC, Session end: 2017-07-08 19:13:26 UTC
 Server: 192.168.134.132 [APLOVERS-765952] (Windows) TCP 135
 Server: 192.168.134.132 [APLOVERS-765952] (Windows) TCP 139

14.

Filter keyword: 192.168.134.129							
Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destination port	Timestamp
SMB Native LAN Manager	Windows 2000 5.0	34	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB Native OS	Windows 2000 2195	34	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB Native LAN Manager	Windows 2000 5.0	36	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB Native OS	Windows 2000 2195	36	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB Native LAN Manager	Windows 2000 5.0	38	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB Native OS	Windows 2000 2195	38	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB File Connect AndX Request	23793	40	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB NT Create AndX Request	23793	42	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB NT Create AndX Request	23795	44	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB NT Create AndX Request	23795	46	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB NT Create AndX Request	23795	48	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB NT Create AndX Request	23795	50	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB NT Create AndX Request	23795	52	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB NT Create AndX Request	23795	54	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 41254	192.168.134.132 (Windows)	TCP 445	2017-07-08 18:09:40 UTC
SMB Native LAN Manager	Windows 2000 5.0	2057	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB Native OS	Windows 2000 2195	2057	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB Native LAN Manager	Windows 2000 5.0	2059	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB Native OS	Windows 2000 2195	2059	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB Native LAN Manager	Windows 2000 5.0	2061	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB Native OS	Windows 2000 2195	2061	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB File Connect AndX Request	20600	2063	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB NT Create AndX Request	20601	2065	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB NT Create AndX Request	20601	2067	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB NT Create AndX Request	20601	2069	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB NT Create AndX Request	20601	2071	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC
SMB NT Create AndX Request	20601	2073	192.168.134.129 [MS-GSS-Mech220-2] (Linux)	TCP 57607	192.168.134.132 (APL0VDR9-765952) (Windows)	TCP 445	2017-07-08 18:13:26 UTC



15.

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Maybe Hacked Box--Capture.pcap...

```

et_get_tlv_group_entry.packet_get_tlv_meta.packet_get_tlv_string.packet_get_tlv_v
alue_bool.packet_get_tlv_value_qword.packet_get_tlv_value_raw.packet_get_tlv_valu
e_string.packet_get_tlv_value_uint.packet_get_type.packet_is_tlv_null_terminated.
packet_receive.packet_receive_via_http.packet_remove_completion_handler.packet_tr
ansmit.packet_transmit_empty_response.packet_transmit_via_http.packet_transmit_v
ia_http_wininet.packet_transmit_via_ssl.scheduler_destroy.scheduler_initialize.sch
eduler_insert_waitable.scheduler_remove_waitable._scheduler_waitable_thread@4.sen
d_core_console_write.....
.....
.....
..ntdll...NtMapViewOfSection...NtQueryAttributesFile...NtOpenFile...NtCreateSection
.NtOpenSection...ntdll...NtMapViewOfSection...NtQueryAttributesFile...NtOpenFile..
NtCreateSection.NtOpenSection...NtLockVirtualMemory.ntdll...
..
..InitServerExtension.DeinitServerExtension...InitServerExtension.DeinitServerExt
ension...
..core_loadlib.....D.
.....
.....
..METERPRETER_TRANSPORT_SSL.....
..https://
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX/....
..METERPRETER_UA.....

```

176 client pkts, 1,164 server pkts, 105 turns.

Entire conversation (1751kB) Show data as ASCII Stream 1

Find: preter Find Next

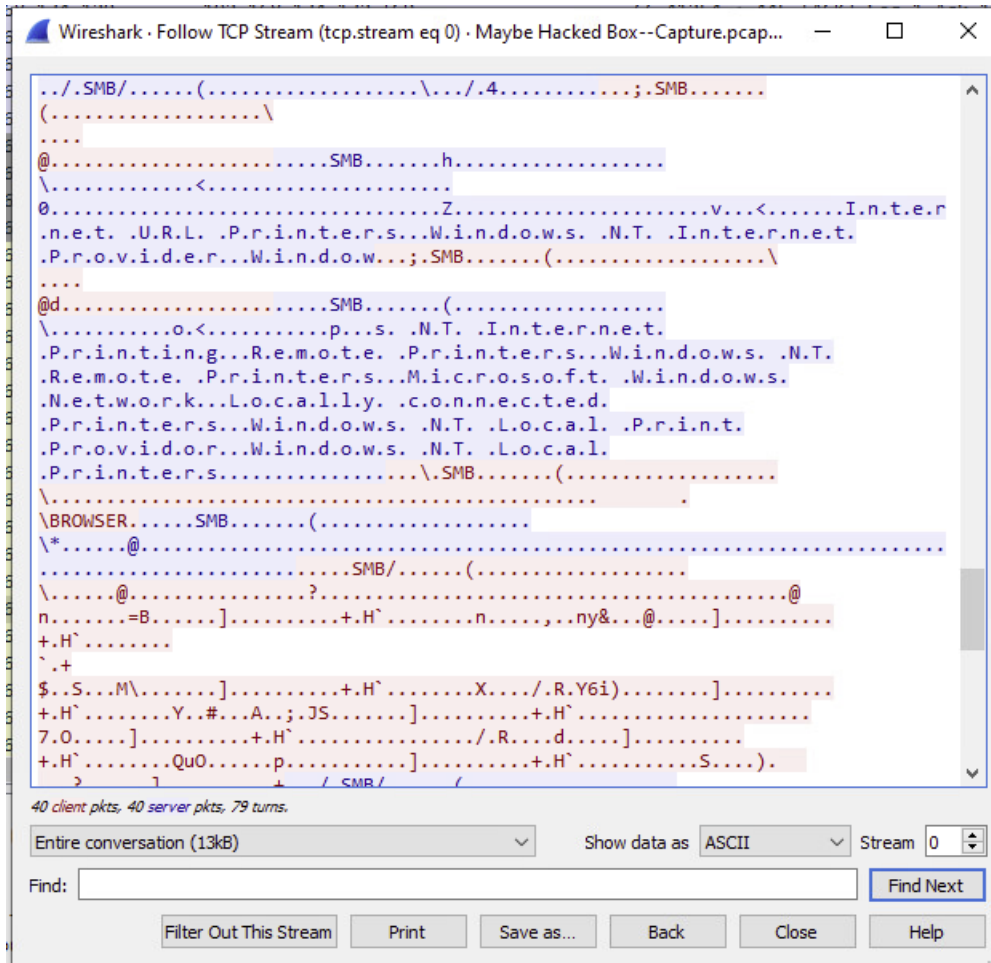
Filter Out This Stream Print Save as... Back Close Help

17.

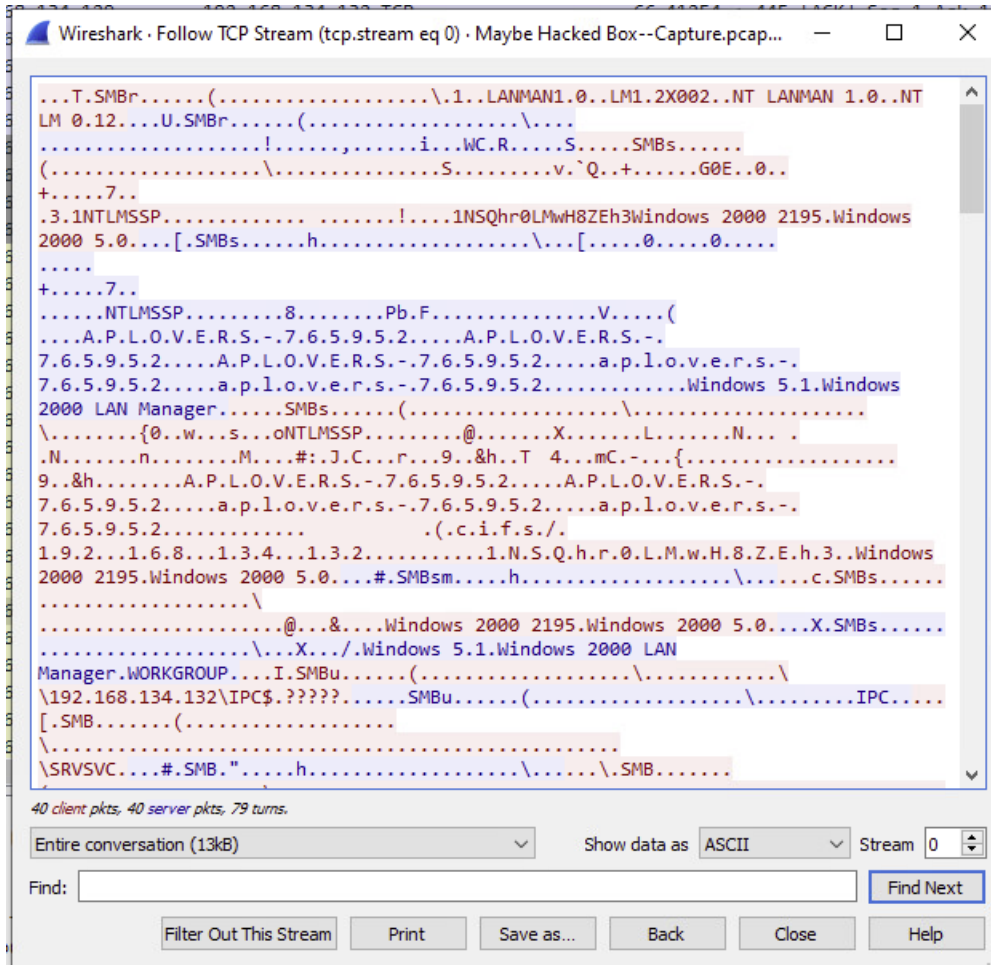
18.

Wireshark · Expert Information · Maybe Hacked Box--Capture.pcapng

Packet	Summary	Group	Protocol	Count
▼ Error	Malformed Packet (Exception occurred)	Malformed	HTTP	1
698	29922 → 1241 [ACK] Seq=737789 Ack=1 Win=14600 Len=1...	Malformed	HTTP	1
▼ Error	Malformed Packet (Exception occurred)	Malformed	SPOOLSS	2
87	EnumPrinters response, level 1 [Malformed Packet]	Malformed	SPOOLSS	1
2310	EnumPrinters response, level 1 [Malformed Packet]	Malformed	SPOOLSS	1
Warning	Connection reset (RST)	Sequence	TCP	148
Warning	TCP Zero Window segment	Sequence	TCP	2
Warning	Illegal characters found in header name	Protocol	HTTP	156
Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	6
Warning	Long frame	Protocol	SRVSVC	3
Warning	DNS query retransmission. Original request in frame 17	Protocol	LLMNR	16
Note	Fault: nca_s_fault ndr	Response	DCERPC	2
Chat	M-SEARCH * HTTP/1.1 (/v)	Sequence	SSDP	8
Chat	TCP window update	Sequence	TCP	32
Chat	Connection finish (FIN)	Sequence	TCP	12
Chat	Connection establish acknowledge (SYN+ACK) server por...	Sequence	TCP	7
Chat	Connection establish request (SYN) server port 445	Sequence	TCP	155



19.



20.

Citations:

Cherry, Denny. “What exactly is MSDTC, and when do I need it? – Denny Cherry & Associates

Consulting.” *Denny Cherry & Associates Consulting*, 13 November 2008,

<https://www.dcac.com/2008/11/13/what-exactly-is-msdtc-any-when-do-i-need-it/>.

Accessed 4 May 2024.

Double Octopus. “Meterpreter.” *Secret Double Octopus*, [https://doubleoctopus.com/security-](https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/)

[wiki/threats-and-tools/meterpreter/](https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/). Accessed 5 May 2024.

EPSON. “FAQ Article Page.” *FAQ Article Page | Epson Europe*,

https://www.epson.eu/en_EU/faq/KA-01651/contents?loc=en-us. Accessed 5 May 2024.

Kyriakos, Akriotis. “Install the Routing and Remote Access Server (RRAS) on Windows Server

2022.” *Akriotis Kyriakos*, 19 May 2022, [https://akyriako.medium.com/install-the-routing-](https://akyriako.medium.com/install-the-routing-and-remote-access-server-rras-on-windows-server-2022-8b0c2d880507)

[and-remote-access-server-rras-on-windows-server-2022-8b0c2d880507](https://akyriako.medium.com/install-the-routing-and-remote-access-server-rras-on-windows-server-2022-8b0c2d880507). Accessed 4 May 2024.

Microsoft. “Crypt32.dll Versions - Win32 apps | Microsoft Learn.” *Learn Microsoft*, 26 January

2022, <https://learn.microsoft.com/en-us/windows/win32/seccrypto/crypt32-dll-versions>.

Accessed 4 May 2024.

Microsoft. “Distributed Transaction Coordinator Service must start before setup can continue.”

Learn Microsoft, 25 January 2023, [https://learn.microsoft.com/en-](https://learn.microsoft.com/en-us/exchange/msdtcstopped-exchange-2013-help)

[us/exchange/msdtcstopped-exchange-2013-help](https://learn.microsoft.com/en-us/exchange/msdtcstopped-exchange-2013-help). Accessed 4 May 2024.

Microsoft. “Do You Need MSDTC?” *Microsoft*, [https://techcommunity.microsoft.com/t5/sql-](https://techcommunity.microsoft.com/t5/sql-server-blog/do-you-need-msdtc/ba-p/383785)

[server-blog/do-you-need-msdtc/ba-p/383785](https://techcommunity.microsoft.com/t5/sql-server-blog/do-you-need-msdtc/ba-p/383785). Accessed 4 May 2024.

Microsoft. "How to solve "WmiApRpl failed with error code device is not ready."" *Microsoft*, <https://learn.microsoft.com/en-us/answers/questions/1191960/how-to-solve-wmiaprpl-failed-with-error-code-devic>. Accessed 4 May 2024.

Microsoft. "[MS-SMB2]: Executing an Operation on a Named Pipe." *Microsoft Learn*, 27 February 2023, https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/777d08d4-56cd-4072-9cef-33056d87b51d. Accessed 5 May 2024.

Microsoft. "[MS-SMB2]: SMB2 TREE_CONNECT Request | Microsoft Learn." *Learn Microsoft*, 4 October 2021, https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/832d2130-22e8-4afb-aafd-b30bb0901798. Accessed 5 May 2024.

Microsoft. "Remote Desktop Services (Remote Desktop Services) - Win32 apps | Microsoft Learn." *Learn Microsoft*, 10 December 2020, <https://learn.microsoft.com/en-us/windows/win32/termserv/terminal-services-portal>. Accessed 4 May 2024.

microsoft. "RSVP PATH and RESV Messages." *microsoft*, <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/qos/rsvp-path-and-resv-messages>. Accessed 4 May 2024.

Microsoft. "RSVP Service Provider | Microsoft Learn." *Learn Microsoft*, 31 May 2018, <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/qos/rsvp-service-provider>. Accessed 4 May 2024.

Microsoft. "RSVP SP and RSVP | Microsoft Learn." *Learn Microsoft*, 31 May 2018, <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/qos/rsvp-sp-and-rsvp>. Accessed 4 May 2024.

Microsoft. "Starting and stopping the WMI service - Win32 apps." *Learn Microsoft*, 7 March 2023, <https://learn.microsoft.com/en-us/windows/win32/wmisdk/starting-and-stopping-the-wmi-service>. Accessed 4 May 2024.

Microsoft. "Terminal Services has been renamed - Win32 apps." *Learn Microsoft*, 7 February 2022, <https://learn.microsoft.com/en-us/windows/win32/termserv/terminal-services-is-now-remote-desktop-services>. Accessed 4 May 2024.

Microsoft. "What is Terminal Services?" *Microsoft*, <https://answers.microsoft.com/en-us/windows/forum/all/what-is-terminal-services/d9951f3d-15e5-42f8-b395-dfdd4d9933c7>. Accessed 4 May 2024.

Microsoft. "winmgmt - Win32 apps | Microsoft Learn." *Learn Microsoft*, 3 November 2023, <https://learn.microsoft.com/en-us/windows/win32/wmisdk/winmgmt>. Accessed 4 May 2024.

Microsoft. "WmiApRpl." *Microsoft*, <https://answers.microsoft.com/en-us/windows/forum/all/wmiaprpl-folder-in-inf-file-of-windows-10-need/a5990b27-6581-44e7-93bd-d6475ea78750>. Accessed 4 May 2024.

MSRC. "Notes on exploitability of the recent Windows BROWSER protocol issue | MSRC Blog." *Microsoft Security Response Center*, 16 February 2011, <https://msrc.microsoft.com/blog/2011/02/notes-on-exploitability-of-the-recent-windows-browser-protocol-issue/>. Accessed 5 May 2024.

Netsurion. "Event ID - 3012." *Event Tracker*, https://kb.eventtracker.com/evtpass/evtpages/EventId_3012_Microsoft-Windows-LoadPerf_65967.asp. Accessed 4 May 2024.

PC Review. “What is WmiApRpl service for ?” *PC Review*, 2 April 2006,
<https://www.pcreview.co.uk/threads/what-is-wmiaprpl-service-for.2479963/>. Accessed 4
May 2024.

Rouse, Margaret. “What is Routing and Remote Access Service (RRAS)? - Definition from
Techopedia.” *Techopedia*, 11 July 2023,
<https://www.techopedia.com/definition/3424/routing-and-remote-access-service-rras>.
Accessed 4 May 2024.

Skyway West. “What is an SSDP Service Exploit, what is the risk and how can you mitigate that
risk?” *Skyway West*, <https://www.skywaywest.com/2021/01/what-is-an-ssdp-service-exploit/>. Accessed 5 May 2024.

Spy Shelter. “What’s WinMgmt.exe (WMI Service Control Utility)? Is it safe or a virus?” *Spy
Shelter*, <https://spyshelter.com/exe/microsoft-windows-winmgmt-exe/>. Accessed 4 May
2024.

Strontic. “WmiApRpl.dll.” *github*, [https://strontic.github.io/xcyclopedia/library/WmiApRpl.dll-
6AD0CEECBE1C4DDDE0D88A848E54F4A8.html](https://strontic.github.io/xcyclopedia/library/WmiApRpl.dll-6AD0CEECBE1C4DDDE0D88A848E54F4A8.html). Accessed 4 May 2024.

Tenable. “5.26 Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled.'” *Tenable*, 5.26 Ensure
'SSDP Discovery (SSDPSRV)' is set to 'Disabled'. Accessed 5 5 2024.

University Information Technology Services. “ARCHIVED: What is the Microsoft Windows
Security Center?” *IU*, <https://kb.iu.edu/d/arly>. Accessed 4 May 2024.