GROUP 2.3 PROJECT ID 014
ENDPOINT FORENSIC

INTRODUCTION

A method of keeping an eye on each packet that travels over the network is called packet capture, sometimes called packet sniffing. A hardware or software device that tracks all network activity is called a packet sniffer. Sniffers provide a security risk since they can intercept all incoming and outgoing communication, including usernames, passwords, and other private information in clear text (Sam, 2024).

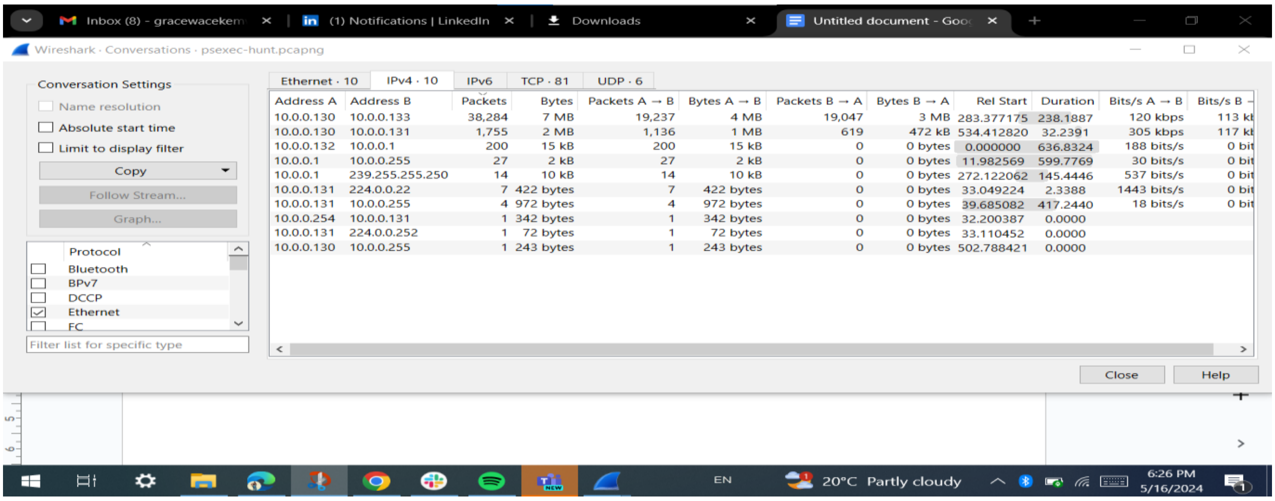
A free tool for monitoring network traffic is called Wireshark. Network administrators use it to identify security flaws or fix issues (Delija, 2021).

Network Miner is an open-source network forensic analysis tool that can be used as a passive network sniffer or packet-capturing tool to find hostnames, operating systems, available ports, and other information. In addition, it can generate/reassemble sent files and certificates from PCAP files and parse PCAP files for offline analysis (Sam, 2024).

1.0 Method

Using Wireshark and Network Miner to analyze a PCAP file.

1. Using IPv4, we can successfully track the attacker's activity within our network by identifying the malicious device's IP address. This is because higher packet counts correspond to increased device traffic (Abd-Ulalieem, 2023).



Conversation Settings

☐ Name resolution
☐ Absolute start time
☐ Limit to display filter

	Protocol
☐	Bluetooth
☐	BPv7
☐	DCCP
☑	Ethernet
☐	FC

Filter list for specific type

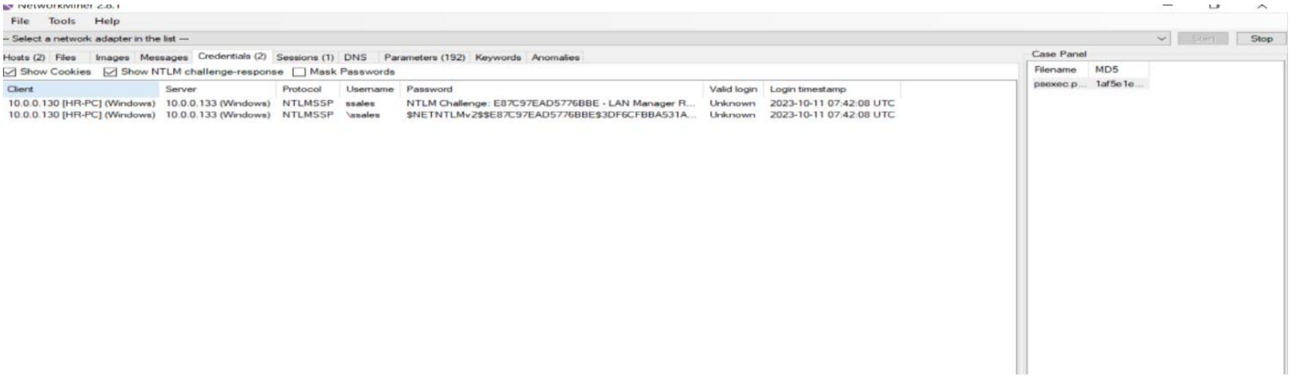
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B –
10.0.0.130	10.0.0.133	38,284	7 MB	19,237	4 MB	19,047	3 MB	283.377175	238.1887	120 kbps	113 k
10.0.0.130	10.0.0.131	1,755	2 MB	1,136	1 MB	619	472 kB	534.412820	32.2391	305 kbps	117 k
10.0.0.132	10.0.0.1	200	15 kB	200	15 kB	0	0 bytes	0.000000	636.8324	188 bits/s	0 bit
10.0.0.1	10.0.0.255	27	2 kB	27	2 kB	0	0 bytes	11.982569	599.7769	30 bits/s	0 bit
10.0.0.1	239.255.255.250	14	10 kB	14	10 kB	0	0 bytes	272.122062	145.4446	537 bits/s	0 bit
10.0.0.131	224.0.0.22	7	422 bytes	7	422 bytes	0	0 bytes	33.049224	2.3388	1443 bits/s	0 bit
10.0.0.131	10.0.0.255	4	972 bytes	4	972 bytes	0	0 bytes	39.685082	417.2440	18 bits/s	0 bit
10.0.0.254	10.0.0.131	1	342 bytes	1	342 bytes	0	0 bytes	32.200387	0.0000		
10.0.0.131	224.0.0.252	1	72 bytes	1	72 bytes	0	0 bytes	33.110452	0.0000		
10.0.0.130	10.0.0.255	1	243 bytes	1	243 bytes	0	0 bytes	502.788421	0.0000		

Figure 1

2. We use the SMB2 filter, which helps us focus on SMB2 protocol packets that aid in analyzing file sharing and network communication activities, which includes detecting compromised hosts, to ascertain the machine's hostname to which the

attacker initially shifted (Shah, 2022). Next, we look for session setup request packets, which frequently include the username and domain (WireShark, 2020). We next examine these packets' headers to find the path field, which reveals the hostname, SALES-PC.

3. Network traffic must be analyzed to detect authentication protocols and credentials being transmitted to determine the username that an attacker is using for authentication. Usernames and other credentials are typically included in Network Miner (Abd-Ulalieem, 2023). If we examine the 'NTLMSSP-AUTH' message for NTLM, we will see that the username is present. (Shah, 2022).

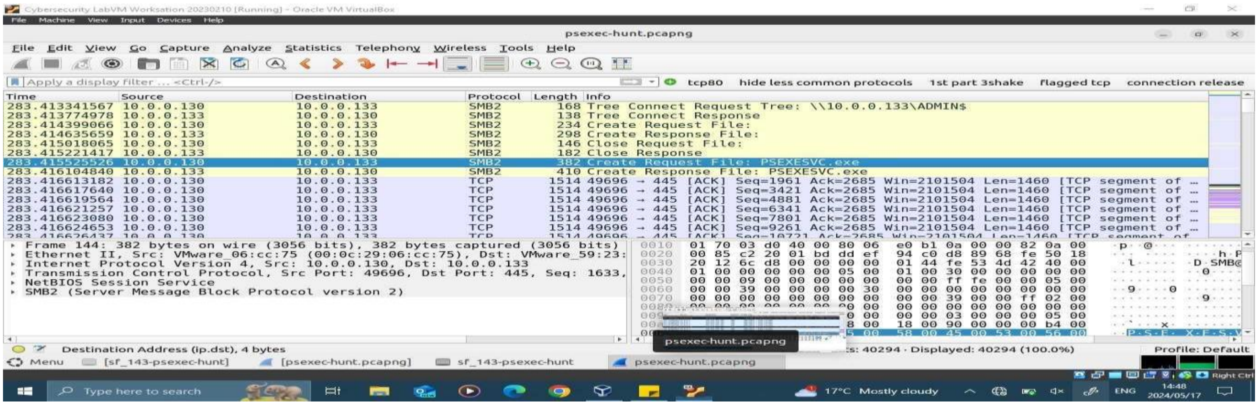


Client	Server	Protocol	Username	Password	Valid login	Login timestamp
10.0.0.130 [HR-PC] (Windows)	10.0.0.133 (Windows)	NTLMSSP	ssales	NTLM Challenge: E87C97EAD5776BBE - LAN Manager R...	Unknown	2023-10-11 07:42:08 UTC
10.0.0.130 [HR-PC] (Windows)	10.0.0.133 (Windows)	NTLMSSP	\ssales	$NETNTLMv2$$E87C97EAD5776BBE$3DF6CFBBA531A...	Unknown	2023-10-11 07:42:08 UTC

Filename	MD5
psexec.p...	1af5e1e...

Figure 2

4. When a user clicks on a file icon on a computer, the system can immediately execute an encoded set of instructions included in the executable file (EXE file) (Renard, 2024). Microsoft created the SysInternals tool suite, which includes Psexesvc.exe. It's a small remote administration program that allows you to run commands on other computers. The Server Message Block (SMB) protocol, which operates on TCP port 445, is used for this over a named pipe. This gives attackers the ability to migrate laterally with PSExec. Although PsExec is not malware, attackers may nonetheless exploit it for nefarious purposes (Lutkevich, 2022).



```
Time         Source      Destination  Protocol Length Info
283.413341567 10.0.0.130 10.0.0.133   SMB2     168 Tree Connect Request Tree: \\10.0.0.133\ADMIN$
283.413774978 10.0.0.133 10.0.0.130   SMB2     138 Tree Connect Response
283.414399066 10.0.0.130 10.0.0.133   SMB2     234 Create Request File:
283.414635659 10.0.0.133 10.0.0.130   SMB2     298 Create Response File:
283.415018065 10.0.0.130 10.0.0.133   SMB2     146 Close Request File:
283.415221417 10.0.0.133 10.0.0.130   SMB2     182 Close Response
283.415525526 10.0.0.130 10.0.0.133   SMB2     382 Create Request File: PSEXESVC.exe
283.416104840 10.0.0.133 10.0.0.130   SMB2     410 Create Response File: PSEXESVC.exe
283.416613182 10.0.0.130 10.0.0.133   TCP      1514 49696 → 445 [ACK] Seq=1961 Ack=2685 Win=2101504 Len=1460 [TCP segment of ...
283.416617640 10.0.0.130 10.0.0.133   TCP      1514 49696 → 445 [ACK] Seq=3421 Ack=2685 Win=2101504 Len=1460 [TCP segment of ...
283.416619564 10.0.0.130 10.0.0.133   TCP      1514 49696 → 445 [ACK] Seq=4881 Ack=2685 Win=2101504 Len=1460 [TCP segment of ...
283.416621257 10.0.0.130 10.0.0.133   TCP      1514 49696 → 445 [ACK] Seq=6341 Ack=2685 Win=2101504 Len=1460 [TCP segment of ...
283.416623080 10.0.0.130 10.0.0.133   TCP      1514 49696 → 445 [ACK] Seq=7801 Ack=2685 Win=2101504 Len=1460 [TCP segment of ...
283.416624653 10.0.0.130 10.0.0.133   TCP      1514 49696 → 445 [ACK] Seq=9261 Ack=2685 Win=2101504 Len=1460 [TCP segment of ...
283.416626437 10.0.0.130 10.0.0.133   TCP      1514 49696 → 445 [ACK] Seq=10721 Ack=2685 Win=2101504 Len=1460 [TCP segment of
```

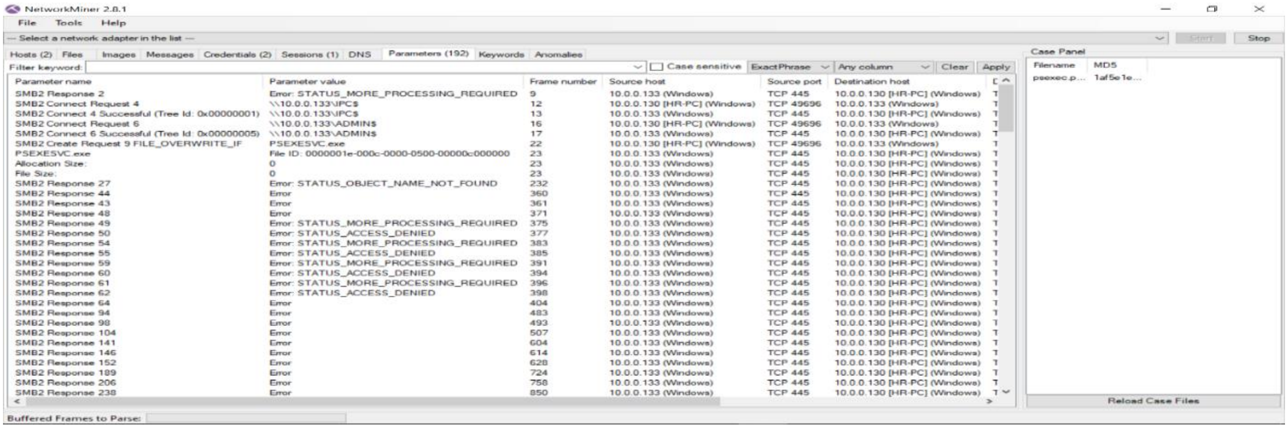
```
▸ Frame 144: 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits)
▸ Ethernet II, Src: VMware_06:cc:75 (00:0c:29:06:cc:75), Dst: VMware_59:23:
▸ Internet Protocol Version 4, Src: 10.0.0.130, Dst: 10.0.0.133
▸ Transmission Control Protocol, Src Port: 49696, Dst Port: 445, Seq: 1633,
▸ NetBIOS Session Service
▸ SMB2 (Server Message Block Protocol version 2)
```

```
0010  01 70 03 d0 40 00 80 06  e0 b1 0a 00 00 82 0a 00   ·p··@···  ········
0020  00 85 c2 20 01 bd dd ef  94 c0 d8 89 68 fe 50 18   ········  ····h·P
0030  20 12 6c d8 00 00 00 00  01 44 fe 53 4d 42 40 00    ·l·····  ·D·SMB@
0040  01 00 00 00 00 00 05 00  01 00 30 00 00 00 00 00   ········  ··0·····
0050  00 00 09 00 00 00 00 00  00 00 ff fe 00 00 05 00   ········  ········
0060  00 00 39 00 00 00 00 30  00 00 00 00 00 00 00 00   ··9····0  ········
0070  00 00 00 00 00 00 00 00  00 00 39 00 00 ff 02 00   ········  ··9·····
0080                       00  00 00 00 00 00 00 00 00
0090                    0  00  00 00 03 00 00 00 05 00
00a0                    8  00  18 00 90 00 00 00 b4 00               `···x·
00b0                           58 00 45 00 53 00 56 00             ·P·S·E·  X·E·S·V·
```

Destination Address (ip.dst), 4 bytes
psexec-hunt.pcapng
...s: 40294 · Displayed: 40294 (100.0%)
Profile: Default

Figure 3

5. & 6. By examining the request pattern in question 4, we can observe that the attacker created a request PSEXEC.exe file to install malware using the SMB2 protocol. we analyzed the request packets and identified IPC$ and Admin$, A secret administrative share is called Admin$, and a hidden share for inter-process communication is called IPC$ (Abd-Ulalieem, 2023). The attacker will use Admin$ to obtain elevated privileges (Hackerson, 2024).

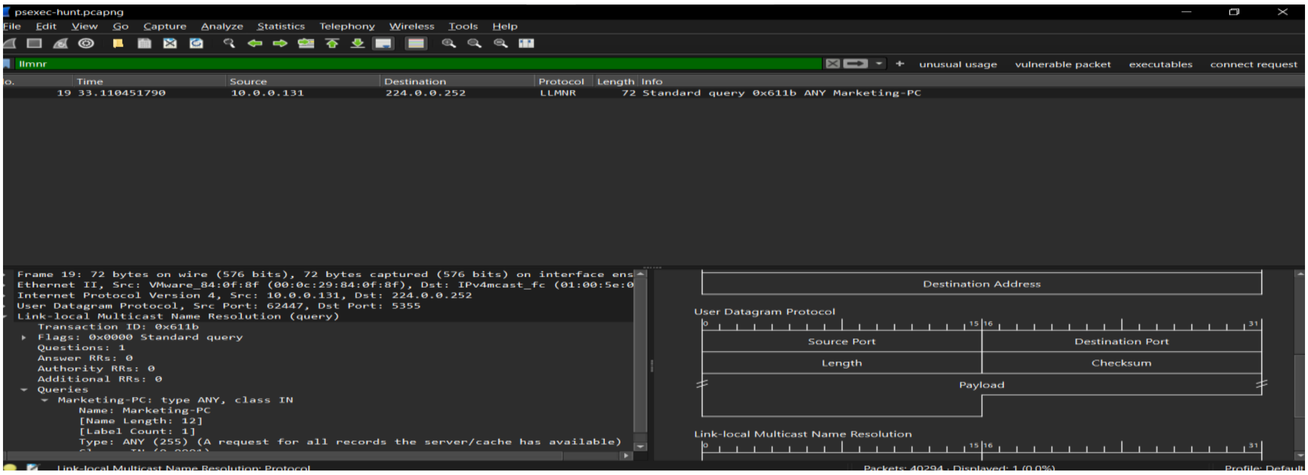


Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	D
SMB2 Response 2	Error: STATUS_MORE_PROCESSING_REQUIRED	9	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Connect Request 4	\\10.0.0.133\IPC$	12	10.0.0.130 [HR-PC] (Windows)	TCP 49696	10.0.0.133 (Windows)	T
SMB2 Connect 4 Successful (Tree Id: 0x00000001)	\\10.0.0.133\IPC$	13	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Connect Request 6	\\10.0.0.133\ADMIN$	16	10.0.0.130 [HR-PC] (Windows)	TCP 49696	10.0.0.133 (Windows)	T
SMB2 Connect 6 Successful (Tree Id: 0x00000005)	\\10.0.0.133\ADMIN$	17	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Create Request 9 FILE_OVERWRITE_IF	PSEXESVC.exe	22	10.0.0.130 [HR-PC] (Windows)	TCP 49696	10.0.0.133 (Windows)	T
PSEXESVC.exe	File ID: 0000001e-000c-0000-0500-00000c000000	23	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
Allocation Size:	0	23	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
File Size:	0	23	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 27	Error: STATUS_OBJECT_NAME_NOT_FOUND	232	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 44	Error	360	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 43	Error	361	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 48	Error	371	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 49	Error: STATUS_MORE_PROCESSING_REQUIRED	375	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 50	Error: STATUS_ACCESS_DENIED	377	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 54	Error: STATUS_MORE_PROCESSING_REQUIRED	383	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 55	Error: STATUS_ACCESS_DENIED	385	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 59	Error: STATUS_MORE_PROCESSING_REQUIRED	391	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 60	Error: STATUS_ACCESS_DENIED	394	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 61	Error: STATUS_MORE_PROCESSING_REQUIRED	396	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 62	Error: STATUS_ACCESS_DENIED	398	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 64	Error	404	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 94	Error	483	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 98	Error	493	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 104	Error	507	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 141	Error	604	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 146	Error	614	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 152	Error	628	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 189	Error	724	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 206	Error	758	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T
SMB2 Response 238	Error	850	10.0.0.133 (Windows)	TCP 445	10.0.0.130 [HR-PC] (Windows)	T

Filename	MD5
psexec.p...	1af5e1e...

Figure 4

7. To determine the hostname of the machine that an attacker tried to change without using our network. We display lateral movement by filtering the traffic. To limit traffic to internal IP addresses, we install filters. Select Statistics, Conversations, IPv4, and then filter by internal IP addresses that are communicating with external IP addresses (Abd-Ulalieem, 2023). Use the filter Ip 10.0.0.131 > 224.0.0.252. The conversation's specifics demonstrate that the attacker is conversing via the link-local multicast Name Resolution protocol or LLMNR. "Marketing-pc" is the machine's hostname that is displayed (Chris, 2021).



llmnr

```
o.        Time              Source          Destination     Protocol  Length Info
       19 33.110451790      10.0.0.131      224.0.0.252     LLMNR         72 Standard query 0x611b ANY Marketing-PC
```

```
Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface ens
Ethernet II, Src: VMware_84:0f:8f (00:0c:29:84:0f:8f), Dst: IPv4mcast_fc (01:00:5e:0
Internet Protocol Version 4, Src: 10.0.0.131, Dst: 224.0.0.252
User Datagram Protocol, Src Port: 62447, Dst Port: 5355
Link-local Multicast Name Resolution (query)
   Transaction ID: 0x611b
 ▸ Flags: 0x0000 Standard query
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
 ▾ Queries
   ▾ Marketing-PC: type ANY, class IN
       Name: Marketing-PC
       [Name Length: 12]
       [Label Count: 1]
       Type: ANY (255) (A request for all records the server/cache has available)
```

Figure 5

The results of Cyber Defenders Blue teams CTF challenges | PsExec Hunt lab can be found in Appendix A and B.

CONCLUSION

In this investigation, we used Wireshark and Network Miner to analyze a PCAP file and track an attacker's activities on our network. By using a variety of filters and forensic approaches, our process was able to determine the IP address, hostname, and authentication credentials of the attacker.

Important Discoveries:

1. Malicious IP Address: Found through IPv4 traffic with excessive packet counts.
2. Hostname Discovery: We discovered the hostname of the compromised system, "SALES-PC," by using Wireshark's SMB2 filter.
3. Authentication Credentials: Using the 'ntlmssp' filter, the username "ssales" was extracted from NTLMSSP-AUTH communications using Network Miner.
4. Executable File Execution: The attacker remotely executed SMB commands using PsExec.
5. Privilege Escalation: Identified the escalation of privileges by using Admin$ and IPC$ shares.
6. Lateral Movement: By examining LLMNR protocol traffic, the attacker focused on "Marketing-pc".

Our extensive analysis of the network data revealed how the attacker used several protocols and tools to enter and traverse the network. This emphasizes the value of strong security protocols, ongoing observation, and sophisticated forensic tools like Wireshark and Network Miner. From our observations, Network Miner is user friendly and easier to use while Wireshark depends on filters to analyze data.

References

Abd-Ulalieem, A. (2023, Novemeber 12). *PsExec Hunt-CyberDefenders*. Retrieved from Medium: https://medium.com/@anasabdelalieem9/psexec-hunt-cyberdefenders-1776d3b39ca1

Chris, G. (2021, Feb 25). *Wireshark Tutorial for BEGINNERS // Where to start with Wireshark*. Retrieved from youtube: https://www.youtube.com/watch?v=OU-A2EmVrKQ&list=PLW8bTPfXNGdC5Co0VnBK1yVzAwSSphzpJ

Delija, D. M. (2021). Comparative Analysis of Network Forensic Tools on Different Operating Systems. *ResearchGate*, 1231-1235.

Hackerson, H. (2024, Jan). *Network Forensics Using NetworkMiner - PCAP Analysis Like a Boss / Security Analyst Training*. Retrieved from You-tube: https://www.youtube.com/watch?v=e58Wgkkb0G0

Lutkevich, B. (2022, January). *executable file (EXE file)*. Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/executable-file-exe-file

Renard, J. (2024, January). *Lateral Movement with PSExec*. Retrieved from Mind Point Group: https://www.mindpointgroup.com/blog/lateral-movement-with-psexec

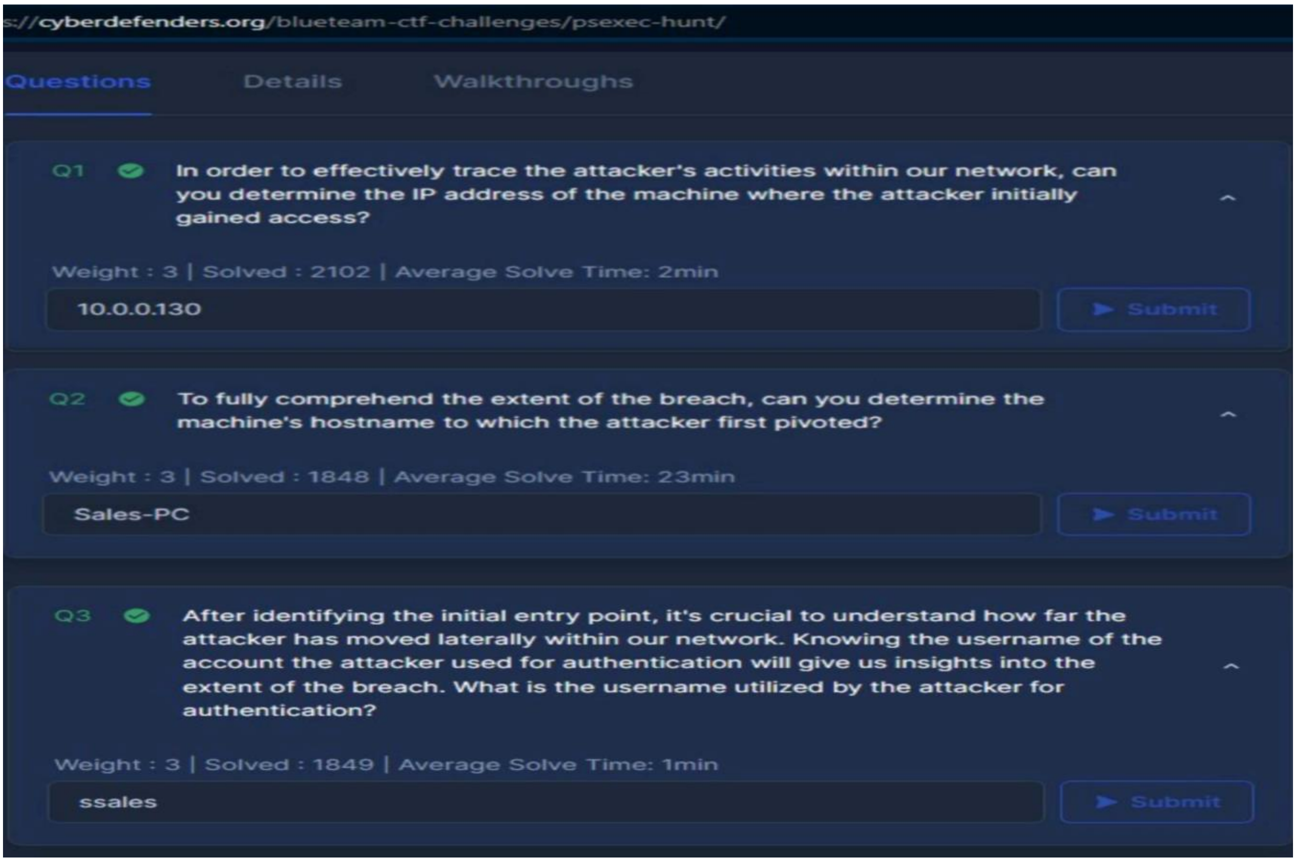
Sam, C. (2024, May 22). *Network mapping tools comparision.* Retrieved from Aditya Educational Institutions: https://aditya.ac.in/forensic-science/projects/Computer%20Forensics/christy%20sam-Network%20mapping%20tools%20comparision.pdf

Shah, Z. (2022, Nov 2). *Malware Traffic Analysis with Wireshark - 2*. Retrieved from youtube: https://www.youtube.com/watch?v=T_41vAOHfZ4

WireShark. (2020, August). Retrieved from WireShark: https://wiki.wireshark.org/SMB2

APPENDIX

Screenshots of the completed lab questions



s://cyberdefenders.org/blueteam-ctf-challenges/psexec-hunt/

Q1 ✓ In order to effectively trace the attacker's activities within our network, can you determine the IP address of the machine where the attacker initially gained access?

Weight : 3 | Solved : 2102 | Average Solve Time: 2min

10.0.0.130

Q2 ✓ To fully comprehend the extent of the breach, can you determine the machine's hostname to which the attacker first pivoted?

Weight : 3 | Solved : 1848 | Average Solve Time: 23min

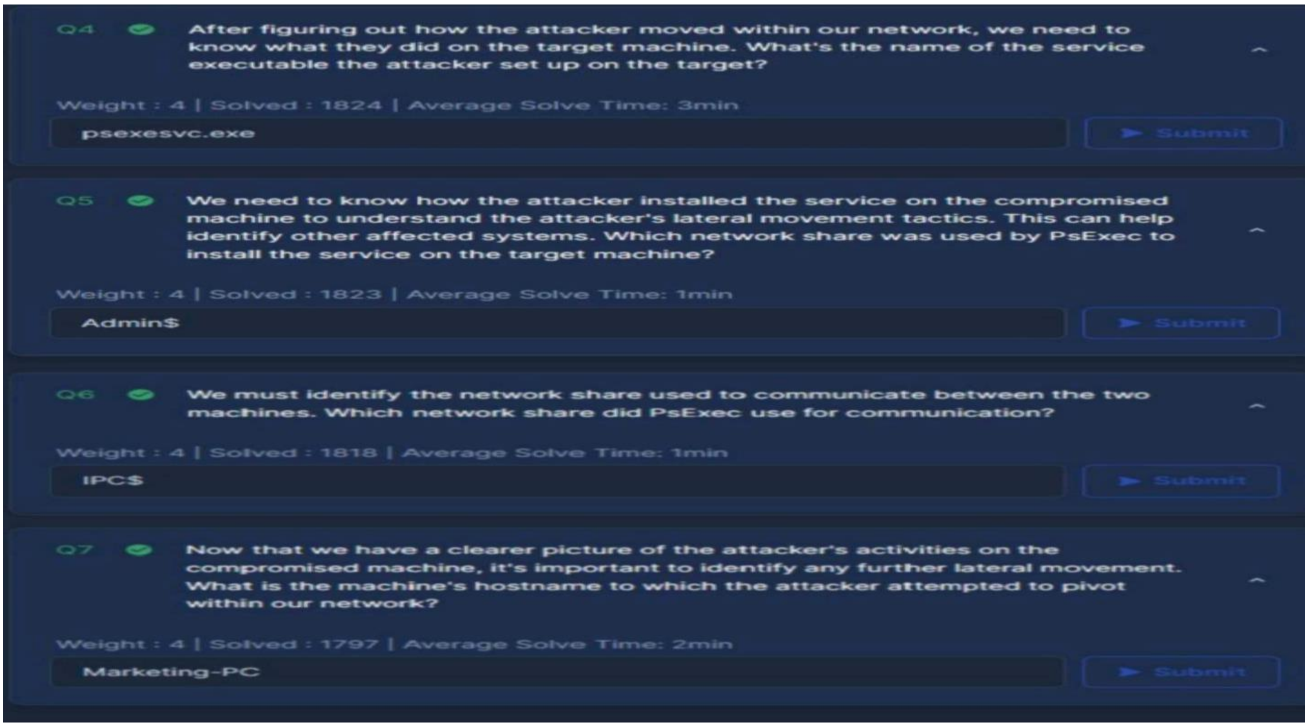
Sales-PC

Q3 ✓ After identifying the initial entry point, it's crucial to understand how far the attacker has moved laterally within our network. Knowing the username of the account the attacker used for authentication will give us insights into the extent of the breach. What is the username utilized by the attacker for authentication?

Weight : 3 | Solved : 1849 | Average Solve Time: 1min

ssales

A



Q4 ✓ After figuring out how the attacker moved within our network, we need to know what they did on the target machine. What's the name of the service executable the attacker set up on the target?

Weight : 4 | Solved : 1824 | Average Solve Time: 3min

psexesvc.exe

Q5 ✓ We need to know how the attacker installed the service on the compromised machine to understand the attacker's lateral movement tactics. This can help identify other affected systems. Which network share was used by PsExec to install the service on the target machine?

Weight : 4 | Solved : 1823 | Average Solve Time: 1min

Admin$

Q6 ✓ We must identify the network share used to communicate between the two machines. Which network share did PsExec use for communication?

Weight : 4 | Solved : 1818 | Average Solve Time: 1min

IPC$

Q7 ✓ Now that we have a clearer picture of the attacker's activities on the compromised machine, it's important to identify any further lateral movement. What is the machine's hostname to which the attacker attempted to pivot within our network?

Weight : 4 | Solved : 1797 | Average Solve Time: 2min

Marketing-PC

B