Robert Carpenter
github.com/robertmcarpenter
April 4th 2025

PSExec Hunt Lab: Analyzing a PCAP File For Signs of PsExec Lateral Movement

A Follow-Along lab from Cyberdefenders.org

Lab Goal: In this lab my goal is to analyze a given .pcap file to check for signs of PsExec execution, a popular tool used by threat actors , to issue remote commands on a Windows Endpoint within a LAN.

Lab Scenario: ***An alert from the Intrusion Detection System (IDS) flagged suspicious lateral movement activity involving PsExec. This indicates potential unauthorized access and movement across the network. As a SOC Analyst, your task is to investigate the provided PCAP file to trace the attacker's activities. Identify their entry point, the machines targeted, the extent of the breach, and any critical indicators that reveal their tactics and objectives within the compromised environment.***

Note to Reader: PsExec is a binary tool which is code signed by Microsoft and provided by SysInternals. It is a legitimate tool used in some enterprise environments to connect to their Windows endpoints. It is often abused by threat actors post-exploitation to give themselves remote access. This can be an example of a LOLBIN (Living Off the Land BINary) Click here for more information on Psexec.exe.

Questions/Objectives to Answer:

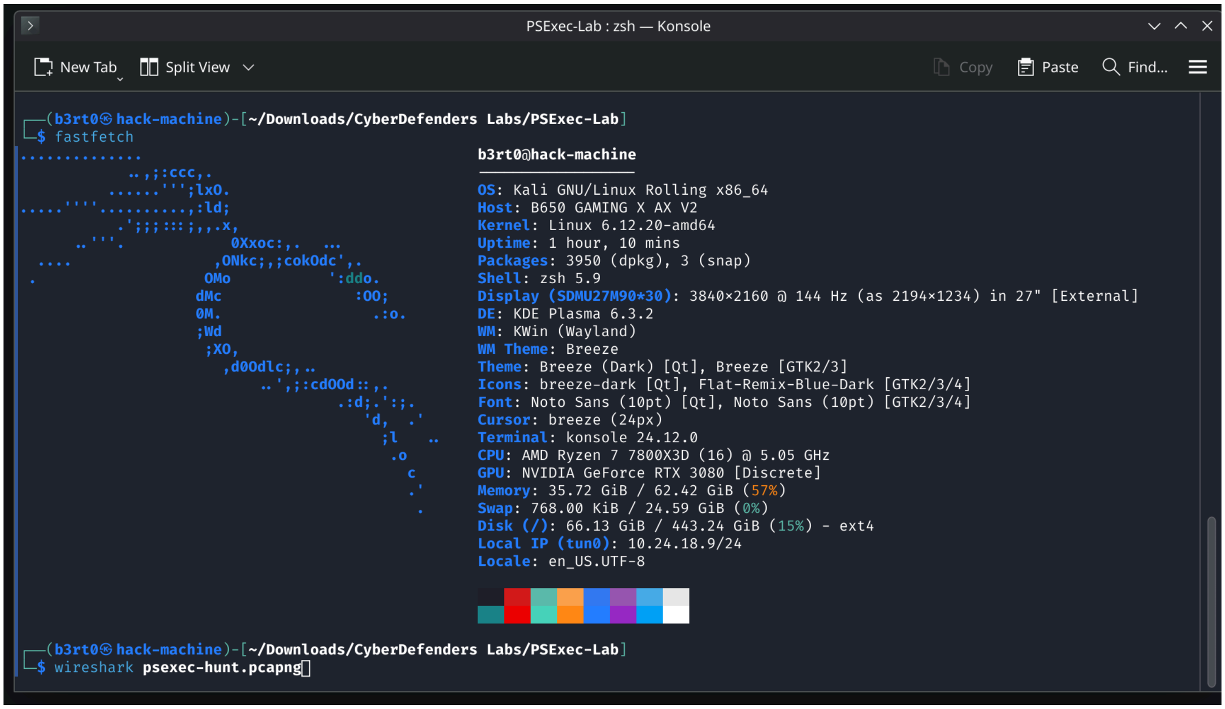
1. To effectively trace the attacker's activities within our network, can you identify the IP address of the machine from which the attacker initially gained access?
2. To fully understand the extent of the breach, can you determine the machine's hostname to which the attacker first pivoted?
3. Knowing 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?
4. 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?
5. 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?
6. We must identify the network share used to communicate between the two machines. Which network share did PsExec use for communication?

Robert Carpenter
github.com/robertmcarpenter
April 4th 2025

7. 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 hostname of the second machine the attacker targeted to pivot within our network?

Okay! Let's start!

My first objective of this lab is to figure out what machine the attacker FIRST gained access to. I will open up the provided .pcap file to take a look at the data within wireshark.

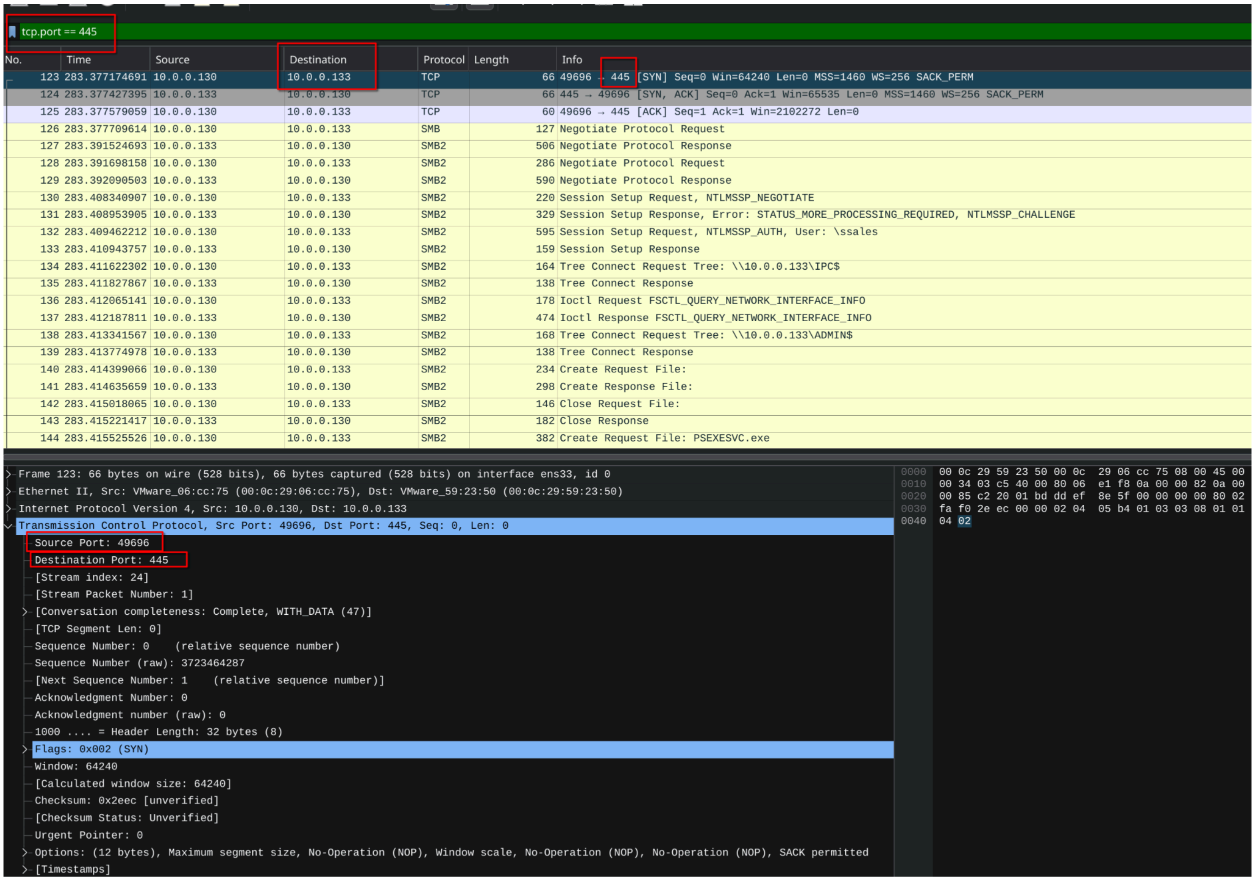


```
┌──(b3rt0㉿hack-machine)-[~/Downloads/CyberDefenders Labs/PSExec-Lab]
└─$ fastfetch
..............                                          b3rt0@hack-machine
            ..,;:ccc,.                                  ──────────────────
          ......''';lxO.                                OS: Kali GNU/Linux Rolling x86_64
.....''''..........,:ld;                                Host: B650 GAMING X AX V2
           .';;;:::;,,.x,                               Kernel: Linux 6.12.20-amd64
      ..'''.            0Xxoc:,.  ...                   Uptime: 1 hour, 10 mins
  ....                ,ONkc;,;cokOdc',.                 Packages: 3950 (dpkg), 3 (snap)
 .                   OMo           ':ddo.               Shell: zsh 5.9
                    dMc               :OO;              Display (SDMU27M90*30): 3840×2160 @ 144 Hz (as 2194×1234) in 27" [External]
                    0M.                 .:o.            DE: KDE Plasma 6.3.2
                    ;Wd                                 WM: KWin (Wayland)
                     ;XO,                               WM Theme: Breeze
                       ,d0Odlc;,..                      Theme: Breeze (Dark) [Qt], Breeze [GTK2/3]
                           ..',;:cdOOd::,.              Icons: breeze-dark [Qt], Flat-Remix-Blue-Dark [GTK2/3/4]
                                    .:d;.':;.           Font: Noto Sans (10pt) [Qt], Noto Sans (10pt) [GTK2/3/4]
                                       'd,  .'          Cursor: breeze (24px)
                                         ;l   ..        Terminal: konsole 24.12.0
                                          .o            CPU: AMD Ryzen 7 7800X3D (16) @ 5.05 GHz
                                            c           GPU: NVIDIA GeForce RTX 3080 [Discrete]
                                            .'          Memory: 35.72 GiB / 62.42 GiB (57%)
                                             .          Swap: 768.00 KiB / 24.59 GiB (0%)
                                                        Disk (/): 66.13 GiB / 443.24 GiB (15%) - ext4
                                                        Local IP (tun0): 10.24.18.9/24
                                                        Locale: en_US.UTF-8

┌──(b3rt0㉿hack-machine)-[~/Downloads/CyberDefenders Labs/PSExec-Lab]
└─$ wireshark psexec-hunt.pcapng
```

Based on the scenario I know that the attacker was moving laterally within the network using the tool Psexec. I know that Psexec uses ports 445 (SMB) and 135 (RPC) for communication. I will filter the packets within wireshark to look for packets that contain traffic for Ports 445 and Ports 135.

Robert Carpenter
github.com/robertmcarpenter
April 4th 2025



tcp.port == 445

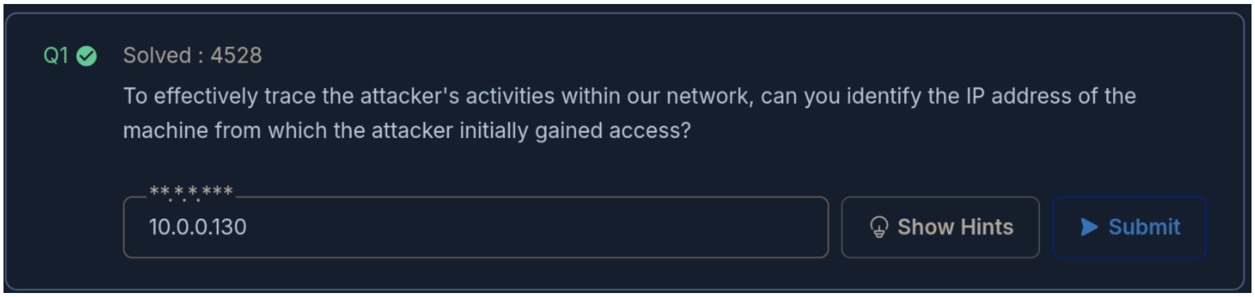
```
No.  Time            Source      Destination  Protocol Length Info
 123 283.377174691 10.0.0.130  10.0.0.133   TCP         66 49696 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 124 283.377427395 10.0.0.133  10.0.0.130   TCP         66 445 → 49696 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 125 283.377579059 10.0.0.130  10.0.0.133   TCP         60 49696 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
 126 283.377709614 10.0.0.130  10.0.0.133   SMB        127 Negotiate Protocol Request
 127 283.391524693 10.0.0.133  10.0.0.130   SMB2       506 Negotiate Protocol Response
 128 283.391698158 10.0.0.130  10.0.0.133   SMB2       286 Negotiate Protocol Request
 129 283.392090503 10.0.0.133  10.0.0.130   SMB2       590 Negotiate Protocol Response
 130 283.408340907 10.0.0.130  10.0.0.133   SMB2       220 Session Setup Request, NTLMSSP_NEGOTIATE
 131 283.408953905 10.0.0.133  10.0.0.130   SMB2       329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
 132 283.409462212 10.0.0.130  10.0.0.133   SMB2       595 Session Setup Request, NTLMSSP_AUTH, User: \ssales
 133 283.410943757 10.0.0.133  10.0.0.130   SMB2       159 Session Setup Response
 134 283.411622302 10.0.0.130  10.0.0.133   SMB2       164 Tree Connect Request Tree: \\10.0.0.133\IPC$
 135 283.411827867 10.0.0.133  10.0.0.130   SMB2       138 Tree Connect Response
 136 283.412065141 10.0.0.130  10.0.0.133   SMB2       178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
 137 283.412187811 10.0.0.133  10.0.0.130   SMB2       474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
 138 283.413341567 10.0.0.130  10.0.0.133   SMB2       168 Tree Connect Request Tree: \\10.0.0.133\ADMIN$
 139 283.413774978 10.0.0.133  10.0.0.130   SMB2       138 Tree Connect Response
 140 283.414399066 10.0.0.130  10.0.0.133   SMB2       234 Create Request File:
 141 283.414635659 10.0.0.133  10.0.0.130   SMB2       298 Create Response File:
 142 283.415018065 10.0.0.130  10.0.0.133   SMB2       146 Close Request File:
 143 283.415221417 10.0.0.133  10.0.0.130   SMB2       182 Close Response
 144 283.415525526 10.0.0.130  10.0.0.133   SMB2       382 Create Request File: PSEXESVC.exe
```

```
> Frame 123: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_06:cc:75 (00:0c:29:06:cc:75), Dst: VMware_59:23:50 (00:0c:29:59:23:50)
> Internet Protocol Version 4, Src: 10.0.0.130, Dst: 10.0.0.133
v Transmission Control Protocol, Src Port: 49696, Dst Port: 445, Seq: 0, Len: 0
    Source Port: 49696
    Destination Port: 445
    [Stream index: 24]
    [Stream Packet Number: 1]
  > [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3723464287
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x2eec [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

```
0000  00 0c 29 59 23 50 00 0c  29 06 cc 75 08 00 45 00
0010  00 34 03 c5 40 00 80 06  e1 f8 0a 00 00 82 0a 00
0020  00 85 c2 20 01 bd dd ef  8e 5f 00 00 00 00 80 02
0030  fa f0 2e ec 00 00 02 04  05 b4 01 03 03 08 01 01
0040  04 02
```

Here , I can see that the attacker is beginning a TCP 3 Way SYN ACK Handshake with this 10.0.0.133 host over Port 445. This could very well be just them accessing an SMB Share however since I know PSExec uses Port 445 this is relevant to my investigation.

The Question asks me *what host did the attacker initially gain access to?* Since they have already intruded into the network and is attempting to laterally move to 10.0.0.133 I can simply look at the Source IP for Packet #125 in the screenshot above. It appears that they have compromised the 10.0.0.130 host and are trying to laterally move using PSExec to 10.0.0.133!



Q1 ✓ Solved : 4528

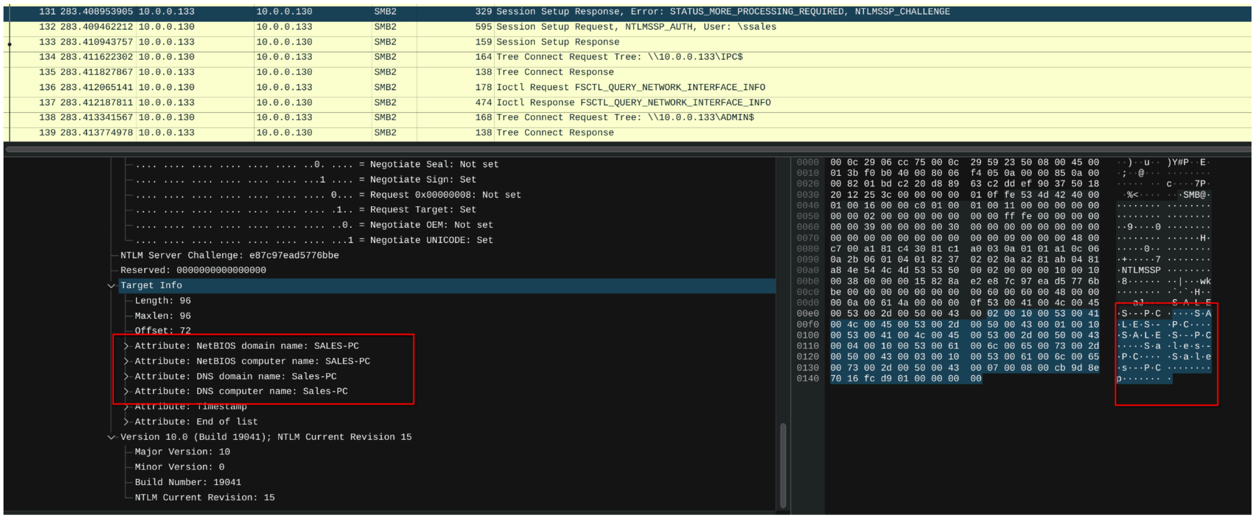
To effectively trace the attacker's activities within our network, can you identify the IP address of the machine from which the attacker initially gained access?

****

10.0.0.130

Robert Carpenter
github.com/robertmcarpenter
April 4th 2025

My next objective is to determine the machine's hostname to which the attacker first pivoted. I will analyze the SMB packets sent and received to discover the NetBIOS Target name.

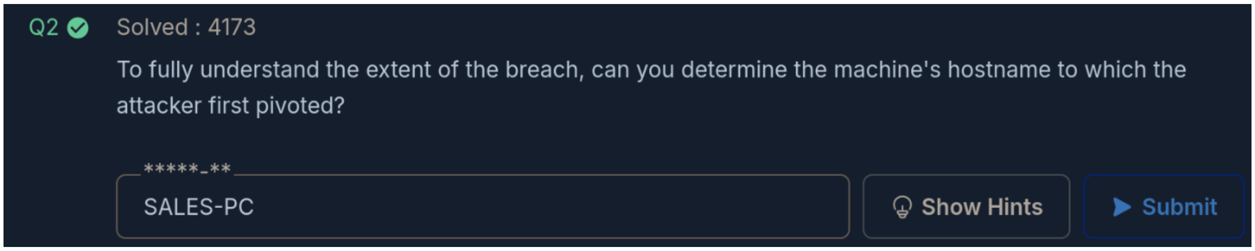


```
131 283.408953905 10.0.0.133   10.0.0.130   SMB2   329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
132 283.409462212 10.0.0.130   10.0.0.133   SMB2   595 Session Setup Request, NTLMSSP_AUTH, User: \ssales
133 283.410943757 10.0.0.133   10.0.0.130   SMB2   159 Session Setup Response
134 283.411622302 10.0.0.130   10.0.0.133   SMB2   164 Tree Connect Request Tree: \\10.0.0.133\IPC$
135 283.411827867 10.0.0.133   10.0.0.130   SMB2   138 Tree Connect Response
136 283.412065141 10.0.0.130   10.0.0.133   SMB2   178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
137 283.412187811 10.0.0.133   10.0.0.130   SMB2   474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
138 283.413341567 10.0.0.130   10.0.0.133   SMB2   168 Tree Connect Request Tree: \\10.0.0.133\ADMIN$
139 283.413774978 10.0.0.133   10.0.0.130   SMB2   138 Tree Connect Response
```

```
    .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
    .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
    .... .... .... .... .... .... .... 0... = Request 0x00000008: Not set
    .... .... .... .... .... .... .... .1.. = Request Target: Set
    .... .... .... .... .... .... .... ..0. = Negotiate OEM: Not set
    .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
  NTLM Server Challenge: e87c97ead5776bbe
  Reserved: 0000000000000000
  Target Info
    Length: 96
    Maxlen: 96
    Offset: 72
  > Attribute: NetBIOS domain name: SALES-PC
  > Attribute: NetBIOS computer name: SALES-PC
  > Attribute: DNS domain name: Sales-PC
  > Attribute: DNS computer name: Sales-PC
  > Attribute: Timestamp
  > Attribute: End of list
  Version 10.0 (Build 19041); NTLM Current Revision 15
    Major Version: 10
    Minor Version: 0
    Build Number: 19041
    NTLM Current Revision: 15
```

```
0000  00 0c 29 06 cc 75 00 0c  29 59 23 50 08 00 45 00   ··)··u·· )Y#P··E·
0010  01 3b f0 b0 40 00 80 06  f4 05 0a 00 00 85 0a 00   ·;··@··· ········
0020  00 82 01 bd c2 20 d8 89  63 c2 dd ef 90 37 50 18   ····· ·· c····7P·
0030  20 12 25 3c 00 00 00 00  01 0f fe 53 4d 42 40 00    ·%<···· ···SMB@·
0040  01 00 16 00 00 c0 01 00  01 00 11 00 00 00 00 00   ········ ········
0050  00 00 02 00 00 00 00 00  00 00 ff fe 00 00 00 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 09 00 00 00 48 00   ········ ······H·
0080  c7 00 a1 81 c4 30 81 c1  a0 03 0a 01 01 a1 0c 06   ·····0·· ········
0090  0a 2b 06 01 04 01 82 37  02 02 0a a2 81 ab 04 81   ·+·····7 ········
00a0  a8 4e 54 4c 4d 53 53 50  00 02 00 00 00 10 00 10   ·NTLMSSP ········
00b0  00 38 00 00 00 15 82 8a  e2 e8 7c 97 ea d5 77 6b   ·8······ ··|···wk
00c0  be 00 00 00 00 00 00 00  00 60 00 60 00 48 00 00   ········ ·`·`·H··
00d0  00 0a 00 61 4a 00 00 00  0f 53 00 41 00 4c 00 45   ···aJ··· ·S·A·L·E
00e0  00 53 00 2d 00 50 00 43  00 02 00 10 00 53 00 41   ·S·-·P·C ·····S·A
00f0  00 4c 00 45 00 53 00 2d  00 50 00 43 00 01 00 10   ·L·E·S·- ·P·C····
0100  00 53 00 41 00 4c 00 45  00 53 00 2d 00 50 00 43   ·S·A·L·E ·S·-·P·C
0110  00 04 00 10 00 53 00 61  00 6c 00 65 00 73 00 2d   ·····S·a ·l·e·s·-
0120  00 50 00 43 00 03 00 10  00 53 00 61 00 6c 00 65   ·P·C···· ·S·a·l·e
0130  00 73 00 2d 00 50 00 43  00 07 00 08 00 cb 9d 8e   ·s·-·P·C ········
0140  70 16 fc d9 01 00 00 00  00                        p······· ·
```

In the above screenshot you can see that inside Packet #131 the target machine responded with a challenge and inside the packet it gives it’s own NetBIOS name which is SALES-PC. This is the Hostname of the machine 10.0.0.133, the one that the attacker is trying to pivot/laterally move to.



Q2 Solved : 4173

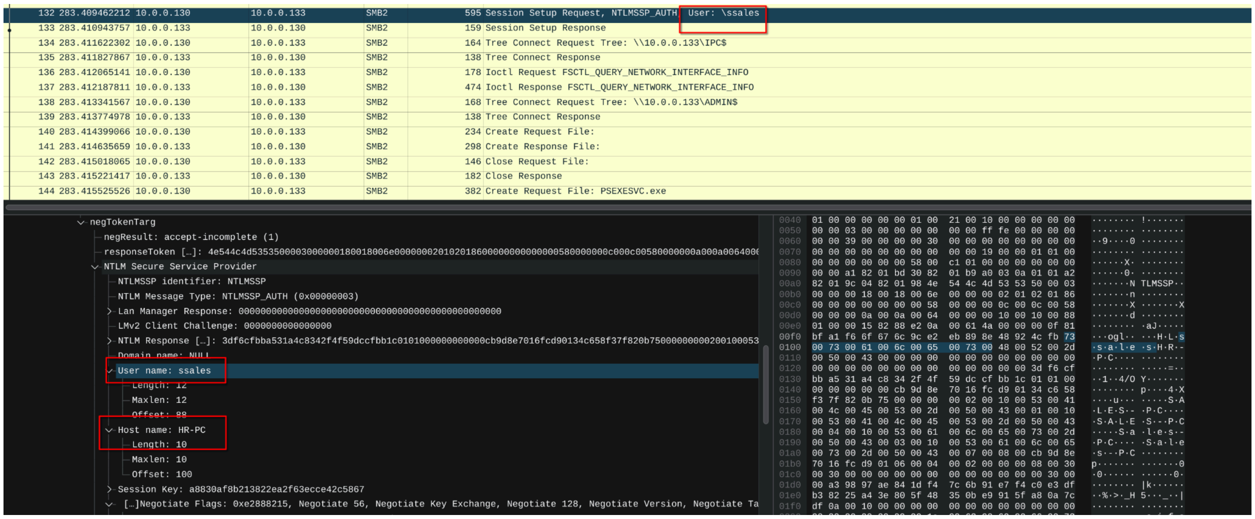
To fully understand the extent of the breach, can you determine the machine's hostname to which the attacker first pivoted?

*****-**

SALES-PC

Moving on, I need to now figure out the username utilized by the attacker for authentication. I will right click the packet and follow the TCP Stream to see what the attacker is sending to SALES-PC. Perhaps I can take a look to see what commands they are issuing via PsExec.

Robert Carpenter
github.com/robertmcarpenter
April 4th 2025



```
132 283.409462212 10.0.0.130   10.0.0.133   SMB2   595 Session Setup Request, NTLMSSP_AUTH, User: \ssales
133 283.410943757 10.0.0.133   10.0.0.130   SMB2   159 Session Setup Response
134 283.411622302 10.0.0.130   10.0.0.133   SMB2   164 Tree Connect Request Tree: \\10.0.0.133\IPC$
135 283.411827867 10.0.0.133   10.0.0.130   SMB2   138 Tree Connect Response
136 283.412065141 10.0.0.130   10.0.0.133   SMB2   178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
137 283.412187811 10.0.0.133   10.0.0.130   SMB2   474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
138 283.413341567 10.0.0.130   10.0.0.133   SMB2   168 Tree Connect Request Tree: \\10.0.0.133\ADMIN$
139 283.413774978 10.0.0.133   10.0.0.130   SMB2   138 Tree Connect Response
140 283.414399066 10.0.0.130   10.0.0.133   SMB2   234 Create Request File:
141 283.414635659 10.0.0.133   10.0.0.130   SMB2   298 Create Response File:
142 283.415018065 10.0.0.130   10.0.0.133   SMB2   146 Close Request File:
143 283.415221417 10.0.0.133   10.0.0.130   SMB2   182 Close Response
144 283.415525526 10.0.0.130   10.0.0.133   SMB2   382 Create Request File: PSEXESVC.exe
```

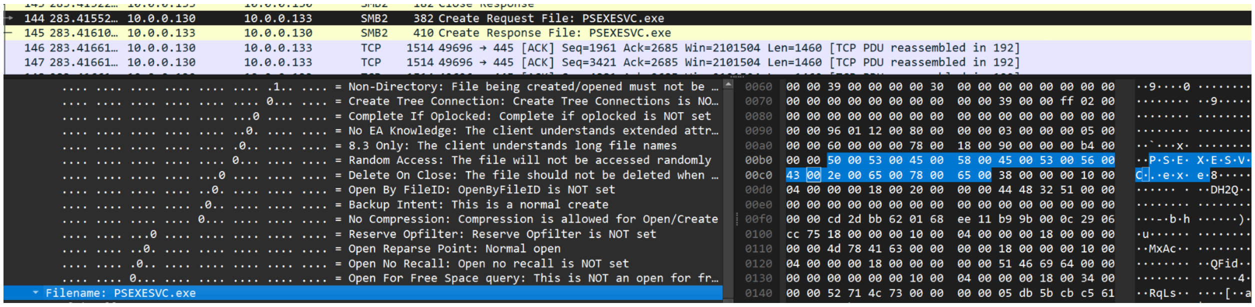
```
v negTokenTarg
    negResult: accept-incomplete (1)
    responseToken […]: 4e544c4d53535000030000001800180006e000000020102018600000000000000580000000c000c00580000000a000a006400
  v NTLM Secure Service Provider
      NTLMSSP identifier: NTLMSSP
      NTLM Message Type: NTLMSSP_AUTH (0x00000003)
    > Lan Manager Response: 000000000000000000000000000000000000000000000000
      LMv2 Client Challenge: 0000000000000000
    > NTLM Response […]: 3df6cfbba531a4c8342f4f59dccfbb1c0101000000000000cb9d8e7016fcd90134c658f37f820b7500000000000200100053
      Domain name: NULL
    v User name: ssales
        Length: 12
        Maxlen: 12
        Offset: 88
    v Host name: HR-PC
        Length: 10
        Maxlen: 10
        Offset: 100
    > Session Key: a8830af8b213822ea2f63ecce42c5867
    v  […]Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Ta
```

```
0040  01 00 00 00 00 00 01 00  21 00 10 00 00 00 00 00   ········ !·······
0050  00 00 03 00 00 00 00 00  00 00 ff fe 00 00 00 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 19 00 00 01 01 00   ········ ········
0080  00 00 00 00 00 00 58 00  c1 01 00 00 00 00 00 00   ······X· ········
0090  00 00 a1 82 01 bd 30 82  01 b9 a0 03 0a 01 01 a2   ······0· ········
00a0  82 01 9c 04 82 01 98 4e  54 4c 4d 53 53 50 00 03   ·······N TLMSSP··
00b0  00 00 00 18 00 18 00 6e  00 00 00 02 01 02 01 86   ·······n ········
00c0  00 00 00 00 00 00 00 58  00 00 00 0c 00 0c 00 58   ·······X ·······X
00d0  00 00 00 0a 00 0a 00 64  00 00 00 10 00 10 00 88   ·······d ········
00e0  01 00 00 15 82 88 e2 0a  00 61 4a 00 00 00 0f 81   ········ ·aJ·····
00f0  bf a1 f6 6f 67 6c 9c e2  eb 89 8e 48 92 4c fb 73   ···ogl·· ···H·L·s
0100  00 73 00 61 00 6c 00 65  00 73 00 48 00 52 00 2d   ·s·a·l·e ·s·H·R·-
0110  00 50 00 43 00 00 00 00  00 00 00 00 00 00 00 00   ·P·C···· ········
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 3d f6 cf   ········ ·····=··
0130  bb a5 31 a4 c8 34 2f 4f  59 dc cf bb 1c 01 01 00   ··1··4/O Y·······
0140  00 00 00 00 00 cb 9d 8e  70 16 fc d9 01 34 c6 58   ········ p····4·X
0150  f3 7f 82 0b 75 00 00 00  00 02 00 10 00 53 00 41   ····u··· ·····S·A
0160  00 4c 00 45 00 53 00 2d  00 50 00 43 00 01 00 10   ·L·E·S·- ·P·C····
0170  00 53 00 41 00 4c 00 45  00 53 00 2d 00 50 00 43   ·S·A·L·E ·S·-·P·C
0180  00 04 00 10 00 53 00 61  00 6c 00 65 00 73 00 2d   ·····S·a ·l·e·s·-
0190  00 50 00 43 00 03 00 10  00 53 00 61 00 6c 00 65   ·P·C···· ·S·a·l·e
01a0  00 73 00 2d 00 50 00 43  00 07 00 08 00 cb 9d 8e   ·s·-·P·C ········
01b0  70 16 fc d9 01 06 00 04  00 02 00 00 00 08 00 30   p······· ·······0
01c0  00 30 00 00 00 00 00 00  00 00 00 00 00 00 30 00   ·0······ ······0·
01d0  00 a3 98 97 ae 84 1d f4  7c 6b 91 e7 f4 c0 e3 df   ········ |k······
01e0  b3 82 25 a4 3e 80 5f 48  35 0b e9 91 5f a8 0a 7c   ··%·>·_H 5···_··|
01f0  df 0a 00 10 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

I can see in Packet #132 that they are attempting to login with the username **/ssales.** I also see another Hostname in this packet, this time it is named "HR-PC" (note to self: could this be the Active Directory Domain Controller?).

My next objective is to figure out what Service was started / added to the target machine. I know that when PsExec connects to a host, it drops a file called PsExecSvc.exe which is a service that runs on the target to allow the facilitation of its processes.

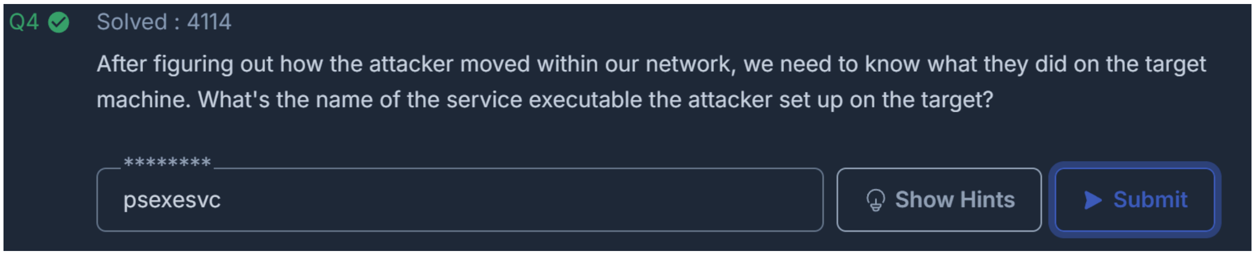
Looking down at Packet #144 I indeed see that the file was dropped.



```
144 283.41552…  10.0.0.130   10.0.0.133   SMB2    382 Create Request File: PSEXESVC.exe
145 283.41610…  10.0.0.133   10.0.0.130   SMB2    410 Create Response File: PSEXESVC.exe
146 283.41661…  10.0.0.130   10.0.0.133   TCP    1514 49696 → 445 [ACK] Seq=1961 Ack=2685 Win=2101504 Len=1460 [TCP PDU reassembled in 192]
147 283.41661…  10.0.0.130   10.0.0.133   TCP    1514 49696 → 445 [ACK] Seq=3421 Ack=2685 Win=2101504 Len=1460 [TCP PDU reassembled in 192]
```

```
.... .... .... .... .... .... .1.. .... = Non-Directory: File being created/opened must not be …
.... .... .... .... .... .... 0... .... = Create Tree Connection: Create Tree Connections is NO…
.... .... .... .... .... ...0 .... .... = Complete If Oplocked: Complete if oplocked is NOT set
.... .... .... .... .... ..0. .... .... = No EA Knowledge: The client understands extended attr…
.... .... .... .... .... .0.. .... .... = 8.3 Only: The client understands long file names
.... .... .... .... .... 0... .... .... = Random Access: The file will not be accessed randomly
.... .... .... .... ...0 .... .... .... = Delete On Close: The file should not be deleted when …
.... .... .... .... ..0. .... .... .... = Open By FileID: OpenByFileID is NOT set
.... .... .... .... .0.. .... .... .... = Backup Intent: This is a normal create
.... .... .... .... 0... .... .... .... = No Compression: Compression is allowed for Open/Create
.... .... ...0 .... .... .... .... .... = Reserve Opfilter: Reserve Opfilter is NOT set
.... .... ..0. .... .... .... .... .... = Open Reparse Point: Normal open
.... .... .0.. .... .... .... .... .... = Open No Recall: Open no recall is NOT set
.... .... 0... .... .... .... .... .... = Open For Free Space query: This is NOT an open for fr…
  Filename: PSEXESVC.exe
```

```
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 00 00 00 00 00 00 00   ········ ········
0090  00 00 96 01 12 00 80 00  00 00 03 00 00 00 05 00   ········ ········
00a0  00 00 60 00 00 00 78 00  18 00 90 00 00 00 b4 00   ··`···x· ········
00b0  00 00 50 00 53 00 45 00  58 00 45 00 53 00 56 00   ··P·S·E· X·E·S·V·
00c0  43 00 2e 00 65 00 78 00  65 00 38 00 00 00 10 00   C·.·e·x· e·8·····
00d0  04 00 00 00 18 00 20 00  00 00 44 48 32 51 00 00   ······ · ··DH2Q··
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 cd 2d bb 62 01 68  ee 11 b9 9b 00 0c 29 06   ···-·b·h ······)·
0100  cc 75 18 00 00 00 10 00  04 00 00 00 18 00 00 00   ·u······ ········
0110  00 00 4d 78 41 63 00 00  00 00 18 00 00 00 10 00   ··MxAc·· ········
0120  04 00 00 00 18 00 00 00  00 00 51 46 69 64 00 00   ········ ··QFid··
0130  00 00 00 00 00 00 10 00  04 00 00 00 18 00 34 00   ········ ······4·
0140  00 00 52 71 4c 73 00 00  00 00 05 db 5b cb c5 61   ··RqLs·· ····[··a
```



Q4 ✓ Solved : 4114

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?

****

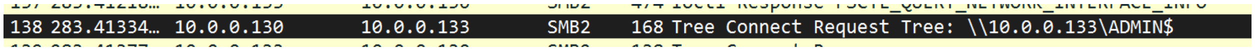
psexesvc

Robert Carpenter
github.com/robertmcarpenter
April 4th 2025

Now that I've figured out what service was dropped and started on the target machine I need to figure out how the attacker was able to achieve this.

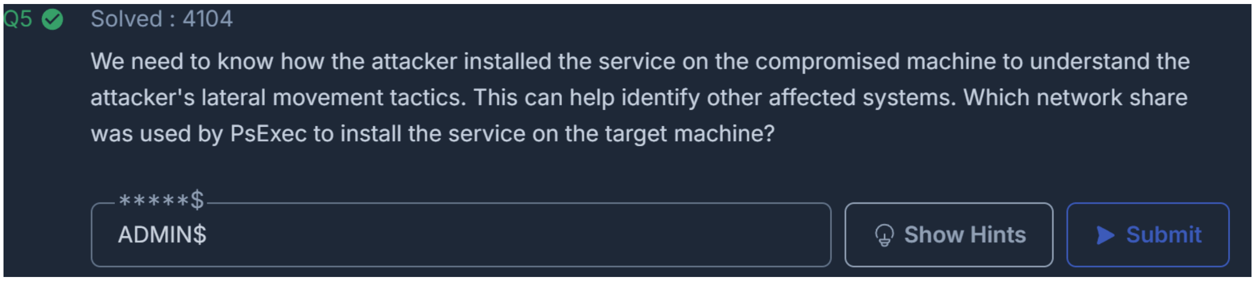
Question #5 asks:
We need to know how the attacker installed the service on the compromised machine to understand the attacker's lateral movement tactics. This can help identify other affected systems. Which network share was used by PsExec to install the service on the target machine?

Looking down the capture file , It brings me to packet #138 which states that they sent a request to connect to the ADMIN$ share.



```
138 283.41334…  10.0.0.130        10.0.0.133        SMB2    168 Tree Connect Request Tree: \\10.0.0.133\ADMIN$
```

Note to myself and the reader: The SMB Share ADMIN$ is a network share of the target system's %SYSTEMROOT% File Directory. This means that if an attacker is able to connect to a target using this share, they have access to the machine's C:\Windows\ directory and subdirectories. This is how the attacker was able to install this service.



Q5 ✓ Solved : 4104

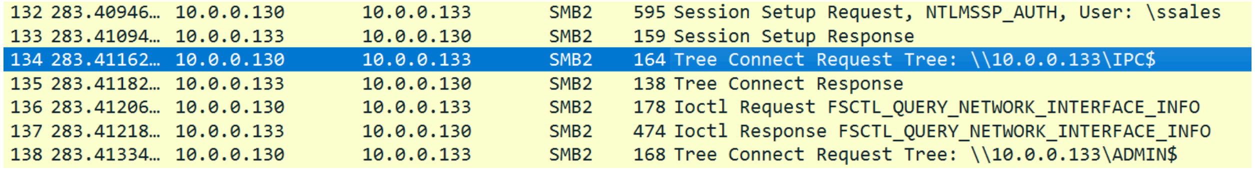
We need to know how the attacker installed the service on the compromised machine to understand the attacker's lateral movement tactics. This can help identify other affected systems. Which network share was used by PsExec to install the service on the target machine?

*****$
ADMIN$

My next objective after this is:
We must identify the network share used to communicate between the two machines. Which network share did PsExec use for communication?

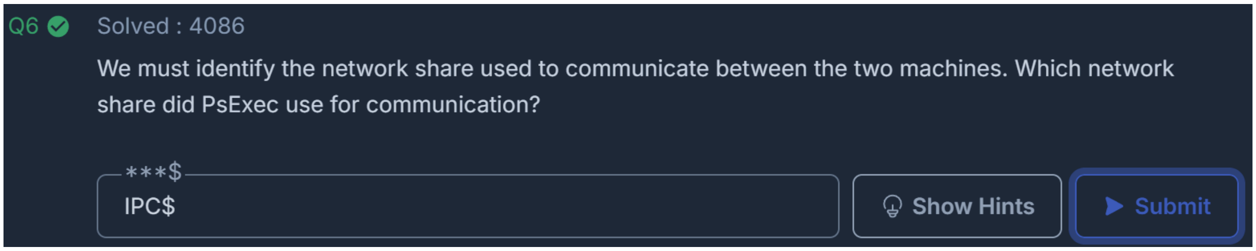
Looking back at the timeline of the SMB Connection requests I can see that the attacker first accessed the IPC$ share using the sales users, then opened a request to connect to the ADMIN$ share from there.

Attacker ———-> IPC$ Share ——-> ADMIN$ Share



```
132 283.40946…  10.0.0.130        10.0.0.133        SMB2    595 Session Setup Request, NTLMSSP_AUTH, User: \ssales
133 283.41094…  10.0.0.133        10.0.0.130        SMB2    159 Session Setup Response
134 283.41162…  10.0.0.130        10.0.0.133        SMB2    164 Tree Connect Request Tree: \\10.0.0.133\IPC$
135 283.41182…  10.0.0.133        10.0.0.130        SMB2    138 Tree Connect Response
136 283.41206…  10.0.0.130        10.0.0.133        SMB2    178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
137 283.41218…  10.0.0.133        10.0.0.130        SMB2    474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
138 283.41334…  10.0.0.130        10.0.0.133        SMB2    168 Tree Connect Request Tree: \\10.0.0.133\ADMIN$
```

Robert Carpenter
github.com/robertmcarpenter
April 4th 2025

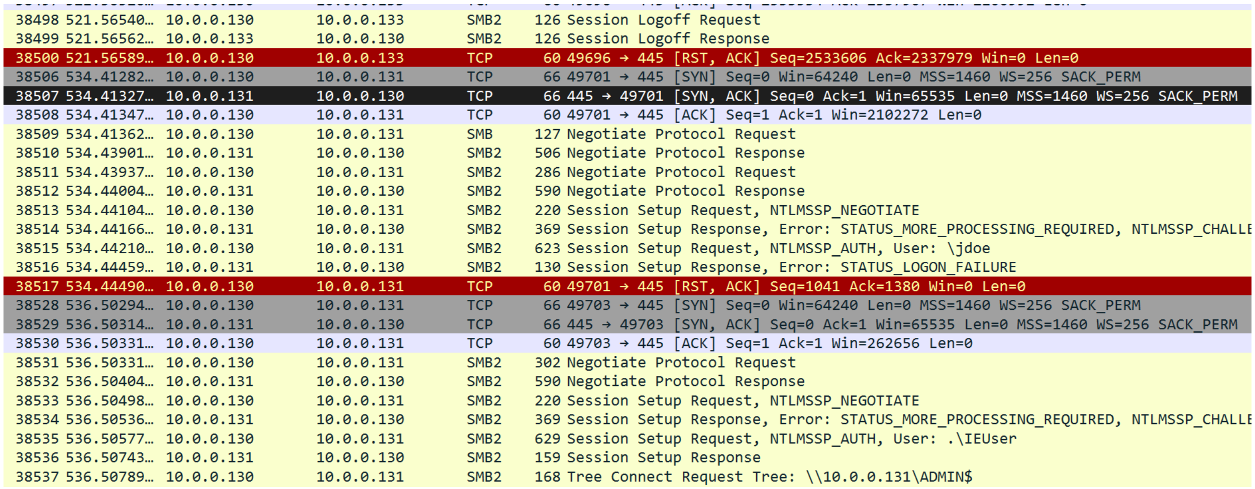


We must identify the network share used to communicate between the two machines. Which network share did PsExec use for communication?

***$
IPC$

The last task of this lab is to identify any further hosts that the attacker attempted to reach.

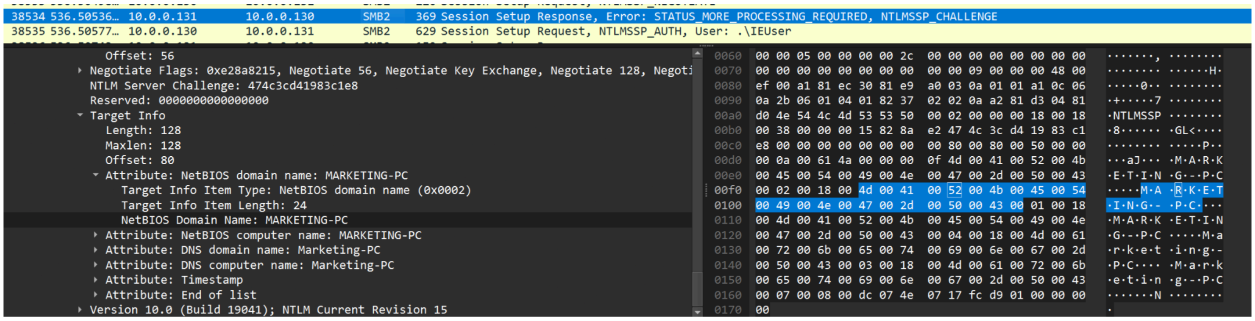
I will scroll down the .pcap file to check for any other IP addresses after the attacker closes the connection to 10.0.0.133.



```
38498 521.56540… 10.0.0.130     10.0.0.133     SMB2   126 Session Logoff Request
38499 521.56562… 10.0.0.133     10.0.0.130     SMB2   126 Session Logoff Response
38500 521.56589… 10.0.0.130     10.0.0.133     TCP     60 49696 → 445 [RST, ACK] Seq=2533606 Ack=2337979 Win=0 Len=0
38506 534.41282… 10.0.0.130     10.0.0.131     TCP     66 49701 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
38507 534.41327… 10.0.0.131     10.0.0.130     TCP     66 445 → 49701 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
38508 534.41347… 10.0.0.130     10.0.0.131     TCP     60 49701 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
38509 534.41362… 10.0.0.130     10.0.0.131     SMB    127 Negotiate Protocol Request
38510 534.43901… 10.0.0.131     10.0.0.130     SMB2   506 Negotiate Protocol Response
38511 534.43937… 10.0.0.130     10.0.0.131     SMB2   286 Negotiate Protocol Request
38512 534.44004… 10.0.0.131     10.0.0.130     SMB2   590 Negotiate Protocol Response
38513 534.44104… 10.0.0.130     10.0.0.131     SMB2   220 Session Setup Request, NTLMSSP_NEGOTIATE
38514 534.44166… 10.0.0.131     10.0.0.130     SMB2   369 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLE
38515 534.44210… 10.0.0.130     10.0.0.131     SMB2   623 Session Setup Request, NTLMSSP_AUTH, User: \jdoe
38516 534.44459… 10.0.0.131     10.0.0.130     SMB2   130 Session Setup Response, Error: STATUS_LOGON_FAILURE
38517 534.44490… 10.0.0.130     10.0.0.131     TCP     60 49701 → 445 [RST, ACK] Seq=1041 Ack=1380 Win=0 Len=0
38528 536.50294… 10.0.0.130     10.0.0.131     TCP     66 49703 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
38529 536.50314… 10.0.0.131     10.0.0.130     TCP     66 445 → 49703 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
38530 536.50331… 10.0.0.130     10.0.0.131     TCP     60 49703 → 445 [ACK] Seq=1 Ack=1 Win=262656 Len=0
38531 536.50331… 10.0.0.130     10.0.0.131     SMB2   302 Negotiate Protocol Request
38532 536.50404… 10.0.0.131     10.0.0.130     SMB2   590 Negotiate Protocol Response
38533 536.50498… 10.0.0.130     10.0.0.131     SMB2   220 Session Setup Request, NTLMSSP_NEGOTIATE
38534 536.50536… 10.0.0.131     10.0.0.130     SMB2   369 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLE
38535 536.50577… 10.0.0.130     10.0.0.131     SMB2   629 Session Setup Request, NTLMSSP_AUTH, User: .\IEUser
38536 536.50743… 10.0.0.131     10.0.0.130     SMB2   159 Session Setup Response
38537 536.50789… 10.0.0.130     10.0.0.131     SMB2   168 Tree Connect Request Tree: \\10.0.0.131\ADMIN$
```

I can see later on down the communications, packet #38498 the attacker Logs off the connection and then attempts to log in to a new endpoint located at 10.0.0.131.They first try to access the ADMIN$ share using the jdoe user. This fails then they attempt the IEUser. Ultimately, this ends up succeeding and they are able to access the network share. This happens to be the MARKETING-PC.

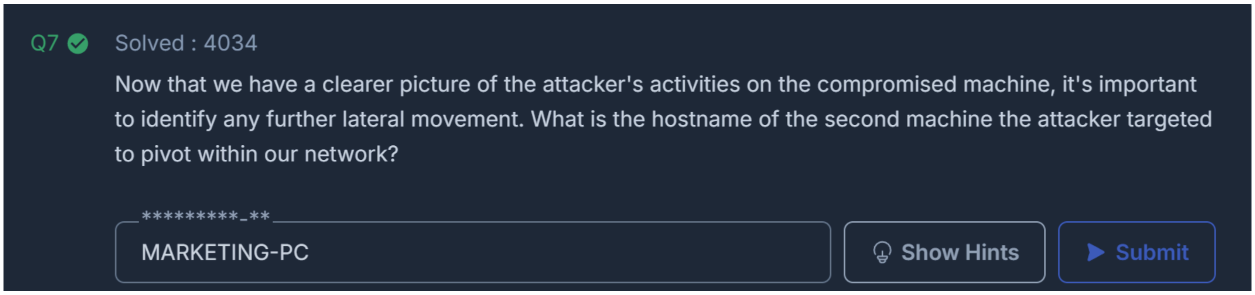
Robert Carpenter
github.com/robertmcarpenter
April 4th 2025



```
38534 536.50536… 10.0.0.131   10.0.0.130   SMB2   369 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
38535 536.50577… 10.0.0.130   10.0.0.131   SMB2   629 Session Setup Request, NTLMSSP_AUTH, User: .\IEUser
```

```
        Offset: 56
      › Negotiate Flags: 0xe28a8215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negoti
      NTLM Server Challenge: 474c3cd41983c1e8
      Reserved: 0000000000000000
    ⌄ Target Info
        Length: 128
        Maxlen: 128
        Offset: 80
      ⌄ Attribute: NetBIOS domain name: MARKETING-PC
          Target Info Item Type: NetBIOS domain name (0x0002)
          Target Info Item Length: 24
          NetBIOS Domain Name: MARKETING-PC
      › Attribute: NetBIOS computer name: MARKETING-PC
      › Attribute: DNS domain name: Marketing-PC
      › Attribute: DNS computer name: Marketing-PC
      › Attribute: Timestamp
      › Attribute: End of list
    › Version 10.0 (Build 19041); NTLM Current Revision 15
```

```
0060  00 00 05 00 00 00 00 2c  00 00 00 00 00 00 00 00   ·······, ········
0070  00 00 00 00 00 00 00 00  00 00 09 00 00 00 48 00   ········ ······H·
0080  ef 00 a1 81 ec 30 81 e9  a0 03 0a 01 01 a1 0c 06   ·····0·· ········
0090  0a 2b 06 01 04 01 82 37  02 02 0a a2 81 d3 04 81   ·+·····7 ········
00a0  d0 4e 54 4c 4d 53 53 50  00 02 00 00 00 18 00 18   ·NTLMSSP ········
00b0  00 38 00 00 00 15 82 8a  e2 47 4c 3c d4 19 83 c1   ·8······ ·GL<····
00c0  e8 00 00 00 00 00 00 00  00 80 00 80 00 50 00 00   ········ ·····P··
00d0  00 0a 00 61 4a 00 00 00  0f 4d 00 41 00 52 00 4b   ···aJ··· ·M·A·R·K
00e0  00 45 00 54 00 49 00 4e  00 47 00 2d 00 50 00 43   ·E·T·I·N ·G·-·P·C
00f0  00 02 00 18 00 4d 00 41  00 52 00 4b 00 45 00 54   ·····M·A ·R·K·E·T
0100  00 49 00 4e 00 47 00 2d  00 50 00 43 00 01 00 18   ·I·N·G·- ·P·C····
0110  00 4d 00 41 00 52 00 4b  00 45 00 54 00 49 00 4e   ·M·A·R·K ·E·T·I·N
0120  00 47 00 2d 00 50 00 43  00 04 00 18 00 4d 00 61   ·G·-·P·C ·····M·a
0130  00 72 00 6b 00 65 00 74  00 69 00 6e 00 67 00 2d   ·r·k·e·t ·i·n·g·-
0140  00 50 00 43 00 03 00 18  00 4d 00 61 00 72 00 6b   ·P·C···· ·M·a·r·k
0150  00 65 00 74 00 69 00 6e  00 67 00 2d 00 50 00 43   ·e·t·i·n ·g·-·P·C
0160  00 07 00 08 00 dc 07 4e  07 17 fc d9 01 00 00 00   ·······N ········
0170  00                                                 ·
```



Q7 ✓ Solved : 4034

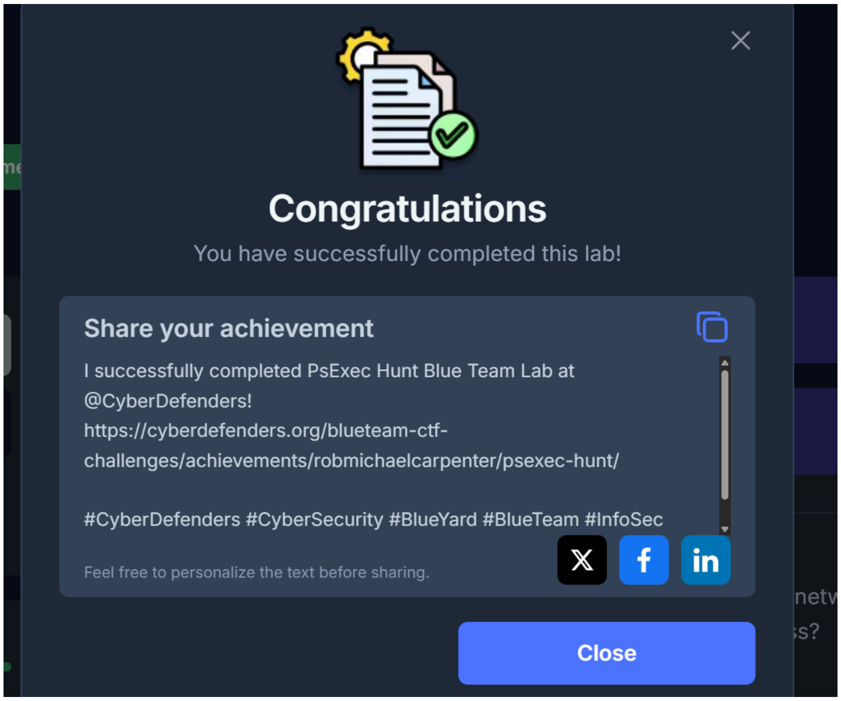
Now that we have a clearer picture of the attacker's activities on the compromised machine, it's important to identify any further lateral movement. What is the hostname of the second machine the attacker targeted to pivot within our network?

*********_**

MARKETING-PC

I have now tackled all 7 objectives of this lab!

In this lab I learned how to analyze a .pcap file to look for signs of lateral movement in a Windows Domain. The attacker used a popular LOLBIN name PsExec.exe which is used to execute remote commands to other Windows Endpoints across a domain.



Congratulations

You have successfully completed this lab!

Share your achievement

I successfully completed PsExec Hunt Blue Team Lab at @CyberDefenders! https://cyberdefenders.org/blueteam-ctf-challenges/achievements/robmichaelcarpenter/psexec-hunt/

#CyberDefenders #CyberSecurity #BlueYard #BlueTeam #InfoSec

Feel free to personalize the text before sharing.