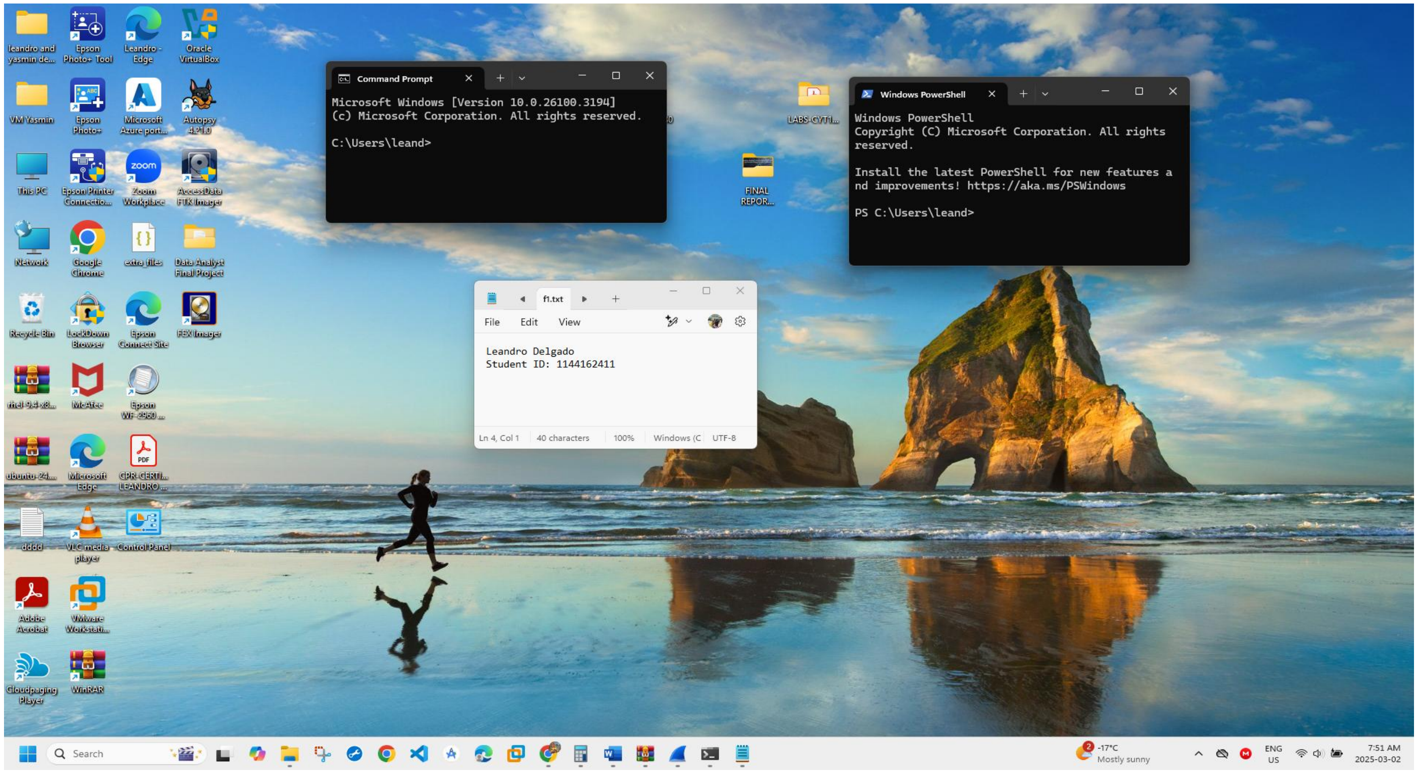
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
LEANDRO DELGADO	114416241	As Posted	6%

Name	Lab6: PsExec Hunt Network Forensics Challenge
Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above. • Show your genuine signs of your work is done on your machine. This includes: o Screenshots that show your desktop background with Date/Time. o Show a pop-up bx that shows "your name + IP". o Show your logged account when applicable. Optional: Your photo. • Submit your report name: CYT215-Lab6-Student Name & ID
Challenge Scenario	Our Intrusion Detection System (IDS) has raised an alert, indicating suspicious lateral movement activity involving the use of PsExec. To effectively respond to this incident, your role as a SOC Analyst is to analyze the captured network traffic stored in a PCAP file.
Challenge Questions To be Answered	

```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\leand>
```

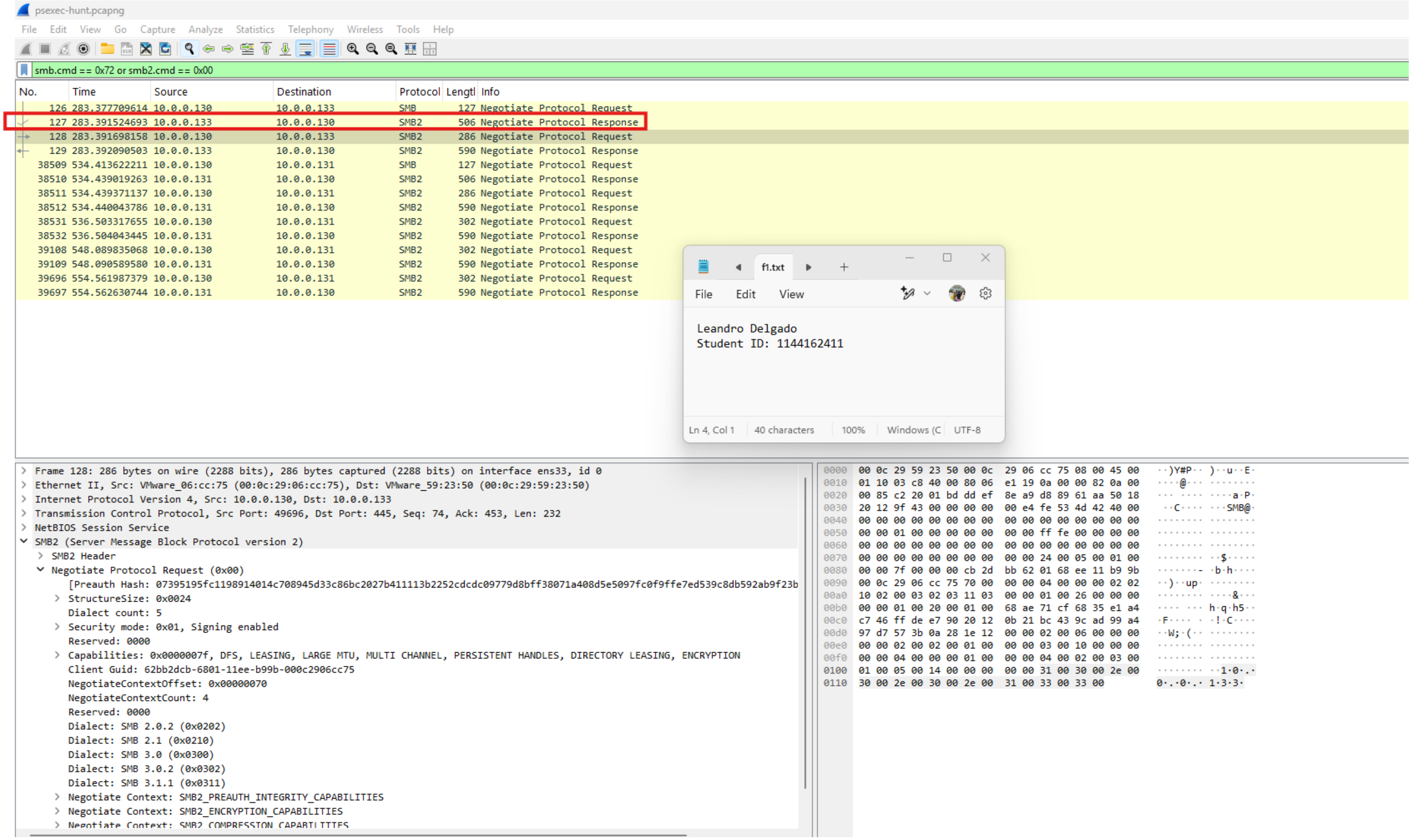
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights
reserved.

Install the latest PowerShell for new features a
nd improvements! https://aka.ms/PSWindows

PS C:\Users\leand>
```

Leandro Delgado
Student ID: 1144162411

1. 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? The IP adress is 10.0.0.130


psexec-hunt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb.cmd == 0x72 or smb2.cmd == 0x00

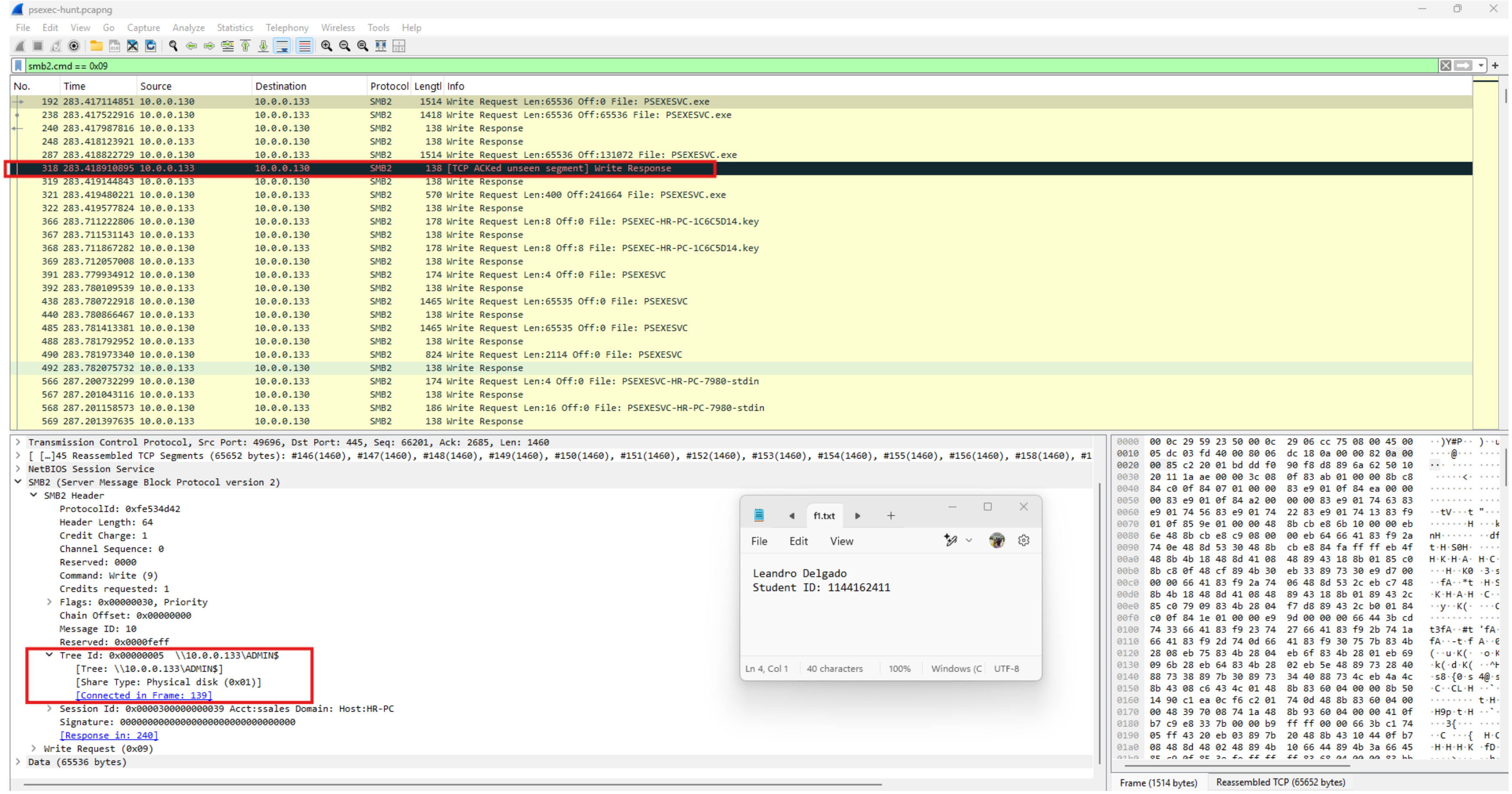
```
No.   Time          Source      Destination  Protocol Length Info
  126 283.377709614 10.0.0.130  10.0.0.133   SMB      127 Negotiate Protocol Request
  127 283.391524693 10.0.0.133  10.0.0.130   SMB2     506 Negotiate Protocol Response
  128 283.391698158 10.0.0.130  10.0.0.133   SMB2     286 Negotiate Protocol Request
  129 283.392090503 10.0.0.133  10.0.0.130   SMB2     590 Negotiate Protocol Response
38509 534.413622211 10.0.0.130  10.0.0.131   SMB      127 Negotiate Protocol Request
38510 534.439019263 10.0.0.131  10.0.0.130   SMB2     506 Negotiate Protocol Response
38511 534.439371137 10.0.0.130  10.0.0.131   SMB2     286 Negotiate Protocol Request
38512 534.440043786 10.0.0.131  10.0.0.130   SMB2     590 Negotiate Protocol Response
38531 536.503317655 10.0.0.130  10.0.0.131   SMB2     302 Negotiate Protocol Request
38532 536.504043445 10.0.0.131  10.0.0.130   SMB2     590 Negotiate Protocol Response
39108 548.089835068 10.0.0.130  10.0.0.131   SMB2     302 Negotiate Protocol Request
39109 548.090589580 10.0.0.131  10.0.0.130   SMB2     590 Negotiate Protocol Response
39696 554.561987379 10.0.0.130  10.0.0.131   SMB2     302 Negotiate Protocol Request
39697 554.562630744 10.0.0.131  10.0.0.130   SMB2     590 Negotiate Protocol Response
```

Leandro Delgado
Student ID: 1144162411

```
> Frame 128: 286 bytes on wire (2288 bits), 286 bytes captured (2288 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
> Transmission Control Protocol, Src Port: 49696, Dst Port: 445, Seq: 74, Ack: 453, Len: 232
> NetBIOS Session Service
v SMB2 (Server Message Block Protocol version 2)
  > SMB2 Header
  v Negotiate Protocol Request (0x00)
      [Preauth Hash: 07395195fc1198914014c708945d33c86bc2027b411113b2252cdcdc09779d8bff38071a408d5e5097fc0f9ffe7ed539c8db592ab9f23b
    > StructureSize: 0x0024
      Dialect count: 5
    > Security mode: 0x01, Signing enabled
      Reserved: 0000
    > Capabilities: 0x0000007f, DFS, LEASING, LARGE MTU, MULTI CHANNEL, PERSISTENT HANDLES, DIRECTORY LEASING, ENCRYPTION
      Client Guid: 62bb2dcb-6801-11ee-b99b-000c2906cc75
      NegotiateContextOffset: 0x00000070
      NegotiateContextCount: 4
      Reserved: 0000
      Dialect: SMB 2.0.2 (0x0202)
      Dialect: SMB 2.1 (0x0210)
      Dialect: SMB 3.0 (0x0300)
      Dialect: SMB 3.0.2 (0x0302)
      Dialect: SMB 3.1.1 (0x0311)
    > Negotiate Context: SMB2_PREAUTH_INTEGRITY_CAPABILITIES
    > Negotiate Context: SMB2_ENCRYPTION_CAPABILITIES
    > Negotiate Context: SMB2_COMPRESSION_CAPABILITIES
```

```
0000  00 0c 29 59 23 50 00 0c  29 06 cc 75 08 00 45 00   ··)Y#P·· )··u··E·
0010  01 10 03 c8 40 00 80 06  e1 19 0a 00 00 82 0a 00   ····@··· ········
0020  00 85 c2 20 01 bd dd ef  8e a9 d8 89 61 aa 50 18   ··· ···· ····a·P·
0030  20 12 9f 43 00 00 00 00  00 e4 fe 53 4d 42 40 00    ··C···· ···SMB@·
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 01 00 00 00 00 00  00 00 ff fe 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 24 00 05 00 01 00   ········ ··$·····
0080  00 00 7f 00 00 00 cb 2d  bb 62 01 68 ee 11 b9 9b   ·······- ·b·h····
0090  00 0c 29 06 cc 75 70 00  00 00 04 00 00 00 02 02   ··)··up· ········
00a0  10 02 00 03 02 03 11 03  00 00 01 00 26 00 00 00   ········ ····&···
00b0  00 00 01 00 20 00 01 00  68 ae 71 cf 68 35 e1 a4   ···· ··· h·q·h5··
00c0  c7 46 ff de e7 90 20 12  0b 21 bc 43 9c ad 99 a4   ·F···· · ·!·C····
00d0  97 d7 57 3b 0a 28 1e 12  00 00 02 00 06 00 00 00   ··W;·(·· ········
00e0  00 00 02 00 02 00 01 00  00 00 03 00 10 00 00 00   ········ ········
00f0  00 00 04 00 00 00 01 00  00 00 04 00 02 00 03 00   ········ ········
0100  01 00 05 00 14 00 00 00  00 00 31 00 30 00 2e 00   ········ ··1·0·.·
0110  30 00 2e 00 30 00 2e 00  31 00 33 00 33 00         0·.·0·.· 1·3·3·
```

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



psexec-hunt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb2.cmd == 0x09

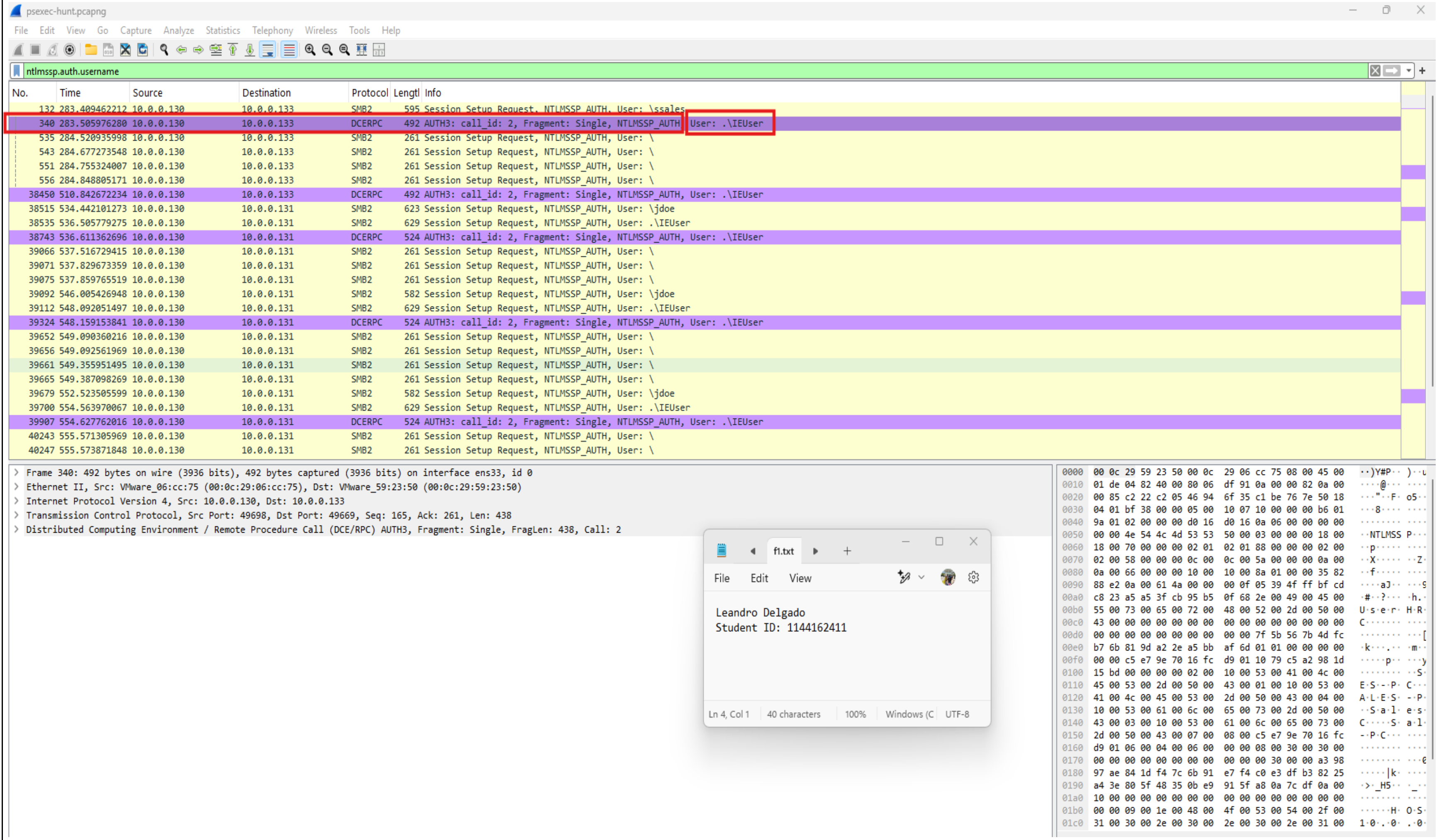
```
No.  Time          Source      Destination  Protocol Length Info
192 283.417114851 10.0.0.130  10.0.0.133   SMB2   1514 Write Request Len:65536 Off:0 File: PSEXESVC.exe
238 283.417522916 10.0.0.130  10.0.0.133   SMB2   1418 Write Request Len:65536 Off:65536 File: PSEXESVC.exe
240 283.417987816 10.0.0.133  10.0.0.130   SMB2    138 Write Response
248 283.418123921 10.0.0.133  10.0.0.130   SMB2    138 Write Response
287 283.418822729 10.0.0.130  10.0.0.133   SMB2   1514 Write Request Len:65536 Off:131072 File: PSEXESVC.exe
318 283.418910895 10.0.0.133  10.0.0.130   SMB2    138 [TCP ACKed unseen segment] Write Response
319 283.419144843 10.0.0.133  10.0.0.130   SMB2    138 Write Response
321 283.419480221 10.0.0.130  10.0.0.133   SMB2    570 Write Request Len:400 Off:241664 File: PSEXESVC.exe
322 283.419577824 10.0.0.133  10.0.0.130   SMB2    138 Write Response
366 283.711222806 10.0.0.130  10.0.0.133   SMB2    178 Write Request Len:8 Off:0 File: PSEXEC-HR-PC-1C6C5D14.key
367 283.711531143 10.0.0.133  10.0.0.130   SMB2    138 Write Response
368 283.711867282 10.0.0.130  10.0.0.133   SMB2    178 Write Request Len:8 Off:8 File: PSEXEC-HR-PC-1C6C5D14.key
369 283.712057008 10.0.0.133  10.0.0.130   SMB2    138 Write Response
391 283.779934912 10.0.0.130  10.0.0.133   SMB2    174 Write Request Len:4 Off:0 File: PSEXESVC
392 283.780109539 10.0.0.133  10.0.0.130   SMB2    138 Write Response
438 283.780722918 10.0.0.130  10.0.0.133   SMB2   1465 Write Request Len:65535 Off:0 File: PSEXESVC
440 283.780866467 10.0.0.133  10.0.0.130   SMB2    138 Write Response
485 283.781413381 10.0.0.130  10.0.0.133   SMB2   1465 Write Request Len:65535 Off:0 File: PSEXESVC
488 283.781792952 10.0.0.133  10.0.0.130   SMB2    138 Write Response
490 283.781973340 10.0.0.130  10.0.0.133   SMB2    824 Write Request Len:2114 Off:0 File: PSEXESVC
492 283.782075732 10.0.0.133  10.0.0.130   SMB2    138 Write Response
566 287.200732299 10.0.0.130  10.0.0.133   SMB2    174 Write Request Len:4 Off:0 File: PSEXESVC-HR-PC-7980-stdin
567 287.201043116 10.0.0.133  10.0.0.130   SMB2    138 Write Response
568 287.201158573 10.0.0.130  10.0.0.133   SMB2    186 Write Request Len:16 Off:0 File: PSEXESVC-HR-PC-7980-stdin
569 287.201397635 10.0.0.133  10.0.0.130   SMB2    138 Write Response
```

```
> Transmission Control Protocol, Src Port: 49696, Dst Port: 445, Seq: 66201, Ack: 2685, Len: 1460
> [ […]45 Reassembled TCP Segments (65652 bytes): #146(1460), #147(1460), #148(1460), #149(1460), #150(1460), #151(1460), #152(1460), #153(1460), #154(1460), #155(1460), #156(1460), #158(1460), #1
> NetBIOS Session Service
v SMB2 (Server Message Block Protocol version 2)
  v SMB2 Header
      ProtocolId: 0xfe534d42
      Header Length: 64
      Credit Charge: 1
      Channel Sequence: 0
      Reserved: 0000
      Command: Write (9)
      Credits requested: 1
    > Flags: 0x00000030, Priority
      Chain Offset: 0x00000000
      Message ID: 10
      Reserved: 0x0000feff
    v Tree Id: 0x00000005  \\10.0.0.133\ADMIN$
        [Tree: \\10.0.0.133\ADMIN$]
        [Share Type: Physical disk (0x01)]
        [Connected in Frame: 139]
    > Session Id: 0x0000300000000039 Acct:ssales Domain: Host:HR-PC
      Signature: 00000000000000000000000000000000
      [Response in: 240]
  > Write Request (0x09)
> Data (65536 bytes)
```

```
0000  00 0c 29 59 23 50 00 0c  29 06 cc 75 08 00 45 00   ··)Y#P·· )··u
0010  05 dc 03 fd 40 00 80 06  dc 18 0a 00 00 82 0a 00   ····@··· ····
0020  00 85 c2 20 01 bd dd f0  90 f8 d8 89 6a 62 50 10   ··· ···· ····
0030  20 11 1a ae 00 00 3c 08  0f 83 ab 01 00 00 8b c8    ······< ····
0040  84 c0 0f 84 07 01 00 00  83 e9 01 0f 84 ea 00 00   ········ ····
0050  00 83 e9 01 0f 84 a2 00  00 00 83 e9 01 74 63 83   ········ ····
0060  e9 01 74 56 83 e9 01 74  22 83 e9 01 74 13 83 f9   ··tV···t "···
0070  01 0f 85 9e 01 00 00 48  8b cb e8 6b 10 00 00 eb   ·······H ···k
0080  6e 48 8b cb e8 c9 08 00  00 eb 64 66 41 83 f9 2a   nH······ ··df
0090  74 0e 48 8d 53 30 48 8b  cb e8 84 fa ff ff eb 4f   t·H·S0H· ····
00a0  48 8b 4b 18 48 8d 41 08  48 89 43 18 8b 01 85 c0   H·K·H·A· H·C·
00b0  8b c8 0f 48 cf 89 4b 30  eb 33 89 73 30 e9 d7 00   ···H··K0 ·3·s
00c0  00 00 66 41 83 f9 2a 74  06 48 8d 53 2c eb c7 48   ··fA··*t ·H·S
00d0  8b 4b 18 48 8d 41 08 48  89 43 18 8b 01 89 43 2c   ·K·H·A·H ·C··
00e0  85 c0 79 09 83 4b 28 04  f7 d8 89 43 2c b0 01 84   ··y··K(· ···C
00f0  c0 0f 84 1e 01 00 00 e9  9d 00 00 00 66 44 3b cd   ········ ····
0100  74 33 66 41 83 f9 23 74  27 66 41 83 f9 2b 74 1a   t3fA··#t 'fA·
0110  66 41 83 f9 2d 74 0d 66  41 83 f9 30 75 7b 83 4b   fA··-t·f A··0
0120  28 08 eb 75 83 4b 28 04  eb 6f 83 4b 28 01 eb 69   (··u·K(· ·o·K
0130  09 6b 28 eb 64 83 4b 28  02 eb 5e 48 89 73 28 40   ·k(·d·K( ··^H
0140  88 73 38 89 7b 30 89 73  34 40 88 73 4c eb 4a 4c   ·s8·{0·s 4@·s
0150  8b 43 08 c6 43 4c 01 48  8b 83 60 04 00 00 8b 50   ·C··CL·H ··`·
0160  14 90 c1 ea 0c f6 c2 01  74 0d 48 8b 83 60 04 00   ········ t·H·
0170  00 48 39 70 08 74 1a 48  8b 93 60 04 00 00 41 0f   ·H9p·t·H ··`·
0180  b7 c9 e8 33 7b 00 00 b9  ff ff 00 00 66 3b c1 74   ···3{··· ····
0190  05 ff 43 20 eb 03 89 7b  20 48 8b 43 10 44 0f b7   ··C ···{  H·C
01a0  08 48 8d 48 02 48 89 4b  10 66 44 89 4b 3a 66 45   ·H·H·H·K ·fD·
```

Leandro Delgado
Student ID: 1144162411

3. 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?


psexec-hunt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ntlmssp.auth.username

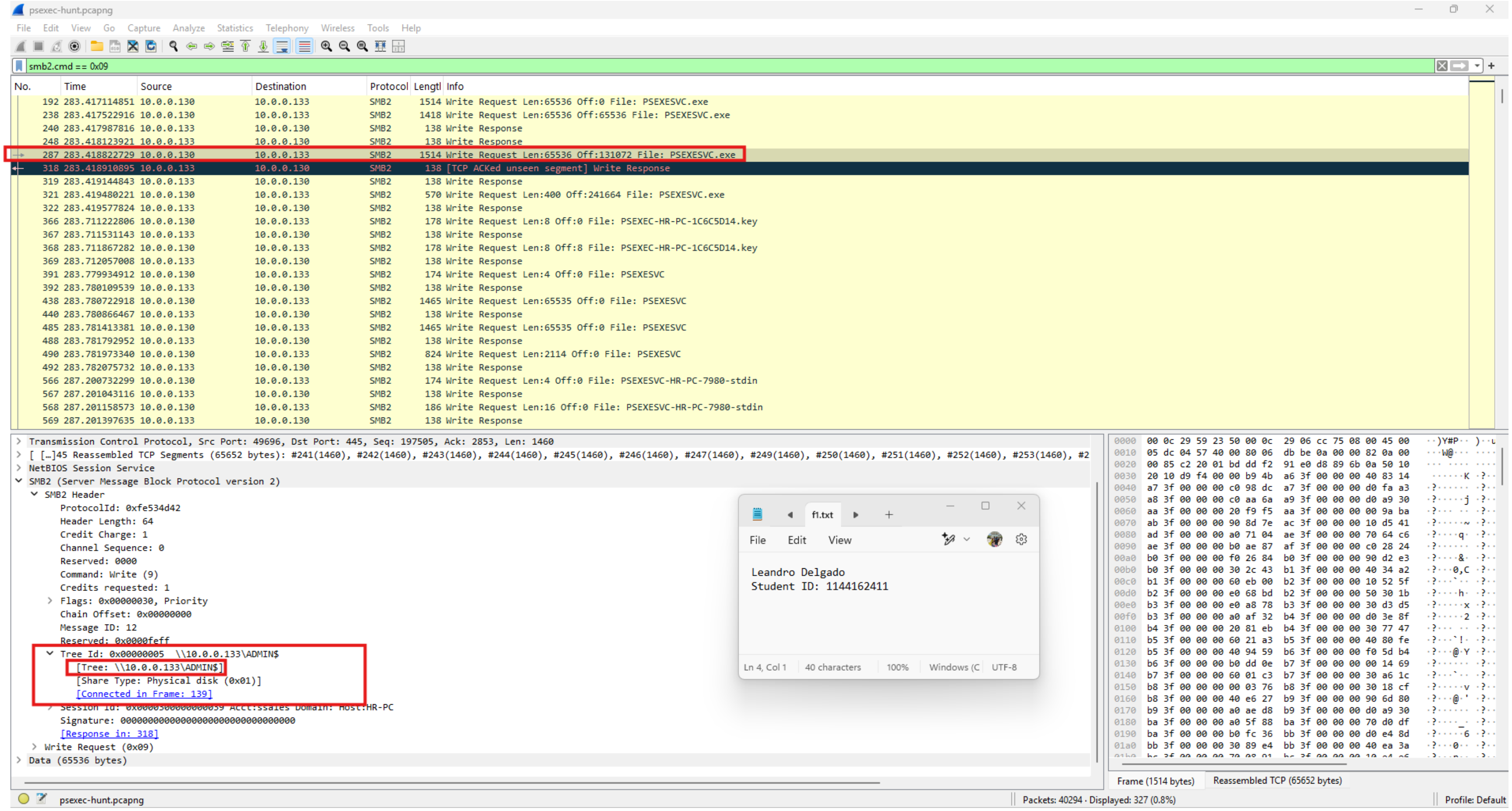
```
No.    Time          Source      Destination  Protocol Lengtl Info
  132 283.409462212 10.0.0.130  10.0.0.133   SMB2      595 Session Setup Request, NTLMSSP_AUTH, User: \ssales
  340 283.505976280 10.0.0.130  10.0.0.133   DCERPC    492 AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User: .\IEUser
  535 284.520935998 10.0.0.130  10.0.0.133   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
  543 284.677273548 10.0.0.130  10.0.0.133   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
  551 284.755324007 10.0.0.130  10.0.0.133   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
  556 284.848805171 10.0.0.130  10.0.0.133   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
38450 510.842672234 10.0.0.130  10.0.0.133   DCERPC    492 AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User: .\IEUser
38515 534.442101273 10.0.0.130  10.0.0.131   SMB2      623 Session Setup Request, NTLMSSP_AUTH, User: \jdoe
38535 536.505779275 10.0.0.130  10.0.0.131   SMB2      629 Session Setup Request, NTLMSSP_AUTH, User: .\IEUser
38743 536.611362696 10.0.0.130  10.0.0.131   DCERPC    524 AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User: .\IEUser
39066 537.516729415 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
39071 537.829673359 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
39075 537.859765519 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
39092 546.005426948 10.0.0.130  10.0.0.131   SMB2      582 Session Setup Request, NTLMSSP_AUTH, User: \jdoe
39112 548.092051497 10.0.0.130  10.0.0.131   SMB2      629 Session Setup Request, NTLMSSP_AUTH, User: .\IEUser
39324 548.159153841 10.0.0.130  10.0.0.131   DCERPC    524 AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User: .\IEUser
39652 549.090360216 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
39656 549.092561969 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
39661 549.355951495 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
39665 549.387098269 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
39679 552.523505599 10.0.0.130  10.0.0.131   SMB2      582 Session Setup Request, NTLMSSP_AUTH, User: \jdoe
39700 554.563970067 10.0.0.130  10.0.0.131   SMB2      629 Session Setup Request, NTLMSSP_AUTH, User: .\IEUser
39907 554.627762016 10.0.0.130  10.0.0.131   DCERPC    524 AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User: .\IEUser
40243 555.571305969 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
40247 555.573871848 10.0.0.130  10.0.0.131   SMB2      261 Session Setup Request, NTLMSSP_AUTH, User: \
```

```
> Frame 340: 492 bytes on wire (3936 bits), 492 bytes captured (3936 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
> Transmission Control Protocol, Src Port: 49698, Dst Port: 49669, Seq: 165, Ack: 261, Len: 438
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) AUTH3, Fragment: Single, FragLen: 438, Call: 2
```

```
0000  00 0c 29 59 23 50 00 0c  29 06 cc 75 08 00 45 00   ··)Y#P·· )··u
0010  01 de 04 82 40 00 80 06  df 91 0a 00 00 82 0a 00   ····@··· ····
0020  00 85 c2 22 c2 05 46 94  6f 35 c1 be 76 7e 50 18   ···"··F· o5··
0030  04 01 bf 38 00 00 05 00  10 07 10 00 00 00 b6 01   ···8···· ····
0040  9a 01 02 00 00 00 d0 16  d0 16 0a 06 00 00 00 00   ········ ····
0050  00 00 4e 54 4c 4d 53 53  50 00 03 00 00 00 18 00   ··NTLMSS P···
0060  18 00 70 00 00 00 02 01  02 01 88 00 00 00 02 00   ··p····· ····
0070  02 00 58 00 00 00 0c 00  0c 00 5a 00 00 00 0a 00   ··X····· ··Z·
0080  0a 00 66 00 00 00 10 00  10 00 8a 01 00 00 35 82   ··f····· ····
0090  88 e2 0a 00 61 4a 00 00  00 0f 05 39 4f ff bf cd   ····aJ·· ···9
00a0  c8 23 a5 a5 3f cb 95 b5  0f 68 2e 00 49 00 45 00   ·#··?··· ·h.·
00b0  55 00 73 00 65 00 72 00  48 00 52 00 2d 00 50 00   U·s·e·r· H·R·
00c0  43 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   C······· ····
00d0  00 00 00 00 00 00 00 00  00 00 7f 5b 56 7b 4d fc   ········ ···[
00e0  b7 6b 81 9d a2 2e a5 bb  af 6d 01 01 00 00 00 00   ·k···.·· ·m··
00f0  00 00 c5 e7 9e 70 16 fc  d9 01 10 79 c5 a2 98 1d   ·····p·· ···y
0100  15 bd 00 00 00 00 02 00  10 00 53 00 41 00 4c 00   ········ ··S·
0110  45 00 53 00 2d 00 50 00  43 00 01 00 10 00 53 00   E·S·-·P· C···
0120  41 00 4c 00 45 00 53 00  2d 00 50 00 43 00 04 00   A·L·E·S· -·P·
0130  10 00 53 00 61 00 6c 00  65 00 73 00 2d 00 50 00   ··S·a·l· e·s·
0140  43 00 03 00 10 00 53 00  61 00 6c 00 65 00 73 00   C·····S· a·l·
0150  2d 00 50 00 43 00 07 00  08 00 c5 e7 9e 70 16 fc   -·P·C··· ····
0160  d9 01 06 00 04 00 06 00  00 00 08 00 30 00 30 00   ········ ····
0170  00 00 00 00 00 00 00 00  00 00 00 30 00 00 a3 98   ········ ···0
0180  97 ae 84 1d f4 7c 6b 91  e7 f4 c0 e3 df b3 82 25   ·····|k· ····
0190  a4 3e 80 5f 48 35 0b e9  91 5f a8 0a 7c df 0a 00   ·>·_H5·· ·_··
01a0  10 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ····
01b0  00 00 09 00 1e 00 48 00  4f 00 53 00 54 00 2f 00   ······H· O·S·
01c0  31 00 30 00 2e 00 30 00  2e 00 30 00 2e 00 31 00   1·0·.·0· .·0·
```

Leandro Delgado
Student ID: 1144162411

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?


psexec-hunt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb2.cmd == 0x09

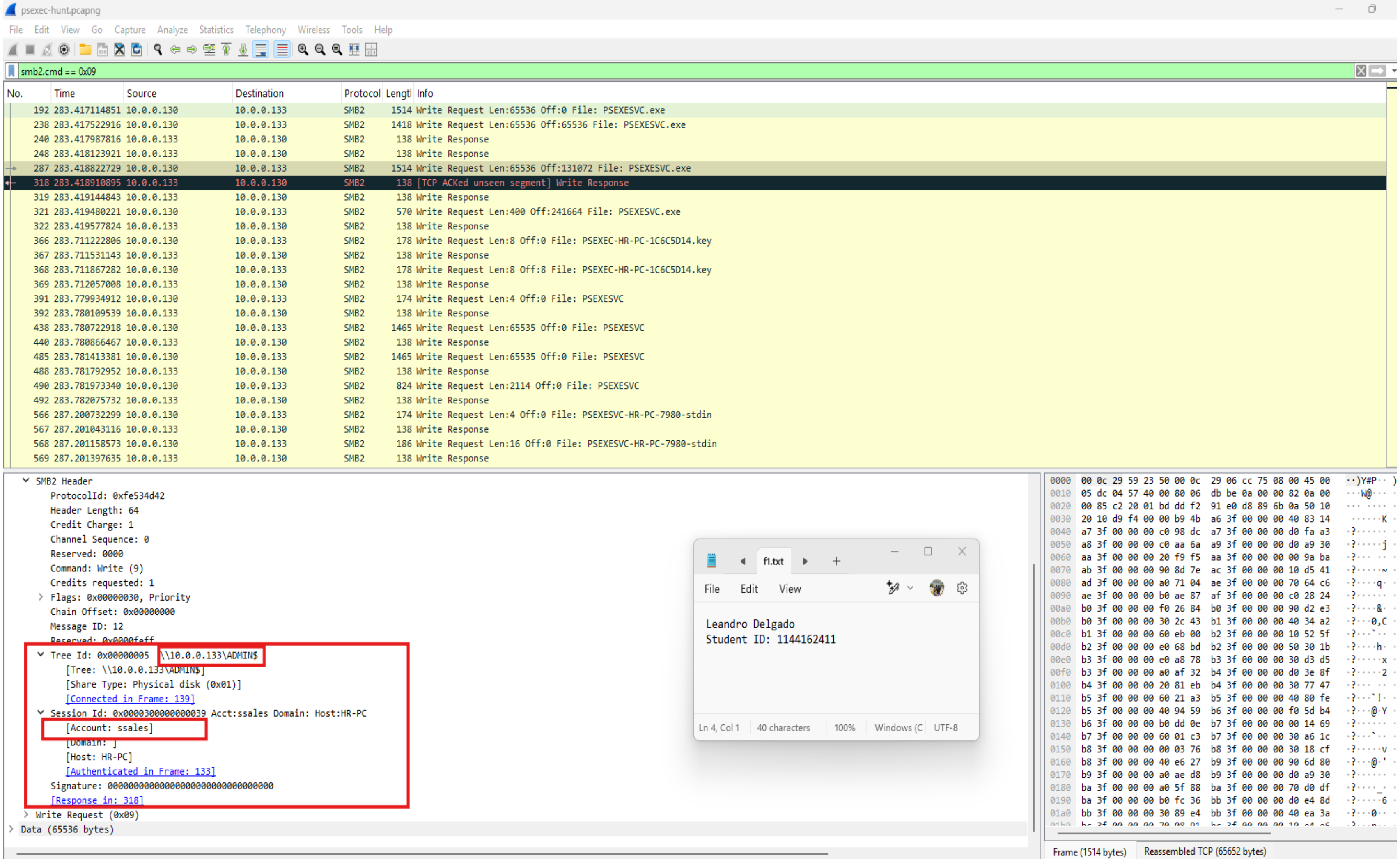
```
No.   Time          Source       Destination   Protocol Lengtl Info
  192 283.417114851 10.0.0.130   10.0.0.133    SMB2     1514 Write Request Len:65536 Off:0 File: PSEXESVC.exe
  238 283.417522916 10.0.0.130   10.0.0.133    SMB2     1418 Write Request Len:65536 Off:65536 File: PSEXESVC.exe
  240 283.417987816 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  248 283.418123921 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  287 283.418822729 10.0.0.130   10.0.0.133    SMB2     1514 Write Request Len:65536 Off:131072 File: PSEXESVC.exe
  318 283.418910895 10.0.0.133   10.0.0.130    SMB2      138 [TCP ACKed unseen segment] Write Response
  319 283.419144843 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  321 283.419480221 10.0.0.130   10.0.0.133    SMB2      570 Write Request Len:400 Off:241664 File: PSEXESVC.exe
  322 283.419577824 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  366 283.711222806 10.0.0.130   10.0.0.133    SMB2      178 Write Request Len:8 Off:0 File: PSEXEC-HR-PC-1C6C5D14.key
  367 283.711531143 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  368 283.711867282 10.0.0.130   10.0.0.133    SMB2      178 Write Request Len:8 Off:8 File: PSEXEC-HR-PC-1C6C5D14.key
  369 283.712057008 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  391 283.779934912 10.0.0.130   10.0.0.133    SMB2      174 Write Request Len:4 Off:0 File: PSEXESVC
  392 283.780109539 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  438 283.780722918 10.0.0.130   10.0.0.133    SMB2     1465 Write Request Len:65535 Off:0 File: PSEXESVC
  440 283.780866467 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  485 283.781413381 10.0.0.130   10.0.0.133    SMB2     1465 Write Request Len:65535 Off:0 File: PSEXESVC
  488 283.781792952 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  490 283.781973340 10.0.0.130   10.0.0.133    SMB2      824 Write Request Len:2114 Off:0 File: PSEXESVC
  492 283.782075732 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  566 287.200732299 10.0.0.130   10.0.0.133    SMB2      174 Write Request Len:4 Off:0 File: PSEXESVC-HR-PC-7980-stdin
  567 287.201043116 10.0.0.133   10.0.0.130    SMB2      138 Write Response
  568 287.201158573 10.0.0.130   10.0.0.133    SMB2      186 Write Request Len:16 Off:0 File: PSEXESVC-HR-PC-7980-stdin
  569 287.201397635 10.0.0.133   10.0.0.130    SMB2      138 Write Response
```

```
> Transmission Control Protocol, Src Port: 49696, Dst Port: 445, Seq: 197505, Ack: 2853, Len: 1460
> [ […]45 Reassembled TCP Segments (65652 bytes): #241(1460), #242(1460), #243(1460), #244(1460), #245(1460), #246(1460), #247(1460), #249(1460), #250(1460), #251(1460), #252(1460), #253(1460), #2
> NetBIOS Session Service
v SMB2 (Server Message Block Protocol version 2)
  v SMB2 Header
      ProtocolId: 0xfe534d42
      Header Length: 64
      Credit Charge: 1
      Channel Sequence: 0
      Reserved: 0000
      Command: Write (9)
      Credits requested: 1
    > Flags: 0x00000030, Priority
      Chain Offset: 0x00000000
      Message ID: 12
      Reserved: 0x0000feff
    v Tree Id: 0x00000005  \\10.0.0.133\ADMIN$
        [Tree: \\10.0.0.133\ADMIN$]
        [Share Type: Physical disk (0x01)]
        [Connected in Frame: 139]
    > Session Id: 0x0000030000000039 Acct:ssales Domain: Host:HR-PC
      Signature: 00000000000000000000000000000000
      [Response in: 318]
  > Write Request (0x09)
> Data (65536 bytes)
```

```
0000  00 0c 29 59 23 50 00 0c  29 06 cc 75 08 00 45 00
0010  05 dc 04 57 40 00 80 06  db be 0a 00 00 82 0a 00
0020  00 85 c2 20 01 bd dd f2  91 e0 d8 89 6b 0a 50 10
0030  20 10 d9 f4 00 00 b9 4b  a6 3f 00 00 00 40 83 14
0040  a7 3f 00 00 00 c0 98 dc  a7 3f 00 00 00 d0 fa a3
0050  a8 3f 00 00 00 c0 aa 6a  a9 3f 00 00 00 d0 a9 30
0060  aa 3f 00 00 00 20 f9 f5  aa 3f 00 00 00 00 9a ba
0070  ab 3f 00 00 00 90 8d 7e  ac 3f 00 00 00 10 d5 41
0080  ad 3f 00 00 00 a0 71 04  ae 3f 00 00 00 70 64 c6
0090  ae 3f 00 00 00 b0 ae 87  af 3f 00 00 00 c0 28 24
00a0  b0 3f 00 00 00 f0 26 84  b0 3f 00 00 00 90 d2 e3
00b0  b0 3f 00 00 00 30 2c 43  b1 3f 00 00 00 40 34 a2
00c0  b1 3f 00 00 00 60 eb 00  b2 3f 00 00 00 10 52 5f
00d0  b2 3f 00 00 00 e0 68 bd  b2 3f 00 00 00 50 30 1b
00e0  b3 3f 00 00 00 e0 a8 78  b3 3f 00 00 00 30 d3 d5
00f0  b3 3f 00 00 00 a0 af 32  b4 3f 00 00 00 d0 3e 8f
0100  b4 3f 00 00 00 20 81 eb  b4 3f 00 00 00 30 77 47
0110  b5 3f 00 00 00 60 21 a3  b5 3f 00 00 00 40 80 fe
0120  b5 3f 00 00 00 40 94 59  b6 3f 00 00 00 f0 5d b4
0130  b6 3f 00 00 00 b0 dd 0e  b7 3f 00 00 00 00 14 69
0140  b7 3f 00 00 00 60 01 c3  b7 3f 00 00 00 30 a6 1c
0150  b8 3f 00 00 00 00 03 76  b8 3f 00 00 00 30 18 cf
0160  b8 3f 00 00 00 40 e6 27  b9 3f 00 00 00 90 6d 80
0170  b9 3f 00 00 00 a0 ae d8  b9 3f 00 00 00 d0 a9 30
0180  ba 3f 00 00 00 a0 5f 88  ba 3f 00 00 00 70 d0 df
0190  ba 3f 00 00 00 b0 fc 36  bb 3f 00 00 00 d0 e4 8d
01a0  bb 3f 00 00 00 30 89 e4  bb 3f 00 00 00 40 ea 3a
```

Leandro Delgado
Student ID: 1144162411

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?


psexec-hunt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb2.cmd == 0x09

```
No.  Time          Source      Destination  Protocol Lengtl Info
 192 283.417114851 10.0.0.130  10.0.0.133   SMB2     1514 Write Request Len:65536 Off:0 File: PSEXESVC.exe
 238 283.417522916 10.0.0.130  10.0.0.133   SMB2     1418 Write Request Len:65536 Off:65536 File: PSEXESVC.exe
 240 283.417987816 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 248 283.418123921 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 287 283.418822729 10.0.0.130  10.0.0.133   SMB2     1514 Write Request Len:65536 Off:131072 File: PSEXESVC.exe
 318 283.418910895 10.0.0.133  10.0.0.130   SMB2      138 [TCP ACKed unseen segment] Write Response
 319 283.419144843 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 321 283.419480221 10.0.0.130  10.0.0.133   SMB2      570 Write Request Len:400 Off:241664 File: PSEXESVC.exe
 322 283.419577824 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 366 283.711222806 10.0.0.130  10.0.0.133   SMB2      178 Write Request Len:8 Off:0 File: PSEXEC-HR-PC-1C6C5D14.key
 367 283.711531143 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 368 283.711867282 10.0.0.130  10.0.0.133   SMB2      178 Write Request Len:8 Off:8 File: PSEXEC-HR-PC-1C6C5D14.key
 369 283.712057008 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 391 283.779934912 10.0.0.130  10.0.0.133   SMB2      174 Write Request Len:4 Off:0 File: PSEXESVC
 392 283.780109539 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 438 283.780722918 10.0.0.130  10.0.0.133   SMB2     1465 Write Request Len:65535 Off:0 File: PSEXESVC
 440 283.780866467 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 485 283.781413381 10.0.0.130  10.0.0.133   SMB2     1465 Write Request Len:65535 Off:0 File: PSEXESVC
 488 283.781792952 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 490 283.781973340 10.0.0.130  10.0.0.133   SMB2      824 Write Request Len:2114 Off:0 File: PSEXESVC
 492 283.782075732 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 566 287.200732299 10.0.0.130  10.0.0.133   SMB2      174 Write Request Len:4 Off:0 File: PSEXESVC-HR-PC-7980-stdin
 567 287.201043116 10.0.0.133  10.0.0.130   SMB2      138 Write Response
 568 287.201158573 10.0.0.130  10.0.0.133   SMB2      186 Write Request Len:16 Off:0 File: PSEXESVC-HR-PC-7980-stdin
 569 287.201397635 10.0.0.133  10.0.0.130   SMB2      138 Write Response
```

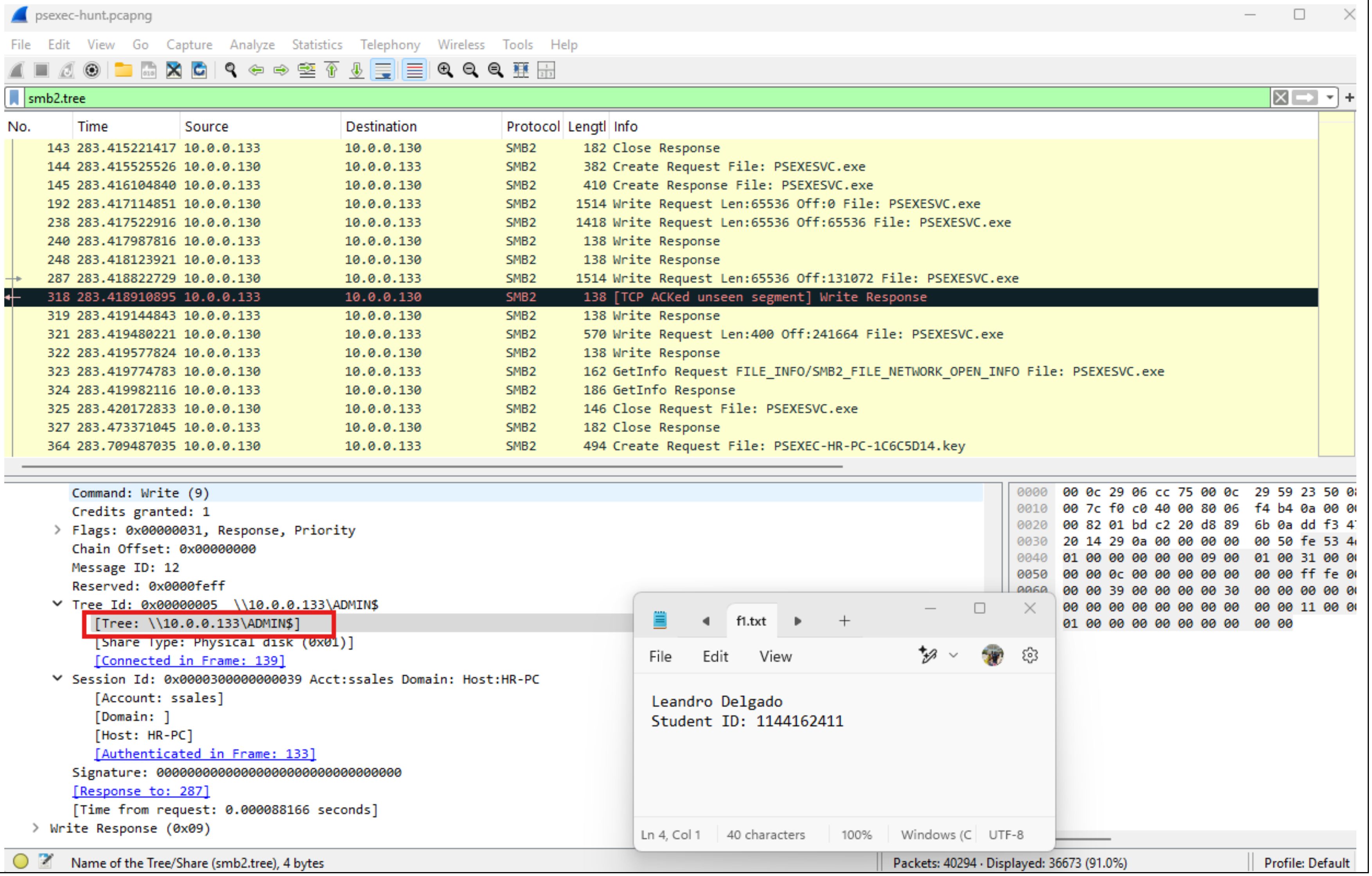
```
  SMB2 Header
    ProtocolId: 0xfe534d42
    Header Length: 64
    Credit Charge: 1
    Channel Sequence: 0
    Reserved: 0000
    Command: Write (9)
    Credits requested: 1
  > Flags: 0x00000030, Priority
    Chain Offset: 0x00000000
    Message ID: 12
    Reserved: 0x0000feff
  Tree Id: 0x00000005  \\10.0.0.133\ADMIN$
      [Tree: \\10.0.0.133\ADMIN$]
      [Share Type: Physical disk (0x01)]
      [Connected in Frame: 139]
  Session Id: 0x0000300000000039 Acct:ssales Domain: Host:HR-PC
      [Account: ssales]
      [Domain: ]
      [Host: HR-PC]
      [Authenticated in Frame: 133]
    Signature: 00000000000000000000000000000000
    [Response in: 318]
> Write Request (0x09)
> Data (65536 bytes)
```

```
0000  00 0c 29 59 23 50 00 0c  29 06 cc 75 08 00 45 00   ··)Y#P·· )
0010  05 dc 04 57 40 00 80 06  db be 0a 00 00 82 0a 00   ···W@···
0020  00 85 c2 20 01 bd dd f2  91 e0 d8 89 6b 0a 50 10   ···  ····
0030  20 10 d9 f4 00 00 b9 4b  a6 3f 00 00 00 40 83 14    ······K
0040  a7 3f 00 00 00 c0 98 dc  a7 3f 00 00 00 d0 fa a3   ·?······
0050  a8 3f 00 00 00 c0 aa 6a  a9 3f 00 00 00 d0 a9 30   ·?·····j
0060  aa 3f 00 00 00 20 f9 f5  aa 3f 00 00 00 00 9a ba   ·?··· ··
0070  ab 3f 00 00 00 90 8d 7e  ac 3f 00 00 00 10 d5 41   ·?·····~
0080  ad 3f 00 00 00 a0 71 04  ae 3f 00 00 00 70 64 c6   ·?····q·
0090  ae 3f 00 00 00 b0 ae 87  af 3f 00 00 00 c0 28 24   ·?······
00a0  b0 3f 00 00 00 f0 26 84  b0 3f 00 00 00 90 d2 e3   ·?····&·
00b0  b0 3f 00 00 00 30 2c 43  b1 3f 00 00 00 40 34 a2   ·?···0,C
00c0  b1 3f 00 00 00 60 eb 00  b2 3f 00 00 00 10 52 5f   ·?···`··
00d0  b2 3f 00 00 00 e0 68 bd  b2 3f 00 00 00 50 30 1b   ·?····h·
00e0  b3 3f 00 00 00 e0 a8 78  b3 3f 00 00 00 30 d3 d5   ·?·····x
00f0  b3 3f 00 00 00 a0 af 32  b4 3f 00 00 00 d0 3e 8f   ·?·····2
0100  b4 3f 00 00 00 20 81 eb  b4 3f 00 00 00 30 77 47   ·?··· ··
0110  b5 3f 00 00 00 60 21 a3  b5 3f 00 00 00 40 80 fe   ·?···`!·
0120  b5 3f 00 00 00 40 94 59  b6 3f 00 00 00 f0 5d b4   ·?···@·Y
0130  b6 3f 00 00 00 b0 dd 0e  b7 3f 00 00 00 00 14 69   ·?······
0140  b7 3f 00 00 00 60 01 c3  b7 3f 00 00 00 30 a6 1c   ·?···`··
0150  b8 3f 00 00 00 00 03 76  b8 3f 00 00 00 30 18 cf   ·?·····v
0160  b8 3f 00 00 00 40 e6 27  b9 3f 00 00 00 90 6d 80   ·?···@·'
0170  b9 3f 00 00 00 a0 ae d8  b9 3f 00 00 00 d0 a9 30   ·?······
0180  ba 3f 00 00 00 a0 5f 88  ba 3f 00 00 00 70 d0 df   ·?····_·
0190  ba 3f 00 00 00 b0 fc 36  bb 3f 00 00 00 d0 e4 8d   ·?·····6
01a0  bb 3f 00 00 00 30 89 e4  bb 3f 00 00 00 40 ea 3a   ·?···0··
```

Frame (1514 bytes) Reassembled TCP (65652 bytes)

Leandro Delgado
Student ID: 1144162411

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


psexec-hunt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb2.tree

```
No.   Time           Source      Destination  Protocol Lengtl Info
  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
  145 283.416104840 10.0.0.133  10.0.0.130   SMB2      410 Create Response File: PSEXESVC.exe
  192 283.417114851 10.0.0.130  10.0.0.133   SMB2     1514 Write Request Len:65536 Off:0 File: PSEXESVC.exe
  238 283.417522916 10.0.0.130  10.0.0.133   SMB2     1418 Write Request Len:65536 Off:65536 File: PSEXESVC.exe
  240 283.417987816 10.0.0.133  10.0.0.130   SMB2      138 Write Response
  248 283.418123921 10.0.0.133  10.0.0.130   SMB2      138 Write Response
  287 283.418822729 10.0.0.130  10.0.0.133   SMB2     1514 Write Request Len:65536 Off:131072 File: PSEXESVC.exe
  318 283.418910895 10.0.0.133  10.0.0.130   SMB2      138 [TCP ACKed unseen segment] Write Response
  319 283.419144843 10.0.0.133  10.0.0.130   SMB2      138 Write Response
  321 283.419480221 10.0.0.130  10.0.0.133   SMB2      570 Write Request Len:400 Off:241664 File: PSEXESVC.exe
  322 283.419577824 10.0.0.133  10.0.0.130   SMB2      138 Write Response
  323 283.419774783 10.0.0.130  10.0.0.133   SMB2      162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: PSEXESVC.exe
  324 283.419982116 10.0.0.133  10.0.0.130   SMB2      186 GetInfo Response
  325 283.420172833 10.0.0.130  10.0.0.133   SMB2      146 Close Request File: PSEXESVC.exe
  327 283.473371045 10.0.0.133  10.0.0.130   SMB2      182 Close Response
  364 283.709487035 10.0.0.130  10.0.0.133   SMB2      494 Create Request File: PSEXEC-HR-PC-1C6C5D14.key
```

```
    Command: Write (9)
    Credits granted: 1
  > Flags: 0x00000031, Response, Priority
    Chain Offset: 0x00000000
    Message ID: 12
    Reserved: 0x0000feff
  ˅ Tree Id: 0x00000005  \\10.0.0.133\ADMIN$
      [Tree: \\10.0.0.133\ADMIN$]
      [Share Type: Physical disk (0x01)]
      [Connected in Frame: 139]
  ˅ Session Id: 0x0000300000000039 Acct:ssales Domain: Host:HR-PC
      [Account: ssales]
      [Domain: ]
      [Host: HR-PC]
      [Authenticated in Frame: 133]
    Signature: 00000000000000000000000000000000
    [Response to: 287]
    [Time from request: 0.000088166 seconds]
> Write Response (0x09)
```

```
0000  00 0c 29 06 cc 75 00 0c  29 59 23 50 0
0010  00 7c f0 c0 40 00 80 06  f4 b4 0a 00 0
0020  00 82 01 bd c2 20 d8 89  6b 0a dd f3 4
0030  20 14 29 0a 00 00 00 00  00 50 fe 53 4
0040  01 00 00 00 00 00 09 00  01 00 31 00 0
0050  00 00 0c 00 00 00 00 00  00 00 ff fe 0
0060  00 00 39 00 00 00 00 30  00 00 00 00 0
      00 00 00 00 00 00 00 00  00 00 11 00 0
      01 00 00 00 00 00 00 00  00 00
```

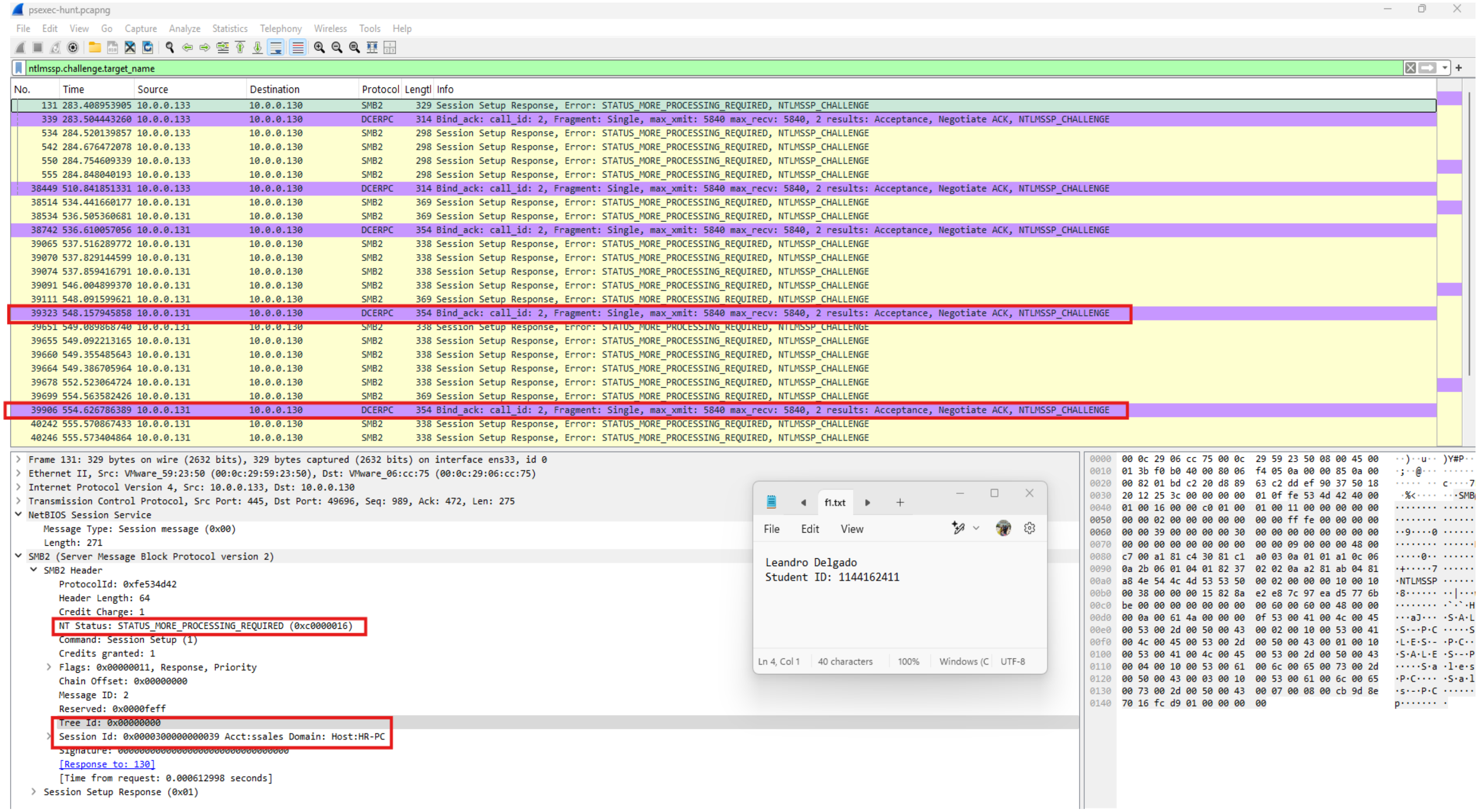
Leandro Delgado
Student ID: 1144162411

Name of the Tree/Share (smb2.tree), 4 bytes

Packets: 40294 · Displayed: 36673 (91.0%)

Profile: Default

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 machine's hostname to which the attacker attempted to pivot within our network?


psexec-hunt.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ntlmssp.challenge.target_name

```
No.   Time          Source      Destination  Protocol Lengtl Info
  131 283.408953905 10.0.0.133  10.0.0.130   SMB2     329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
  339 283.504443260 10.0.0.133  10.0.0.130   DCERPC   314 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Negotiate ACK, NTLMSSP_CHALLENGE
  534 284.520139857 10.0.0.133  10.0.0.130   SMB2     298 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
  542 284.676472078 10.0.0.133  10.0.0.130   SMB2     298 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
  550 284.754609339 10.0.0.133  10.0.0.130   SMB2     298 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
  555 284.848040193 10.0.0.133  10.0.0.130   SMB2     298 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
38449 510.841851331 10.0.0.133  10.0.0.130   DCERPC   314 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Negotiate ACK, NTLMSSP_CHALLENGE
38514 534.441660177 10.0.0.131  10.0.0.130   SMB2     369 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
38534 536.505360681 10.0.0.131  10.0.0.130   SMB2     369 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
38742 536.610057056 10.0.0.131  10.0.0.130   DCERPC   354 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Negotiate ACK, NTLMSSP_CHALLENGE
39065 537.516289772 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39070 537.829144599 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39074 537.859416791 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39091 546.004899370 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39111 548.091599621 10.0.0.131  10.0.0.130   SMB2     369 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39323 548.157945858 10.0.0.131  10.0.0.130   DCERPC   354 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Negotiate ACK, NTLMSSP_CHALLENGE
39651 549.089868740 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39655 549.092213165 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39660 549.355485643 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39664 549.386705964 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39678 552.523064724 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39699 554.563582426 10.0.0.131  10.0.0.130   SMB2     369 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
39906 554.626786389 10.0.0.131  10.0.0.130   DCERPC   354 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Negotiate ACK, NTLMSSP_CHALLENGE
40242 555.570867433 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
40246 555.573404864 10.0.0.131  10.0.0.130   SMB2     338 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
```

```
> Frame 131: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_59:23:50 (00:0c:29:59:23:50), Dst: VMware_06:cc:75 (00:0c:29:06:cc:75)
> Internet Protocol Version 4, Src: 10.0.0.133, Dst: 10.0.0.130
> Transmission Control Protocol, Src Port: 445, Dst Port: 49696, Seq: 989, Ack: 472, Len: 275
v NetBIOS Session Service
    Message Type: Session message (0x00)
    Length: 271
v SMB2 (Server Message Block Protocol version 2)
  v SMB2 Header
      ProtocolId: 0xfe534d42
      Header Length: 64
      Credit Charge: 1
      NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
      Command: Session Setup (1)
      Credits granted: 1
    > Flags: 0x00000011, Response, Priority
      Chain Offset: 0x00000000
      Message ID: 2
      Reserved: 0x0000feff
      Tree Id: 0x00000000
    > Session Id: 0x0000300000000039 Acct:ssales Domain: Host:HR-PC
      Signature: 00000000000000000000000000000000
      [Response to: 130]
      [Time from request: 0.000612998 seconds]
  > Session Setup Response (0x01)
```

```
0000  00 0c 29 06 cc 75 00 0c  29 59 23 50 08 00 45 00   ··)··u·· )Y#P··
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····7
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   ········ ······
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······ ··|···
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
00e0  00 53 00 2d 00 50 00 43  00 02 00 10 00 53 00 41   ·S·-·P·C ·····S
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
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
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······· ·
```

Leandro Delgado
Student ID: 1144162411

The packets challenge NTLMSSP in the capture to confirm that the attacker, after hacking 10.0.0.133, attempted to pivot to 10.0.0.131. These are authentication challenge responses that show that 10.0.0.133 initiated an authentication request to the internal 10.0.0.131 address, which indicates full movement inside the network. This is quite a powerful indicator that the attacker has broadened his access using PsExec or an equivalent method to initiate commands on other computers.

	Summary "The PsExec Hunt Lab highlights the risks of SMB abuse, NTLM authentication misuse, and lateral movement techniques. Security teams can detect unauthorized access early by monitoring SMB2 traffic, NTLMSSP authentication requests, and network shares like ADMIN$. Threat mitigation involves identifying the creation of PSEXESVC.exe and tracking system pivot attempts. Implementing least privilege access, endpoint monitoring, and proactive logging is essential to prevent such attacks.
Students Work required for this activity	• Go to the challenge https://cyberdefenders.org/blueteam-ctf-challenges/143#nav-questions • Create an account and Login. • Download the Challenge (Attached also hereby). Uncompress the challenge (pass: cyberdefenders.org) • Answer the 7 challenge questions. Tool Used: Wireshark. • Show complete screenshots of all your work.
Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.