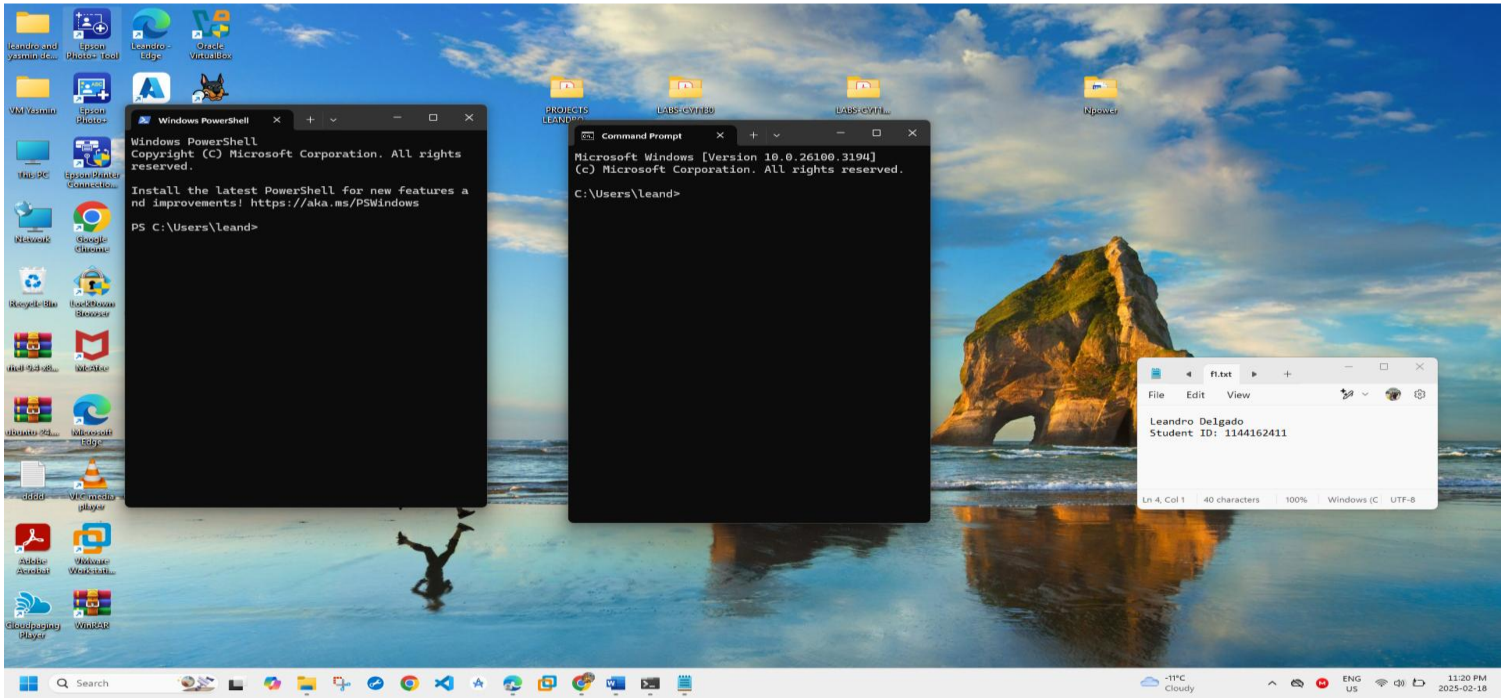
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Leandro Delgado	114416241	As Posted	6%

Name	Lab5: PoisonedCredentials Network Forensics Challenge
Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above. • Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY. • Show your genuine signs of your work is done on your machine. This includes: ○ Screenshots that show your desktop background with Date/Time. ○ Show a pop-up bx that shows "your name + IP". ○ Show your logged account when applicable. Optional: Your photo. • Submit your report name: CYT215-Lab5-Student Name & ID
Challenge Scenario	Your organization's security team has detected a surge in suspicious network activity. There are concerns that LLMNR (Link-Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) poisoning attacks may be occurring within your network. These attacks are known for exploiting these protocols to intercept network traffic and potentially compromise user credentials. Your task is to investigate the network logs and examine captured network traffic.
	

```
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>
```

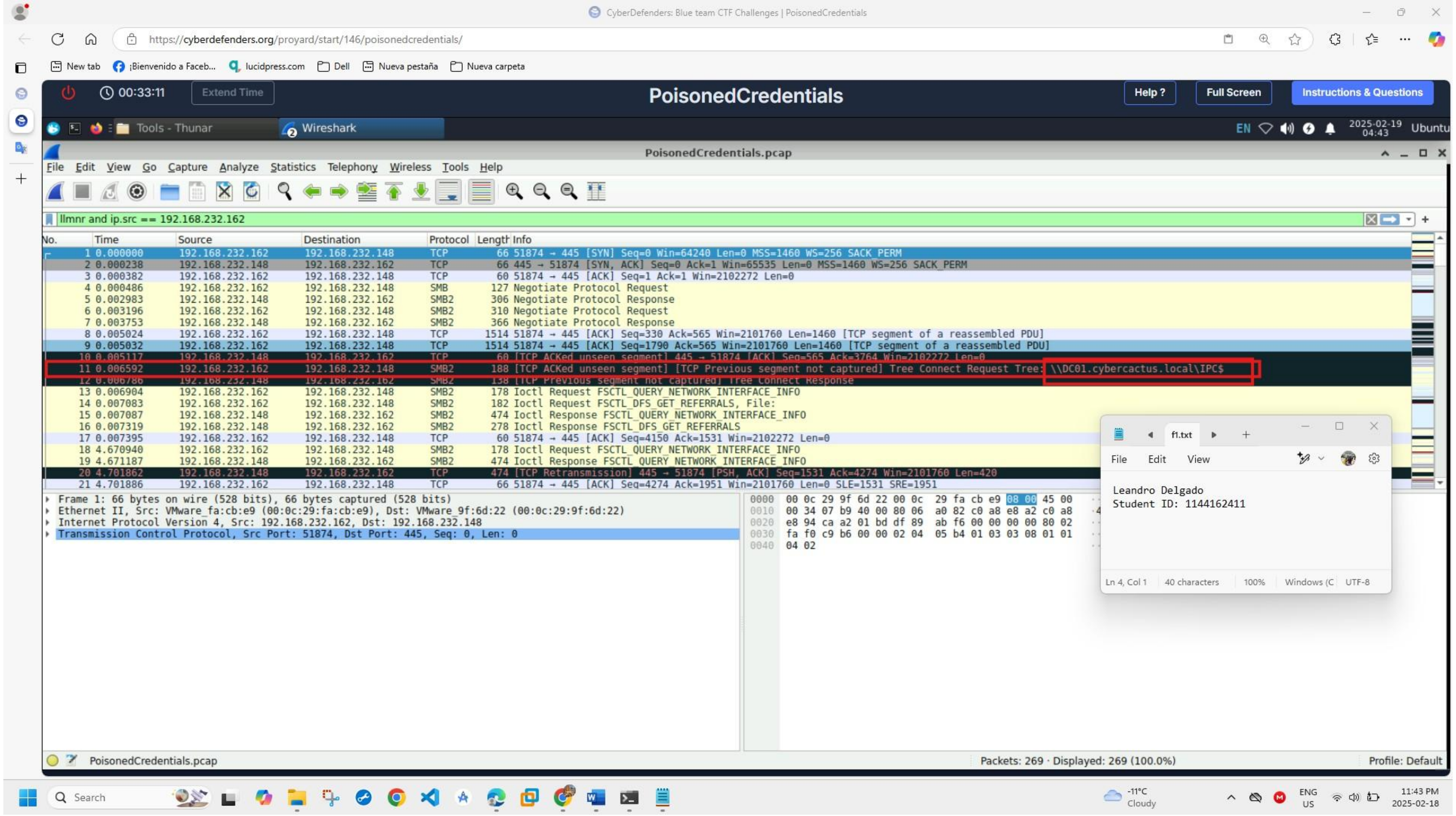
```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\leand>
```

```
Leandro Delgado
Student ID: 1144162411
```

Challenge Questions To be Answered

1. In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify the specific mistyped query made by the machine with the IP address 192.168.232.162?



```
llmnr and ip.src == 192.168.232.162
```

```
No.  Time      Source           Destination      Protocol Length Info
   1 0.000000  192.168.232.162  192.168.232.148  TCP        66 51874 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   2 0.000238  192.168.232.148  192.168.232.162  TCP        66 445 → 51874 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   3 0.000382  192.168.232.162  192.168.232.148  TCP        60 51874 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
   4 0.000486  192.168.232.162  192.168.232.148  SMB       127 Negotiate Protocol Request
   5 0.002983  192.168.232.148  192.168.232.162  SMB2      306 Negotiate Protocol Response
   6 0.003196  192.168.232.162  192.168.232.148  SMB2      310 Negotiate Protocol Request
   7 0.003753  192.168.232.148  192.168.232.162  SMB2      366 Negotiate Protocol Response
   8 0.005024  192.168.232.162  192.168.232.148  TCP      1514 51874 → 445 [ACK] Seq=330 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
   9 0.005032  192.168.232.162  192.168.232.148  TCP      1514 51874 → 445 [ACK] Seq=1790 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
  10 0.005117  192.168.232.148  192.168.232.162  TCP        60 [TCP ACKed unseen segment] 445 → 51874 [ACK] Seq=565 Ack=3764 Win=2102272 Len=0
  11 0.006592  192.168.232.162  192.168.232.148  SMB2      188 [TCP ACKed unseen segment] [TCP Previous segment not captured] Tree Connect Request Tree: \\DC01.cybercactus.local\IPC$
  12 0.006786  192.168.232.148  192.168.232.162  SMB2      138 [TCP Previous segment not captured] Tree Connect Response
  13 0.006904  192.168.232.162  192.168.232.148  SMB2      178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
  14 0.007083  192.168.232.162  192.168.232.148  SMB2      182 Ioctl Request FSCTL_DFS_GET_REFERRALS, File:
  15 0.007087  192.168.232.148  192.168.232.162  SMB2      474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
  16 0.007319  192.168.232.148  192.168.232.162  SMB2      278 Ioctl Response FSCTL_DFS_GET_REFERRALS
  17 0.007395  192.168.232.162  192.168.232.148  TCP        60 51874 → 445 [ACK] Seq=4150 Ack=1531 Win=2102272 Len=0
  18 4.670940  192.168.232.162  192.168.232.148  SMB2      178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
  19 4.671187  192.168.232.148  192.168.232.162  SMB2      474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
  20 4.701862  192.168.232.148  192.168.232.162  TCP       474 [TCP Retransmission] 445 → 51874 [PSH, ACK] Seq=1531 Ack=4274 Win=2101760 Len=420
  21 4.701886  192.168.232.162  192.168.232.148  TCP        66 51874 → 445 [ACK] Seq=4274 Ack=1951 Win=2101760 Len=0 SLE=1531 SRE=1951
```

```
▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: VMware_fa:cb:e9 (00:0c:29:fa:cb:e9), Dst: VMware_9f:6d:22 (00:0c:29:9f:6d:22)
▸ Internet Protocol Version 4, Src: 192.168.232.162, Dst: 192.168.232.148
▸ Transmission Control Protocol, Src Port: 51874, Dst Port: 445, Seq: 0, Len: 0
```

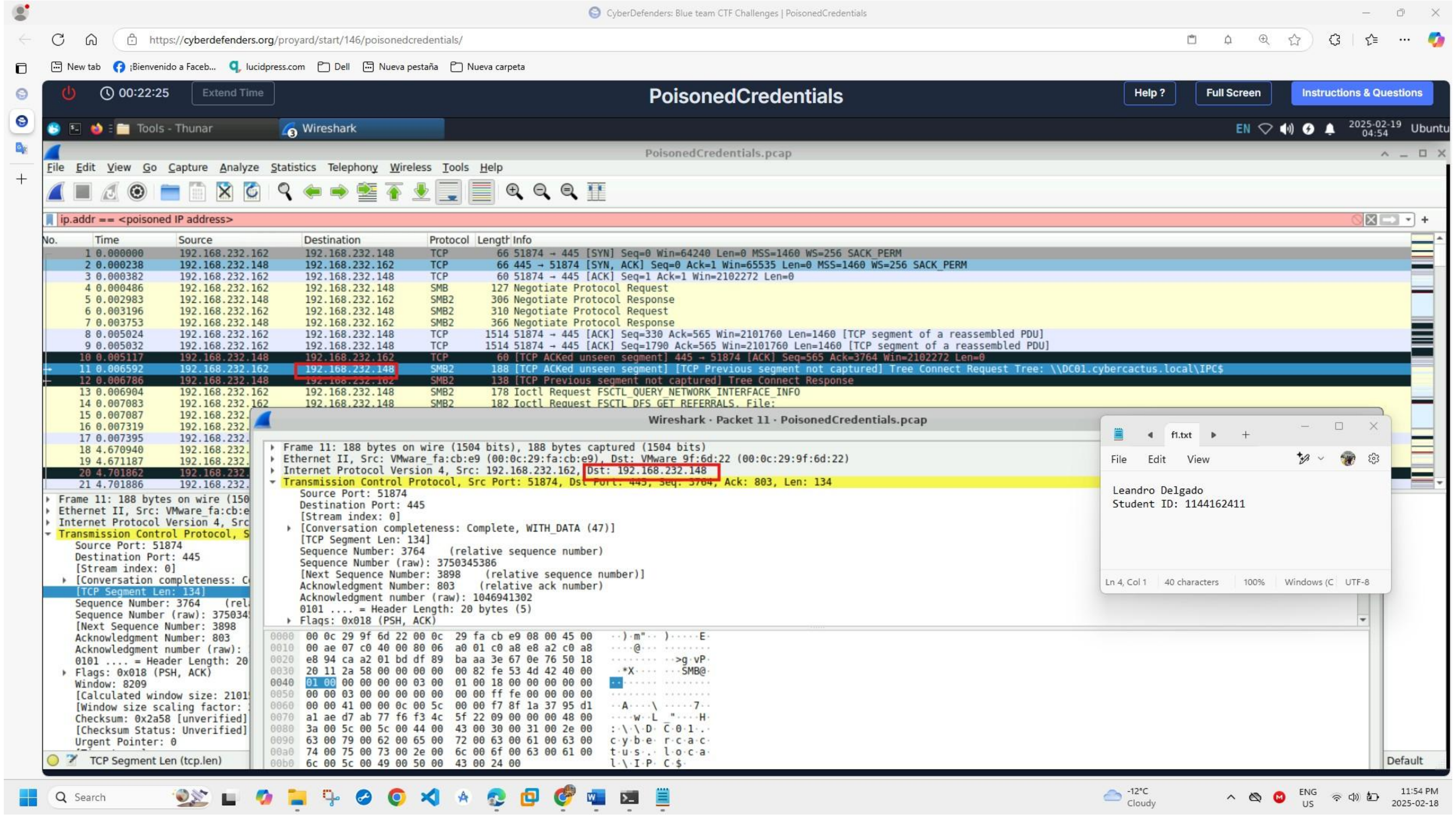
```
0000  00 0c 29 9f 6d 22 00 0c  29 fa cb e9 08 00 45 00
0010  00 34 07 b9 40 00 80 06  a0 82 c0 a8 e8 a2 c0 a8
0020  e8 94 ca a2 01 bd df 89  ab f6 00 00 00 00 80 02
0030  fa f0 c9 b6 00 00 02 04  05 b4 01 03 03 08 01 01
0040  04 02
```

```
Leandro Delgado
Student ID: 1144162411
```

Ln 4, Col 1 | 40 characters | 100% | Windows (C | UTF-8

PoisonedCredentials.pcap | Packets: 269 · Displayed: 269 (100.0%) | Profile: Default

2. We are investigating a network security incident. For a thorough investigation, we need to determine the IP address of the rogue machine. What is the IP address of the machine acting as the rogue entity?



```
ip.addr == <poisoned IP address>
```

```
No.  Time      Source           Destination      Protocol Length Info
   1 0.000000  192.168.232.162  192.168.232.148  TCP      66 51874 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   2 0.000238  192.168.232.148  192.168.232.162  TCP      66 445 → 51874 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   3 0.000382  192.168.232.162  192.168.232.148  TCP      60 51874 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
   4 0.000486  192.168.232.162  192.168.232.148  SMB     127 Negotiate Protocol Request
   5 0.002983  192.168.232.148  192.168.232.162  SMB2    306 Negotiate Protocol Response
   6 0.003196  192.168.232.162  192.168.232.148  SMB2    310 Negotiate Protocol Request
   7 0.003753  192.168.232.148  192.168.232.162  SMB2    366 Negotiate Protocol Response
   8 0.005024  192.168.232.162  192.168.232.148  TCP    1514 51874 → 445 [ACK] Seq=330 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
   9 0.005032  192.168.232.162  192.168.232.148  TCP    1514 51874 → 445 [ACK] Seq=1790 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
  10 0.005117  192.168.232.148  192.168.232.162  TCP      60 [TCP ACKed unseen segment] 445 → 51874 [ACK] Seq=565 Ack=3764 Win=2102272 Len=0
  11 0.006592  192.168.232.162  192.168.232.148  SMB2    188 [TCP ACKed unseen segment] [TCP Previous segment not captured] Tree Connect Request Tree: \\DC01.cybercactus.local\IPC$
  12 0.006786  192.168.232.148  192.168.232.162  SMB2    138 [TCP Previous segment not captured] Tree Connect Response
  13 0.006904  192.168.232.162  192.168.232.148  SMB2    178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
  14 0.007083  192.168.232.162  192.168.232.148  SMB2    182 Ioctl Request FSCTL_DFS_GET_REFERRALS, File:
  15 0.007087  192.168.232.
  16 0.007319  192.168.232.
  17 0.007395  192.168.232.
  18 4.670940  192.168.232.
  19 4.671187  192.168.232.
  20 4.701862  192.168.232.
  21 4.701886  192.168.232.
```

```
▸ Frame 11: 188 bytes on wire (150
▸ Ethernet II, Src: VMware_fa:cb:e
▸ Internet Protocol Version 4, Src
▾ Transmission Control Protocol, S
    Source Port: 51874
    Destination Port: 445
    [Stream index: 0]
  ▸ [Conversation completeness: C
    [TCP Segment Len: 134]
    Sequence Number: 3764    (rel
    Sequence Number (raw): 375034
    [Next Sequence Number: 3898
    Acknowledgment Number: 803
    Acknowledgment number (raw):
    0101 .... = Header Length: 20
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 8209
    [Calculated window size: 2101
    [Window size scaling factor:
    Checksum: 0x2a58 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

TCP Segment Len (tcp.len)

Wireshark · Packet 11 · PoisonedCredentials.pcap

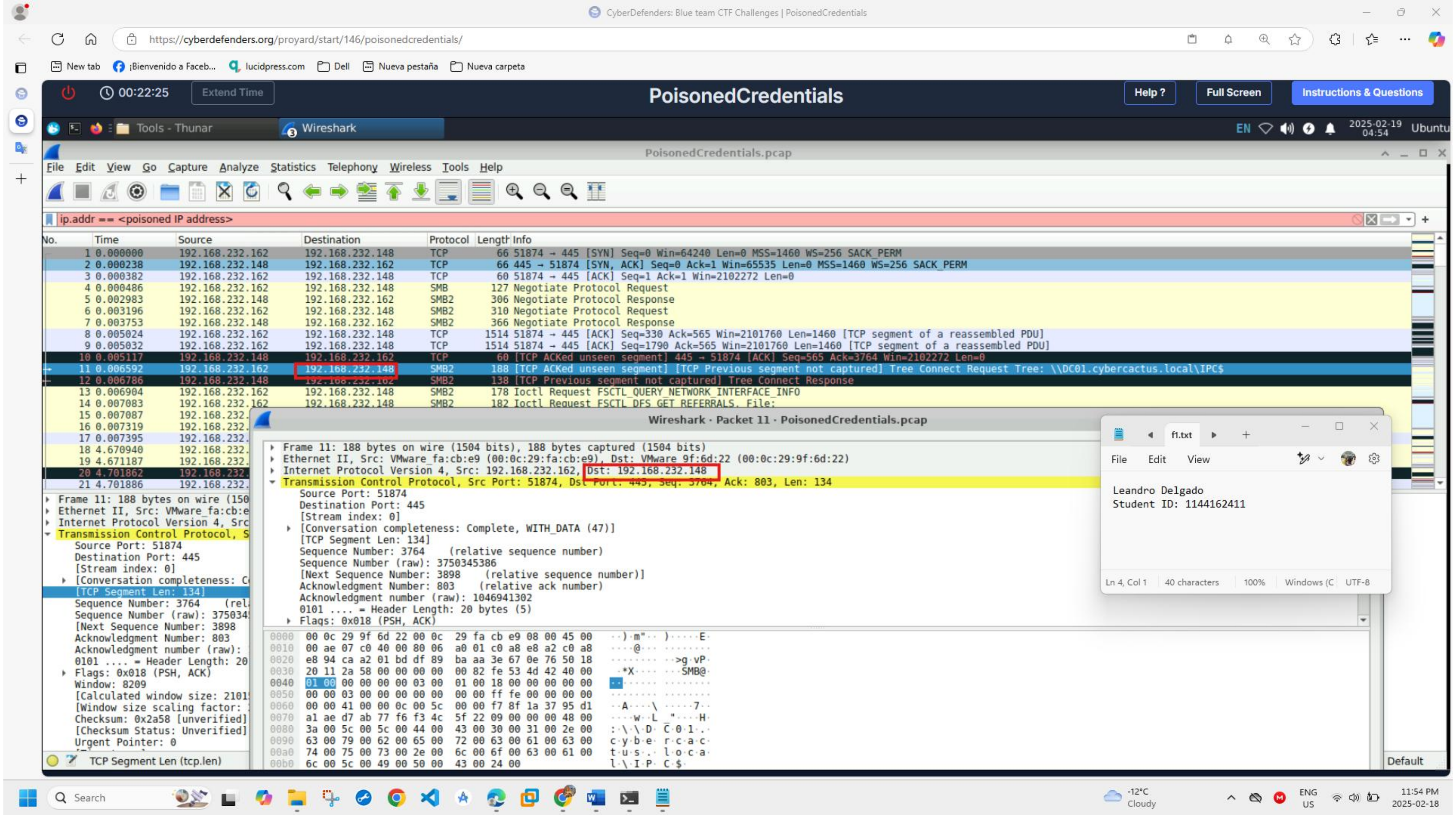
```
▸ Frame 11: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
▸ Ethernet II, Src: VMware_fa:cb:e9 (00:0c:29:fa:cb:e9), Dst: VMware_9f:6d:22 (00:0c:29:9f:6d:22)
▸ Internet Protocol Version 4, Src: 192.168.232.162, Dst: 192.168.232.148
▾ Transmission Control Protocol, Src Port: 51874, Dst Port: 445, Seq: 3764, Ack: 803, Len: 134
    Source Port: 51874
    Destination Port: 445
    [Stream index: 0]
  ▸ [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 134]
    Sequence Number: 3764    (relative sequence number)
    Sequence Number (raw): 3750345386
    [Next Sequence Number: 3898    (relative sequence number)]
    Acknowledgment Number: 803    (relative ack number)
    Acknowledgment number (raw): 1046941302
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
```

```
0000  00 0c 29 9f 6d 22 00 0c  29 fa cb e9 08 00 45 00   ··)·m"·· )·····E·
0010  00 ae 07 c0 40 00 80 06  a0 01 c0 a8 e8 a2 c0 a8   ····@··· ········
0020  e8 94 ca a2 01 bd df 89  ba aa 3e 67 0e 76 50 18   ········ ··>g·vP·
0030  20 11 2a 58 00 00 00 00  00 82 fe 53 4d 42 40 00    ·*X···· ···SMB@·
0040  01 00 00 00 00 00 03 00  01 00 18 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 41 00 00 0c 00 5c  00 00 f7 8f 1a 37 95 d1   ··A····\ ·····7··
0070  a1 ae d7 ab 77 f6 f3 4c  5f 22 09 00 00 00 48 00   ····w··L _"····H·
0080  3a 00 5c 00 5c 00 44 00  43 00 30 00 31 00 2e 00   :·\·\·D· C·0·1·.·
0090  63 00 79 00 62 00 65 00  72 00 63 00 61 00 63 00   c·y·b·e· r·c·a·c·
00a0  74 00 75 00 73 00 2e 00  6c 00 6f 00 63 00 61 00   t·u·s·.· l·o·c·a·
00b0  6c 00 5c 00 49 00 50 00  43 00 24 00               l·\·I·P· C·$·
```

f1.txt

```
Leandro Delgado
Student ID: 1144162411
```

3. During our investigation, it's crucial to identify all affected machines. What is the IP address of the second machine that received poisoned responses from the rogue machine?



ip.addr == <poisoned IP address>

```
No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.232.162  192.168.232.148  TCP        66 51874 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    2 0.000238   192.168.232.148  192.168.232.162  TCP        66 445 → 51874 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
    3 0.000382   192.168.232.162  192.168.232.148  TCP        60 51874 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
    4 0.000486   192.168.232.162  192.168.232.148  SMB       127 Negotiate Protocol Request
    5 0.002983   192.168.232.148  192.168.232.162  SMB2      306 Negotiate Protocol Response
    6 0.003196   192.168.232.162  192.168.232.148  SMB2      310 Negotiate Protocol Request
    7 0.003753   192.168.232.148  192.168.232.162  SMB2      366 Negotiate Protocol Response
    8 0.005024   192.168.232.162  192.168.232.148  TCP      1514 51874 → 445 [ACK] Seq=330 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
    9 0.005032   192.168.232.162  192.168.232.148  TCP      1514 51874 → 445 [ACK] Seq=1790 Ack=565 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
   10 0.005117   192.168.232.148  192.168.232.162  TCP        60 [TCP ACKed unseen segment] 445 → 51874 [ACK] Seq=565 Ack=3764 Win=2102272 Len=0
   11 0.006592   192.168.232.162  192.168.232.148  SMB2      188 [TCP ACKed unseen segment] [TCP Previous segment not captured] Tree Connect Request Tree: \\DC01.cybercactus.local\IPC$
   12 0.006786   192.168.232.148  192.168.232.162  SMB2      138 [TCP Previous segment not captured] Tree Connect Response
   13 0.006904   192.168.232.162  192.168.232.148  SMB2      178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
   14 0.007083   192.168.232.162  192.168.232.148  SMB2      182 Ioctl Request FSCTL_DFS_GET_REFERRALS, File:
   15 0.007087   192.168.232.
   16 0.007319   192.168.232.
   17 0.007395   192.168.232.
   18 4.670940   192.168.232.
   19 4.671187   192.168.232.
   20 4.701862   192.168.232.
   21 4.701886   192.168.232.
```

```
▸ Frame 11: 188 bytes on wire (150
▸ Ethernet II, Src: VMware_fa:cb:e
▸ Internet Protocol Version 4, Src
▾ Transmission Control Protocol, S
    Source Port: 51874
    Destination Port: 445
    [Stream index: 0]
  ▸ [Conversation completeness: C
    [TCP Segment Len: 134]
    Sequence Number: 3764    (rel
    Sequence Number (raw): 375034
    [Next Sequence Number: 3898
    Acknowledgment Number: 803
    Acknowledgment number (raw):
    0101 .... = Header Length: 20
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 8209
    [Calculated window size: 2101
    [Window size scaling factor:
    Checksum: 0x2a58 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

TCP Segment Len (tcp.len)

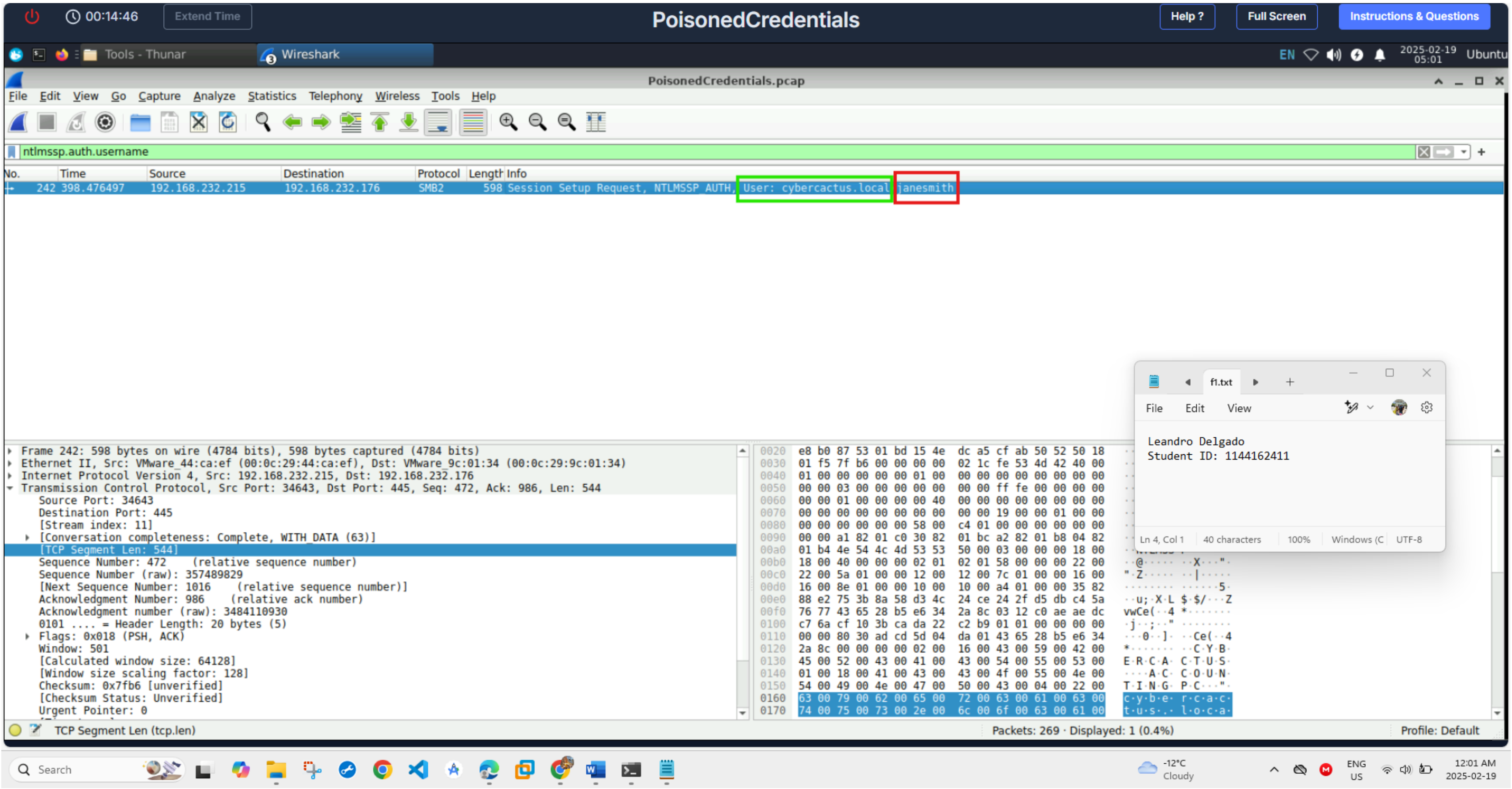
Wireshark · Packet 11 · PoisonedCredentials.pcap

```
▸ Frame 11: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
▸ Ethernet II, Src: VMware_fa:cb:e9 (00:0c:29:fa:cb:e9), Dst: VMware_9f:6d:22 (00:0c:29:9f:6d:22)
▸ Internet Protocol Version 4, Src: 192.168.232.162, Dst: 192.168.232.148
▾ Transmission Control Protocol, Src Port: 51874, Dst Port: 445, Seq: 3764, Ack: 803, Len: 134
    Source Port: 51874
    Destination Port: 445
    [Stream index: 0]
  ▸ [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 134]
    Sequence Number: 3764    (relative sequence number)
    Sequence Number (raw): 3750345386
    [Next Sequence Number: 3898    (relative sequence number)]
    Acknowledgment Number: 803    (relative ack number)
    Acknowledgment number (raw): 1046941302
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
```

```
0000  00 0c 29 9f 6d 22 00 0c  29 fa cb e9 08 00 45 00   ··)·m"·· )·····E·
0010  00 ae 07 c0 40 00 80 06  a0 01 c0 a8 e8 a2 c0 a8   ····@··· ········
0020  e8 94 ca a2 01 bd df 89  ba aa 3e 67 0e 76 50 18   ········ ··>g·vP·
0030  20 11 2a 58 00 00 00 00  00 82 fe 53 4d 42 40 00    ·*X···· ···SMB@·
0040  01 00 00 00 00 00 03 00  01 00 18 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 41 00 00 0c 00 5c  00 00 f7 8f 1a 37 95 d1   ··A····\ ·····7··
0070  a1 ae d7 ab 77 f6 f3 4c  5f 22 09 00 00 00 48 00   ····w··L _"····H·
0080  3a 00 5c 00 5c 00 44 00  43 00 30 00 31 00 2e 00   :·\·\·D· C·0·1·.·
0090  63 00 79 00 62 00 65 00  72 00 63 00 61 00 63 00   c·y·b·e· r·c·a·c·
00a0  74 00 75 00 73 00 2e 00  6c 00 6f 00 63 00 61 00   t·u·s·.· l·o·c·a·
00b0  6c 00 5c 00 49 00 50 00  43 00 24 00               l·\·I·P· C·$·
```

Leandro Delgado
Student ID: 1144162411

4. We suspect that user accounts may have been compromised. To assess this, we must determine the username associated with the compromised account. What is the username of the account that the attacker compromised?



ntlmssp.auth.username

No.	Time	Source	Destination	Protocol	Length	Info
242	398.476497	192.168.232.215	192.168.232.176	SMB2	598	Session Setup Request, NTLMSSP_AUTH, User: cybercactus.local\janesmith

```
Frame 242: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits)
Ethernet II, Src: VMware_44:ca:ef (00:0c:29:44:ca:ef), Dst: VMware_9c:01:34 (00:0c:29:9c:01:34)
Internet Protocol Version 4, Src: 192.168.232.215, Dst: 192.168.232.176
Transmission Control Protocol, Src Port: 34643, Dst Port: 445, Seq: 472, Ack: 986, Len: 544
    Source Port: 34643
    Destination Port: 445
    [Stream index: 11]
  [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 544]
    Sequence Number: 472    (relative sequence number)
    Sequence Number (raw): 357489829
    [Next Sequence Number: 1016    (relative sequence number)]
    Acknowledgment Number: 986    (relative ack number)
    Acknowledgment number (raw): 3484110930
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    Window: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0x7fb6 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

```
0020  e8 b0 87 53 01 bd 15 4e  dc a5 cf ab 50 52 50 18
0030  01 f5 7f b6 00 00 00 00  02 1c fe 53 4d 42 40 00
0040  01 00 00 00 00 00 01 00  00 00 00 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 01 00 00 00 00 40  00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 19 00 00 01 00 00
0080  00 00 00 00 00 00 58 00  c4 01 00 00 00 00 00 00
0090  00 00 a1 82 01 c0 30 82  01 bc a2 82 01 b8 04 82
00a0  01 b4 4e 54 4c 4d 53 53  50 00 03 00 00 00 18 00
00b0  18 00 40 00 00 00 02 01  02 01 58 00 00 00 22 00   ··@·····  ··X···"·
00c0  22 00 5a 01 00 00 12 00  12 00 7c 01 00 00 16 00   "·Z·····  ··|·····
00d0  16 00 8e 01 00 00 10 00  10 00 a4 01 00 00 35 82   ········  ······5·
00e0  88 e2 75 3b 8a 58 d3 4c  24 ce 24 2f d5 db c4 5a   ··u;·X·L  $·$/···Z
00f0  76 77 43 65 28 b5 e6 34  2a 8c 03 12 c0 ae ae dc   vwCe(··4  *·······
0100  c7 6a cf 10 3b ca da 22  c2 b9 01 01 00 00 00 00   ·j··;··"  ········
0110  00 00 80 30 ad cd 5d 04  da 01 43 65 28 b5 e6 34   ···0··]·  ··Ce(··4
0120  2a 8c 00 00 00 00 02 00  16 00 43 00 59 00 42 00   *·······  ··C·Y·B·
0130  45 00 52 00 43 00 41 00  43 00 54 00 55 00 53 00   E·R·C·A·  C·T·U·S·
0140  01 00 18 00 41 00 43 00  43 00 4f 00 55 00 4e 00   ····A·C·  C·O·U·N·
0150  54 00 49 00 4e 00 47 00  50 00 43 00 04 00 22 00   T·I·N·G·  P·C···"·
0160  63 00 79 00 62 00 65 00  72 00 63 00 61 00 63 00   c·y·b·e·  r·c·a·c·
0170  74 00 75 00 73 00 2e 00  6c 00 6f 00 63 00 61 00   t·u·s·.·  l·o·c·a·
```

TCP Segment Len (tcp.len)

Packets: 269 · Displayed: 1 (0.4%)

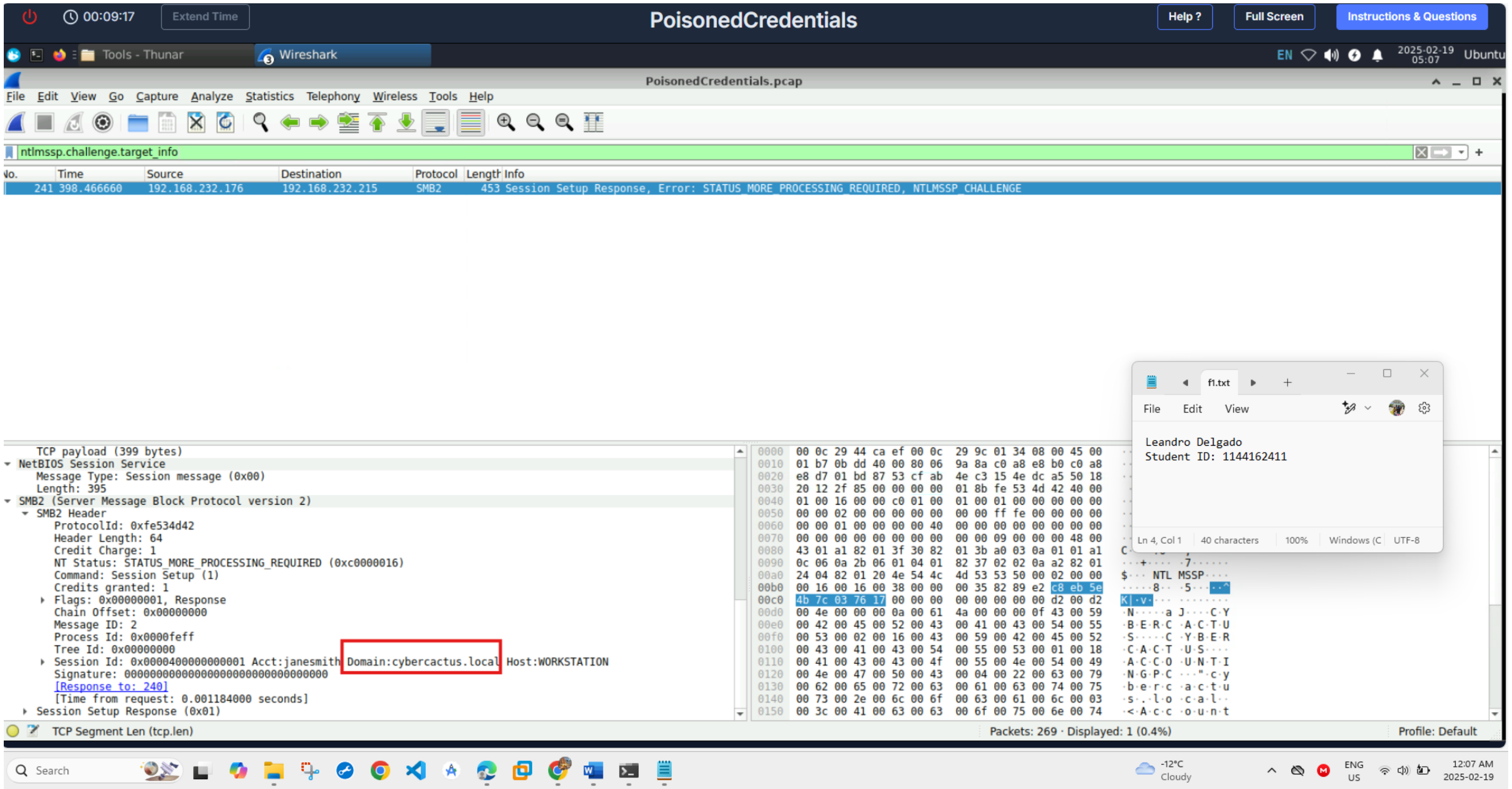
Profile: Default

f1.txt

Leandro Delgado
Student ID: 1144162411

Ln 4, Col 1 | 40 characters | 100% | Windows (C | UTF-8

5. As part of our investigation, we aim to understand the extent of the attacker's activities. What is the hostname of the machine that the attacker accessed via SMB?



ntlmssp.challenge.target_info

```
No.  Time        Source           Destination      Protocol Length Info
  241 398.466660  192.168.232.176  192.168.232.215  SMB2      453 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
```

```
    TCP payload (399 bytes)
▾ NetBIOS Session Service
    Message Type: Session message (0x00)
    Length: 395
▾ SMB2 (Server Message Block Protocol version 2)
  ▾ 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: 0x00000001, Response
      Chain Offset: 0x00000000
      Message ID: 2
      Process Id: 0x0000feff
      Tree Id: 0x00000000
    ▸ Session Id: 0x0000400000000001 Acct:janesmith Domain:cybercactus.local Host:WORKSTATION
      Signature: 00000000000000000000000000000000
      [Response to: 240]
      [Time from request: 0.001184000 seconds]
  ▸ Session Setup Response (0x01)
```

```
0000  00 0c 29 44 ca ef 00 0c  29 9c 01 34 08 00 45 00
0010  01 b7 0b dd 40 00 80 06  9a 8a c0 a8 e8 b0 c0 a8
0020  e8 d7 01 bd 87 53 cf ab  4e c3 15 4e dc a5 50 18
0030  20 12 2f 85 00 00 00 00  01 8b fe 53 4d 42 40 00
0040  01 00 16 00 00 c0 01 00  01 00 01 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 01 00 00 00 00 40  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
0080  43 01 a1 82 01 3f 30 82  01 3b a0 03 0a 01 01 a1   C
0090  0c 06 0a 2b 06 01 04 01  82 37 02 02 0a a2 82 01   ···+···· ·7······
00a0  24 04 82 01 20 4e 54 4c  4d 53 53 50 00 02 00 00   $··· NTL MSSP····
00b0  00 16 00 16 00 38 00 00  00 35 82 89 e2 c8 eb 5e   ·····8·· ·5·····^
00c0  4b 7c 03 76 17 00 00 00  00 00 00 00 00 d2 00 d2   K|·v···· ········
00d0  00 4e 00 00 00 0a 00 61  4a 00 00 00 0f 43 00 59   ·N·····a J····C·Y
00e0  00 42 00 45 00 52 00 43  00 41 00 43 00 54 00 55   ·B·E·R·C ·A·C·T·U
00f0  00 53 00 02 00 16 00 43  00 59 00 42 00 45 00 52   ·S·····C ·Y·B·E·R
0100  00 43 00 41 00 43 00 54  00 55 00 53 00 01 00 18   ·C·A·C·T ·U·S····
0110  00 41 00 43 00 43 00 4f  00 55 00 4e 00 54 00 49   ·A·C·C·O ·U·N·T·I
0120  00 4e 00 47 00 50 00 43  00 04 00 22 00 63 00 79   ·N·G·P·C ···"·c·y
0130  00 62 00 65 00 72 00 63  00 61 00 63 00 74 00 75   ·b·e·r·c ·a·c·t·u
0140  00 73 00 2e 00 6c 00 6f  00 63 00 61 00 6c 00 03   ·s·.·l·o ·c·a·l··
0150  00 3c 00 41 00 63 00 63  00 6f 00 75 00 6e 00 74   ·<·A·c·c ·o·u·n·t
```

Leandro Delgado
Student ID: 1144162411

TCP Segment Len (tcp.len)

Packets: 269 · Displayed: 1 (0.4%)

Profile: Default

Summary:

The workshop gave an excellent opportunity to practice the detection of LLMNR and NBT-NS poisoning attacks with the aid of Wireshark. I learned how attackers use network queries for the interception of credentials and taught me how to use packet analysis to identify rogue machines. The tracking of mistyped queries, compromised user accounts, and unauthorized SMB access incidents served to bolster investigative techniques. The challenge gave further weight to the need to disable vulnerable protocols, secure logs, and adhere to forensic best practices. With this, the most pertinent thing learned from this training was honing my network forensics skill set and gaining insight into credential theft attacks in the real world.

Students Work required for this activity	• Go to the challenge https://cyberdefenders.org/blueteam-ctf-challenges/146#nav-overview • Create an account and Login. • Download the Challenge (Attached also hereby). Uncompress the challenge (pass: cyberdefenders.org) • Answer the 5 challenge questions. • Tool Used: Wireshark. • Show complete screenshots of all your work.
Grading Alerts	• Use the provided template • Show your account real name • Show your machine desktop background (with date & time) for all the screenshots Write in your own words and do not copy from other resources