Reaper Challenge

Sherlock Scenario
Our SIEM alerted us to a suspicious logon event which needs to be looked at immediately . The alert details were that the IP Address and the Source Workstation name were a mismatch .You are provided a network capture and event logs from the surrounding time around the incident timeframe. Corelate the given evidence and report back to your SOC Manager.

Task 1:
What is the IP Address for Forela-Wkstn001?

I opened the Wireshark file and checked the Conversations

Address A	Address B	Packets
172.17.79.129	172.17.79.4	465
172.17.79.136	172.17.79.4	172
172.17.79.135	172.17.79.136	69

Answer: 172.17.79.129

Task 2:
What is the IP Address for Forela-Wkstn002?

Same like task 1

Address A	Address B	Packets
172.17.79.129	172.17.79.4	465
172.17.79.136	172.17.79.4	172
172.17.79.135	172.17.79.136	69

Answer: 172.17.79.136

Task 3:
Which user account's hash was stolen by attacker?

The only user in the Security logs is "arthur.kyle"

Subject:
Security ID: S-1-5-21-3239415629-1862073780-2394361899-1601
Account Name: arthur.kyle
Account Domain: FORELA
Logon ID: 0x64a799

Answer: arthur kyle

Task 4:
What is the IP Address of Unknown Device used by the attacker to intercept credentials?

I checked the Security logs and found a different source IP which accessed a network share

Description

A network share object was accessed.

Subject:
Security ID: S-1-5-21-3239415629-1862073780-2394361899-1601
Account Name: arthur.kyle
Account Domain: FORELA
Logon ID: 0x64a799

Network Information:
Object Type: File
Source Address: 172.17.79.135
Source Port: 40252

Share Information:
Share Name: *\IPC$
Share Path:

Access Request Information:
Access Mask: 0x1
Accesses: ReadData (or ListDirectory)

Answer: 172.17.79.135

Task 5:
What was the fileshare navigated by the victim user account?

I filtered in Wireshark for smb2 and saw several path until I found the right one.

1411	2024-07-31 04:55:28.138614967	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\IPC$
1412	2024-07-31 04:55:28.138749057	172.17.79.4	445	172.17.79.136	50152	SMB2	138	Tree Connect Response
1413	2024-07-31 04:55:28.138920446	172.17.79.136	50152	172.17.79.4	445	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
1414	2024-07-31 04:55:28.139015924	172.17.79.136	50152	172.17.79.4	445	SMB2	202	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \DC01\Trip
1415	2024-07-31 04:55:28.139016034	172.17.79.4	445	172.17.79.136	50152	SMB2	474	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
1416	2024-07-31 04:55:28.147433891	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Ioctl Response, Error: STATUS_NOT_FOUND
1418	2024-07-31 04:55:28.147771119	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1419	2024-07-31 04:55:28.148017658	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1420	2024-07-31 04:55:28.148185020	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1421	2024-07-31 04:55:28.148293852	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1422	2024-07-31 04:55:28.148477824	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1423	2024-07-31 04:55:28.148586918	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1424	2024-07-31 04:55:28.148768705	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1425	2024-07-31 04:55:28.148854405	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1426	2024-07-31 04:55:28.149214285	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1427	2024-07-31 04:55:28.149290206	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1428	2024-07-31 04:55:28.149470182	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1429	2024-07-31 04:55:28.149548097	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1430	2024-07-31 04:55:28.149747678	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1431	2024-07-31 04:55:28.149855920	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
1432	2024-07-31 04:55:28.150044761	172.17.79.136	50152	172.17.79.4	445	SMB2	152	Tree Connect Request Tree: \\DC01\Trip
1433	2024-07-31 04:55:28.150099002	172.17.79.4	445	172.17.79.136	50152	SMB2	130	Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME

Answer: \\DC01\Trip

Task 6:
What is the source port used to logon to target workstation using the compromised account?

I saw the event ID 4624 with logon type 3 from the source IP in task 4

An account was successfully logged on.

Subject:
- Security ID: S-1-0-0
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Information:
- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:
- Security ID: S-1-5-21-3239415629-1862073780-2394361899-1601
- Account Name: arthur.kyle
- Account Domain: FORELA
- Logon ID: 0x64a799
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name: FORELA-WKSTN002
- Source Network Address: 172.17.79.135
- Source Port: 40252

Detailed Authentication Information:
- Logon Process: NtLmSsp
- Authentication Package: NTLM
- Transited Services: -
- Package Name (NTLM only): NTLM V2
- Key Length: 128

Answer: 40252

Task 7:
What is the Logon ID for the malicious session?

Found this logon ID from event ID 5140 which is a network share object was accessed

A network share object was accessed.

Subject:
- Security ID: S-1-5-21-3239415629-1862073780-2394361899-1601
- Account Name: arthur.kyle
- Account Domain: FORELA
- Logon ID: 0x64a799

Network Information:
- Object Type: File
- Source Address: 172.17.79.135
- Source Port: 40252

Share Information:
- Share Name: *\IPC$
- Share Path:

Access Request Information:
- Access Mask: 0x1
- Accesses: ReadData (or ListDirectory)

Answer: 0x64A799

Task 8:
The detection was based on the mismatch of hostname and the assigned IP Address.What is the workstation name and the source IP Address from which the malicious logon occur?

In the event ID 4624 we can see the hostname and the IP.
But when we start the challenge, in task 2 we asked what Is the IP of Forela-Wkstn002? And it was

172.17.79.136

Network Information:
Workstation Name: FORELA-WKSTN002
Source Network Address: 172.17.79.135
Source Port: 40252

Answer: FORELA-WKSTN002, 172.17.79.135

Task 9:
When did the malicious logon happened. Please make sure the timestamp is in UTC?

Same log with event ID 4624 from task 6

- **TimeCreated**
  [**SystemTime**] 2024-07-31T04:55:16.2405897Z
  EventRecordID 14610

Answer: 2024-07-31 04:55:16

Task 10:
What is the share Name accessed as part of the authentication process by the malicious tool used by the attacker?

Same log with event ID 5140 from task 7

A network share object was accessed.

Subject:
Security ID: S-1-5-21-3239415629-1862073780-2394361899-1601
Account Name: arthur.kyle
Account Domain: FORELA
Logon ID: 0x64a799

Network Information:
Object Type: File
Source Address: 172.17.79.135
Source Port: 40252

Share Information:
Share Name: *\IPC$
Share Path:

Access Request Information:
Access Mask: 0x1
Accesses: ReadData (or ListDirectory)

Answer: *\IPC$