HACKTHEBOX

Reaper Writeup

Scenario

```
Our SIEM alerted us to a suspicious logon event which needs to be looked at
immediately. The alert details were that 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 time. Corelate the given evidence and report
back to your SOC Manager.
```

Description

```
In this sherlock players will analyze network traffic and window event logs to
find evidence of NTLM relay attack which are common in active directory
environments.
```

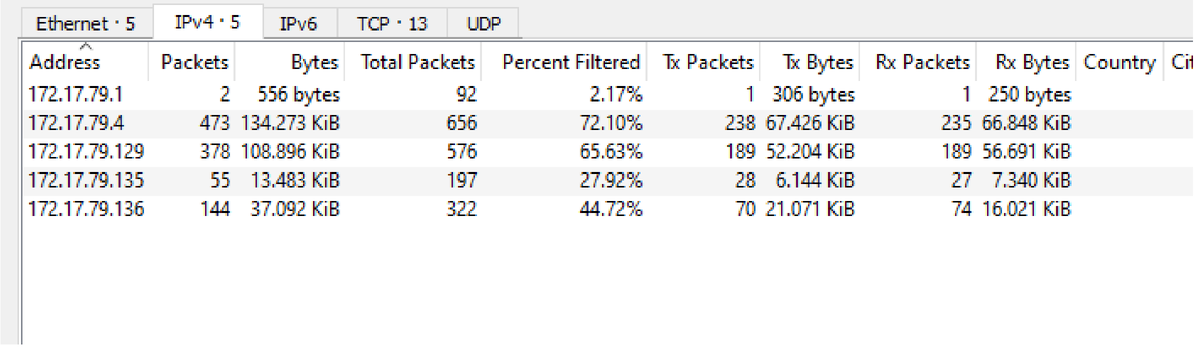
Initial Analysis :

Let's first start by discussing the given artifact. We are given a zip file which upon extraction gives us a PCAP file. The incident concerns the Credential stealing technique using responder tool in an active directory network. You may find the full details of the attack and detection techniques in our blog.

What is PCAP? :

PCAP files are data files created using a program. These files contain packet data of a network and are used to analyze the network characteristics. They also contribute to controlling the network traffic and determining network status. Using PCAP files, teams can attend to detect network problems and resolve data communications using various programs. Security teams can use a network packet capture tool to identify, analyze, inspect, and monitor network traffic. Unusual traffic spikes can be due to a faulty application or a security breach. The packet capture tool allows IT teams to identify the root cause of the issues by tracking network packets.

Let's start by opening the PCAP file in Wireshark. Going over Statistics-> Endpoints we can see top most IP Addresses.



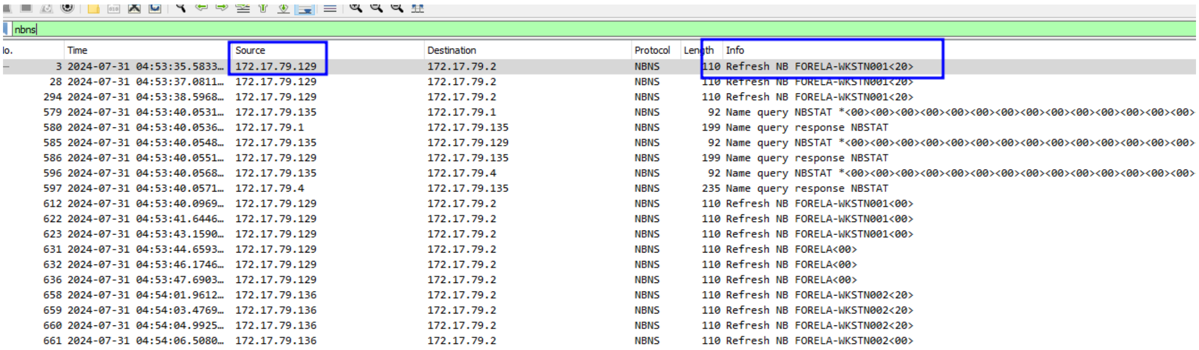
Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	Cit
172.17.79.1	2	556 bytes	92	2.17%	1	306 bytes	1	250 bytes		
172.17.79.4	473	134.273 KiB	656	72.10%	238	67.426 KiB	235	66.848 KiB		
172.17.79.129	378	108.896 KiB	576	65.63%	189	52.204 KiB	189	56.691 KiB		
172.17.79.135	55	13.483 KiB	197	27.92%	28	6.144 KiB	27	7.340 KiB		
172.17.79.136	144	37.092 KiB	322	44.72%	70	21.071 KiB	74	16.021 KiB		

Analysis :

Q1 What is the IP Address for Forela-Wkstn001?

Hint : Filter for nbns protocol to find the relevant IP Address.

Lets first add the nbns filter.


nbns

lo.	Time	Source	Destination	Protocol	Length	Info
3	2024-07-31 04:53:35.5833…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN001<20>
28	2024-07-31 04:53:37.0811…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN001<20>
294	2024-07-31 04:53:38.5968…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN001<20>
579	2024-07-31 04:53:40.0531…	172.17.79.135	172.17.79.1	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00>
580	2024-07-31 04:53:40.0536…	172.17.79.1	172.17.79.135	NBNS	199	Name query response NBSTAT
585	2024-07-31 04:53:40.0548…	172.17.79.135	172.17.79.129	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00>
586	2024-07-31 04:53:40.0551…	172.17.79.129	172.17.79.135	NBNS	199	Name query response NBSTAT
596	2024-07-31 04:53:40.0568…	172.17.79.135	172.17.79.4	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00>
597	2024-07-31 04:53:40.0571…	172.17.79.4	172.17.79.135	NBNS	235	Name query response NBSTAT
612	2024-07-31 04:53:40.0969…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN001<00>
622	2024-07-31 04:53:41.6446…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN001<00>
623	2024-07-31 04:53:43.1590…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN001<00>
631	2024-07-31 04:53:44.6593…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA<00>
632	2024-07-31 04:53:46.1746…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA<00>
636	2024-07-31 04:53:47.6903…	172.17.79.129	172.17.79.2	NBNS	110	Refresh NB FORELA<00>
658	2024-07-31 04:54:01.9612…	172.17.79.136	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN002<20>
659	2024-07-31 04:54:03.4769…	172.17.79.136	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN002<20>
660	2024-07-31 04:54:04.9925…	172.17.79.136	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN002<20>
661	2024-07-31 04:54:06.5080…	172.17.79.136	172.17.79.2	NBNS	110	Refresh NB FORELA-WKSTN002<00>

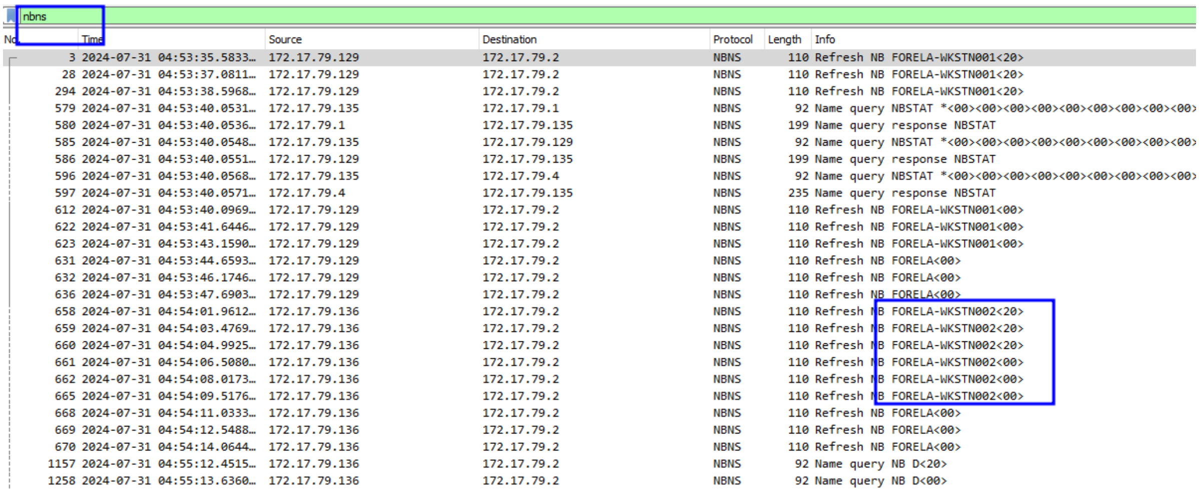
and we can see the relevant ip address.

Ans 172.17.79.129

Q2 What is the IP Address for Forela-Wkstn002?

Hint : Filter for nbns protocol to find the relevant IP Address.

doing the same for second workstation.



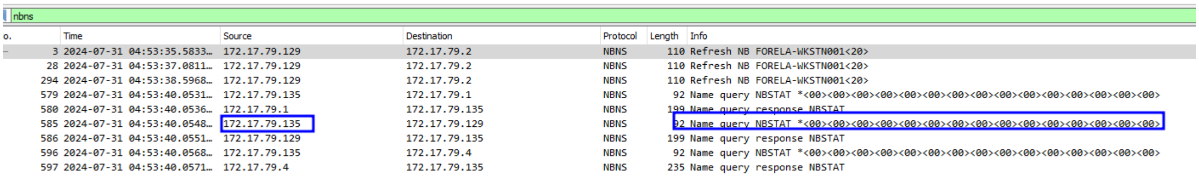
```
nbns
No.  Time                          Source          Destination      Protocol Length Info
   3 2024-07-31 04:53:35.5833…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<20>
  28 2024-07-31 04:53:37.0811…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<20>
 294 2024-07-31 04:53:38.5968…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<20>
 579 2024-07-31 04:53:40.0531…  172.17.79.135   172.17.79.1      NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
 580 2024-07-31 04:53:40.0536…  172.17.79.1     172.17.79.135    NBNS     199 Name query response NBSTAT
 585 2024-07-31 04:53:40.0548…  172.17.79.135   172.17.79.129    NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
 586 2024-07-31 04:53:40.0551…  172.17.79.129   172.17.79.135    NBNS     199 Name query response NBSTAT
 596 2024-07-31 04:53:40.0568…  172.17.79.135   172.17.79.4      NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
 597 2024-07-31 04:53:40.0571…  172.17.79.4     172.17.79.135    NBNS     235 Name query response NBSTAT
 612 2024-07-31 04:53:40.0969…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<00>
 622 2024-07-31 04:53:41.6446…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<00>
 623 2024-07-31 04:53:43.1590…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<00>
 631 2024-07-31 04:53:44.6593…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA<00>
 632 2024-07-31 04:53:46.1746…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA<00>
 636 2024-07-31 04:53:47.6903…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA<00>
 658 2024-07-31 04:54:01.9612…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN002<20>
 659 2024-07-31 04:54:03.4769…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN002<20>
 660 2024-07-31 04:54:04.9925…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN002<20>
 661 2024-07-31 04:54:06.5080…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN002<00>
 662 2024-07-31 04:54:08.0173…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN002<00>
 665 2024-07-31 04:54:09.5176…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN002<00>
 668 2024-07-31 04:54:11.0333…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA<00>
 669 2024-07-31 04:54:12.5488…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA<00>
 670 2024-07-31 04:54:14.0644…  172.17.79.136   172.17.79.2      NBNS     110 Refresh NB FORELA<00>
1157 2024-07-31 04:55:12.4515…  172.17.79.136   172.17.79.2      NBNS      92 Name query NB D<20>
1258 2024-07-31 04:55:13.6360…  172.17.79.136   172.17.79.2      NBNS      92 Name query NB D<00>
```

Ans 172.17.79.136

Q3 Which user account's hash was stolen by attacker?

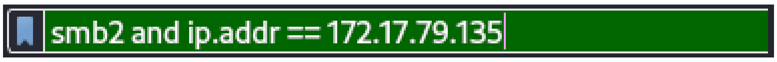
Hint : Filter for ntlmssp protocol in wireshark OR Filter for 4624 event ID and Look for an odd looking logon event.

We see another suspicious internal ip but with no hostname.

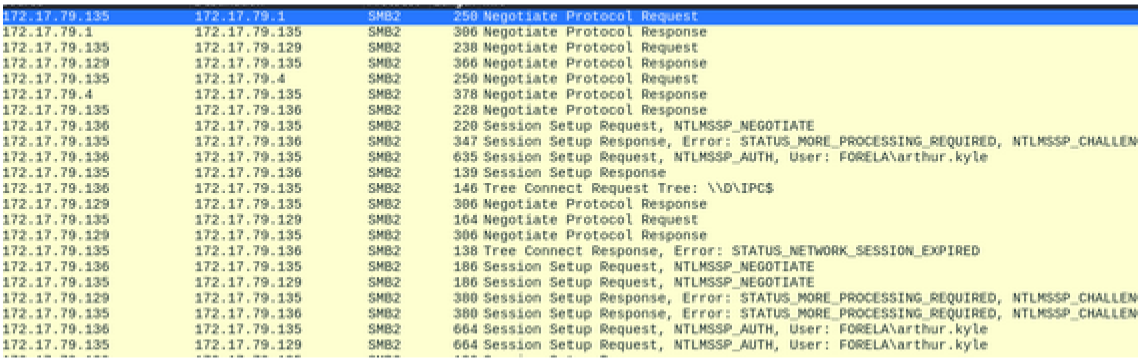


```
nbns
o.   Time                          Source          Destination      Protocol Length Info
   3 2024-07-31 04:53:35.5833…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<20>
  28 2024-07-31 04:53:37.0811…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<20>
 294 2024-07-31 04:53:38.5968…  172.17.79.129   172.17.79.2      NBNS     110 Refresh NB FORELA-WKSTN001<20>
 579 2024-07-31 04:53:40.0531…  172.17.79.135   172.17.79.1      NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 580 2024-07-31 04:53:40.0536…  172.17.79.1     172.17.79.135    NBNS     199 Name query response NBSTAT
 585 2024-07-31 04:53:40.0548…  172.17.79.135   172.17.79.129    NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 586 2024-07-31 04:53:40.0551…  172.17.79.129   172.17.79.135    NBNS     199 Name query response NBSTAT
 596 2024-07-31 04:53:40.0568…  172.17.79.135   172.17.79.4      NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 597 2024-07-31 04:53:40.0571…  172.17.79.4     172.17.79.135    NBNS     235 Name query response NBSTAT
```

Now let's add a filter for smb traffic to and from the unknown device since we suspect it to be the attacker’s machine acting as a Man In The Middle (MITM).



```
smb2 and ip.addr == 172.17.79.135
```



```
172.17.79.135    172.17.79.1      SMB2   250 Negotiate Protocol Request
172.17.79.1      172.17.79.135    SMB2   306 Negotiate Protocol Response
172.17.79.135    172.17.79.129    SMB2   238 Negotiate Protocol Request
172.17.79.129    172.17.79.135    SMB2   366 Negotiate Protocol Response
172.17.79.135    172.17.79.4      SMB2   250 Negotiate Protocol Request
172.17.79.4      172.17.79.135    SMB2   378 Negotiate Protocol Response
172.17.79.135    172.17.79.136    SMB2   228 Negotiate Protocol Response
172.17.79.136    172.17.79.135    SMB2   220 Session Setup Request, NTLMSSP_NEGOTIATE
172.17.79.135    172.17.79.136    SMB2   347 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLEN
172.17.79.136    172.17.79.135    SMB2   635 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
172.17.79.135    172.17.79.136    SMB2   139 Session Setup Response
172.17.79.136    172.17.79.135    SMB2   146 Tree Connect Request Tree: \\D\IPC$
172.17.79.129    172.17.79.135    SMB2   306 Negotiate Protocol Response
172.17.79.135    172.17.79.129    SMB2   164 Negotiate Protocol Request
172.17.79.129    172.17.79.135    SMB2   306 Negotiate Protocol Response
172.17.79.135    172.17.79.136    SMB2   138 Tree Connect Response, Error: STATUS_NETWORK_SESSION_EXPIRED
172.17.79.136    172.17.79.135    SMB2   186 Session Setup Request, NTLMSSP_NEGOTIATE
172.17.79.135    172.17.79.129    SMB2   186 Session Setup Request, NTLMSSP_NEGOTIATE
172.17.79.129    172.17.79.135    SMB2   380 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLEN
172.17.79.135    172.17.79.136    SMB2   380 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLEN
172.17.79.136    172.17.79.135    SMB2   664 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
172.17.79.135    172.17.79.129    SMB2   664 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
```

In above image, we can see that user “arthur.kyle” was involved in the authentication process and the unknown device is involved in this as well.

Ans arthur kyle

Q4 What is the IP Address of Unknown Device used by the attacker to intercept credentials?

Hint : Look for an IP Address that do not belong to any workstation but is involved in authentication flow for the victim user. Alternatively you can also filter for NBNS protocol and the device with no hostname is the device we looking for. Another method is to look for the anomalous logon event and see the source IP Address.

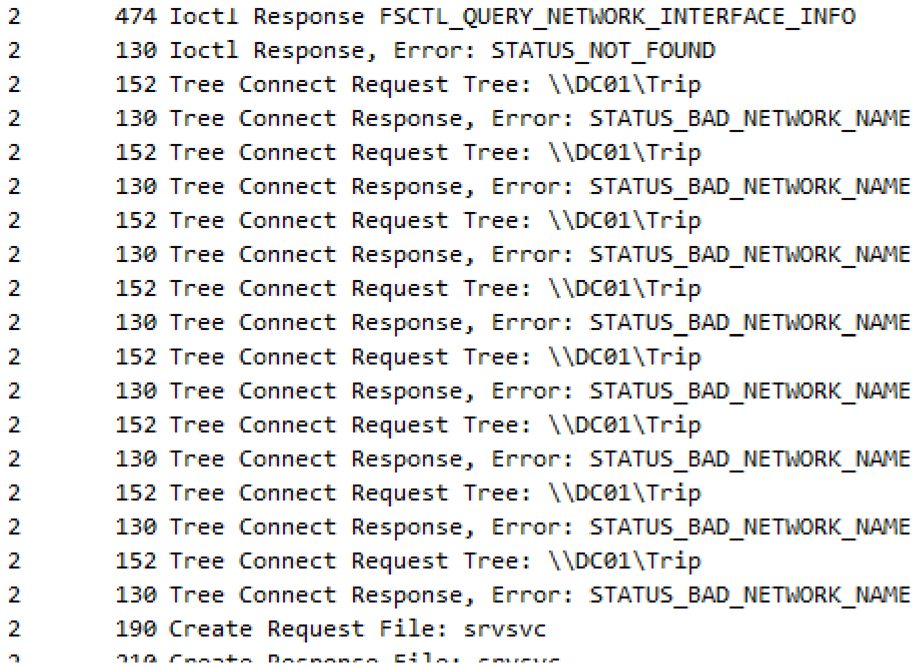
We already found this in previous question.

Ans 172.17.79.135

Q5 Shortly after entering the wrong path and triggering the relay attack, the user tried again and entered the intended path. What was this fileshare path which victim tried navigating to?

Hint : Filter for smb2 traffic in wireshark. Search for keywords "Tree connect Request Tree" in packet details. Now look for any file share path which seems like a legit path a day to day user might visit.

We first filter for 'smb2' traffic and then search for BAD_NETWORK_NAME.



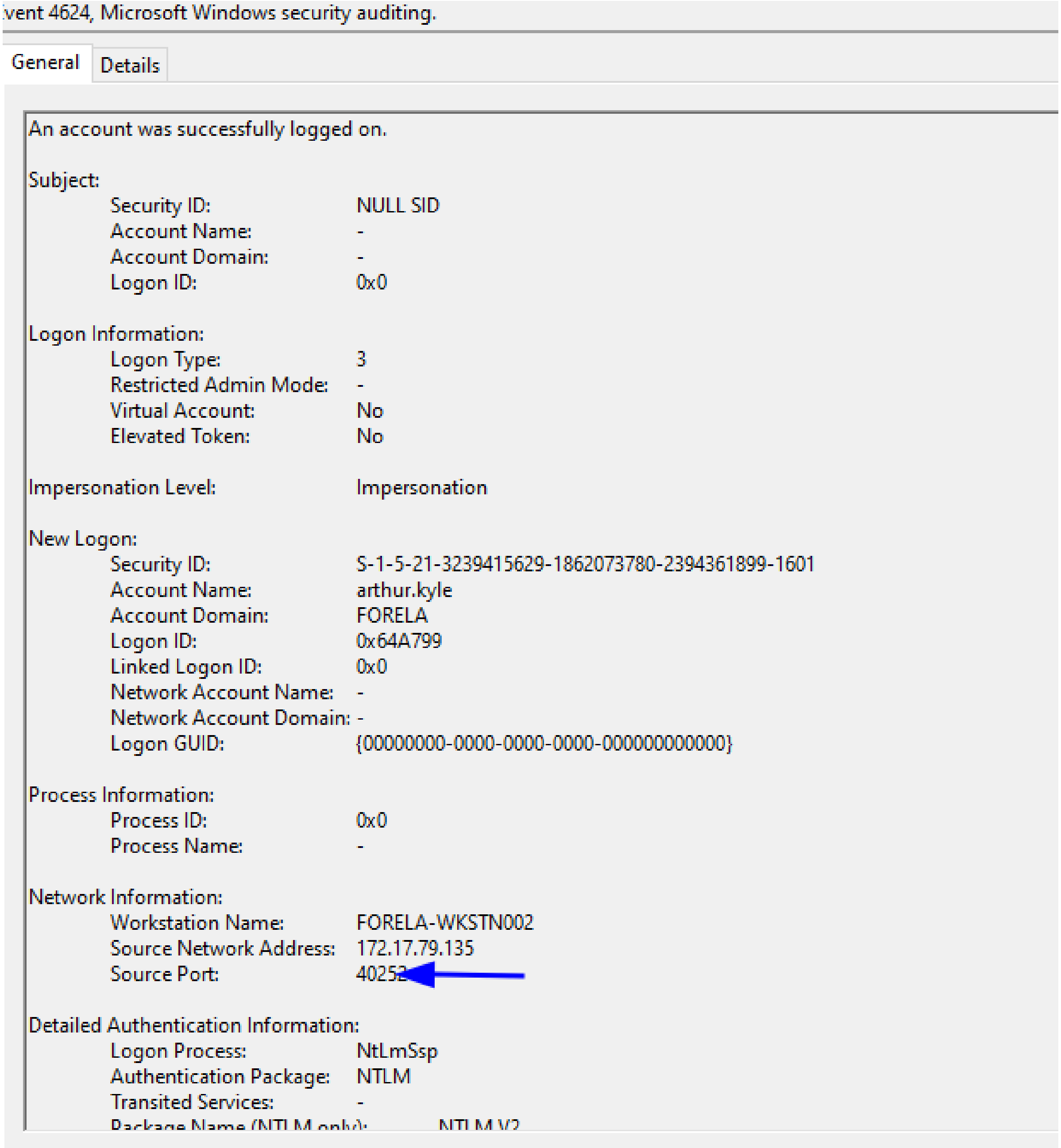
```
2       474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
2       130 Ioctl Response, Error: STATUS_NOT_FOUND
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       152 Tree Connect Request Tree: \\DC01\Trip
2       130 Tree Connect Response, Error: STATUS_BAD_NETWORK_NAME
2       190 Create Request File: srvsvc
2       210 Create Response File: srvsvc
```

Ans \\DC01\Trip

Q6 What is the source port used to logon to target workstation using the compromised account?

Hint : In provided Event logs, filter for event ID 4624 and look for a event where Security ID is NULL and logon type is 3.The logon process value will be NtlmSSP and authentication package value is NTLM. Then look for Source Port value in event details.

Lets open event log file and see the relevant event id as mentioned in the hint.

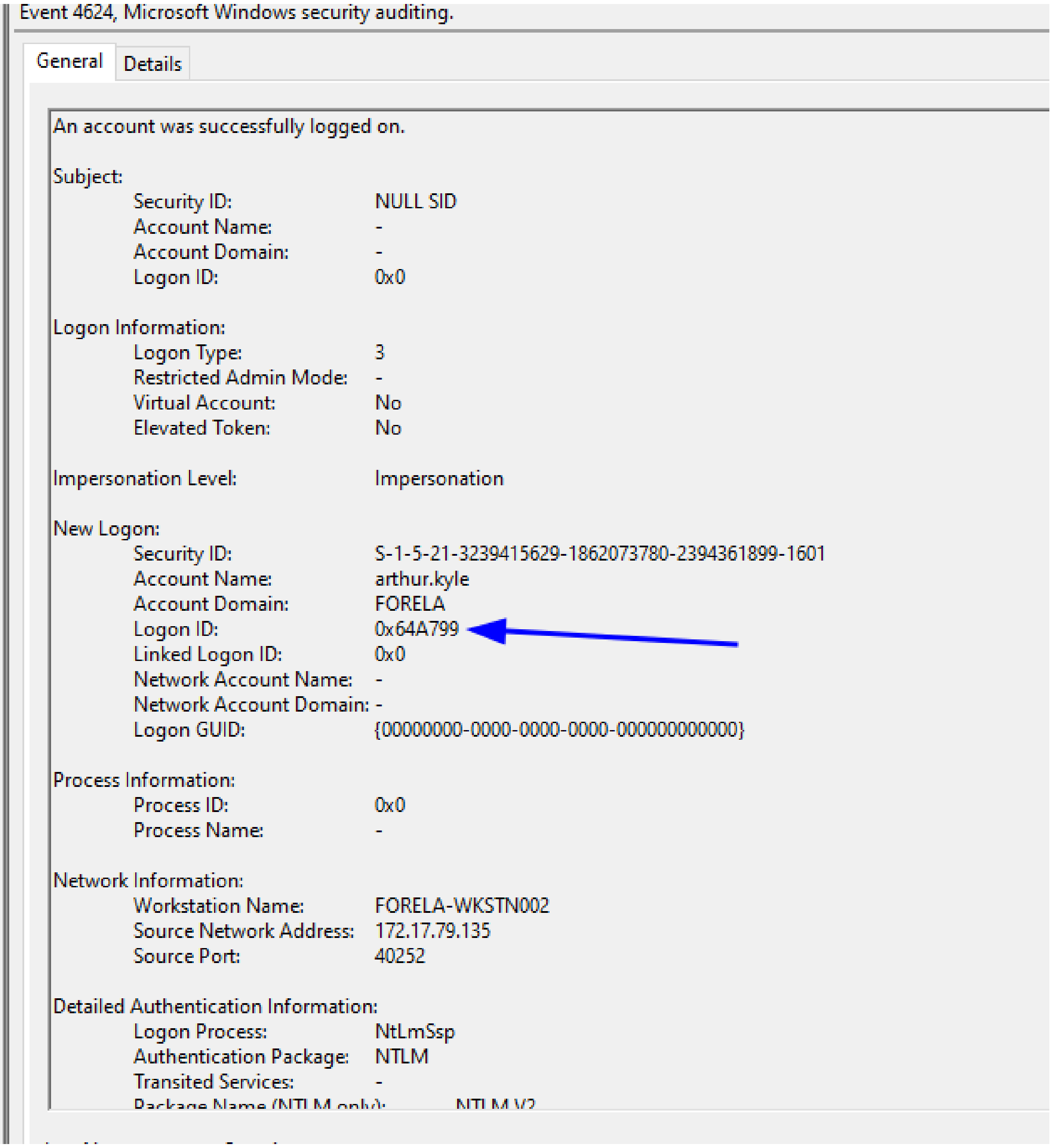


```
vent 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:
        Security ID:                NULL SID
        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
```

Ans 40252

Q7 What is the Logon ID for the malicious session?

Hint : In the same event, look for LOGON ID Value



Event 4624, Microsoft Windows security auditing.

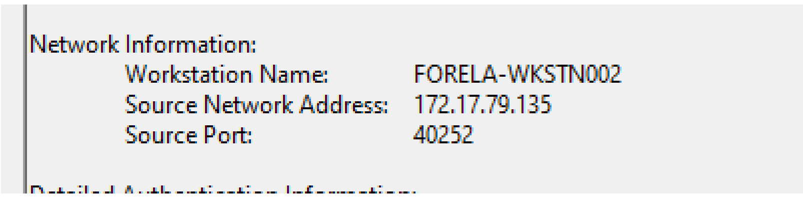
```
An account was successfully logged on.

Subject:
        Security ID:                NULL SID
        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
```

Ans 0x64A799

Q8 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?

Hint : We already found all the IP Addresses for all the devices in the network. In the specified event ID 4624 , find both the workstation and IP from network information section. The workstation name is false as its assigned IP will not be the one you see in the event log.

We can get this information from network information tab in event logs.



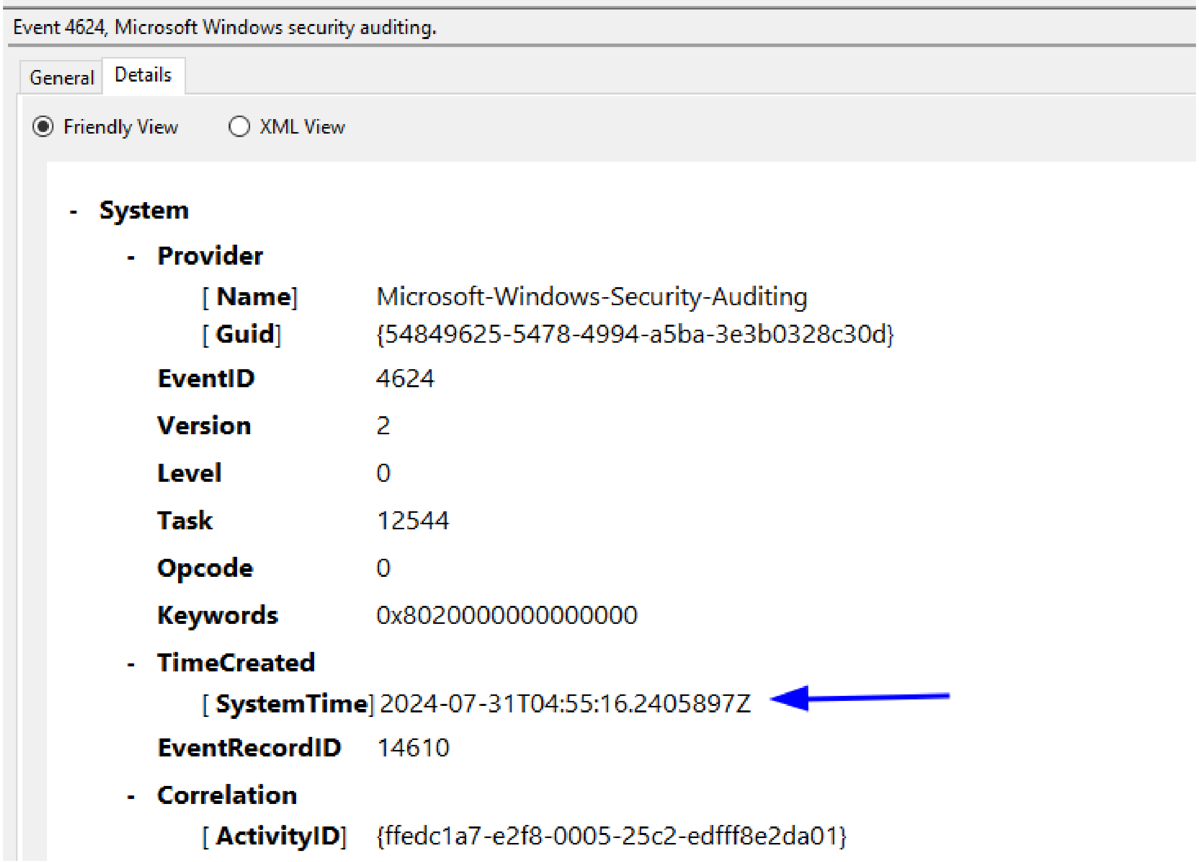
```
Network Information:
        Workstation Name:           FORELA-WKSTN002
        Source Network Address:     172.17.79.135
        Source Port:                40252

Detailed Authentication Information:
```

Ans FORELA-WKSTN002, 172.17.79.135

Q9 When did the malicious logon happened. Please make sure the timestamp is in UTC?

Hint : Look in details tab for the UTC Time

We look in the details tab for System Time for the relevant event log.



Event 4624, Microsoft Windows security auditing.

● Friendly View ○ XML View

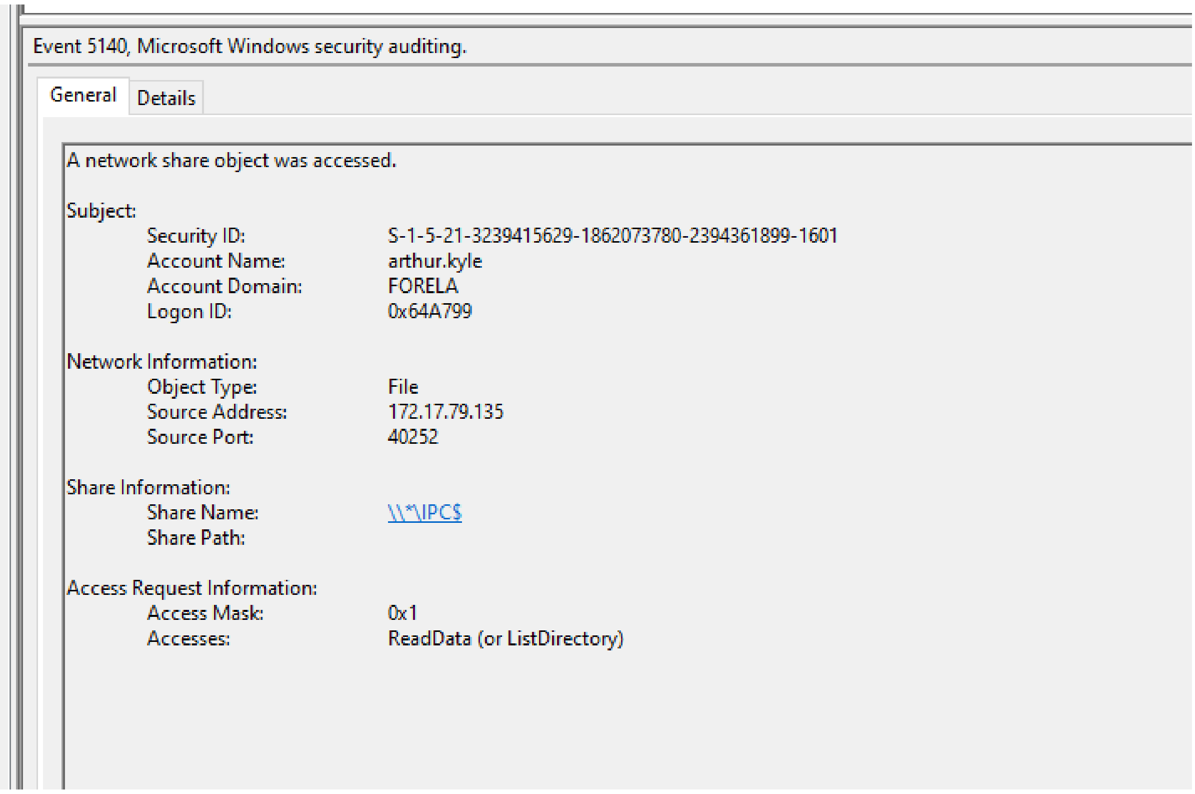
```
- System
    - Provider
          [ Name]        Microsoft-Windows-Security-Auditing
          [ Guid]        {54849625-5478-4994-a5ba-3e3b0328c30d}
      EventID            4624
      Version            2
      Level              0
      Task               12544
      Opcode             0
      Keywords           0x8020000000000000
    - TimeCreated
          [ SystemTime] 2024-07-31T04:55:16.2405897Z
      EventRecordID      14610
    - Correlation
          [ ActivityID]  {ffedc1a7-e2f8-0005-25c2-edfff8e2da01}
```

Ans   2024-07-31 04:55:16

Q10 What is the share Name accessed as part of the authentication process by the malicious tool used by the attacker?Look for the answer in Provided Event logs.

Hint : Look for event ID 5140 and see the share name accessed. We can corelate this event with the malicious session via the Logon ID we found before.

Filtering for the specific event id we see the share details.



```
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)
```

Ans \\*\IPC$