Reaper - Walkthrough

Friday, August 16, 2024 2:14 PM

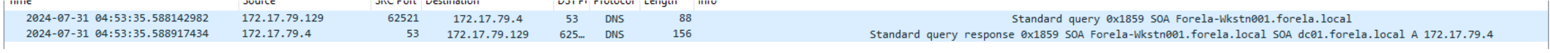
Story:
Our SIEM alerted us to a suspicious logon event which needs to be looked at immediately .
The alert details were that the IP Address and the Source Workstation name were a mismatch .
You are provided a network capture and event logs from the surrounding time around the incident timeframe.
Corelate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

- Open Wireshark and 'Event Log Explorer' and load the logs

Task1: What is the IP Address for Forela-Wkstn001?

- To find the answer and filtered 'dns', we can see in the first log a DNS query is asking for the SOA (Start of Authority) record for Forela-Wkstn001.forela.local.
  This query was sent from **172.17.79.129** to the DNS server 172.17.79.4, which responded in the second line.

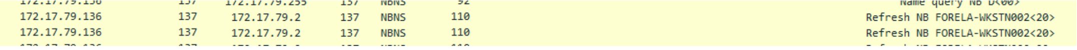
  Since Forela-wkstn001 initiated the query, its IP address is 172.17.79.129.



```
2024-07-31 04:53:35.588142982   172.17.79.129   62521   172.17.79.4     53     DNS   88    Standard query 0x1859 SOA Forela-Wkstn001.forela.local
2024-07-31 04:53:35.588917434   172.17.79.4        53   172.17.79.129   625…   DNS   156   Standard query response 0x1859 SOA Forela-Wkstn001.forela.local SOA dc01.forela.local A 172.17.79.4
```

Task2: What is the IP Address for Forela-Wkstn002?

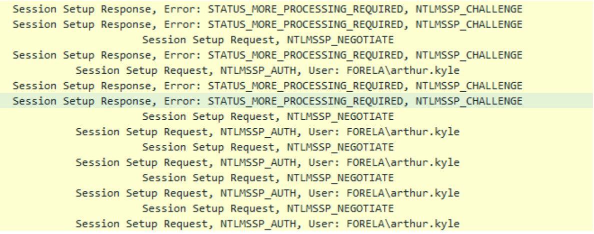
- The second way to find the IP of a workstation is the filter 'nbns' (NetBios) a protocol that allows applications on different computers to communicate within a local network when DNS failed.



```
172.17.79.136   137   172.17.79.2   137   NBNS   110   Refresh NB FORELA-WKSTN002<20>
172.17.79.136   137   172.17.79.2   137   NBNS   110   Refresh NB FORELA-WKSTN002<20>
```

Task3: Which user account's hash was stolen by attacker?

- To find the username, we should filter for NTLMSSP in the network traffic. NTLMSSP is part of the NTLM (NT LAN Manager) authentication protocol, which works by exchanging hashed credentials rather than sending plaintext passwords.
  By filtering for NTLMSSP traffic in a PCAP file, we can identify authentication attempts and extract the username associated with the compromised account.



```
Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
                   Session Setup Request, NTLMSSP_NEGOTIATE
Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
         Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
                   Session Setup Request, NTLMSSP_NEGOTIATE
         Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
                   Session Setup Request, NTLMSSP_NEGOTIATE
         Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
                   Session Setup Request, NTLMSSP_NEGOTIATE
         Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
                   Session Setup Request, NTLMSSP_NEGOTIATE
         Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
```

Task4: What is the IP Address of Unknown Device used by the attacker to intercept credentials?

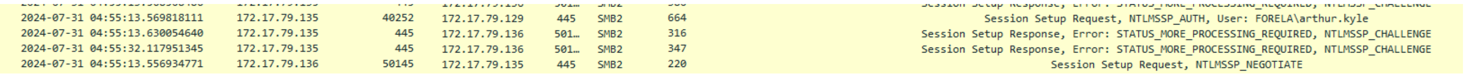
- We can identify answer in the same logs, In an NTLM relay attack, the attacker intercepts NTLM authentication requests and relays them to another service to authenticate on behalf of the victim, effectively impersonating them.

  The attack involves two main IP addresses:
  Victim IP: The IP address of the device that initially sends the NTLM authentication request.
  Attacker's IP: The IP address of the device intercepting and relaying the authentication traffic.

  The source IP sends an **NTLMSSP_AUTH** request to an intermediate IP

  The **intermediate IP** (Attacker IP) then relays this NTLMSSP_AUTH request to another server (target server).

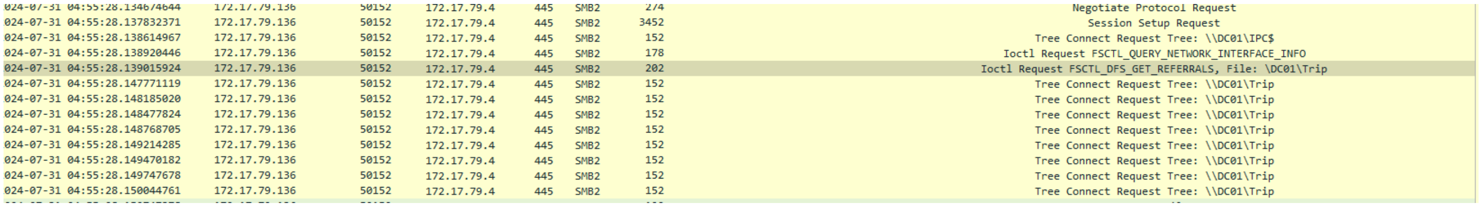
  The **Attacker IP** will be the one relaying the NTLMSSP messages between the Victim IP and the Target Server.



```
2024-07-31 04:55:13.569818111   172.17.79.135   40252   172.17.79.129   445    SMB2   664   Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
2024-07-31 04:55:13.630054640   172.17.79.135     445   172.17.79.136   501…   SMB2   316   Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
2024-07-31 04:55:32.117951345   172.17.79.135     445   172.17.79.136   501…   SMB2   347   Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
2024-07-31 04:55:13.556934771   172.17.79.136   50145   172.17.79.135   445    SMB2   220   Session Setup Request, NTLMSSP_NEGOTIATE
```

Task5: What was the fileshare navigated by the victim user account?

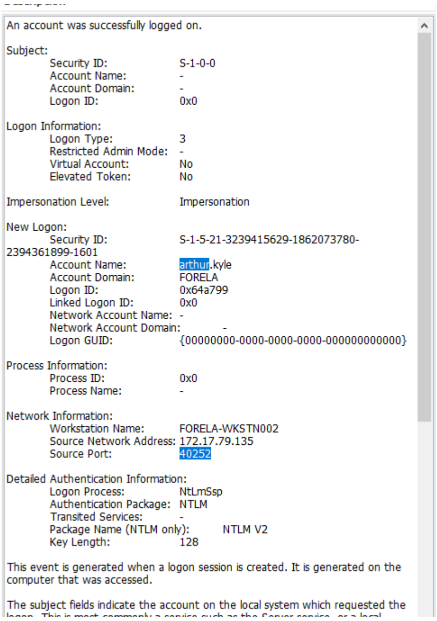
- In the previous question, we discovered that the user likely made an error with the FileShare name, allowing the attacker to intercept the request.
  To investigate further, we should search for packets where the attacker's IP initiated a connection.
  These packets will contain information about the requested share.



```
024-07-31 04:55:28.134674644   172.17.79.136   50152   172.17.79.4   445   SMB2   274    Negotiate Protocol Request
024-07-31 04:55:28.137832371   172.17.79.136   50152   172.17.79.4   445   SMB2   3452   Session Setup Request
024-07-31 04:55:28.138614967   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\IPC$
024-07-31 04:55:28.138920446   172.17.79.136   50152   172.17.79.4   445   SMB2   178    Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
024-07-31 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
024-07-31 04:55:28.147771119   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
024-07-31 04:55:28.148185020   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
024-07-31 04:55:28.148477824   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
024-07-31 04:55:28.148768705   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
024-07-31 04:55:28.149214285   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
024-07-31 04:55:28.149470182   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
024-07-31 04:55:28.149747678   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
024-07-31 04:55:28.150044761   172.17.79.136   50152   172.17.79.4   445   SMB2   152    Tree Connect Request Tree: \\DC01\Trip
```

Task6: What is the source port used to logon to target workstation using the compromised account?

- To find the answer, you should filter in the 'Security' logs event ID '4624' and 'arthur' to find the authentication log:



```
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

This event is generated when a logon session is created. It is generated on the
computer that was accessed.

The subject fields indicate the account on the local system which requested the
```

Task7: What is the Logon ID for the malicious session?

- In the same log: 0x64a799

**Task8: 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 same log:

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

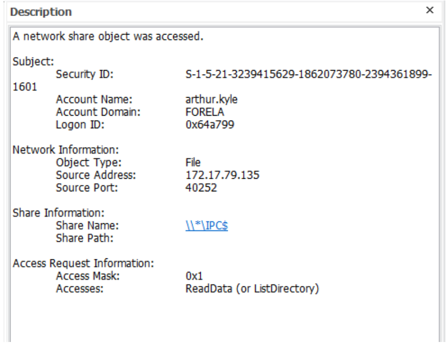
Task9: When did the malicious logon happened. Please make sure the timestamp is in UTC

- In the same log:

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

Task10: **What is the share Name accessed as part of the authentication process by the malicious tool used by the attacker?**

- Pretty simple, filter in Security logs the event ID '5140' which related to 'A network share object was accessed' and find in the answer in the log:



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)
```