HTB- Sherlocks: Reaper – Level: Very Easy
Amit Persky

Table of Contents

Intro:

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.

Tools that I used in this Sherlock:

1. Wireshark
2. Event Viewer

About:

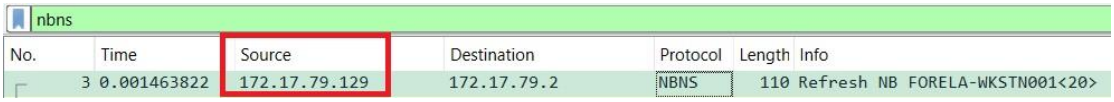
Reaper is a very easy Sherlock which covers NTLM relay attacks , comprised of AD Forensics, MITM Attack detection & network forensics. In this sherlock players will analyze network traffic and window event logs to find evidence of NTLM relay attack which are common in active directory environments.

Task 1:

What is the IP Address for Forela-Wkstn001?

Ok so we got 2 files:

So I opened the network recording file in Wireshark and filtered for nbns protocol (because it used for name resolution in Windows networks, allowing computers to find each other):



As we can see that Forela-Wkstn001 source IP 172.17.79.129.

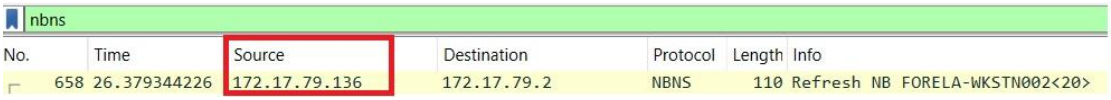
Answer:

172.17.79.129

Task 2:

What is the IP Address for Forela-Wkstn002?

As the last question, same method just scrolling down:



As we can see Forela-Wkstn002 IP is 172.17.79.136.

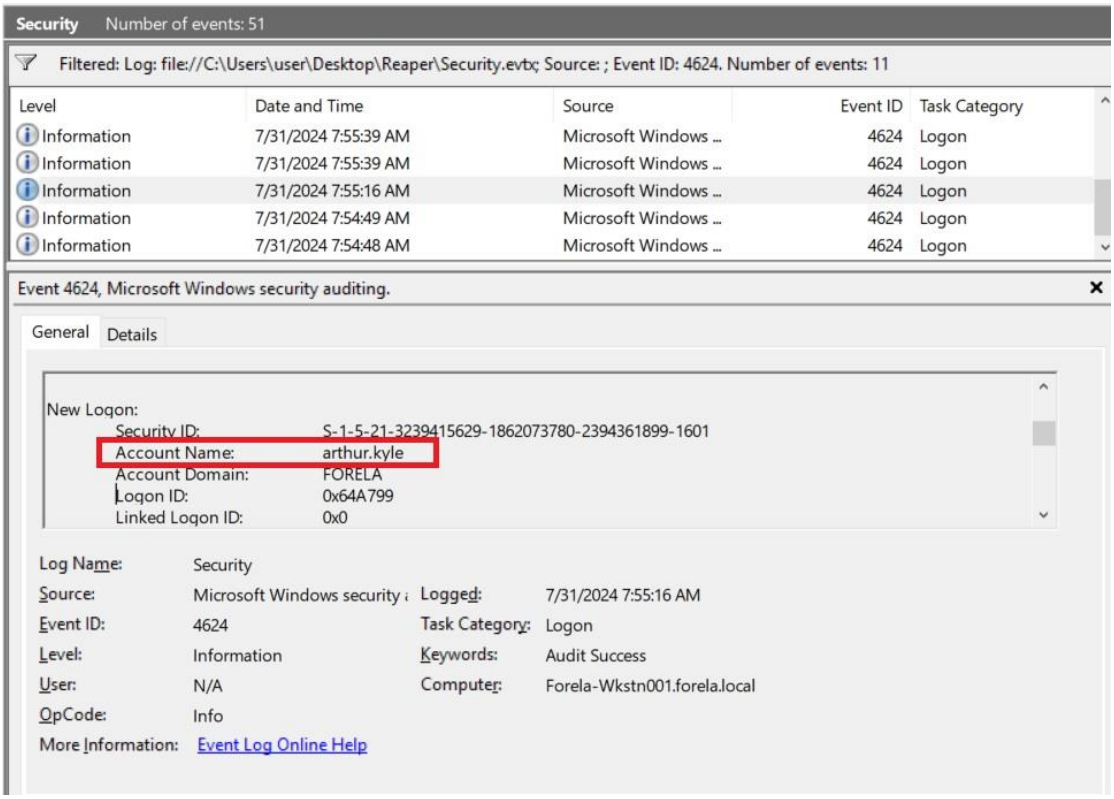
Answer:

172.17.79.136

Task 3:

Which user account's hash was stolen by attacker?

ok for this question we are going to use Event Viewer, and going to filter for 4624. After that we are going to look for something that are irregular:



After some search you can observe that 1 event is with account name of some human, Arthur.kyle and this is the answer.

Answer:

arthur kyle

Task 4:

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

ok for answering this question I scrolled down in the general data of the event from the last question and saw this:

As we can see, the IP is 172.17.79.135

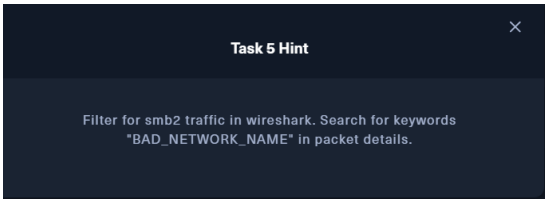
Answer:

172.17.79.135

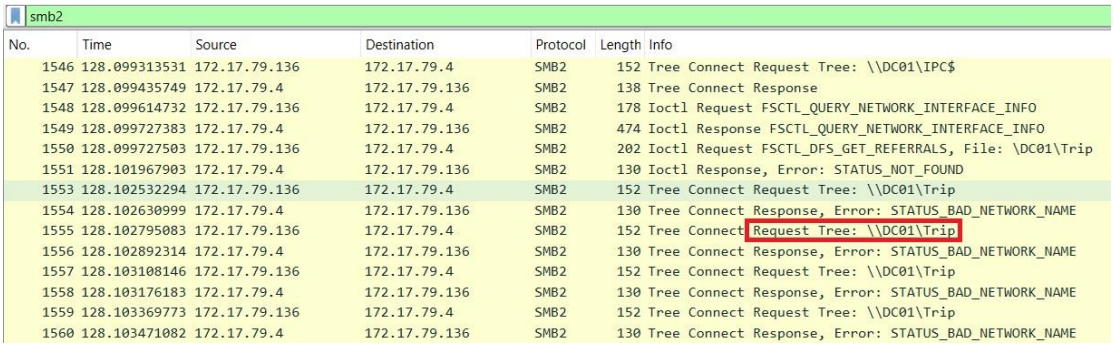
Task 5:

What was the fileshare navigated by the victim user account?

Ok for answering this question I look at HTB hint:



I filtered the network file for smb2 and looked for BAD_NETWORK_NAME:



As we can see the path coming after STATUS_BAD_NETWORK_NAME:

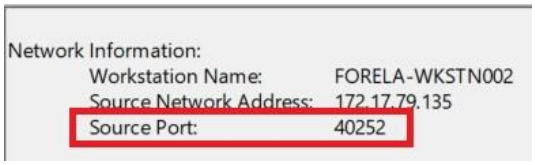
Answer:

\\DC01\Trip

Task 6:

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

Ok for answering this question I moved back to the suspicious event in the event viewer that we say before and saw this:



As we can see the source Port is 40252 and this is what we looked for.

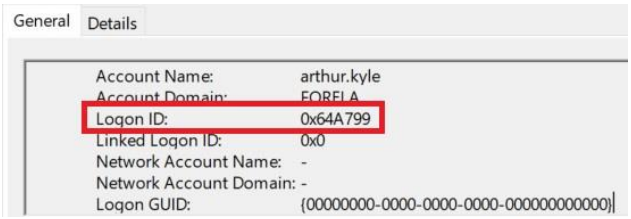
Answer:

40252

Task 7:

What is the Logon ID for the malicious session?

To answer this question I scrolled up in the suspicious event and saw this:



As we can see the answer is written in the general data.

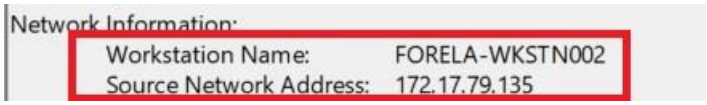
Answer:

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?

I looked at our suspicious event and looked for the workstation name and the IP to combine them for the answer:



As we can see we just need to put this answers in one line.

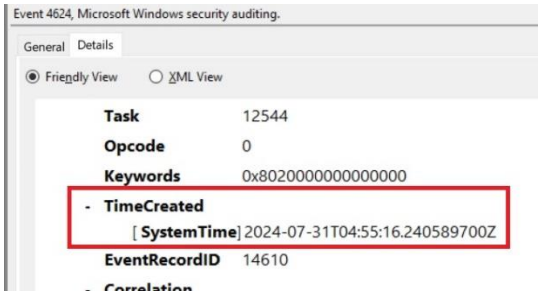
Answer:

FORELA-WKSTN002, 172.17.79.135

Task 9:

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

To answer that question we need to look at the suspicious logon in the Details date and look for that:



As we can see the time is on TimeCreated.

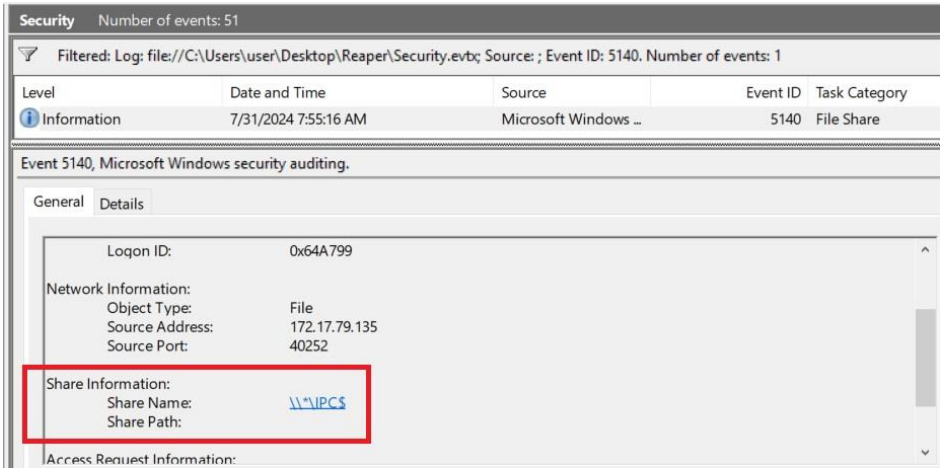
Answer:

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?

for answering that question we need to filter for event 5140 because he is indicates that a network share was accessed on a Windows system:



As we can see, in the Share Information we get the answer:

Answer:

***\IPC$**