Tracer Challenge

Sherlock Scenario

A junior SOC analyst on duty has reported multiple alerts indicating the presence of PsExec on a workstation. They verified the alerts and escalated the alerts to tier II. As an Incident responder you triaged the endpoint for artefacts of interest. Now please answer the questions regarding this security event so you can report it to your incident manager.

Task 1:
The SOC Team suspects that an adversary is lurking in their environment and are using PsExec to move laterally. A junior SOC Analyst specifically reported the usage of PsExec on a WorkStation. How many times was PsExec executed by the attacker on the system?

I used PECmd.exe on the prefetch directory and opened it with Timeline Explorer

Run Count
=
9

Answer: 9

Task 2:
What is the name of the service binary dropped by PsExec tool allowing attacker to execute remote commands?

I checked the "Files Loaded" tab

Cell contents

```
\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\NTDLL.DLL,
\VOLUME{01d951602330db46-52233816}\WINDOWS\PSEXESVC.EXE,
```

Answer: psexesvc.exe

Task 3:
Now we have confirmed that PsExec ran multiple times, we are particularly interested in the 5th Last instance of the PsExec. What is the timestamp when the PsExec Service binary ran?

I checked the "Previous Run3" tab

Previous Run3
=
2023-09-07 12:06:54

Answer: 07/09/2023 12:06:54

Task 4:
Can you confirm the hostname of the workstation from which attacker moved laterally?

I checked the event ID 4624 in Security logs

Description

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: Yes

Impersonation Level: Impersonation

New Logon:
- Security ID: S-1-5-21-3239415629-1862073780-2394361899-500
- Account Name: Administrator
- Account Domain: FORELA
- Logon ID: 0x61f9a5
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

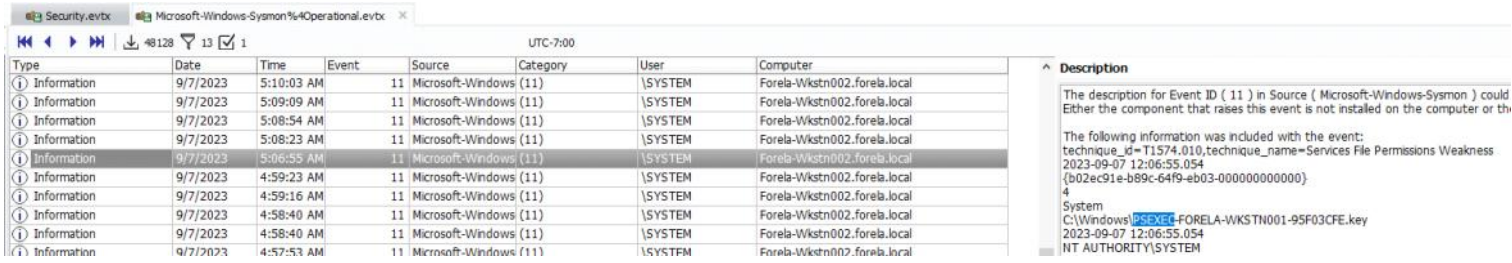
Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name: FORELA-WKSTN001
- Source Network Address: 172.17.79.129
- Source Port: 49924

Answer: Forela-Wkstn001

Task 5:
What is full name of the Key File dropped by 5th last instance of the Psexec?

I filtered for psexec and event ID 1 in Sysmon logs



Answer: PSEXEC-FORELA-WKSTN001-95F03CFE.key

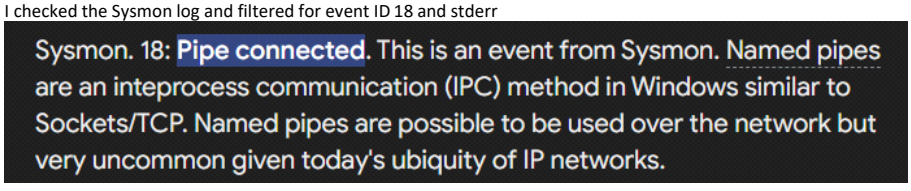
Task 6:
Can you confirm the timestamp when this key file was created on disk?

Answer is in the same picture from task 5

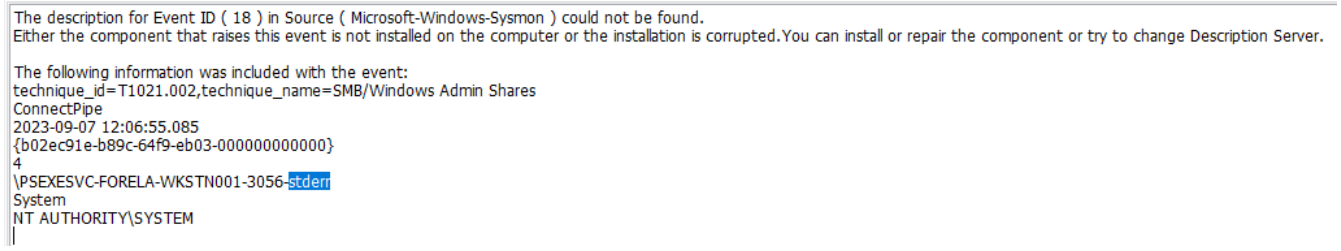
Answer: 07/09/2023 12:06:55

Task 7:
What is the full name of the Named Pipe ending with the "stderr" keyword for the 5th last instance of the PsExec?

I checked the Sysmon log and filtered for event ID 18 and stderr



Description



Answer: \PSEXESVC-FORELA-WKSTN001-3056-stderr