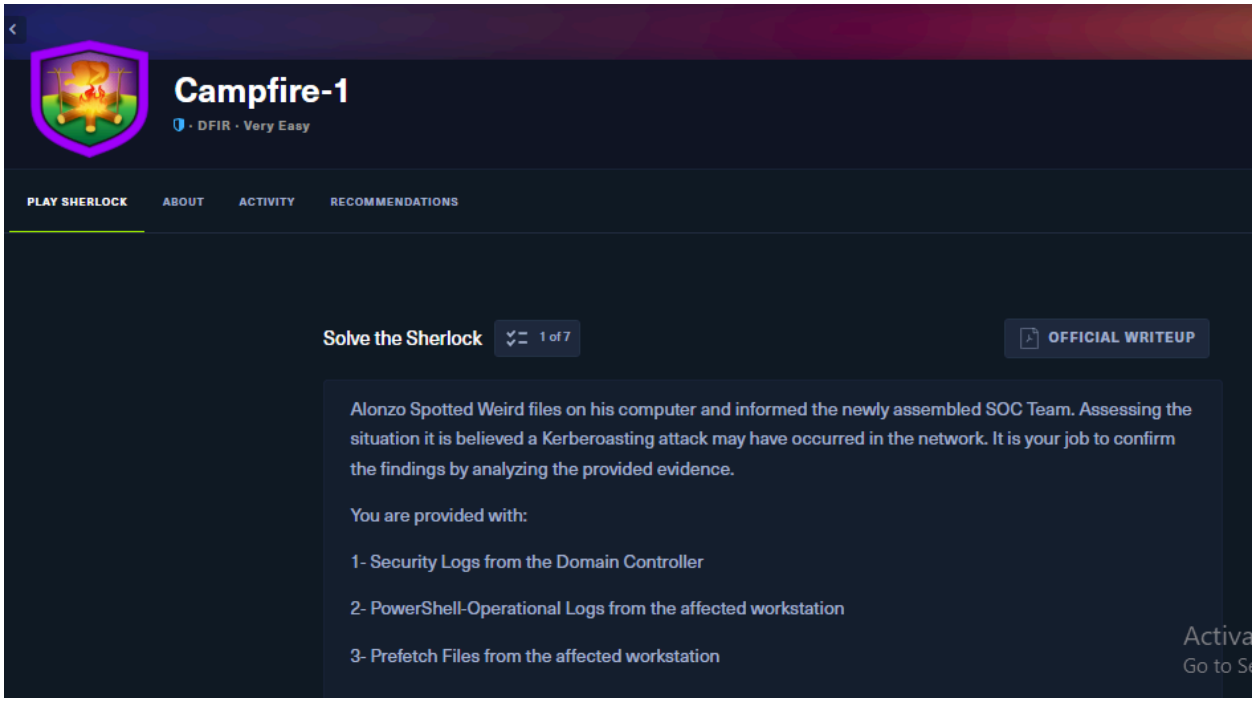
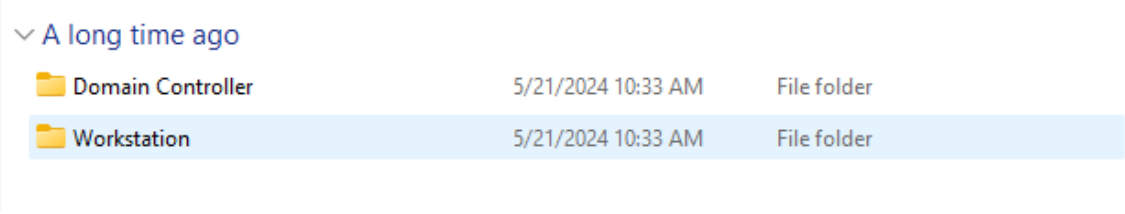
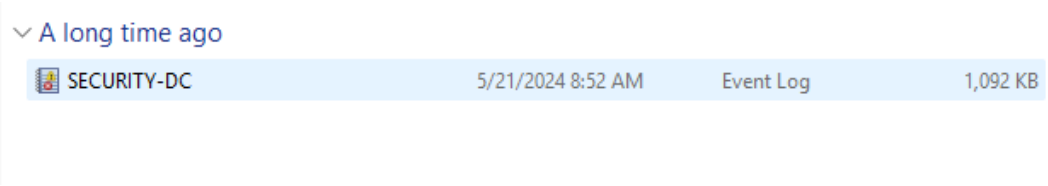
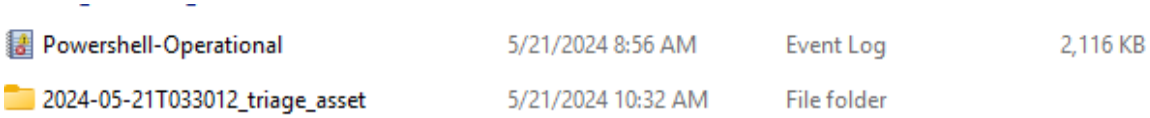
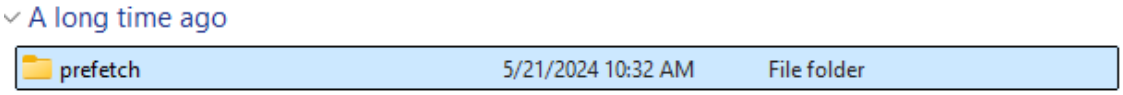

Campfire-1
· DFIR · Very Easy
PLAY SHERLOCK
ABOUT
ACTIVITY
RECOMMENDATIONS
Solve the Sherlock
1 of 7
OFFICIAL WRITEUP
Alonzo Spotted Weird files on his computer and informed the newly assembled SOC Team. Assessing the situation it is believed a Kerberoasting attack may have occurred in the network. It is your job to confirm the findings by analyzing the provided evidence.
You are provided with:
1- Security Logs from the Domain Controller
2- PowerShell-Operational Logs from the affected workstation
3- Prefetch Files from the affected workstation

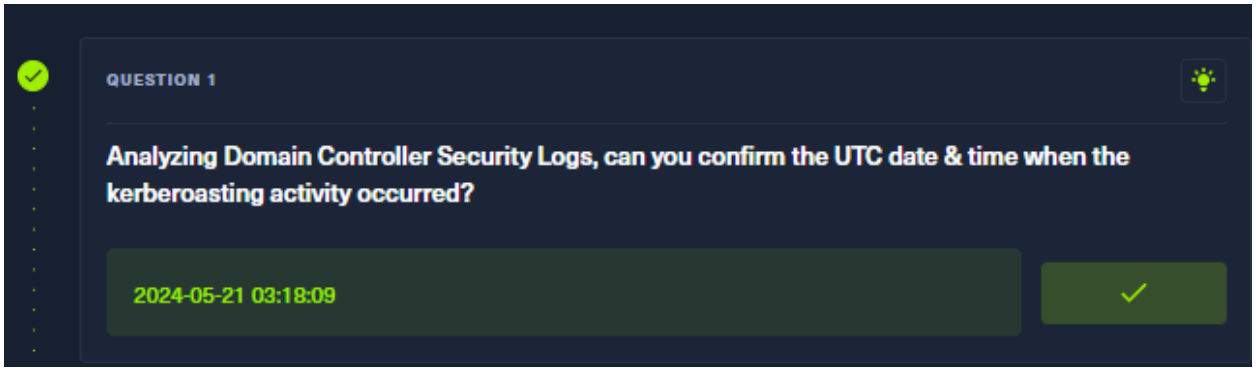

A long time ago
Domain Controller 5/21/2024 10:33 AM File folder
Workstation 5/21/2024 10:33 AM File folder


A long time ago
SECURITY-DC 5/21/2024 8:52 AM Event Log 1,092 KB

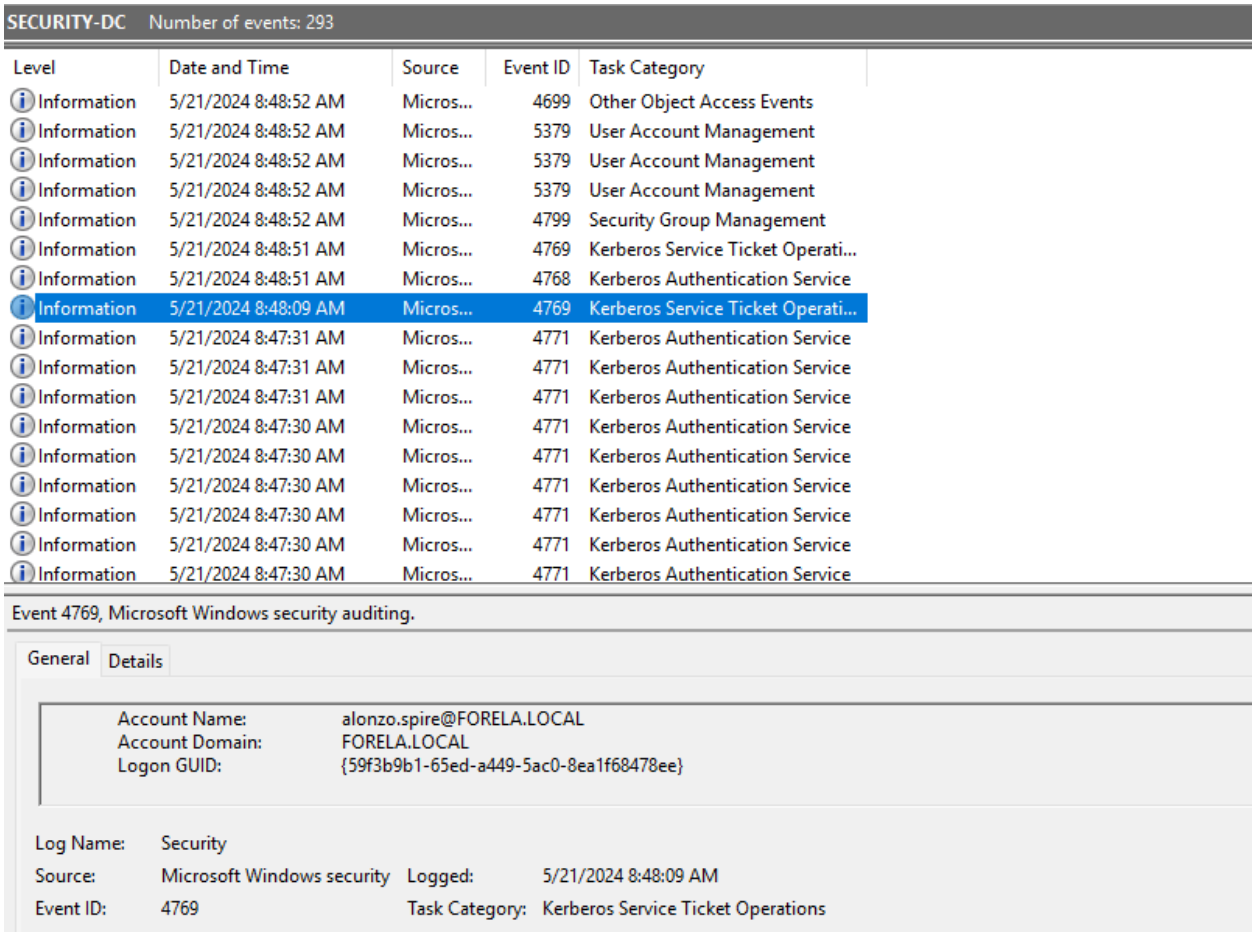

Powershell-Operational 5/21/2024 8:56 AM Event Log 2,116 KB
2024-05-21T033012_triage_asset 5/21/2024 10:32 AM File folder

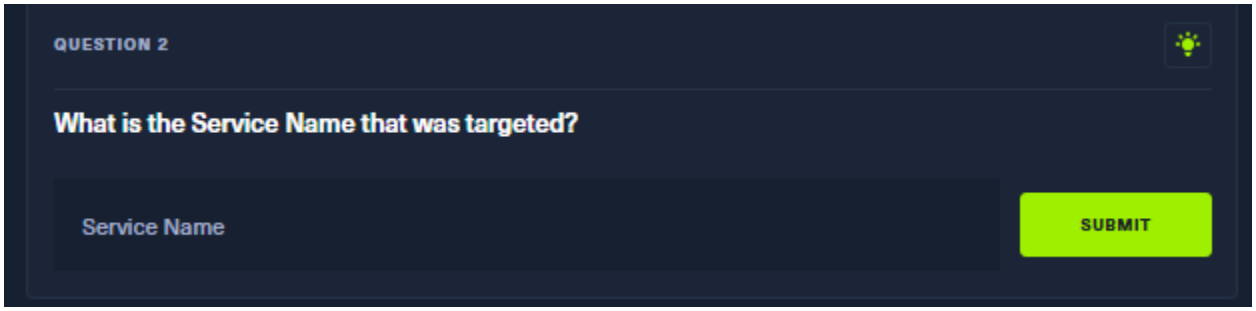

A long time ago
prefetch 5/21/2024 10:32 AM File folder

SVCHOST.EXE-C25BD44A.pf	5/21/2024 9:00 AM	PF File	8 KB
AUDIODG.EXE-AB22E9A6.pf	5/21/2024 8:58 AM	PF File	8 KB
CONSENT.EXE-40419367.pf	5/21/2024 8:58 AM	PF File	122 KB
SVCHOST.EXE-262B838E.pf	5/21/2024 8:58 AM	PF File	6 KB
SVCHOST.EXE-D4A56B1A.pf	5/21/2024 8:58 AM	PF File	4 KB
SVCHOST.EXE-9D041ABC.pf	5/21/2024 8:58 AM	PF File	5 KB
SVCHOST.EXE-852EC587.pf	5/21/2024 8:58 AM	PF File	16 KB
FILECOAUTH.EXE-88F71F64.pf	5/21/2024 8:58 AM	PF File	12 KB
SMARTSCREEN.EXE-EACC1250.pf	5/21/2024 8:58 AM	PF File	15 KB
DLLHOST.EXE-7D5CE0CA.pf	5/21/2024 8:58 AM	PF File	4 KB
RUNDLL32.EXE-75313621.pf	5/21/2024 8:58 AM	PF File	4 KB
WINRAR.EXE-BA8CDB31.pf	5/21/2024 8:58 AM	PF File	80 KB
SVCHOST.EXE-F952D9A9.pf	5/21/2024 8:57 AM	PF File	9 KB
TIWORKER.EXE-FBD79BD6.pf	5/21/2024 8:57 AM	PF File	15 KB
TRUSTEDINSTALLER.EXE-766EFF52.pf	5/21/2024 8:57 AM	PF File	5 KB
TASKHOSTW.EXE-2E5D4B75.pf	5/21/2024 8:57 AM	PF File	28 KB
SEARCHFILTERHOST.EXE-44162447.pf	5/21/2024 8:57 AM	PF File	5 KB
SEARCHPROTOCOLHOST.EXE-69C456C3....	5/21/2024 8:57 AM	PF File	6 KB

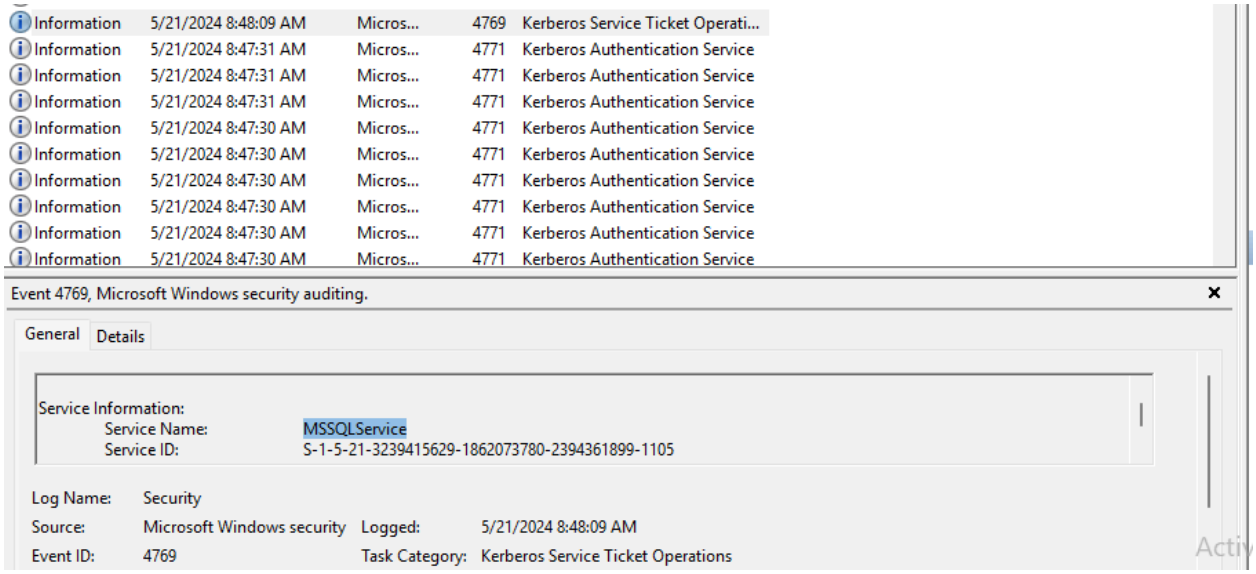


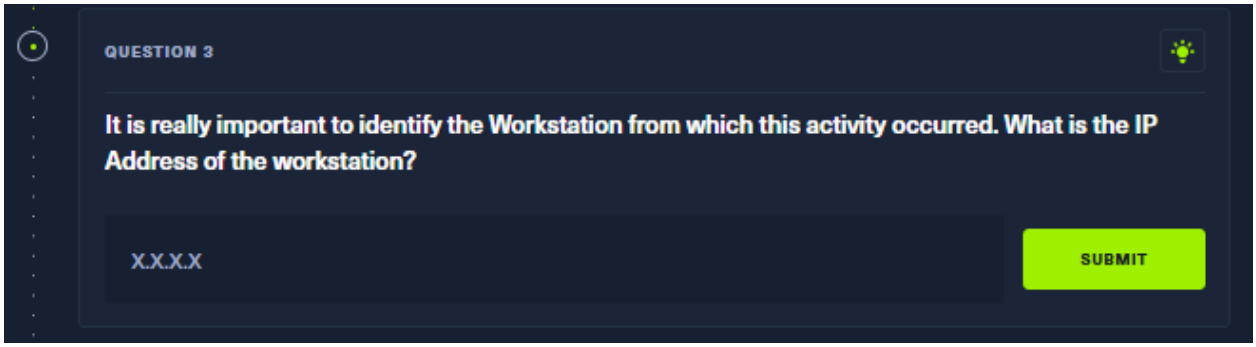
Sol:

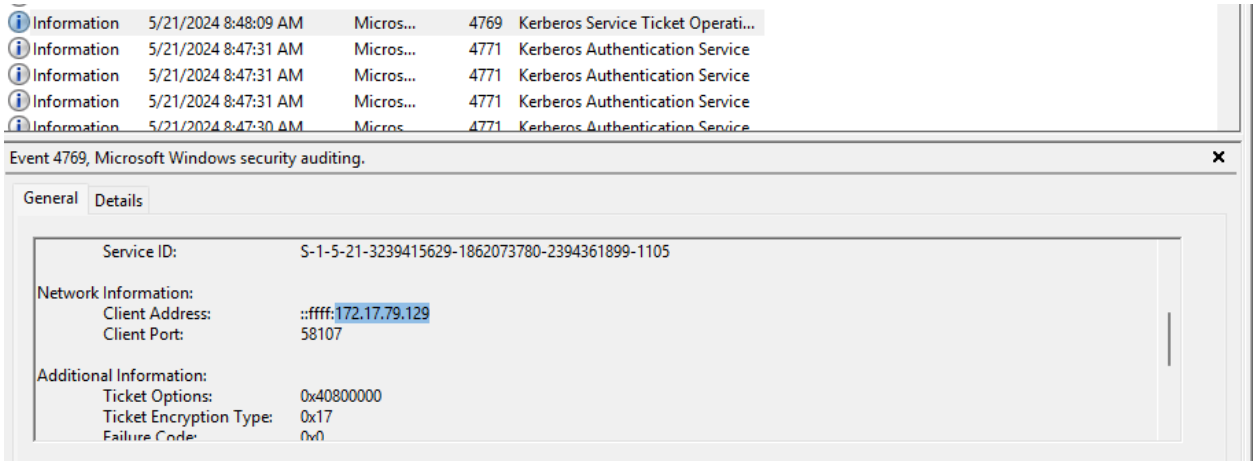


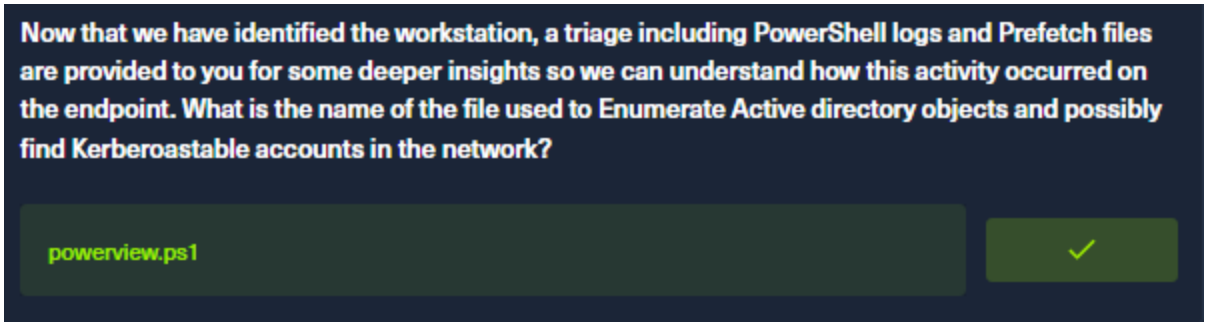


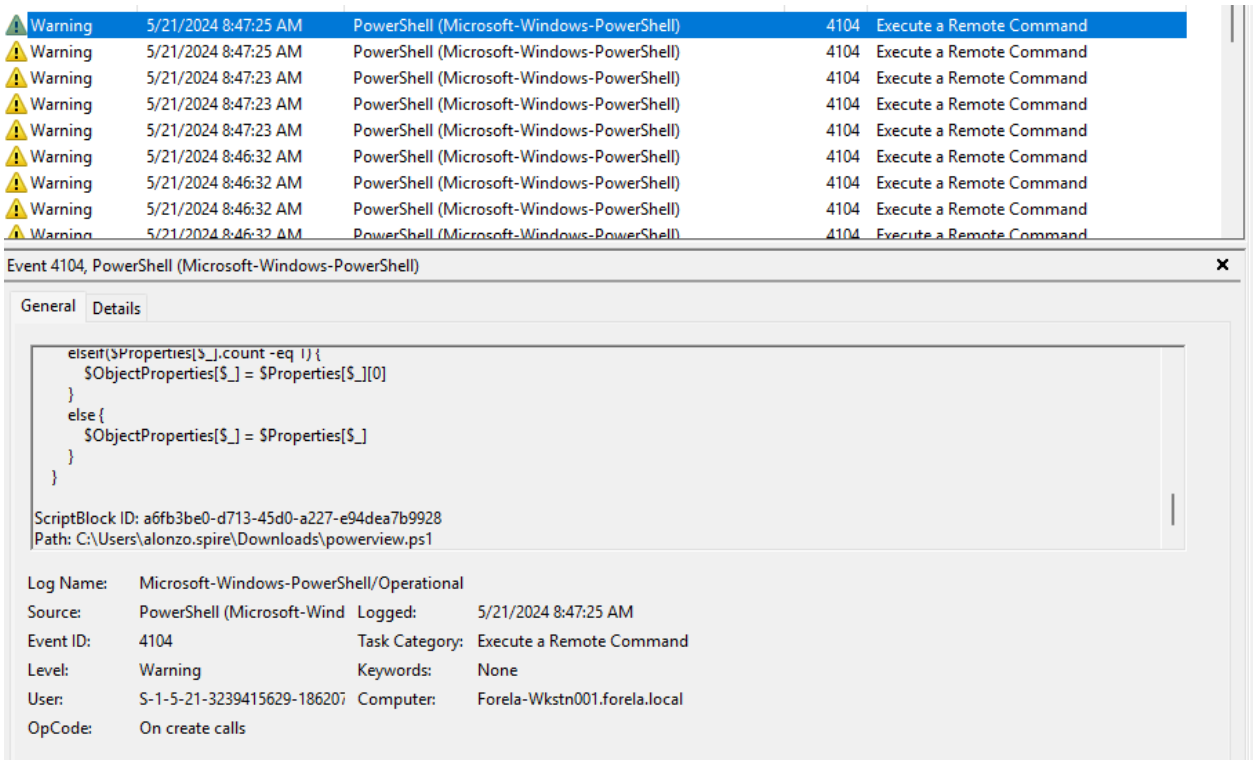
Sol:
MSSQLService

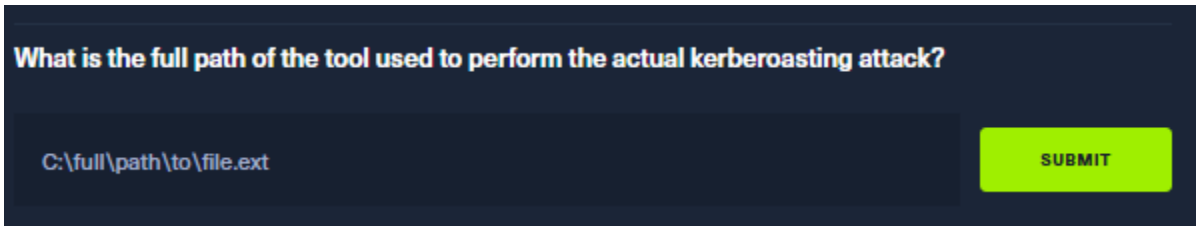

Information 5/21/2024 8:48:09 AM Micros... 4769 Kerberos Service Ticket Operati...
Information 5/21/2024 8:47:31 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:31 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:31 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:30 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:30 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:30 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:30 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:30 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:30 AM Micros... 4771 Kerberos Authentication Service
Event 4769, Microsoft Windows security auditing.
General Details
Service Information:
Service Name: MSSQLService
Service ID: S-1-5-21-3239415629-1862073780-2394361899-1105
Log Name: Security
Source: Microsoft Windows security Logged: 5/21/2024 8:48:09 AM
Event ID: 4769 Task Category: Kerberos Service Ticket Operations


QUESTION 3
It is really important to identify the Workstation from which this activity occurred. What is the IP Address of the workstation?
X.X.X.X
SUBMIT


Information 5/21/2024 8:48:09 AM Micros... 4769 Kerberos Service Ticket Operati...
Information 5/21/2024 8:47:31 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:31 AM Micros... 4771 Kerberos Authentication Service
Information 5/21/2024 8:47:31 AM Micros... 4771 Kerberos Authentication Service
Event 4769, Microsoft Windows security auditing.
General Details
Service ID: S-1-5-21-3239415629-1862073780-2394361899-1105
Network Information:
Client Address: ::ffff:172.17.79.129
Client Port: 58107
Additional Information:
Ticket Options: 0x40800000
Ticket Encryption Type: 0x17

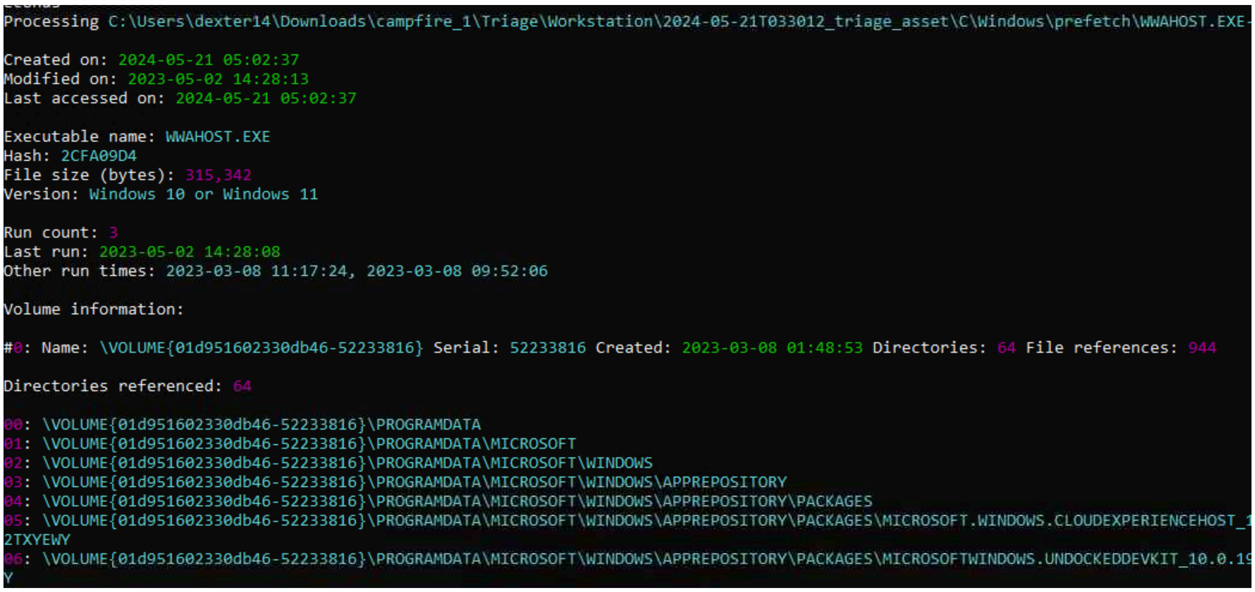


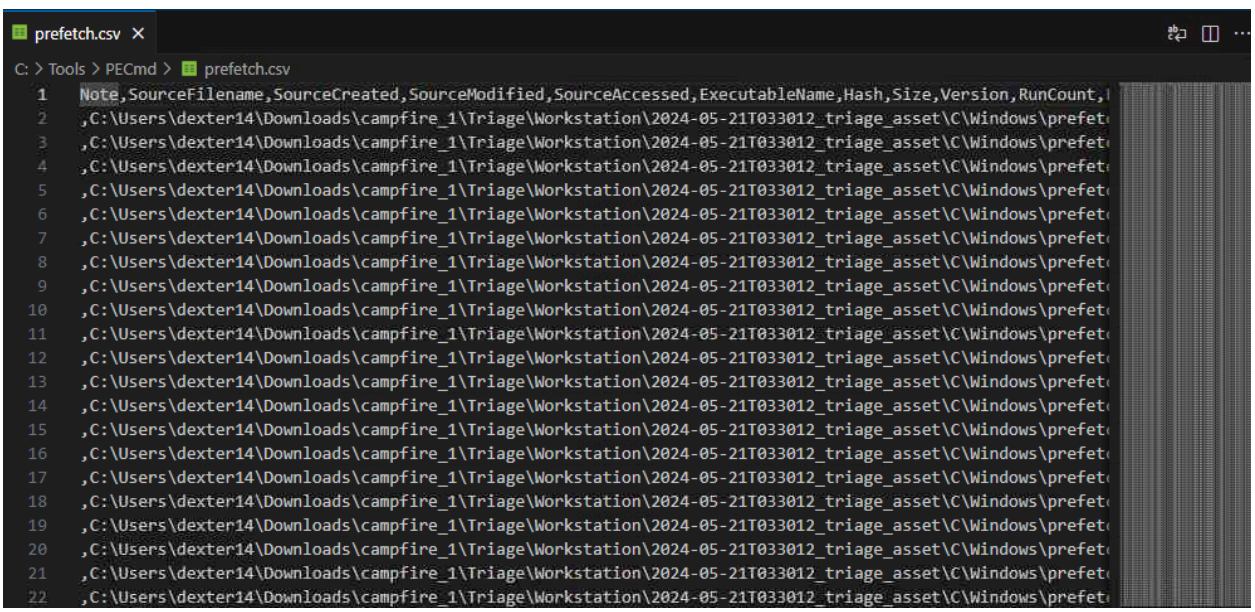


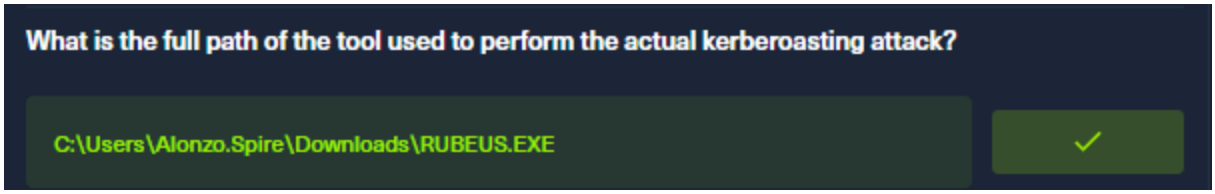


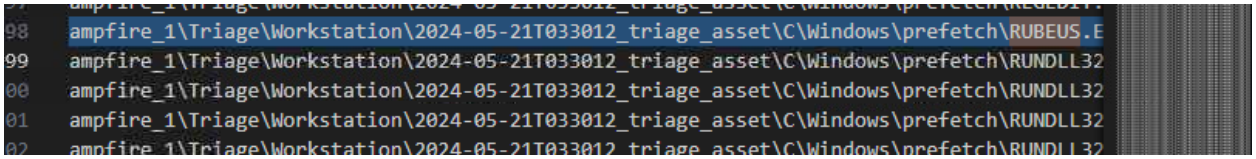
There are several tool that can be used to perform kerberoasting like impacket, Rubeus, PowerSploit (Invoke-Kerberoast) but when we given with prefetch mean its 90% Rubeus since impacket was written

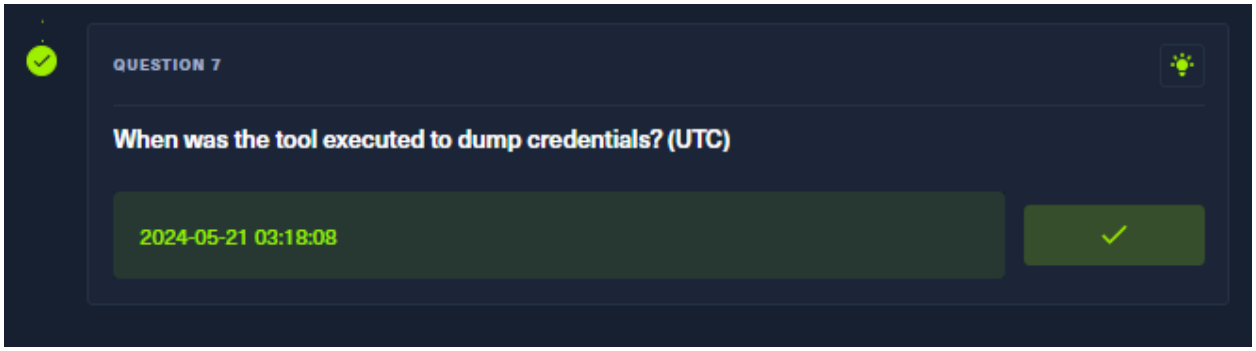
in python and PowerSploit is powershell script and to confirm this we will use `PECmd.exe -d prefetch --csv . --csvf prefetch.csv` to parse prefetch files, process them and output it in csv format











`RUBEUS.EXE-5873E24B.pf`

Key Learning:

🔑 Key Learnings – Campfire-1 (Kerberoasting Investigation)

1️⃣ Prefetch is critical for proving execution

> Domain Controller Security logs (Event ID 4769) indicate Kerberos service ticket activity, but they do not prove which tool was executed on the endpoint. Prefetch artifacts provide definitive evidence of **actual binary execution**, including execution timestamps and run count.

2️⃣ Correlation of multiple artifacts is essential

Kerberoasting detection requires correlating **DC Kerberos logs**, **PowerShell operational logs**, and **endpoint Prefetch artifacts**. No single log source provides the full picture on its own.

3️⃣ Single execution is enough to leave evidence

Even a **single execution** of an attacker tool (e.g., Rubeus.exe) generates a Prefetch file, making Prefetch a reliable artifact for detecting one-time post-exploitation activity.

4️⃣ Prefetch timestamps help confirm attack timing

Prefetch last-execution timestamps can be aligned with Kerberos TGS request spikes to accurately determine **when Kerberoasting occurred**, even if command-line arguments are not available.

5️⃣ Command-line arguments are not always recoverable

Prefetch artifacts do not store full command-line arguments. Analysts must infer attacker intent through **behavioral correlation** rather than relying solely on direct command reconstruction.

6️⃣ Security logs show impact, not cause

Windows Security logs show the **effect** of Kerberoasting (ticket requests), while Prefetch artifacts reveal the **cause** (tool execution), reinforcing the need for endpoint-level forensic analysis.