Campfire-2,evtx(EvtxECmd、Timeline Explorer)

```
Sherlock Scenario
Our SOC team detected suspicious activity in Network Traffic, the machine
has been compromised and company information that should not have been there
has now been stolen — it's up to you to figure out what has happened and
what data has been taken.
* * *
About Campfire-2
In this Sherlock, players will go through Security logs from the Domain
controller. We will work through what to look for to properly identify ASREP
Roasting attack activity and to avoid false positives due to the complexity
of Active Directory.
```

文件：Security.evtx
使用工具：EvtxECmd、Timeline Explorer

工具參考：

- https://ericzimmerman.github.io/#!index.md
- https://github.com/EricZimmerman/evtx

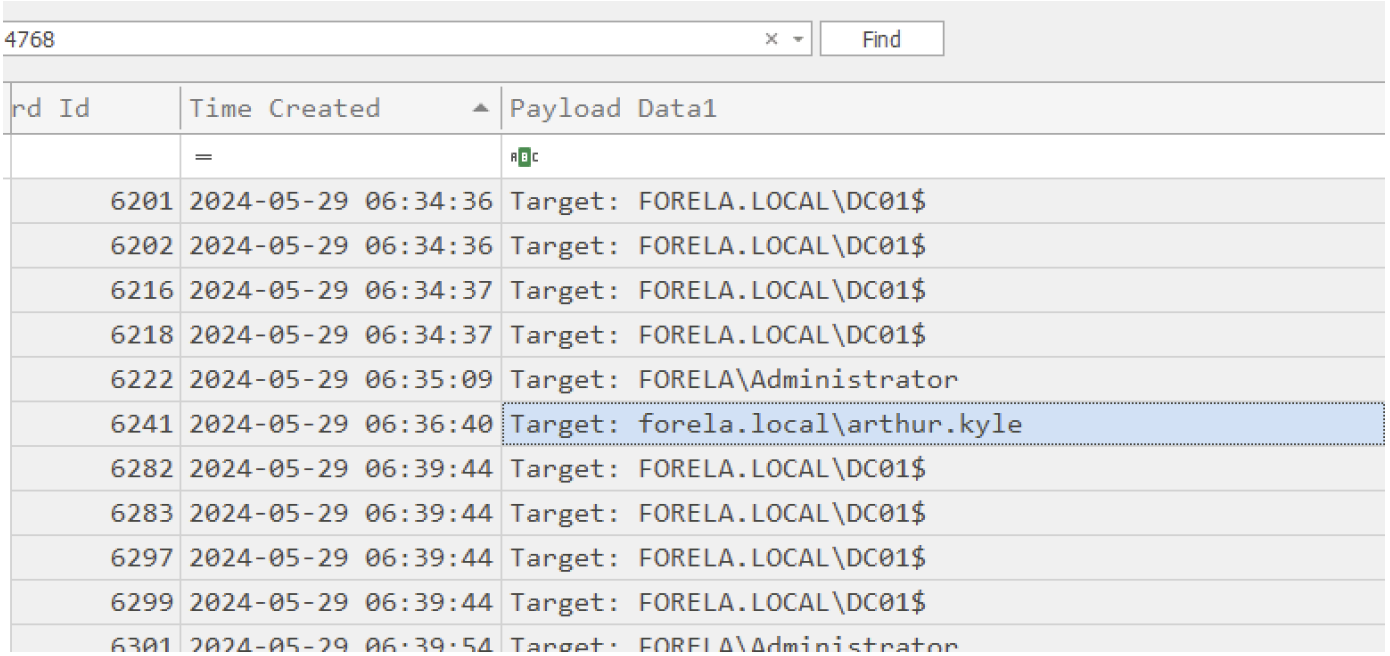
指令：

```
EvtxECmd.exe -f "C:\Users\TSO\Downloads\Security.evtx" --csv
"C:\Users\TSO\Downloads\LOG" --csvf Security.csv
```

Task 1

When did the ASREP Roasting attack occur, and when did the attacker request the Kerberos ticket for the vulnerable user?

event id `4768`



`2024-05-29 06:36:40`

Task 2

Please confirm the User Account that was targeted by the attacker.

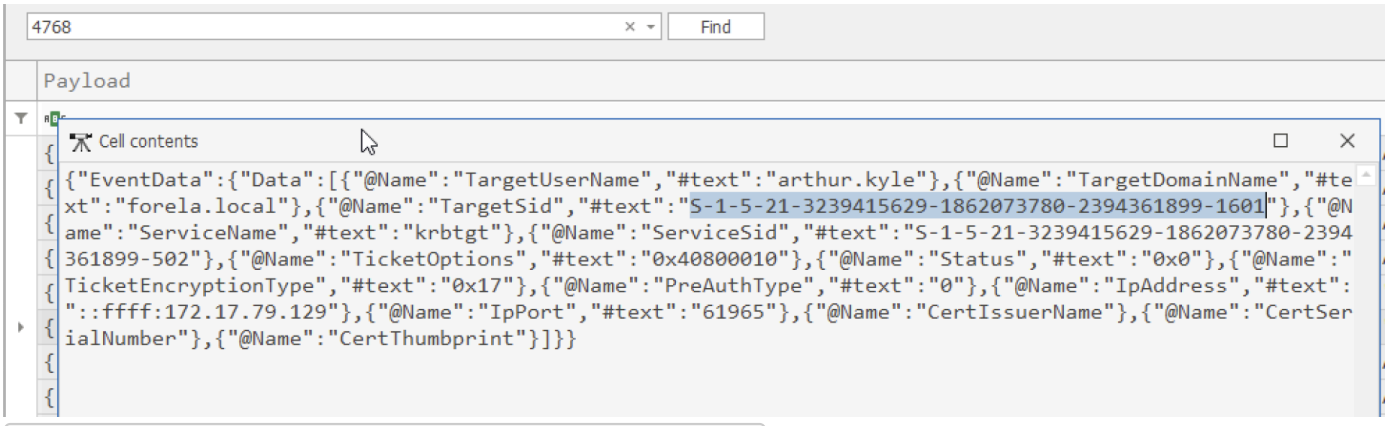
同上

`arthur.kyle`

Task 3

What was the SID of the account?

同上



`S-1-5-21-3239415629-1862073780-2394361899-1601`

Task 4

It is crucial to identify the compromised user account and the workstation responsible for this attack. Please list the internal IP address of the compromised asset to assist our threat-hunting team.

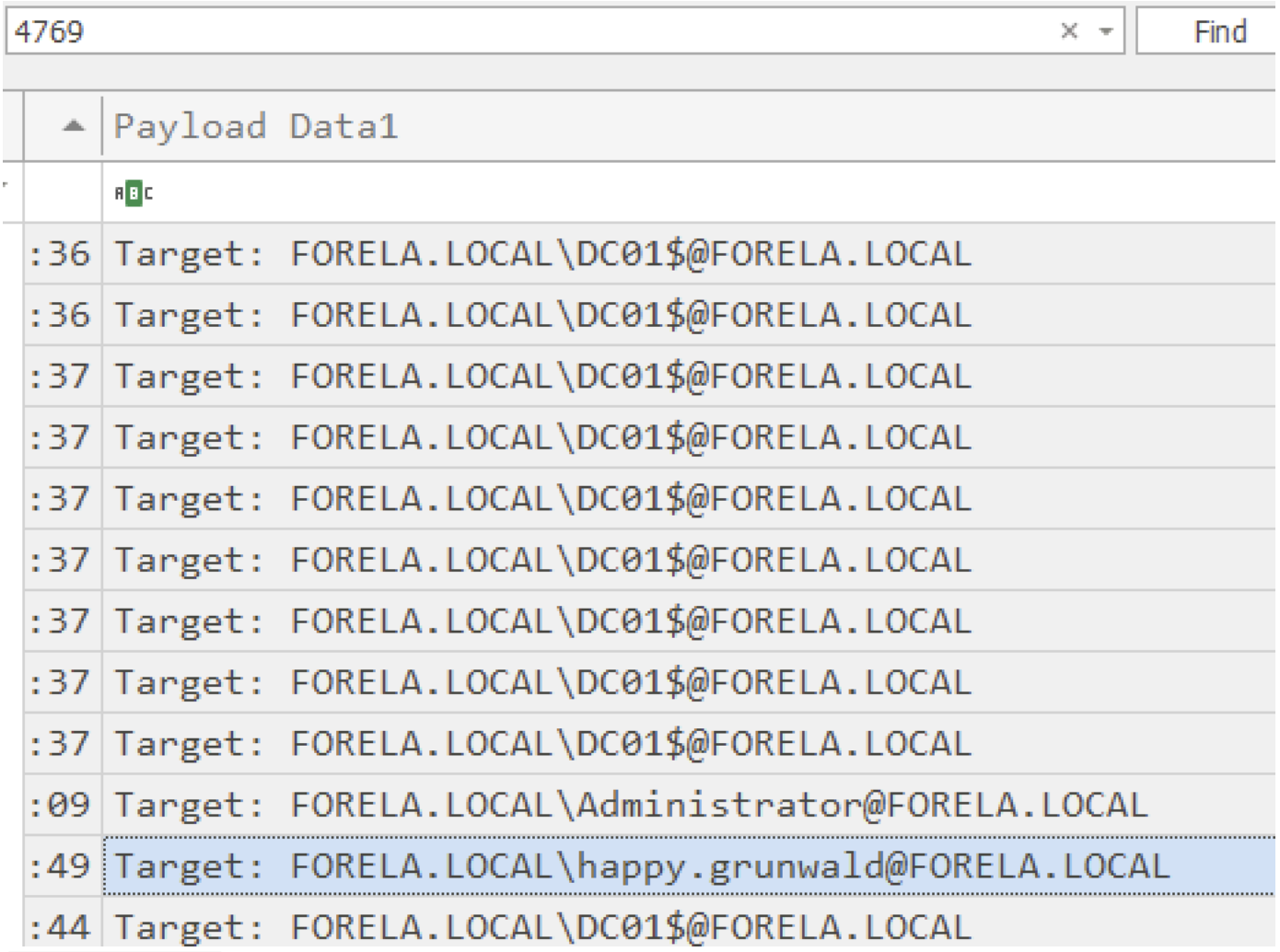
同上

`172.17.79.129`

Task 5

We do not have any artifacts from the source machine yet. Using the same DC Security logs, can you confirm the user account used to perform the ASREP Roasting attack so we can contain the compromised account/s?

event id 改為4769



`happy.grunwald`