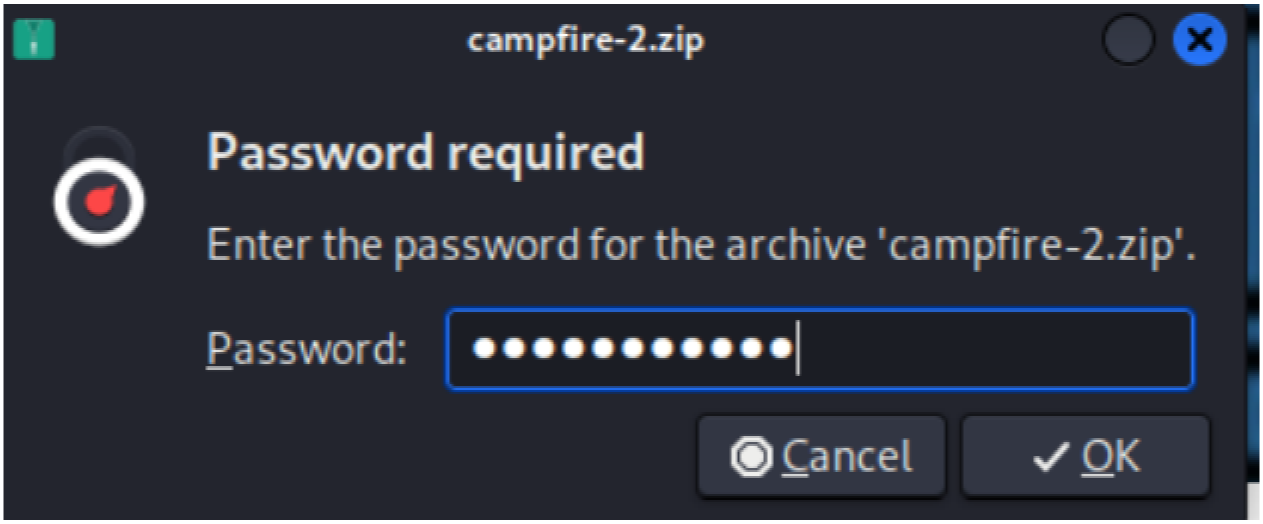
https://app.hackthebox.com/sherlocks/campfire-2/play

Forela's Network is constantly under attack. The security system raised an alert about an old admin account requesting a ticket from KDC on a domain controller. Inventory shows that this user account is not used as of now so you are tasked to take a look at this. This may be an AsREP roasting attack as anyone can request any user's ticket which has preauthentication disabled.

First things first, let's download the zip from Hack the Box onto my Kali Virtual Machine.

campfire-2.zip
24 KB

Next, we need to unzip the files using the password provided by HTB.



campfire-2.zip

Password required

Enter the password for the archive 'campfire-2.zip'.

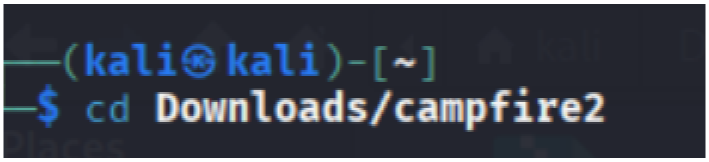
Password: ●●●●●●●●●●●

Inside the zip there's a Windows event log file.

Security.evtx

To analyze this, I'll be using Chainsaw to parse through this file. Chainsaw is an open-source tool used to quickly analyze threats in Windows artifacts.

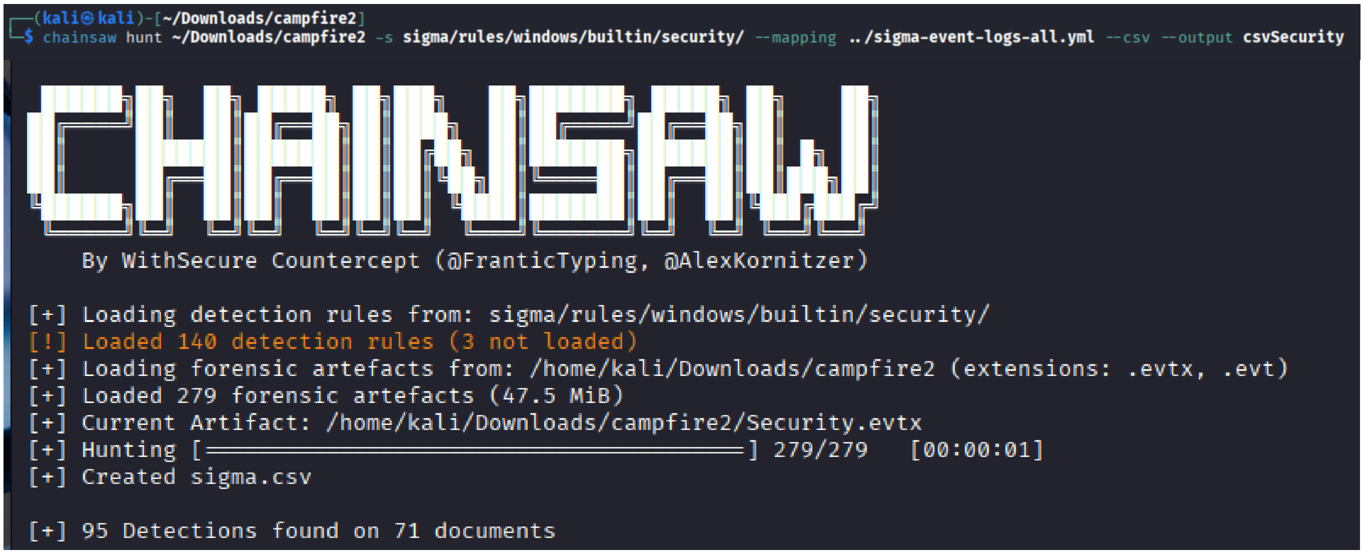
First we need to navigate to the directory where the event log is located.



```
┌──(kali㉿kali)-[~]
└─$ cd Downloads/campfire2
```

Next, let's build a chainsaw command to parse this file and output it into a csv, so we can read it.

The 'hunt' command analyzes event logs for malicious activity while referencing Sigma rules, specifically windows built in security rules. The flags specify to output to a csv file called "csvSecurity".

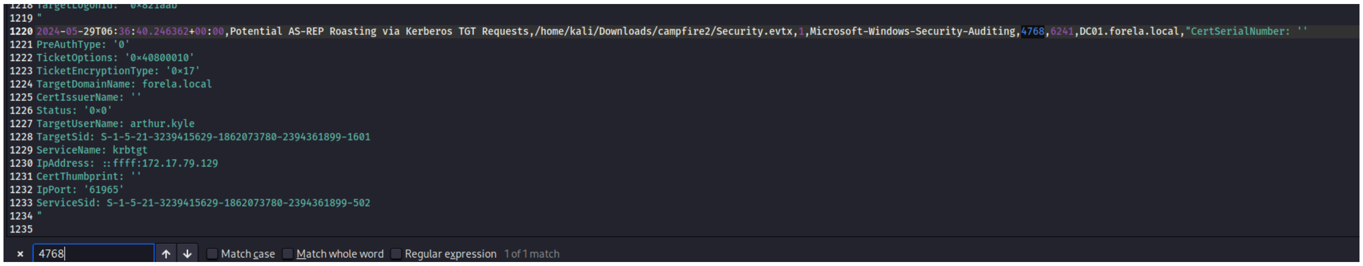


```
┌──(kali㉿kali)-[~/Downloads/campfire2]
└─$ chainsaw hunt ~/Downloads/campfire2 -s sigma/rules/windows/builtin/security/ --mapping ../sigma-event-logs-all.yml --csv --output csvSecurity
```

```
    By WithSecure Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading detection rules from: sigma/rules/windows/builtin/security/
[!] Loaded 140 detection rules (3 not loaded)
[+] Loading forensic artefacts from: /home/kali/Downloads/campfire2 (extensions: .evtx, .evt)
[+] Loaded 279 forensic artefacts (47.5 MiB)
[+] Current Artifact: /home/kali/Downloads/campfire2/Security.evtx
[+] Hunting [========================================] 279/279   [00:00:01]
[+] Created sigma.csv

[+] 95 Detections found on 71 documents
```

We can see that 95 detections were found in our event log. Let's take a look at the output.

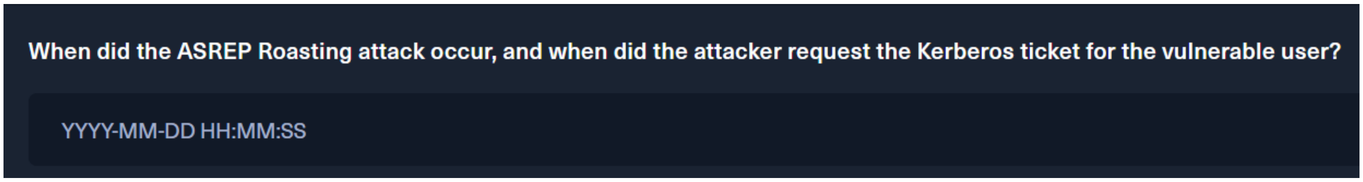
The Event ID for Kerberos authentication attempts is 4768, so I search our output for that ID, and find a potential ASREP Roasting attack.



```
TargetLogonId: '0×821aab'
"
2024-05-29T06:36:40.246362+00:00,Potential AS-REP Roasting via Kerberos TGT Requests,/home/kali/Downloads/campfire2/Security.evtx,1,Microsoft-Windows-Security-Auditing,4768,6241,DC01.forela.local,"CertSerialNumber: ''
PreAuthType: '0'
TicketOptions: '0×40800010'
TicketEncryptionType: '0×17'
TargetDomainName: forela.local
CertIssuerName: ''
Status: '0×0'
TargetUserName: arthur.kyle
TargetSid: S-1-5-21-3239415629-1862073780-2394361899-1601
ServiceName: krbtgt
IpAddress: ::ffff:172.17.79.129
CertThumbprint: ''
IpPort: '61965'
ServiceSid: S-1-5-21-3239415629-1862073780-2394361899-502
"
```

× 4768 ↑ ↓ □ Match case □ Match whole word □ Regular expression 1 of 1 match

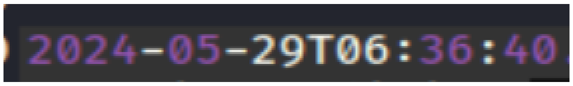
Let's see if we can answer the first question.



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

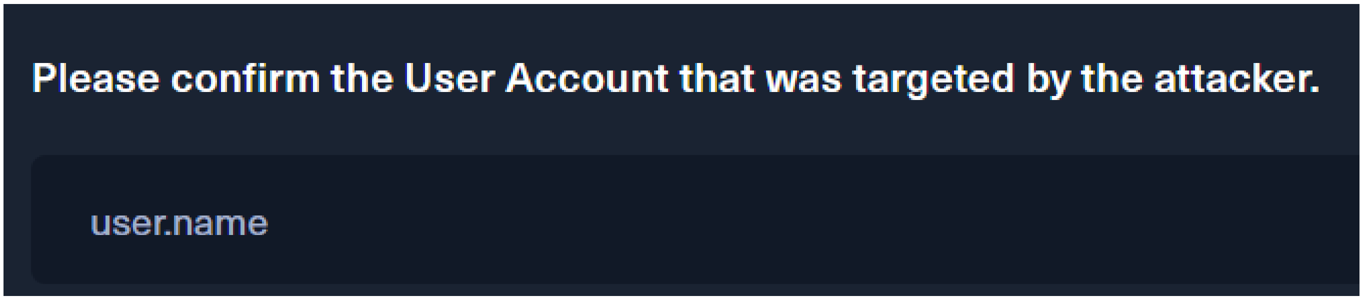
YYYY-MM-DD HH:MM:SS

At the beginning of this event, we can see the date, and the time is specified after 'T'.



```
2024-05-29T06:36:40
```

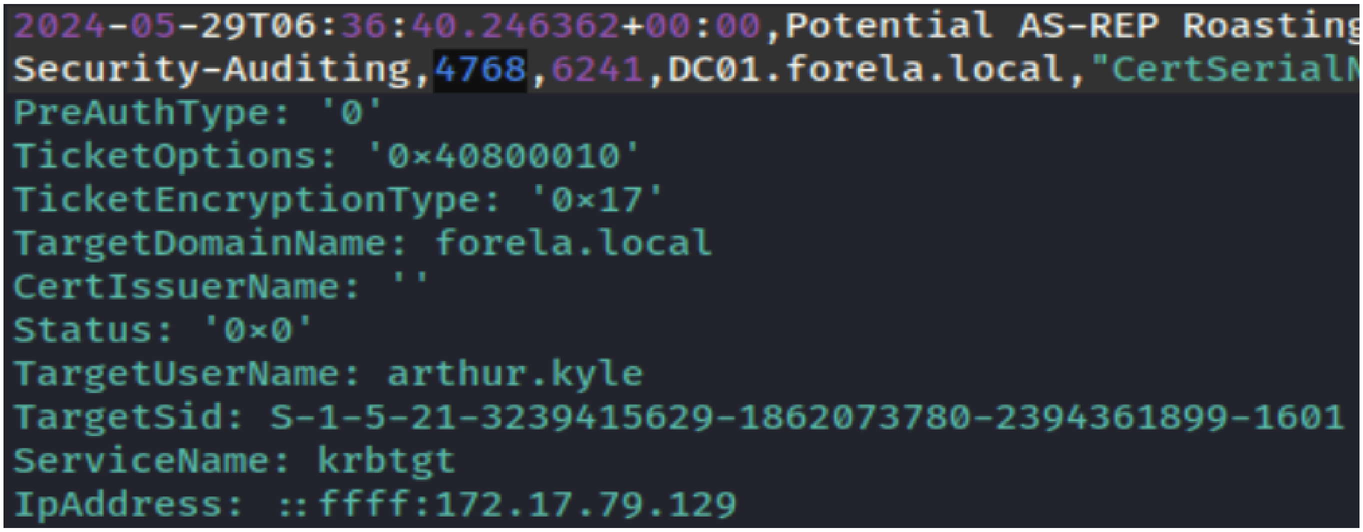
So, the attack occurred on 2024-05-29 at 06:36:40.



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

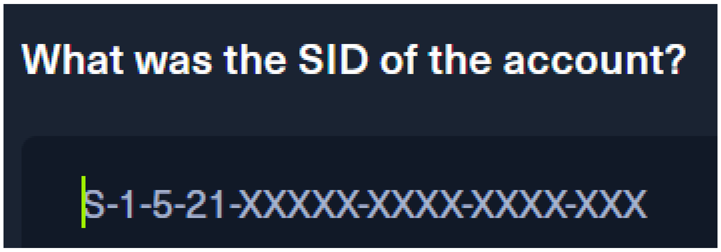
user.name

Let's look back at our chainsaw output. Below the attack event we can see more details, including "TargetUserName".



```
2024-05-29T06:36:40.246362+00:00,Potential AS-REP Roasting
Security-Auditing,4768,6241,DC01.forela.local,"CertSerialN
PreAuthType: '0'
TicketOptions: '0x40800010'
TicketEncryptionType: '0x17'
TargetDomainName: forela.local
CertIssuerName: ''
Status: '0x0'
TargetUserName: arthur.kyle
TargetSid: S-1-5-21-3239415629-1862073780-2394361899-1601
ServiceName: krbtgt
IpAddress: ::ffff:172.17.79.129
```

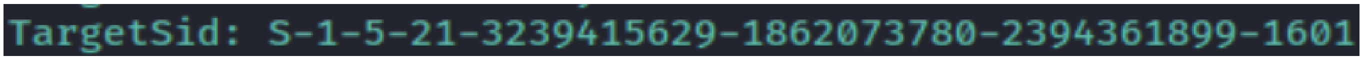
The targeted user in this case is "arthur.kyle".



What was the SID of the account?

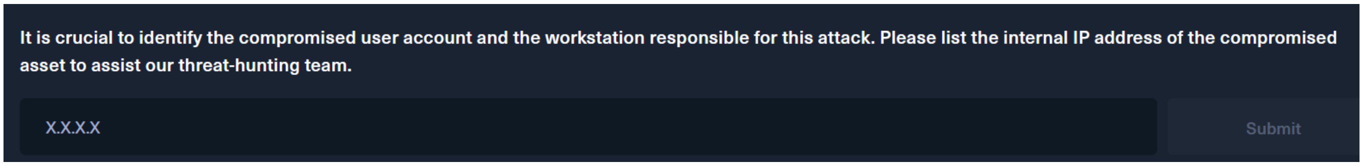
S-1-5-21-XXXXX-XXXX-XXXX-XXX

Directly below the TargetUserName we can find the TargetSid:



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

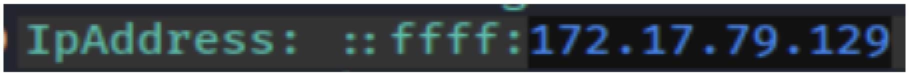
The SID of the account is S-1-5-21-3239415629-1862073780-2394361899-1601.



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.

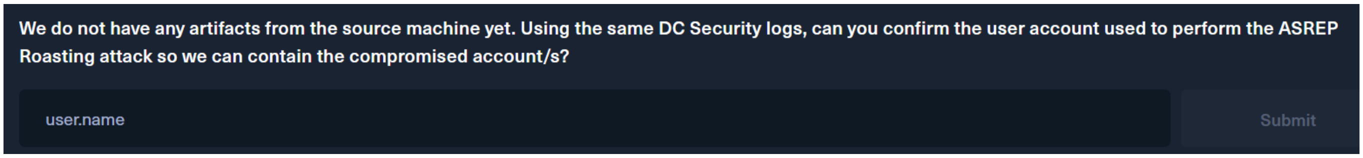
X.X.X.X

Again, we can find the desired information below the attack event, under IpAddress.



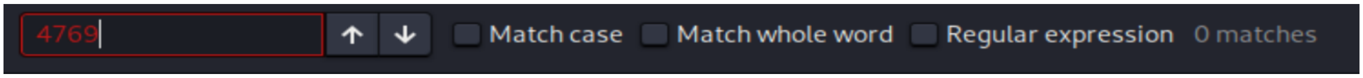
```
IpAddress: ::ffff:172.17.79.129
```

The IP address has a 'ffff:' prefix attached (to represent IPV4 addresses within IPV6 space). Hack The Box is only asking for the IPV4 address here. That address is 172.17.79.129.


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?

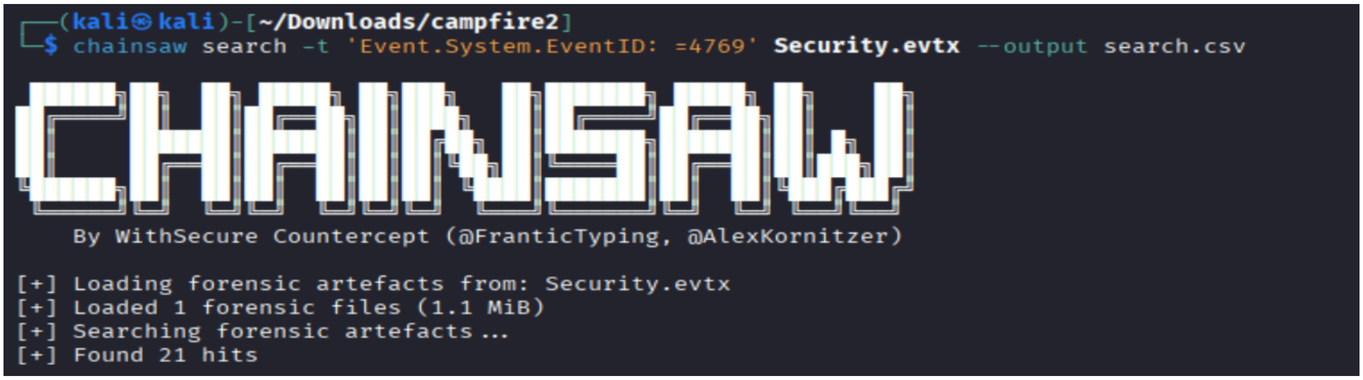
To track down the compromised account, let's first look at the sherlock description. "*The security system raised an alert about an old admin account requesting a ticket from KDC on a domain controller*".

The Event ID for requesting a Kerberos service ticket is 4769. So, let's ctrl+f and look for 4769.

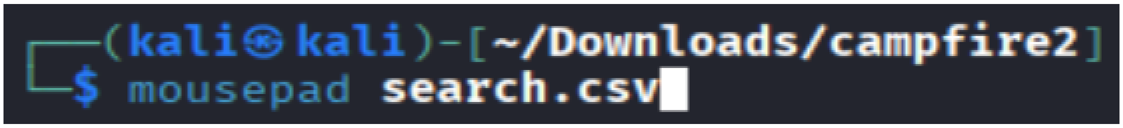

4769
↑ ↓
□ Match case □ Match whole word □ Regular expression 0 matches

No matches. In that case, let's go back to chainsaw and hunt the Event log again, this time looking specifically for Kerberos service tickets.

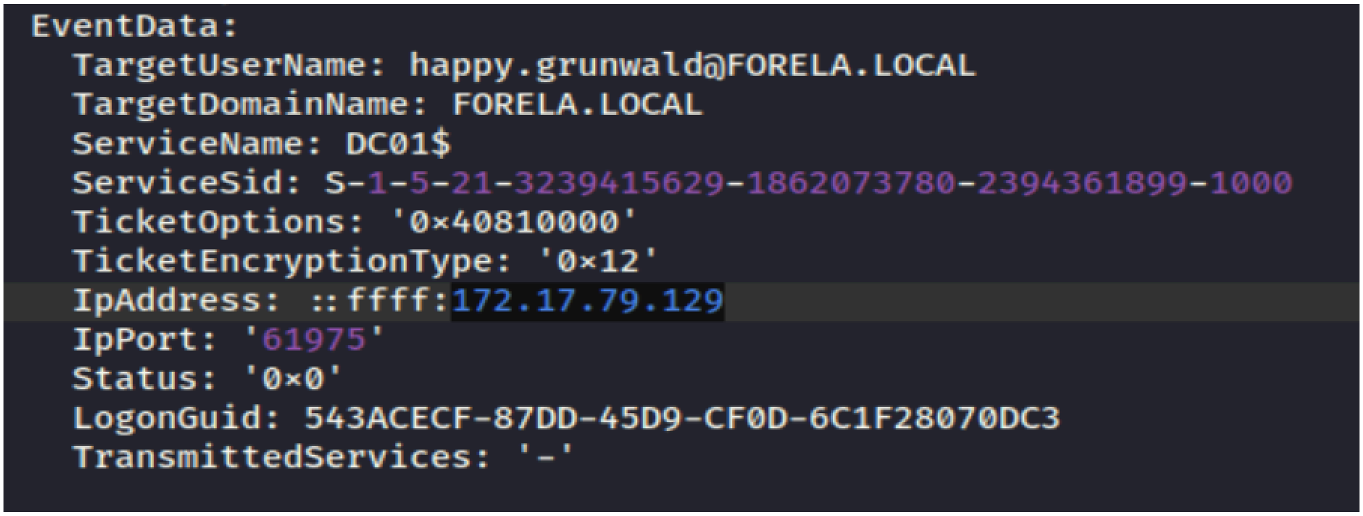
We'll search the event log file specifically for events with the ID 4769, and output to a csv file.


```
┌──(kali㉿kali)-[~/Downloads/campfire2]
└─$ chainsaw search -t 'Event.System.EventID: =4769' Security.evtx --output search.csv

 CHAINSAW

    By WithSecure Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading forensic artefacts from: Security.evtx
[+] Loaded 1 forensic files (1.1 MiB)
[+] Searching forensic artefacts ...
[+] Found 21 hits
```

Let's open the output file in mousepad.


```
┌──(kali㉿kali)-[~/Downloads/campfire2]
└─$ mousepad search.csv
```

We can see multiple Kerberos service ticket requests in the output file. However, we are only looking for Kerberos service ticket requests that came from the attacker's IP address. So, we ctrl+f the output file for the IP address we found earlier.



```
EventData:
  TargetUserName: happy.grunwald@FORELA.LOCAL
  TargetDomainName: FORELA.LOCAL
  ServiceName: DC01$
  ServiceSid: S-1-5-21-3239415629-1862073780-2394361899-1000
  TicketOptions: '0x40810000'
  TicketEncryptionType: '0x12'
  IpAddress: ::ffff:172.17.79.129
  IpPort: '61975'
  Status: '0x0'
  LogonGuid: 543ACECF-87DD-45D9-CF0D-6C1F28070DC3
  TransmittedServices: '-'
```

We've got a hit! It looks like the attacker used the user account happy.grunwald to perform the AS-REP attack.

Conclusion:

After finishing this lab writeup, I saw a lot of other writeups manually searching through the event logs to find the information we needed. This was a great lab to show how tools like Chainsaw can cut down on the manual searching and make our job much easier (and quicker).