



# HACKTHEBOX

## CampFire-2 Writeup

---



Prepared by: Cyberjunkie & Sebh24

Machine Author(s): CyberJunkie

Difficulty: **Very Easy**

## Scenario

---

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.

## Artefacts provided

1- CampFire2.zip , sha1 : C3C701AA1E4A8A95108710300EA8C80E18963754

## Skills Learnt

- Active Directory Attacks Analysis
- Timeline creation
- AS-REP Roast attack Analysis
- Windows Event log analysis

- Windows Forensics
- Chaining of multiple Artefacts

## Initial Analysis :

---

Lets start by validating the hash of the artifacts.

```
PS H:\Project-Sherlock\Camp Fire 2> get-filehash -algorithm sha1 '.\Camp Fire 2.zip'
```

Algorithm	Hash	Path
SHA1	C3C701AA1E4A8A95108710300EA8C80E18963754	H:\Project-Sherlock\Camp Fire...

We are provided with a security event log file acquired from an infected Domain Controller (DC). We will use Event Viewer to go through the logs in the writeup, but feel free to use any SIEM or tools like EvtxEcmd.

### What is a SIEM?

**SIEM** stands for **Security Information and Event Management**. It is a comprehensive solution that combines **Security Information Management (SIM)** and **Security Event Management (SEM)**. SIEM systems provide real-time analysis of security alerts generated by applications and network hardware.

### What is EvtxEcmd?

**EvtxEcmd** is a command-line tool used for parsing and analyzing Windows Event Log files, specifically those with the `.evtx` extension. Here's a brief overview of what EvtxEcmd does:

1. **Parsing EVTX Files:** EvtxEcmd reads and parses `.evtx` files, which are the event log files used by Windows to record system, security, and application logs.
2. **Custom Queries:** Allows users to perform custom queries on the event logs to filter out specific events based on criteria such as Event ID, Event Source, and Event Level.
3. **Exporting Data:** Provides functionality to export the parsed data into various formats such as CSV, XML, or JSON for further analysis or reporting.
4. **Scripting:** As a command-line tool, EvtxEcmd can be used in scripts to automate the process of event log analysis, making it useful for batch processing and large-scale log analysis.
5. **Event Details:** Extracts detailed information from each event, including timestamps, event data, user information, and more.

Since this is a beginner-friendly investigation, we only see a few events. In a real case, there can be thousands or millions of events as a domain controller gets quite busy.

The screenshot shows the Windows Event Viewer interface. The top pane displays a list of security events. The bottom pane shows the details for Event 4702, 'Microsoft Windows security auditing'.

Level	Date and Time	Source	Event ID	Task Category
Information	5/29/2024 11:41:14 AM	Microsoft Windows security auditing	4702	Other Object Access Events
Information	5/29/2024 11:40:30 AM	Microsoft Windows security auditing	4702	Other Object Access Events
Information	5/29/2024 11:40:30 AM	Microsoft Windows security auditing	4702	Other Object Access Events
Information	5/29/2024 11:40:06 AM	Microsoft Windows security auditing	5140	File Share
Information	5/29/2024 11:39:57 AM	Microsoft Windows security auditing	5379	User Account Management
Information	5/29/2024 11:39:55 AM	Microsoft Windows security auditing	5379	User Account Management
Information	5/29/2024 11:39:55 AM	Microsoft Windows security auditing	5379	User Account Management
Information	5/29/2024 11:39:55 AM	Microsoft Windows security auditing	5379	User Account Management
Information	5/29/2024 11:39:55 AM	Microsoft Windows security auditing	5379	User Account Management

**Event 4702, Microsoft Windows security auditing.**

**General Details**

A scheduled task was updated.

**Subject:**

- Security ID: SYSTEM
- Account Name: DC015
- Account Domain: FORELA
- Logon ID: 0x3E7

**Task Information:**

- Task Name: \Microsoft\Windows\Application Experience\PcaPatchDbTask
- Task New Content: <?xml version="1.0" encoding="UTF-16"?><Task version="1.0" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"><RegistrationInfo><Source>Microsoft Corporation</Source><Author>Microsoft Corporation</Author><Version>1.0</Version><Description>Updates compatibility database</Description><URI>\Microsoft\Windows\Application Experience\PcaPatchDbTask</URI><SecurityDescriptor>D:(A;;GA;;;BA)(A;;GA;;;SY)(A;;FRFX;;;LS)</SecurityDescriptor></RegistrationInfo><Triggers><TimeTrigger><Repetition><Interval>PT12H</Interval><StopAtDurationEnd>false</StopAtDurationEnd></Repetition><StartBoundary>2008-09-01T03:00:00</StartBoundary></TimeTrigger></Triggers></Task></xml>

**Log Name:** Security  
**Source:** Microsoft Windows security  
**Event ID:** 4702  
**Level:** Information  
**User:** N/A  
**Task Category:** Other Object Access Events  
**Keywords:** Audit Success  
**Computer:** DC01.forela.local

## AS-REP Roasting :

ASREPRoast is a security attack that exploits users who lack the Kerberos pre-authentication required attribute. Essentially, this vulnerability allows attackers to request authentication for a user from the Domain Controller (DC) without needing the user's password. The DC then responds with a message encrypted with the user's password-derived key, which attackers can attempt to crack offline to discover the user's password.

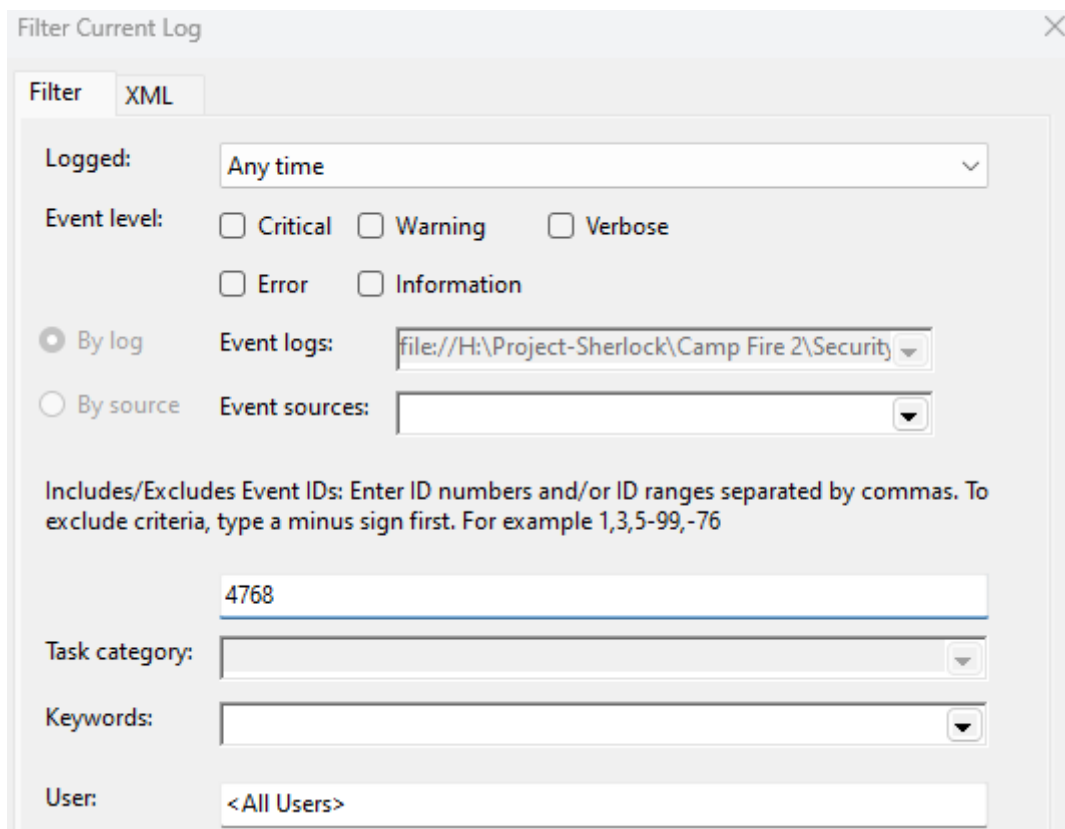
We discuss how this attack works and how to perform detection and analysis in [our blog](#) synced with this sherlock

## Analysis :

Q1 When did the ASREP Roasting attack occur and the Kerberos ticket was requested by attacker for the vulnerable user?

Hint: Filter For event ID 4768 where Pre authentication type is 0, Ticket encryption type is 0x17 and the service name is krbtgt(Service requesting the ticket on behalf of the user). The event where all these conditions are being fulfilled indicates that an attacker managed to perform ASREP roasting attack.

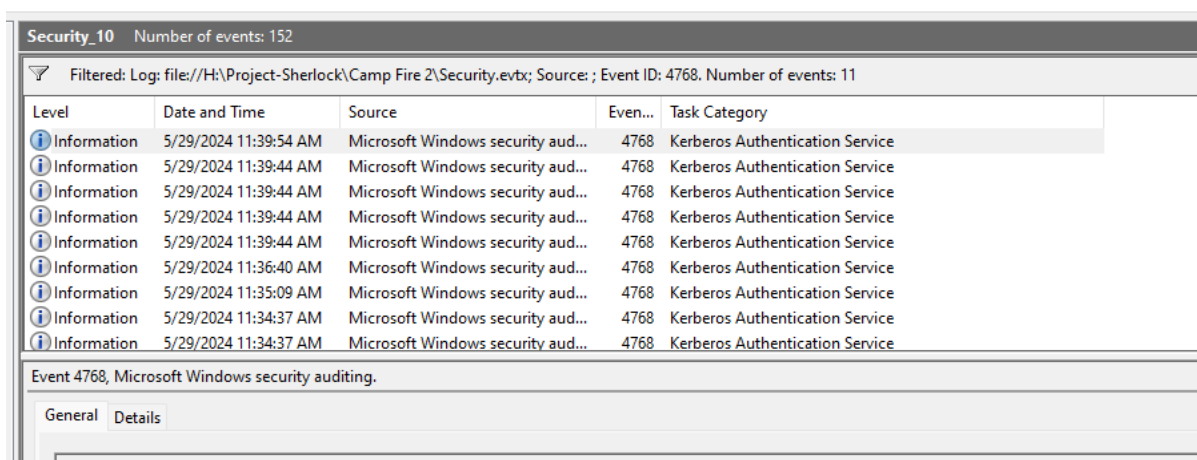
Lets start by filtering for Event ID 4768.



Filter Current Log dialog box showing filter settings:

- Filter: XML
- Logged: Any time
- Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information
- By log: Event logs: file://H:\Project-Sherlock\Camp Fire 2\Security
- By source: Event sources:
- Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
- 4768
- Task category:
- Keywords:
- User: <All Users>

We can see after filtering, we are only left with 11 events.



Security\_10 Number of events: 152

Filtered: Log: file://H:\Project-Sherlock\Camp Fire 2\Security.evtx; Source: ; Event ID: 4768. Number of events: 11

Level	Date and Time	Source	Even...	Task Category
Information	5/29/2024 11:39:54 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:39:44 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:39:44 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:39:44 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:39:44 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:36:40 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:35:09 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:34:37 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service
Information	5/29/2024 11:34:37 AM	Microsoft Windows security aud...	4768	Kerberos Authentication Service

Event 4768, Microsoft Windows security auditing.

General Details

A Kerberos authentication ticket/TGT was requested.

We can easily go through each of these events since there are only 11 events to read through. If there were considerably more events utilising a tool such as Splunk or ELK would be beneficial.

There are plenty of ways we can go over this. We will take a shortcut and search for the "0x17" keyword, which will take us to the event with this keyword.



Find dialog box showing search settings:

- Find what: 0x17
- Find Next
- Cancel

It takes us to this event:

General Details

A Kerberos authentication ticket (TGT) was requested.

## Account Information:

Account Name: arthur.kyle  
Supplied Realm Name: forela.local  
User ID: S-1-5-21-3239415629-1862073780-2394361899-1601

## Service Information:

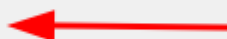
Service Name: krbtgt  
Service ID: S-1-5-21-3239415629-1862073780-2394361899-502

## Network Information:

Client Address: ::ffff:172.17.79.129  
Client Port: 61965

## Additional Information:

Ticket Options: 0x40800010  
Result Code: 0x0  
Ticket Encryption Type: 0x17  
Pre-Authentication Type: 0



## Certificate Information:

Certificate Issuer Name:  
Certificate Serial Number:  
Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-authentication.

Reading the hint, we see that all the necessary requirements indicating an AS-REP Attack are present. The ticket encryption type is 0x17 (RC4), Pre-authentication type is 0 (disabled), and the service name is krbtgt.

We can look for the UTC time in details tab of this event

Event 4768, Microsoft Windows security auditing.

General Details

☒ Friendly View ☐ XML View

- System

- Provider
  - [ Name] Microsoft-Windows-Security-Auditing
  - [ Guid] {54849625-5478-4994-a5ba-3e3b0328c30d}
  - EventID 4768
  - Version 0
  - Level 0
  - Task 14339
  - Opcode 0
  - Keywords 0x8020000000000000
- TimeCreated
  - [ SystemTime] 2024-05-29T06:36:40.2463627Z ←
  - EventRecordID 6241
  - Correlation
- Execution
  - [ ProcessID] 752
  - [ ThreadID] 3188

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

Q2 Please confirm the User Account that was targeted by the attacker.

Hint: In the same identified event, look for Account Name.

We can see this in the Account Name field:

A Kerberos authentication ticket (TGT) was requested.

Account Information:

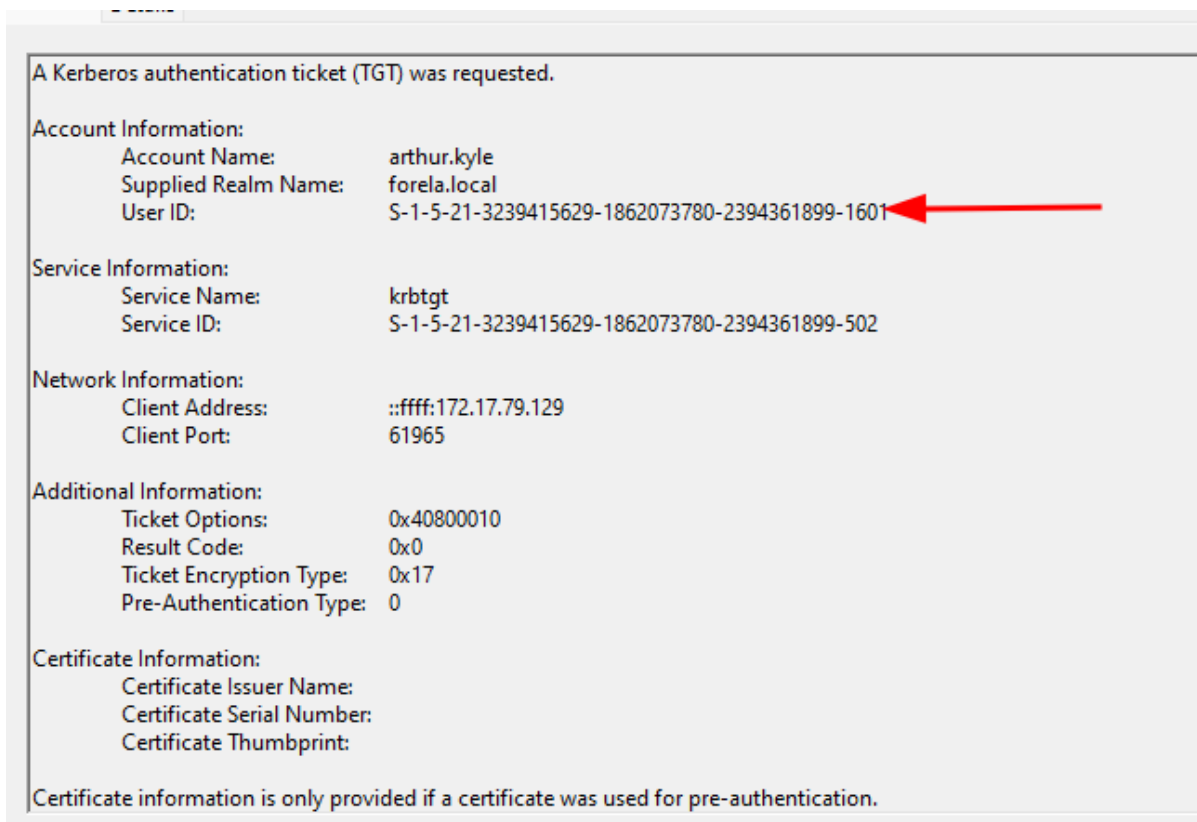
Account Name:	arthur.kyle ←
Supplied Realm Name:	forela.local
User ID:	S-1-5-21-3239415629-1862073780-2394361899-1601

Service Information:

Answer: arthur.kyle

Q3 What was the SID of the account?

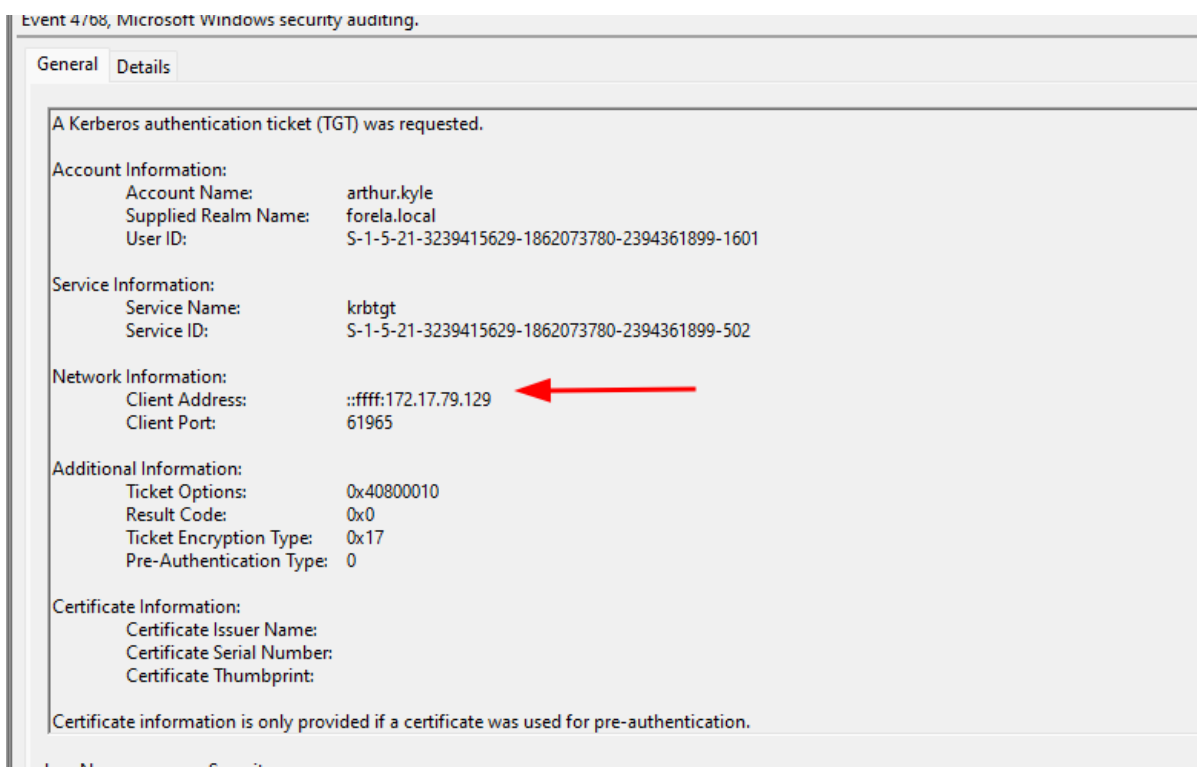
Hint: Look for "User ID" field in the same event



Answer: S-1-5-21-3239415629-1862073780-2394361899-1601

Q4 It's crucial to identify the compromised user account and the workstation that are the source of this attack. Please list down the Internal Ip Address of the compromised asset to assist our threat-hunting team.

Hint: Look for the Client Address field in the same event.



Answer: 172.17.79.129

Q5 We don't have any artifacts from the source machine yet. Utilizing the same DC Security logs, can you confirm the user account used to perform the ASREP roast attack so we can contain the compromised accounts?

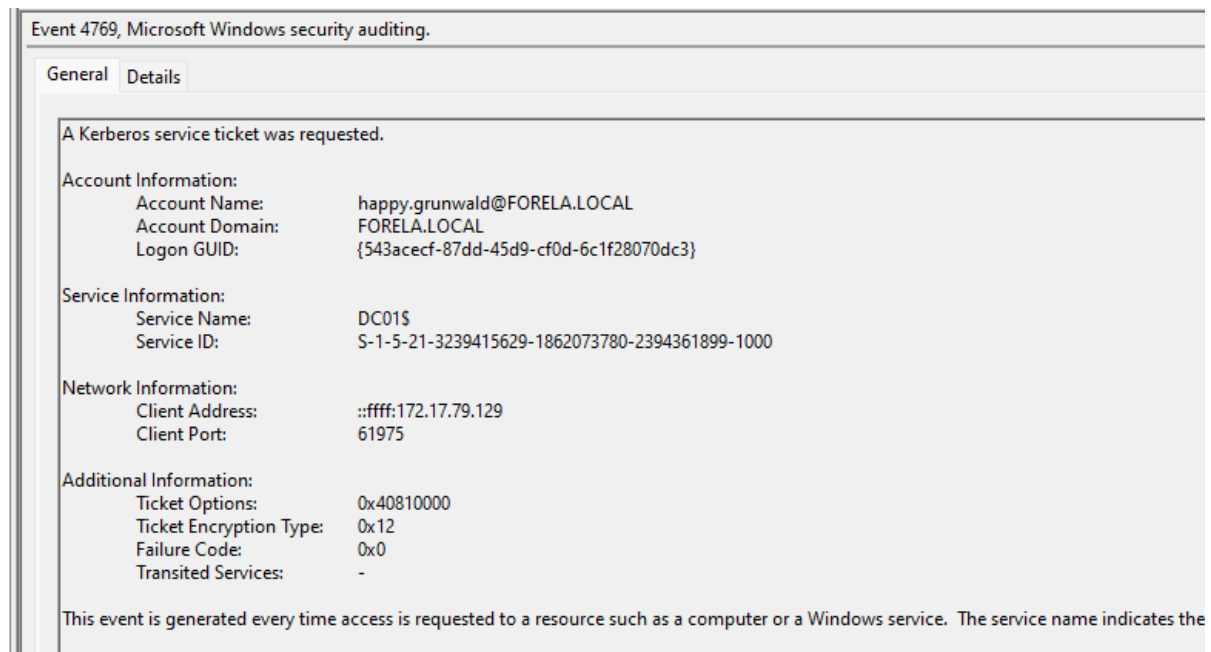
Hint: Look for the immediate next event from the event we have been analyzing so far. The event

ID would be 4769 and the event will contain the user account, and the IP address as well. The IP Address will be the same as we identified before, hence strongly indicating that the subject user account is the compromised account doing the attack.

Previous questions were all based on the identified anomalous event. Now, for this last question, we should understand the wider picture. The question asks about the user account performing this attack. It's important to note that the arthur.kyle user is the victim in this attack. This question asks for the user account that was used to exploit the arthur.kyle account. For example, it may be the case that another domain user account got compromised, and the attacker is using that account to further pivot to the account to escalate privileges and perform lateral movement.

That is exactly the case here. Looking back at the information we have so far, we have the IP address of the machine used to perform the attack. We can search for that in our logs.

We get to this event, and coincidentally, it was the next event from our identified malicious event:



Here we can see the details that the happy.grunwald account was being used on the attacking source machine. In the event, the account is requesting a service ticket from the DC, which is part of normal operations. Nothing in this event is malicious, but we do get the insights we were looking for as in normal operations of the domain environment we saw the user account being used at the suspect machine.

Answer: happy.grunwald