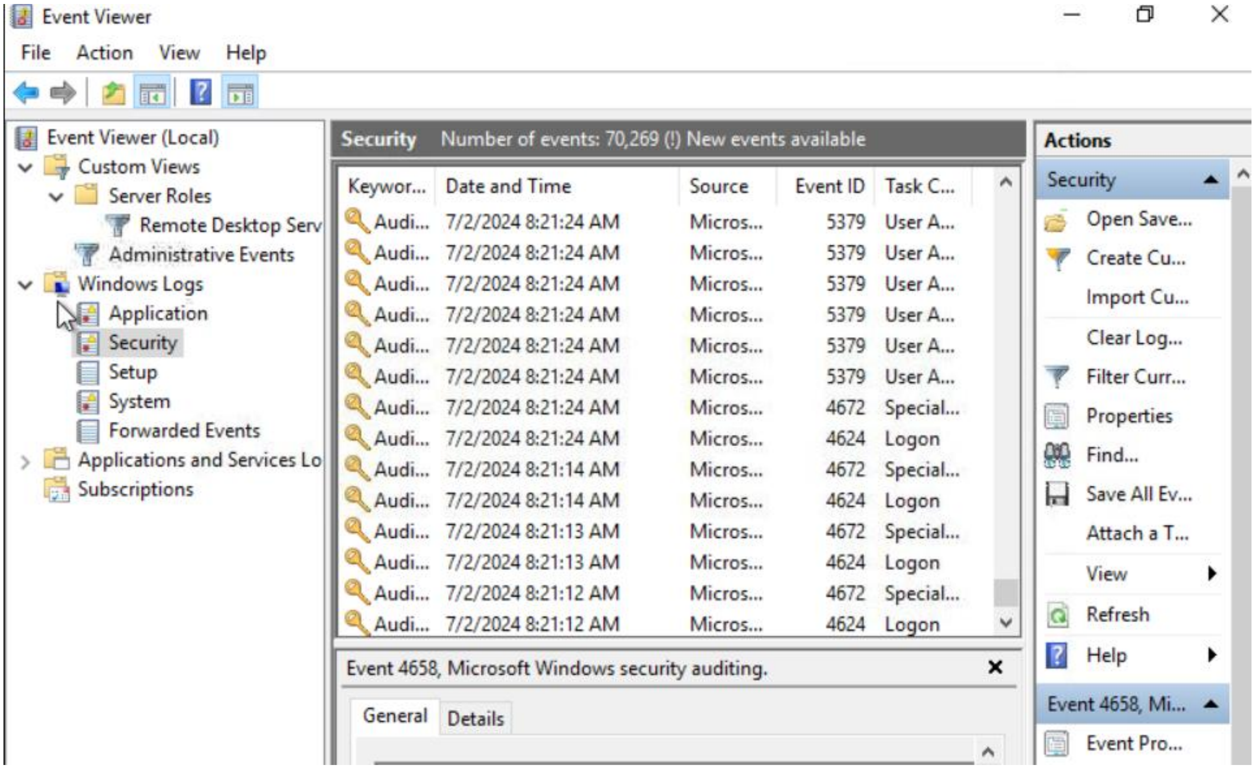
WINDOWS EVENT LOGS ANALYSIS Report 2025/12/07

> On Friday, a critical organization reported being a victim of a cyber attack. Upon investigation, critical data was exfiltrated from a file server in the organization's network. The security team was successful in determining the user name and IP address of the compromised system in the network, which had access to the file server at the time of the attack.

I was tasked to find out the activities of the attacker in this compromised system before he took access to the file server.

STEP 1: I was prompted to look for the name of last user account that was created on the system.

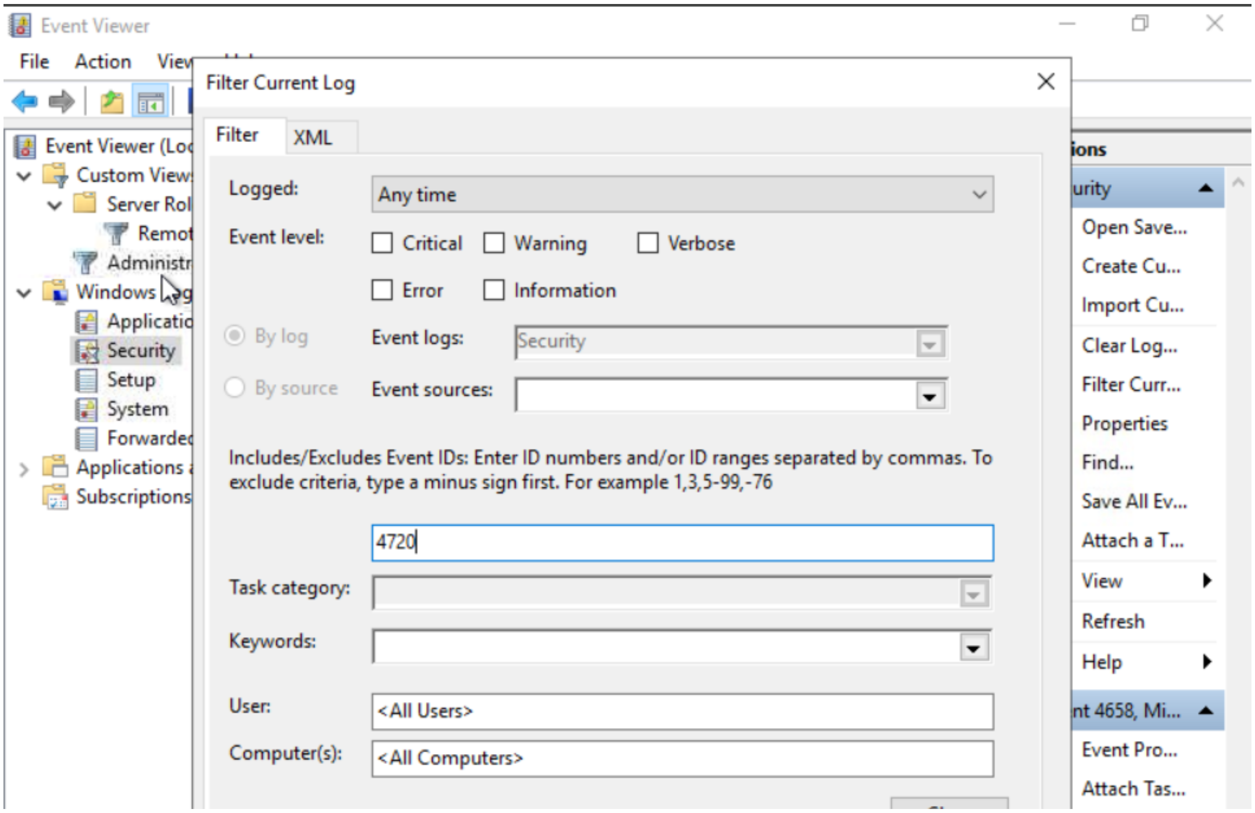


Security Number of events: 70,269 (!) New events available

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	7/2/2024 8:21:24 AM	Micros...	5379	User A...
Audi...	7/2/2024 8:21:24 AM	Micros...	5379	User A...
Audi...	7/2/2024 8:21:24 AM	Micros...	5379	User A...
Audi...	7/2/2024 8:21:24 AM	Micros...	5379	User A...
Audi...	7/2/2024 8:21:24 AM	Micros...	5379	User A...
Audi...	7/2/2024 8:21:24 AM	Micros...	5379	User A...
Audi...	7/2/2024 8:21:24 AM	Micros...	4672	Special...
Audi...	7/2/2024 8:21:24 AM	Micros...	4624	Logon
Audi...	7/2/2024 8:21:14 AM	Micros...	4672	Special...
Audi...	7/2/2024 8:21:14 AM	Micros...	4624	Logon
Audi...	7/2/2024 8:21:13 AM	Micros...	4672	Special...
Audi...	7/2/2024 8:21:13 AM	Micros...	4624	Logon
Audi...	7/2/2024 8:21:12 AM	Micros...	4672	Special...
Audi...	7/2/2024 8:21:12 AM	Micros...	4624	Logon

Event 4658, Microsoft Windows security auditing.

I opened up Event Viewer, clicked the drop down on the Windows Logs folder in the left pane, then clicked on Security to look through the Event IDs.



Filter Current Log

Filter | XML

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: 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

4720

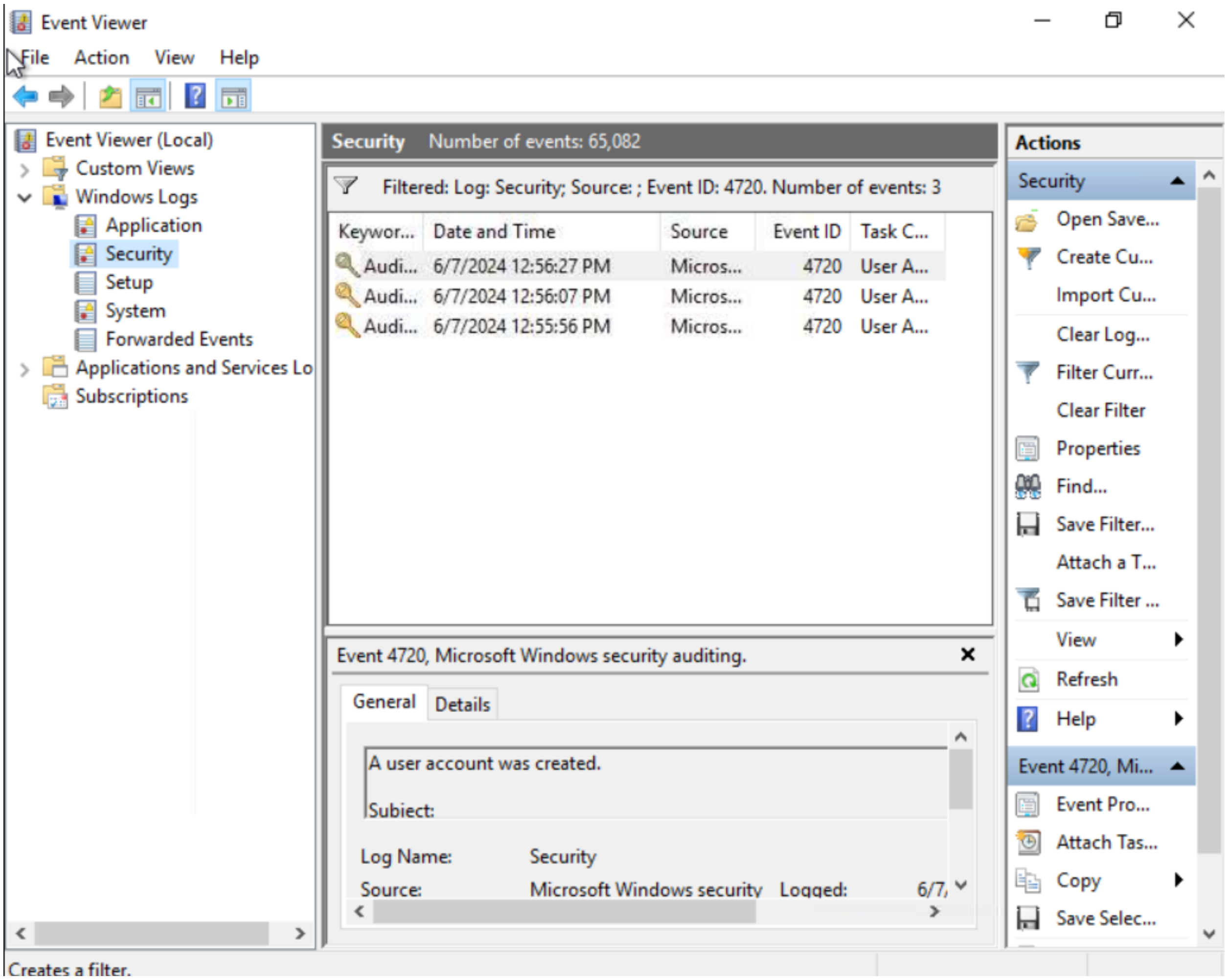
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Since there are many Events recorded, I clicked the Filter Current Log option on the right pane then proceeded to enter the exact **event ID - 4720(A user account was created)**, which would allow me to skim through the accounts created then look for the most recently created account.



Security Number of events: 65,082

Filtered: Log: Security; Source: ; Event ID: 4720. Number of events: 3

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	6/7/2024 12:56:27 PM	Micros...	4720	User A...
Audi...	6/7/2024 12:56:07 PM	Micros...	4720	User A...
Audi...	6/7/2024 12:55:56 PM	Micros...	4720	User A...

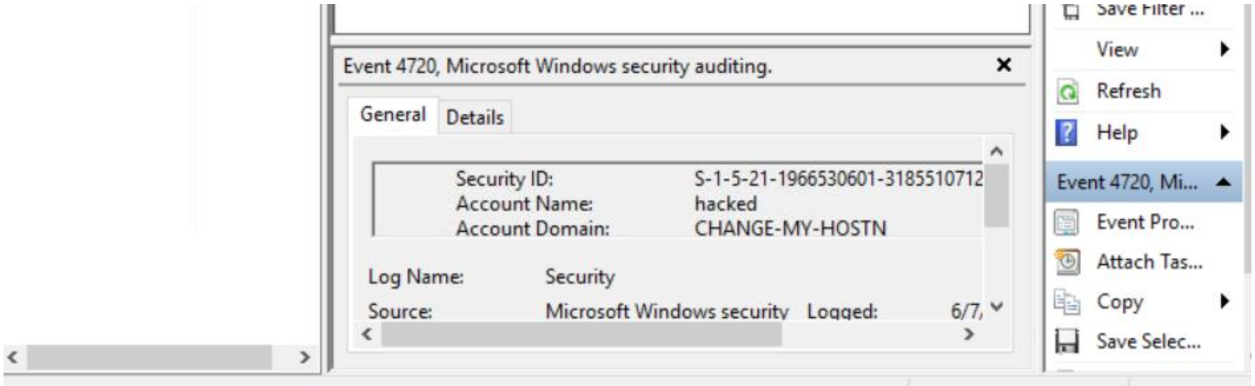
Event 4720, Microsoft Windows security auditing.

A user account was created.

Subject:

Log Name: Security
Source: Microsoft Windows security Logged: 6/7,

Three accounts appeared when I applied the filter and I looked at the dates as well as the times at which the accounts were created. I clicked on the account that was most recently created as that is what we were looking for in this task.



Event 4720, Microsoft Windows security auditing.

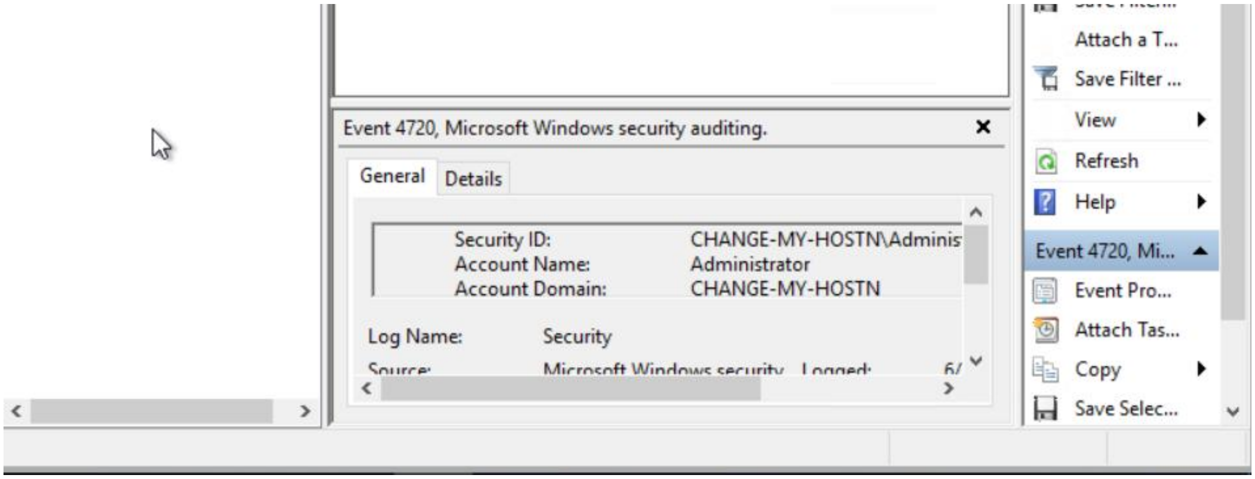
General | Details

```
Security ID:        S-1-5-21-1966530601-3185510712
Account Name:       hacked
Account Domain:     CHANGE-MY-HOSTN

Log Name:     Security
Source:       Microsoft Windows security   Logged:   6/7,
```

I looked at the bottom of the page in the General section under new account to find the Account Name and I found it – Hacked.

STEP 2: Finding the user account which created the above account.



Event 4720, Microsoft Windows security auditing.

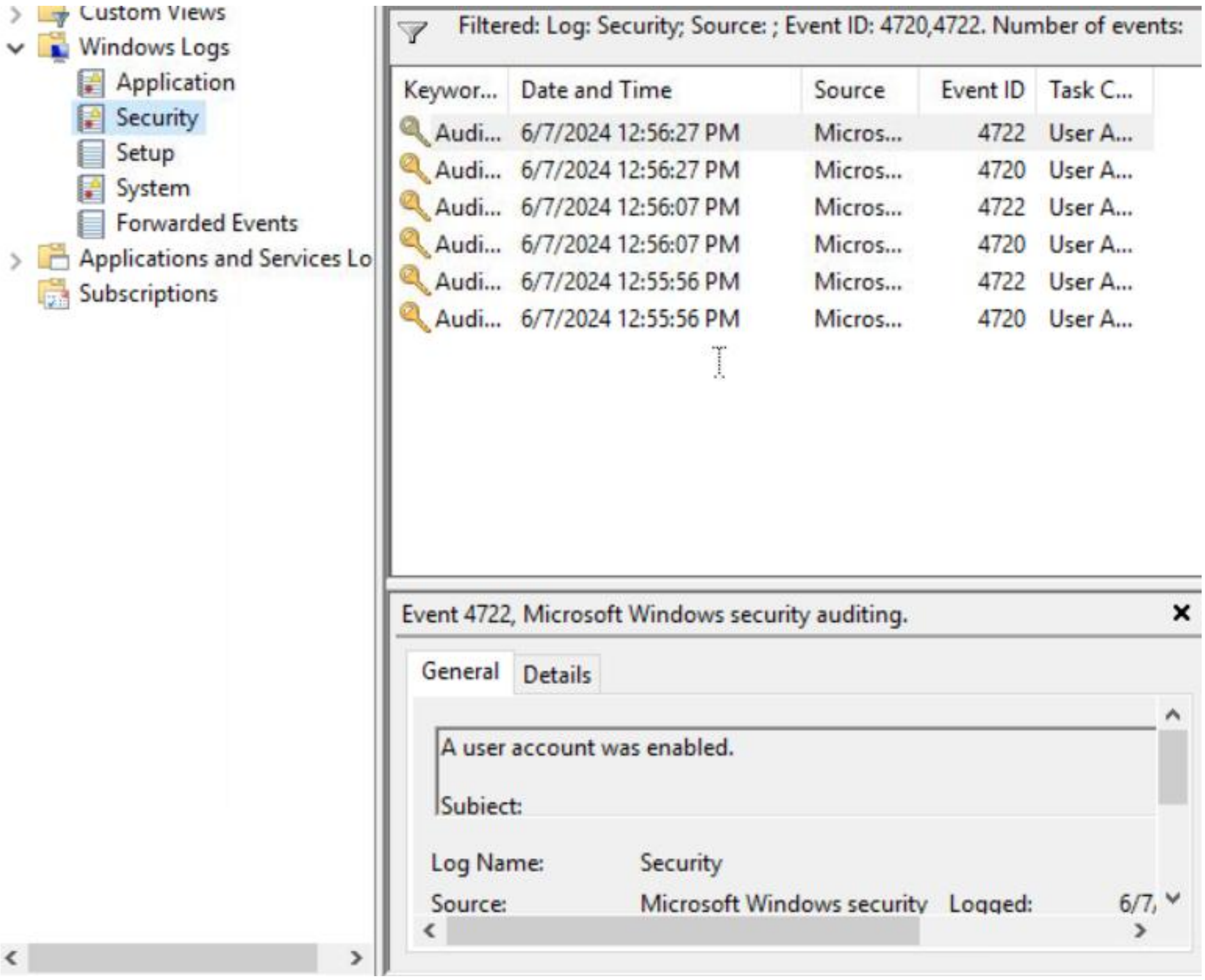
General | Details

```
Security ID:        CHANGE-MY-HOSTN\Adminis
Account Name:       Administrator
Account Domain:     CHANGE-MY-HOSTN

Log Name:     Security
Source:       Microsoft Windows security   Logged:   6/
```

I found the user account that created the above account after scrolling up a bit and looking under subject.

STEP 3: Acknowledging the date on which the account was enabled.



Filtered: Log: Security; Source: ; Event ID: 4720,4722. Number of events:

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	6/7/2024 12:56:27 PM	Micros...	4722	User A...
Audi...	6/7/2024 12:56:27 PM	Micros...	4720	User A...
Audi...	6/7/2024 12:56:07 PM	Micros...	4722	User A...
Audi...	6/7/2024 12:56:07 PM	Micros...	4720	User A...
Audi...	6/7/2024 12:55:56 PM	Micros...	4722	User A...
Audi...	6/7/2024 12:55:56 PM	Micros...	4720	User A...

Event 4722, Microsoft Windows security auditing.

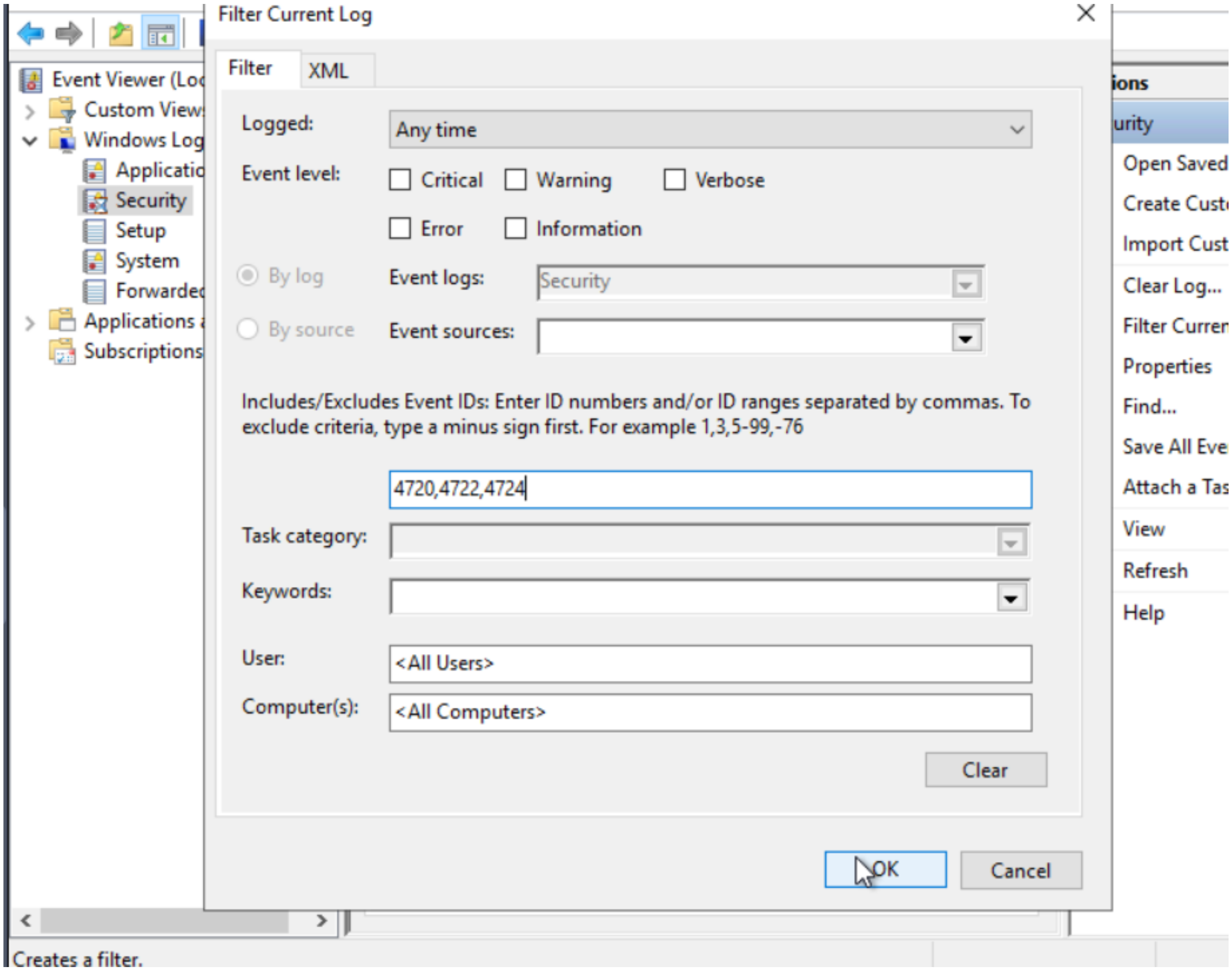
A user account was enabled.

Subject:

Log Name: Security
Source: Microsoft Windows security Logged: 6/7,

I added an **event ID 4722(A user account was enabled)** in the filter next to the previous event IT separated by a comma and clicked OK. I was then presented with this and found the exact date the account was created.

STEP 4: Finding out if the account went through a password reset as well.



Filter Current Log

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: 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

4720,4722,4724

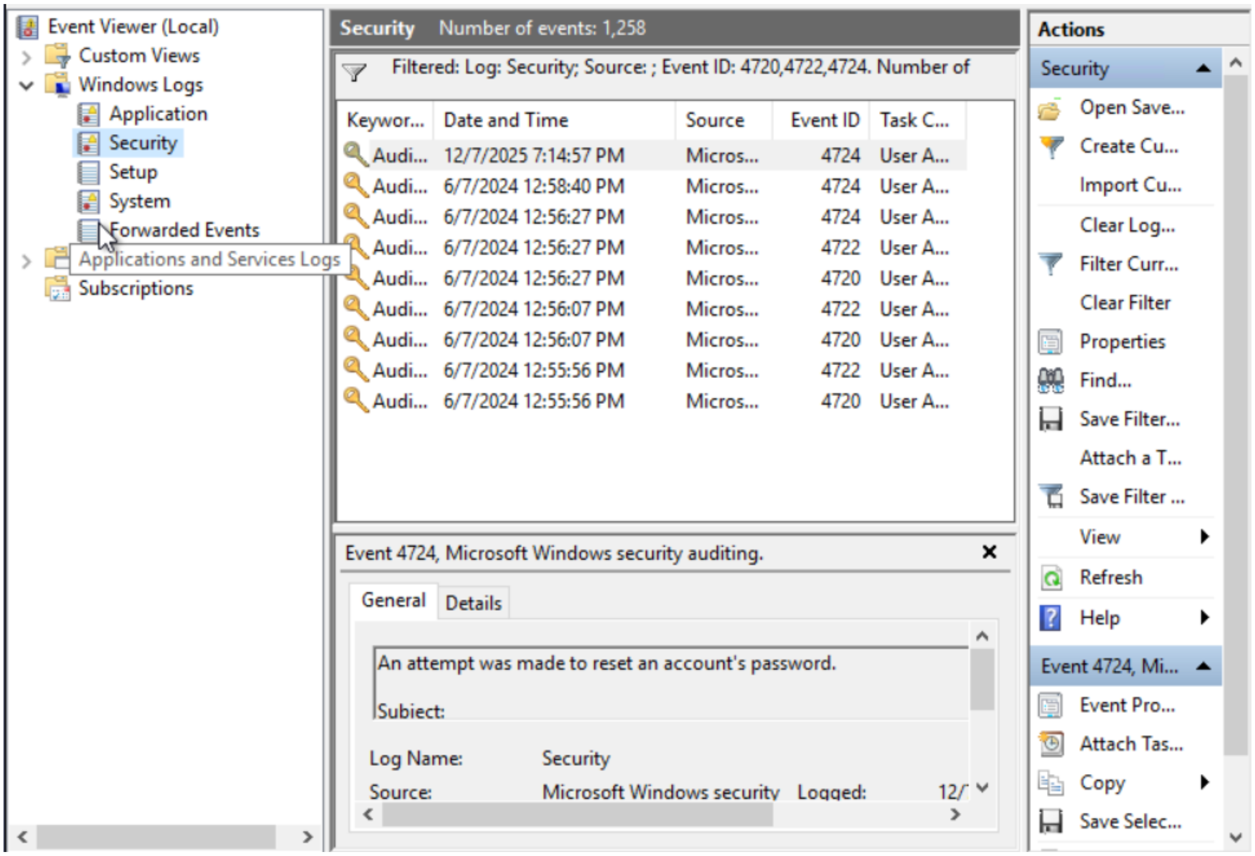
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

I clicked the ‘Filter current logs’ on the right pane again and added **another event ID 4724(An attempt was made to reset an account’s password)** to find out if this was true.



Security Number of events: 1,258

Filtered: Log: Security; Source: ; Event ID: 4720,4722,4724. Number of

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	12/7/2025 7:14:57 PM	Micros...	4724	User A...
Audi...	6/7/2024 12:58:40 PM	Micros...	4724	User A...
Audi...	6/7/2024 12:56:27 PM	Micros...	4724	User A...
Audi...	6/7/2024 12:56:27 PM	Micros...	4722	User A...
Audi...	6/7/2024 12:56:27 PM	Micros...	4720	User A...
Audi...	6/7/2024 12:56:07 PM	Micros...	4722	User A...
Audi...	6/7/2024 12:56:07 PM	Micros...	4720	User A...
Audi...	6/7/2024 12:55:56 PM	Micros...	4722	User A...
Audi...	6/7/2024 12:55:56 PM	Micros...	4720	User A...

Event 4724, Microsoft Windows security auditing.

```
An attempt was made to reset an account's password.

Subject:

Log Name:        Security
Source:          Microsoft Windows security   Logged:   12/
```

Indeed, the operation was undergone as evidence shows by the bottom in the general section that there was an attempt at resetting the users account password.

Summary Conclusion

In this Windows Event Logs analysis, I identified the attacker’s actions on the compromised system by examining key security events. By filtering for Event IDs 4720, 4722, and 4724, I located the most recently created account (**Hacked**), identified the user who created it, confirmed when it was enabled, and verified that a password reset attempt was made. This investigation demonstrates effective use of Event Viewer filtering to trace malicious account activity and understand the attacker’s steps prior to accessing the file server.