Incident Response: Windows Account Management Event (Part 1)

hackingarticles.in/incident-response-windows-account-management-event-part-1

Raj August 29, 2020

For a system to perform well and ensure its maintenance, it is extremely important to monitor and manage events on a system. Event Logs are part of the Windows system, that are created by on a system and can be checked locally or remotely on regular intervals by an administrator or any user. These logs can then be imported and viewed in a SIEM tool to ensure efficient Incident Response.

Table of Contents

Security Policy Settings

They are set of rules that an administrator uses to configure a computer or multiple devices for securing resources on a device or network. The Security Settings extension of the Local Group Policy Editor allows you to define a security configuration as part of a Group Policy Object (GPO).

The GPOs are linked to Active Directory containers such as sites, domains, or organizational units, and they enable you to manage security settings for multiple devices from any device joined to the domain. Security settings policies are used as part of your overall security implementation to help secure domain controllers, servers, clients, and other resources in your organization.

Advantage of Security Setting

- User is authenticated in a network or device.
- The defined resources that any user is permitted to access.
- Whether to record a user’s or group’s actions in the event log.
- Membership of a user in a group.

Event Log

The event logs usually keep a record of services from various sources and then stores them in a single place. Events logs can be of Security, System and Application event. As an incident responder, you should look for multiple sources of log information and should

not forget to look at the older log files which may be present in backup systems or volume shadow copies.

When the Event logs are assessed, the Event ID have various field details with them;

Field	Function
Log name	Defines the name of the event log
Source	The place from where it is generated in the system
Event ID	The identification number of the log
Level	The seriousness of the log
User	The account to which the log is related to
Logged	The systems date and time when the event was generated
Task Category	It is assigned by the source of log
Keywords	Its is used to group or categorise the events
Computer	The system on which the log was created
Description	It it's the information about the log

Account Management Events

The Account Management is extremely important and these events can be used to track the maintenance of users, group, and computer objects in Local users and groups, Active Directory.

Account Management events can be used to track a new user account, any password resets, or any new members being added to groups or being deleted from the group.

The account management events can be categorised into different types:

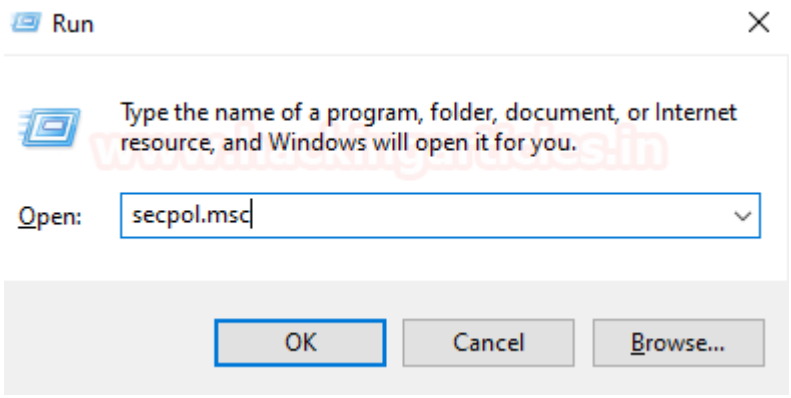
No.	Task Category
1.	User Account Management
2.	Computer Account Management
3.	Security Group Management

Events in Windows 10 system

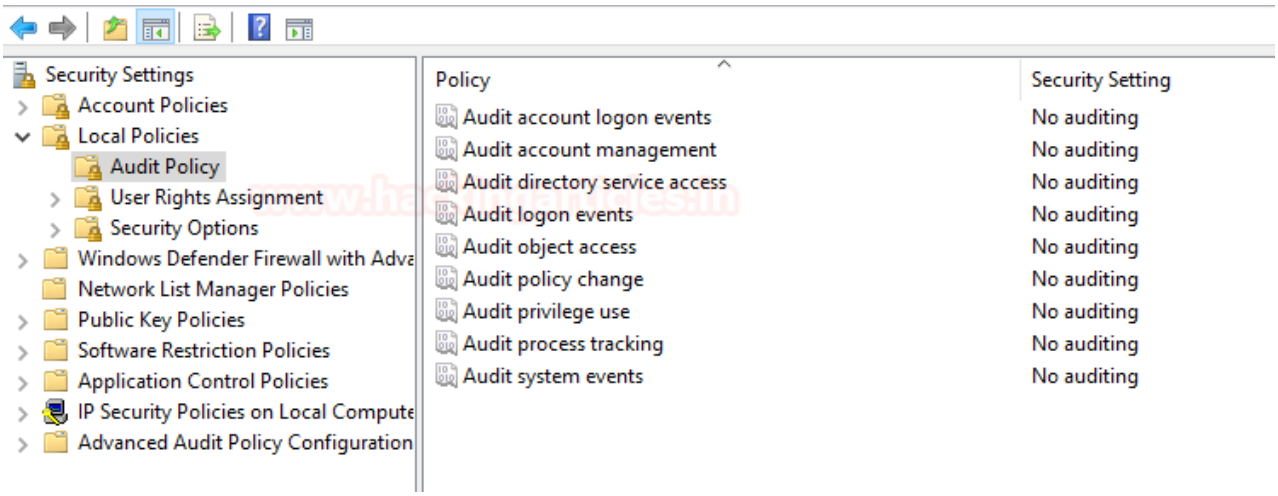
To see how this works, let's get you started with Account Management Events.

To view the security policy and setting, press '**Windows+R**' and type

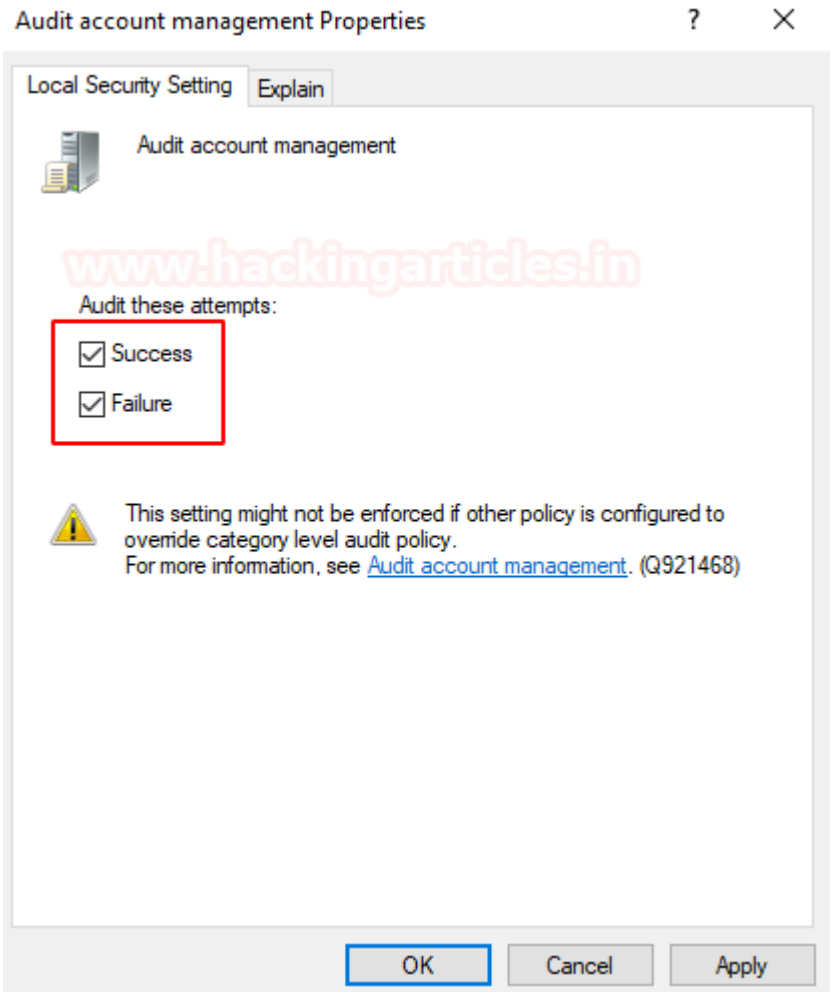
```
secpol.msc
```



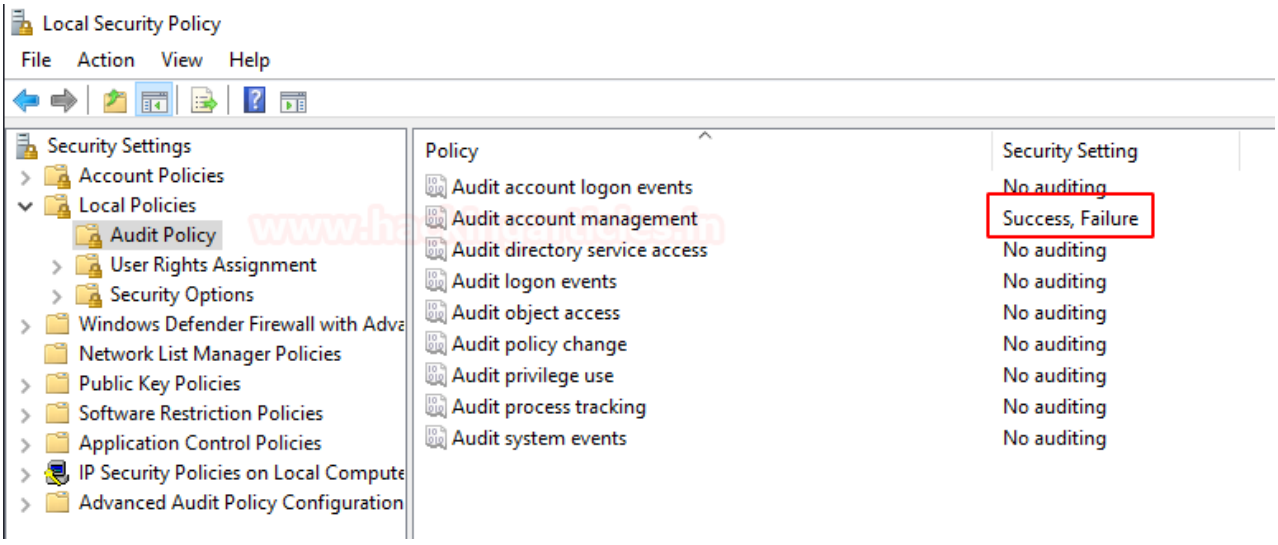
Here you see that in audit policies, there is ‘no auditing ‘ being displayed and to view these event we need to activate them.



When you open the properties of audit account management, check the success and failure attempts and press **ok.**

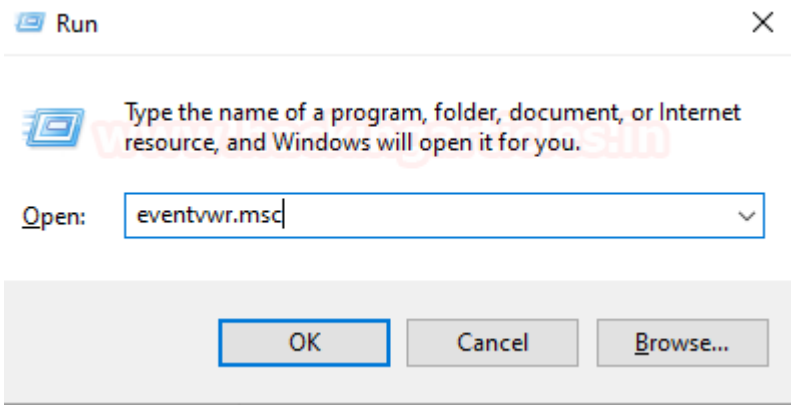


You can see that the security setting has been updated and now the logs for account management are active.



Now to Open Event Viewer, press '**Windows+r**' and type

```
eventvwr.msc
```



So, let's check the logs created by these events. Power on your Windows 10 systems.

Event ID 4720

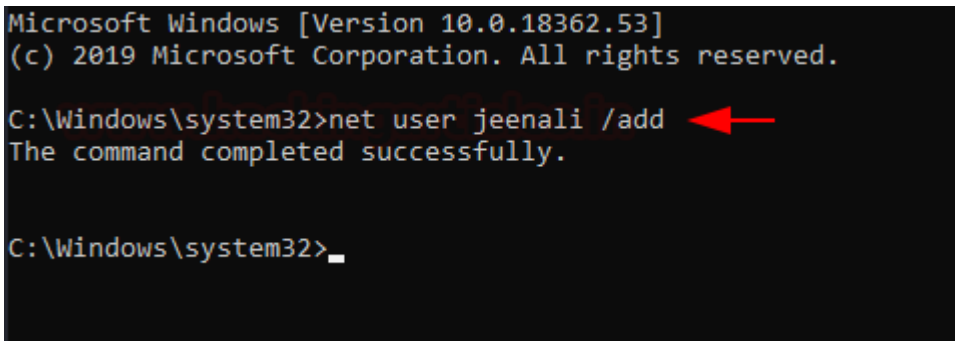
Event ID	Description
4720	A user account was created.

Purpose of monitoring this Log

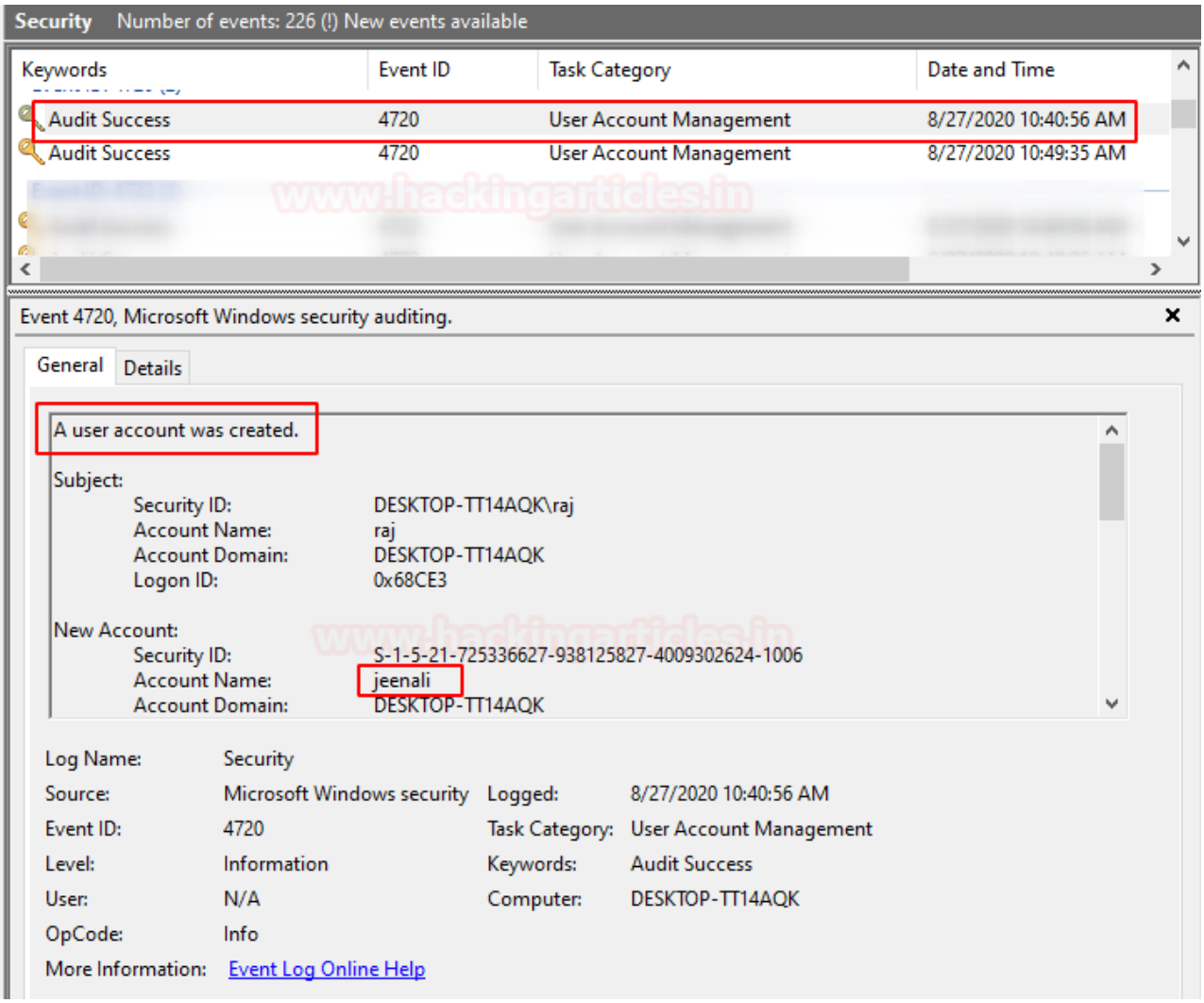
- To check SAM Account name field which could indicate an anomaly
- To keep a check on the logon hours activity of a user account.

To see how this works, open command-prompt, create a new user.

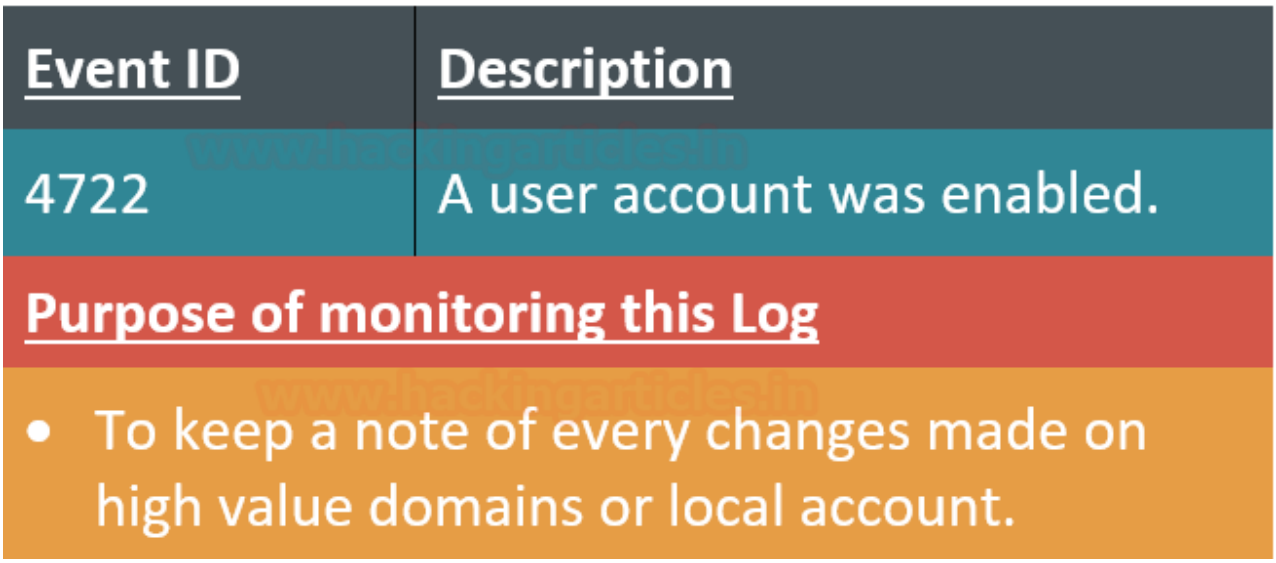
```
net user username /add
```



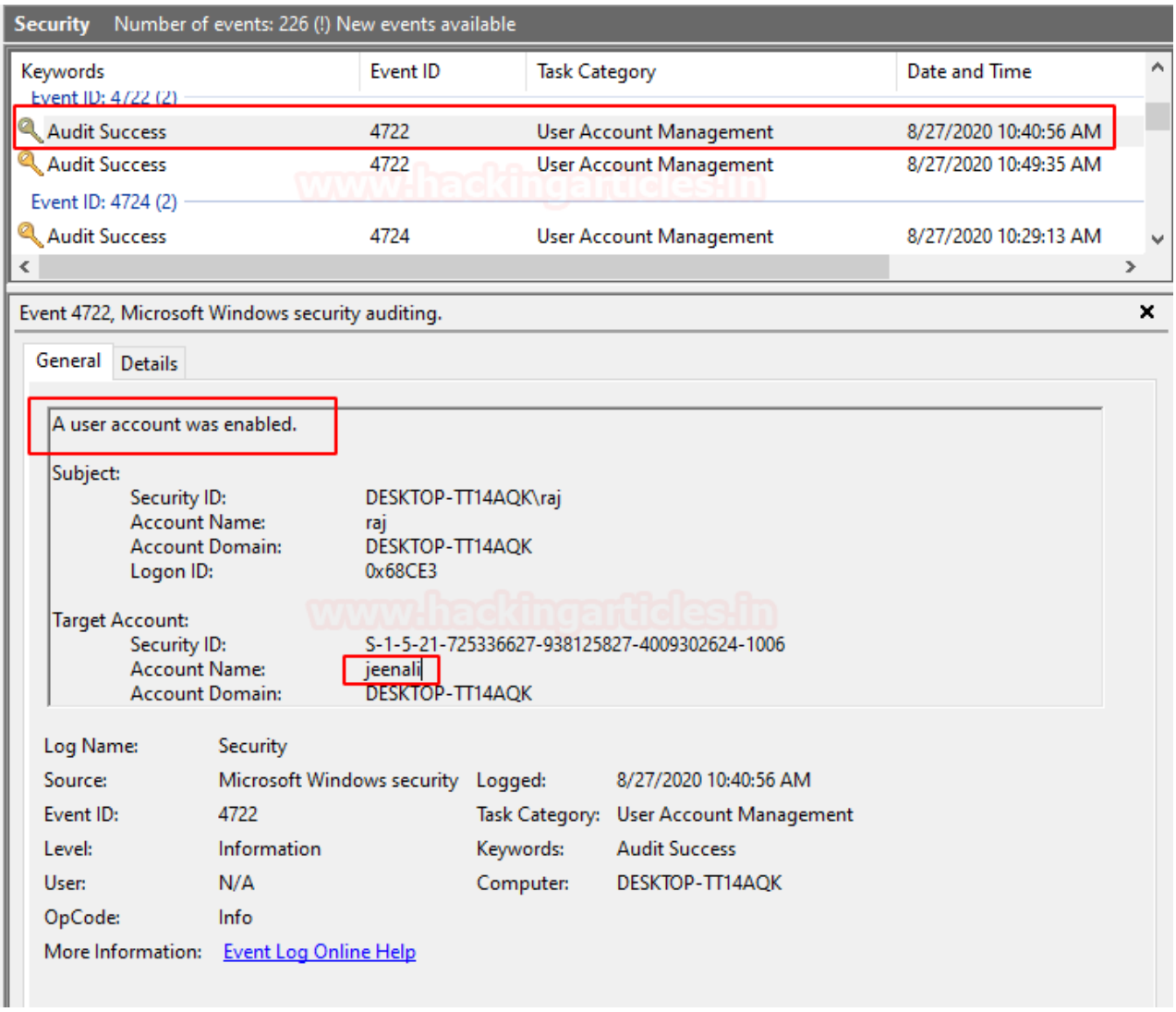
After you create a new user, you can see below that 4720 event is created and you can also see the account name.



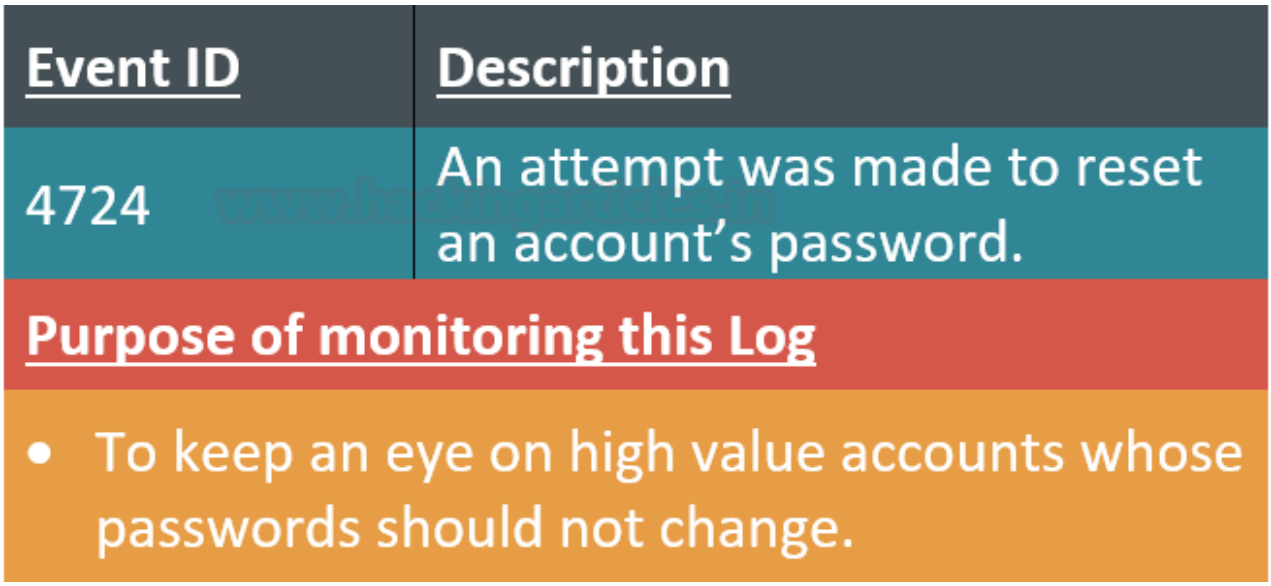
Event ID 4722



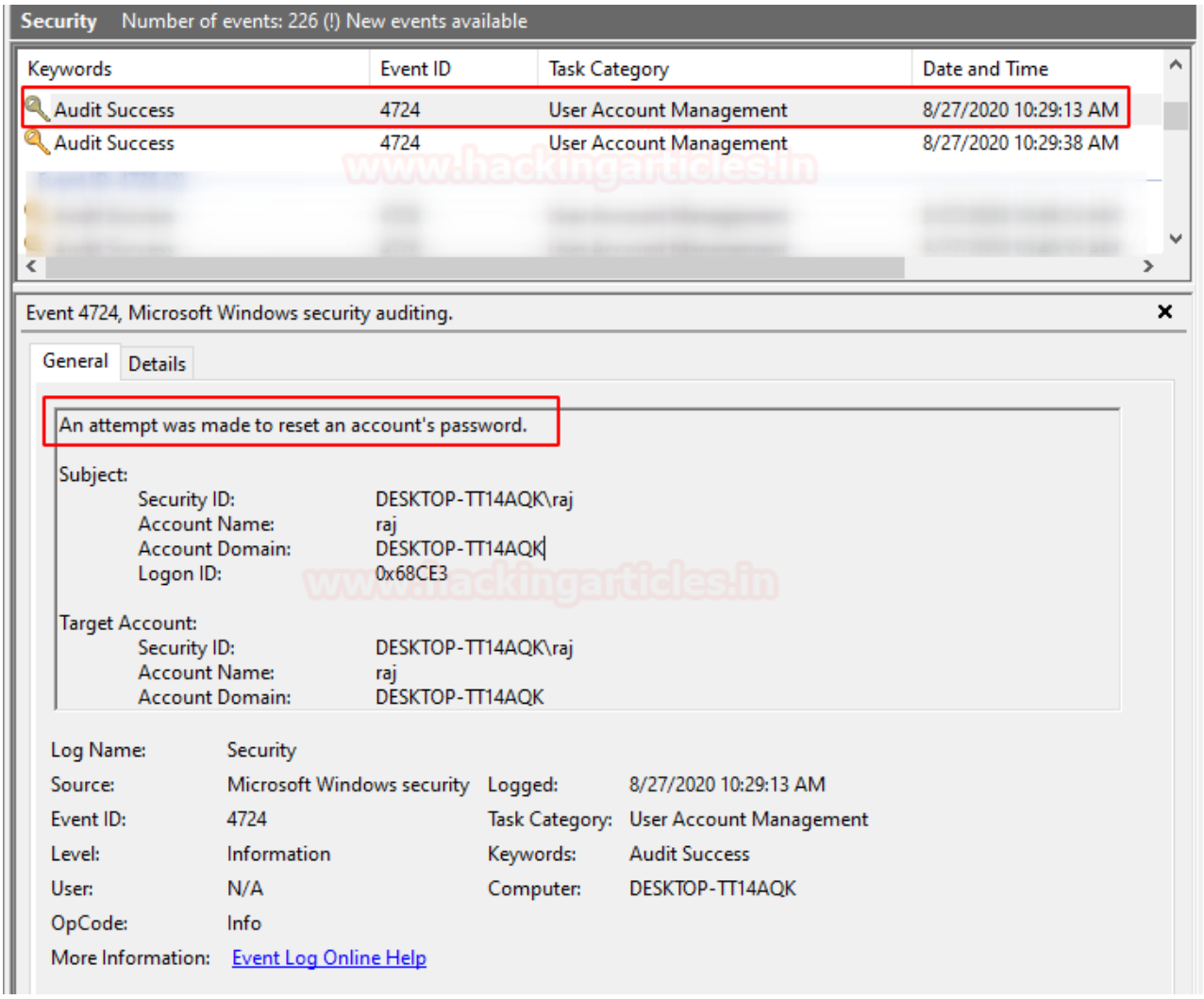
After a new user account is enabled, you can see the event 4722 is generated with the account name.



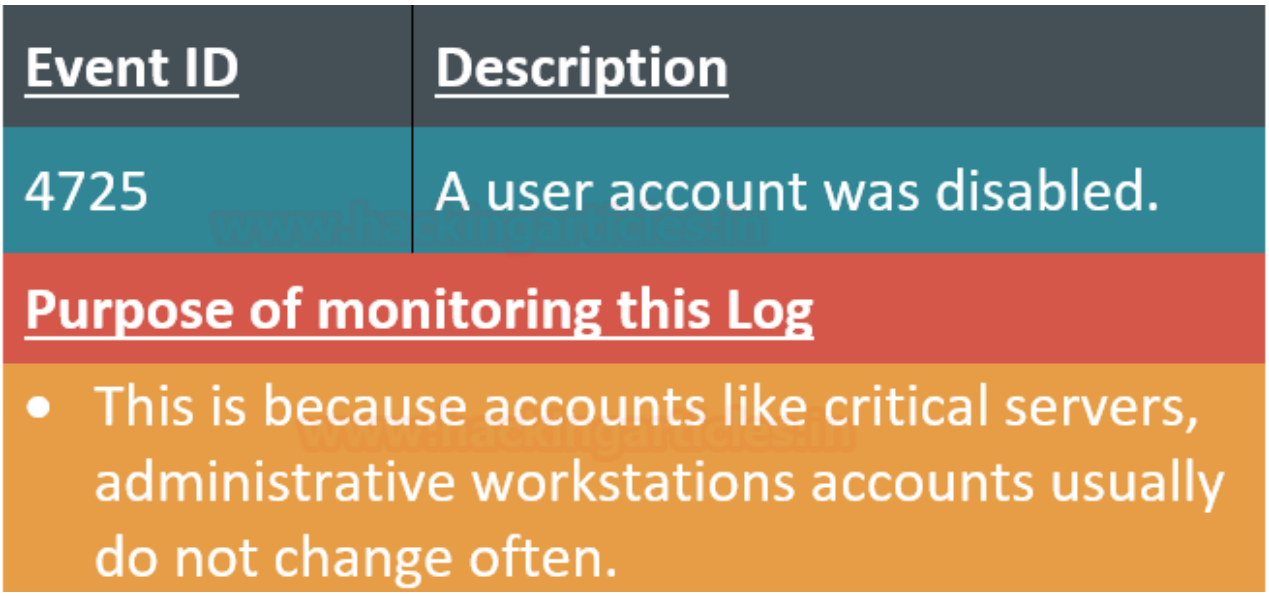
Event ID 4724



When the password for a user account was changed, it displays that an attempt to change the password was successful.

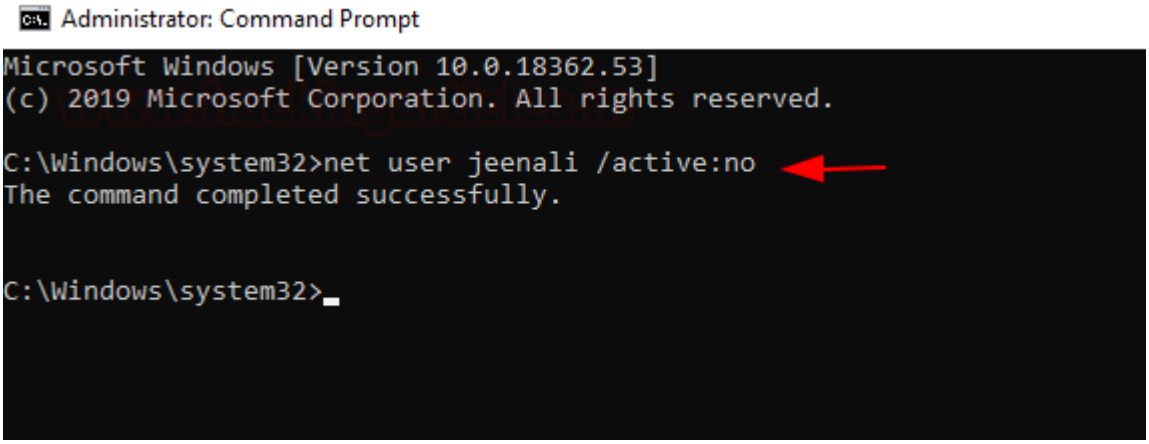


Event ID 4725

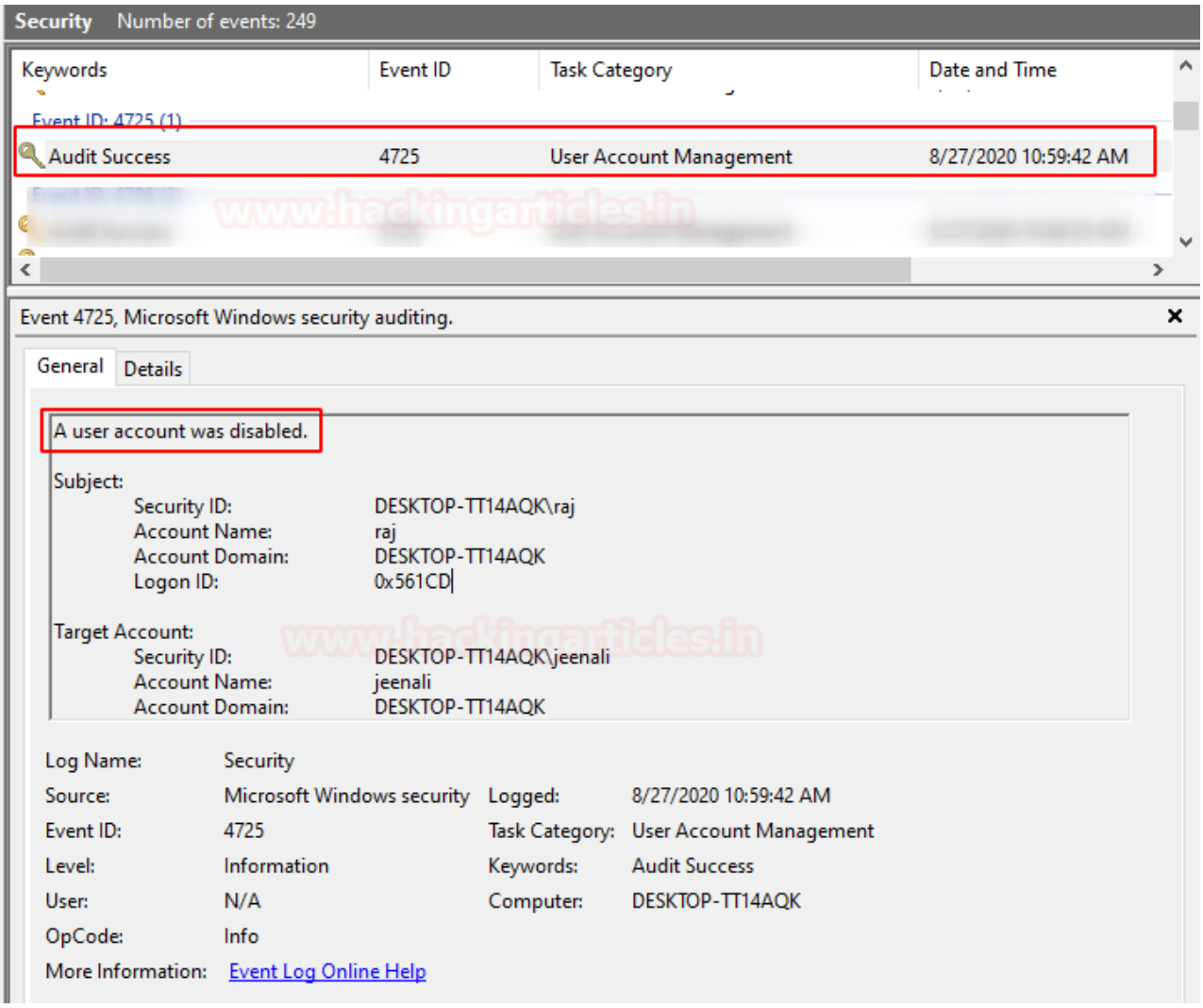


To disable a user account using command prompt, you can type

```
net user username /active:no
```



When you successfully disabled an account the results in the event viewer are displayed as below.



Event ID 4726

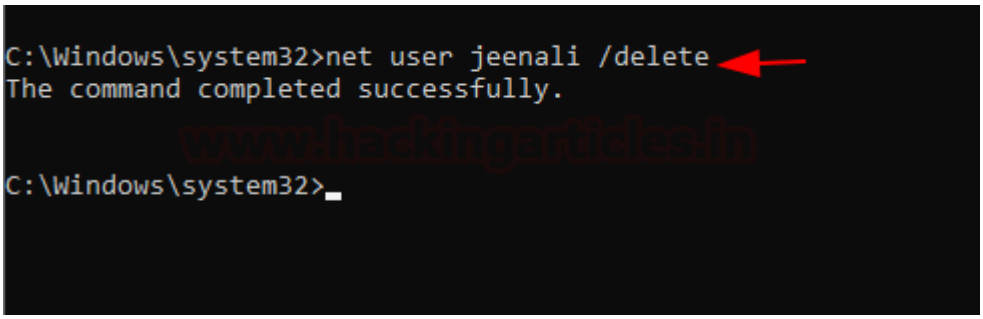
Event ID	Description
4726	A user account was deleted

Purpose of monitoring this Log

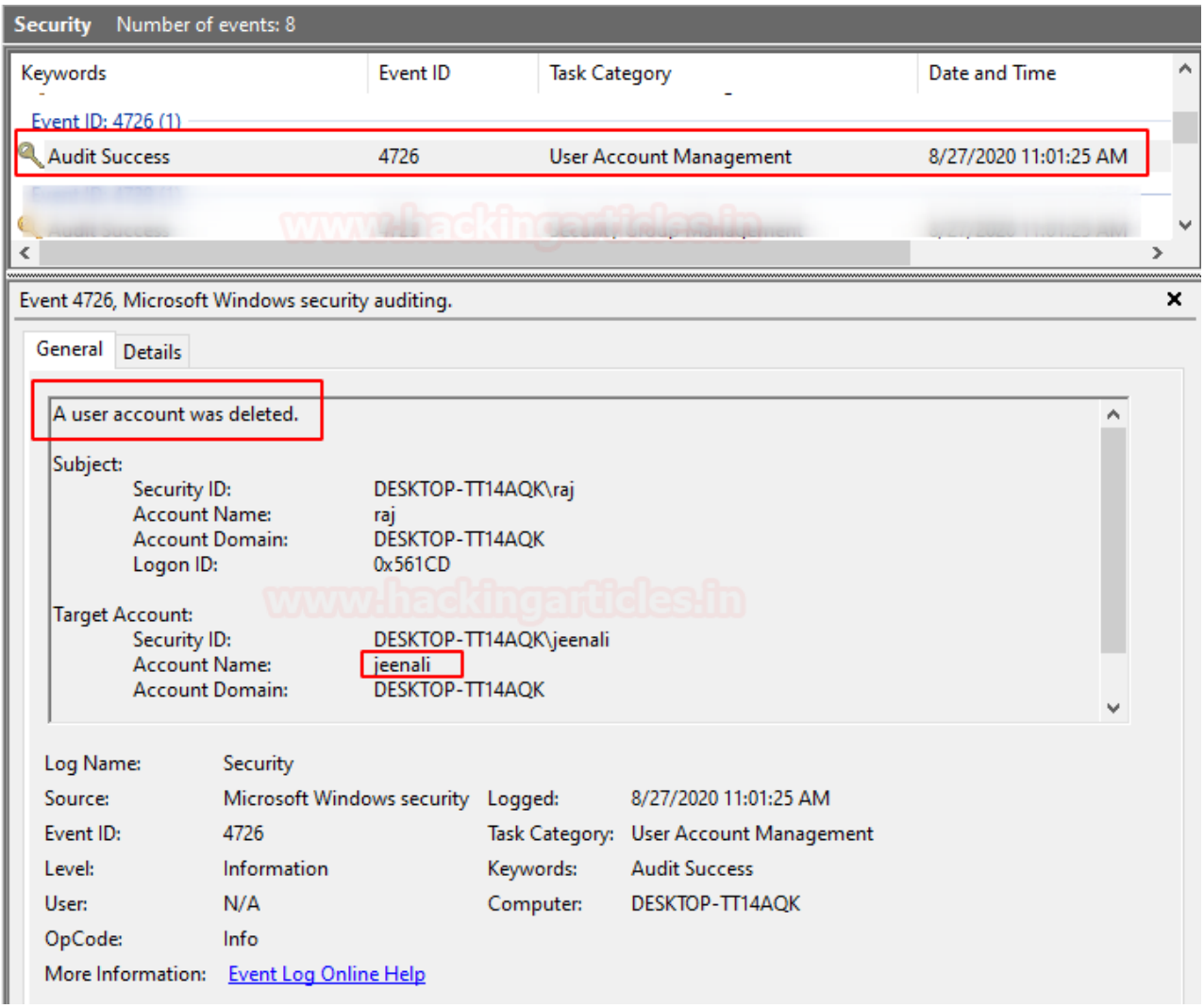
- To monitor Accounts after every changes.
- Local accounts are usually not deleted and could hence be a possible malicious activity.
- It could be an account that shouldn't have been deleted in the first place.

To delete a user account using command prompt, you can type

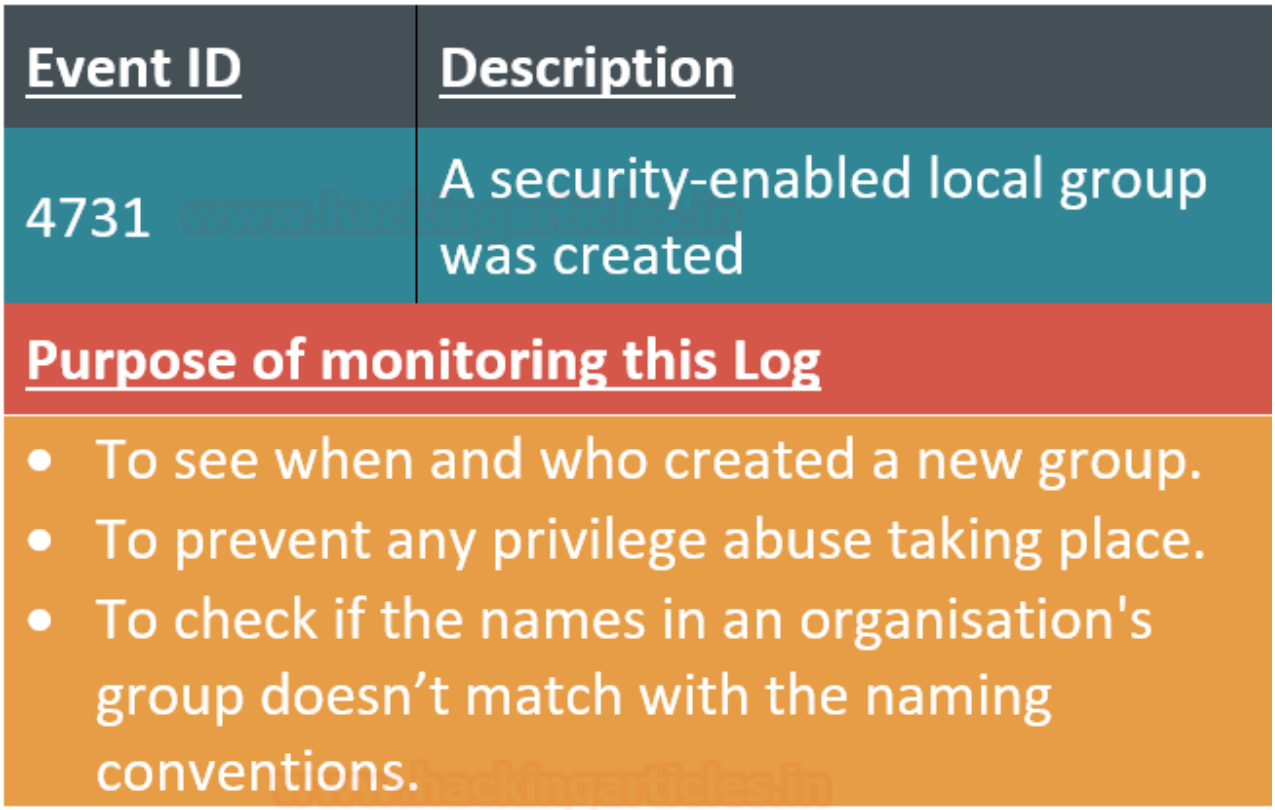
```
net user username /delete
```



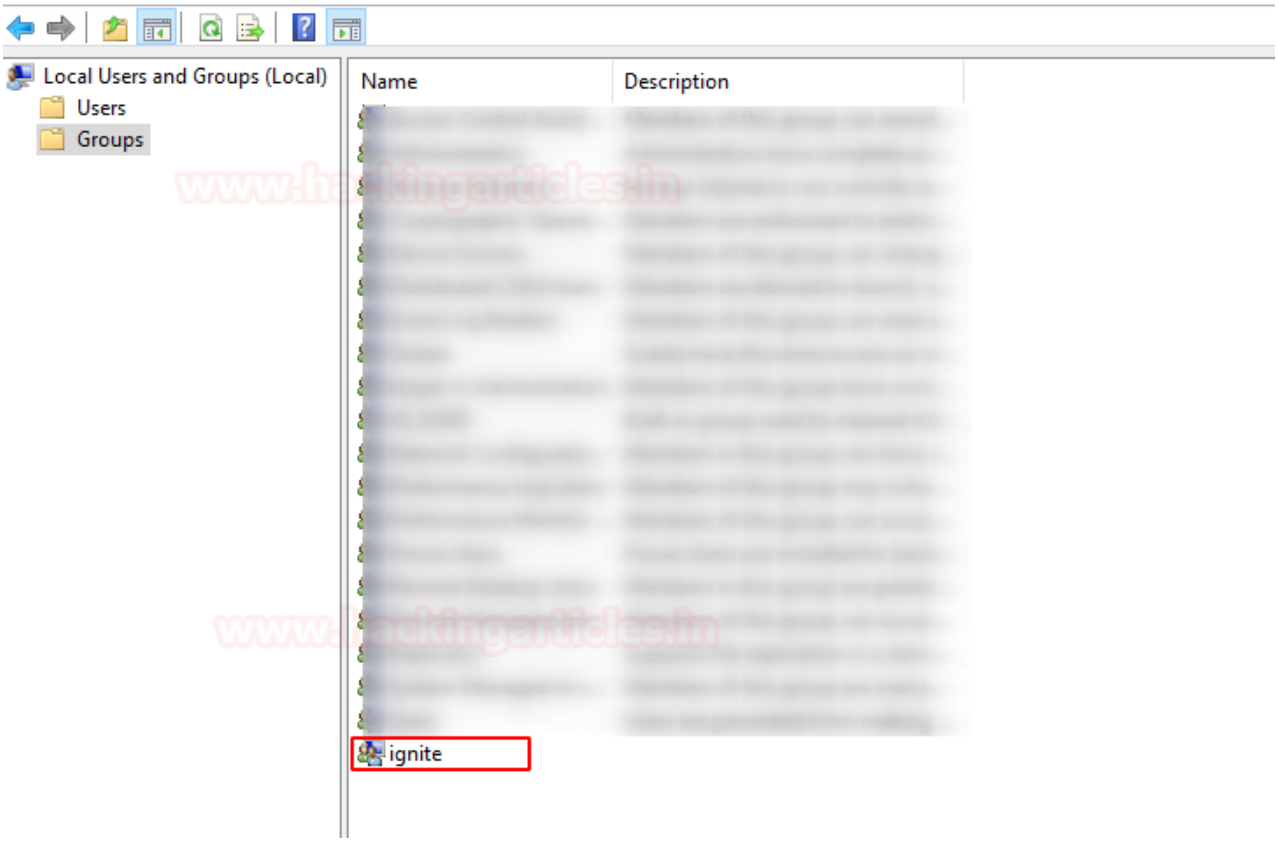
When the account is deleted successfully, this event is created and the user account name is also displayed.



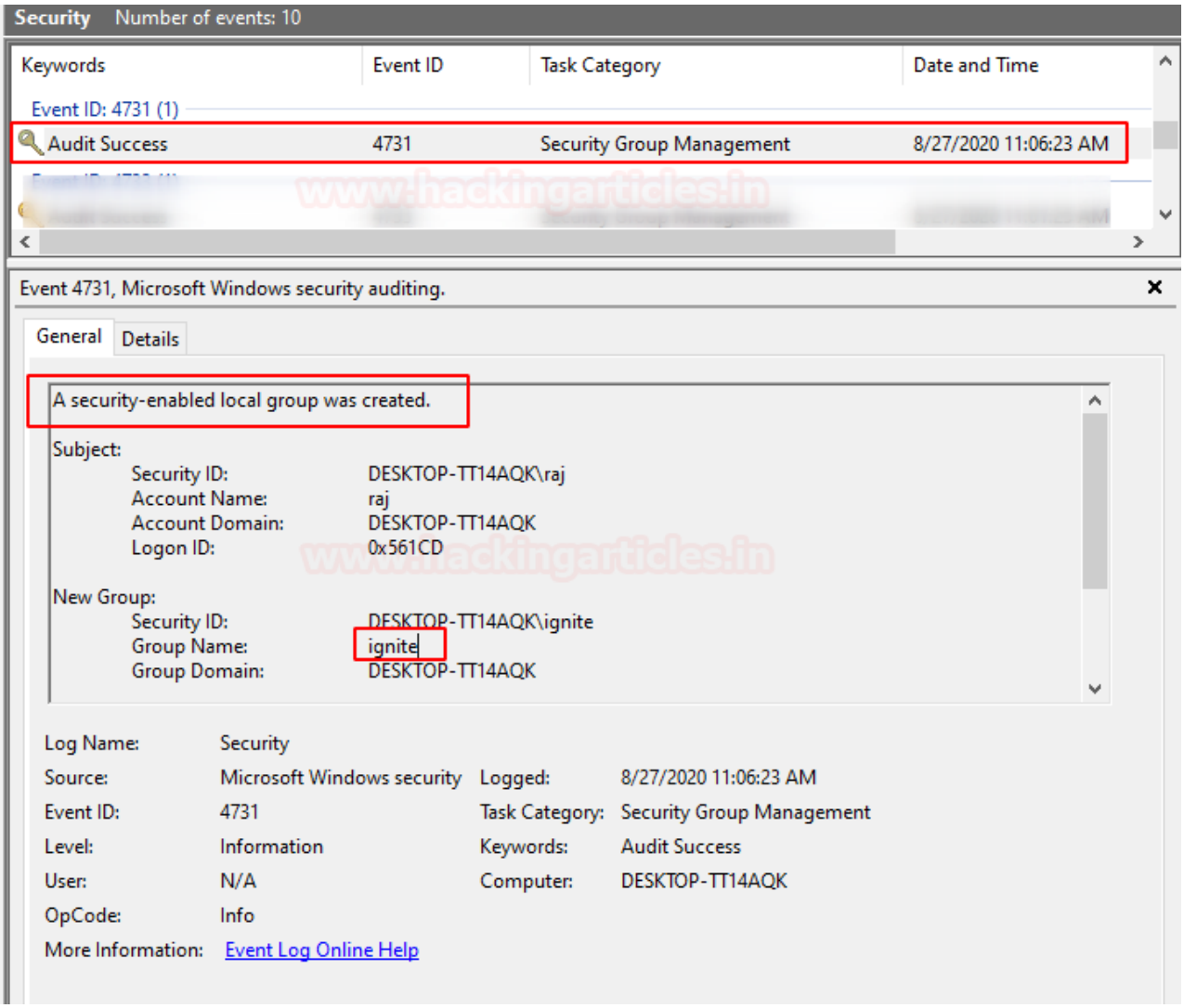
Event ID 4731



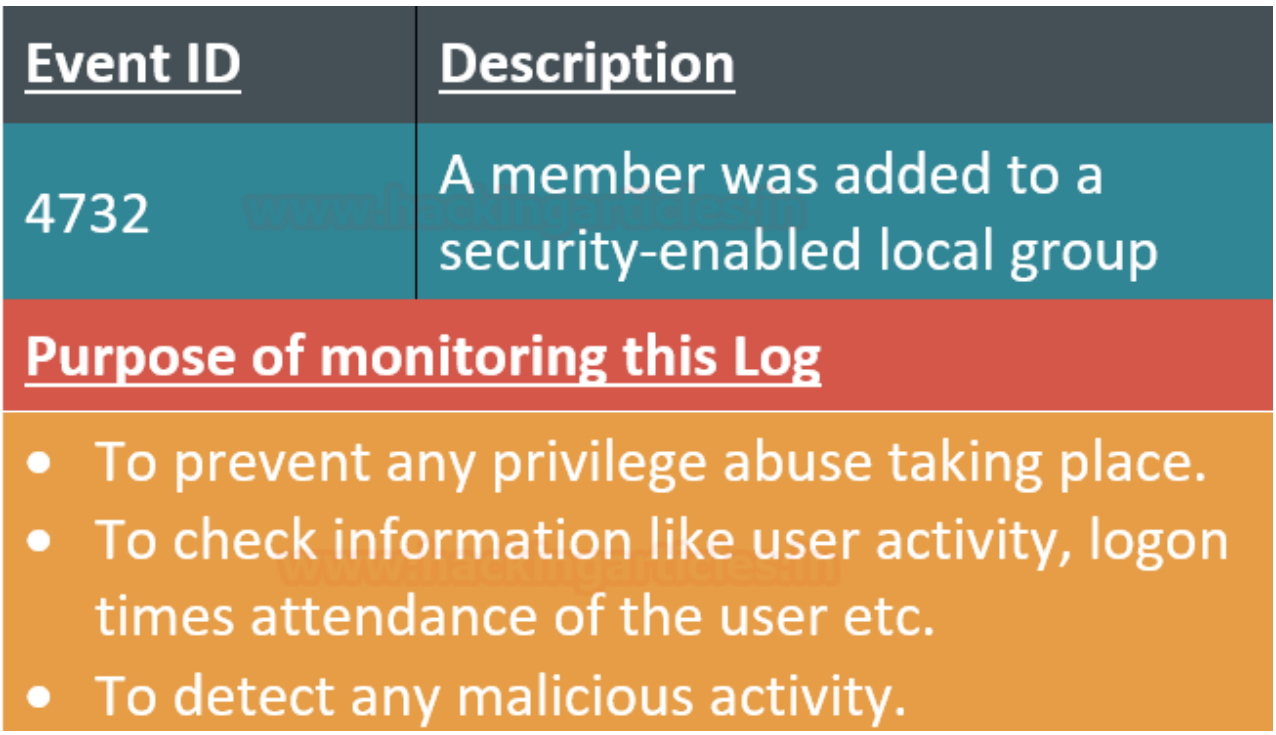
Go to local users and groups and created a new group. Here you see that a new group is created named ignite.



When the new security-enabled local group is created, you can see that this event will be generated in the Event viewer with its name.



Event ID 4732



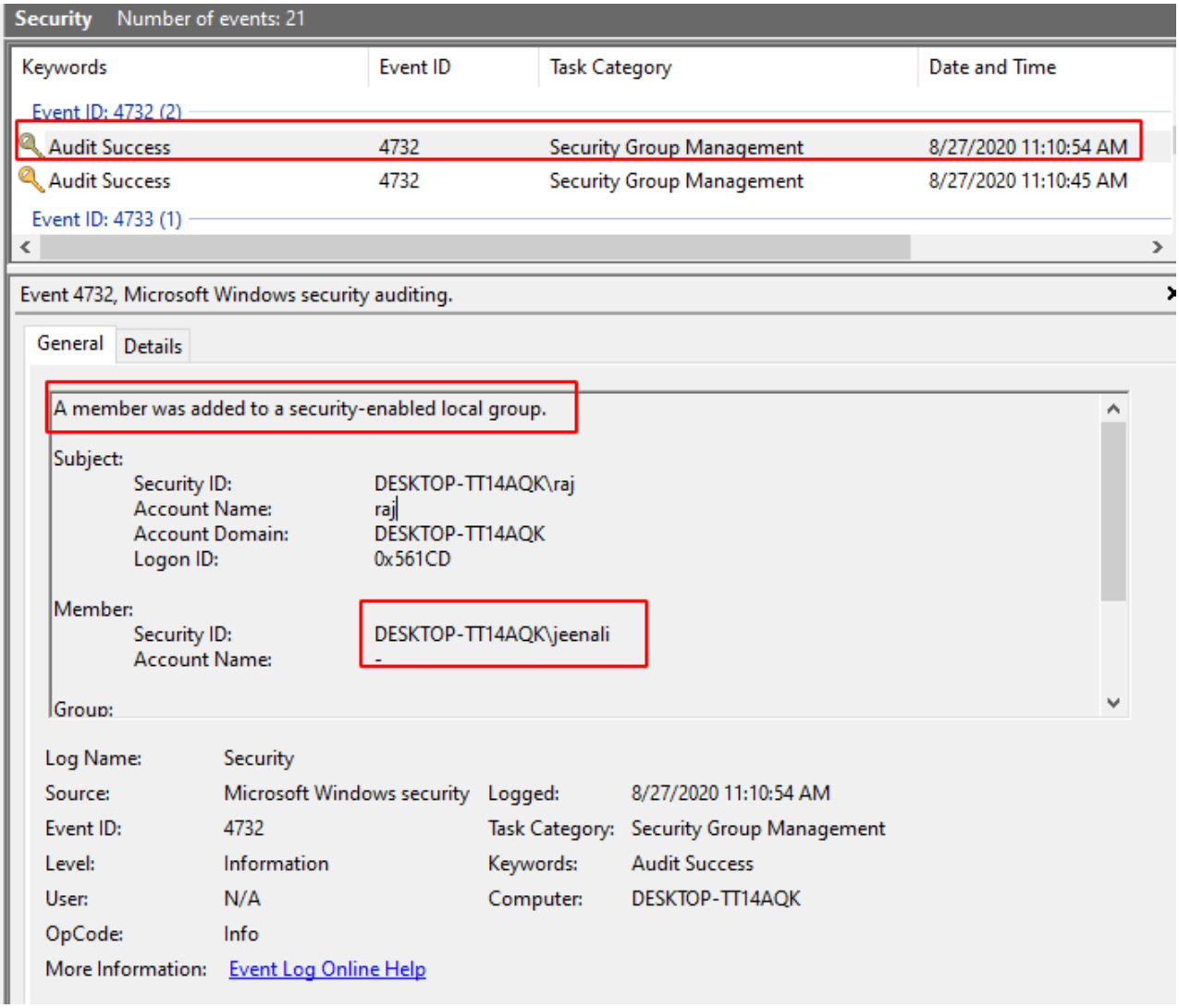
To add a new member to the security-enabled local group, type

```
net localgroup groupname username /add
```

```
C:\Windows\system32>net localgroup administrators jeenali /add
The command completed successfully.


C:\Windows\system32>_
```

You see that the new member is added to the group and the user name is also displayed.



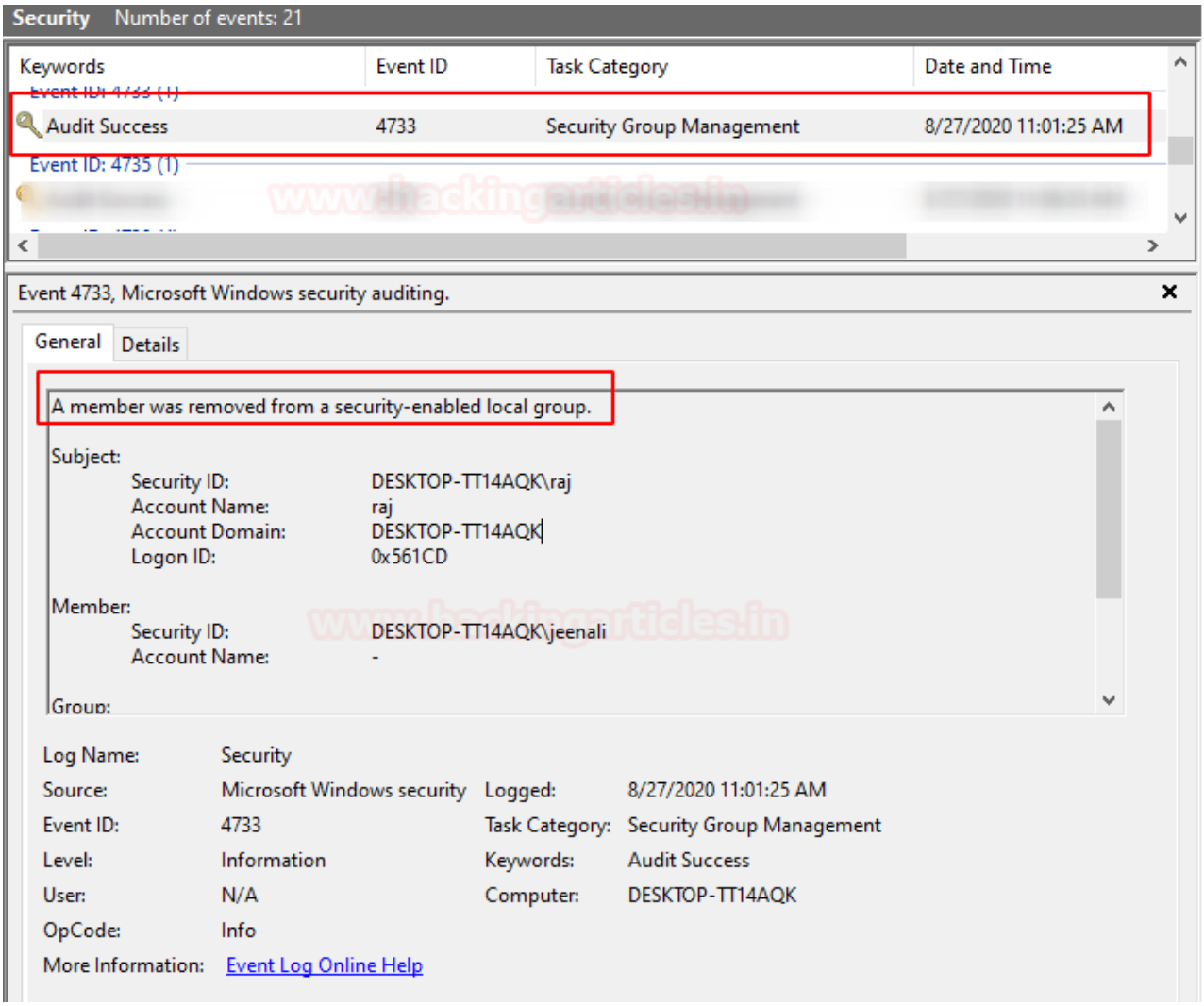
Event ID 4733

Event ID	Description
4733	A member was removed from a security enabled local group

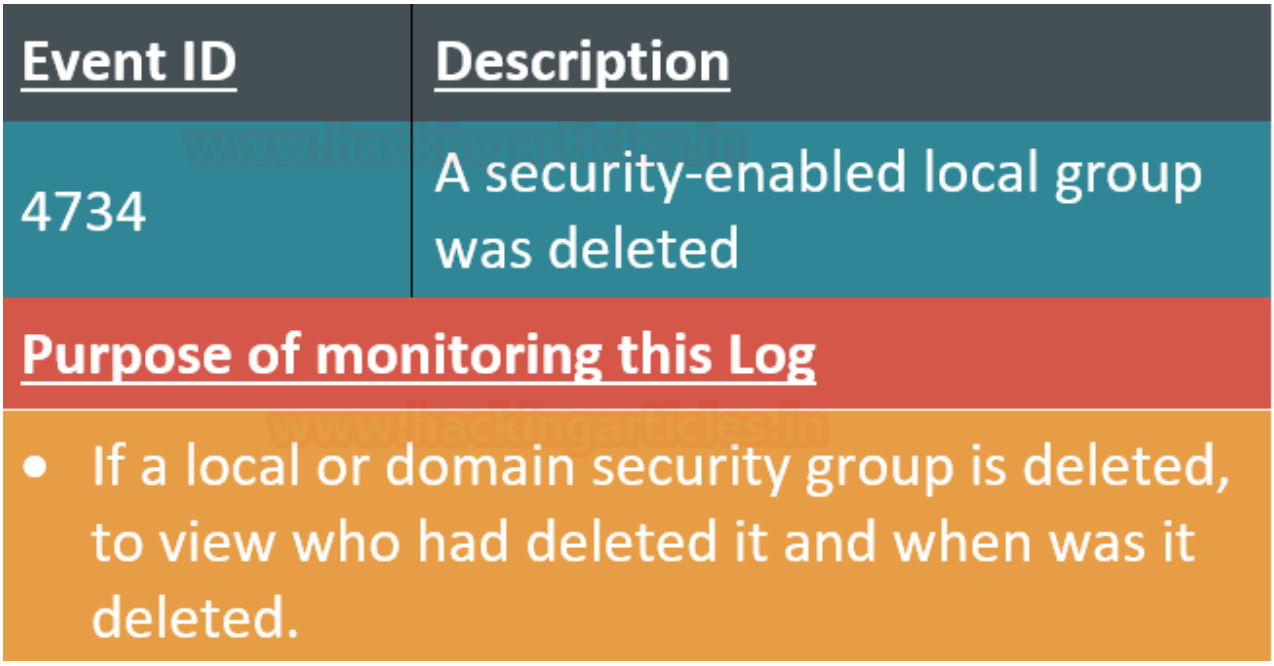
Purpose of monitoring this Log

- As you might need to check for the use of an account outside of normal working hours.
- To keep a check on accounts from another domain, or any external accounts that are not allowed to perform certain actions.

As a member is removed from the group, this event is generated.



Event ID 4734



To delete a security-enabled group using command prompt, you can type,

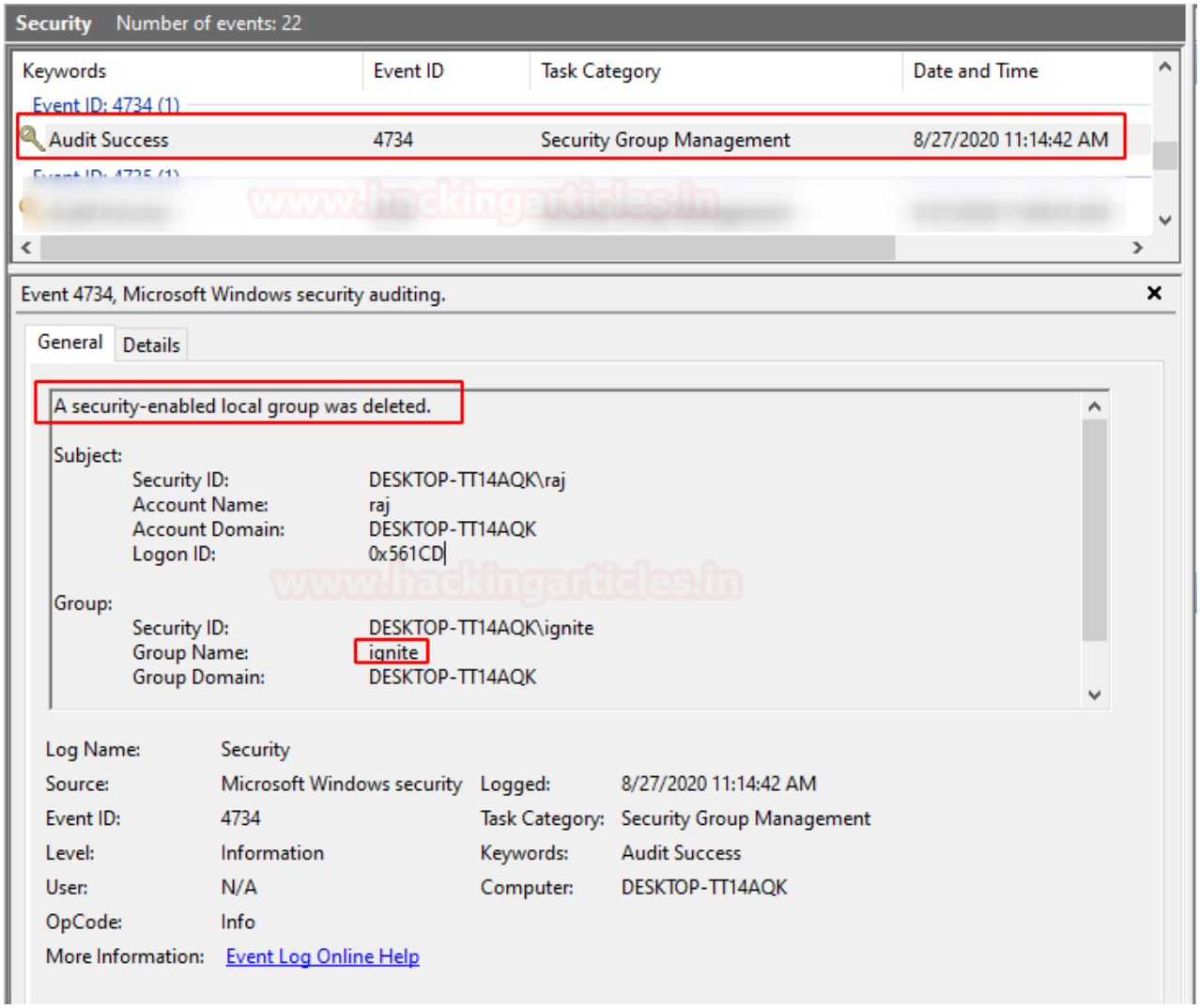
```
net localgroup groupname /delete
```

```
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net localgroup ignite /delete
The command completed successfully.


C:\Windows\system32>_
```

When the security-enabled local group is deleted, this event is generated and the name of the deleted group is also displayed.



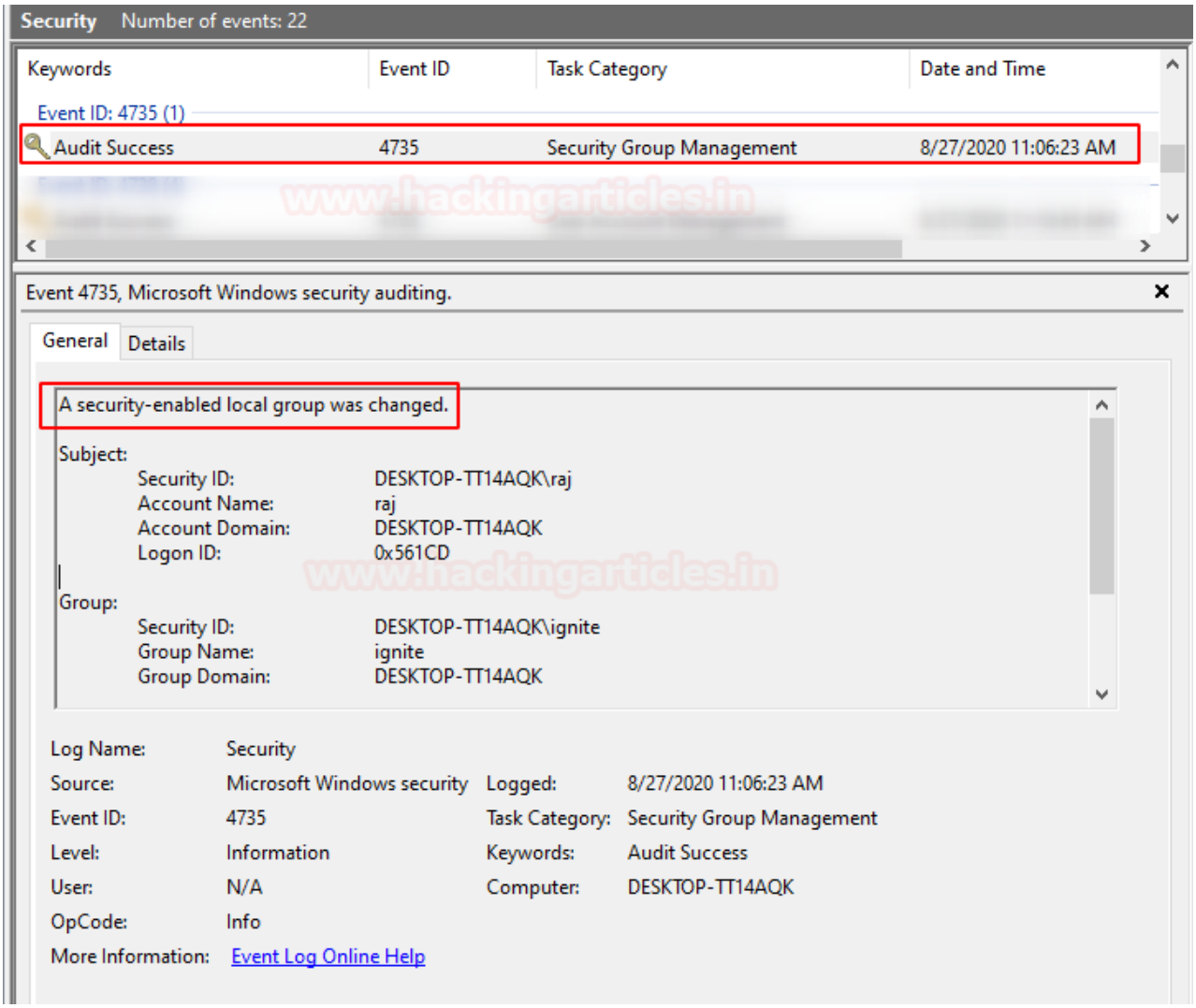
Event ID 4735

Event ID	Description
4735	A security-enabled local group was changed

Purpose of monitoring this Log

- For every time a member is added to a local or domain security group.

When the security-enabled local group is changed, this event is generated and the name of the group is also displayed.



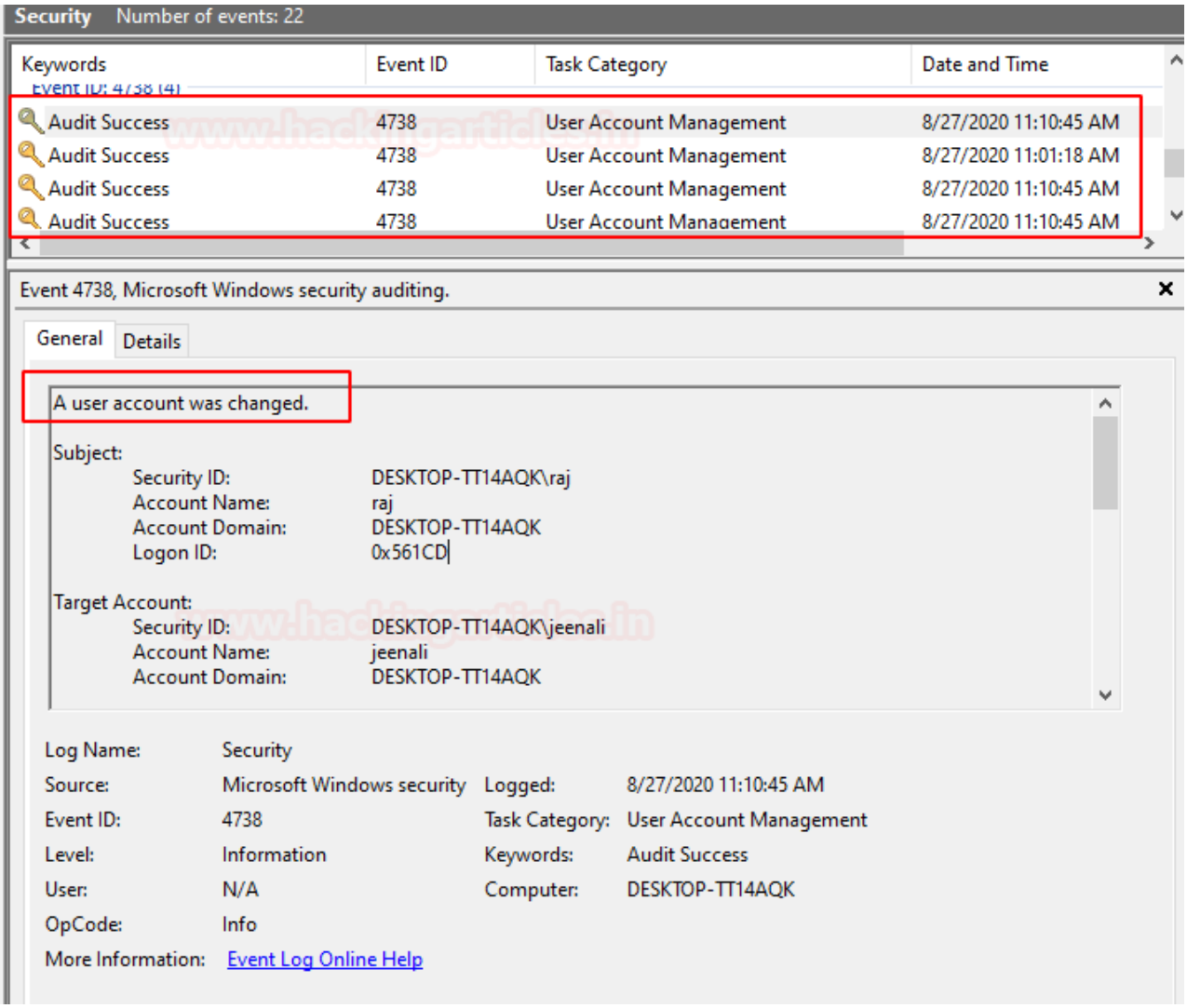
Event ID 4738

Event ID	Description
4738	A user account was changed

Purpose of monitoring this Log

- If there is any change in the services list on the Delegation tab, which should be checked.

When the user account is changed, this event is displayed.



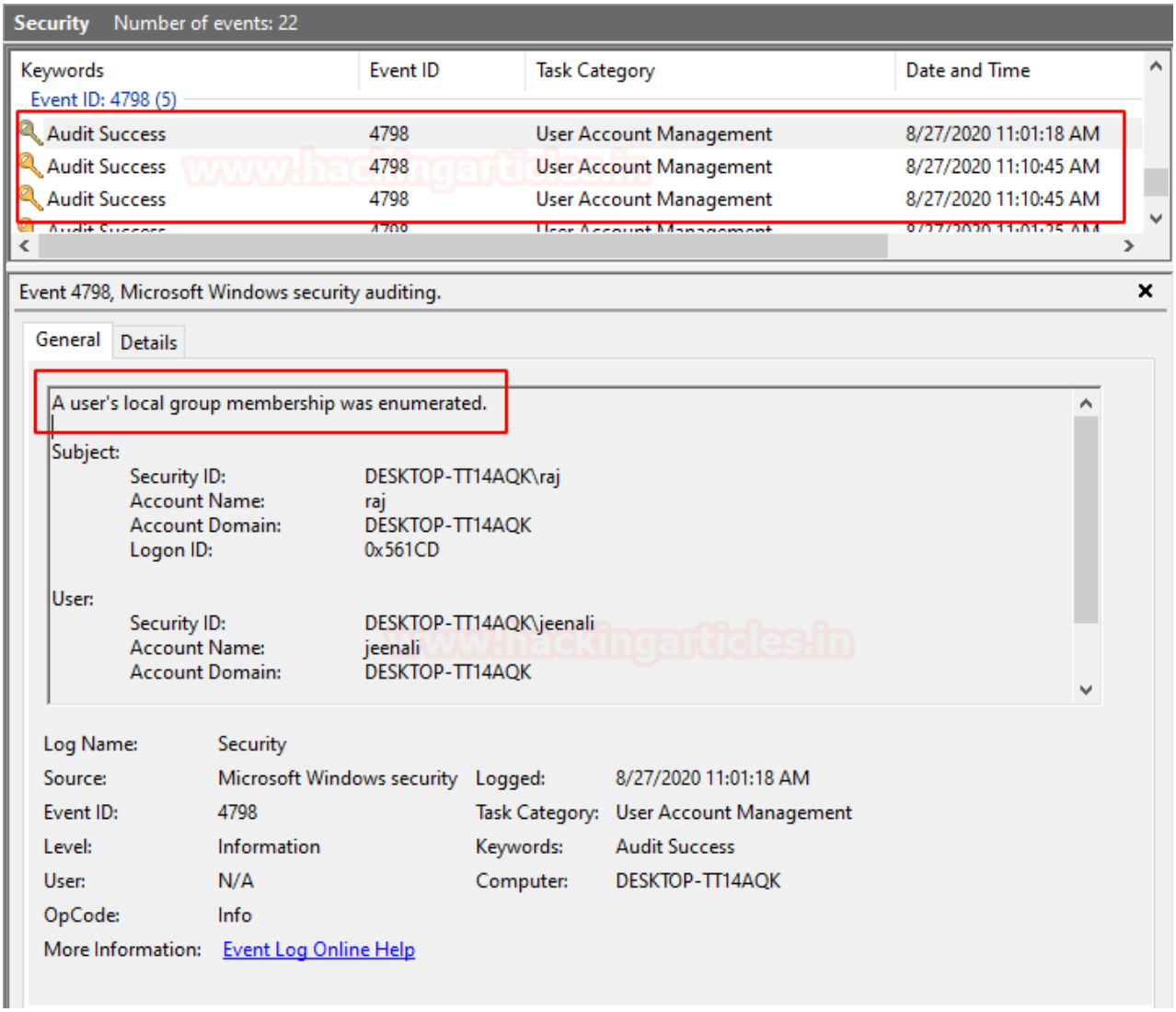
Event ID 4798

Event ID	Description
4798	A user's local group membership was enumerated. Large numbers of these events may be indicative of adversary account enumeration.

Purpose of monitoring this Log

- To check whether the Process Name is not in a standard folder
- To check for every enumeration of the group or any access attempt was made

When a local user's group is enumerated, you see that this log is created.



Conclusion: These were the Account management events in Windows 10, to view more on Windows Server 2016, **part 2** is here.

Author: Jeenali Kothari is a Digital Forensics enthusiast and enjoys technical content writing. You can reach her on **Here**