Incident Response: Windows Account Logon and logon Events

hackingarticles.in/incident-response-windows-account-logon-and-logon-events

Raj September 2, 2020

A user when authenticates a Windows endpoint, then an Account Logon event will be generated and will be recorded. These account logon events will be recorded in the Security event log of the system which will be responsible for authentication of the user.

On accessing an account for a resource, a Logon event will be recorded. These logon events will be recorded in the Security event log of the system being accessed.

As an incident responder, if you spot account logon events on a machine other than the Domain Controller, it could be a sign of local user account usage.

Local user account usage is abnormal on domain environments and can indicate a compromise

Table of Contents

Introduction

A windows system has various authentication and logon methods to establish remote sessions between different systems over a network. In this article, we will be learning about different account logon events and authentication protocols like Kerberos.

The methods of Windows authentication range from a simple logon-based thing depending on the user's knowledge like a password, tokens, public key certificates, and biometrics, etc.

An authentication protocol like Kerberos defines rules and conventions and serves the authentication of users, computers, and services. The process of authentication allows an authorized user and services and gives access to resources in a much secure way.

Logon Events

The Audit logon events are usually settings in the policy that records all attempts to log on to the local computer, whether by using a domain account or a local account. Audit Logon/Logoff events generate on the creation and destruction of logon sessions. These events occur on the machine that was accessed.

Account Logon

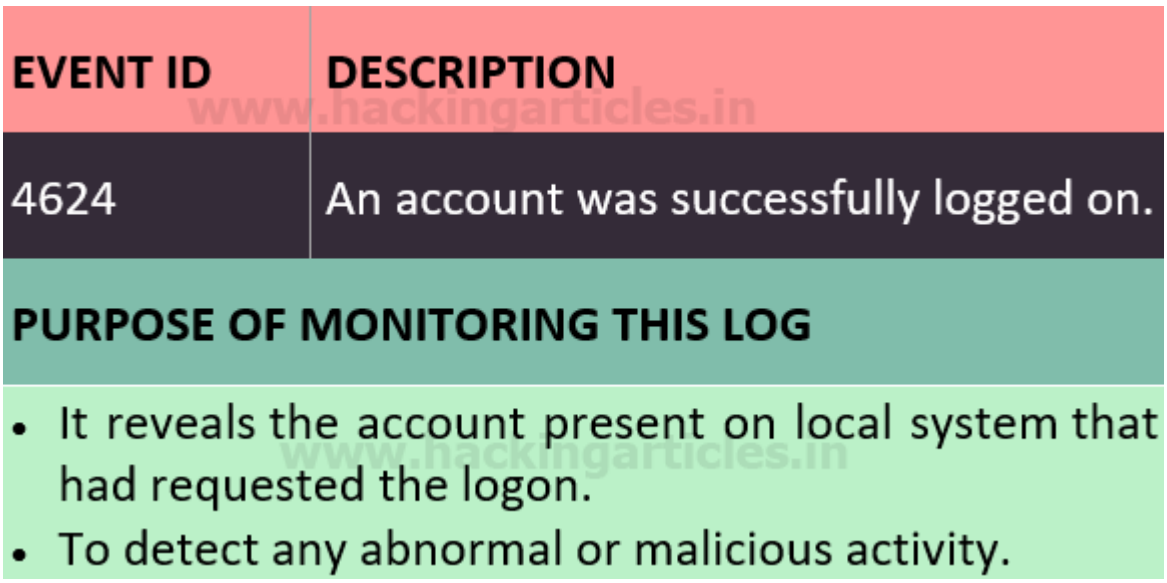
Account Logon policy setting generates events for any type of credential validation. These events occur on the machine that is authoritative for the credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local machine is authoritative.

So, let's see these event IDs one by one across the Windows server.

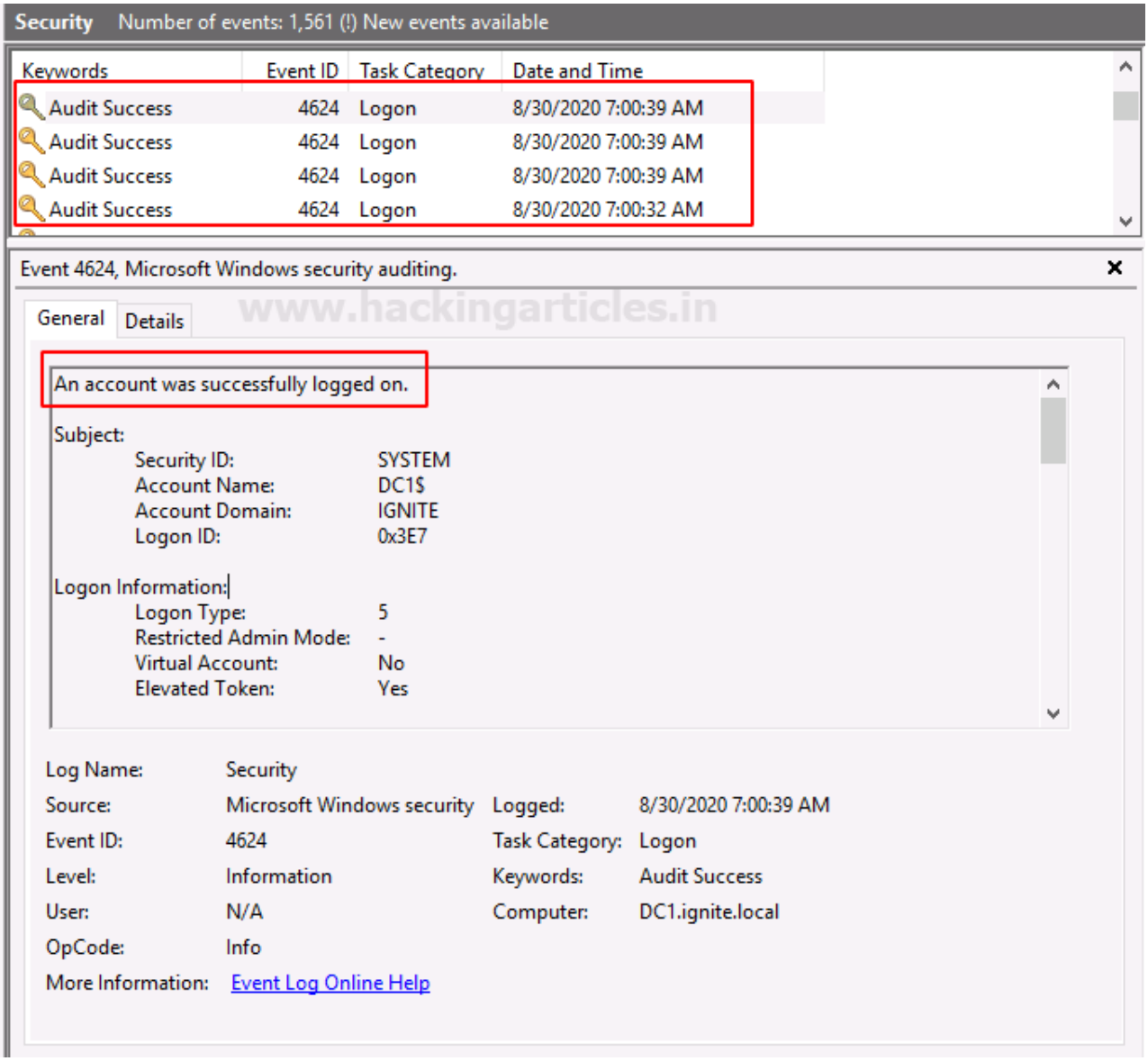
Event ID 4624

This event usually is generated for a successful logon. This event will contain information about the host and the name of the account involved. For remote logons, an incident responder should focus on the Network Information section of the event description for remote host information.

The fields Caller Process Name and Caller Process ID in the Process Information section of this event description provides more details about the process of initiating the logon.



When a user successfully logs on to a computer, this event will be generated.



Event ID 4625

This event is created on a failed logon attempt. Usually, these logs in a network may indicate password guessing attacks. The Network Information of this event can provide valuable information if a remote host is attempting to log on to the system.

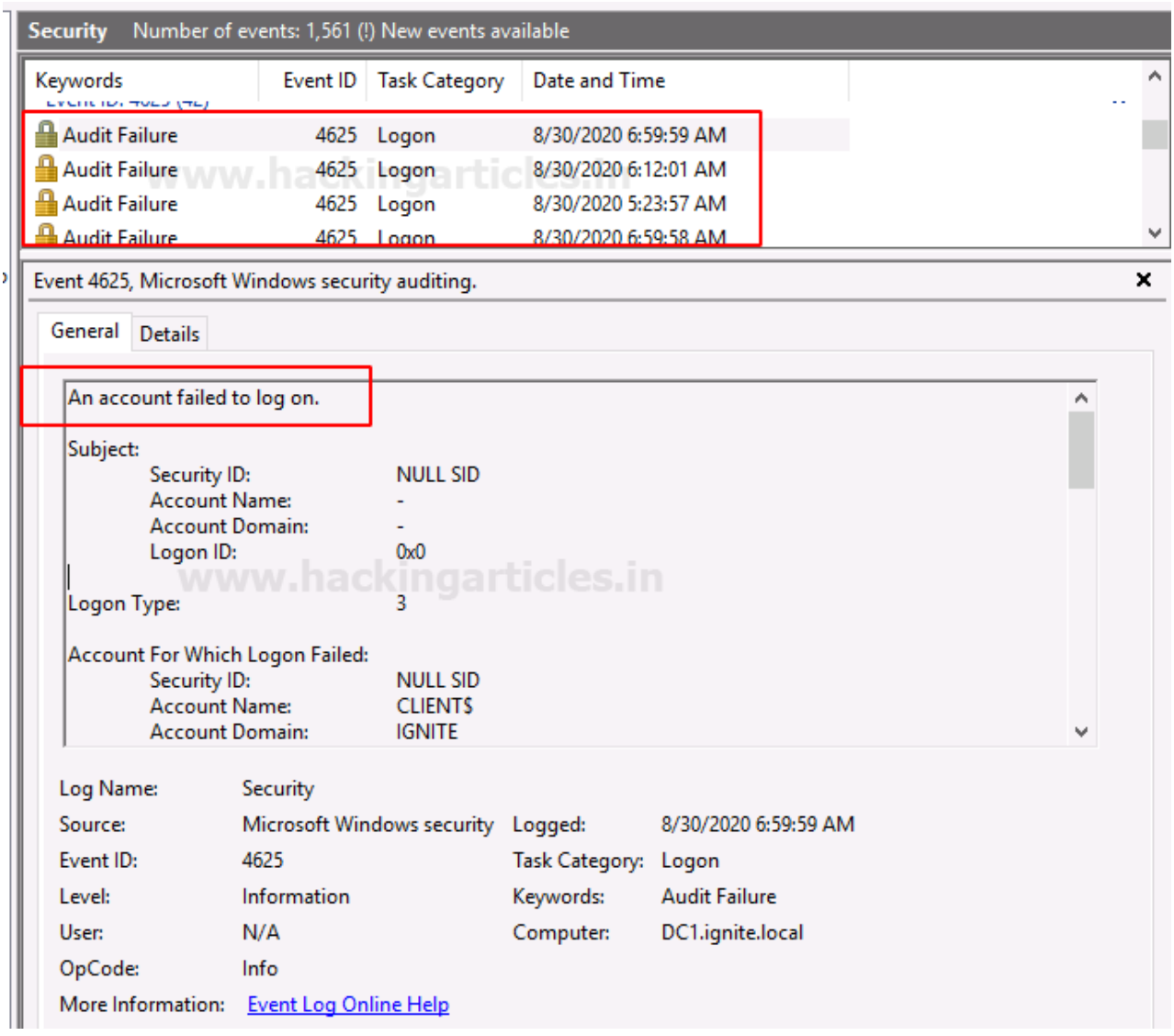
As an incident responder, you can determine more about the reason for the failure by going through the description.

EVENT ID	DESCRIPTION
4625	An account failed to log on.

PURPOSE OF MONITORING THIS LOG

- As it lists every failed attempt on the system that is regardless of logon type, user location or its account type.

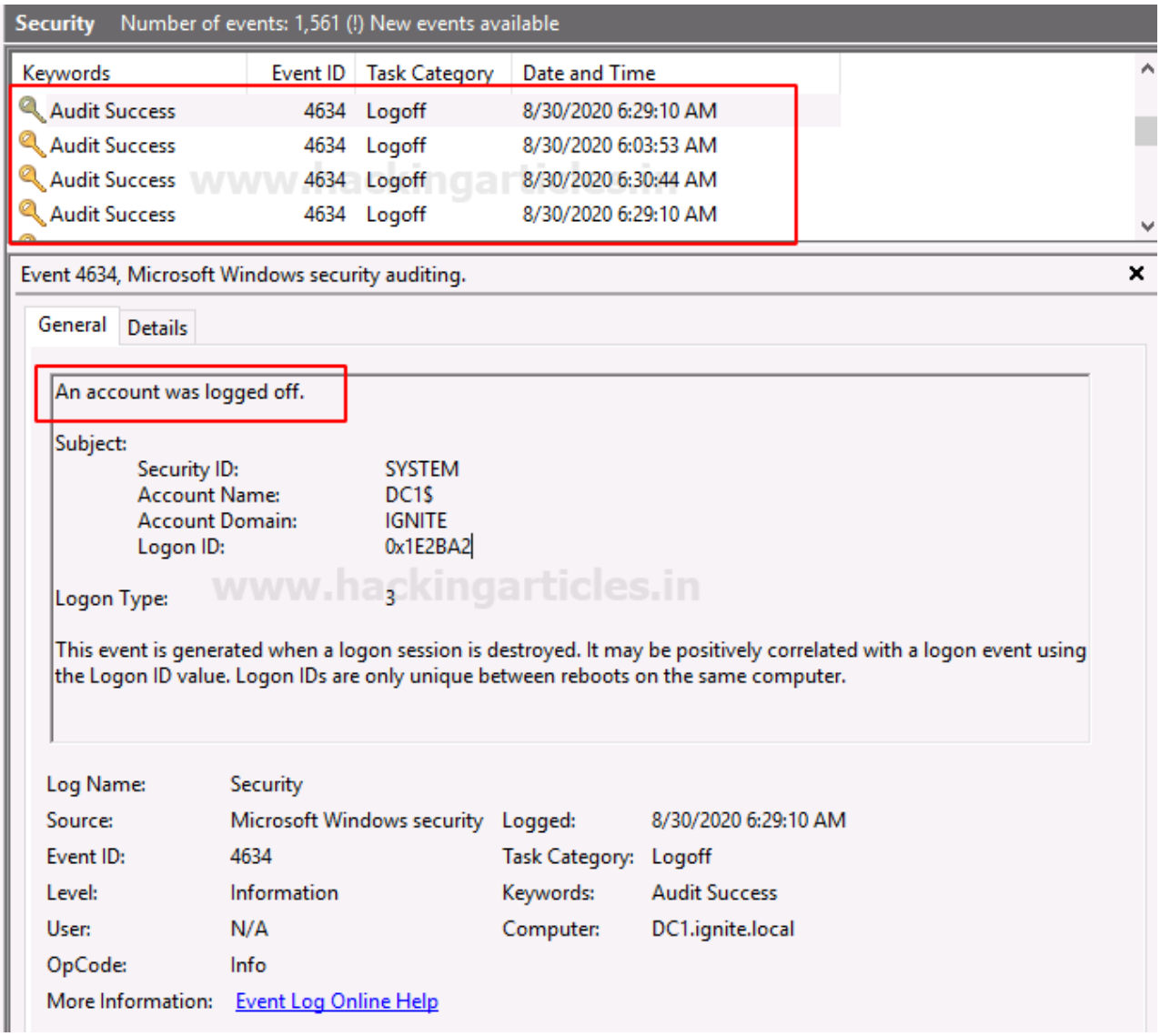
When a user has a failed login attempt on to a computer, this event will be generated.



Event ID 4634

When a user logs off from his system, it is recorded by Event ID 4634. If a system doesn't show an event showing a logoff, you as an incident responder you should not be considered overly suspicious.

EVENT ID	DESCRIPTION
4634	An account was logged off.
PURPOSE OF MONITORING THIS LOG	
It indicates the account logoff of a session including RDP.	



Event ID 4647

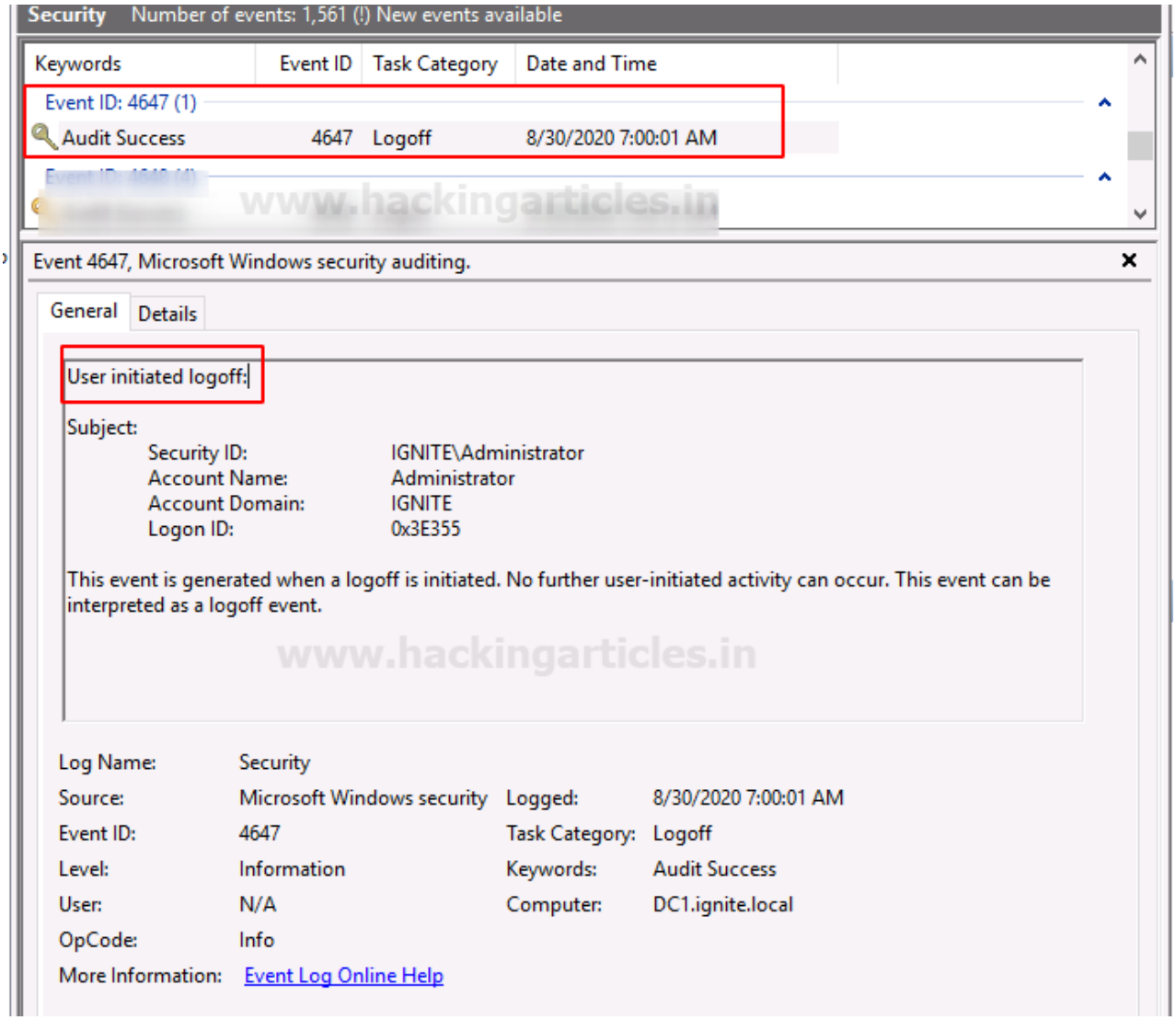
This event is usually triggered when no user-initiated activities no longer occur. This is different from event 4634, that is generally generated when a session no longer exists because of termination.

This event generates when a user logon is of remote type and the logoff was with some standard method.

EVENT ID	DESCRIPTION
4647	User initiated logoff.

PURPOSE OF MONITORING THIS LOG

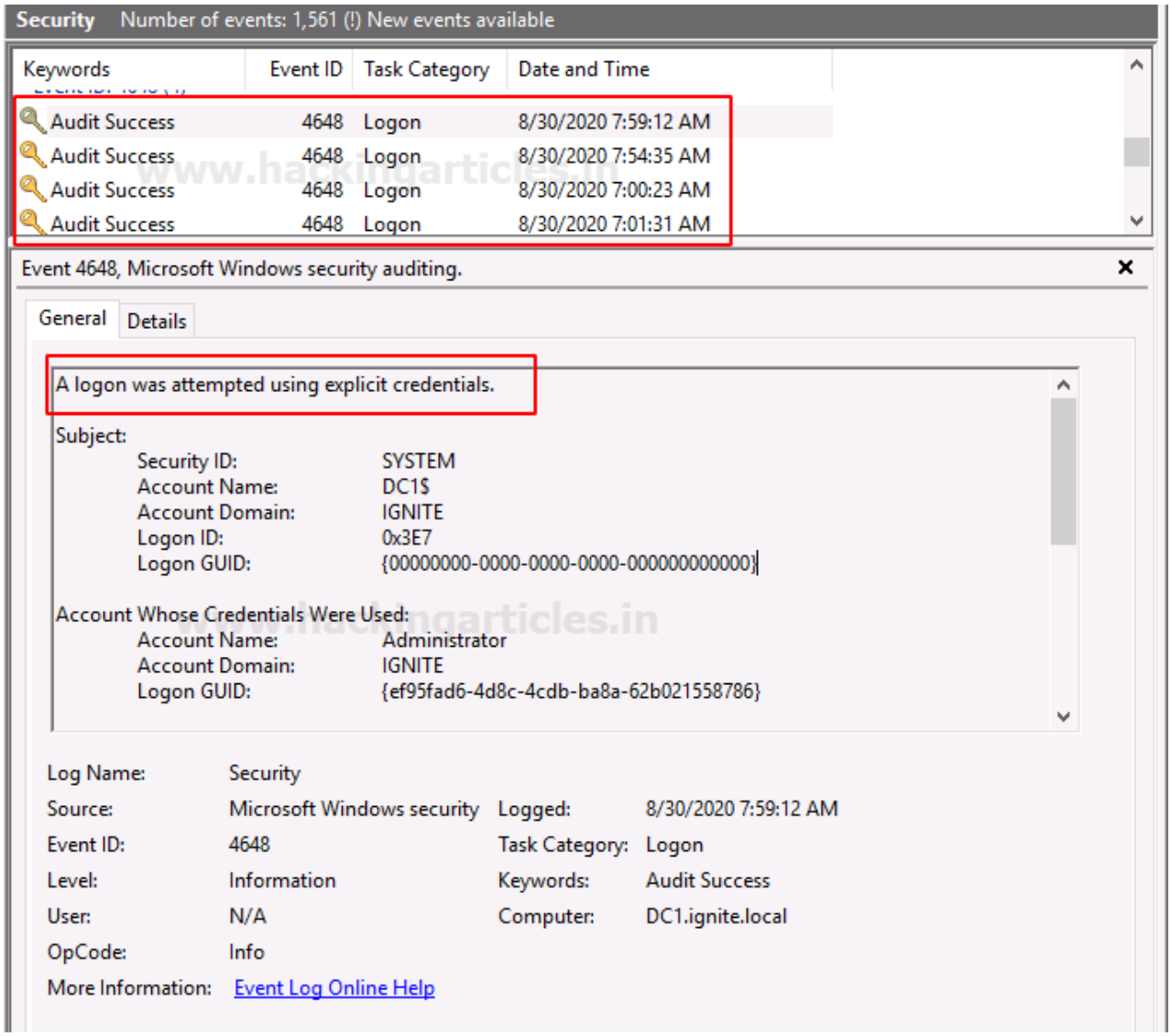
As it shows a difference between logs that result due to idle sessions and where a user himself logs off from his system.



Event ID 4648

A logon was attempted using explicit credentials. When a user attempts to use credentials that are of other than his, or if there is a user account control bypass to open a process with administrator permissions, this event is logged.

EVENT ID	DESCRIPTION
4648	A logon was attempted using explicit credentials.
PURPOSE OF MONITORING THIS LOG	
To keep an eye on processes in this event To monitor when and how a particular account is accessed. To monitor actions of high value accounts	



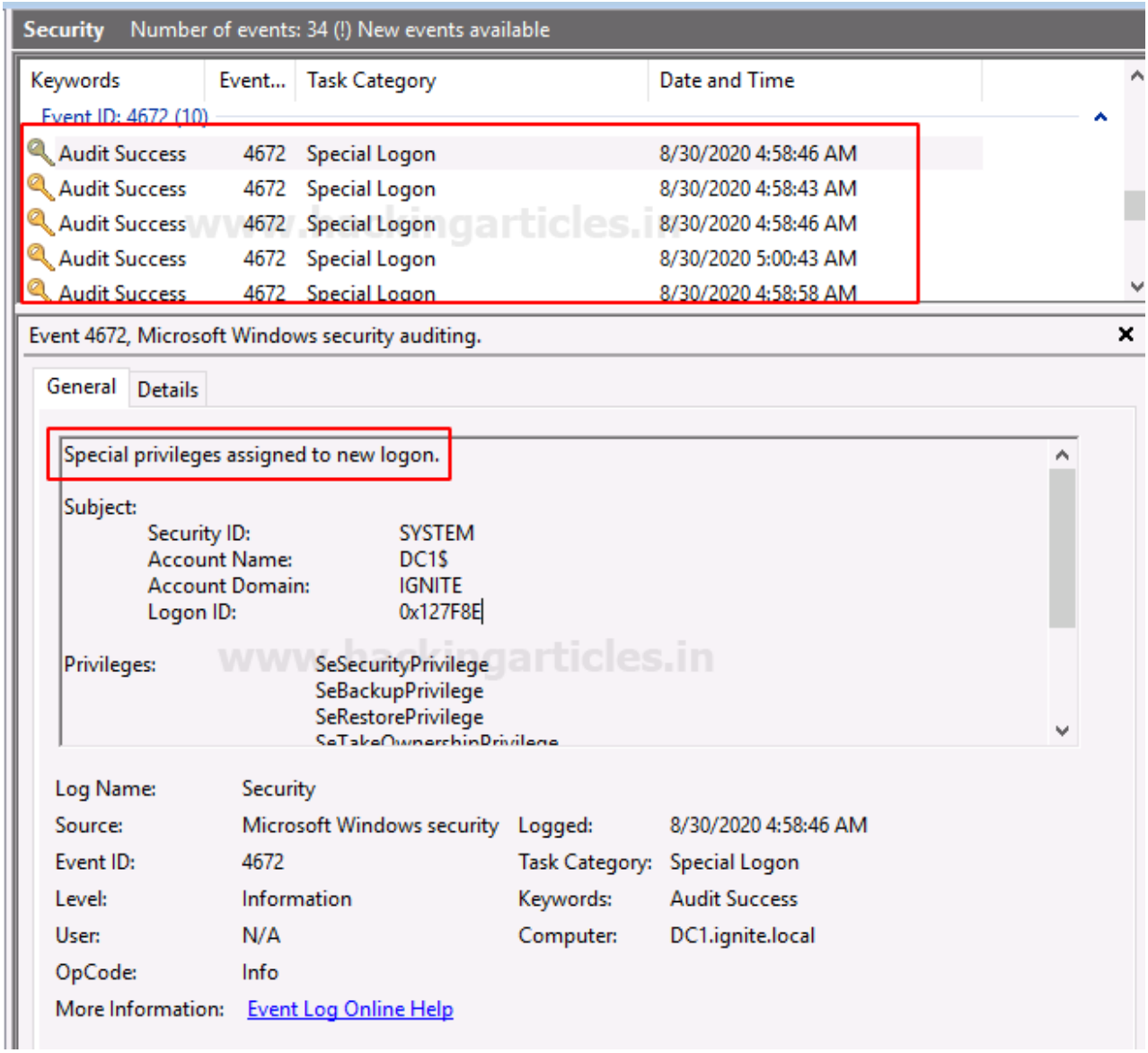
Event ID 4672

When a set of sensitive privileges are assigned to a new logon session, this event is generated for that particular new logon. This event is usually recorded in the event viewer as and when a single local system account logon triggers this event.

EVENT ID	DESCRIPTION
4672	Special privileges assigned to new logon.

PURPOSE OF MONITORING THIS LOG

- To make sure that certain privileges are never granted
- To monitor certain sensitive privileges.



Kerberos Authentication Protocol

Kerberos is an **authentication protocol** that works on the basis of tickets that allows the **nodes** to communicate over a non-secure network to prove their identity to each other in a secure manner.

So, let us understand the basics of Kerberos and then go ahead with Kerberos authentication protocol and the proceed with the event logs.

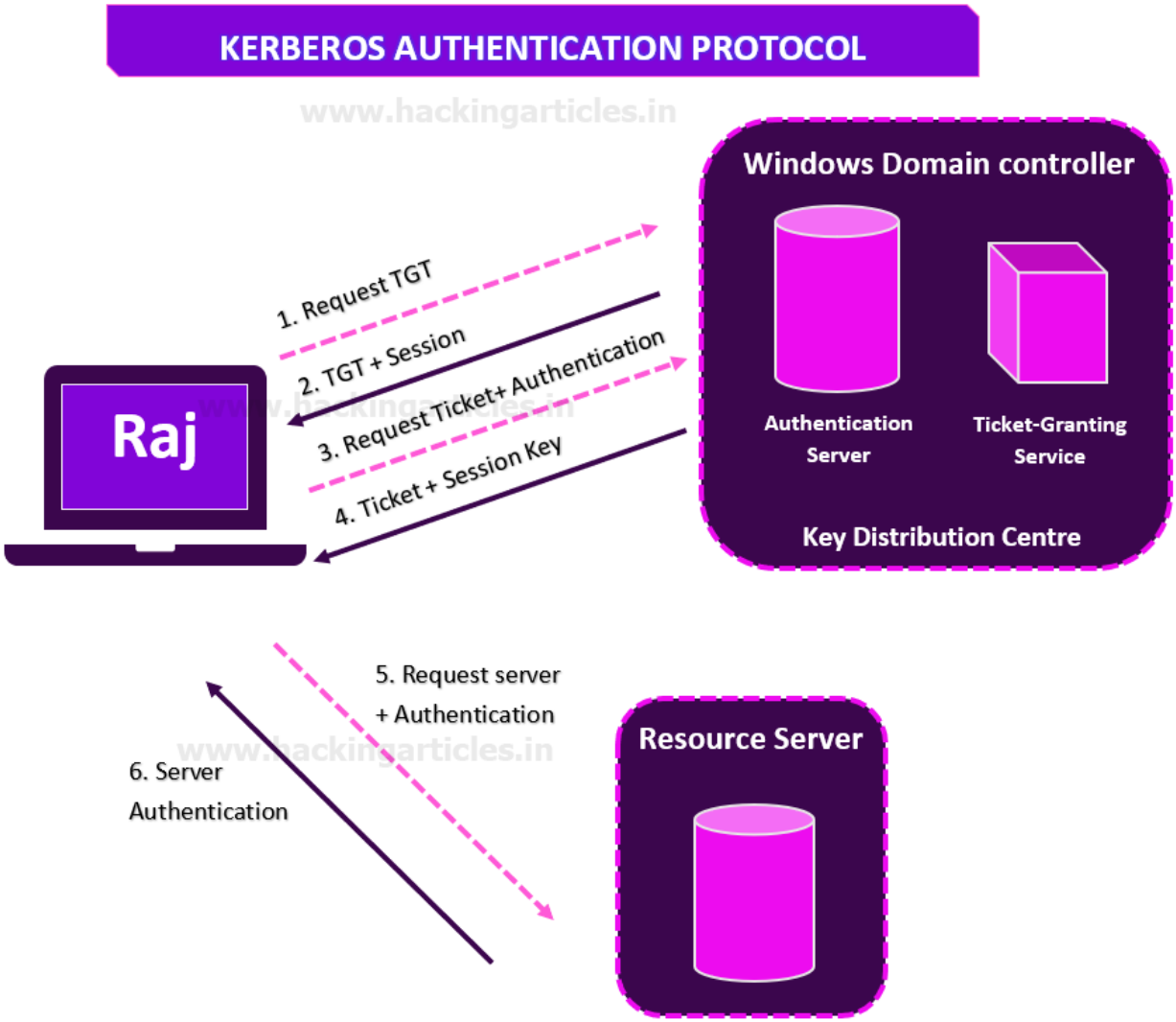
Client: A user that requests communication service request.

Resource Server: The server with the service the user wants to access.

Authentication Sever: It performs client authentication, issues TGS on successful authentication.

Key Distribution Centre: Database, Authentication Server and Ticket Granting Server collectively is called Key Distribution Centre.

Ticket Granting Server: It is an application server that provides the issuing of service tickets as a service.



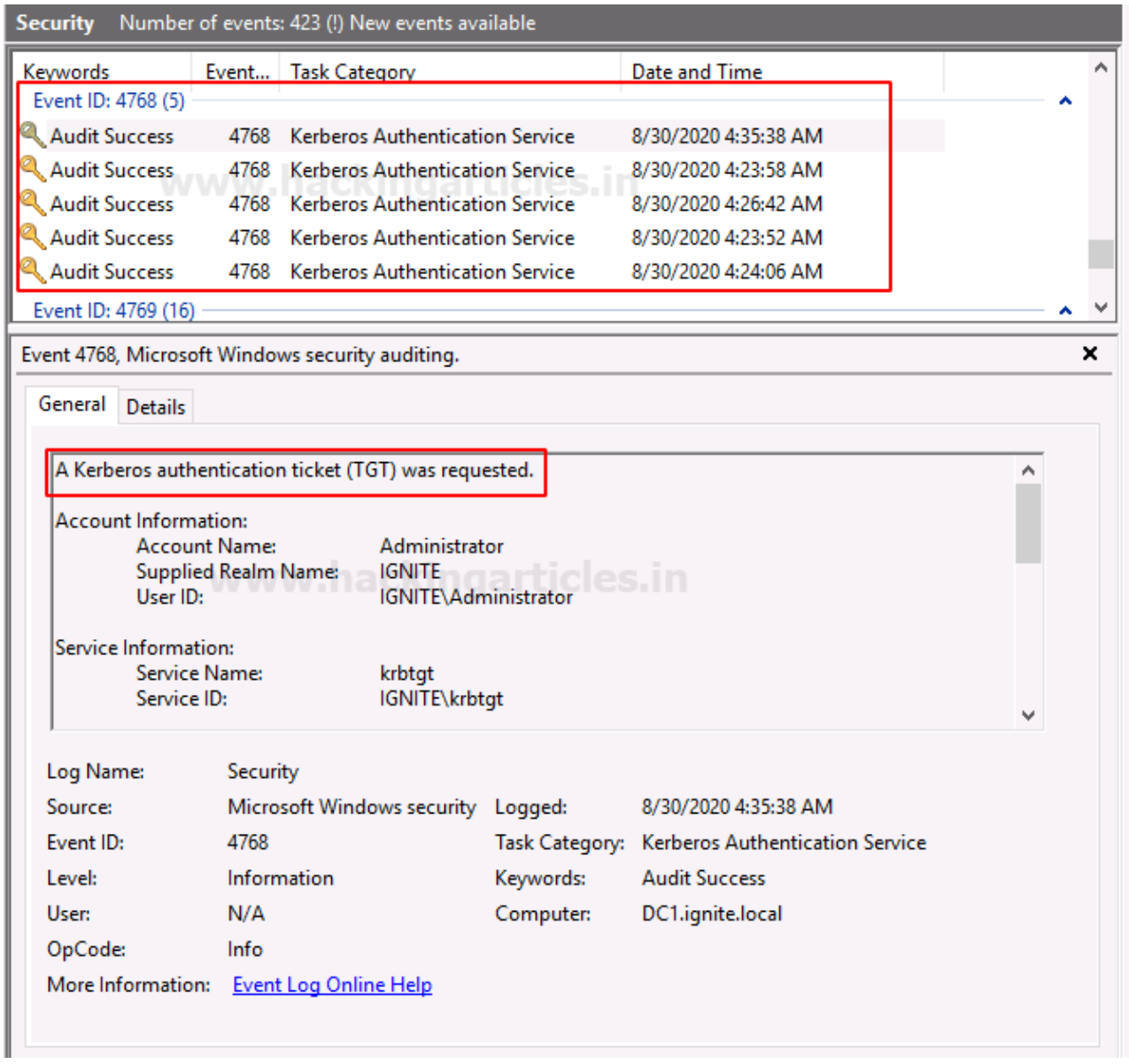
Event ID 4768

On successful issuance of a TGT, it will show that a user account was authenticated by the domain controller. The Keywords field would indicate whether the authentication attempt was successful or failed.

EVENT ID	DESCRIPTION
4768	A Kerberos service ticket (TGT)was requested.

PURPOSE OF MONITORING THIS LOG

- To keep a watch on accounts whose Account Name corresponds with high-value accounts, that includes administrators, built-in local administrators, domain administrators, and service accounts.



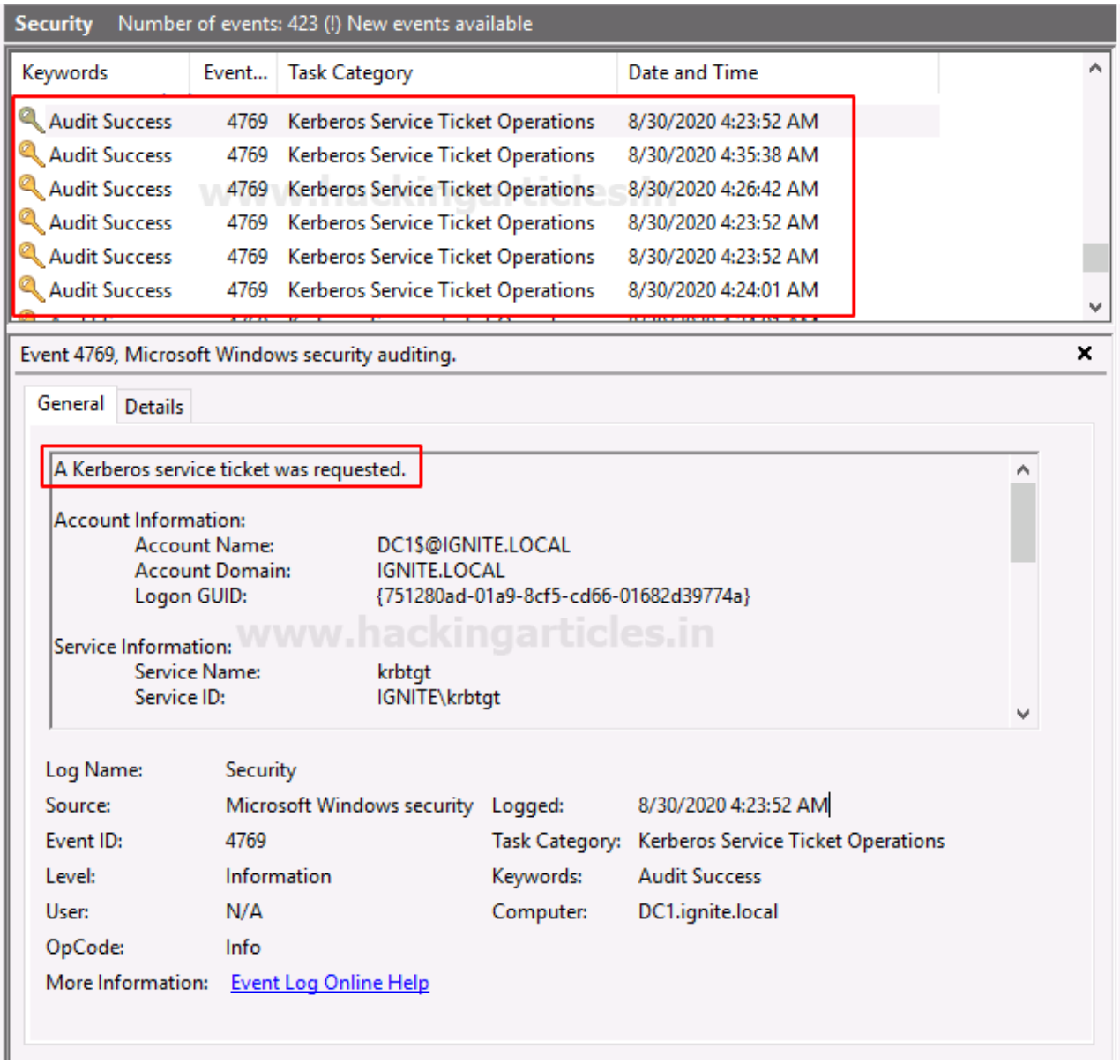
Event ID 4769

Once the client successfully receives a ticket-granting ticket from the KDC, it will store that TGT and send it to the TGS with the Service Principal Name (SPN) of the resource that the client wants to access. TGTs are valid for a certain period of time only.

EVENT ID	DESCRIPTION
4769	A Kerberos service ticket was requested.

PURPOSE OF MONITORING THIS LOG

- To keep a track of logon attempts that are outside an internal IP range.



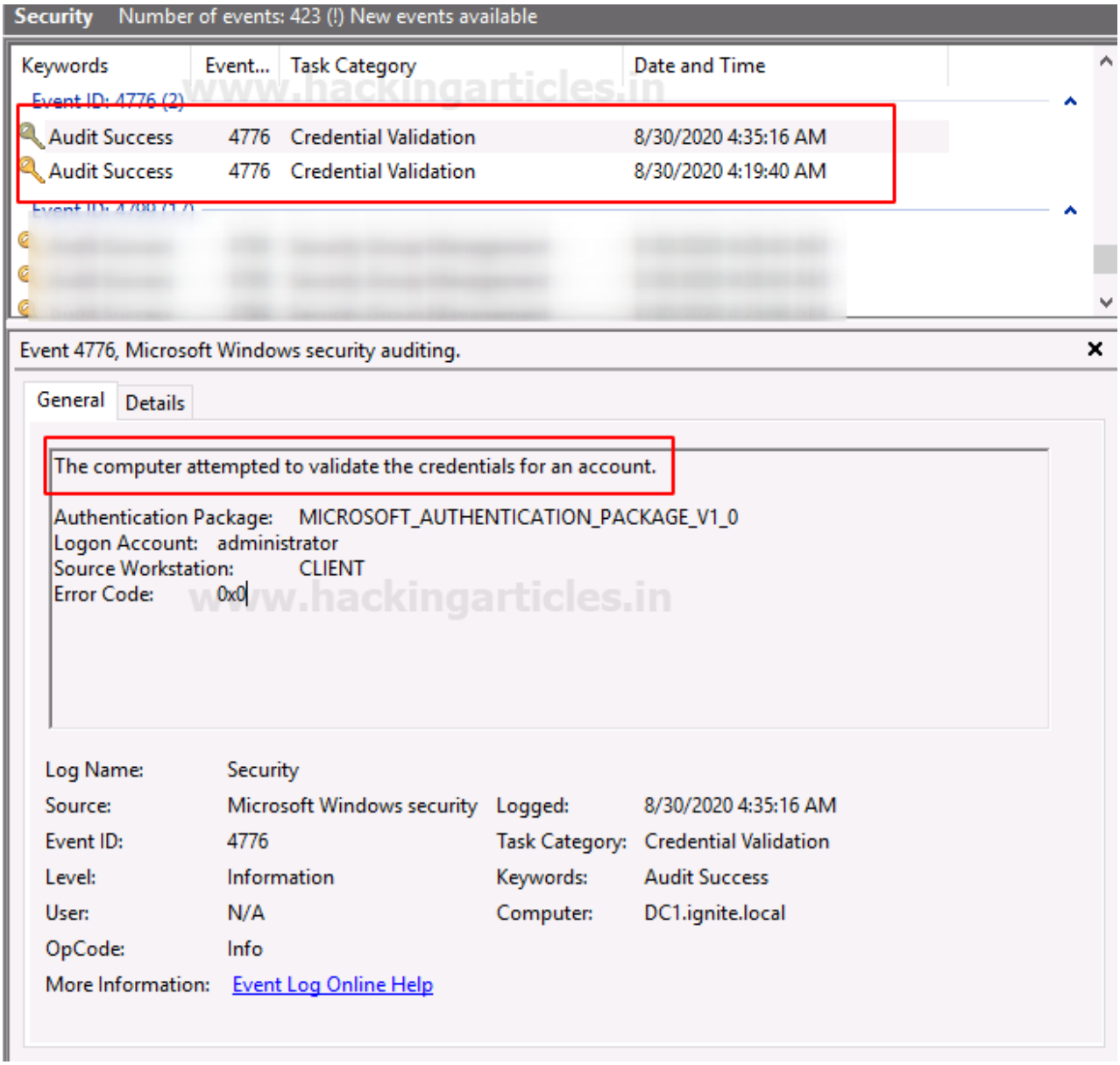
Event ID 4776

When the computer logon is to be verified, this even is created. It contains additional information about the remote host in the event of a remote logon attempt. The Keywords field indicates whether the authentication attempt succeeded or failed

EVENT ID	DESCRIPTION
4776	The computer attempted to validate the credentials for an account.

PURPOSE OF MONITORING THIS LOG

- To identify multiple logons attempts with to check for brute-force attacks on your network.
- To check for attempts from unauthorized endpoints, or attempts outside of business hours, with malicious intent for high-value accounts



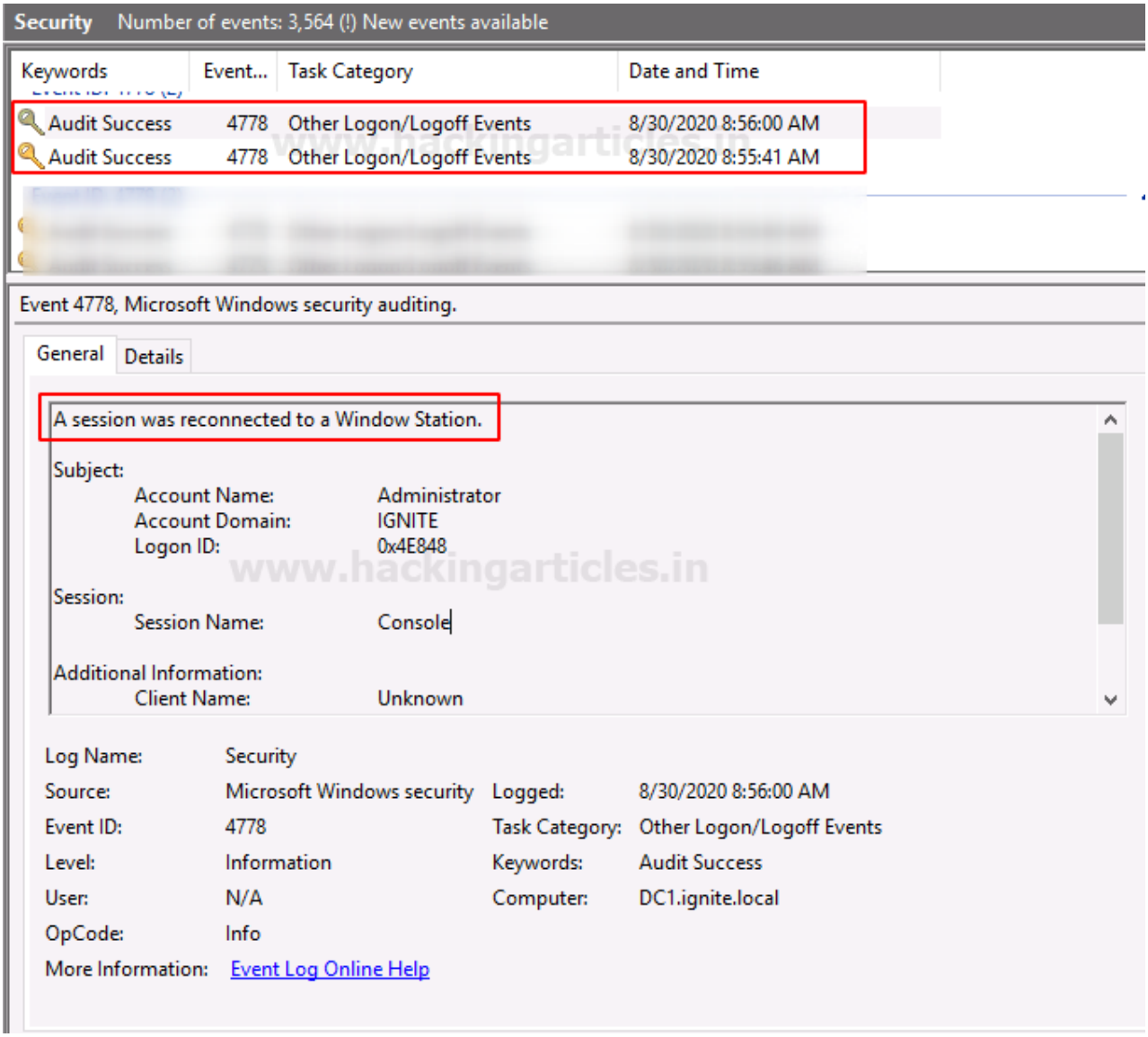
Event ID 4778

This event is created when a session is reconnected to a Windows station. If a user reconnects with an existing Terminal Services session, or switches to an existing desktop using Fast User Switching, event 4778 is generated. This event is also triggered when a user reconnects to a virtual host.

EVENT ID	DESCRIPTION
4778	A session was reconnected to a Window Station.

PURPOSE OF MONITORING THIS LOG

- To check on sessions when Fast User Switching has been disabled
- To keep an eye when remote desktop connections are not allowed for certain users.



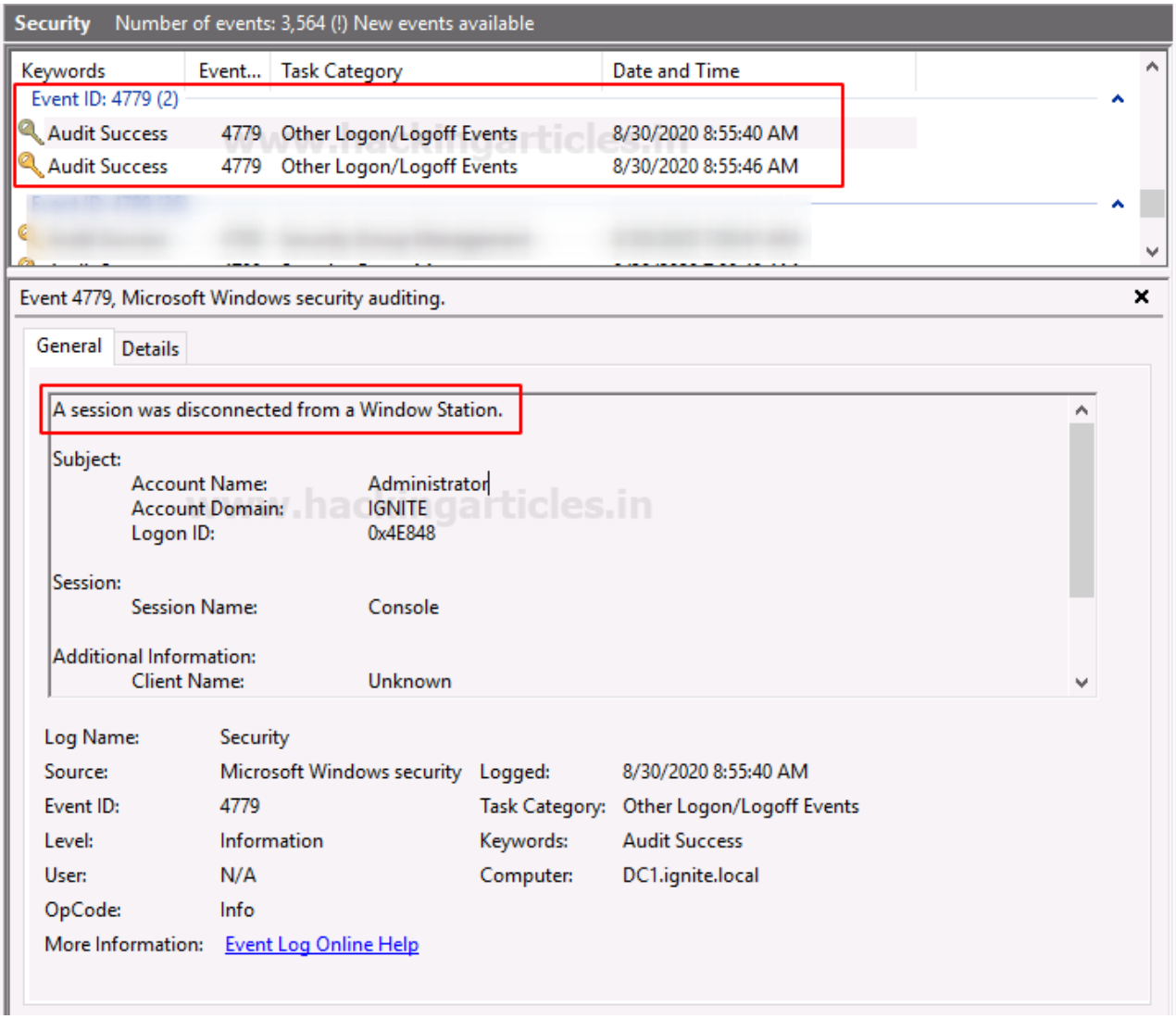
Event ID 4779

If a user disconnects from an existing Terminal Services session, or switches away from an existing desktop using Fast User Switching, this event is generated. This event is also created when a user disconnects from a virtual host.

EVENT ID	DESCRIPTION
4779	A session was disconnected from a Window Station.

PURPOSE OF MONITORING THIS LOG

- To make sure that non-active, external or any restricted accounts are not used.
- To make sure that only specific accounts can perform certain actions.



You can also try out some other event ID's from below.

EVENT ID	DESCRIPTION
4770	A service ticket was renewed. The account name, service name, client IP address, and encryption type are recorded.
4771	Kerberos pre-authentication failed.
4772	A Kerberos authentication ticket request failed.
4773	A Kerberos service ticket request failed.

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