



**National Forensic  
Sciences University**  
**Knowledge | Wisdom | Fulfilment**  
**An Institution of National Importance**  
**(Ministry of Home Affairs, Government of India)**

**M.Tech. Artificial Intelligence & Data Science  
(Specialization in Cyber Security)**

**School of Cyber Security and Digital Forensics**

**Incident Response and Audit Compliances  
Laboratory**

**Lab practical Work**

**Semester: 1**

**Session: 2024-25**

**Date: 16/12/2024**

**Submitted to**

**Mr. Prakash Khasor Sir**

**Submitted by**

**Pratham Badge**

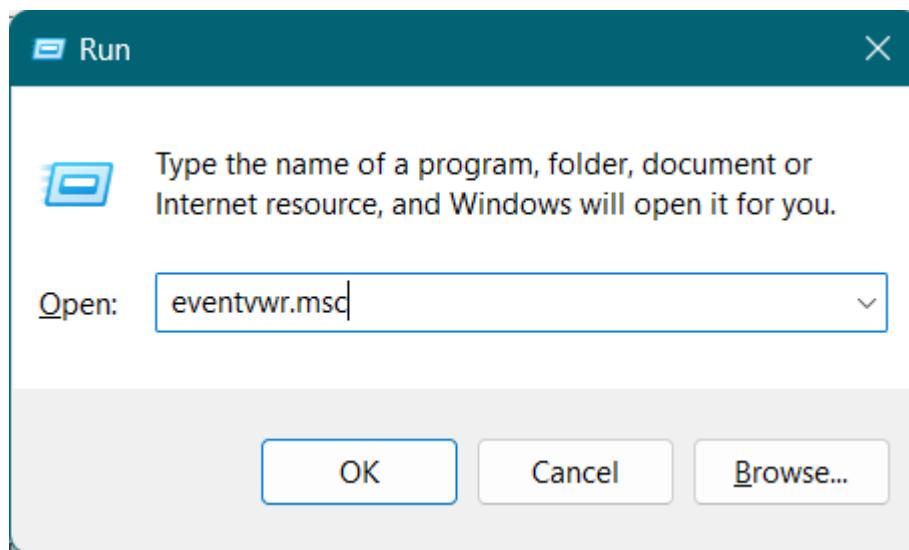
# Windows Event Viewer Practical Tasks

## Practical 1: Basic Navigation and Event Filtering

**Objective:** Understand how to navigate and filter events in the Event Viewer.

### Steps:

1. Open Event Viewer (`eventvwr.msc` via the Run dialog).

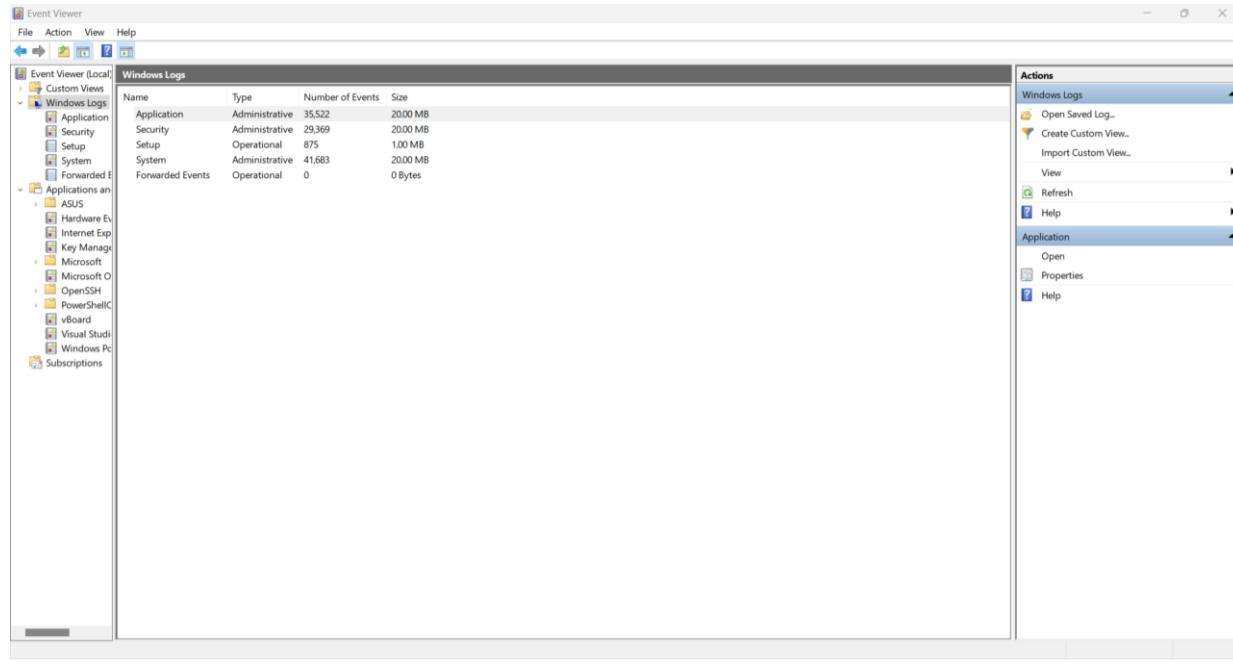
A screenshot of the Event Viewer (Local) application window. The menu bar includes File, Action, View, and Help. The left sidebar shows nodes like Event Viewer (Local), Custom Views, Windows Logs, Applications and Services, and Subscriptions. The main area has several panes:

- Overview and Summary:** Displays a summary of administrative events. A table shows counts for Critical, Error, Warning, Information, and Audit Success events over the last hour, 24 hours, and 7 days.
- Log Summary:** Shows log details for Windows PowerShell, Visual Studio, vBoard, System, and Security logs.
- Actions:** A list of actions including Open Saved Log..., Create Custom View..., Import Custom View..., Connect to Another Computer..., View, Refresh, and Help.

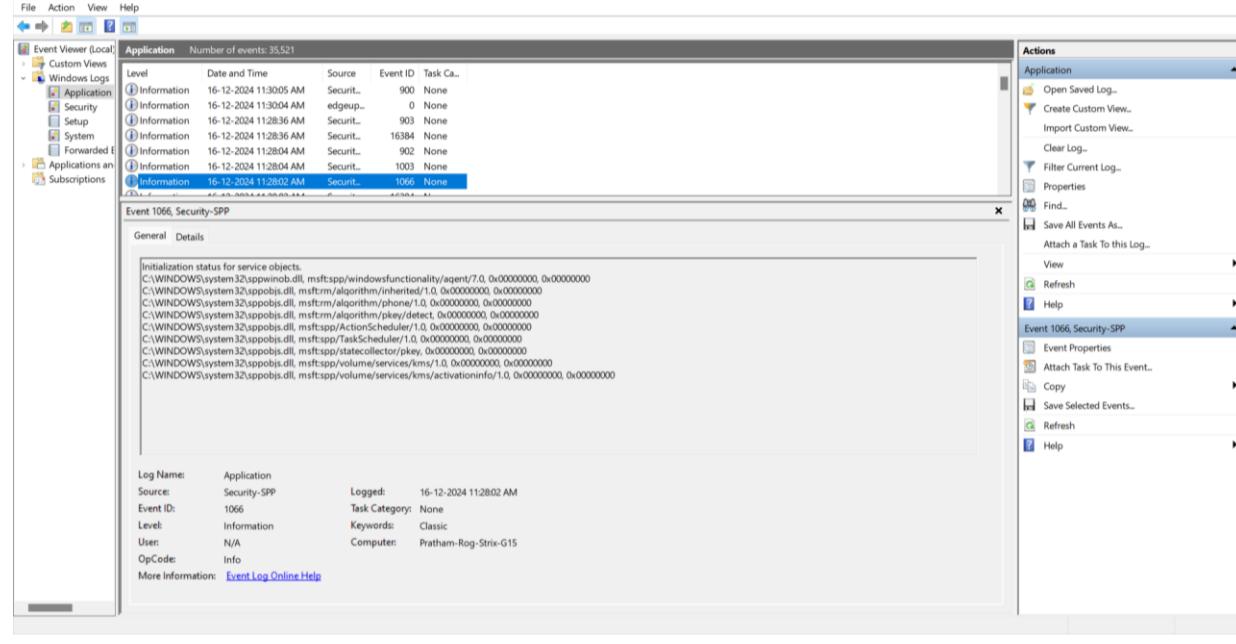
The "Recently Viewed Nodes" pane lists nodes like Windows Logs\Security, Windows Logs\Application, Applications and Services, Custom Views\Kibana, and Custom Views\Google.

## 2. Explore the main sections:

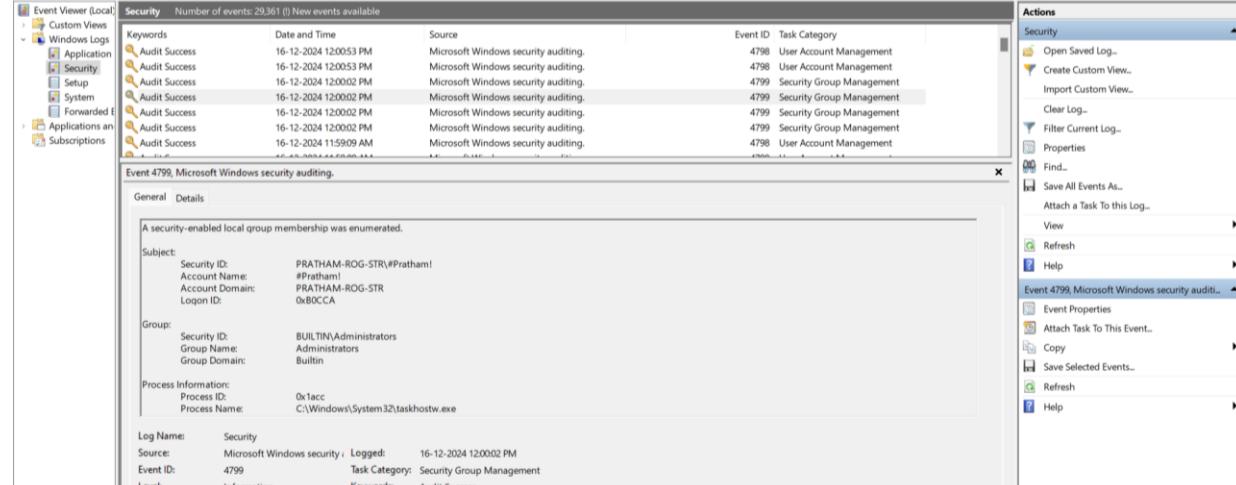
### 2.1. - Windows Logs (Application, Security, System, etc.)



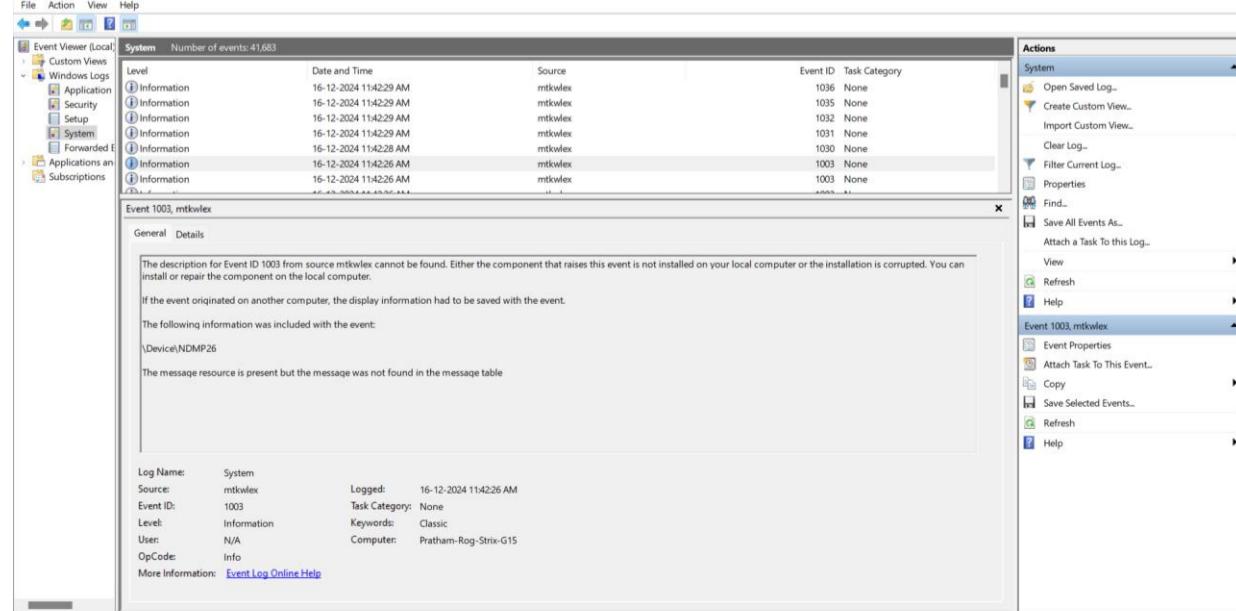
#### 2.1.1. Application



#### 2.1.2. Security



#### 2.1.3. System



## 2.2. - Applications and Services Logs.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of log sources, and the right pane shows a detailed list of events for the selected log source.

**Event Viewer (Local)**

**File Action View Help**

**Applications and Services Logs**

**Name Type Number of Events Size**

Name	Type	Number of Events	Size
ASUS			
Hardware Events	Administrative	0	68 KB
Internet Explorer	Administrative	0	68 KB
Key Management Service	Administrative	0	68 KB
Microsoft			
Microsoft Office Alerts	Administrative	2,255	1.00 MB
OpenSSH	Folder		
PowerShellCore	Folder		
vBoard	Administrative	21	68 KB
Visual Studio	Administrative	0	68 KB
Windows PowerShell	Administrative	10,175	15.00 MB

**Actions**

**Applications and Services Logs**

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- View
- Refresh
- Help

**ASUS**

- Open
- Help

### 3. Select System Logs and filter by:

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of log sources, including Event Viewer (Local), Custom View, Server Roles, Windows Logs, Applications, and Subscriptions. The Windows Logs node is expanded, showing categories like Application, Security, Setup, System, Forwarded Events, and Applications. The System category is selected, showing a list of 41,683 events. The right pane shows a detailed view of event 1014, titled "Event 1014, DNS Client Events". The event details are as follows:

Level	Date and Time	Source	Event ID	Task Category
Warning	16-12-2024 12:03:28 PM	DNS Client Events	1014	(1014)
Information	16-12-2024 12:00:00 PM	EventLog	6013	None
Information	16-12-2024 11:59:21 AM	Service Control Manager	7040	None
Information	16-12-2024 11:56:56 AM	Service Control Manager	7040	None
Warning	16-12-2024 11:56:56 AM	DistributedCOM	10016	None
Warning	16-12-2024 11:45:15 AM	DistributedCOM	10016	None
Information	16-12-2024 11:42:27 AM	mktwlex	1050	None

The event details pane shows the following information for event 1014:

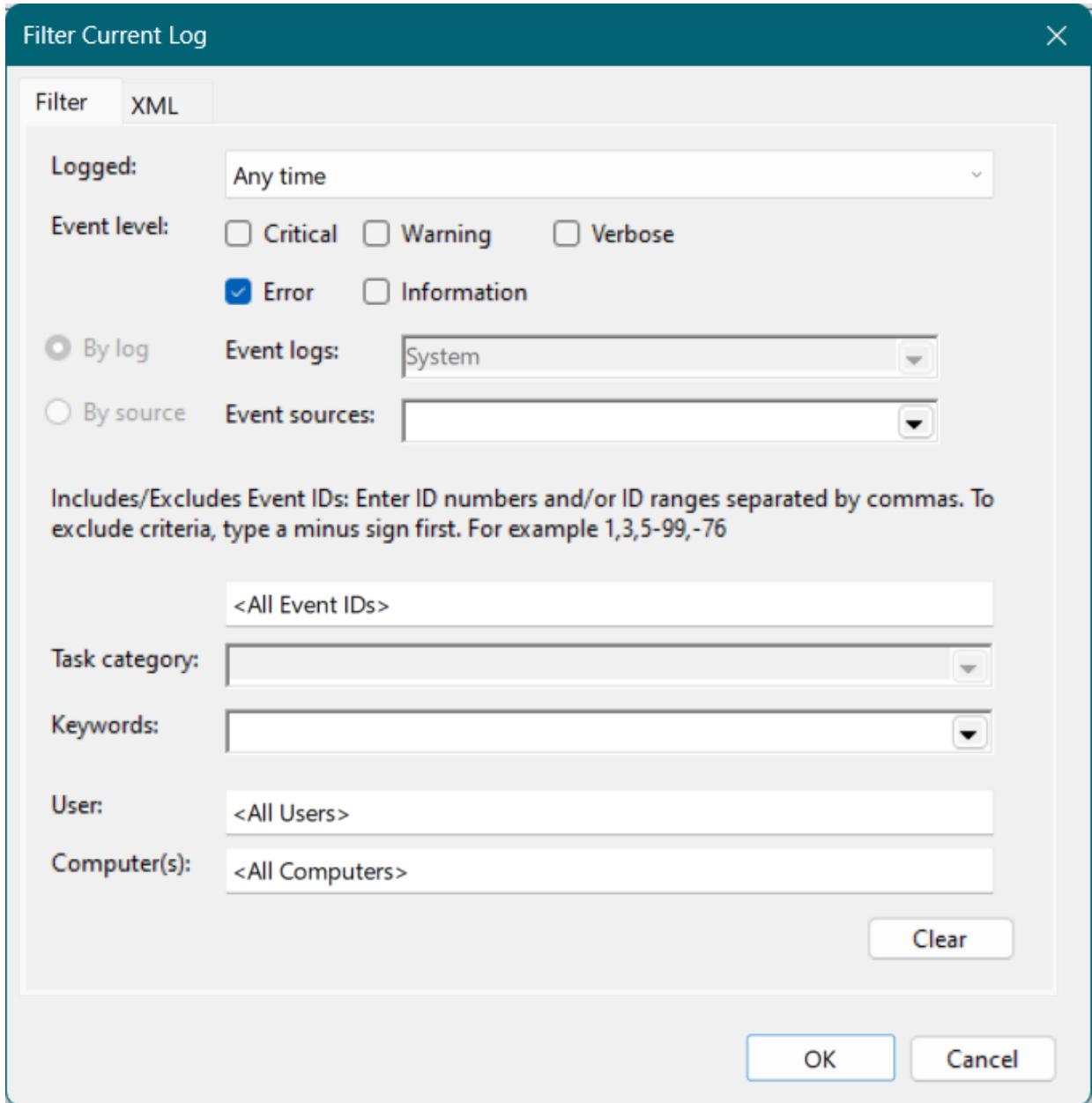
Name resolution for the name t-ring-fdv2.msedge.net timed out after none of the configured DNS servers responded. Client PID 9648.

Log Name: System  
Source: DNS Client Events  
Event ID: 1014  
Level: Warning  
User: NETWORK SERVICE  
OpCode: Info  
More Information: [Event Log Online Help](#)

The Actions pane on the right lists various options for managing events, including Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To this Log..., View, Refresh, Help, Event Properties, Attach Task To This Event..., Copy, Save Selected Events..., Refresh, and Help.

### 3.1. Event Level (e.g., Errors or Warnings).

#### 3.1.1. Error



The screenshot shows the Event Viewer main window. The left pane displays a tree view of event logs: Event Viewer (Local), Windows Logs (Application, Security, System), Applications and Services Logs (ASUS, Hardware Events, Internet Explorer, Key Management, Microsoft, OpenSSH, PowerShell, vBoard, Visual Studio, Windows PowerShell, Subscriptions). The 'System' log is selected. The right pane shows a table of filtered events:

Level	Date and Time	Source	Event ID	Task Category
Error	11-12-2024 04:01:37 PM	NetBT	4321	None
Error	11-12-2024 04:01:21 PM	Tcpip	4207	None
Error	11-12-2024 04:01:21 PM	Tcpip	4207	None
Error	11-12-2024 04:00:42 PM	NetBT	4321	None
Error	11-12-2024 04:00:30 PM	Tcpip	4207	None
Error	11-12-2024 04:00:30 PM	Tcpip	4207	None

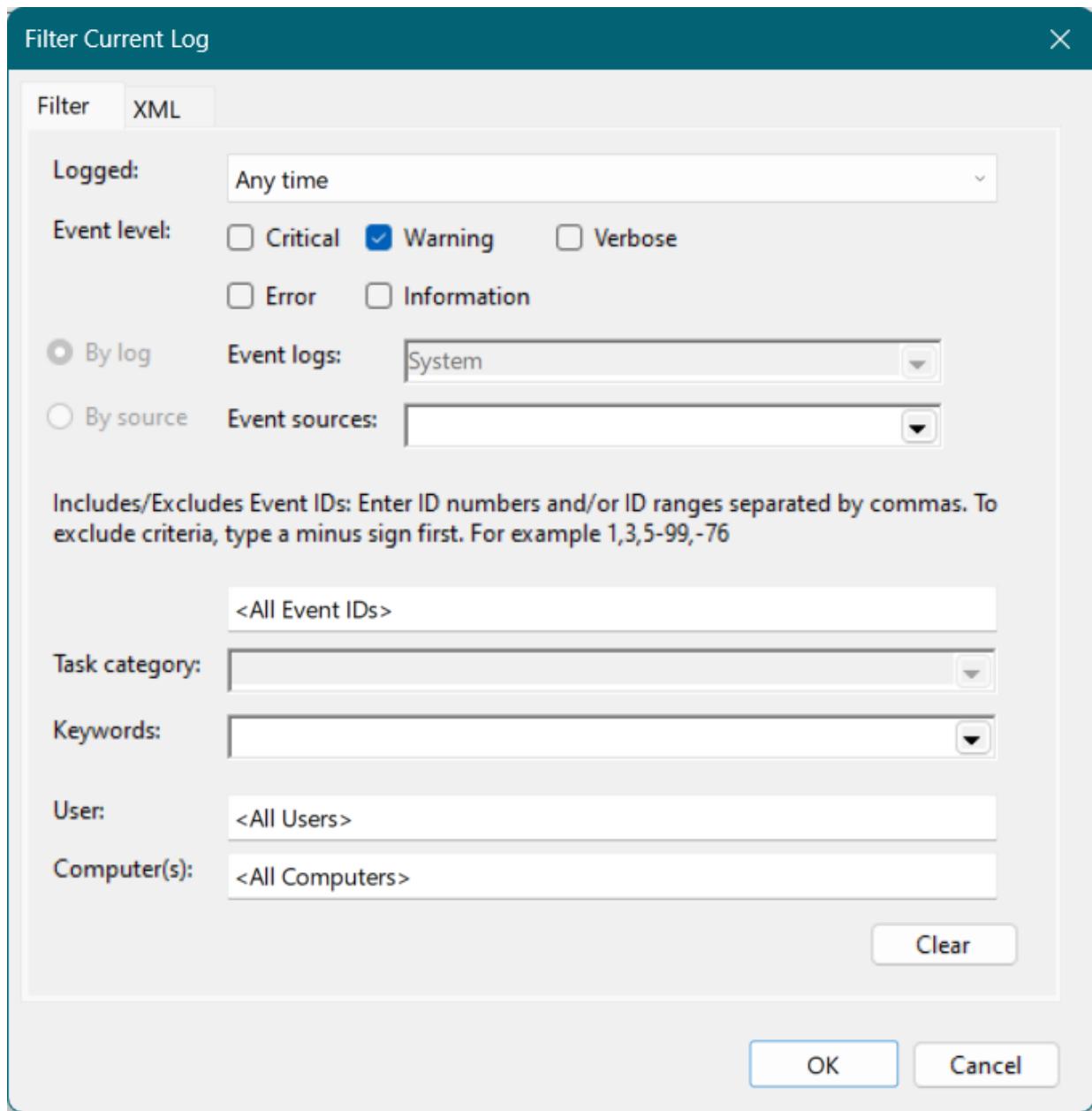
A tooltip for the last event says: 'The IPv4 TCP/IP interface with index 11 failed to bind to its provider.' Below the table, detailed information for the last event is shown:

Event 4207, Tcpip  
General Details  
The IPv4 TCP/IP interface with index 11 failed to bind to its provider.

Log Name: System  
Source: Tcpip  
Event ID: 4207  
Level: Error  
User: N/A  
OpCode: Info

Event Properties  
Attach Task To This Event...  
Copy  
Save Selected Events...  
Refresh  
Help

### 3.1.2. Warnings



The screenshot shows the main Event Viewer window. The left pane displays a tree view of logs and views, with 'System' selected. The center pane shows a table of events:

Level	Date and Time	Source	Event ID	Task Category
Warning	16-12-2024 12:03:28 PM	DNS Client Events	1014	(1014)
Warning	16-12-2024 11:56:56 AM	DistributedCOM	10016	None
Warning	16-12-2024 11:45:15 AM	DistributedCOM	10016	None
Warning	16-12-2024 11:42:26 AM	WLAN-AutoConfig	10002	None
Warning	16-12-2024 11:42:19 AM	WLAN-AutoConfig	4003	None
Warning	16-12-2024 11:31:17 AM	WLAN-AutoConfig	10002	None

The status bar at the bottom left says 'Creates a filter.' The right pane contains an 'Actions' menu with various options like Open Saved Log, Create Custom View, and Help.

### 3.2. - Time period (e.g., last 24 hours).

**Filter Current Log**

Filter XML

Logged: Last 24 hours

Event level:  Critical  Warning  Verbose  
 Error  Information

By log Event logs: System

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

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

**Clear**

**OK** **Cancel**

**Event Viewer**

File Action View Help

System Number of events: 41,683

Filtered: Log: System; Source: Date Range: Last 24 hours. Number of events: 1,489

Level	Date and Time	Source	Event ID	Task Category
Information	15-12-2024 12:33:27 PM	Service Control Manager	7040	None
Information	15-12-2024 12:31:25 PM	Kernel-Power	506	(157)
Information	15-12-2024 12:31:25 PM	Kernel-Power	566	(268)
Information	15-12-2024 12:25:58 PM	WindowsUpdateClient	19	Windows Update Agent
Information	15-12-2024 12:25:51 PM	WindowsUpdateClient	43	Windows Update Agent
Information	15-12-2024 12:25:51 PM	WindowsUpdateClient	44	Windows Update Agent

Event 44, WindowsUpdateClient

General Details

Windows Update started downloading an update.

Log Name: System  
Source: WindowsUpdateClient  
Event ID: 44  
Level: Information  
User: SYSTEM  
OpCode: Download  
More Information: [Event Log Online Help](#)

Actions

- System
  - Open Saved Log...
  - Create Custom View...
  - Import Custom View...
  - Clear Log...
  - Filter Current Log...
  - Clear Filter
  - Properties
  - Find...
  - Save Filtered Log File As...
  - Attach a Task To This Log...
  - Save Filter to Custom View...
  - View
  - Refresh
  - Help
- Event 44, WindowsUpdateClient
  - Event Properties
  - Attach Task To This Event...
  - Copy
  - Save Selected Events...
  - Refresh
  - Help

4. Note down a critical or warning event, including the event ID and description.

The screenshot shows the Windows Event Viewer interface. In the center, a table lists five warning events from the System log. The first event, with Event ID 4003, is highlighted. A detailed view of this event is shown in a modal window. The modal window has tabs for General and Details. The General tab shows the event details: Log Name: System, Source: WLAN-AutoConfig, Logged: 16-12-2024 11:42:19 AM, Event ID: 4003, Task Category: None, Level: Warning, Keywords: {536870912}, User: SYSTEM, Computer: Pratham-Rog-Strix-G15, and OpCode: Info. The Details tab contains the event description: "WLAN AutoConfig detected limited connectivity, attempting automatic recovery." Below the modal, the Actions pane is open, showing various options like Open Saved Log..., Create Custom View..., Import Custom View..., and Save Filter to Custom View... for the selected event.

## Warning Event

**Event ID:** 4003

**Description:**

**WLAN AutoConfig detected limited connectivity, attempting automatic recovery.**

**Recovery Type:** 4

**Error Code:** 0x0

**Trigger Reason:** 5

**IP Family:** 0

5. **Outcome:** Learn how to filter and identify specific events.

# Practical 2: Analyze Boot and Shutdown Events

**Objective:** Track system boot and shutdown activities.

## Steps:

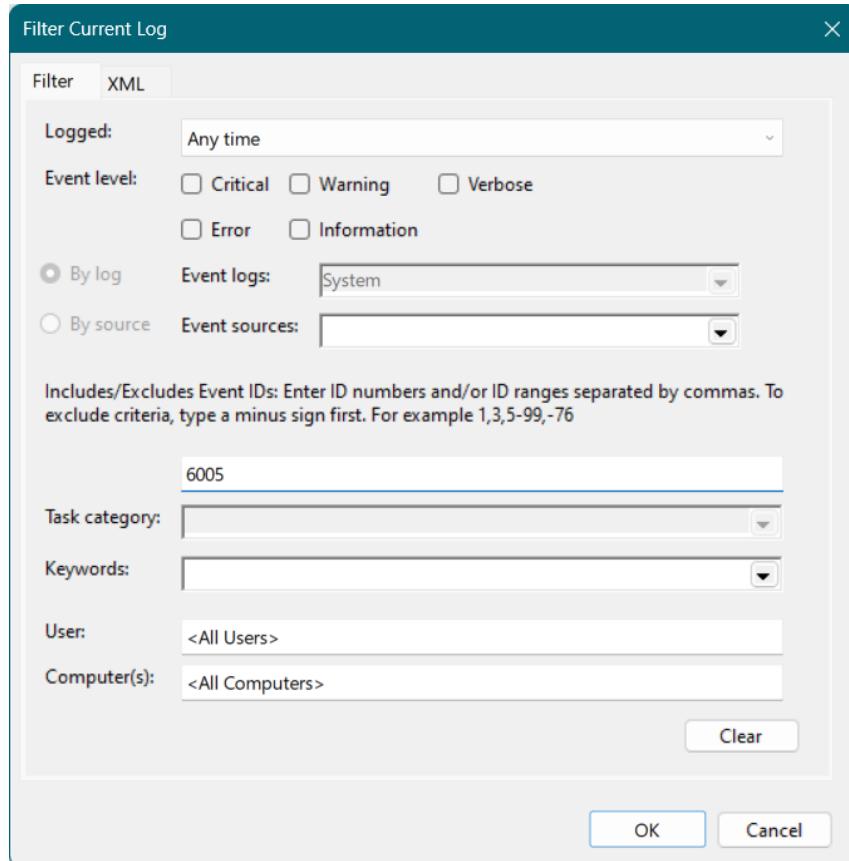
1. Navigate to Windows Logs > System.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Custom Views, Windows Logs (selected), Application, Security, Setup, System (selected), Forwarded Events, Applications and Services, and Subscriptions. The right pane shows the System log with 41,683 events. A specific event, Event 1014, is selected. The details pane shows the event information: General tab (Event ID: 1014, Source: DNS Client Events, Level: Warning, Date and Time: 16-12-2024 12:03:28 PM) and Details tab (Message: Name resolution for the name t-ring-fdv2.msedge.net timed out after none of the configured DNS servers responded. Client PID 9648). The bottom pane provides event properties: Log Name: System, Source: DNS Client Events, Event ID: 1014, Task Category: (1014), Level: Warning, User: NETWORK SERVICE, OpCode: Info, Logged: 16-12-2024 12:03:28 PM, Task ID: (268435456), Computer: Pratham-Rog-Strix-G15, and Keywords: (268435456). The Actions pane on the right lists various options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To This Log..., View, Refresh, Help, Event Properties, Attach Task To This Event..., Save Selected Events..., Copy, Refresh, and Help.

Level	Date and Time	Source	Event ID	Task Category
Warning	16-12-2024 12:03:28 PM	DNS Client Events	1014 (1014)	
Information	16-12-2024 12:00:00 PM	EventLog	6013	None
Information	16-12-2024 11:59:21 AM	Service Control Manager	7040	None
Information	16-12-2024 11:56:56 AM	Service Control Manager	7040	None
Warning	16-12-2024 11:56:56 AM	DistributedCOM	10016	None
Warning	16-12-2024 11:48:15 AM	DistributedCOM	10016	None
Information	16-12-2024 11:48:27 AM	mktwlex	1090	None

**2. Use the following Event IDs to filter:**

**2.1. 6005: System Startup.**



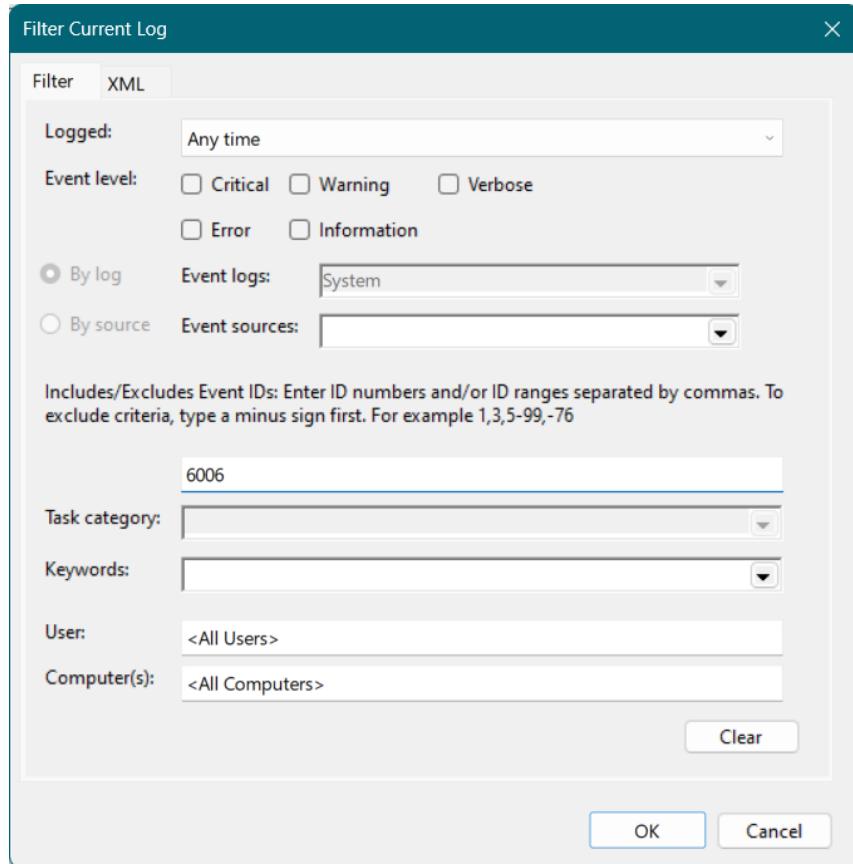
The Event Viewer window shows a filtered list of events for 'System' log, source 'EventLog', and event ID 6005. There are 12 events listed, all of level 'Information' occurring between 16-12-2024 09:48:18 AM and 14:12-2024 06:37:00 PM. The details pane shows the message 'The Event log service was started.' The properties pane shows the following details:

Log Name:	System
Source:	EventLog
Event ID:	6005
Level:	Information
User:	N/A
OpCode:	Info

Event ID: 6005, EventLog  
General Details  
The Event log service was started.

Actions pane includes: Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Clear Filter, Properties, Find..., Save Filter to Custom View..., Refresh, Help, Event 6005, EventLog, Event Properties, Attach Task To This Event..., Save Selected Events..., Copy, Refresh, Help.

## 2.2. 6006: System Shutdown.



The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (Application, Setup, System, Forwarded Events, Applications and Services, Subscriptions), and Security. The 'System' node under 'Windows Logs' is selected, showing 'Number of events: 41,683'. A filter bar indicates: 'Filtered: Log: System; Source: ; Event ID: 6006. Number of events: 112'. The main pane lists 112 events for 'Event 6006, EventLog'. The first few entries are:

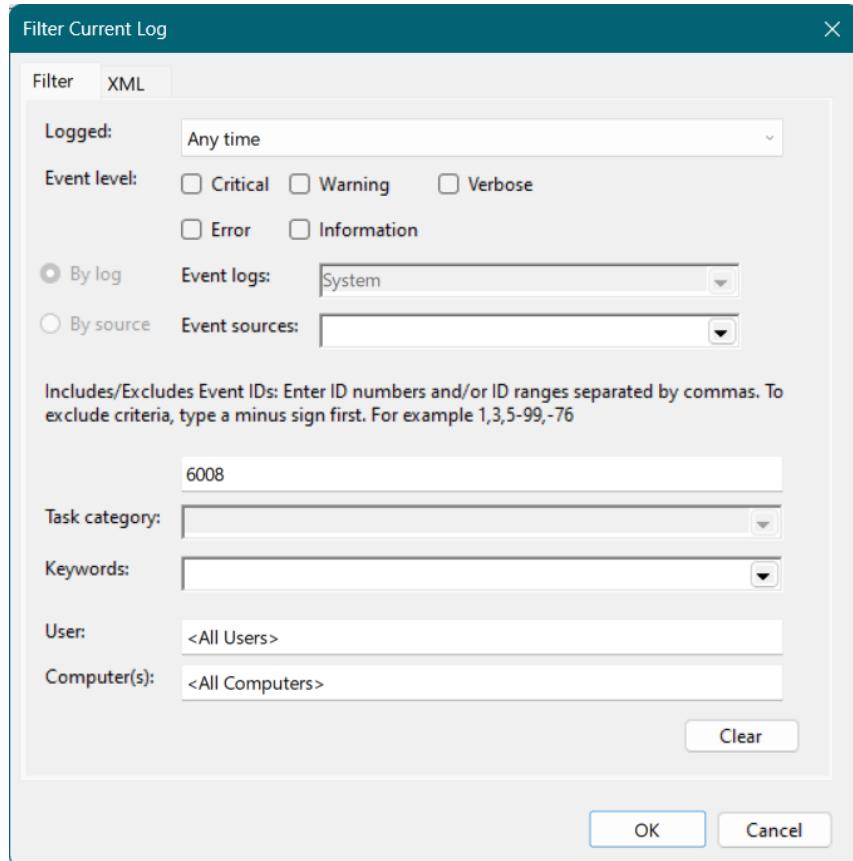
Level	Date and Time	Source	Event ID	Task Category
Information	16-12-2024 10:23:04 AM	EventLog	6006	None
Information	16-12-2024 01:36:21 AM	EventLog	6006	None
Information	15-12-2024 03:16:53 AM	EventLog	6006	None
Information	14-12-2024 11:46:48 PM	EventLog	6006	None
Information	14-12-2024 09:22:20 PM	EventLog	6006	None
Information	14-12-2024 06:03:45 PM	EventLog	6006	None

A details window for 'Event 6006, EventLog' is open, showing the message: 'The Event log service was stopped.' The 'General' tab displays event properties:

Log Name:	System
Source:	EventLog
Event ID:	6006
Level:	Information
User:	N/A
OpCode:	Info
More Information: <a href="#">Event Log Online Help</a>	

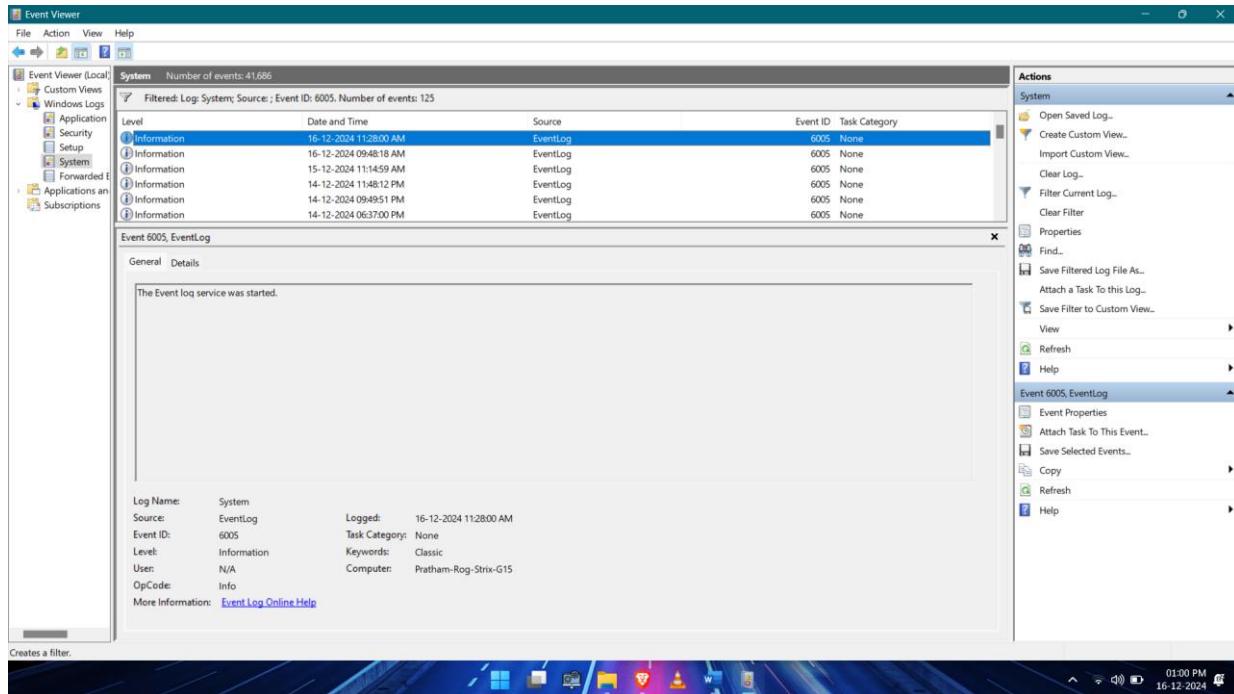
The right pane shows the 'Actions' menu with options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Clear Filter, Properties, Find..., Save Filter to Custom View..., Refresh, Help, Event 6006, EventLog, Event Properties, Attach Task To This Event..., Save Selected Events..., Copy, Refresh, and Help.

## 2.3. 6008: Unexpected Shutdown.



The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (Application, Setup, System, Forwarded Events, Subscriptions), Applications and Services Logs, and Security. The 'System' node under 'Windows Logs' is selected, showing 'Number of events: 41,683'. A sub-view for 'Event 6008, EventLog' is open, showing a list of events with columns: Level, Date and Time, Source, Event ID, and Task Category. All listed events are of level 'Error' and occurred on 13-12-2024. The first event is highlighted. The right pane is titled 'Actions' and lists various options: Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Clear Filter, Properties, Find..., Save Filtered Log File As..., Attach a Task to This Log..., Save Filter to Custom View..., View, Refresh, Help, Event 6008, EventLog, Event Properties, Attach Task To This Event..., Save Selected Events..., Copy, Refresh, and Help. At the bottom left of the main window, there is a note: 'Creates a filter.'

### 3. Analyze the timestamps to identify system uptime.



System Startup Time: 16-12-2024 11:28:00 AM

Current Time 16-12-2024 01:00:00 PM

System Uptime: 1 hour 32 minutes

#### 4. Document any abnormal shutdowns with their descriptions.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Custom Views, Windows Logs (Application, Security, Setup, System, Forwarded), Applications and Subscriptions. The right pane shows a table of events under the 'System' category. A filter is applied: Log: System; Source: EventLog; Event ID: 6006. The table has columns: Level, Date and Time, Source, Event ID, and Task Category. Six entries are listed, all with Level Information, Source EventLog, Event ID 6006, and Task Category None. The first entry's details are expanded, showing the message 'The Event log service was stopped.' and the event properties: Log Name: System, Source: EventLog, Logged: 16-12-2024 10:23:04 AM, Task Category: None, Level: Information, Keywords: Classic, User: N/A, Computer: Pratham-Rog-Strix-G15, and OpCode: Info. The Actions pane on the right lists various options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Save Filter to Custom View..., and Help.

Level	Date and Time	Source	Event ID	Task Category
Information	16-12-2024 10:23:04 AM	EventLog	6006	None
Information	16-12-2024 01:36:21 AM	EventLog	6006	None
Information	15-12-2024 03:16:53 AM	EventLog	6006	None
Information	14-12-2024 11:46:48 PM	EventLog	6006	None
Information	14-12-2024 09:22:20 PM	EventLog	6006	None
Information	14-12-2024 06:03:45 PM	EventLog	6006	None

**Event ID:** 6006

**Logged:** 16-12-2024 10:23:04 AM

**Description:** The Event log service was stopped.

#### 5. Outcome: Understand how to monitor system startup and shutdown activities.

## Practical 3: Audit Logon Events

**Objective:** Monitor user logon and logoff events.

**Steps:**

1. Navigate to Windows Logs > Security.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Windows Logs (Application, Security, Setup, System, Forwarded Events, Applications and Services, Subscriptions), and Custom Views. The right pane shows the Security log with 29,402 events. A specific event is selected, highlighted in blue. The event details are as follows:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	16-12-2024 01:11:09 PM	Microsoft Windows security auditing.	4798	User Account Management
Audit Success	16-12-2024 01:11:09 PM	Microsoft Windows security auditing.	4798	User Account Management
Audit Success	16-12-2024 01:07:48 PM	Microsoft Windows security auditing.	4798	User Account Management
Audit Success	16-12-2024 01:07:48 PM	Microsoft Windows security auditing.	4798	User Account Management
Audit Success	16-12-2024 01:04:37 PM	Microsoft Windows security auditing.	4798	User Account Management
Audit Success	16-12-2024 01:04:37 PM	Microsoft Windows security auditing.	4798	User Account Management
Audit Success	16-12-2024 01:04:03 PM	Microsoft Windows security auditing.	5379	User Account Management

The detailed view for Event 4798, Microsoft Windows security audit, shows the following information:

**General**

A user's local group membership was enumerated.

**Subject:**

Security ID:	SYSTEM
Account Name:	PRATHAM-ROG-STR\\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

**User:**

Security ID:	PRATHAM-ROG-STR\#Pratham!
Account Name:	#Pratham!
Account Domain:	PRATHAM-ROG-STR

**Process Information:**

Process ID:	0x33e8
Process Name:	C:\Windows\System32\svchost.exe

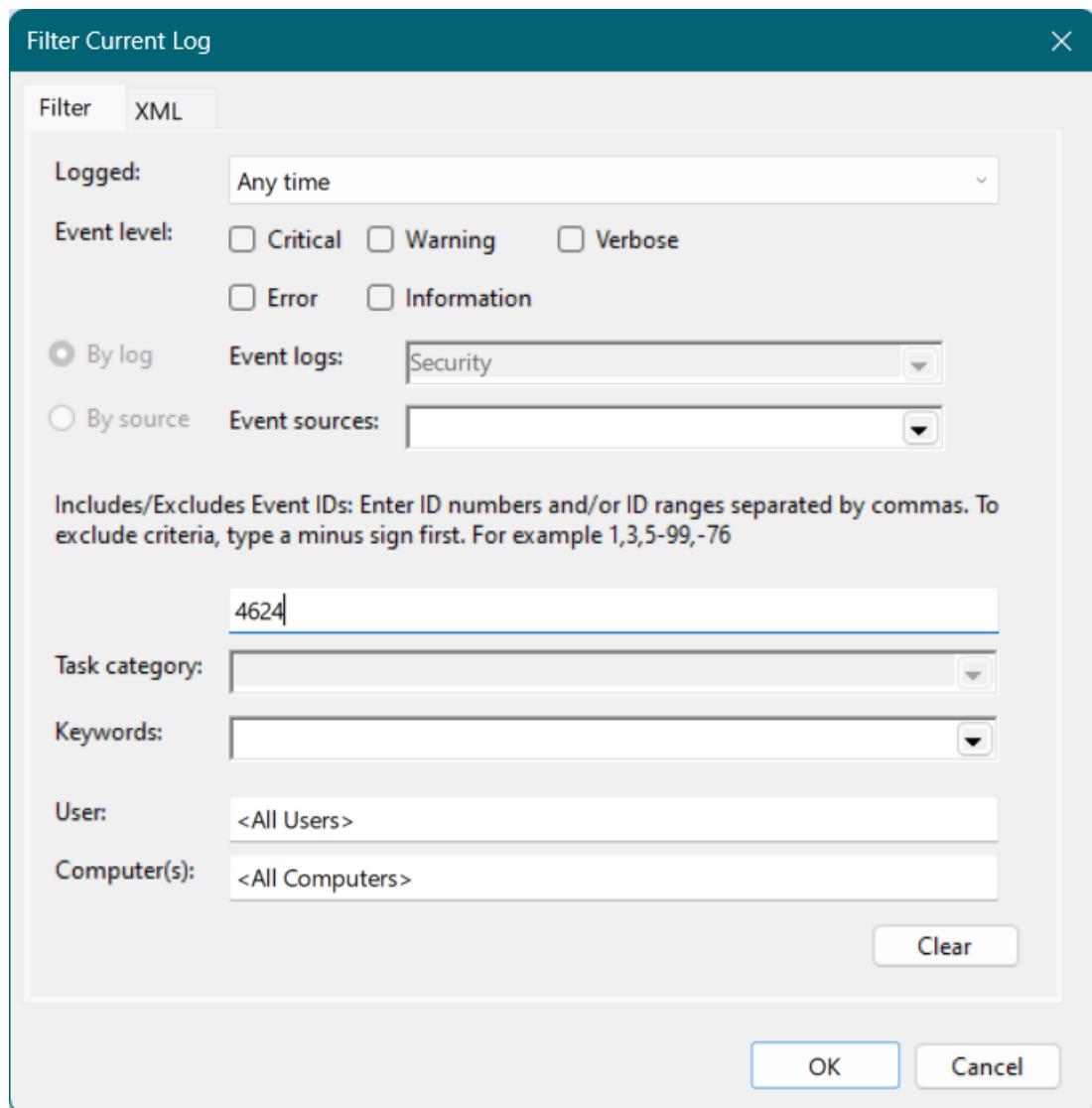
**Log Name:** Security  
**Source:** Microsoft Windows security  
**Event ID:** 4798  
**Level:** Information  
**User:** N/A  
**OpCode:** Info  
**More Information:** [Event Log Online Help](#)

The Actions pane on the right contains the following options:

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To This Log...
- View
- Refresh
- Help

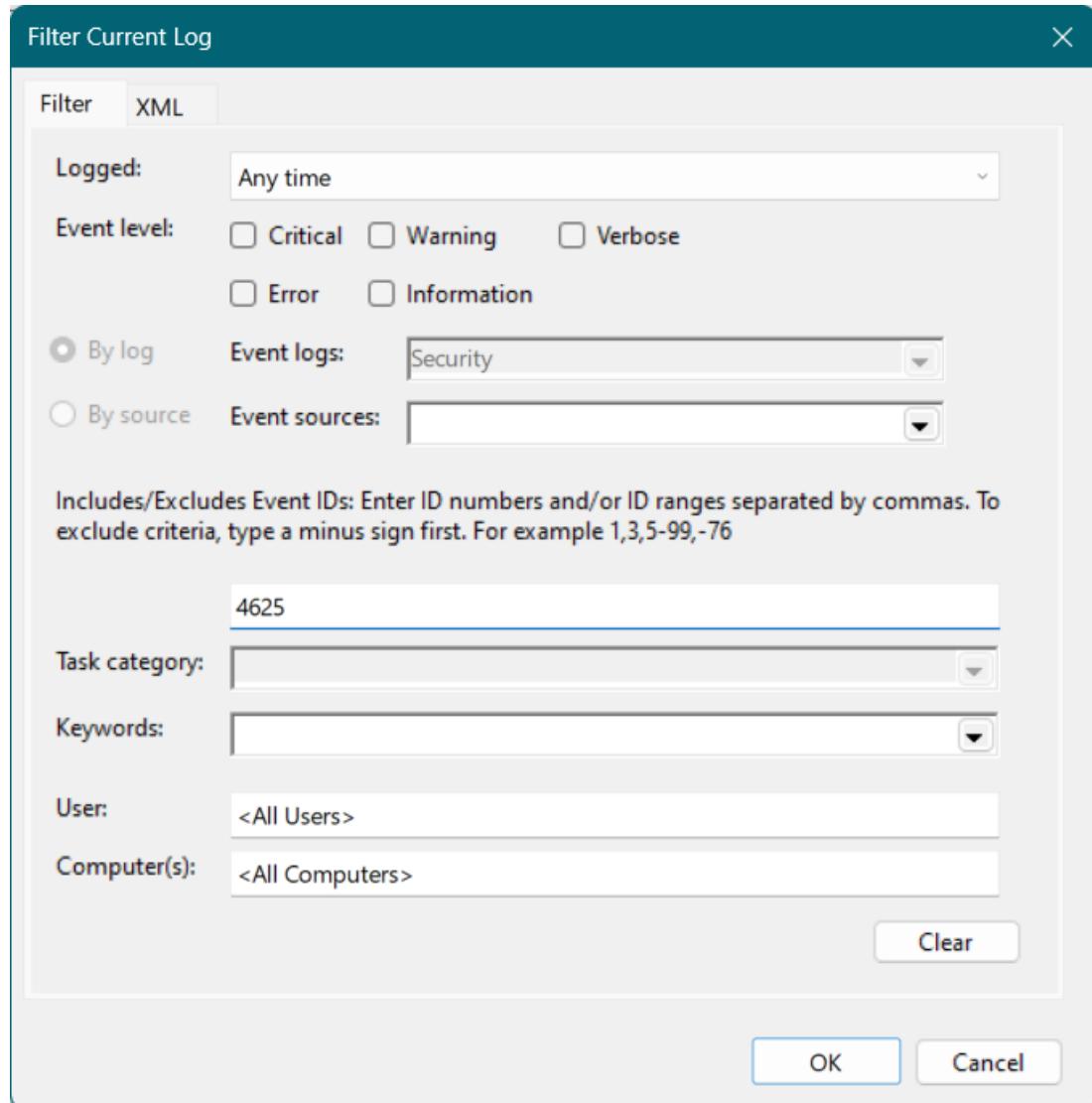
## 2. Filter by Event IDs:

### 2.1. 4624: Successful logon.



The screenshot shows the main Event Viewer window. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (Application, Security, Setup, System, Forwarded Events, Applications and Services Subscriptions). The 'Security' node is selected, and the status bar indicates 'Number of events: 29406'. The right pane shows a list of events under the heading 'Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 2,768'. One event is highlighted in blue. The details pane below shows the event information for the selected event (Event ID 4624, Logon, Audit Success). The properties pane on the right lists actions such as Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Clear Filter, Properties, Find..., Save Filtered Log File As..., Attach Task To This Log..., Save Filter to Custom View..., View, Refresh, Help, Event Properties, Copy, Save Selected Events..., Refresh, and Help. The status bar at the bottom says 'Creates a filter.'.

## 2.2. 4625: Failed logon attempt.



The screenshot shows the main Event Viewer window. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (Application, Security, Setup, System, Forwarded Events, Applications and Subscriptions). The right pane shows the results of a search for event 4625 in the Security log.

**Search Results:**

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	16-12-2024 11:28:04 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	16-12-2024 09:48:22 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	15-12-2024 11:15:04 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	14-12-2024 11:48:15 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	13-12-2024 08:53:12 PM	Microsoft Windows security auditing.	4625	Logon

**Event Details:** Event 4625, Microsoft Windows security auditing.

**General Details:**

An account failed to log on.  
**Subject:**  
 Security ID: SYSTEM  
 Account Name: PRATHAM-ROG-STR\$  
 Account Domain: WORKGROUP  
 Logon ID: 0x3E7

**Logon Type:** 2

**Account For Which Logon Failed:**  
 Security ID: NULL SID  
 Account Name: -  
 Account Domain: -

**Failure Information:**

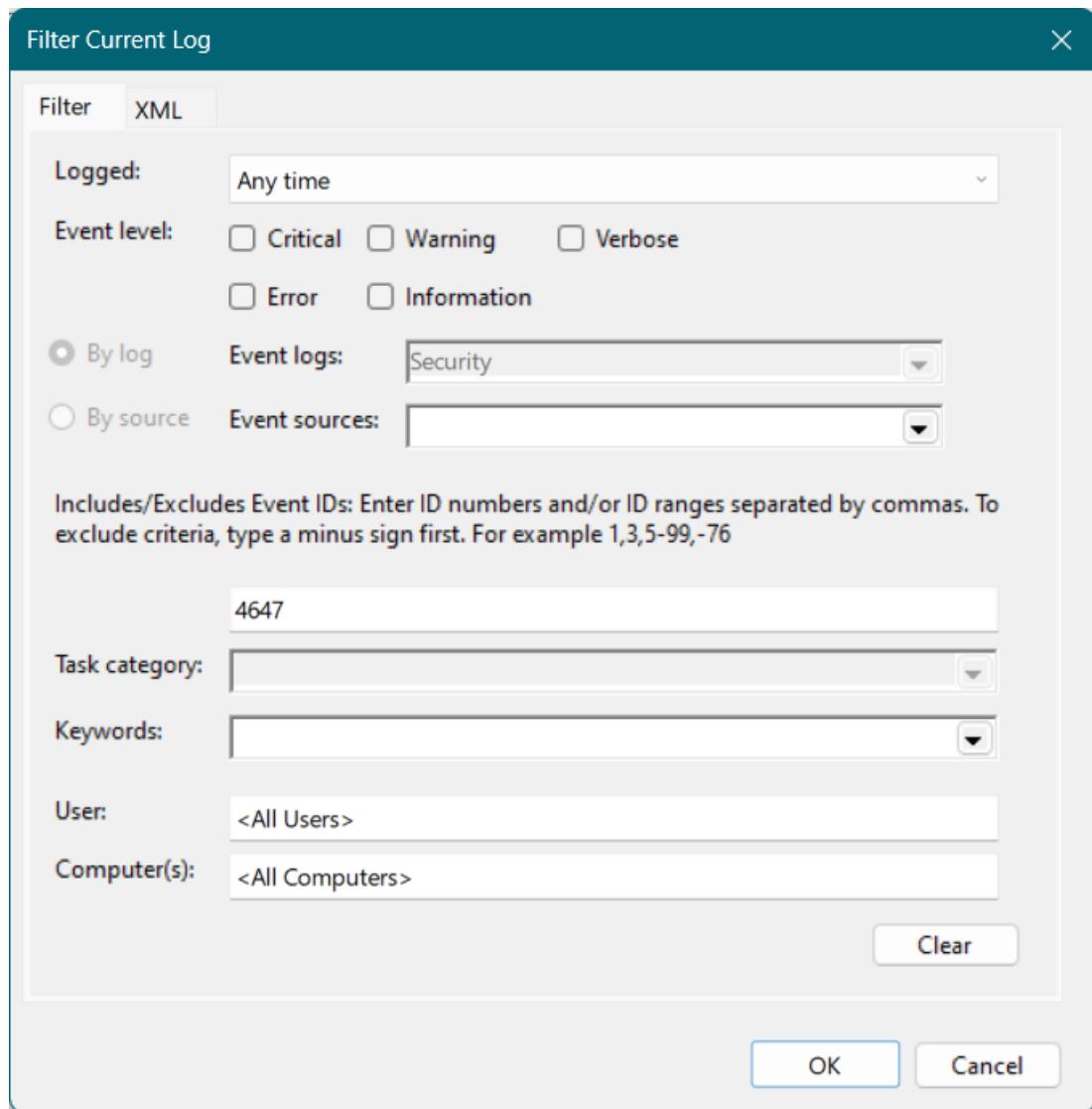
**Log Name:** Security  
**Source:** Microsoft Windows security  
**Event ID:** 4625  
**Level:** Information  
**User:** N/A  
**OpCode:** Info

Logged: 16-12-2024 11:28:04 AM  
**Task Category:** Logon  
**Keywords:** Audit Failure  
**Computer:** Pratham-Rog-Strix-G15

**More Information:** [Event Log Online Help](#)

The right pane also contains an 'Actions' menu with options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save Filtered Log File As..., Attach a Task To This Log..., Save Filter to Custom View..., View, Refresh, Help, and a context menu for the selected event.

### 2.3. 4647: User-initiated logoff.



The screenshot shows the Event Viewer main window. The left pane displays a tree view of logs: Custom Views, Windows Logs (Application, Setup, System, Forwarded Events, Applications and Services, Subscriptions), and Security. The Security node is selected, showing 'Number of events: 29,410'. The right pane shows a table of events filtered for 'Event ID: 4647' and 'Source: Security'. The table has columns: Keywords, Date and Time, Source, Event ID, and Task Category. The data is as follows:

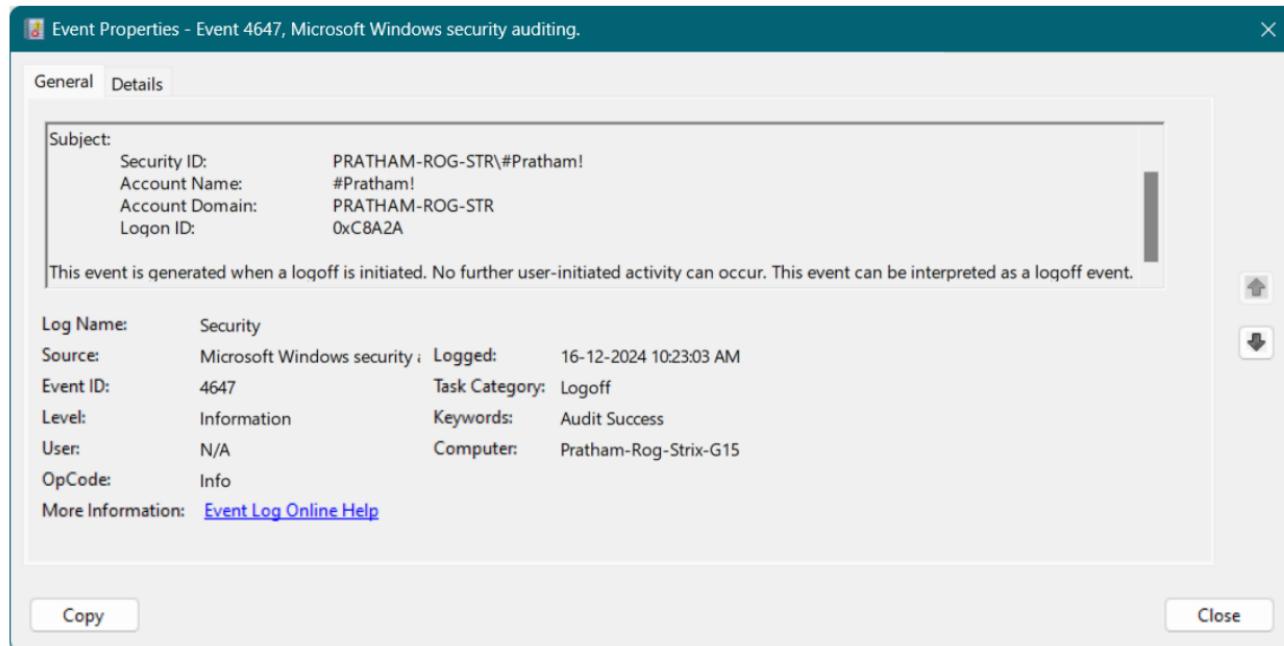
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	16-12-2024 10:23:03 AM	Microsoft Windows security auditing.	4647	Logoff
Audit Success	16-12-2024 01:36:20 AM	Microsoft Windows security auditing.	4647	Logoff
Audit Success	15-12-2024 03:16:52 AM	Microsoft Windows security auditing.	4647	Logoff
Audit Success	14-12-2024 11:46:47 PM	Microsoft Windows security auditing.	4647	Logoff
Audit Success	14-12-2024 09:22:15 PM	Microsoft Windows security auditing.	4647	Logoff
Audit Success	14-12-2024 06:03:41 PM	Microsoft Windows security auditing.	4647	Logoff

An 'Actions' context menu is open on the right side, listing options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Clear Filter, Properties, Find..., Save Filtered Log File As..., Attach Task To This Log..., Save Filter to Custom View..., View, Refresh, Help, Event 4647, Microsoft Windows security audit..., Event Properties, Attach Task To This Event..., Copy, Save Selected Events..., Refresh, and Help.

The bottom left of the main window says 'Creates a filter.' and the bottom right says 'Creates a filter.'

### 3. Identify:

#### 3.1. The user account involved.



**User:** #Pratham!

### 3.2. Logon types (interactive, remote desktop, etc.).

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

**Subject:**

Security ID:	SYSTEM
Account Name:	PRATHAM-ROG-STR\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

**Logon Information:**

Logon Type:	5
Restricted Admin Mode:	-
Remote Credential Guard:	-
Virtual Account:	No
Elevated Token:	Yes

**Impersonation Level:** Impersonation

**New Logon:**

Security ID:	SYSTEM
Account Name:	SYSTEM
Account Domain:	NT AUTHORITY

**Log Name:** Security

**Source:** Microsoft Windows security | **Logged:** 16-12-2024 01:21:42 PM

**Event ID:** 4624 | **Task Category:** Logon

**Level:** Information | **Keywords:** Audit Success

**User:** N/A | **Computer:** Pratham-Rog-Strix-G15

**OpCode:** Info

**More Information:** [Event Log Online Help](#)

**Copy** **Close**

Logon Type: 5 - Service Logon

### 3.3. Investigate any failed logon attempts for potential security issues.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (selected), Application, Security, Setup, System, Forwarded Events, Applications and Services, and Subscriptions. The right pane has tabs for Security, File, Action, View, Help, and Actions. The Security tab is selected, showing 'Number of events: 29433'. A filtered log titled 'Filtered Log: Security; Source: ; Event ID: 4625. Number of events: 5' is displayed. The table lists five audit failure events with the following details:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	16-12-2024 11:28:04 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	16-12-2024 09:48:22 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	15-12-2024 11:15:04 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	14-12-2024 11:48:15 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	13-12-2024 08:53:12 PM	Microsoft Windows security auditing.	4625	Logon

A detailed view of the first event (Event 4625) is shown in a modal window. The General tab displays:

An account failed to log on.  
Subject:  
Security ID: SYSTEM  
Account Name: PRATHAM-ROG-STR\$  
Account Domain: WORKGROUP  
Logon ID: 0x3E7  
Logon Type: 2  
Account For Which Logon Failed:  
Security ID: NULL SID  
Account Name: -  
Account Domain: -  
Failure Information:  
Log Name: Security  
Source: Microsoft Windows security  
Logged: 16-12-2024 11:28:04 AM  
Event ID: 4625  
Task Category: Logon  
Level: Information  
Keywords: Audit Failure  
User: N/A  
Computer: Pratham-Rog-Strix-G15  
OpCode: Info  
More Information: [Event Log Online Help](#)

The Actions pane on the right contains various options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Clear Filter, Properties, Find..., Save Filtered Log File As..., Attach a Task To This Log..., Save Filter to Custom View..., View, Refresh, Help, and a context menu for the selected event (Event 4625, Microsoft Windows security auditing). The context menu includes options like Event Properties, Attach Task To This Event..., Copy, Save Selected Events..., Refresh, and Help.

There are only 5 failed login attempts, but any of it are not suspicious.

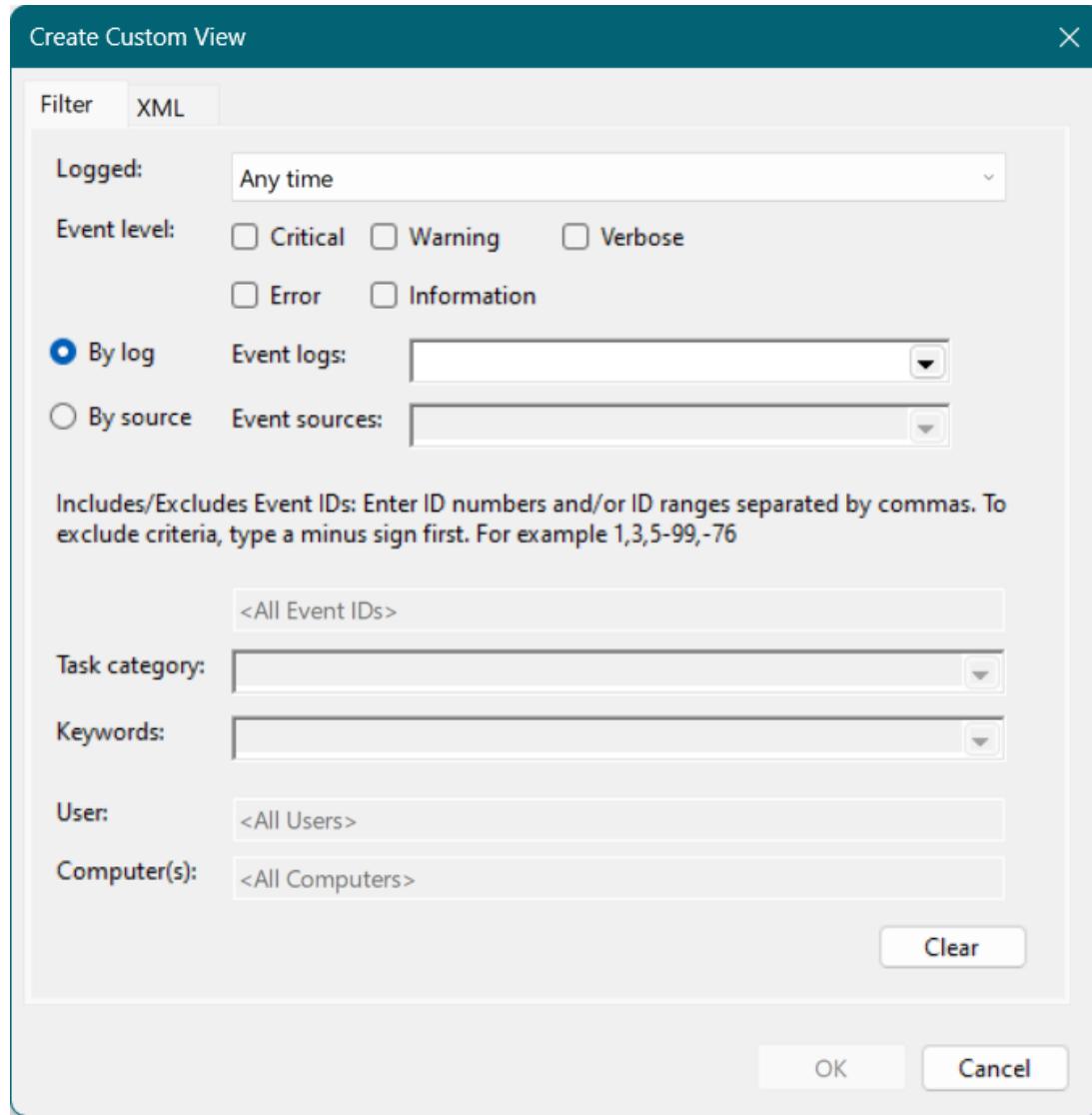
#### 4. Outcome: Learn to track and audit user authentication.

## Practical 4: Create a Custom View

**Objective:** Create a custom view for critical system events.

**Steps:**

1. In Event Viewer, click Action > Create Custom View.



**2. Select:**

**2.1. Event Levels: Critical, Warning, and Error.**

Create Custom View X

Filter XML

Logged: Any time

Event level:  Critical  Warning  Verbose  
 Error  Information

By log      Event logs:

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

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

## 2.2. Logs: System and Application.

Create Custom View X

Filter XML

Logged: Any time

Event level:  Critical  Warning  Verbose  
 Error  Information

By log Event logs: Application,System

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

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

### 2.3. Time Range: Last 7 days.

Create Custom View X

Filter XML

Logged:

Event level:  Critical  Warning  Verbose  
 Error  Information

By log Event logs:

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

<All Event IDs>

Task category:

Keywords:

User:

Computer(s):

### 3. Save the custom view with a name (e.g., "Critical System Events").

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane displays various logs and custom views. A custom view named "Critical System Events" is selected. The main pane shows a table of events with columns: Level, Date and Time, Source, Event ID, and Task Category. The table contains five entries, all of which are "Warning" level events from the "DNS Client Events" source. The right pane, titled "Actions", lists options for managing the custom view, including opening the saved log, creating or importing custom views, filtering current views, saving all events, and deleting the view. Below the main table, a detailed view of the first event (Event ID 1014) is shown, including its properties like Log Name, Source, and Logged date.

Level	Date and Time	Source	Event ID	Task Category
Warning	16-12-2024 12:03:28 PM	DNS Client Events	1014 (1014)	
Warning	16-12-2024 11:56:56 AM	DistributedCOM	10016	None
Warning	16-12-2024 11:45:15 AM	DistributedCOM	10016	None
Warning	16-12-2024 11:42:26 AM	WLAN-AutoConfig	10002	None
Error	16-12-2024 11:42:24 AM	Application Error	1000	Application Crashing

**Event 1014, DNS Client Events**

Name resolution for the name t-ring-fdv2.msedqe.net timed out after none of the configured DNS servers responded. Client PID 9648.

**Log Name:** System  
**Source:** DNS Client Events  
**Event ID:** 1014  
**Level:** Warning  
**User:** NETWORK SERVICE  
**OpCode:** Info  
**Keywords:** (268435456)  
**Computer:** Pratham-Rog-Strix-G15

More Information: [Event Log Online Help](#)

**Actions**

- Critical System Events
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Custom View...
- Properties
- Find...
- Save All Events in Custom View As...
- Export Custom View...
- Copy Custom View...
- Attach Task To This Custom View...
- View
  - Delete
  - Rename
  - Refresh
  - Help
- Event 1014, DNS Client Events
  - Event Properties
  - Attach Task To This Event...
  - Copy
  - Save Selected Events...
  - Refresh
  - Help

#### 4. Document and analyze any recurring critical errors.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Server Roles, Administrative Events, Device Manager - MediaTek, Device Manager - MediaTek, Google, Critical System Events, Windows Logs, Application, Security, Setup, System, Forwarded Events, Applications and Services Logs, and Subscriptions. The right pane shows a table titled "Critical System Events" with the message "Number of events: 974". The table has columns: Level, Date and Time, Source, Event ID, and Task Category. A specific event is selected, highlighted in blue, with the details: Event ID: 6155 (240), Level: Warning, Date and Time: 12-12-2024 05:21:39 PM, Source: LSA (LsaSrv), Event ID: 6147, Task Category: None. The Actions pane on the right provides options like Open Saved Log..., Create Custom View..., Import Custom View..., Filter Current Custom View..., Properties, Find..., Save All Events in Custom View..., Export Custom View..., Copy Custom View..., Attach Task To This Custom View..., View, Delete, Rename, Refresh, and Help. The status bar at the bottom indicates "Event 6155, LSA (LsaSrv)".

The screenshot shows the "Event Properties - Event 6155, LSA (LsaSrv)" dialog. It has tabs for General and Details. The General tab contains the following information:

- LSA package is not signed as expected. This can cause unexpected behaviour with Credential Guard.**
- PackageName:** schannel

The Details tab displays the event properties:

<b>Log Name:</b>	System		
<b>Source:</b>	LSA (LsaSrv)	<b>Logged:</b>	12-12-2024 05:21:39 PM
<b>Event ID:</b>	6155	<b>Task Category:</b>	None
<b>Level:</b>	Warning	<b>Keywords:</b>	
<b>User:</b>	SYSTEM	<b>Computer:</b>	Pratham-Rog-Strix-G15
<b>OpCode:</b>	Info		
<b>More Information:</b>	<a href="#">Event Log Online Help</a>		

At the bottom of the dialog are "Copy" and "Close" buttons.

There are **240 Recurring Logs** of Event ID: 6155

**Description:**

LSA package is not signed as expected. This can cause unexpected behaviour with Credential Guard.

**PackageName:** schannel

#### 5. Outcome: Learn to customize event views for efficient monitoring.