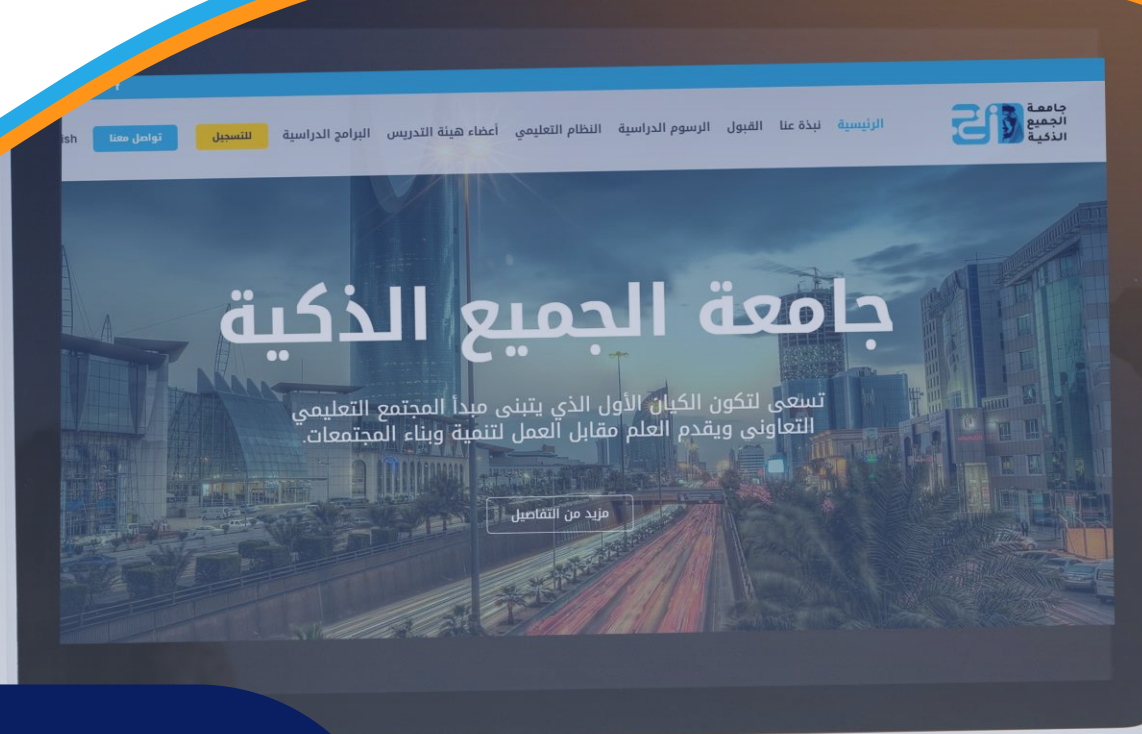




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

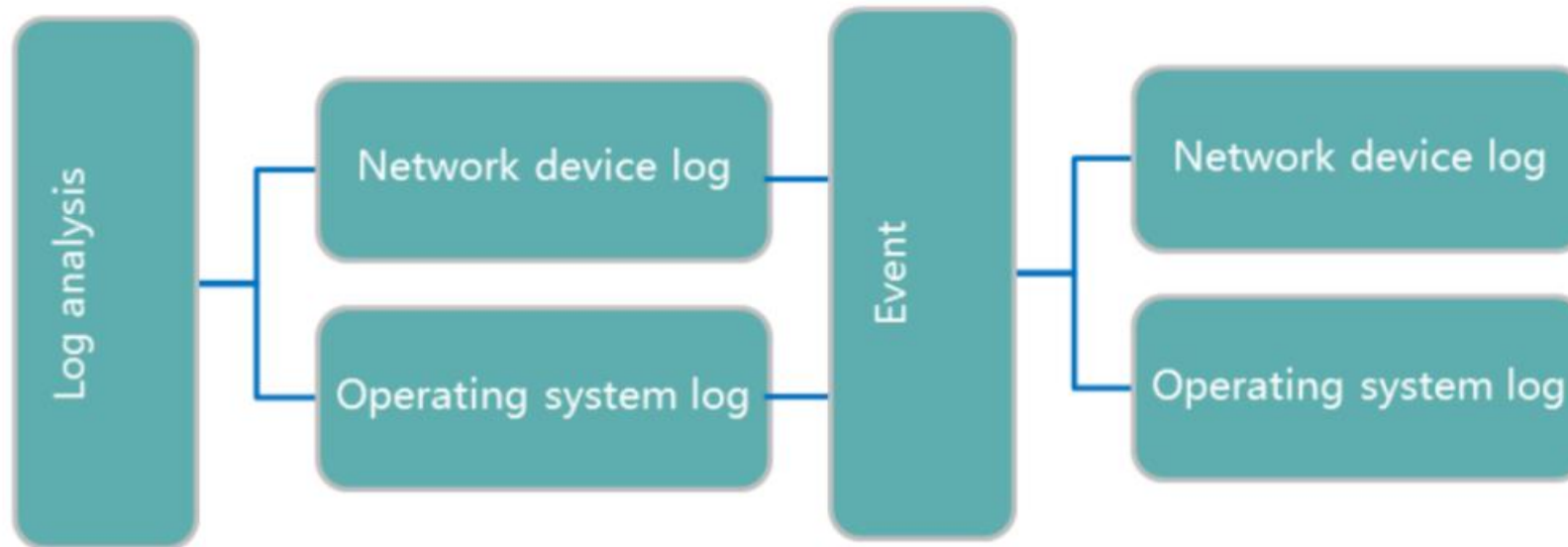


HCIA Security
Prepared by Eng. Abdelrhman Ahmed
Lecture 10

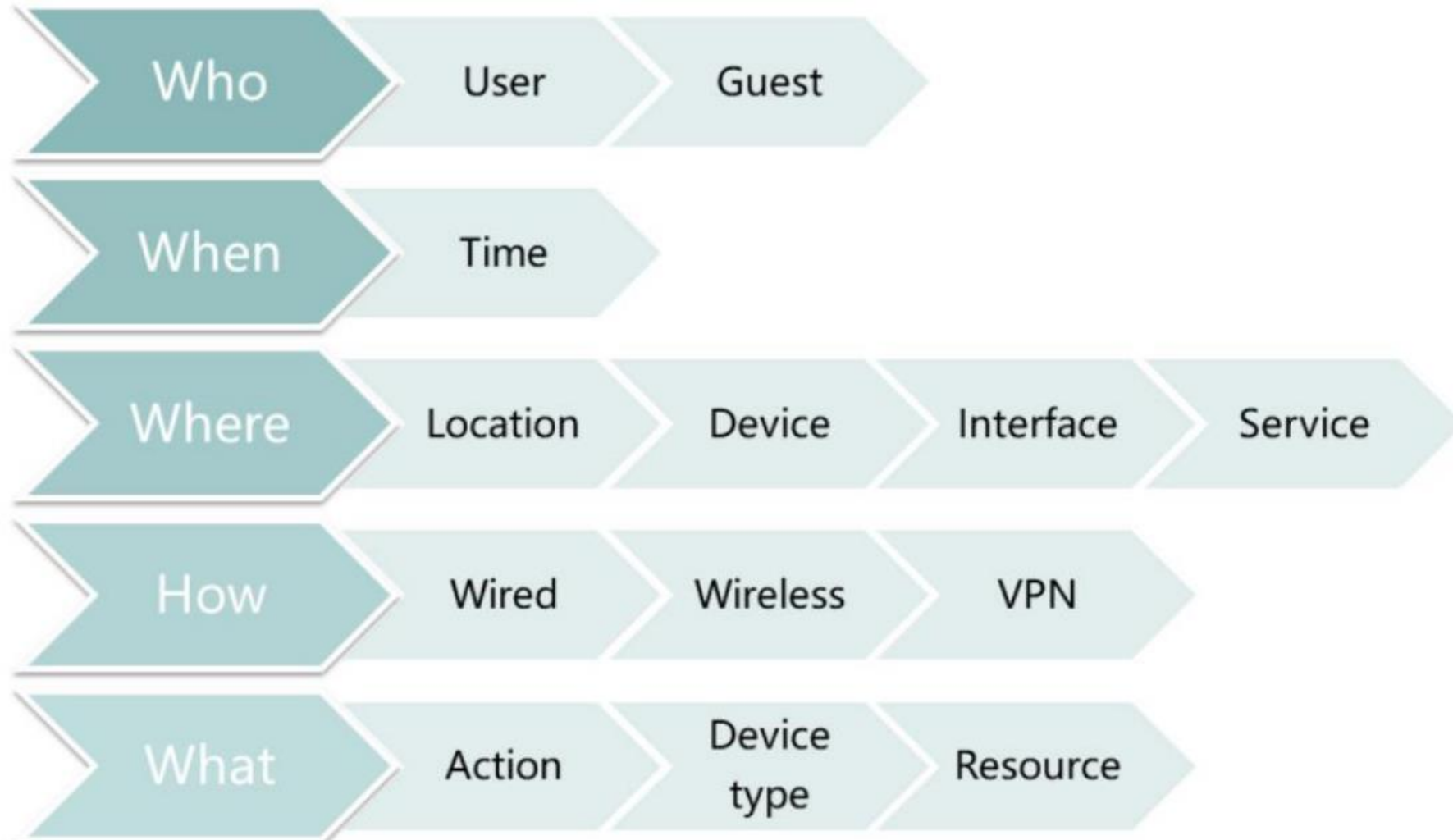
Data Analysis

Log Analysis

- The primary method to locate attackers is to extract and analyze the "traces" of perpetrators in computer systems.
- Important network events are recorded in logs. Analyzing logs plays a vital role in cracking down on network crimes.



Key Log Analysis Points



Analysis of Network Device Logs

- This example uses the firewall to describe how to analyze attacks based on logs.
- Click Threat Log in the navigation sidebar. As shown in the figure, information about an IP spoofing attack, including the attack time, protocol used, and target interface, is displayed.

The screenshot displays a network management interface with a sidebar on the left containing various log categories: Log, Traffic Log, Threat Log (highlighted), URL Log, Content Log, Operation Log, System Log, User Activity Log, Policy Matching Log, Mail Filtering Log, Report, Traffic Map, Threat Map, Session Table, System Statistics, Diagnosis Center, Quintuple Packet Capture, and Quintuple Packet Discard.

The main panel shows the 'Threat Log List' with a table containing one entry:

View	Time	Threat Type	Threat ID	Threat Name	Source Zone	Destination Zone	At
	2017/03/19 12:02:45	Attack	25	IP spoof attack			10

Below the table, the 'View Threat Log Details(Attack)' window is open, showing two sections:

Common Log Field

- Attack Start Time: 2017/03/19 12:02:20
- Attack End Time: 2017/03/19 12:02:20
- Protocol: UDP
- Virtual System: root
- Application Category:
- Application Subcategory:
- Application:

Threat

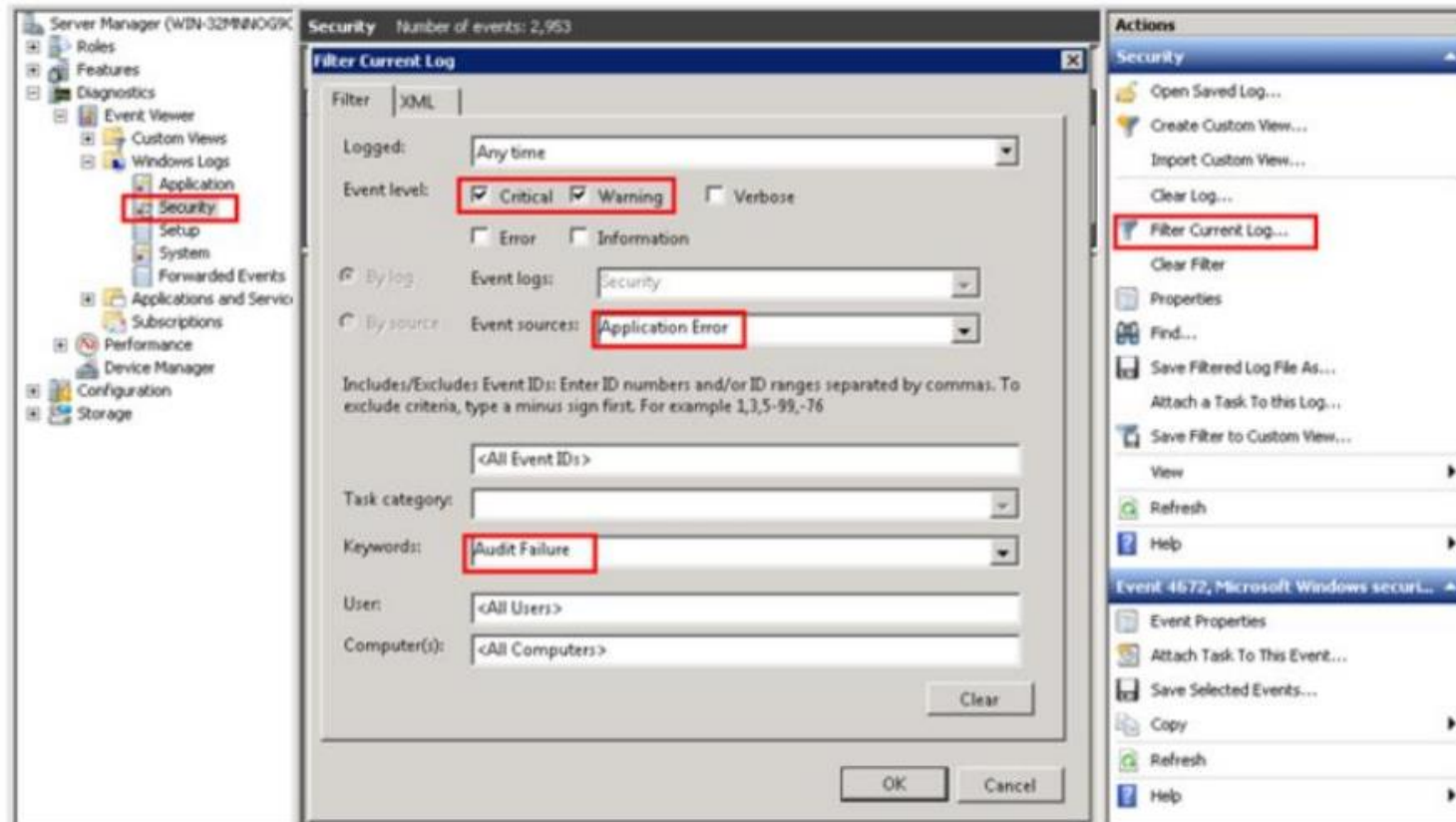
- Threat Type: Attack
- Threat Name: IP spoof attack
- Threat Count: 1
- Action: Alert
- Target Interface: GE1/0/2
- Packet Count: 1
- Maximum Attack Packet Rate: 0

At the bottom, a table shows the source and destination addresses:

Source Address:Source...	Attacker	Source Country/Region	Destination Address:D...	Victim	Destination Country/Re...
10.1.11.100.137	10.1.11.100	unknown-zone	10.1.11.255.137	10.1.11.255	unknown-zone

Analysis of Operating System Logs

- Logs record all events of the operating system. It is vital to quickly identify key information from a large amount data. In the Windows operating system, you can filter key events as required.



Analysis of Login and Logout Events

- **Application scenarios:**

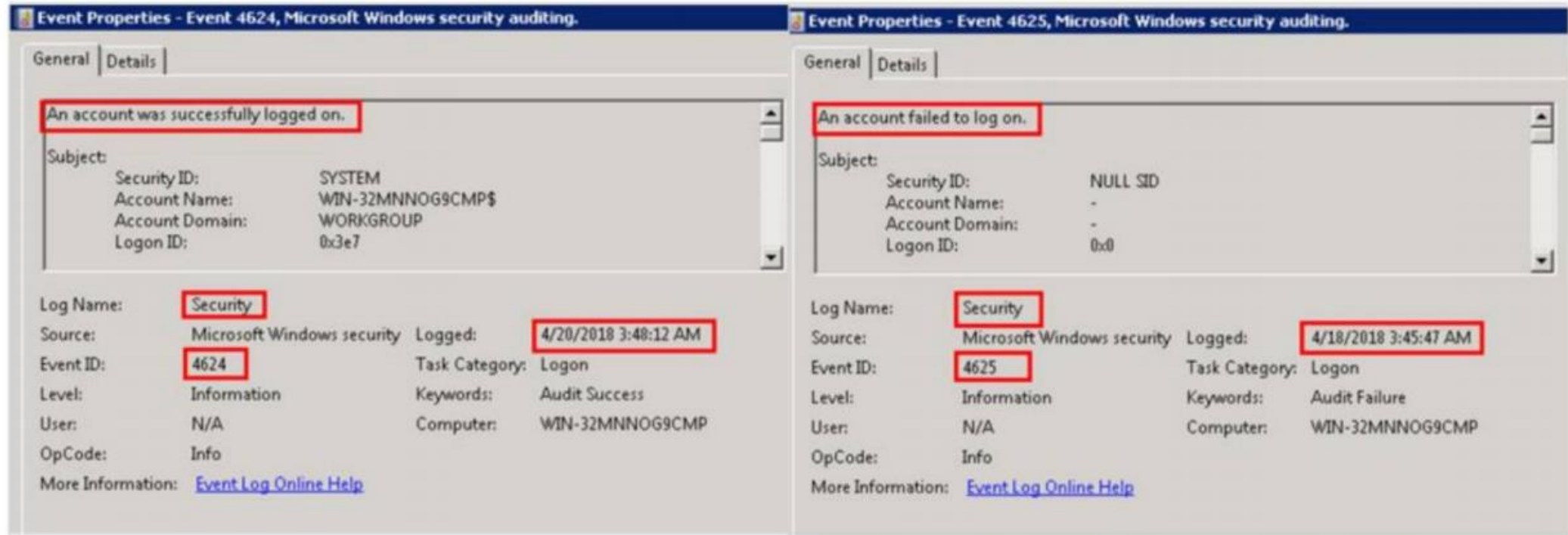
- ☐ Identifying users who have logged in to the operating system.
- ☐ Analyzing how the operating system is used.

- **Event ID:**

- ☐ 4624-Login success (security log)
- ☐ 4625 - Login failure (security log)
- ☐ 4634- Logout success (security log)
- ☐ 4672 - Login as an administrator (security log)

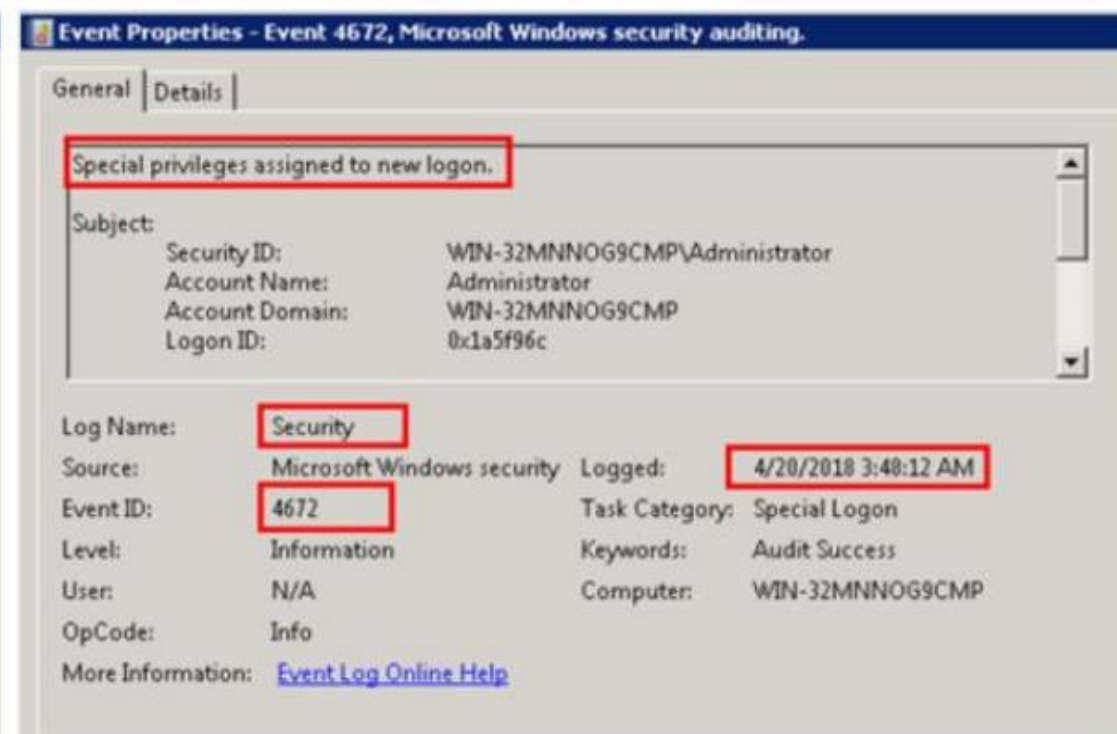
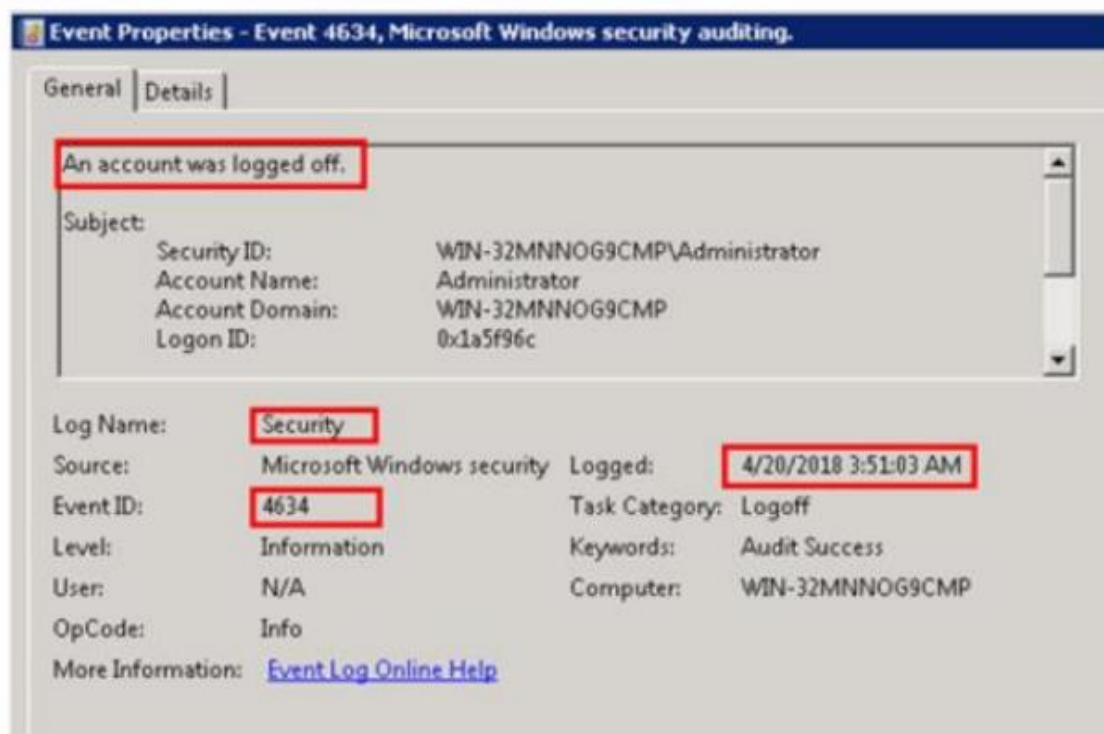
Login Success and Failure Events

- The following figure displays the security log information regarding login success and login failure.



Logout and Privileged Login Events

- The following figure displays the security log information regarding logout and privileged login.

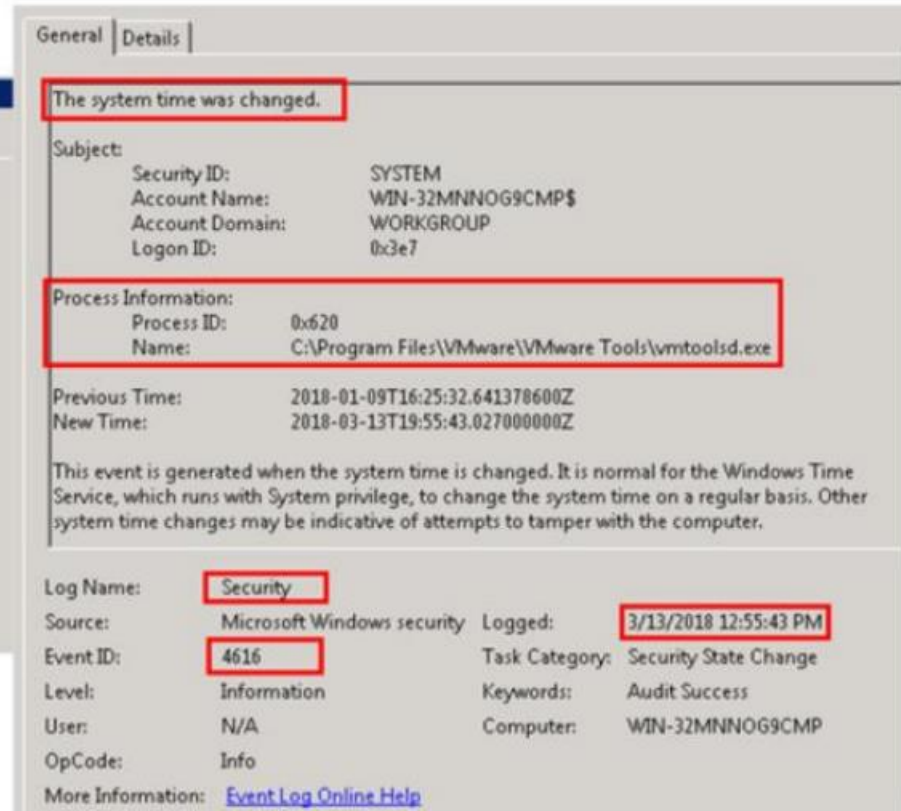
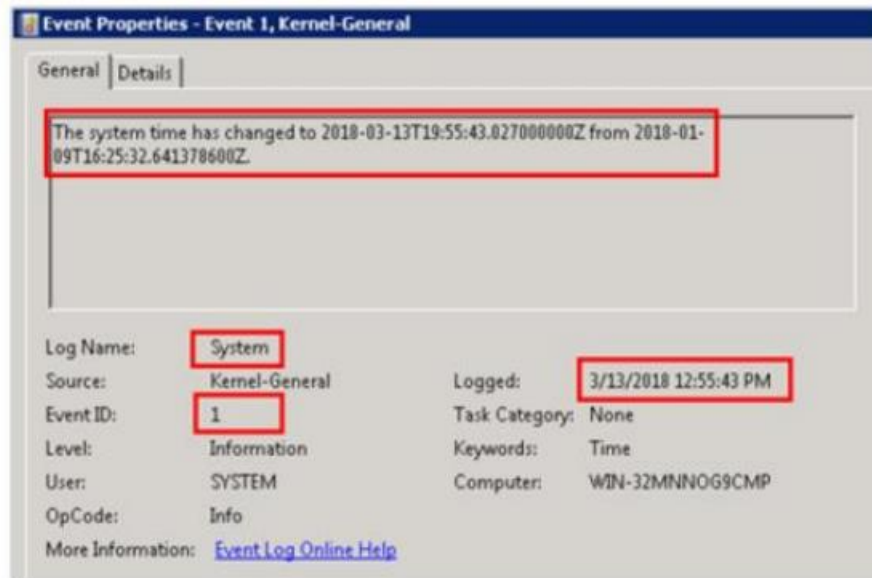


Analysis of System Time Change Events

- **Application scenario:**
 - ❑ **Collecting evidence proving that a user has changed the system time.**
- **Event ID:**
 - ❑ **1 - Kernel-General (system log)**
 - ❑ **4616 - Change system time (security log)**

Logs About System Time Change Events

- The following figures show the system log and security log for system time change events.



Analysis of External Device Use Events

- **Application scenario:**
 - **Analyzing the time when hardware devices are installed in the system.**
- **Event ID:**
 - **20001/20003- Plug-and-play drive installation (system log)**

Logs About External Device Use Events

- The following figure shows the system log's record of the external drive installation event.

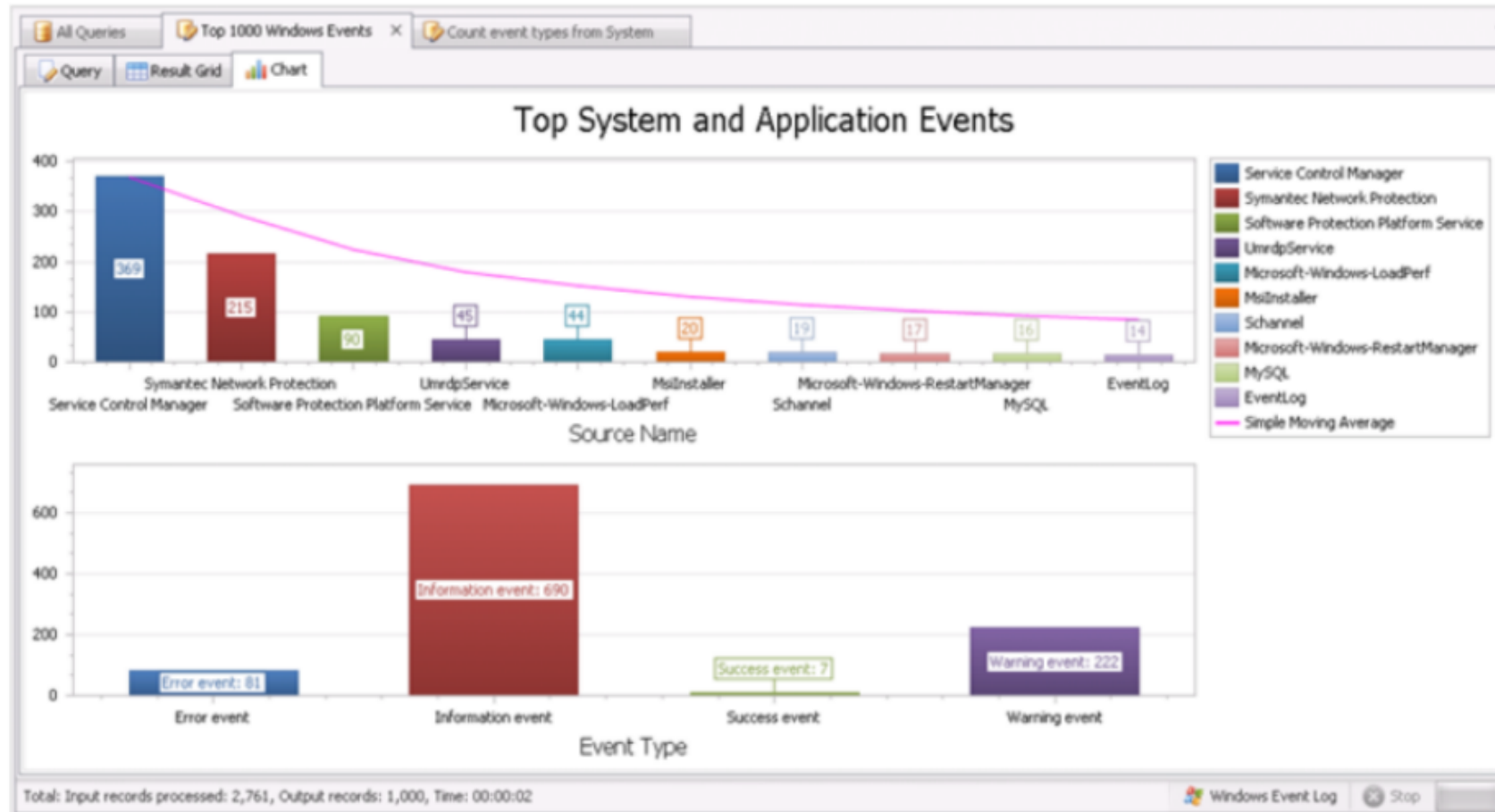


Log Analysis Tools

- **Log Parser** is a high-performance and easy-to-use log analysis tool developed by Microsoft. It can analyze text log files, Extensible Markup Language (XML) files, comma separated values (CSV) files, event logs, registries, file systems, and Active Directory of the operating system.
- To use Log Parser, you must be skilled in SQL language.
- **Log Parser Lizard** is a GUI and saves users from remembering complicated commands. Users can obtain the analysis results by setting the basic SQL statements.

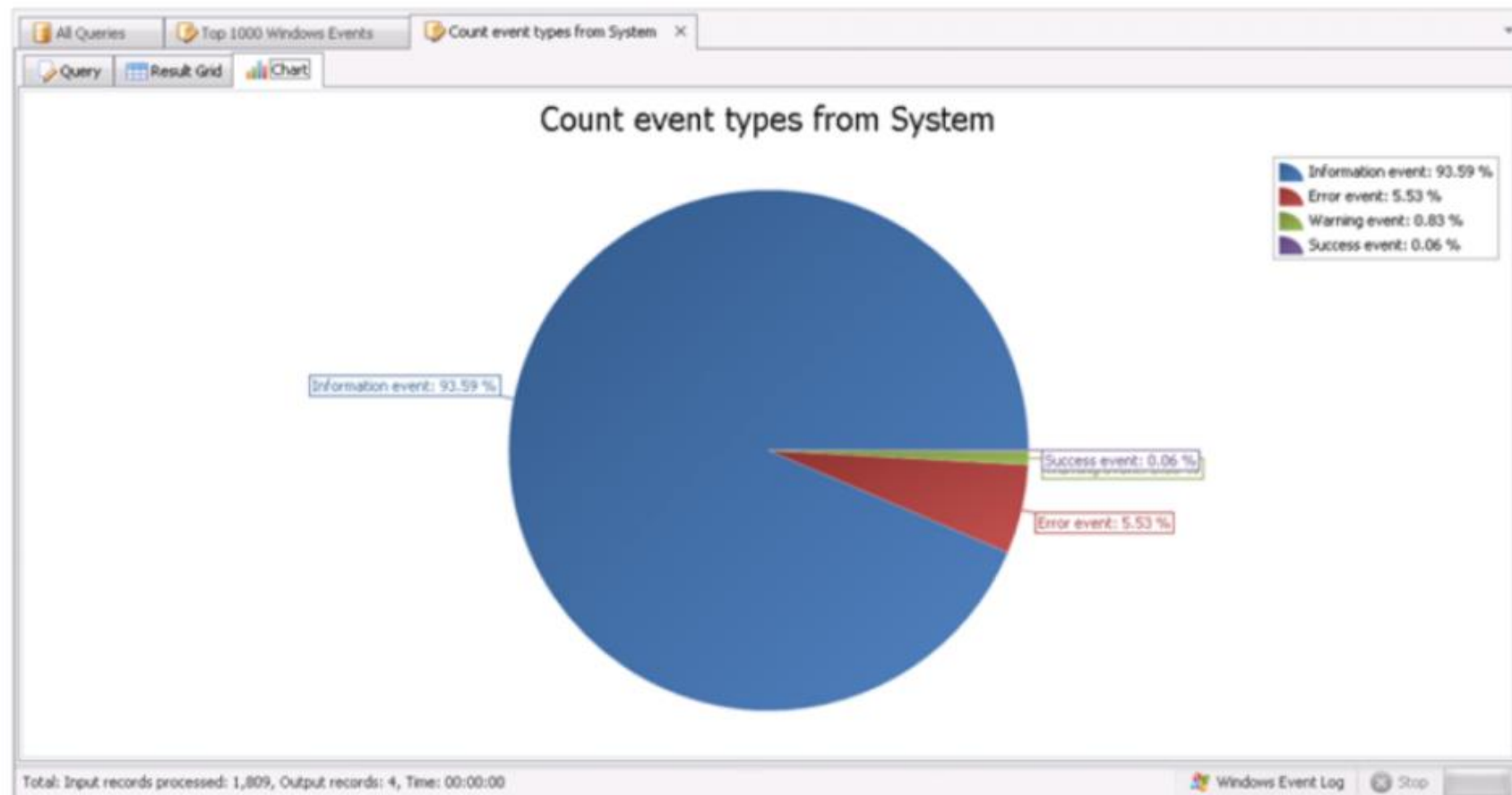
Use of Log Parser Lizard (1)

- The following figure shows the Top 1000 Windows Events results filtered by Log Parser Lizard.



Use of Log Parser Lizard (2)

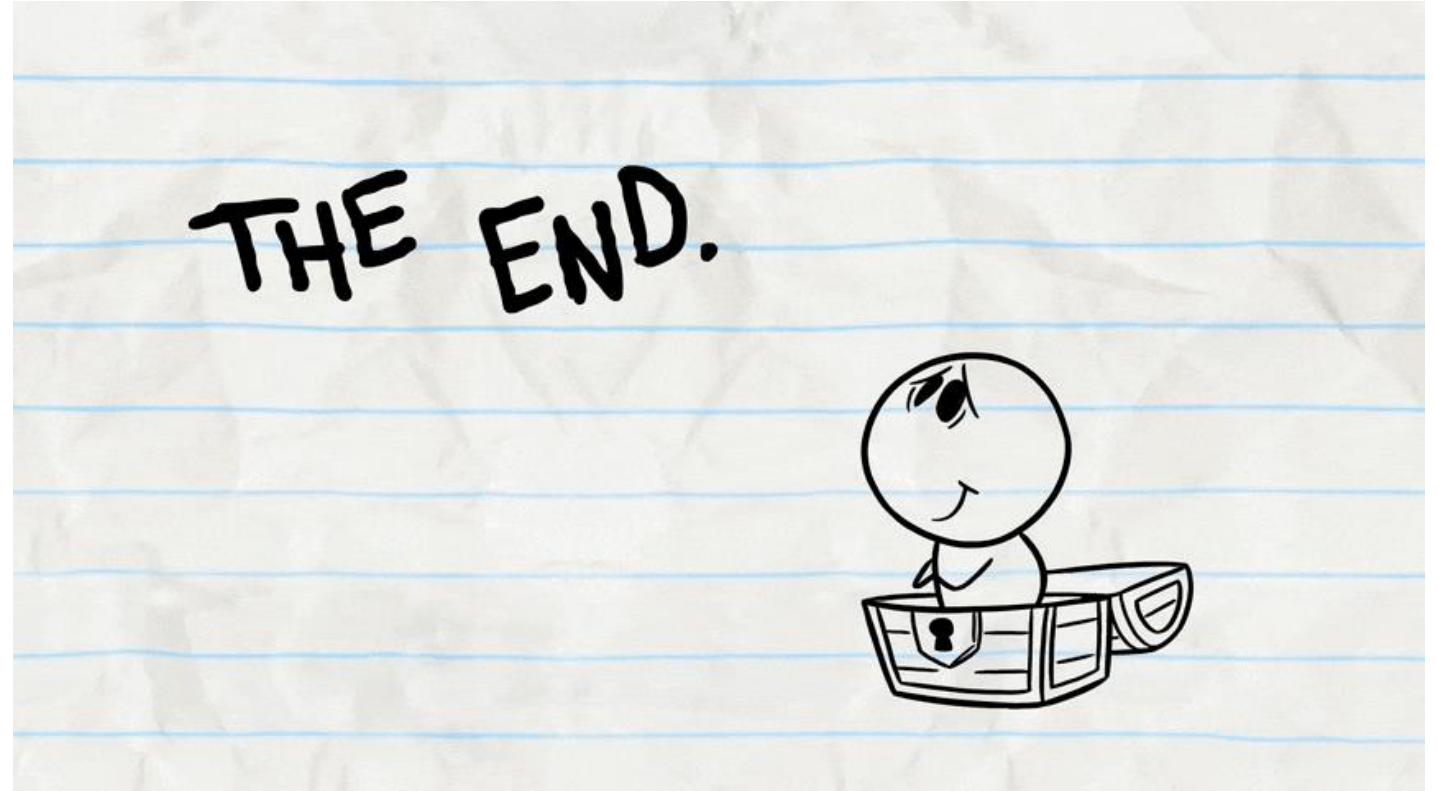
- The following figure shows the Count event types from System results filtered by Log Parser Lizard.



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY