TASK 12

What is a log?

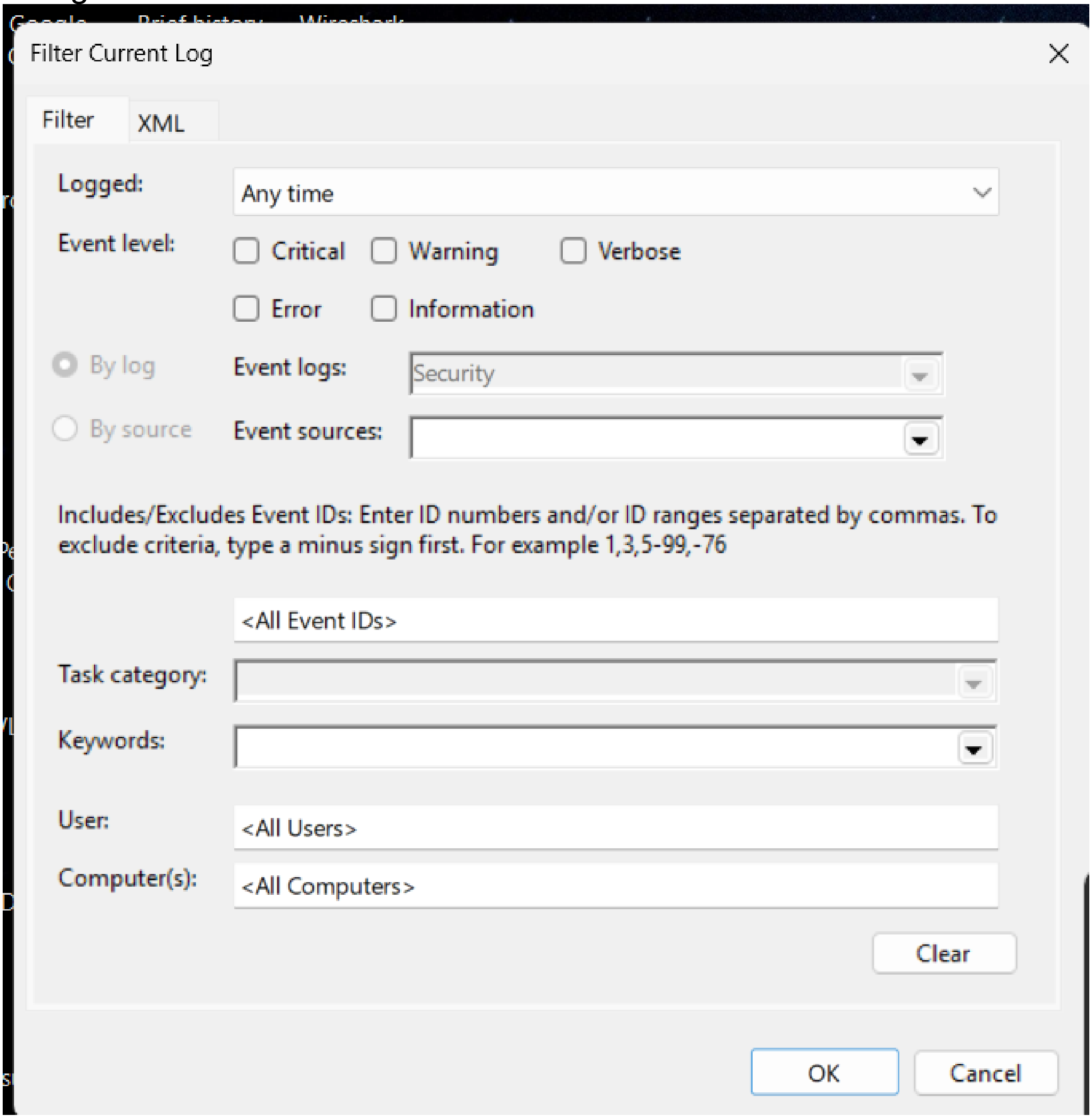
A log is a record of events generated by:

- Operating system
- Applications
- Security controls

Network logs are digital records of events and activities occurring across network devices such as routers, switches, firewalls, and servers. They capture critical data like connection attempts, traffic patterns, login events, errors, and security-related activities, serving as a "journal-of-record" for network operations.

ACESSING THE LOGS:

Using windows event viewer



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

<All Event IDs>

Task category:

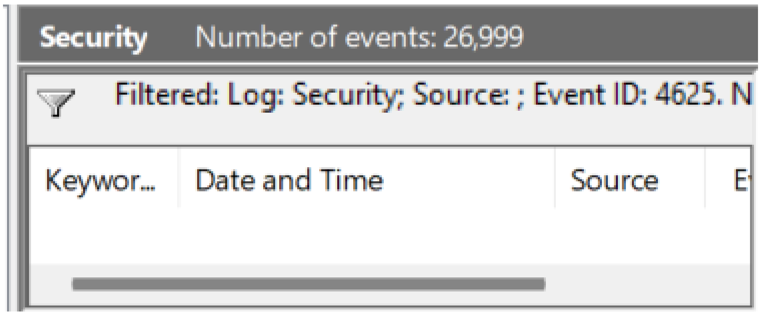
Keywords:

User: <All Users>

Computer(s): <All Computers>

FILTERING THE LOGS:

Event id: 4025

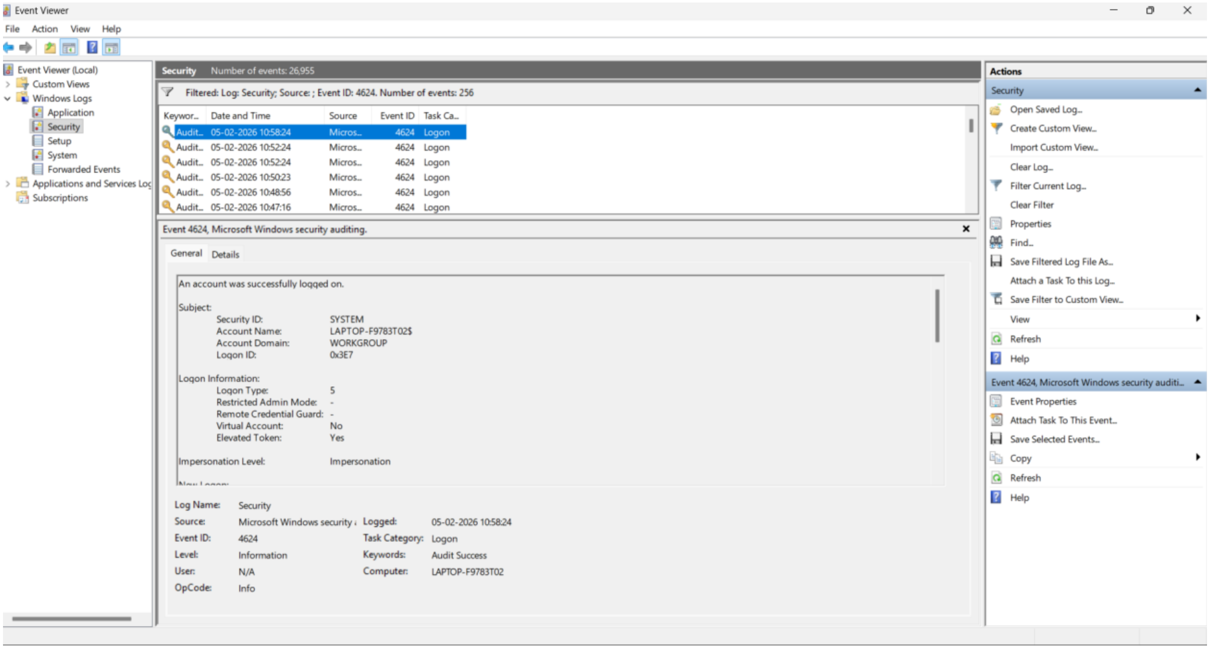


Security Number of events: 26,999

Filtered: Log: Security; Source: ; Event ID: 4625. N

Keywor...	Date and Time	Source	E

Event id:4624



Security Number of events: 26,955

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 256

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	05-02-2026 10:58:24	Micros...	4624	Logon
Audit...	05-02-2026 10:52:24	Micros...	4624	Logon
Audit...	05-02-2026 10:52:24	Micros...	4624	Logon
Audit...	05-02-2026 10:50:23	Micros...	4624	Logon
Audit...	05-02-2026 10:48:56	Micros...	4624	Logon
Audit...	05-02-2026 10:47:16	Micros...	4624	Logon

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:                SYSTEM
        Account Name:               LAPTOP-F9783T02$
        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
```

```
Log Name:   Security
Source:     Microsoft Windows security a   Logged:          05-02-2026 10:58:24
Event ID:   4624                           Task Category:   Logon
Level:      Information                    Keywords:        Audit Success
User:       N/A                            Computer:        LAPTOP-F9783T02
OpCode:     Info
```

Event in windows referred as a record of action. Like performing an action in system and type of actions are described with numeric id's called event id's.

ID	Meaning
4624	Successful login
4625	Failed login
4740	Account locked
4798	Group membership checked

Anomalies is a concept of describing something is perform than normal behaviour. From analyze there is no anomaly is recorded