Auditing Logs

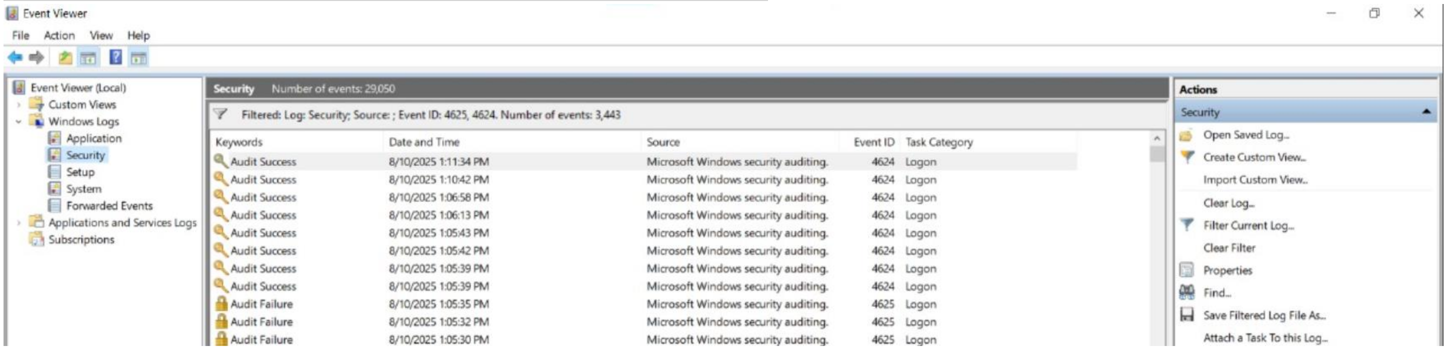
WE Innovate X Zero$ploit

*PREPARED BY : **Omar Hassan – Mohamed Haytham – Ali Abdelrahman***

*Supervised By **: Eng.Adel Ahmed***

Viewing Windows Logs

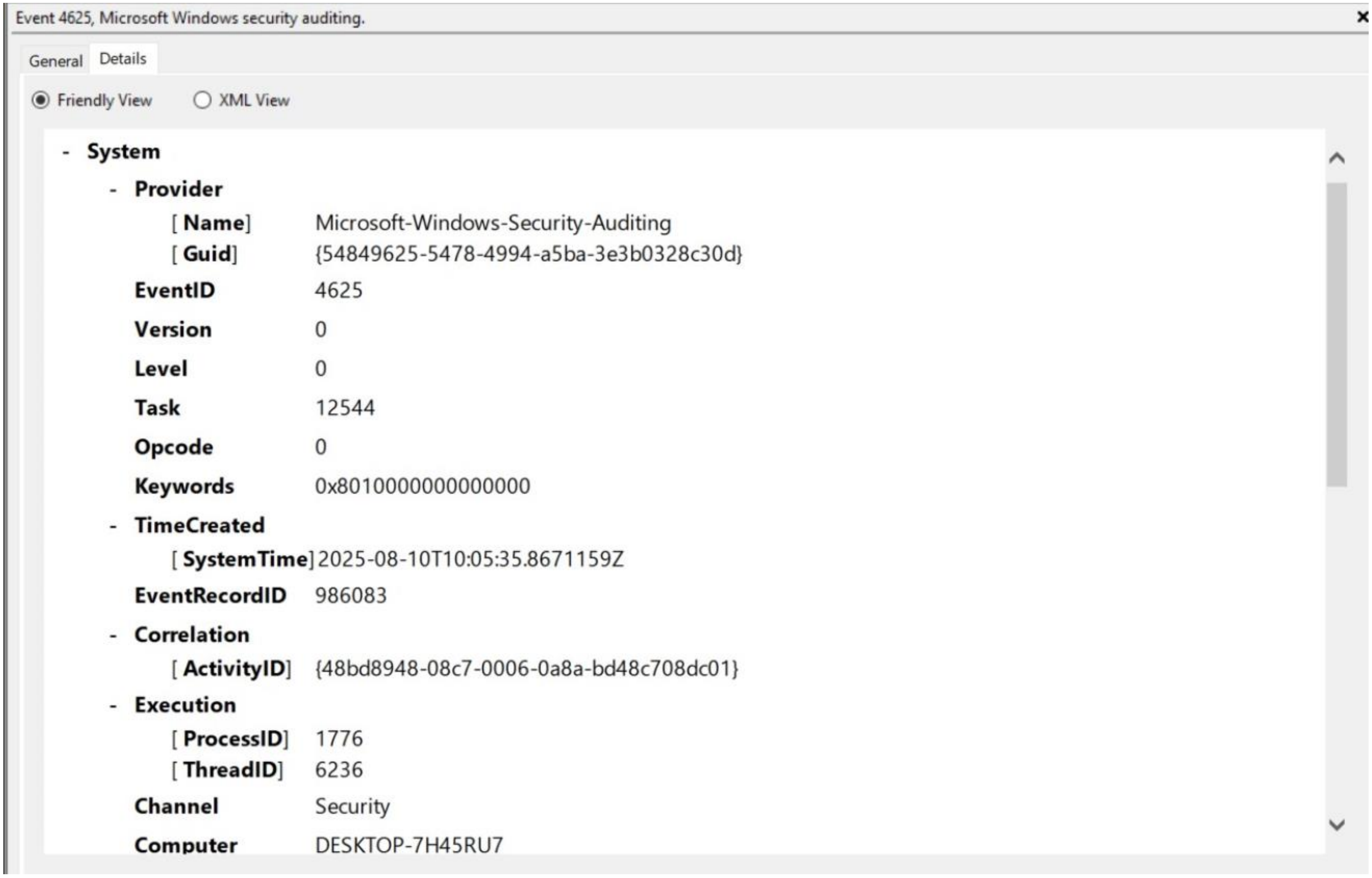
Through Event viewer > Windows Logs > Security



Security   Number of events: 29,050

Filtered: Log: Security; Source: ; Event ID: 4625, 4624. Number of events: 3,443

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/10/2025 1:11:34 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/10/2025 1:10:42 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/10/2025 1:06:58 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/10/2025 1:06:13 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/10/2025 1:05:43 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/10/2025 1:05:42 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/10/2025 1:05:39 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/10/2025 1:05:39 PM	Microsoft Windows security auditing.	4624	Logon
Audit Failure	8/10/2025 1:05:35 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/10/2025 1:05:32 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/10/2025 1:05:30 PM	Microsoft Windows security auditing.	4625	Logon



Event 4625, Microsoft Windows security auditing.

```
- System
   - Provider
        [ Name]       Microsoft-Windows-Security-Auditing
        [ Guid]       {54849625-5478-4994-a5ba-3e3b0328c30d}
     EventID          4625
     Version          0
     Level            0
     Task             12544
     Opcode           0
     Keywords         0x8010000000000000
   - TimeCreated
        [ SystemTime] 2025-08-10T10:05:35.8671159Z
     EventRecordID    986083
   - Correlation
        [ ActivityID] {48bd8948-08c7-0006-0a8a-bd48c708dc01}
   - Execution
        [ ProcessID]  1776
        [ ThreadID]   6236
     Channel          Security
     Computer         DESKTOP-7H45RU7
```

Filter Current Log

Success EventID : 4624 – Failed EventID : 4625

Important fields extracted :

EventID

Time

Correlation : ActivityID

Execution : ProcessID

IP Address

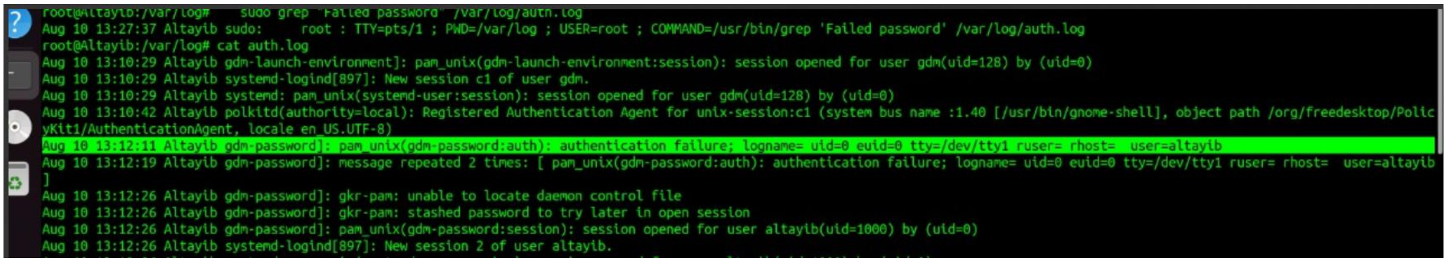
Port Number

Logon type

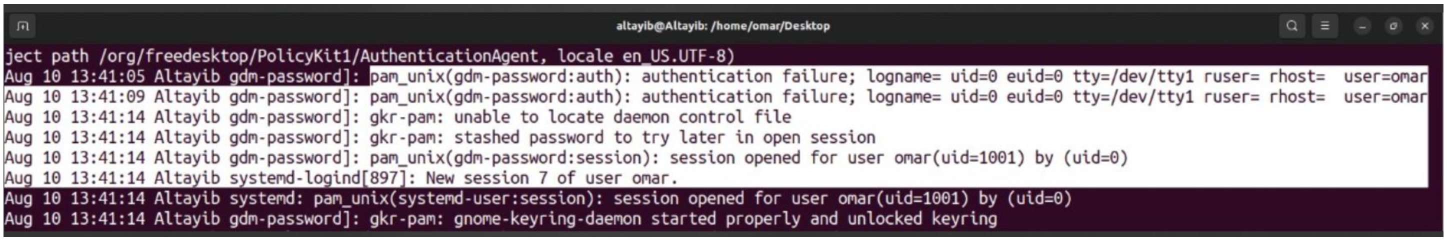
- **EventID** – A unique number that identifies the specific type of event in the log (e.g., logon, file access, process start).
- **Time** – The date and time when the event occurred.
- **Correlation : ActivityID** – An identifier that links related events together so you can trace a full activity/session across multiple logs.
- **Execution : ProcessID** – The ID of the process that triggered the event (used to trace which program was responsible).
- **IP Address** – The network address of the device involved in the event (source or destination).
- **Port Number** – The specific network port used for the communication (helps identify the service or protocol).
- **Logon type** – A code describing how the user logged in (e.g., interactive, remote desktop, network).

Viewing Linux Logs

Location : /var/log/auth.log



```
root@Altayib:/var/log#    sudo grep "Failed password" /var/log/auth.log
Aug 10 13:27:37 Altayib sudo:     root : TTY=pts/1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
root@Altayib:/var/log# cat auth.log
Aug 10 13:10:29 Altayib gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=128) by (uid=0)
Aug 10 13:10:29 Altayib systemd-logind[897]: New session c1 of user gdm.
Aug 10 13:10:29 Altayib systemd: pam_unix(systemd-user:session): session opened for user gdm(uid=128) by (uid=0)
Aug 10 13:10:42 Altayib polkitd(authority=local): Registered Authentication Agent for unix-session:c1 (system bus name :1.40 [/usr/bin/gnome-shell], object path /org/freedesktop/Polic
yKit1/AuthenticationAgent, locale en_US.UTF-8)
Aug 10 13:12:11 Altayib gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=altayib
Aug 10 13:12:19 Altayib gdm-password]: message repeated 2 times: [ pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=altayib
]
Aug 10 13:12:26 Altayib gdm-password]: gkr-pam: unable to locate daemon control file
Aug 10 13:12:26 Altayib gdm-password]: gkr-pam: stashed password to try later in open session
Aug 10 13:12:26 Altayib gdm-password]: pam_unix(gdm-password:session): session opened for user altayib(uid=1000) by (uid=0)
Aug 10 13:12:26 Altayib systemd-logind[897]: New session 2 of user altayib.
```



```
ject path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Aug 10 13:41:05 Altayib gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=omar
Aug 10 13:41:09 Altayib gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=omar
Aug 10 13:41:14 Altayib gdm-password]: gkr-pam: unable to locate daemon control file
Aug 10 13:41:14 Altayib gdm-password]: gkr-pam: stashed password to try later in open session
Aug 10 13:41:14 Altayib gdm-password]: pam_unix(gdm-password:session): session opened for user omar(uid=1001) by (uid=0)
Aug 10 13:41:14 Altayib systemd-logind[897]: New session 7 of user omar.
Aug 10 13:41:14 Altayib systemd: pam_unix(systemd-user:session): session opened for user omar(uid=1001) by (uid=0)
Aug 10 13:41:14 Altayib gdm-password]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
```

Important fields extracted :

UID

EUID

user

Time

Pam unix

- **UID** – The *User ID number* assigned to the account that triggered the action.
- **EUID** – The *Effective User ID*, which determines the actual permissions the process is running with (can differ from UID if privilege escalation occurred).
- **user** – The username of the account involved in the event.
- **Time** – When the event happened.
- **PAM unix** – Refers to the *Pluggable Authentication Module* (PAM) for Unix/Linux; it's the authentication framework logging the event (e.g., login, logout, authentication success/failure).