

# Registros de eventos de autenticación y control de acceso.

**1. Objetivo.** – Analizar los diferentes registros de eventos de autenticación en Linux, para detectar posibles funciones anómalas y accesos no autorizados.

**2. Herramientas.** - Para este laboratorio se utilizaron:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)

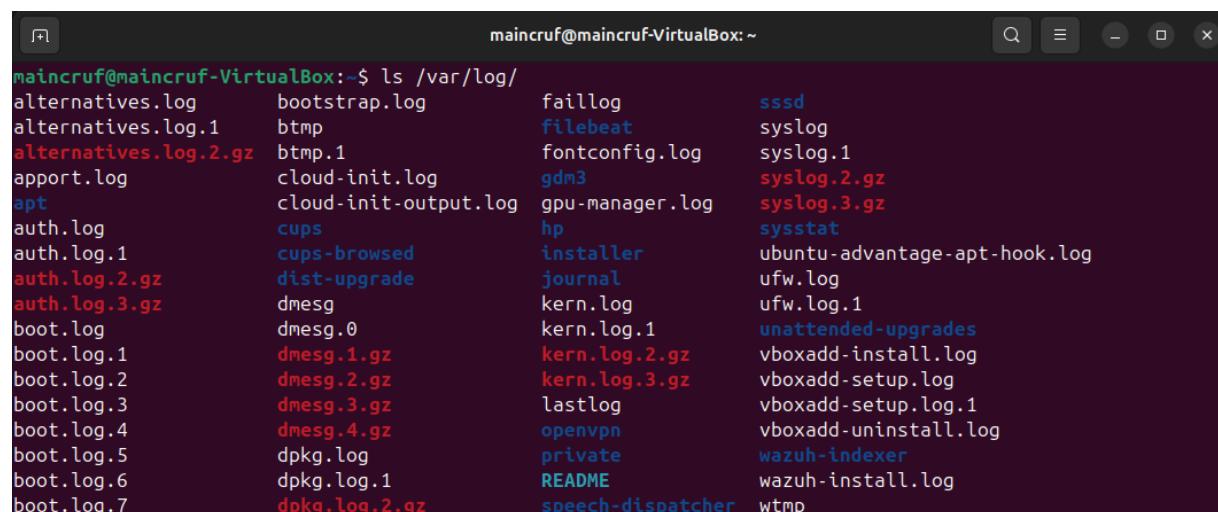
## 3. Metodología / Análisis realizado

Esta sección describe el análisis realizado sobre los logs de autenticación del sistema Linux mediante comandos de línea, monitoreando y simulando acciones sospechosas.

Todos los comandos utilizados se presentan en el Anexo A (página 6).

### 3.1 Verificación de la existencia de logs.

Se identificaron los principales registros de eventos del sistema ubicados en el directorio estándar de logs. Entre los más relevantes se encuentran auth.log, encargado de registrar eventos de autenticación y control de acceso; syslog, que almacena eventos generales del sistema; kern.log, relacionado con eventos del kernel; y ufw.log, que registra actividades del firewall. (ver Figura 1)



```
maincruf@maincruf-VirtualBox:~$ ls /var/log/
alternatives.log      bootstrap.log        faillog          sssd
alternatives.log.1     btmp                filebeat        syslog
alternatives.log.2.gz  btmp.1              fontconfig.log  syslog.1
apport.log             cloud-init.log       gdm3           syslog.2.gz
apt                   cloud-init-output.log gpu-manager.log syslog.3.gz
auth.log               cups                installer       ubuntu-advantage-apt-hook.log
auth.log.1             cups-browsed        journal        ufw.log
auth.log.2.gz          dist-upgrade       kern.log       ufw.log.1
auth.log.3.gz          dmesg              kern.log.1     unattended-upgrades
boot.log               dmesg.0            kern.log.2.gz   vboxadd-install.log
boot.log.1             dmesg.1.gz         kern.log.3.gz   vboxadd-setup.log
boot.log.2             dmesg.2.gz         lastlog        vboxadd-setup.log.1
boot.log.3             dmesg.3.gz         openvpn        vboxadd-uninstall.log
boot.log.4             dmesg.4.gz         private       wazuh-indexer
boot.log.5             dpkg.log          README        wazuh-install.log
boot.log.6             dpkg.log.1        speech-dispatcher  wtmp
boot.log.7             dpkg.log.2.gz
```

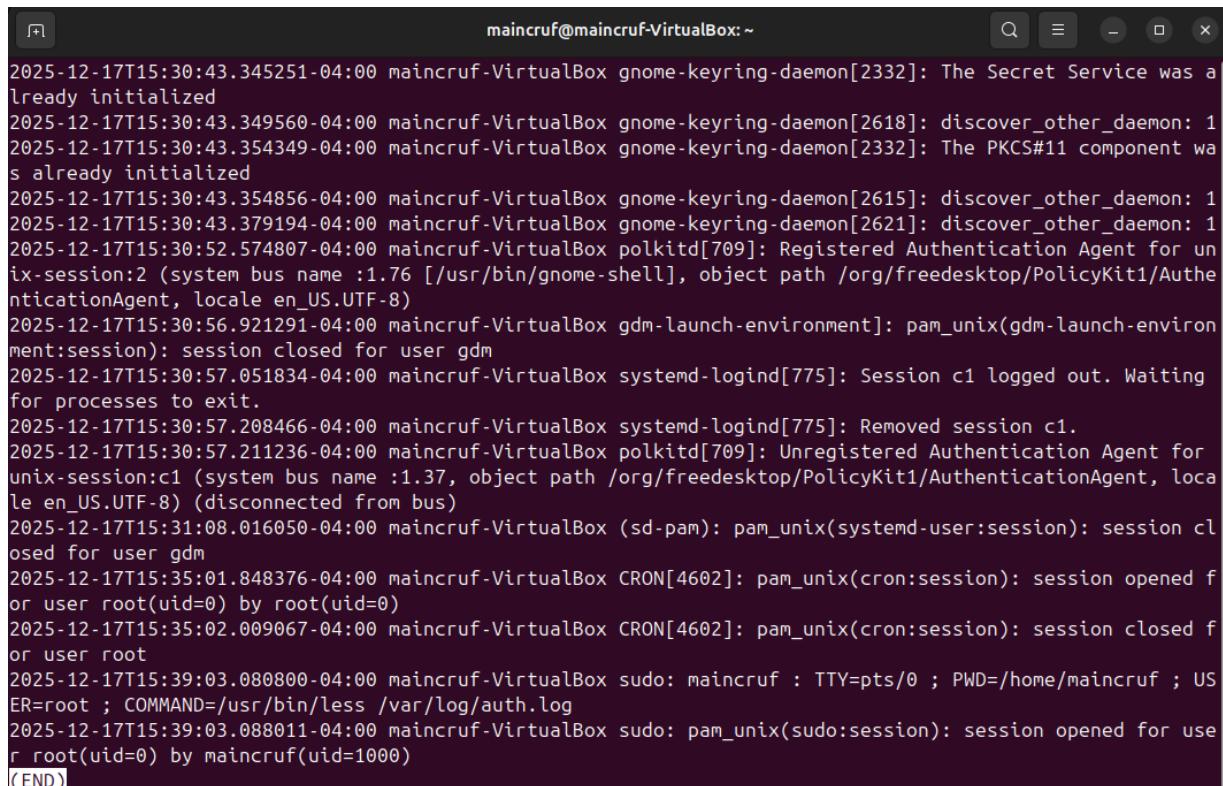
Figura 1. Logs existentes en el sistema

### 3.2 Análisis de eventos de autenticación y control de acceso

Se analizaron los registros de autenticación del sistema con el objetivo de identificar el uso de privilegios elevados, aperturas y cierres de sesión, así como posibles intentos de acceso no autorizado.

Durante el análisis se observaron eventos asociados a la ejecución legítima de comandos mediante el uso de sudo, así como la apertura y cierre controlado de sesiones privilegiadas. No se identificaron intentos fallidos de autenticación ni actividades que sugieran abuso de privilegios. (ver Figura 2)

El análisis de este registro resulta fundamental para detectar accesos no autorizados, escaladas de privilegios indebidas y otros comportamientos anómalos relevantes para la seguridad del sistema.



```
maincruf@maincruf-VirtualBox:~
```

```
2025-12-17T15:30:43.345251-04:00 maincruf-VirtualBox gnome-keyring-daemon[2332]: The Secret Service was already initialized
2025-12-17T15:30:43.349560-04:00 maincruf-VirtualBox gnome-keyring-daemon[2618]: discover_other_daemon: 1
2025-12-17T15:30:43.354349-04:00 maincruf-VirtualBox gnome-keyring-daemon[2332]: The PKCS#11 component was already initialized
2025-12-17T15:30:43.354856-04:00 maincruf-VirtualBox gnome-keyring-daemon[2615]: discover_other_daemon: 1
2025-12-17T15:30:43.379194-04:00 maincruf-VirtualBox gnome-keyring-daemon[2621]: discover_other_daemon: 1
2025-12-17T15:30:52.574807-04:00 maincruf-VirtualBox polkitd[709]: Registered Authentication Agent for unix-session:2 (system bus name :1.76 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
2025-12-17T15:30:56.921291-04:00 maincruf-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session closed for user gdm
2025-12-17T15:30:57.051834-04:00 maincruf-VirtualBox systemd-logind[775]: Session c1 logged out. Waiting for processes to exit.
2025-12-17T15:30:57.208466-04:00 maincruf-VirtualBox systemd-logind[775]: Removed session c1.
2025-12-17T15:30:57.211236-04:00 maincruf-VirtualBox polkitd[709]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.37, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
2025-12-17T15:31:08.016050-04:00 maincruf-VirtualBox (sd-pam): pam_unix(systemd-user:session): session closed for user gdm
2025-12-17T15:35:01.848376-04:00 maincruf-VirtualBox CRON[4602]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-12-17T15:35:02.009067-04:00 maincruf-VirtualBox CRON[4602]: pam_unix(cron:session): session closed for user root
2025-12-17T15:39:03.080800-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/less /var/log/auth.log
2025-12-17T15:39:03.088011-04:00 maincruf-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by maincruf(uid=1000)
(END)
```

Figura 2. Identificación de un usuario y grupos al que pertenece.

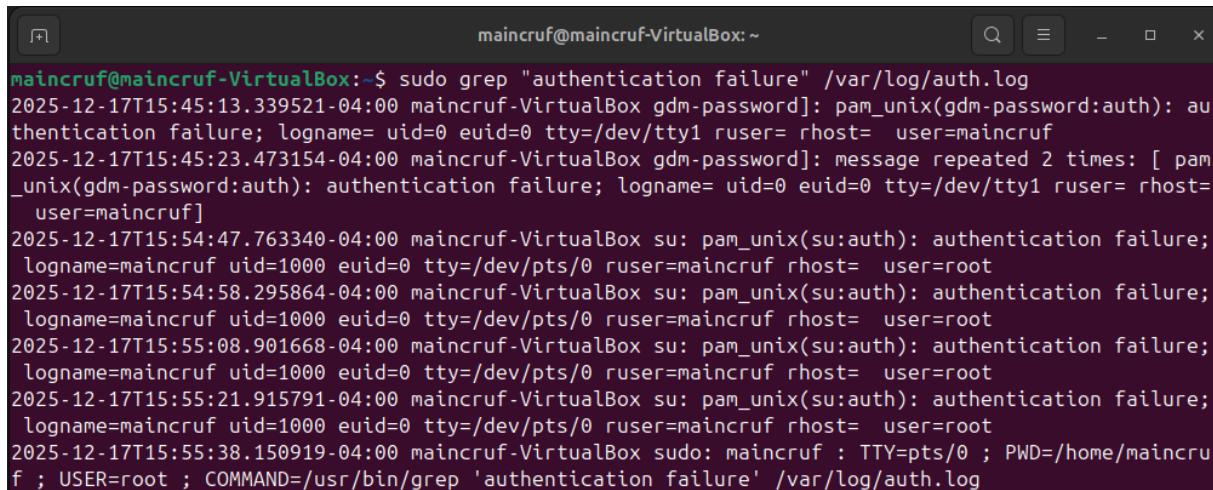
### 3.3 Simulación y monitoreo de eventos de autenticación sospechosos.

Se simularon varios intentos fallidos de autenticación, con el objetivo de generar eventos para lograr visualizarlos. Por otra parte, se utilizó un filtro en el que solo se muestre los eventos de autenticación fallidos para facilitar el monitoreo.

El análisis permitió identificar varios intentos fallidos de autenticación del usuario Maincruf en un lapso de tiempo demasiado corto, pretendiendo subir sus privilegios a

usuario root, utilizando una terminal virtual como medio. Finalmente, se catalogó como un evento sospechoso leve. (ver Figura 3)

Esto resulta relevante desde el punto de vista de la seguridad, ya que permite diferenciar ataques potencialmente peligrosos de falsos positivos.



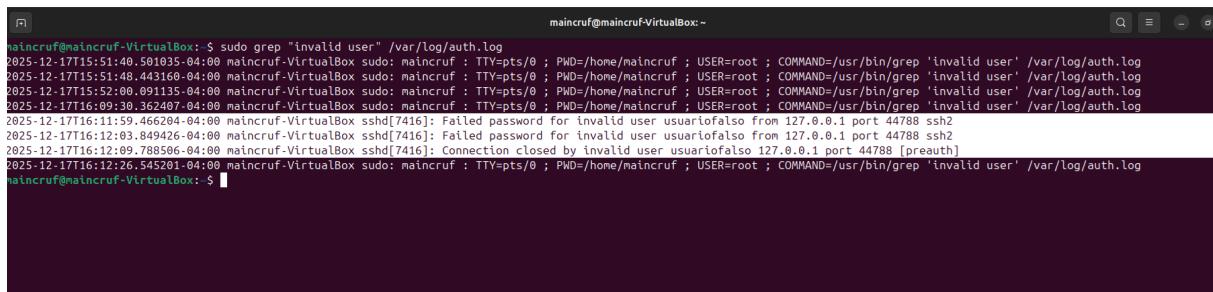
```
maincruf@maincruf-VirtualBox:~$ sudo grep "authentication failure" /var/log/auth.log
2025-12-17T15:45:13.339521-04:00 maincruf-VirtualBox gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=maincruf
2025-12-17T15:45:23.473154-04:00 maincruf-VirtualBox gdm-password]: message repeated 2 times: [ pam_unix(gdm-password:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=maincruf]
2025-12-17T15:54:47.763340-04:00 maincruf-VirtualBox su: pam_unix(su:auth): authentication failure; logname=maincruf uid=1000 euid=0 tty=/dev/pts/0 ruser=maincruf rhost= user=root
2025-12-17T15:54:58.295864-04:00 maincruf-VirtualBox su: pam_unix(su:auth): authentication failure; logname=maincruf uid=1000 euid=0 tty=/dev/pts/0 ruser=maincruf rhost= user=root
2025-12-17T15:55:08.901668-04:00 maincruf-VirtualBox su: pam_unix(su:auth): authentication failure; logname=maincruf uid=1000 euid=0 tty=/dev/pts/0 ruser=maincruf rhost= user=root
2025-12-17T15:55:21.915791-04:00 maincruf-VirtualBox su: pam_unix(su:auth): authentication failure; logname=maincruf uid=1000 euid=0 tty=/dev/pts/0 ruser=maincruf rhost= user=root
2025-12-17T15:55:38.150919-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'authentication failure' /var/log/auth.log
```

**Figura 3.** Autenticaciones fallidas.

### 3.4 Identificación de usuarios inexistentes

Se realizaron varios intentos de autenticación SSH con un usuario inexistente con el propósito de analizar los eventos generados. Posteriormente, se consultó el archivo auth.log con el filtro de usuario no válido para observar dichos eventos, los resultados mostraron la cantidad de intentos, así como la IP y el puerto de origen del usuario no válido, y finalmente el servicio ssh cerró la conexión. (ver Figura 4)

A nivel de un monitoreo de seguridad, estos eventos son muy relevantes para identificar el origen de un ataque malicioso.



```
maincruf@maincruf-VirtualBox:~$ sudo grep "invalid user" /var/log/auth.log
2025-12-17T15:51:40.501035-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'invalid user' /var/log/auth.log
2025-12-17T15:51:48.443160-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'invalid user' /var/log/auth.log
2025-12-17T15:52:00.091135-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'invalid user' /var/log/auth.log
2025-12-17T16:09:30.362407-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'invalid user' /var/log/auth.log
2025-12-17T16:11:59.466204-04:00 maincruf-VirtualBox sshd[7416]: Failed password for invalid user userifalso from 127.0.0.1 port 44788 ssh2
2025-12-17T16:12:03.849426-04:00 maincruf-VirtualBox sshd[7416]: Failed password for invalid user userifalso from 127.0.0.1 port 44788 ssh2
2025-12-17T16:12:09.788506-04:00 maincruf-VirtualBox sshd[7416]: Connection closed by invalid user userifalso 127.0.0.1 port 44788 [preauth]
2025-12-17T16:12:26.545201-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'invalid user' /var/log/auth.log
maincruf@maincruf-VirtualBox:~$
```

**Figura 4.** Detección de usuario no válido

### 3.5 Monitoreo en tiempo real

Se consultaron las últimas líneas del archivo auth.log en tiempo real. Por otra parte, en una segunda terminal, se simularon varios intentos de autenticación fallida para

generar los eventos. Finalmente, se pudieron observar los eventos de autenticación fallida en tiempo real. (Ver Figura 5)

En un escenario de detección temprana, un monitoreo en tiempo real es clave, para una toma de decisiones rápida y oportuna, mejorando así el nivel de seguridad del sistema.

The screenshot shows two terminal windows side-by-side. The left window displays the command `sudo tail -f /var/log/auth.log`, which outputs a stream of log entries from December 17, 2025, at 16:17. These entries include cron jobs running as root and various failed authentication attempts (e.g., su, pam\_unix) from different IP addresses. The right window shows the command `su root` being entered twice, followed by the password prompt and the error message "Authentication failure".

```

Dec 17 16:17
maincruf@maincruf-VirtualBox:~$ sudo tail -f /var/log/auth.log
2025-12-17T16:15:01.197701+04:00 maincruf-VirtualBox CRON[7462]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-12-17T16:15:01.206040+04:00 maincruf-VirtualBox CRON[7462]: pam_unix(cron:session): session closed for user root
2025-12-17T16:15:29.556053+04:00 maincruf-VirtualBox sudo: maincruf : TTY:pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/tail -n 20 /var/log/auth.log
2025-12-17T16:15:29.556986+04:00 maincruf-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by maincruf(uid=1000)
2025-12-17T16:15:29.563001+04:00 maincruf-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-12-17T16:15:50.940614+04:00 maincruf-VirtualBox sudo: maincruf : TTY:pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-12-17T16:15:50.942731+04:00 maincruf-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by maincruf(uid=1000)
2025-12-17T16:15:50.948071+04:00 maincruf-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-12-17T16:16:13.243043+04:00 maincruf-VirtualBox sudo: maincruf : TTY:pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-12-17T16:16:13.248061+04:00 maincruf-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by maincruf(uid=1000)
2025-12-17T16:16:32.675376+04:00 maincruf-VirtualBox su: pam_unix(su:auth): authentication failure; logname=maincruf uid=1000 euid=0 tty=/dev/pts/2 ruser=maincruf rhost= user=root
2025-12-17T16:16:34.119651+04:00 maincruf-VirtualBox su[7593]: FAILED SU (to root) maincruf on pts/2
2025-12-17T16:16:41.681434+04:00 maincruf-VirtualBox su: pam_unix(su:auth): authentication failure; logname=maincruf uid=1000 euid=0 tty=/dev/pts/2 ruser=maincruf rhost= user=root
2025-12-17T16:16:47.249576+04:00 maincruf-VirtualBox su[7594]: FAILED SU (to root) maincruf on pts/2
2025-12-17T16:17:01.249771+04:00 maincruf-VirtualBox CRON[7505]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-12-17T16:17:01.261329+04:00 maincruf-VirtualBox CRON[7505]: pam_unix(cron:session): session closed for user root
maincruf@maincruf-VirtualBox:~$ su root
Password:
su: Authentication failure
maincruf@maincruf-VirtualBox:~$ su root
Password:
su: Authentication failure
maincruf@maincruf-VirtualBox:~$
```

**Figura 5.** Monitoreo en tiempo real.

### 3.6 Identificación de fuerza bruta

Se simularon conexiones SSH con un usuario falso para generar un evento de fuerza bruta. Asimismo, se pudo identificar el origen del ataque y el número de veces que se realizó. (ver Figura 6)

En un contexto de monitoreo, esta información es altamente relevante, ya que se pueden tomar medidas preventivas sobre la IP de origen del ataque, además de analizar si es un falso positivo.

The screenshot shows a terminal window with the command `ssh usuariofalso@localhost`. It displays multiple failed login attempts from the IP address 5.127.0.0.1. The user "usuariofalso" was denied permission on both the local host and the remote host. The final command shown is `sudo grep "Failed password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr`, which counts the occurrences of each IP address in the log file.

```

maincruf@maincruf-VirtualBox:~$ ssh usuariofalso@localhost
usuariofalso@localhost's password:
Permission denied, please try again.
usuariofalso@localhost's password:
Permission denied, please try again.
usuariofalso@localhost's password:
usuariofalso@localhost: Permission denied (publickey,password).
maincruf@maincruf-VirtualBox:~$ sudo grep "Failed password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
5 127.0.0.1
4 COMMAND=/usr/bin/grep
maincruf@maincruf-VirtualBox:~$
```

**Figura 6.** Origen IP del ataque y cantidad de autenticaciones fallidas.

## 4. Acciones recomendadas

Ante la detección de múltiples autenticaciones fallidas e intentos de fuerza bruta, se recomienda aplicar las siguientes medidas:

- Confirmar si hubo accesos exitosos posteriores a los intentos fallidos.
- Bloquear temporalmente la IP origen del ataque.
- Forzar cambio de credenciales del usuario afectado.
- Deshabilitar el login SSH para el usuario root.
- Implementar un mecanismo de protección contra fuerza bruta (fail2ban).

## 5. Resultados obtenidos

En este laboratorio se identificaron varios archivos de registros en el sistema, enfocándose principalmente en el análisis del archivo auth.log para diferenciar los eventos relevantes del ruido. Además, se utilizaron varios comandos en Linux y varias simulaciones de intentos fallidos de autenticación, con el fin de comprender el comportamiento de los eventos que se registran en el sistema.

Como resultado, fue posible identificar distintos registros importantes al momento de detectar posibles ataques o intentos de fuerza bruta, observando tanto el origen como la cantidad de intentos realizados. Si bien un número reducido de intentos fallidos puede corresponder a errores del usuario, patrones repetitivos o distribuidos en el tiempo pueden indicar intentos de fuerza bruta, especialmente cuando afectan a servicios expuestos como SSH. Finalmente, todas estas actividades contribuyeron a mejorar la perspectiva de seguridad que debe tenerse al analizar eventos de autenticación y control de acceso.

## 6. Reflexión final

Este laboratorio permitió comprender la importancia de monitorear, conocer e interpretar los eventos registrados en los procesos de autenticación y control de acceso, aplicando lógica y análisis para determinar si se trata de eventos potencialmente sospechosos o simples falsos positivos. Si bien un SIEM facilita la visualización de este tipo de eventos, la ausencia de esta herramienta obliga a conocer y utilizar comandos en Linux, así como a interpretar manualmente los registros, lo cual fortalece el criterio analítico y la seguridad del sistema.

**Anexo A – Comandos Utilizados**

ls /var/log/

sudo less /var/log/auth.log

sudo grep "authentication failure" /var/log/auth.log

sudo grep "invalid user" /var/log/auth.log

sudo tail -f /var/log/auth.log

su root

ssh usuariofalso@localhost

sudo grep "Failed password" /var/log/auth.log | awk '{print \$(NF-3)}' | sort | uniq -c | sort -nr