***FASE 1:***

## **1. Revisión de logs del sistema**

Se revisaron los siguientes archivos de logs en Linux para detectar eventos sospechosos:

*- /var/log/auth.log*

*- /var/log/syslog*

Comand*o utilizado:*

*sudo less /var/log/auth.log*

Ejemplo de salida:

*2025-07-22T07:19:01.761826+02:00 srv-base-daviniasierra sudo: daviniase : TTY=pts/0 ; PWD=/home/daviniase ; USER=root ; COMMAND=/usr/bin/less /var/log/auth.log*

## **2. Análisis de usuarios conectados y procesos activos**

Se analizaron los usuarios conectados y los procesos en ejecución con los siguientes comandos:

*who  
ps aux*

## **3. Captura y análisis de conexiones de red activas**

Se listaron las conexiones de red activas usando:

*netstat -tulnp  
ss -tulnp*

## **4. Volcado de memoria RAM**

Para capturar la memoria RAM y analizar posibles indicios de actividad maliciosa, se utilizó:

*sudo apt install -y avml*

*sudo ./avml /tmp/memdump.lime*

Este archivo puede analizarse posteriormente con herramientas forenses como Volatility.

***FASE 2:***

# **1. Identificación de accesos fallidos y aceptados vía SSH**

Se utilizaron los comandos *`grep` y `grep -a*` sobre el archivo */var/log/auth.log* para localizar intentos de acceso fallidos y aceptados mediante SSH. El primer intento dio como resultado un mensaje indicando 'coincidencia en fichero binario', por lo que se optó por utilizar *`grep -a*` para forzar la lectura como texto. Las capturas de pantalla muestran la identificación de varios intentos de acceso, incluyendo los aceptados con usuario root, lo cual indica una posible intrusión con éxito.

# **2. Revisión de usuarios en el sistema**

Se consultó el archivo *`/etc/passwd*` para identificar si había usuarios sospechosos o creados recientemente. En las capturas se observan usuarios legítimos como `empleado1` y `empleado2`, sin detectar anomalías evidentes en esta fase.

# **3. Archivos modificados recientemente**

Se utilizó el comando *`find /etc -type f -mtime -3`* para revisar archivos modificados en los últimos 3 días, detectando cambios en archivos críticos como *`/etc/sysctl.conf`, `/etc/ufw/ufw.conf`* y configuraciones de Fail2ban y SSH.

# **4. Revisión de historial de comandos y scripts**

Al intentar leer el historial de comandos de root y del usuario actual, se observó que no existe el archivo *`.bash\_history`*. Además, se buscaron archivos `.sh` en todo el sistema que pudieran indicar presencia de scripts sospechosos, encontrando varios archivos estándar del sistema y configuraciones de OpenVPN. No se detectaron scripts claramente maliciosos, aunque es recomendable revisar su contenido más a fondo.

# **5. Revisión de procesos en ejecución**

Se ejecutó `*ps aux | grep -vE "bash|sshd|init|systemd"*` para filtrar los procesos sospechosos excluyendo los principales del sistema. Las capturas muestran procesos relacionados con el kernel (kthread, kworker), sin indicios claros de procesos maliciosos activos en memoria.

# **Conclusión de la Fase 2**

A pesar de que no se han encontrado evidencias claras de backdoors ni scripts maliciosos activos, la presencia de accesos aceptados con usuario root y modificaciones recientes en archivos críticos justifican una intervención urgente. Es recomendable cambiar contraseñas, revisar los logs con herramientas forenses, y reforzar el sistema con medidas de hardening en la siguiente fase.

***FASE 3:***

**1. Recuperación de archivos eliminados con Foremost**

Se ha utilizado la herramienta Foremost para realizar la recuperación de archivos del disco principal (/dev/sda).

*sudo apt install foremost*

*mkdir ~/recuperacion*

Previamente se ha verificado el dispositivo con el comando `*lsblk*`. La recuperación se ha realizado con el comando:

*sudo foremost -i /dev/sda -o ~/recuperacion*

*lsblk*

La salida de este comando ha generado múltiples archivos con contenido parcialmente legible y otros en formato binario, indicando recuperación de datos eliminados que podrían haber sido manipulados por el atacante. Ver evidencias en las capturas.

**2. Análisis de archivos y binarios recuperados**

Los archivos extraídos contienen tanto datos legibles como contenido en formato binario, lo que indica que podrían tratarse de scripts modificados, ejecutables eliminados o archivos encriptados. Se recomienda un análisis más profundo con herramientas como binwalk, strings o incluso antivirus como ClamAV para confirmar su naturaleza.

**3. Análisis de tráfico de red**

*sudo tcpdump -i any -w captura\_red.pcap*

*tcpdump -nnr captura\_red.pcap | head -n 30*

1. Protocolos detectados:

**ICMPv6 Router Advertisement**: comunicación normal de red para anunciar routers.

**DNS multicast (mDNS, puerto 5353)**: es común en redes locales para resolver nombres tipo \*.local.

**Consultas PTR (reversas de DNS)** hacia ecb5fa93023f.local y Hue Bridge → parece un dispositivo domótico tipo **Philips Hue** o similar.

1. Direcciones IP detectadas:

**192.168.1.153** ↔ red local, no externa.

**224.0.0.251** ↔ IP de multidifusión (usada en mDNS), no peligrosa.

### **Conclusión del análisis de tráfico**

No se detectaron conexiones a servidores externos ni actividades anómalas o maliciosas desde la red. El tráfico capturado parece **propio de una red local doméstica**.

***FASE 4:***

**1. Deshabilitar cuentas comprometidas y restablecer contraseñas**

En esta primera parte de la Fase 4, se procedió a revisar las cuentas de usuario presentes en el sistema, identificar posibles cuentas comprometidas y aplicar medidas correctivas.

1. Revisión de cuentas de usuario en el sistema

Se utilizó el siguiente comando para ver las cuentas registradas en el sistema desde el archivo /etc/passwd:

*sudo tail /etc/passwd*

Esto permitió observar las cuentas de los usuarios 'empleado1' y 'empleado2', así como otras cuentas de sistema.

2. Deshabilitar cuenta de usuario sospechosa

Para prevenir accesos no autorizados, se deshabilitó la cuenta 'empleado2' con el siguiente comando:

*sudo usermod -L empleado2*

3. Restablecimiento de contraseña para usuario

Como medida adicional de seguridad, se restableció la contraseña del usuario 'empleado1':

*sudo passwd empleado1*

Se introdujo una nueva contraseña segura y se confirmó el cambio exitosamente.

## **2. Configuración de Firewall (UFW)**

Se ha utilizado UFW (Uncomplicated Firewall) para configurar políticas más estrictas de acceso.

Ver estado detallado del firewall:  
  *sudo ufw status verbose*

Habilitar el firewall:  
 *sudo ufw enable*

Establecer la política predeterminada:  
 *sudo ufw default deny incoming  
 sudo ufw default allow outgoing*

Permitir acceso por SSH:  
  *sudo ufw allow ssh*

## **3. Implementación de Autenticación Multifactor (2FA)**

Se instaló y configuró Google Authenticator como sistema 2FA para accesos remotos.

Instalación del paquete:  
  *sudo apt install libpam-google-authenticator*

Ejecución del configurador:  
 *google-authenticator*

Modificación del archivo /etc/pam.d/sshd agregando la línea:  
 *auth required pam\_google\_authenticator.so*

Verificación en /etc/ssh/sshd\_config de las siguientes líneas:  
 *ChallengeResponseAuthentication yes  
 UsePAM yes*

Reinicio del servicio SSH:  
 *sudo systemctl restart ssh*

## **4. Gestión de Usuarios**

Se limitaron los accesos únicamente a usuarios autorizados y se bloquearon usuarios comprometidos:

En */etc/ssh/sshd\_config* se añadieron las líneas:  
  *AllowUsers daviniasierra desarrollador  
 DenyUsers elena*

## **5. Habilitación de IDS (Snort)**

Se instaló el sistema de detección de intrusos Snort:

*sudo apt update  
 sudo apt install snort*

Durante la instalación, se configuró el rango de red:  
 *192.168.1.0/24*