***FASE 1:***

**1. Análisis en Windows Server 2022**

Se ha iniciado el análisis a través del Administrador de tareas y con el comando:

*tasklist*

Este comando permite ver todos los procesos activos en el sistema, junto con su PID y uso de memoria.

Posteriormente, se ha guardado esta información en un archivo para su análisis posterior con el comando:

*tasklist > procesos.txt*

Para detectar malware, se ha descargado e instalado la herramienta Malwarebytes desde su página oficial.

Se completó la instalación y se ejecutó el primer escaneo del sistema.

**2. Análisis en Ubuntu Server**

Se ha utilizado el antivirus ClamAV con el fin de escanear el sistema en busca de malware. El comando utilizado fue:

*sudo clamscan -r /*

Durante el análisis aparecieron advertencias relacionadas con la falta de permisos para leer ciertos archivos o módulos del kernel.

Estas advertencias son comunes cuando se escanean rutas del sistema sin permisos suficientes o por archivos protegidos.

**3. Revisión de logs en Linux**

Se ha revisado el archivo de autenticación `/var/log/auth.log` buscando fallos de acceso o errores sospechosos con el comando:

*sudo cat /var/log/auth.log | grep -i "failed\|invalid\|error"*

También se han identificado algunos errores relacionados con conflictos de teclado en el entorno gráfico GNOME y advertencias de librerías (`Gjs-WARNING`),

aunque no están relacionados con malware.

**4. Análisis de puertos y conexiones de red**

Se han listado los servicios que están escuchando en el sistema mediante los comandos:

*sudo ss -tulnp*

*sudo netstat -tulnp*

Se ha detectado que están activos servicios como `squid`, `dovecot`, `mysqld`, `dnsmasq`, y `containerd`,

algunos de los cuales podrían no ser necesarios o haber sido utilizados como punto de entrada o persistencia por un atacante.

**5. Conclusión d**

Se ha completado el análisis inicial de ambos sistemas.

No se han encontrado virus activos visibles en el escaneo,

pero sí advertencias, servicios abiertos innecesarios y configuraciones que podrían ser aprovechadas para comprometer el sistema.

***FASE 2:***

1. Buscar archivos con extensiones inusuales como '.encrypted':

*sudo find / -type f -name "\*.encrypted" 2>/dev/null*

2. Calcular el hash MD5 del archivo comprimido con evidencias:

*sudo md5sum /root/evidencia\_basica.tar.gz*

3. Buscar información sobre ese hash en VirusTotal (si no se encuentra, se analiza manualmente):

Buscar manualmente en *https://www.virustotal.com*

4. Extraer el contenido del archivo .tar.gz en un directorio específico:

*mkdir ~/analisis\_malware  
 sudo tar -xzf /root/evidencia\_basica.tar.gz -C ~/analisis\_malware*

5. Listar todo el contenido extraído de forma recursiva:

*ls -R ~/analisis\_malware*

6. Buscar accesos no autorizados o denegados en logs de MySQL:

*zgrep "unauthorized\|denied" ~/analisis\_malware/var/log/mysql/error.log\**

7. Comprobar existencia de informes de herramientas de seguridad como Lynis (en este caso no se encontró el archivo):

*sudo cat ~/analisis\_malware/var/log/lynis-report.dat*

Con esta información se puede empezar a identificar patrones anómalos en el sistema comprometido. La revisión manual de logs, la identificación de archivos sospechosos y los accesos fallidos permiten comprender mejor la magnitud del ataque.

***FASE 3:***

## **1. Detener procesos maliciosos**

Se utilizó el comando para buscar procesos sospechosos relacionados con malware:

*ps aux | grep -i malware*

No se detectaron procesos activos sospechosos.

## **2. Eliminar archivos infectados de manera segura**

Se utilizaron los comandos para eliminar de forma segura los binarios detectados como sospechosos:

*sudo shred -u /home/davinia/usr/bin/aplaymidi*

*sudo shred -u /home/davinia/usr/bin/ntfswipe*

Archivos eliminados de forma segura.

## **3. Restaurar archivos importantes desde copias de seguridad**

Se intentó restaurar desde una copia de seguridad con:

*sudo tar -xzf /ruta/de/la/copia.tar.gz -C /ruta/de/restauracion*

No se dispone de copias de seguridad disponibles, por lo tanto no se pudo realizar restauración.

## **4. Analizar registros para comprobar limpieza del sistema**

Se buscaron errores o rastros de actividad sospechosa mediante:

*sudo grep -Ei 'error|fail|unauthorized|denied|malware' ~/analisis\_malware/var/log/\*.log*

No se encontraron entradas sospechosas en los registros.

***FASE 4:***

## **Paso 1: Habilitar y configurar antivirus (ClamAV)**

*sudo apt update*

*sudo apt install clamav clamav-daemon -y*

*sudo systemctl stop clamav-freshclam*

*sudo freshclam*

*sudo systemctl start clamav-freshclam*

*sudo systemctl enable clamav-daemon*

*sudo clamscan -r /home*

## **Paso 2: Escaneo y eliminación de malware**

*sudo clamscan -r --remove=yes /ruta/a/escaneo*

## **Paso 3: Aplicar listas blancas con AppArmor**

*sudo apt install apparmor apparmor-utils -y*

*sudo systemctl enable apparmor*

*sudo systemctl start apparmor*

*sudo apparmor\_status*

*sudo aa-enforce /etc/apparmor.d/usr.bin.nano*

## **Paso 4: Fortalecer reglas del firewall (UFW)**

*sudo apt install ufw -y*

*sudo ufw enable*

*sudo ufw default deny incoming*

*sudo ufw default allow outgoing*

*sudo ufw allow ssh*

*sudo ufw deny 4444*

*sudo ufw deny 1337*

*sudo ufw deny 31337*

*sudo ufw status verbose*

## **Paso 5: Activar autenticación 2FA y reforzar accesos**

*sudo apt install libpam-google-authenticator -y*

*google-authenticator*

*sudo nano /etc/pam.d/sshd # Añadir: auth required pam\_google\_authenticator.so*

sudo nano /etc/ssh/sshd\_config # Cambiar:  
 *ChallengeResponseAuthentication yes  
 UsePAM yes*

*sudo systemctl restart sshd*