Reto de Análisis de Red y Auditoría de Seguridad en Linux

🔹 Fase 1: Análisis de red y descubrimiento de hosts

```
nmap -sn 192.168.1.0/24                  # Escaneo de red para descubrir hosts activos
nmap -sS -p- 192.168.1.X                 # Escaneo completo de puertos en un host específico
nmap -sV 192.168.1.X                     # Detección de versiones de servicios
nmap -O 192.168.1.X                      # Detección de sistema operativo (requiere permisos root)
```

🔹 Fase 2: Evaluación de seguridad en servidores Linux

```
sudo apt install lynis chkrootkit rkhunter   # Instalación de herramientas
sudo lynis audit system                      # Auditoría general con Lynis
sudo chkrootkit                              # Búsqueda de rootkits
sudo rkhunter --check                        # Revisión de malware y configuración
sudo cat /etc/passwd | grep -v ':/sbin/nologin'   # Verificación de usuarios con acceso
sudo systemctl list-units --type=service     # Servicios activos
sudo apt list --upgradable                   # Revisión de actualizaciones pendientes
```

🔹 Fase 3: Simulación de riesgos internos

```
nmap -A 192.168.1.0/24                   # Simulación de escaneo tipo atacante interno
netstat -tuln                            # Ver servicios y puertos abiertos
cat /etc/shadow                          # (Solo accesible si se eleva privilegios)
find / -perm -4000 -type f 2>/dev/null   # Archivos con SUID (potenciales vectores)
```

🔹 Fase 4: Propuestas técnicas de mejora

Esta fase es más de análisis y documentación manual:

Puedes usar hojas de cálculo o Markdown para crear:

- Tabla de vulnerabilidades (nombre, criticidad, solución)

- Sugerencias: iptables, bastionado, sshd_config, etc.