Reto de Análisis de Red y Auditoría de Seguridad en Linux

🔹 **Fase 1: Análisis de red y descubrimiento de hosts**

- Se escaneó la red con herramientas como Nmap para identificar dispositivos activos.
- Se registraron puertos abiertos y servicios activos (SSH, HTTP, FTP, etc.).
- Se intentó detectar sistemas operativos en hosts accesibles.

Errores comunes:

- 🔸 *Nmap no detecta dispositivos*: Puede ser por firewall activo o red mal configurada.
  ➤ **Solución**: Verificar conectividad (`ping`) y desactivar temporalmente el firewall si es necesario.
- 🔸 *Permiso denegado para escaneos avanzados*:
  ➤ **Solución**: Ejecutar con `sudo` para permitir escaneo de sistema operativo y servicios.

🔹 **Fase 2: Evaluación de seguridad en servidores Linux**

- Se usaron Lynis, chkrootkit y rkhunter para auditar configuración, usuarios y servicios.
- Se revisaron procesos activos, actualizaciones pendientes y permisos críticos.

Errores comunes:

- 🔸 *Herramientas no instaladas o no detectadas*:
  ➤ **Solución**: Asegurarse de tener acceso a los repositorios (`sudo apt update`) e instalar correctamente.
- 🔸 *Advertencias falsas o genéricas en los informes*:
  ➤ **Solución**: Analizar manualmente los hallazgos y aplicar solo los relevantes.

🔹 **Fase 3: Simulación de riesgos internos**

- Se simuló un escaneo desde un cliente sin privilegios para identificar información expuesta.
- Se documentó el acceso posible sin elevación de permisos.

Errores comunes:

- 🔸 *El usuario no obtiene datos útiles*:
  ➤ **Solución**: Comprobar si hay errores de permisos mal asignados o servicios expuestos de forma innecesaria.
- 🔸 *Escaneo bloqueado por reglas de firewall interno*:
  ➤ **Solución**: Revisar reglas de iptables/ufw que afecten la red interna.

🔹 **Fase 4: Propuestas técnicas de mejora**

- Se redactó una tabla con vulnerabilidades, criticidad y solución propuesta.
- Se recomendó la segmentación de red, cierre de servicios innecesarios y bastionado de sistemas.

Errores comunes:

- 🔸 *No se priorizan bien las vulnerabilidades*:
  ➤ **Solución**: Clasificarlas según impacto y facilidad de explotación (bajo, medio, alto).
- 🔸 *No se aplican medidas por desconocimiento técnico*:
  ➤ **Solución**: Documentar y justificar cada solución de forma clara y comprensible para su implementación.