***FASE 1:***

**1. Descubrimiento de Hosts Activos**

Se ha realizado un escaneo de la red local 192.168.1.0/24 para identificar los dispositivos activos. El comando utilizado fue:

*nmap -sn 192.168.1.0/24*

A continuación se muestran algunos de los dispositivos detectados en la red interna:

IP Detectada Puertos Abiertos Servicios Sistema Operativo (si se detectó)

192.168.1.1 80, 443 HTTP, HTTPS Router Puerta de enlace

192.168.1.128 - - - Equipo activo

192.168.1.130 - - - Equipo activo

192.168.1.201 22 SSH Ubuntu Servidor base (DaviniaSierra)

**2. Conclusiones de la Fase 1**

La red interna contiene múltiples dispositivos activos, algunos con servicios expuestos (como SSH). Esta fase permite sentar las bases para identificar posibles vectores de ataque.

Se recomienda continuar con las siguientes fases de la auditoría para profundizar en la seguridad de configuraciones y sistemas.

***FASE 2:***

# **1. Herramientas de Auditoría Ejecutadas**

- Lynis: ejecutado correctamente con `sudo lynis audit system`.  
 - chkrootkit: ejecutado correctamente con `sudo chkrootkit`, sin infecciones detectadas.  
 - rkhunter: ejecutado con `sudo rkhunter --check`, sin anomalías críticas detectadas.

# **2. Configuraciones y Servicios Analizados**

- Usuarios sin contraseña: NO se detectaron usuarios sin contraseña.

- Servicios activos: Se detectaron muchos servicios en ejecución, incluyendo algunos posiblemente innecesarios como CUPS, Bluetooth, y GNOME Desktop en un servidor.  
 - Sistema actualizado: El sistema indica solo 2 paquetes pendientes de actualización, en general está actualizado.  
 - ACcesos recientes revisados con `last`, sin accesos sospechosos.  
 - Procesos activos revisados con `top` y `ps aux`, los procesos que más consumen recursos son `gnome-shell` y `mysqld`.

# **3. Recomendaciones de Mejora**

- Desactivar servicios innecesarios en servidores, como CUPS, GNOME Desktop o servicios gráficos, si no se utilizan.  
 - Establecer un sistema de actualizaciones regulares para garantizar parches de seguridad al día.  
 - Seguir utilizando herramientas como Lynis periódicamente para detectar cambios en la seguridad del sistema.  
 - Configurar alertas para accesos no autorizados o cambios en servicios críticos.

# **4. Conclusiones**

La auditoría ha demostrado que el sistema es en general seguro, sin presencia de rootkits y con configuración adecuada de usuarios. Se han detectado servicios en ejecución que podrían desactivarse si no se necesitan para mejorar la seguridad y eficiencia del servidor.

***FASE 3:***

En esta tercera fase del reto de Auditoría Técnica de Seguridad de Infraestructura en Codearts Solutions, se ha llevado a cabo una simulación de riesgos internos.  
 El objetivo es analizar qué información puede obtener un usuario con acceso a la red interna y sin privilegios, simulando así el comportamiento de un atacante desde dentro.

# **1. Simulación desde cliente-ntp**

Se ha utilizado la máquina cliente `cliente-ntp` como equipo atacante interno.  
 Desde ella se ha realizado un escaneo con Nmap al servidor `192.168.1.201` utilizando el siguiente comando:  
  
 nmap -sV 192.168.1.201  
  
 El resultado indica que el servidor parece estar activo pero bloquea las peticiones ICMP (ping), por lo que Nmap no pudo detectar los puertos ni servicios abiertos con la configuración inicial.  
  
**2. Posibles vectores de ataque**

Aunque no se obtuvieron resultados específicos en el escaneo debido al bloqueo de ping por parte del servidor, se pueden considerar los siguientes vectores comunes que podrían existir si no se han aplicado buenas prácticas:  
  
 - Puertos abiertos sin cifrado (HTTP, FTP, Telnet)  
 - Versiones de servicios obsoletos o vulnerables  
 - Posibles contraseñas por defecto en servicios como MySQL o SSH  
  
 Para una detección más efectiva, se recomienda usar:  
  
 nmap -Pn -sV 192.168.1.201  
  
 Esto fuerza el escaneo incluso si el host no responde a ping.  
  
**3. Conclusiones**

La simulación demuestra que un atacante interno con acceso a la red puede ejecutar herramientas de escaneo como Nmap.  
 Aunque el servidor auditado bloquea peticiones ping, lo cual mejora la seguridad pasiva, sería recomendable revisar los servicios visibles desde fuera y desactivar aquellos no necesarios o no cifrados.

***FASE 4:***

En esta cuarta y última fase del reto de Auditoría Técnica de Seguridad de Infraestructura en Codearts Solutions, se presentan las propuestas técnicas de mejora en base a las vulnerabilidades y hallazgos detectados durante las fases anteriores.

# **1. Vulnerabilidades Detectadas y Soluciones**

| Vulnerabilidad | Nivel de Criticidad | Solución Recomendada |
| --- | --- | --- |
| Servicios innecesarios activos (ej: CUPS, GNOME) | Media | Desactivar servicios no usados en servidores |
| Bloqueo de ping dificulta auditorías internas | Baja | Permitir ping ICMP desde red local solo para administración |
| Servicios potencialmente visibles sin cifrado | Alta | Reemplazar con versiones cifradas (ej: HTTP → HTTPS) |
| Sistema con paquetes sin actualizar | Media | Ejecutar actualizaciones periódicas automáticas |
| Acceso posible a servicios internos desde otras máquinas | Alta | Usar firewall o listas de control de acceso |

# **2. Propuesta de Segmentación de Red**

Se recomienda dividir la red interna en subredes según su función para limitar el alcance de posibles atacantes internos:  
- Subred para servidores administrativos  
- Subred para estaciones de trabajo de usuarios  
- Subred tipo DMZ para servicios expuestos al exterior  
  
El uso de firewalls internos o VLANs permitirá controlar el tráfico entre segmentos y reducir el riesgo de propagación de ataques.

# **3. Bastionado y Políticas de Seguridad**

- Bastionado de servidores:  
 - Eliminar interfaz gráfica (GNOME) si no es necesaria.  
 - Mantener solo los servicios esenciales: SSH, NTP, MySQL, etc.  
 - Revisar y restringir los permisos de archivos y directorios sensibles.  
  
- Cierre de servicios innecesarios:  
 - Desactivar servicios como `cups`, `bluetooth`, `gnome-remote-desktop`, etc.  
  
- Políticas de registro de logs:  
 - Asegurar que los registros (`logs`) del sistema estén activos y configurados (rsyslog o journald).  
 - Enviar los logs a un servidor externo si es posible para conservarlos seguros.  
 - Revisar los logs de forma periódica para detectar accesos no autorizados o errores críticos.

# **4. Conclusión**

Estas medidas ayudarán a reforzar la seguridad de la infraestructura tecnológica de Codearts Solutions, minimizando los riesgos de accesos no autorizados, propagación de malware o fugas de información interna.