PRÁCTICA N° 1

HARDENING.

# OBJETIVOS

* 1. Fortalecer la seguridad de un computador con distribución Ubuntu mediante configuraciones básicas y avanzadas.
  2. Identificar y mitigar configuraciones inseguras.
  3. Aplicar buenas prácticas de seguridad en dispositivos finales.

# MARCO TEÓRICO

## Hardening

El Hardening consiste en fortalecer un sistema para protegerlo frente a posibles amenazas desconocidas. Los administradores de sistemas deben reforzar las configuraciones de una instalación teniendo en cuenta las amenazas que consideran probables.

Por otro lado, el Hardening de servidores involucra tanto a los equipos de operaciones informáticas como a los de seguridad, y requiere ajustes en las configuraciones predeterminadas basados en las mejores prácticas del sector. En esencia, el Hardening es el arte de implementar medidas adecuadas, incluso si inicialmente no parecen significativas. Siempre se trata de encontrar el equilibrio entre la usabilidad y la protección

# TRABAJO PREPARATORIO

* 1. Revisar y explicar de manera breve comandos básicos para gestionar usuarios y permiso en Linux.
  2. Explicar y detallar para que sirve el comando chmod, sus especificaciones y las formas o modos para asignar permisos
  3. Definir que es tráfico saliente y entrante, además explicar su diferencia.
  4. Investigar que es SSH, configuración básica y la seguridad en SSH en un sistema operativo Linux.
  5. Consultar Consultar que es Lynis y su propósito en la auditoría de seguridad.

# EQUIPO Y MATERIALES

* Oracle VM Virtual Box o VMWare Player.
* Máquina virtual con distribución Ubuntu/Debian/CentOS
* Internet.

# PROCEDIMIENTO

**Parte A: Configuración de *usuarios* y *permisos***

1. **Verificar usuarios y grupos existentes:**

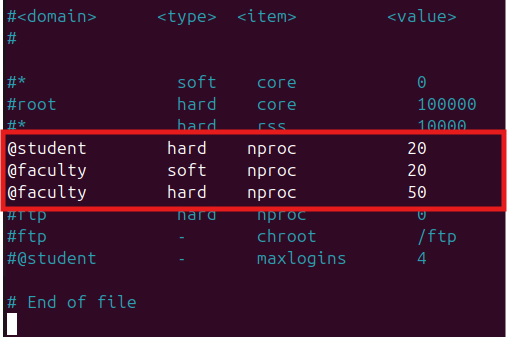
* Se abre un terminal y se ejecuta los siguientes comandos: cat /etc/passwd, cat /etc/group para listar los usuarios y grupos del sistema.
* Identifica usuarios innecesarios y elimínalos con el comando: sudo userdel -r nombre\_usuario.

1. **Configurar permisos en archivos sensibles**

* Verifica los permisos de los archivos críticos /etc/passwd y /etc/shadow con el comando ls -l
* Se ajusta los permisos a niveles recomendados de seguridad con los comandos: sudo chmod 644 /etc/passwd, sudo chmod 600 /etc/shadow.

1. **Configurar restricciones de recursos**

* Edita el archivo de límites de seguridad, para esto se utiliza el comando sudo nano /etc/security/limits.conf.
* Agrega una regla para restringir recursos, con lo siguiente nombre\_usuario hard nproc 50.



Se puede variar el valor y tipo de restricción. Luego se guarda y se cierra el archivo.

**Parte B: Configuración Segura de SSH**

* 1. Instalación del servicio
* Se instala con el siguiente comando sudo apt-get install ssh.
  1. Configurar el servicio SSH
* Edita el archivo de configuración, para esto se utiliza el comando sudo nano /etc/ssh/sshd\_config
* Realiza los siguientes cambios, tal y como se muestra en la figura 2.7.:
  + 1. Deshabilitar acceso como root:

PermitRootLogin no

* + 1. Cambiar el puerto de SSH (se puede cambiar a cualquiera):

Port 2222

* + 1. Asegurar el protocolo:

Protocol 2

* Guarda y reinicia el servicio SSH, con el comando sudo /etc/init.d/ssh restart.

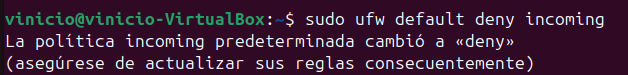
**Parte C: Configuración de Firewall**

1. Instalar UFW si no está disponible con el siguiente comando sudo apt install ufw.
2. Habilita UFW y permite el puerto 2222 con los siguientes comandos:

sudo ufw allow 2222/tcp

sudo ufw enable

1. Verificar las reglas activas con: sudo ufw status verbose.
2. Bloquea todo el tráfico entrante excepto el puerto SSH con: sudo ufw default deny incoming.



**PARTE D: Auditoría del Sistema con Lynis**

1. Instalar Lynis con el siguiente comando sudo apt install lynis.
2. Realizar un análisis del sistema con: sudo lynis audit system.

# INFORME

* 1. Documentar las configuraciones aplicadas.
  2. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.
  3. Generar un par de claves pública y privada utilizando ssh-keygen de manera que se tenga acceso al servidor solo mediante claves SSH.
  4. Instalar y ejecutar chkrootkit para verificar la presencia de rootkits, además documentar y analizar los hallazgos.

# REFERENCIAS

**[1] "The Practical Linux Hardening Guide" GitHub. https://github.com/trimstray/the-practical-linux-hardening-guide?tab=readme-ov-file#the-importance-of-hardening-linux (accessed Dec 03. 2024)**