Autor: Gregorio Camilo Bastreri Barilá

Actividad: Se realizó un escaneo básico para detectar vulnerabilidades de versiones y escaneo de puertos desde una máquina Kali hacia una máquina Debian.

Los comandos que se usaron fueron:
sudo nmap 192.168.1.147

sudo nmap -sV 192.168.1.147

sudo nmap -sV --script=vuln 192.168.1.147

Puerto	Servicio	Versión	Vulnerabilidad	Descripcion	Referencia
22	SSH	OpenSSH	CVE-2023-38408	Es una falla grave en el sistema de reenvío de agentes SSH. En ciertas configuraciones, un atacante que logre conectarse por SSH puede ejecutar comandos o código malicioso en el servidor sin autorización	https://nvd.nist.gov/vuln/detail/CVE-2023-38408
22	SSH	OpenSSH	CVE-2024-6387	Es un problema en cómo SSH maneja señales del sistema. Podría permitir a un atacante remoto ejecutar código en el servidor o hacer que el servicio SSH se cierre inesperadamente.	https://nvd.nist.gov/vuln/detail/CVE-2024-6387
22	SSH	OpenSSH	CVE-2025-26465	Esta vulnerabilidad puede causar un error o bloqueo del servicio SSH durante la autenticación, lo que permite a un atacante provocar una denegación de servicio (DoS) y dejar el servicio temporalmente inaccesible.	https://vulners.com/cve/CVE-2025-26465
80	HTTP	Apache 2.4.65	CVE-2023-25690	Es un fallo en el proxy de Apache. Permite que un	https://nvd.nist.gov/vuln/detail/CVE-2023-25690

				atacante modifique las peticiones HTTP antes de que lleguen al servidor.	
80	HTTP	Apache 2.4.65	CVE-2023-31122	Apache procesa las cabeceras HTTP. Si se envían datos especialmente diseñados, puede provocar un desbordamiento de memoria	https://nvd.nist.gov/vuln/detail/CVE-2023-31122