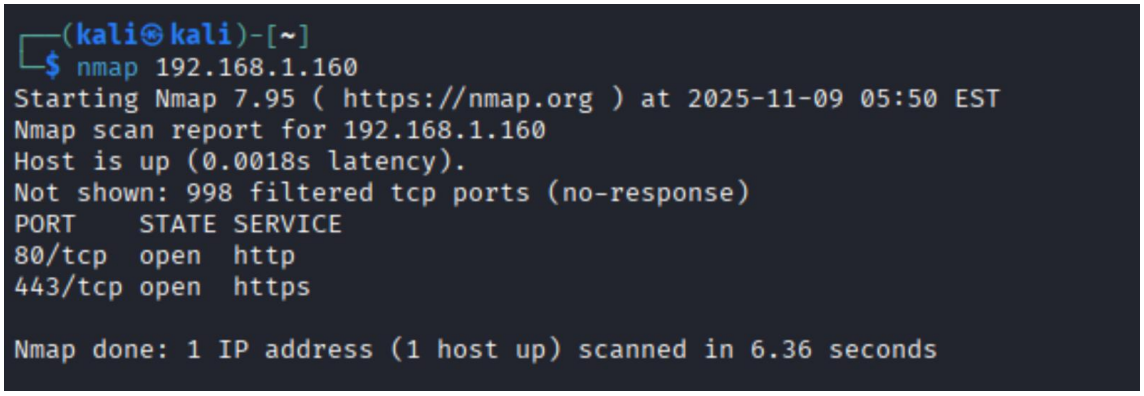
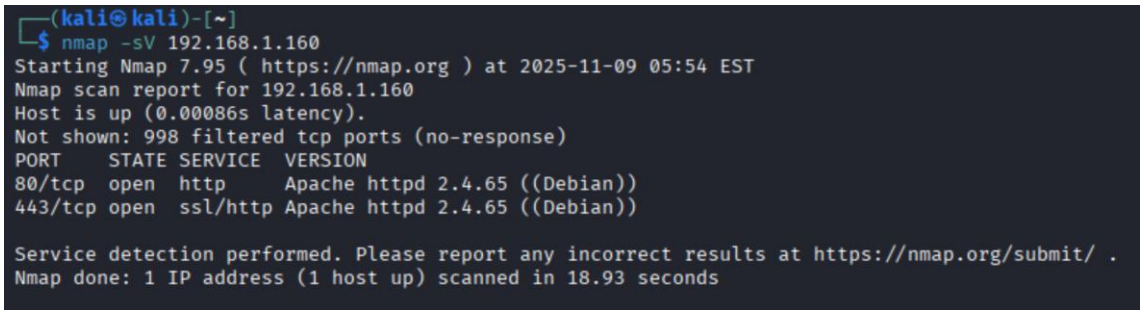
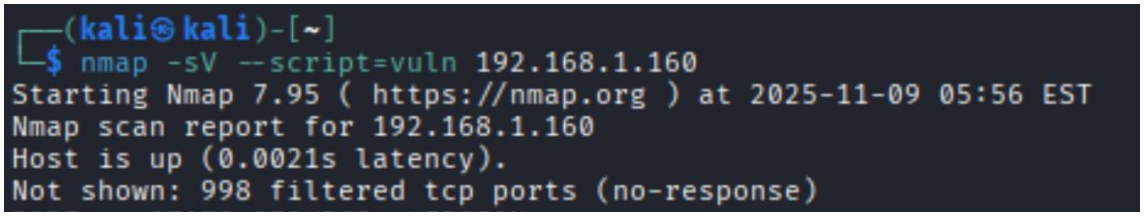
ESCANEO PUERTOS CON NMAP



Se usa el comando nmap IP para detectar los puertos abiertos que tiene una IP, en este caso hay dos puertos abiertos, el 80 para HTTP y el 443 para HTTPS



Se usa el comando nmap -sV IP para detectar los puertos y detectarla versión del servicio que está operando en cada puerto.



Se usa el comando nmap -sV –script=vuln IP para realizar un escaneo detallado y una búsqueda de vulnerabilidades gracias a la ejecución del script “vuln” que tiene incorporado nmap.

Host is up significa que el equipo objetivo está encendido y accesible.

El escaneo de puertos se realiza entre los 1000 puertos más comunes, no han respondido 998, solo han respondido el 80 y 443.

El resultado de la búsqueda de vulnerabilidades ha detectado las mismas vulnerabilidades en el puerto 80 y en el puerto 443 debido a que usan el mismo servicio que es Apache httpd 2.4.65.

Puerto	Estado	Servicio	Versión
80/tcp	open	http	**Apache httpd 2.4.65**
443/tcp	open	ssl/http	**Apache httpd 2.4.65**

No se han detectado las siguientes vulnerabilidades:

- Tipo CSRF (Cross-site request forgery)
- Tipo XSS (Cross-Site Scripting)
- Tipo XSS basado en DOM

Las vulnerabilidades que ha encontrado te las indica de la siguiente manera:

Origen + Nota CVSS + página web donde se puede encontrar información sobre vulnerabilidad + *EXPLOIT* (esta última no siempre aparece, ya que depende de si se ha publicado cómo atacar esta vulnerabilidad, si se ha publicado aparece *EXPLOIT*).

La nota CVSS (Common Vulnerability Scoring System) van desde 0.0 hasta 10.0.

Puntuación CVSS	Categoría de Gravedad
0.0	Ninguna / Informativa
0.1 – 3.9	Baja
4.0 – 6.9	Media
7.0 – 8.9	Alta
9.0 – 10.0	**Crítica**

Ha encontrado 15 vulnerabilidades de categoría crítica con 9 de puntuación CVSS o más, 7 de las 15 tienen el código para llevar a cabo el ataque de acceso público.

Ha encontrado 27 vulnerabilidades de categoría alta con 7 de puntuación CVSS o más, 9 de las 27 tienen el código para llevar a cabo el ataque de acceso público.

Ha encontrado 11 vulnerabilidades de categoría media con 4 de puntuación CVSS o más, 1 de las 11 tienen el código para llevar a cabo el ataque de acceso público.

Ha encontrado 2 vulnerabilidades de categoría informativa con 0 de puntuación CVSS, las 2 tienen el código para llevar a cabo el ataque de acceso público.

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80/443	HTTP/HTTPS	Apache 2.4.65	CNVD-2024-36391	Divulgación de información sensible	https://vulners.com/cnvd/CNVD-2024-36391
80/443	HTTP/HTTPS	Apache 2.4.65	CVE-2020-11984	Desbordamiento de Búfer en el módulo mod_proxy_uwsgi	https://www.cvedetails.com/cve/CVE-2020-11984
80/443	HTTP/HTTPS	Apache 2.4.65	CVE-2024-40898	Falsificación de solicitudes del lado del servidor (SSRF) en sistemas Windows	https://www.cvedetails.com/cve/CVE-2024-40898
80/443	HTTP/HTTPS	Apache 2.4.65	CNVD-2024-33814	Divulgación de hashes NTLM a servidores maliciosos	https://vulners.com/cnvd/CNVD-2024-33814
80/443	HTTP/HTTPS	Apache 2.4.65	CVE-2019-0211	Escalada de privilegios local, se le llama Carpe Diem	https://www.cvedetails.com/cve/CVE-2019-0211
80/443	HTTP/HTTPS	Apache 2.4.65	CNVD-2025-16603	Permite un ataque DoS	https://vulners.com/cnvd/CNVD-2025-16603
80/443	HTTP/HTTPS	Apache 2.4.65	CNVD-2019-08945	Divulgación de información relacionada con el manejo de URL del módulo mod_rewrite	https://vulners.com/cnvd/CNVD-2019-08945

El script http-enum ha descubierto que hay una instalación de WordPress y la página de inicio de sesión de WordPress.