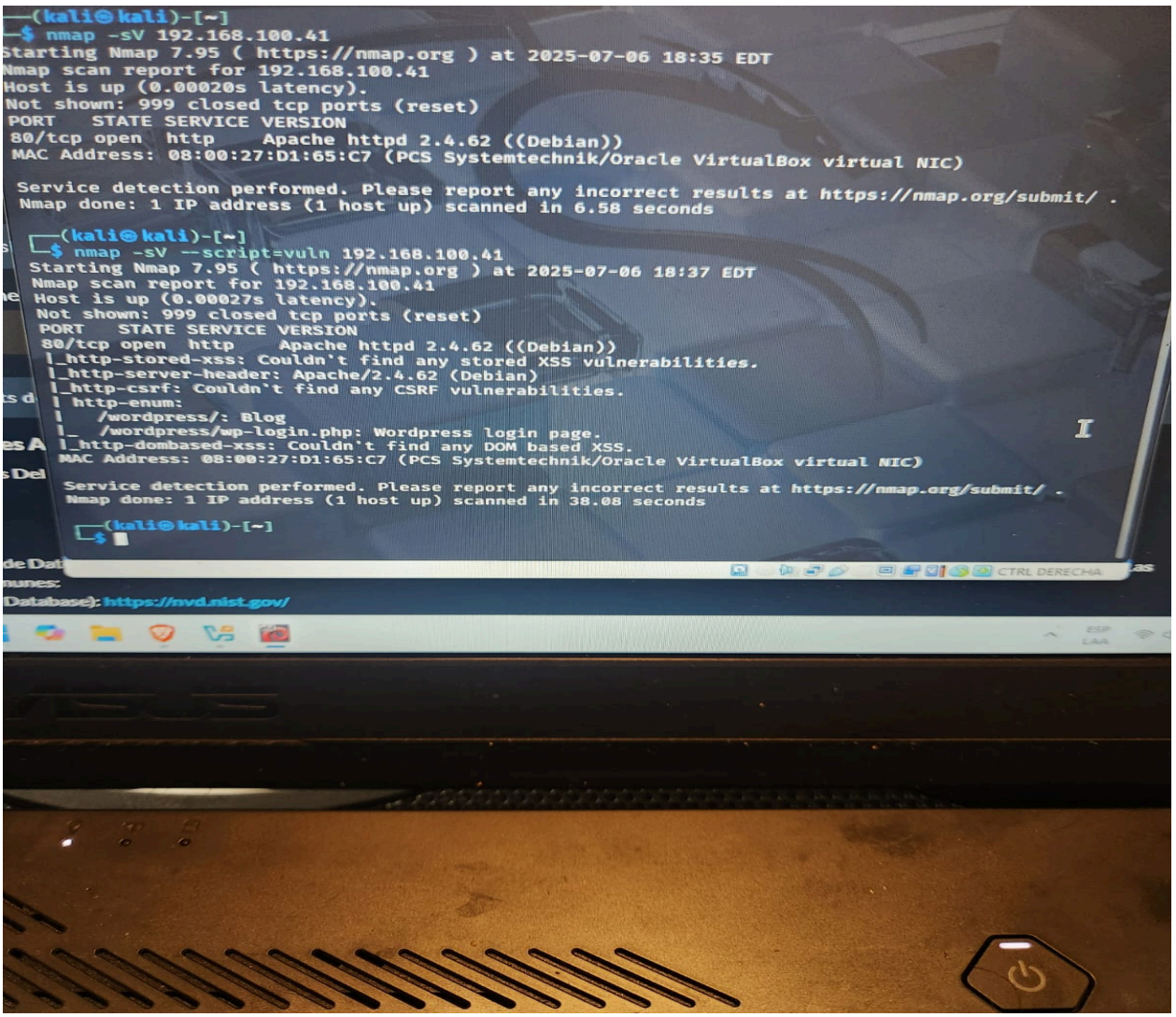
Escaneando vulnerabilidades con nmap

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP	Apache 2.4.62	**CVE-2024-40725**	°Ignora cierto uso de la configuración heredada de controladores basada en tipos de contenido. "AddType" y configuraciones similares, en algunas circunstancias en las que los archivos se solicitan indirectamente, dan como resultado la divulgación del contenido local en el código fuente.	https://nvd.nist.gov/vuln/detail/CVE-2024-40725
			CVE-2024-40898	°Permite potencialmente filtrar hashes NTML a un servidor malicioso a través de SSRF y solicitudes maliciosas.	https://nvd.nist.gov/vuln/detail/CVE-2024-40898


(kali㉿kali)-[~]
$ nmap -sV 192.168.100.41
Starting Nmap 7.95 (https://nmap.org) at 2025-07-06 18:35 EDT
Nmap scan report for 192.168.100.41
Host is up (0.00020s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
(kali㉿kali)-[~]
$ nmap -sV --script=vuln 192.168.100.41
Starting Nmap 7.95 (https://nmap.org) at 2025-07-06 18:37 EDT
Nmap scan report for 192.168.100.41
Host is up (0.00027s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.62 ((Debian))
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.62 (Debian)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
| /wordpress/: Blog
|_ /wordpress/wp-login.php: Wordpress login page.
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.08 seconds
(kali㉿kali)-[~]
$
CTRL DERECHA
Database): https://nvd.nist.gov/