ESCANEO CON NMAP

1- ESCANEO BASICO

Usaremos el comando ‘nmap’, seguido de la ip del objetivo(máquina debian).

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 08:44 EST
Nmap scan report for 192.168.1.14
Host is up (0.00084s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 5.19 seconds
```

2- ESCANEO DE PUERTOS Y SERVICIOS

Usaremos el comando ‘nmap’ añadendo el flag ‘-sV’ para detectar la versión del servicio que usa cada puerto.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 08:46 EST
Nmap scan report for 192.168.1.14
Host is up (0.00070s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
80/tcp  open   http    Apache httpd 2.4.62 ((Debian))
443/tcp closed https
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.80 seconds
```

3- ESCANEO DETALLADO Y BUSQUEDA DE VULNERABILIDADES

Usaremos el comando ‘nmap’, y añadimos el flag ‘--script=vuln’ , el cual ejecuta un script para detectar la vulnerabilidad concreta que encuentre en cada servicio.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=vuln  192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 08:47 EST
Nmap scan report for 192.168.1.14
Host is up (0.0010s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/g
ithubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A       *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2023-28531  9.8     https://vulners.com/cve/CVE-2023-28531
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/g
ithubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23       *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/g
ithubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623       *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/g
ithubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC       *EXPLOIT*
|       887EB570-27D3-11EE-ADBA-C80AA9043978    9.8     https://vulners.com/f
reebsd/887EB570-27D3-11EE-ADBA-C80AA9043978
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/g
ithubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A       *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/g
ithubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340       *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/g
ithubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587       *EXPLOIT*
|       95499236-C9FE-56A6-9D7D-E943A24B633A    8.9     https://vulners.com/g
ithubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A       *EXPLOIT*
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKE
TSTORM:179290   *EXPLOIT*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/g
ithubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134       *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/g
ithubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F       *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/g
ithubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59       *EXPLOIT*
|       F58A5CB2-2174-586F-9CA9-4C47F8F38B5E    8.1     https://vulners.com/g
ithubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F38B5E       *EXPLOIT*
|       F1A00122-3797-11EF-B611-84A93843EB75    8.1     https://vulners.com/f
reebsd/F1A00122-3797-11EF-B611-84A93843EB75
|       EFD615F0-8F17-5471-AA83-0F491FD497AF    8.1     https://vulners.com/g
ithubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF       *EXPLOIT*
|       EC20B9C2-6857-5848-848A-A9F430D13EEB    8.1     https://vulners.com/g
ithubexploit/EC20B9C2-6857-5848-848A-A9F430D13EEB       *EXPLOIT*
|       EB13CBD6-BC93-5F14-A210-AC0B5A1D8572    8.1     https://vulners.com/g
```

```
ithubexploit/39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118       *EXPLOIT*
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-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|_  /wordpress/wp-login.php: Wordpress login page.
443/tcp closed https
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.38 seconds
```

4- DOCUMENTACION Y VULNERABILIDADES

PUERTO	SERVICIO	VERSION	VULNERABILIDAD	DESCRIPCION	REFERENCIA
22/tcp	ssh	OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)	CVE-2023-38408	La función PKCS#11 en ssh-agent en OpenSSH antes de 9.3p2 tiene una ruta de búsqueda insuficientemente confiable, lo que lleva a la ejecución remota de código si un agente se reenvía a un sistema controlado por un atacante. (El código en /usr/lib no es necesariamente seguro para cargar en ssh-agent.) NOTA: este problema existe debido a una corrección incompleta de CVE-2016-10009.	CVE-2023-38408 - vulnerability database | Vulners.com
		OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)	CVE-2023-28531	ssh-add en OpenSSH antes de la versión 9.3 añade claves de tarjeta inteligente a ssh-agent sin las restricciones de destino por salto previstas. La primera versión afectada es la 8.9.	CVE-2023-28531 - vulnerability database | Vulners.com
80/tcp	http	Apache httpd 2.4.62 ((Debian))		No he encontrado ninguna vulnerabilidad.	

5- CONCLUSION

El escaneo de la máquina Debian ha identificado dos puertos abiertos: el puerto 22, que está ejecutando OpenSSH 9.2p1, y el puerto 80, que ejecuta Apache HTTPD 2.4.62. Aunque no se encontraron vulnerabilidades críticas en el servicio HTTP, se detectaron muchas vulnerabilidad en el servicio SSH ,OpenSSH (ver captura) que requieren atención.

Además, se observó la presencia de un sitio Wordpress, lo que podría ser un posible vector de ataque si no se gestiona adecuadamente. Es fundamental aplicar las actualizaciones de seguridad necesarias y mantener un monitoreo constante de las vulnerabilidades para asegurar la protección del sistema.