HACKTHEBOX

Informe Técnico

Máquina Shocker

26 de octubre del 2021

Índice

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Shocker** de la plataforma **HackTheBox**.

Figura 1: Dirección IP de la máquina

Dirección URL

Ir a la máquina.

2. Objetivos

Conocer el estado de seguridad actual del servidor **Shocker**, enumerando posibles vectores de explotación y determinado alcance e impacto que un atacante podria ocasionar sobre el sistema en producción.

2.1. Consideraciones

Una vez finalizadas las joranadas de auditoría, se llevará a cabo una fase de saneamientos y buenas prácticas con el objetivo de securizar el servidor y evitar ser victimas de un futuro ataque en base a los vectores explotados.

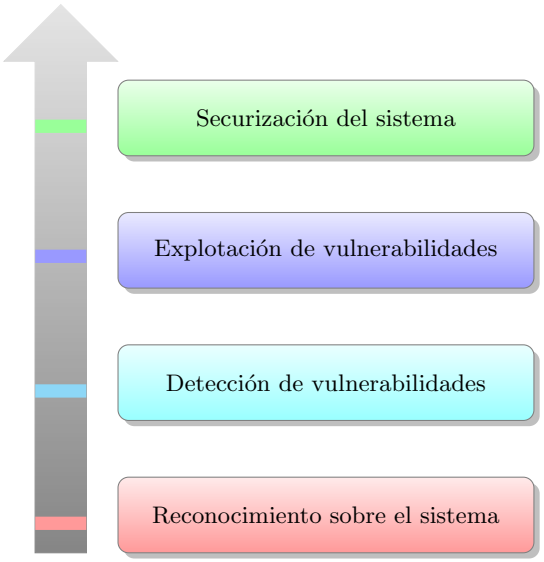

Figura 2: Flujo de trabajo

3. Analisis de vulnerabilidades

3.1. Vulnerabilidades encontradas

Se comenzó realizando un escaneo de puertos abiertos y escaneo de exhaustivo para poder ver como trabaja el sistema. Se observó el puerto 80 abierto por lo que se investigó. Indagando en la pagina y al ver que no teniamos

```
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-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 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.17 seconds
```

Figura 3: nmap

mucho se procedió a realizar fuzzing con wfuzz. Se encontró la ruta cgi-bin por lo que se decidió realizar otro

```
┌──(root㉿kali)-[/home/…/Machines/HTB/Shocker/nmap]
└─# wfuzz -c --hh=137 --hc=404 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt http://10.10.10.56/FUZZ/
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/FUZZ/
Total requests: 220560

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

000000083:   403        11 L     32 W       292 Ch      "icons"
000000035:   403        11 L     32 W       294 Ch      "cgi-bin"
^C /usr/local/lib/python3.9/dist-packages/wfuzz/wfuzz.py:79: UserWarning:Finishing pending requests...

Total time: 0
Processed Requests: 64399
Filtered Requests: 64397
Requests/sec.: 0
```

Figura 4: Primer FUZZ

fuzzing en la ruta para ver más información

```
┌──(root㉿kali)-[/home/…/Machines/HTB/Shocker/nmap]
└─# wfuzz -c --hh=137 --hc=404 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt http://10.10.10.56/cgi-bin/FUZZ
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.56/cgi-bin/FUZZ
Total requests: 220560

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

000000001:   403        11 L     32 W       294 Ch      "# directory-list-2.3-medium.txt"
000000003:   403        11 L     32 W       294 Ch      "# Copyright 2007 James Fisher"
000000004:   403        11 L     32 W       294 Ch      "#"
000000002:   403        11 L     32 W       294 Ch      "#"
000000005:   403        11 L     32 W       294 Ch      "# This work is licensed under the Creative Commons"
000000008:   403        11 L     32 W       294 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000006:   403        11 L     32 W       294 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000009:   403        11 L     32 W       294 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000010:   403        11 L     32 W       294 Ch      "#"
000000011:   403        11 L     32 W       294 Ch      "# Priority ordered case sensative list, where entries were found"
000000012:   403        11 L     32 W       294 Ch      "# on atleast 2 different hosts"
000000013:   403        11 L     32 W       294 Ch      "#"
000000014:   403        11 L     32 W       294 Ch      "http://10.10.10.56/cgi-bin/"
000000007:   403        11 L     32 W       294 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
 /usr/local/lib/python3.9/dist-packages/wfuzz/wfuzz.py:79: UserWarning:Finishing pending requests...

Total time: 137.3586
```

Figura 5: FUZZ 3

Se encontró la ruta user.sh y se decidió aplicar un ataque Shellshock y eso nos dió la reverse shell.

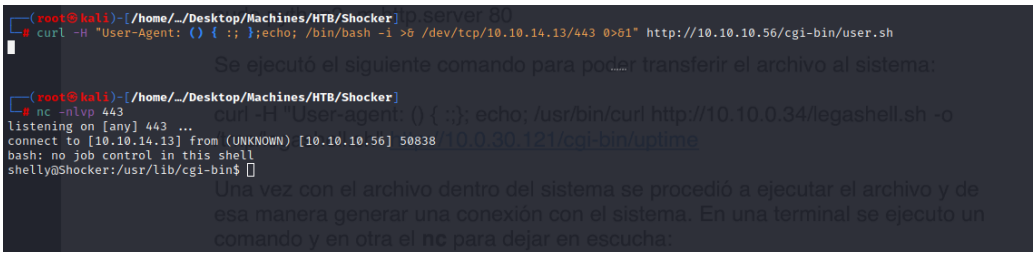

Figura 6: ReverseShell

Una vez accediendo a nivel de usuario se procedió a escalar los privilegios, enlistando las posibles acciones de sudo que tenia el usuario, nos encontramos una ruta putencial de abuso de sudoers así que la explotamos y obtuvimos el root.

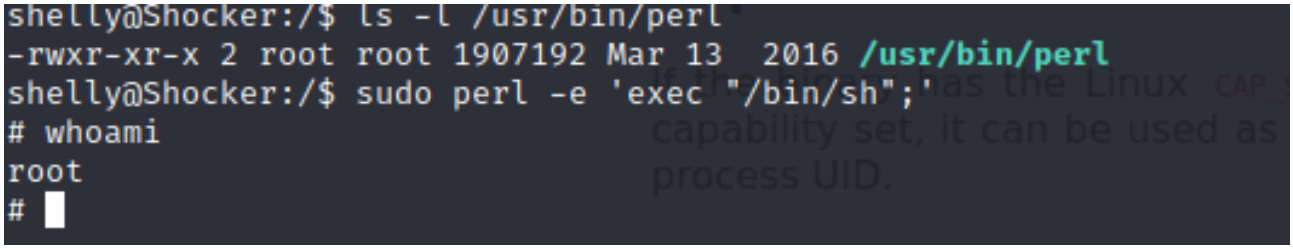

Figura 7: Obteniendo el root