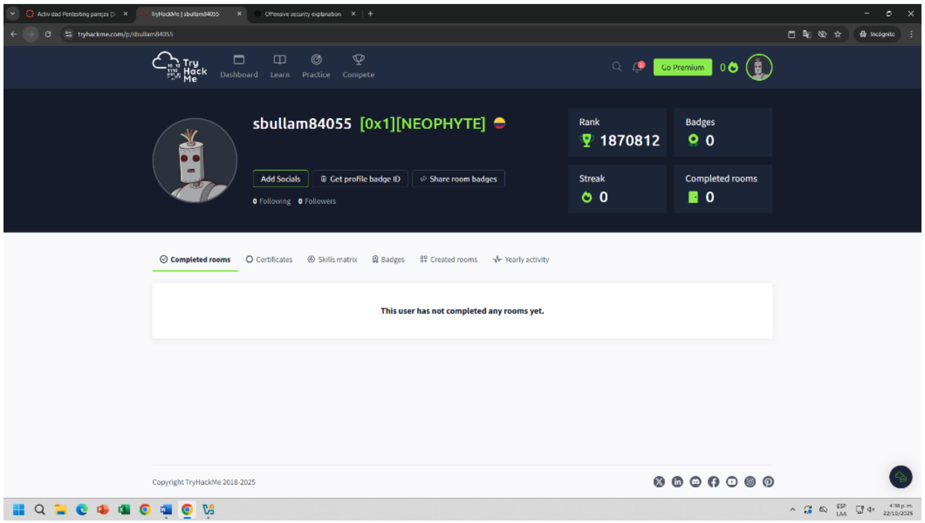
TALLER INDIVIDUAL HACKING ETICO – SEBASTIAN BULLA MATALLANA

Sesión 1 — Fase 1 (60 min)

Objetivo: Iniciar la room, recon y enumeración. Entregable parcial: escaneos y resumen.

00:00–05:00 — **Acceso y evidencia de spawn**



tryhackme.com/p/sbullam84055

sbullam84055 [0x1][NEOPHYTE]

Rank 1870812 | Badges 0 | Streak 0 | Completed rooms 0

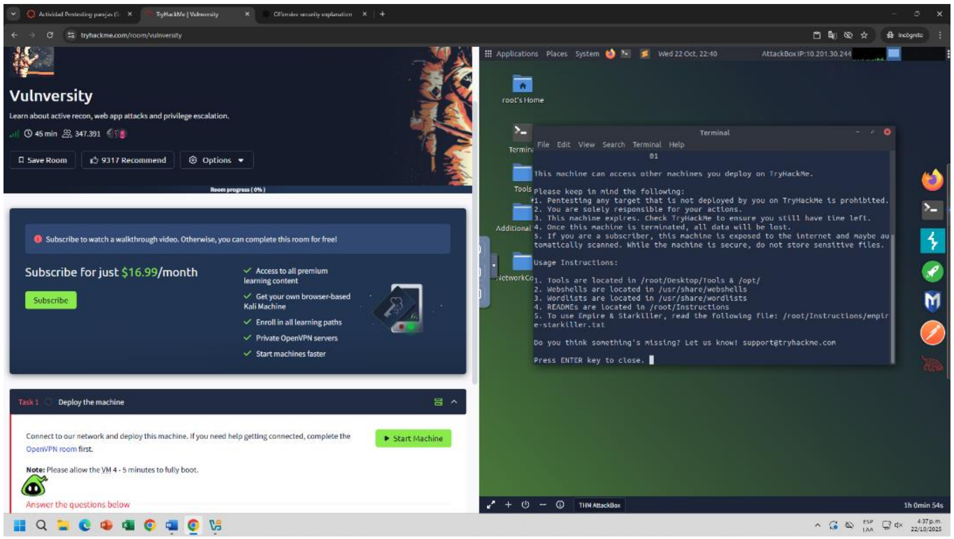
0 Following 0 Followers

This user has not completed any rooms yet.

Copyright TryHackMe 2018-2025

- Entrar a https://tryhackme.com/room/vulnversityEnlaces a un sitio externo. → pulsar **Start Machine** (Start Target).
- Capturar pantalla de la página de la room que muestre *Machine started / IP* o el estado (archivo thm_spawn.png). (TryHackMeEnlaces a un sitio externo.)

05:00–10:00 — **Preparar AttackBox / entorno**



tryhackme.com/room/vulnversity

Vulnversity

Learn about active recon, web app attacks and privilege escalation.

45 min 347.391

Room progress (0%)

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

Subscribe for just $16.99/month

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

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

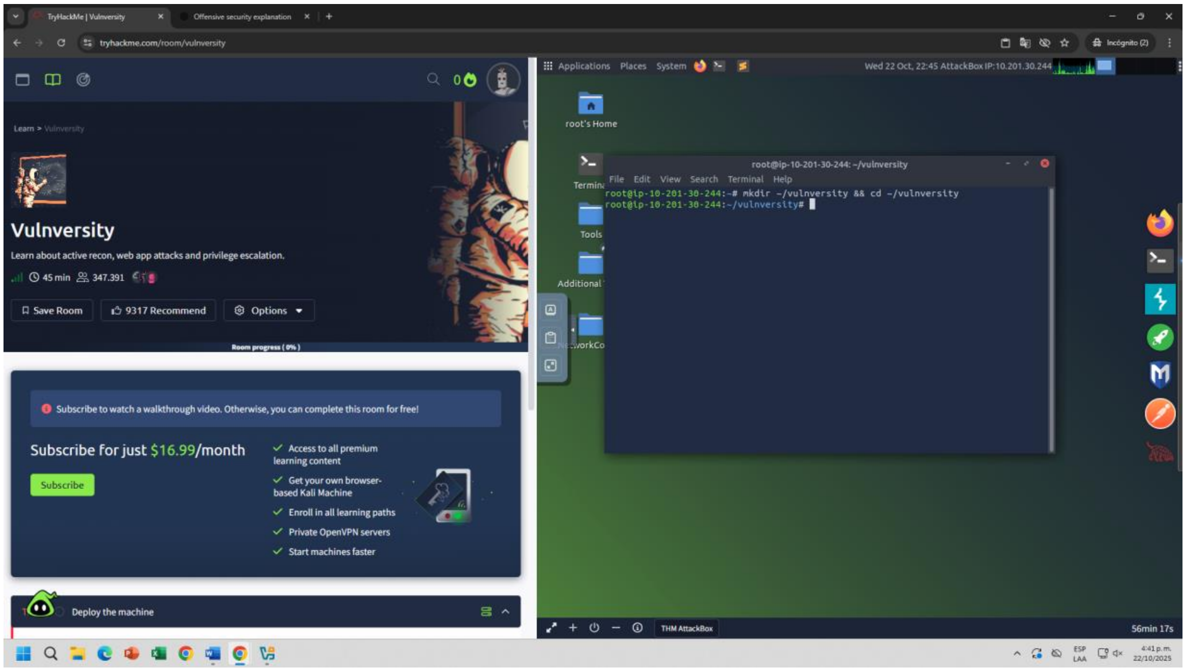
Wed 22 Oct, 22:40 AttackBox IP:10.201.30.244 [redacted]

```
                              01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.
5. If you are a subscriber, this machine is exposed to the internet and maybe au
tomatically scanned. While the machine is secure, do not store sensitive files.

Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. READMEs are located in /root/Instructions
5. To use Empire & Starkiller, read the following file: /root/Instructions/empir
e-starkiller.txt

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.
```

05:00–10:00 — **Preparar AttackBox / entorno**

- Abrir AttackBox → Terminal → crear carpeta de trabajo:

mkdir ~/vulnversity && cd ~/vulnversity



Vulnversity

Learn about active recon, web app attacks and privilege escalation.

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

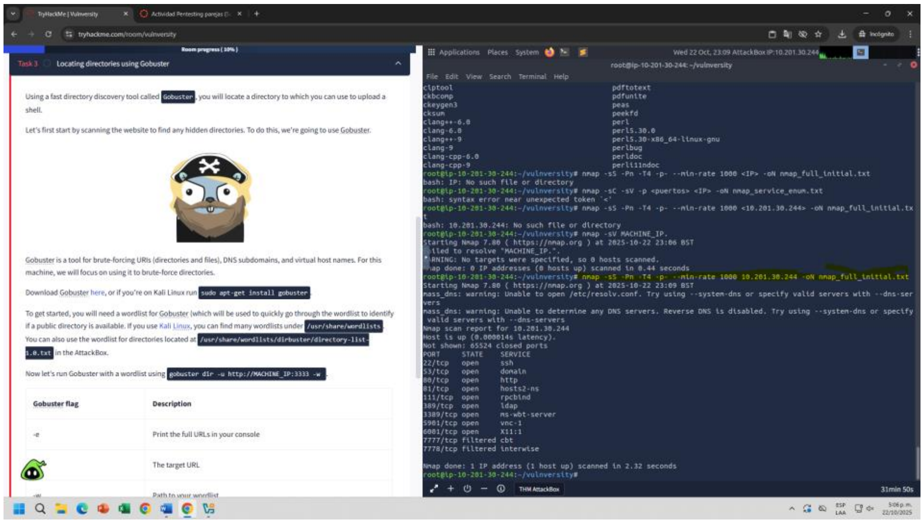
Subscribe for just $16.99/month

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

```
root@ip-10-201-30-244: ~/vulnversity
root@ip-10-201-30-244:~# mkdir ~/vulnversity && cd ~/vulnversity
root@ip-10-201-30-244:~/vulnversity#
```

10:00–30:00 — **Escaneo con nmap** (estudiante A ejecuta)

- Escaneo rápido (todos los puertos):



Task 3 Locating directories using Gobuster

Using a fast directory discovery tool called `Gobuster`, you will locate a directory to which you can use to upload a shell.

Let's first start by scanning the website to find any hidden directories. To do this, we're going to use Gobuster.

Gobuster is a tool for brute-forcing URIs (directories and files), DNS subdomains, and virtual host names. For this machine, we will focus on using it to brute-force directories.

Download Gobuster here, or if you're on Kali Linux run `sudo apt-get install gobuster`.

To get started, you will need a wordlist for Gobuster (which will be used to quickly go through the wordlist to identify if a public directory is available. If you use Kali Linux, you can find many wordlists under `/usr/share/wordlists`. You can also use the wordlist for directories located at `/usr/share/wordlists/dirbuster/directory-list-1.0.txt` in the AttackBox.

Now let's run Gobuster with a wordlist using `gobuster dir -u http://MACHINE_IP:3333 -w`.

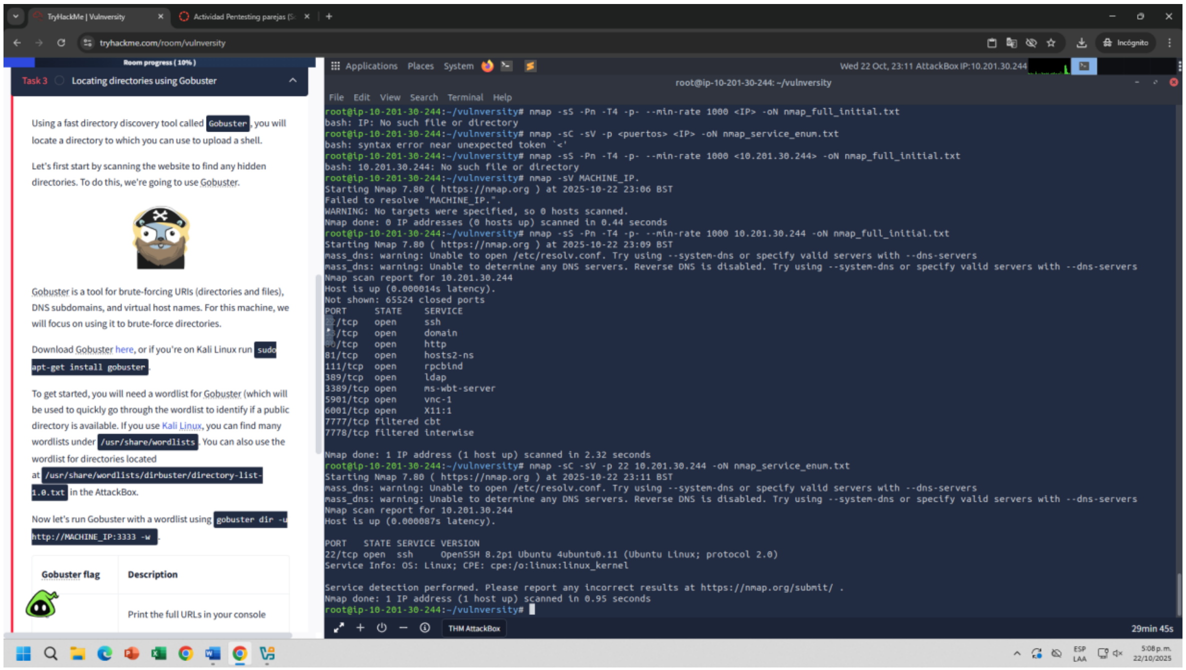
Gobuster flag	Description
-e	Print the full URLs in your console
	The target URL
-w	Path to your wordlist

```
root@ip-10-201-30-244: ~/vulnversity
cliptool                                      pdftotext
ckbcomp                                       pdfunite
ckeygen3                                      peas
cksum                                         peekfd
clang++-6.0                                   perl
clang-6.0                                     perl5.30.0
clang++-9                                     perl5.30-x86_64-linux-gnu
clang-9                                       perlbug
clang-cpp-6.0                                 perldoc
clang-cpp-9                                   perlillndoc
root@ip-10-201-30-244:~/vulnversity# nmap -sS -Pn -T4 -p- --min-rate 1000 <IP> -oN nmap_full_initial.txt
bash: IP: No such file or directory
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p <puertos> <IP> -oN nmap_service_enum.txt
bash: syntax error near unexpected token `<'
root@ip-10-201-30-244:~/vulnversity# nmap -sS -Pn -T4 -p- --min-rate 1000 <10.201.30.244> -oN nmap_full_initial.tx
t
bash: 10.201.30.244: No such file or directory
root@ip-10-201-30-244:~/vulnversity# nmap -sV MACHINE_IP.
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:06 BST
ailed to resolve "MACHINE_IP.".
ARNING: No targets were specified, so 0 hosts scanned.
map done: 0 IP addresses (0 hosts up) scanned in 0.44 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sS -Pn -T4 -p- --min-rate 1000 10.201.30.244 -oN nmap_full_initial.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:09 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-ser
vers
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 10.201.30.244
Host is up (0.000014s latency).
Not shown: 65524 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
53/tcp   open     domain
80/tcp   open     http
81/tcp   open     hosts2-ns
111/tcp  open     rpcbind
389/tcp  open     ldap
3389/tcp open     ms-wbt-server
5901/tcp open     vnc-1
6001/tcp open     X11:1
7777/tcp filtered cbt
7778/tcp filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
root@ip-10-201-30-244:~/vulnversity#
```

- Escaneo detallado de puertos abiertos:

nmap -sC -sV -p <puertos> <IP> -oN nmap_service_enum.txt

Puerto 22 abierto / SSH



TryHackMe | Vulnversity
Actividad Pentesting parejas (S
tryhackme.com/room/vulnversity
Incógnito
Room progress (10%)
Applications Places System
Wed 22 Oct, 23:11 AttackBox IP:10.201.30.244
root@ip-10-201-30-244: ~/vulnversity
File Edit View Search Terminal Help
THM AttackBox
29min 45s
ESP LAA
5:08 p.m. 22/10/2025

Task 3 Locating directories using Gobuster

Using a fast directory discovery tool called `Gobuster`, you will locate a directory to which you can use to upload a shell.

Let's first start by scanning the website to find any hidden directories. To do this, we're going to use Gobuster.

Gobuster is a tool for brute-forcing URIs (directories and files), DNS subdomains, and virtual host names. For this machine, we will focus on using it to brute-force directories.

Download Gobuster here, or if you're on Kali Linux run `sudo apt-get install gobuster`.

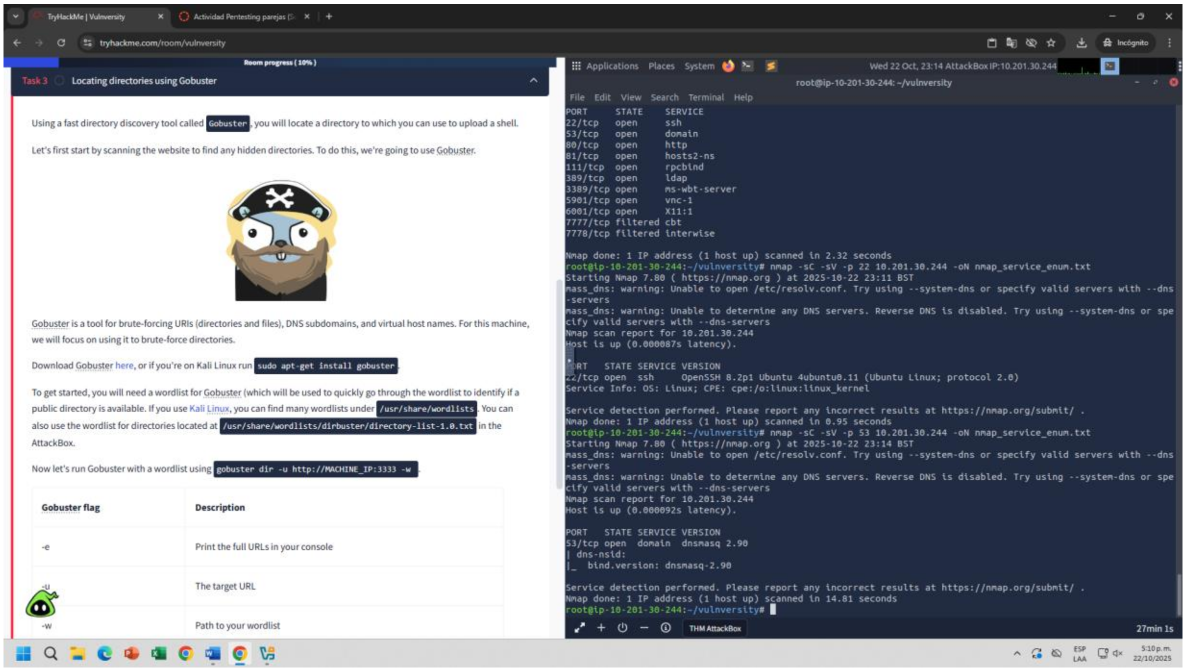
To get started, you will need a wordlist for Gobuster (which will be used to quickly go through the wordlist to identify if a public directory is available. If you use Kali Linux, you can find many wordlists under `/usr/share/wordlists`. You can also use the wordlist for directories located at `/usr/share/wordlists/dirbuster/directory-list-1.0.txt` in the AttackBox.

Now let's run Gobuster with a wordlist using `gobuster dir -u http://MACHINE_IP:3333 -w` .

Gobuster flag	Description
	Print the full URLs in your console

```
root@ip-10-201-30-244:~/vulnversity# nmap -sS -Pn -T4 -p- --min-rate 1000 <IP> -oN nmap_full_initial.txt
bash: IP: No such file or directory
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p <puertos> <IP> -oN nmap_service_enum.txt
bash: syntax error near unexpected token `<'
root@ip-10-201-30-244:~/vulnversity# nmap -sS -Pn -T4 -p- --min-rate 1000 <10.201.30.244> -oN nmap_full_initial.txt
bash: 10.201.30.244: No such file or directory
root@ip-10-201-30-244:~/vulnversity# nmap -sV MACHINE_IP.
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:06 BST
Failed to resolve "MACHINE_IP.".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.44 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sS -Pn -T4 -p- --min-rate 1000 10.201.30.244 -oN nmap_full_initial.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:09 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 10.201.30.244
Host is up (0.000014s latency).
Not shown: 65524 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
53/tcp   open     domain
80/tcp   open     http
81/tcp   open     hosts2-ns
111/tcp  open     rpcbind
389/tcp  open     ldap
3389/tcp open     ms-wbt-server
5901/tcp open     vnc-1
6001/tcp open     X11:1
7777/tcp filtered cbt
7778/tcp filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 22 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:11 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 10.201.30.244
Host is up (0.000087s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
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 0.95 seconds
root@ip-10-201-30-244:~/vulnversity#
```

Puerto 53 abierto



TryHackMe | Vulnversity
Actividad Pentesting parejas (S
tryhackme.com/room/vulnversity
Incógnito
Room progress (10%)
Applications Places System
Wed 22 Oct, 23:14 AttackBox IP:10.201.30.244
root@ip-10-201-30-244: ~/vulnversity
File Edit View Search Terminal Help
THM AttackBox
27min 1s
ESP LAA
5:10 p.m. 22/10/2025

Task 3 Locating directories using Gobuster

Using a fast directory discovery tool called `Gobuster`, you will locate a directory to which you can use to upload a shell.

Let's first start by scanning the website to find any hidden directories. To do this, we're going to use Gobuster.

Gobuster is a tool for brute-forcing URIs (directories and files), DNS subdomains, and virtual host names. For this machine, we will focus on using it to brute-force directories.

Download Gobuster here, or if you're on Kali Linux run `sudo apt-get install gobuster`.

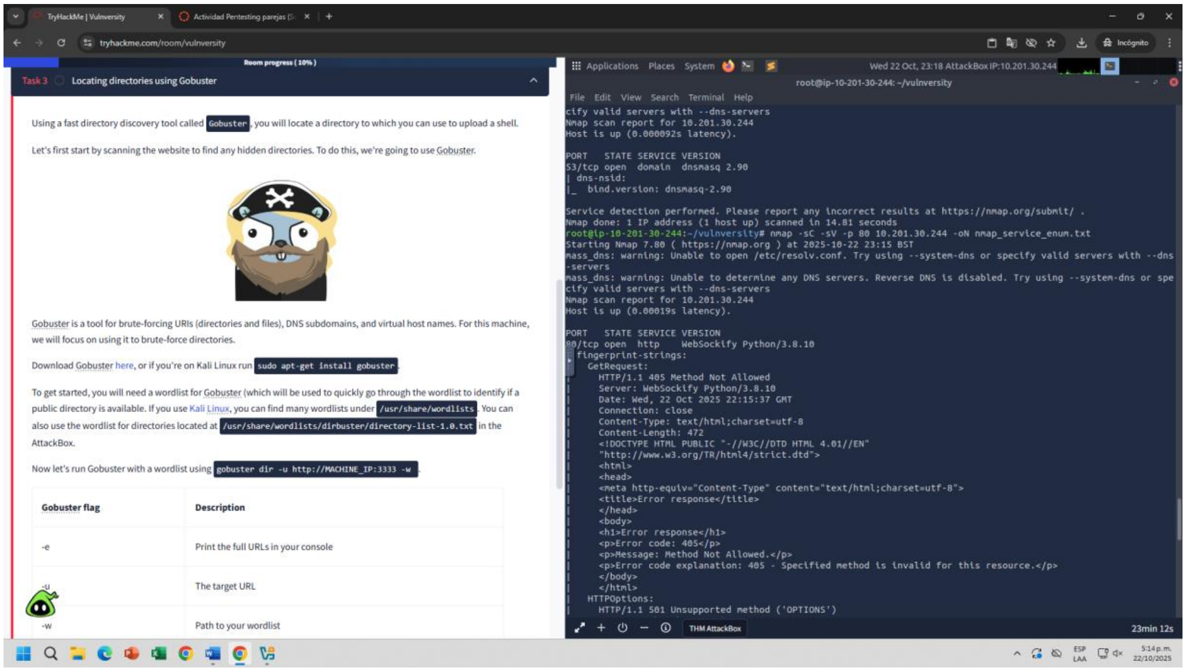
To get started, you will need a wordlist for Gobuster (which will be used to quickly go through the wordlist to identify if a public directory is available. If you use Kali Linux, you can find many wordlists under `/usr/share/wordlists`. You can also use the wordlist for directories located at `/usr/share/wordlists/dirbuster/directory-list-1.0.txt` in the AttackBox.

Now let's run Gobuster with a wordlist using `gobuster dir -u http://MACHINE_IP:3333 -w` .

Gobuster flag	Description
-e	Print the full URLs in your console
-u	The target URL
-w	Path to your wordlist

```
PORT     STATE    SERVICE
22/tcp   open     ssh
53/tcp   open     domain
80/tcp   open     http
81/tcp   open     hosts2-ns
111/tcp  open     rpcbind
389/tcp  open     ldap
3389/tcp open     ms-wbt-server
5901/tcp open     vnc-1
6001/tcp open     X11:1
7777/tcp filtered cbt
7778/tcp filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 22 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:11 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000087s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
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 0.95 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 53 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:14 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000092s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.90
| dns-nsid:
|_  bind.version: dnsmasq-2.90

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds
root@ip-10-201-30-244:~/vulnversity#
```

Puerto 80 abierto / HTTPS


TryHackMe | Vulnversity
Actividad Pentesting parejas (S
tryhackme.com/room/vulnversity
Incógnito
Room progress (10%)
Task 3
Locating directories using Gobuster
Applications
Places
System
Wed 22 Oct, 23:18 AttackBox IP:10.201.30.244
root@ip-10-201-30-244: ~/vulnversity
File
Edit
View
Search
Terminal
Help
THM AttackBox
23min 12s
ESP
LAA
5:14 p.m.
22/10/2025

Using a fast directory discovery tool called `Gobuster`, you will locate a directory to which you can use to upload a shell.

Let's first start by scanning the website to find any hidden directories. To do this, we're going to use Gobuster.

Gobuster is a tool for brute-forcing URIs (directories and files), DNS subdomains, and virtual host names. For this machine, we will focus on using it to brute-force directories.

Download Gobuster here, or if you're on Kali Linux run `sudo apt-get install gobuster`.

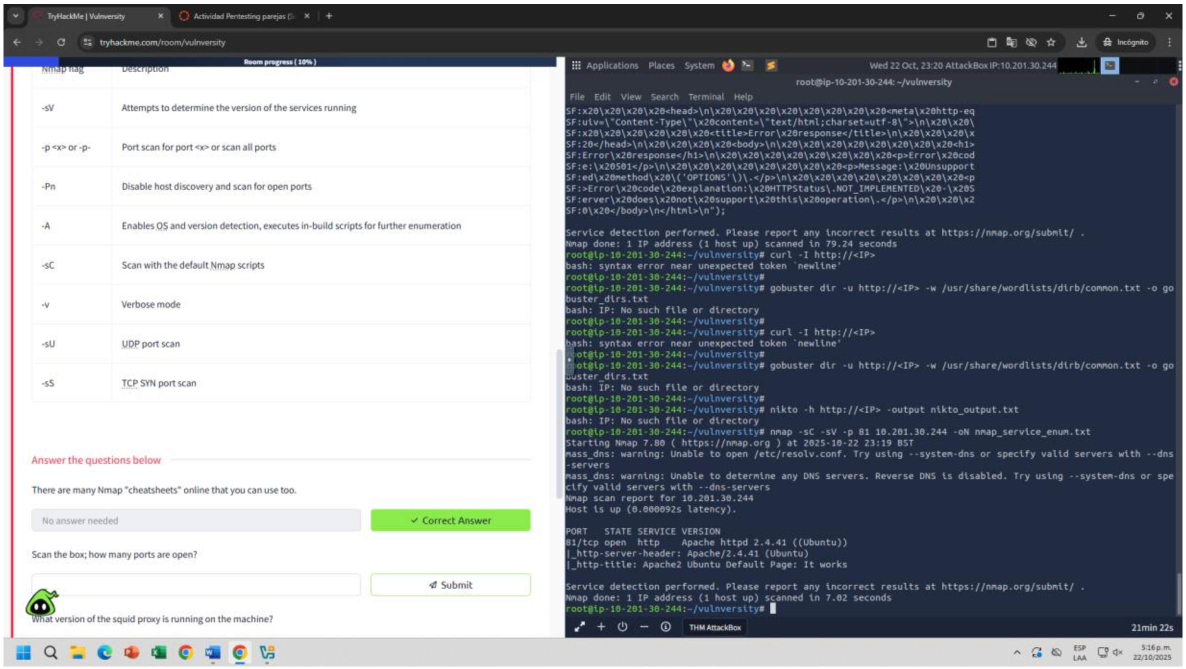
To get started, you will need a wordlist for Gobuster (which will be used to quickly go through the wordlist to identify if a public directory is available. If you use Kali Linux, you can find many wordlists under `/usr/share/wordlists`. You can also use the wordlist for directories located at `/usr/share/wordlists/dirbuster/directory-list-1.0.txt` in the AttackBox.

Now let's run Gobuster with a wordlist using `gobuster dir -u http://MACHINE_IP:3333 -w`.

Gobuster flag	Description
-e	Print the full URLs in your console
-u	The target URL
-w	Path to your wordlist

```
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000092s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.90
| dns-nsid:
|_  bind.version: dnsmasq-2.90

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 80 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:15 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.00019s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    WebSockify Python/3.8.10
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 405 Method Not Allowed
|     Server: WebSockify Python/3.8.10
|     Date: Wed, 22 Oct 2025 22:15:37 GMT
|     Connection: close
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 472
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 405</p>
|     <p>Message: Method Not Allowed.</p>
|     <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 501 Unsupported method ('OPTIONS')
```

Puerto 81 abierto / HTTPS



Nmap flag	Description
-sV	Attempts to determine the version of the services running
-p <x> or -p-	Port scan for port <x> or scan all ports
-Pn	Disable host discovery and scan for open ports
-A	Enables OS and version detection, executes in-build scripts for further enumeration
-sC	Scan with the default Nmap scripts
-v	Verbose mode
-sU	UDP port scan
-sS	TCP SYN port scan

Answer the questions below

There are many Nmap "cheatsheets" online that you can use too.

No answer needed ✓ Correct Answer

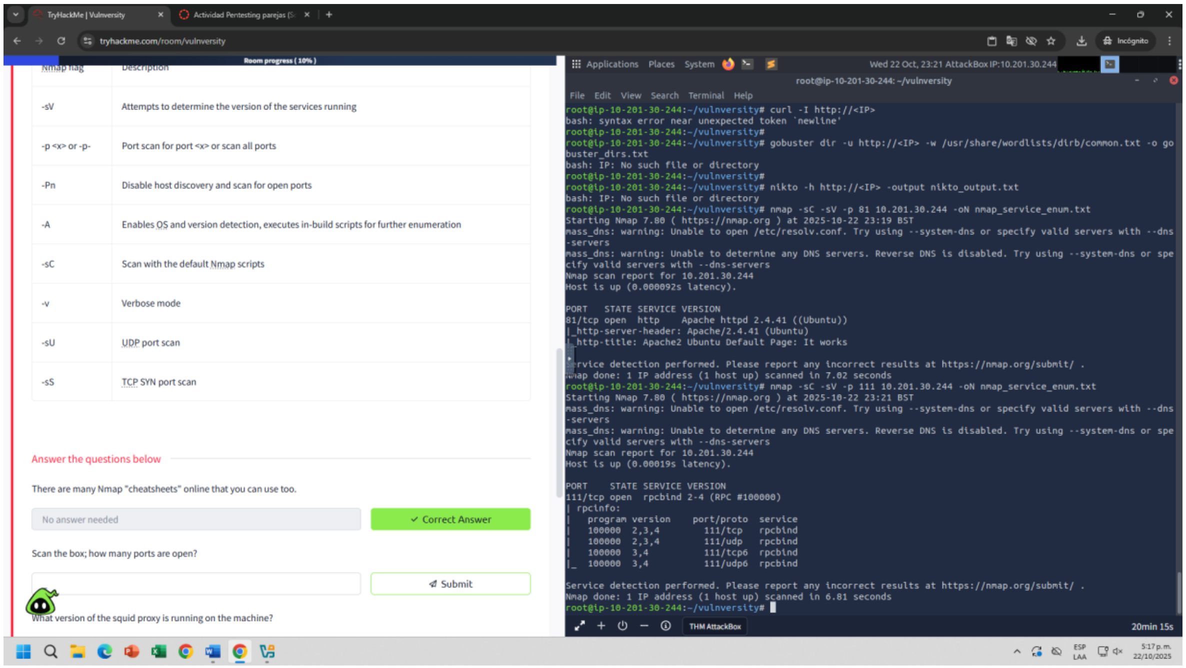
Scan the box; how many ports are open?

Submit

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

```
SF:x20\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-eq
SF:uiv=\"Content-Type\"\x20content=\"text/html;charset=utf-8\">\n\x20\x20\
SF:x20\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x
SF:20</head>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>
SF:Error\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20cod
SF:e:\x20501</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Unsupport
SF:ed\x20method\x20\('OPTIONS'\)\.</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p
SF:>Error\x20code\x20explanation:\x20HTTPStatus\.NOT_IMPLEMENTED\x20-\x20S
SF:erver\x20does\x20not\x20support\x20this\x20operation\.</p>\n\x20\x20\x2
SF:0\x20</body>\n</html>\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.24 seconds
root@ip-10-201-30-244:~/vulnversity# curl -I http://<IP>
bash: syntax error near unexpected token `newline'
root@ip-10-201-30-244:~/vulnversity#
root@ip-10-201-30-244:~/vulnversity# gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt -o go
buster_dirs.txt
bash: IP: No such file or directory
root@ip-10-201-30-244:~/vulnversity#
root@ip-10-201-30-244:~/vulnversity# curl -I http://<IP>
bash: syntax error near unexpected token `newline'
root@ip-10-201-30-244:~/vulnversity#
root@ip-10-201-30-244:~/vulnversity# gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt -o go
buster_dirs.txt
bash: IP: No such file or directory
root@ip-10-201-30-244:~/vulnversity#
root@ip-10-201-30-244:~/vulnversity# nikto -h http://<IP> -output nikto_output.txt
bash: IP: No such file or directory
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 81 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:19 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000092s latency).

PORT   STATE SERVICE VERSION
81/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds
root@ip-10-201-30-244:~/vulnversity#
```

Puerto 111 abierto



Nmap flag	Description
-sV	Attempts to determine the version of the services running
-p <x> or -p-	Port scan for port <x> or scan all ports
-Pn	Disable host discovery and scan for open ports
-A	Enables OS and version detection, executes in-build scripts for further enumeration
-sC	Scan with the default Nmap scripts
-v	Verbose mode
-sU	UDP port scan
-sS	TCP SYN port scan

Answer the questions below

There are many Nmap "cheatsheets" online that you can use too.

No answer needed ✓ Correct Answer

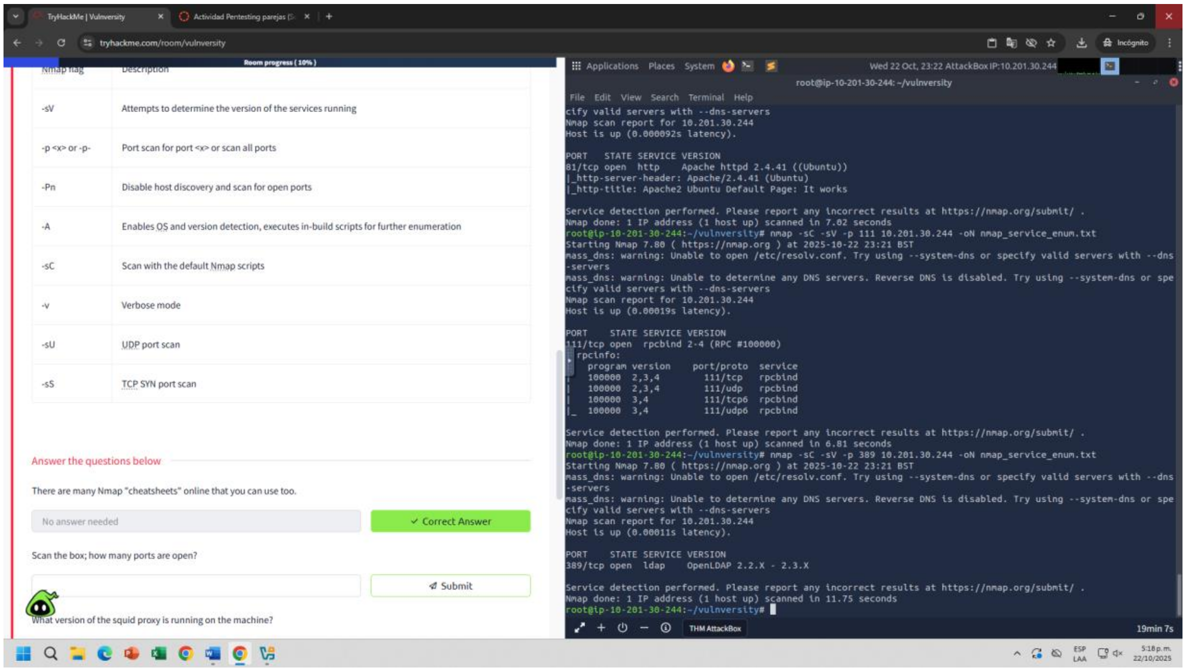
Scan the box; how many ports are open?

Submit

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

```
root@ip-10-201-30-244:~/vulnversity# curl -I http://<IP>
bash: syntax error near unexpected token `newline'
root@ip-10-201-30-244:~/vulnversity#
root@ip-10-201-30-244:~/vulnversity# gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt -o go
buster_dirs.txt
bash: IP: No such file or directory
root@ip-10-201-30-244:~/vulnversity#
root@ip-10-201-30-244:~/vulnversity# nikto -h http://<IP> -output nikto_output.txt
bash: IP: No such file or directory
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 81 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:19 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000092s latency).

PORT   STATE SERVICE VERSION
81/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 111 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:21 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.00019s latency).

PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
root@ip-10-201-30-244:~/vulnversity#
```

Puerto 389 abierto



Nmap flag	Description
-sV	Attempts to determine the version of the services running
-p <x> or -p-	Port scan for port <x> or scan all ports
-Pn	Disable host discovery and scan for open ports
-A	Enables OS and version detection, executes in-build scripts for further enumeration
-sC	Scan with the default Nmap scripts
-v	Verbose mode
-sU	UDP port scan
-sS	TCP SYN port scan

Answer the questions below

There are many Nmap "cheatsheets" online that you can use too.

No answer needed ✓ Correct Answer

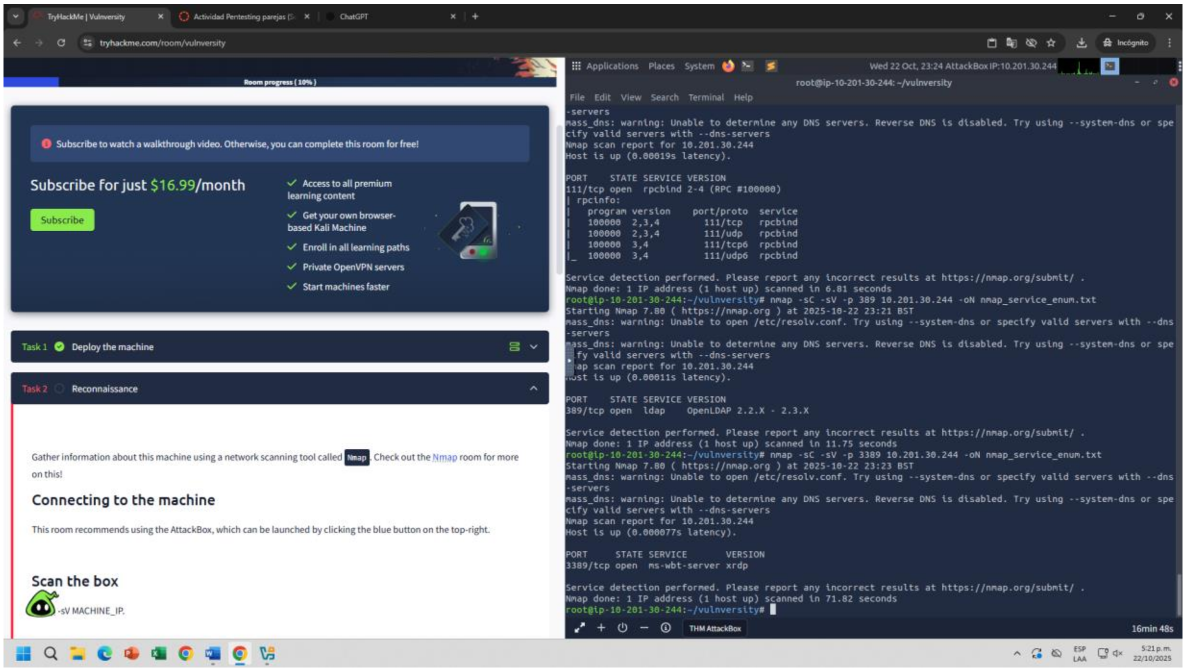
Scan the box; how many ports are open?

Submit

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

```
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000092s latency).

PORT   STATE SERVICE VERSION
81/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 111 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:21 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.00019s latency).

PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 389 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:21 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.00011s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
root@ip-10-201-30-244:~/vulnversity#
```

Puerto 3389 abierto


TryHackMe | Vulnversity
Actividad Pentesting parejas
ChatGPT
tryhackme.com/room/vulnversity
Incógnito
Room progress (10%)
Applications Places System
Wed 22 Oct, 23:24 AttackBox IP:10.201.30.244
root@ip-10-201-30-244: ~/vulnversity
File Edit View Search Terminal Help
THM AttackBox
16min 48s
ESP LAA
5:21 p.m.
22/10/2025

Subscribe to watch a walkthrough video. Otherwise, you can 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

Task 1 Deploy the machine

Task 2 Reconnaissance

Gather information about this machine using a network scanning tool called Nmap. Check out the Nmap room for more on this!

Connecting to the machine

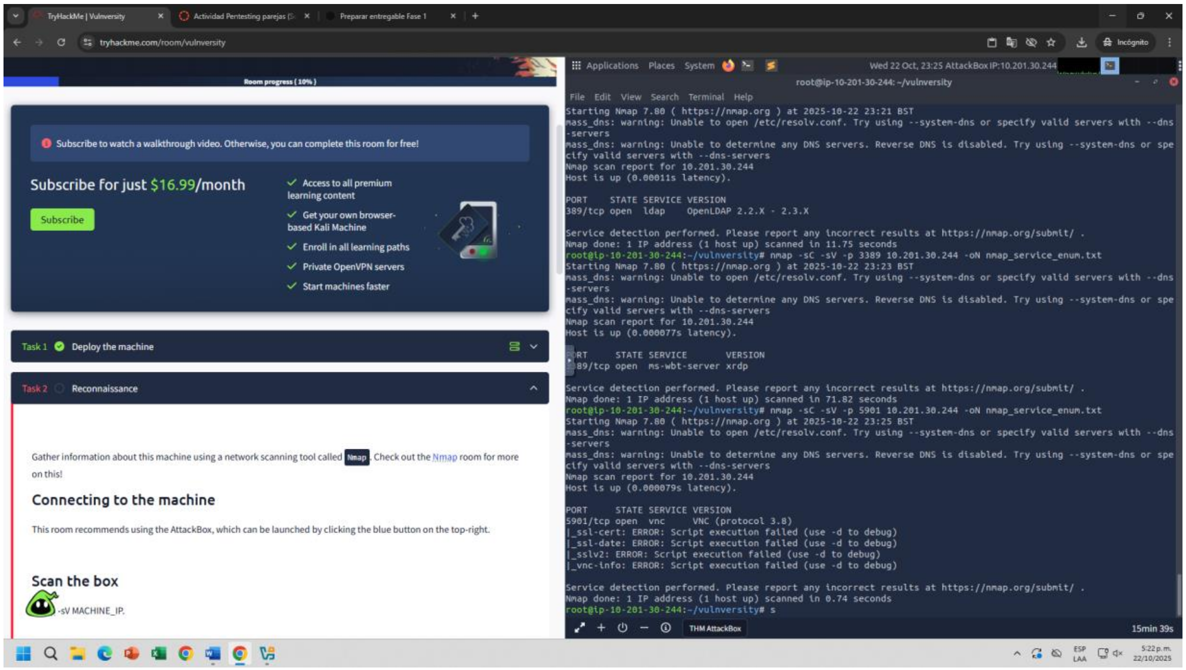
This room recommends using the AttackBox, which can be launched by clicking the blue button on the top-right.

Scan the box

-sV MACHINE_IP.

```
-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.00019s latency).

PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 389 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:21 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 spe
 fy valid servers with --dns-servers
 ap scan report for 10.201.30.244
 ost is up (0.00011s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 3389 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:23 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000077s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server xrdp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.82 seconds
root@ip-10-201-30-244:~/vulnversity# 
```

Puerto 5901 abierto


TryHackMe | Vulnversity
Actividad Pentesting parejas
Preparar entregable Fase 1
tryhackme.com/room/vulnversity
Incógnito
Room progress (10%)
Applications Places System
Wed 22 Oct, 23:25 AttackBox IP:10.201.30.244
root@ip-10-201-30-244: ~/vulnversity
File Edit View Search Terminal Help
THM AttackBox
15min 39s
ESP LAA
5:22 p.m.
22/10/2025

Subscribe to watch a walkthrough video. Otherwise, you can 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

Task 1 Deploy the machine

Task 2 Reconnaissance

Gather information about this machine using a network scanning tool called Nmap. Check out the Nmap room for more on this!

Connecting to the machine

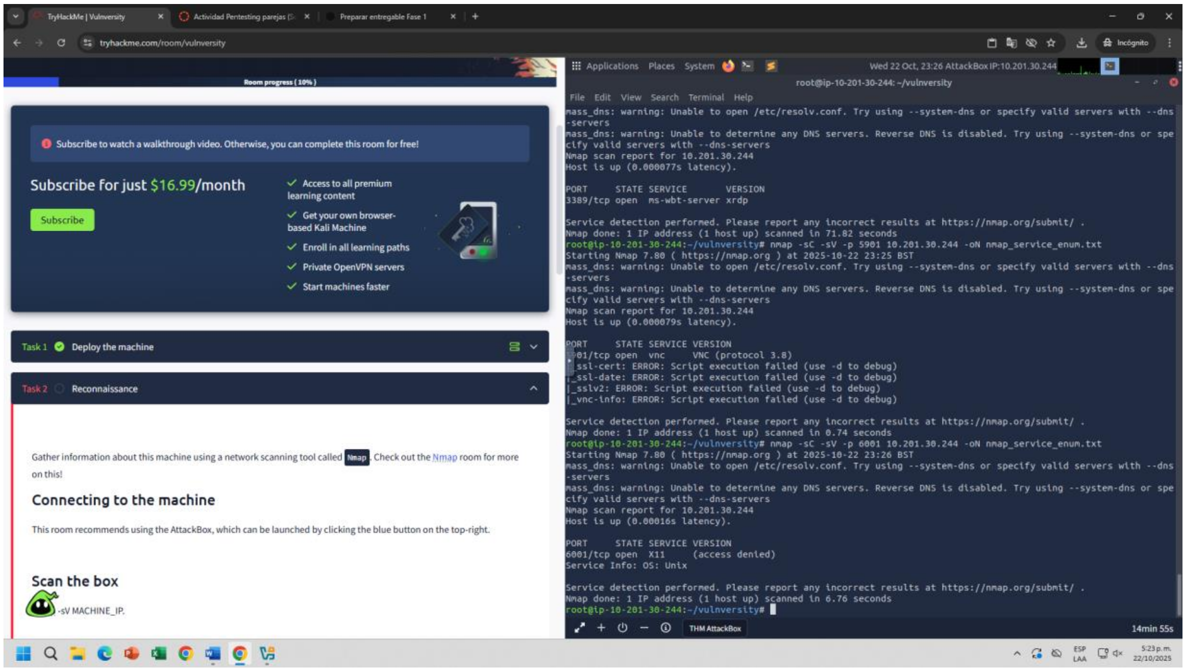
This room recommends using the AttackBox, which can be launched by clicking the blue button on the top-right.

Scan the box

-sV MACHINE_IP.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:21 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.00011s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 3389 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:23 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000077s latency).

 RT      STATE SERVICE       VERSION
 89/tcp open  ms-wbt-server xrdp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.82 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 5901 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:25 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000079s latency).

PORT     STATE SERVICE VERSION
5901/tcp open  vnc     VNC (protocol 3.8)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_vnc-info: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
root@ip-10-201-30-244:~/vulnversity# s
```

Puerto 6001 abierto



TryHackMe | Vulnversity
Actividad Pentesting parejas
Preparar entregable Fase 1
tryhackme.com/room/vulnversity
Incógnito
Room progress (10%)
Subscribe to watch a walkthrough video. Otherwise, you can 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
Task 1 Deploy the machine
Task 2 Reconnaissance
Applications Places System
Wed 22 Oct, 23:26 AttackBox IP:10.201.30.244
root@ip-10-201-30-244: ~/vulnversity
File Edit View Search Terminal Help
THM AttackBox
14min 55s
ESP LAA
5:23 p.m. 22/10/2025

Gather information about this machine using a network scanning tool called Nmap. Check out the Nmap room for more on this!

Connecting to the machine

This room recommends using the AttackBox, which can be launched by clicking the blue button on the top-right.

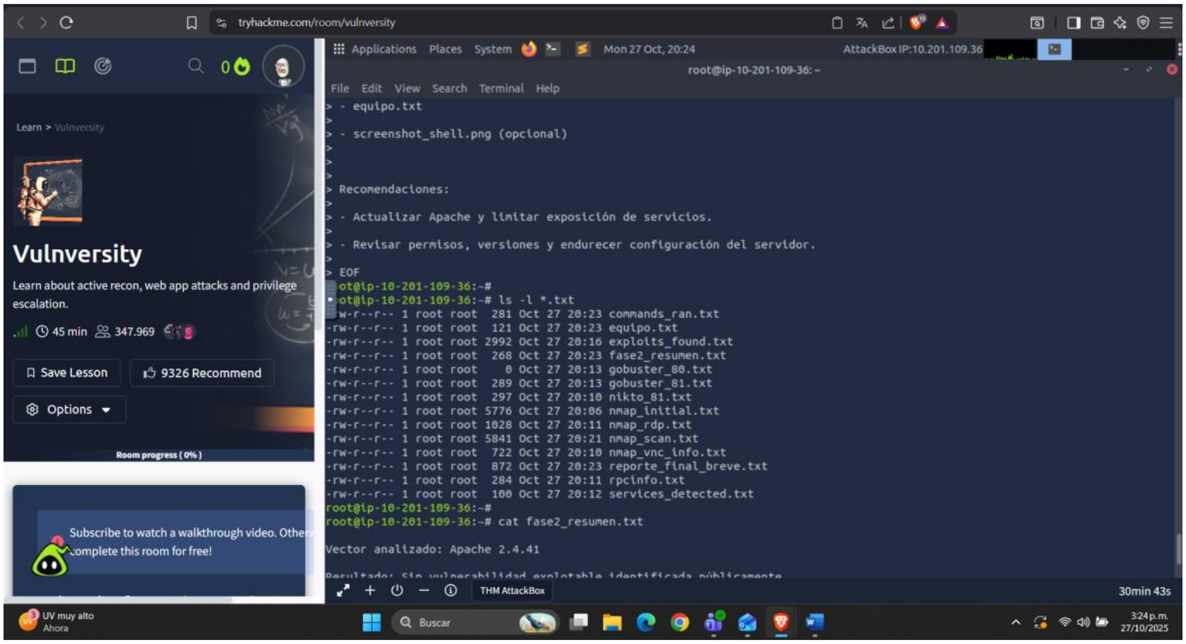
Scan the box

-sV MACHINE_IP.

```
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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000077s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server xrdp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.82 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 5901 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:25 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.000079s latency).

PORT     STATE SERVICE VERSION
 01/tcp open  vnc     VNC (protocol 3.8)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_vnc-info: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
root@ip-10-201-30-244:~/vulnversity# nmap -sC -sV -p 6001 10.201.30.244 -oN nmap_service_enum.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 23:26 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 spe
cify valid servers with --dns-servers
Nmap scan report for 10.201.30.244
Host is up (0.00016s latency).

PORT     STATE SERVICE VERSION
6001/tcp open  X11     (access denied)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
root@ip-10-201-30-244:~/vulnversity#
```

SESIÓN 2

Entregables Fase 2 (subir):



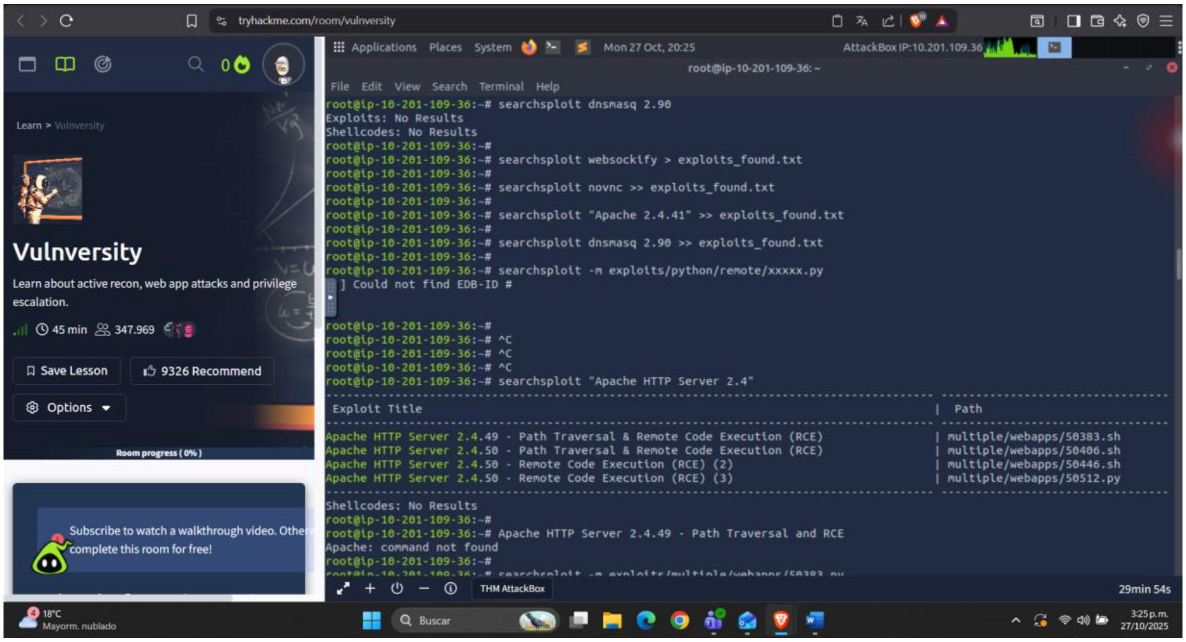
Vulnversity

Learn about active recon, web app attacks and privilege escalation.

45 min 347.969

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

```
> - equipo.txt
>
> - screenshot_shell.png (opcional)
>
>
>
> Recomendaciones:
>
> - Actualizar Apache y limitar exposición de servicios.
>
> - Revisar permisos, versiones y endurecer configuración del servidor.
>
> EOF
ot@ip-10-201-109-36:~#
ot@ip-10-201-109-36:~# ls -l *.txt
w-r--r-- 1 root root  281 Oct 27 20:23 commands_ran.txt
-rw-r--r-- 1 root root  121 Oct 27 20:23 equipo.txt
-rw-r--r-- 1 root root 2992 Oct 27 20:16 exploits_found.txt
-rw-r--r-- 1 root root  268 Oct 27 20:23 fase2_resumen.txt
-rw-r--r-- 1 root root    0 Oct 27 20:13 gobuster_80.txt
-rw-r--r-- 1 root root  289 Oct 27 20:13 gobuster_81.txt
-rw-r--r-- 1 root root  297 Oct 27 20:10 nikto_81.txt
-rw-r--r-- 1 root root 5776 Oct 27 20:06 nmap_initial.txt
-rw-r--r-- 1 root root 1028 Oct 27 20:11 nmap_rdp.txt
-rw-r--r-- 1 root root 5841 Oct 27 20:21 nmap_scan.txt
-rw-r--r-- 1 root root  722 Oct 27 20:10 nmap_vnc_info.txt
-rw-r--r-- 1 root root  872 Oct 27 20:23 reporte_final_breve.txt
-rw-r--r-- 1 root root  284 Oct 27 20:11 rpcinfo.txt
-rw-r--r-- 1 root root  100 Oct 27 20:12 services_detected.txt
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# cat fase2_resumen.txt

Vector analizado: Apache 2.4.41

Resultado: Sin vulnerabilidad explotable identificada públicamente
```



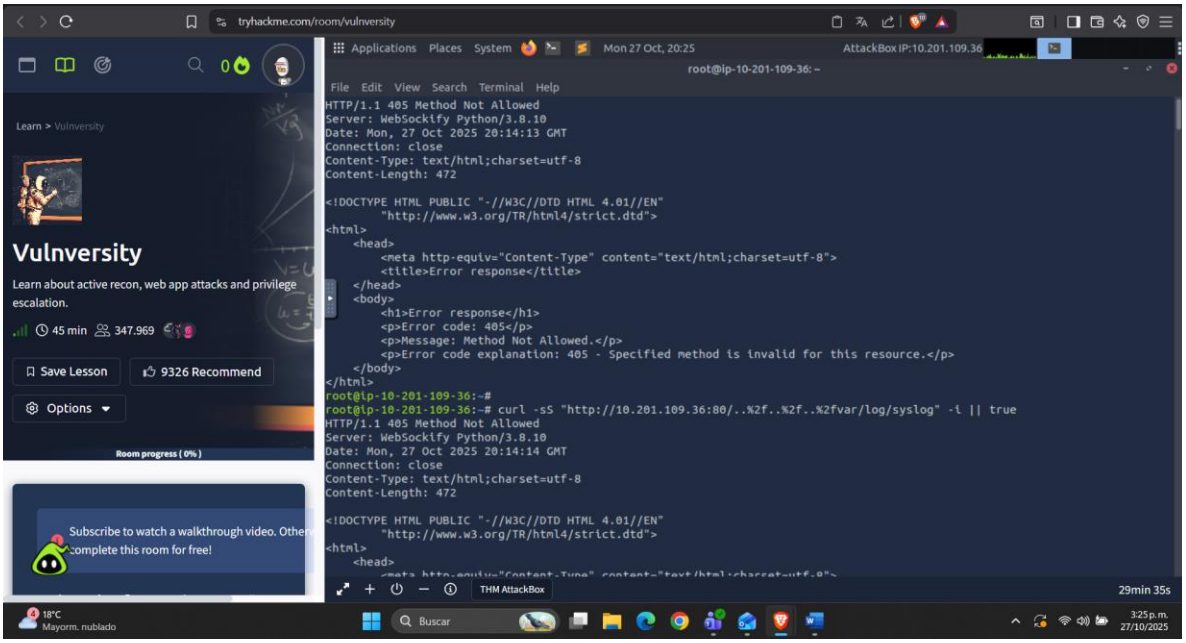
Vulnversity

Learn about active recon, web app attacks and privilege escalation.

45 min 347.969

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

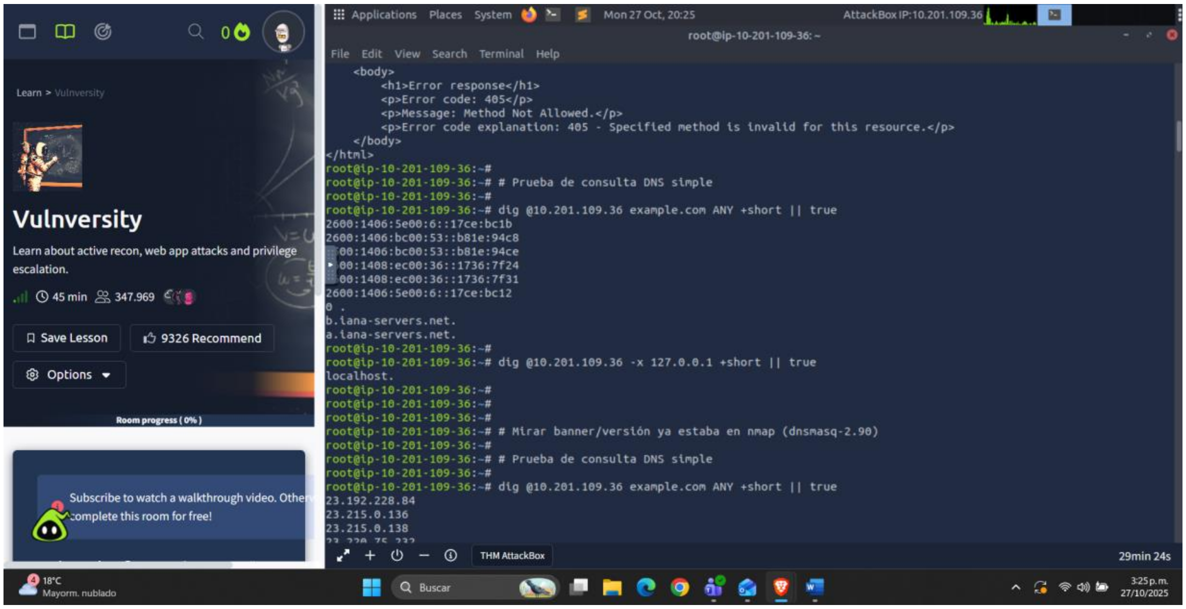
```
root@ip-10-201-109-36:~# searchsploit dnsmasq 2.90
Exploits: No Results
Shellcodes: No Results
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# searchsploit websockify > exploits_found.txt
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# searchsploit novnc >> exploits_found.txt
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# searchsploit "Apache 2.4.41" >> exploits_found.txt
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# searchsploit dnsmasq 2.90 >> exploits_found.txt
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# searchsploit -m exploits/python/remote/xxxxx.py
 ] Could not find EDB-ID #


root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# ^C
root@ip-10-201-109-36:~# ^C
root@ip-10-201-109-36:~# ^C
root@ip-10-201-109-36:~# searchsploit "Apache HTTP Server 2.4"
--------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                         |  Path
--------------------------------------------------------------------------------------- ---------------------------------
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)               | multiple/webapps/50383.sh
Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)               | multiple/webapps/50406.sh
Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)                            | multiple/webapps/50446.sh
Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (3)                            | multiple/webapps/50512.py
--------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# Apache HTTP Server 2.4.49 - Path Traversal and RCE
Apache: command not found
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# searchsploit -m exploits/multiple/webapps/50383.py
```



Learn about active recon, web app attacks and privilege escalation.

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

```
HTTP/1.1 405 Method Not Allowed
Server: WebSockify Python/3.8.10
Date: Mon, 27 Oct 2025 20:14:13 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 472

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 405</p>
        <p>Message: Method Not Allowed.</p>
        <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
    </body>
</html>
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# curl -sS "http://10.201.109.36:80/..%2f..%2f..%2fvar/log/syslog" -i || true
HTTP/1.1 405 Method Not Allowed
Server: WebSockify Python/3.8.10
Date: Mon, 27 Oct 2025 20:14:14 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 472

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
```



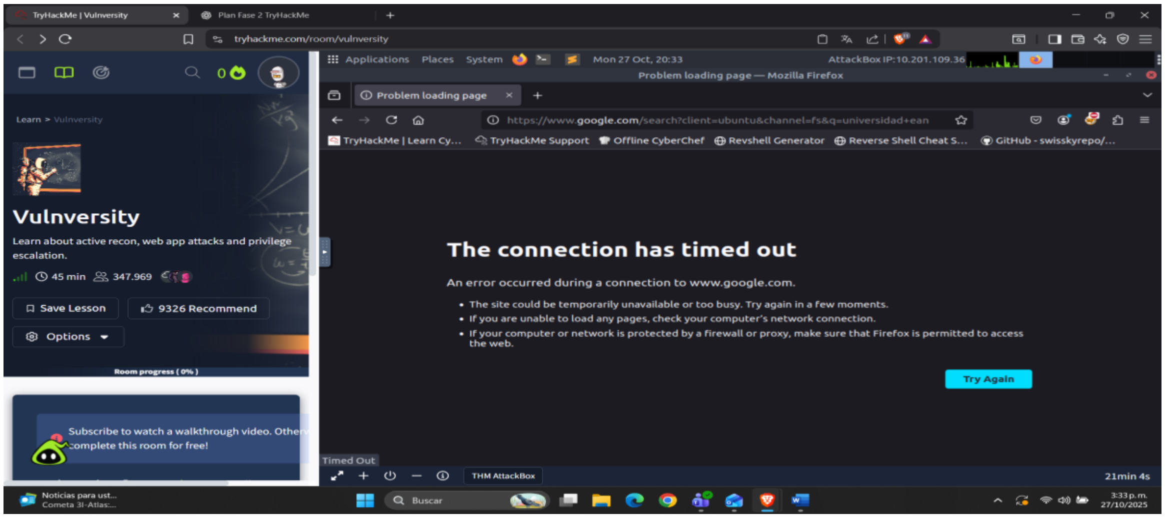
Learn about active recon, web app attacks and privilege escalation.

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

```
    <body>
        <h1>Error response</h1>
        <p>Error code: 405</p>
        <p>Message: Method Not Allowed.</p>
        <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
    </body>
</html>
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# # Prueba de consulta DNS simple
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# dig @10.201.109.36 example.com ANY +short || true
2600:1406:5e00:6::17ce:bc1b
2600:1406:bc00:53::b81e:94c8
 00:1406:bc00:53::b81e:94ce
 00:1408:ec00:36::1736:7f24
 00:1408:ec00:36::1736:7f31
2600:1406:5e00:6::17ce:bc12
0 .
b.iana-servers.net.
a.iana-servers.net.
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# dig @10.201.109.36 -x 127.0.0.1 +short || true
localhost.
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# # Mirar banner/versión ya estaba en nmap (dnsmasq-2.90)
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# # Prueba de consulta DNS simple
root@ip-10-201-109-36:~#
root@ip-10-201-109-36:~# dig @10.201.109.36 example.com ANY +short || true
23.192.228.84
23.215.0.136
23.215.0.138
```

REPORTE SESIÓN 2

En el reporte de la sesión 2 hubo un problema y es que no permitía abrir en el Firefox, paginas como Outlook para hacer el envió de esto .txt, sin embargo, adjunte imágenes donde da veracidad al trabajo realizado en la maquina virtual, la cantidad de documentos que se crearon en el intento y los documentos solicitados para la entrega de la sesión 2, cabe decir que estoy de forma individual.



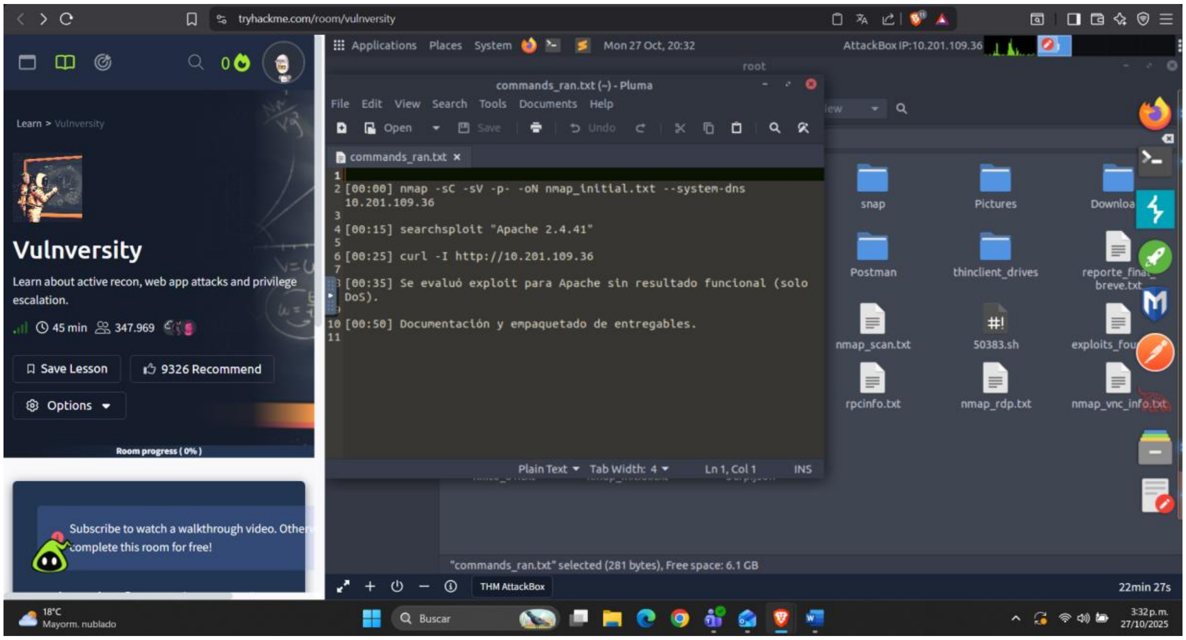
TryHackMe | Vulnversity
Plan Fase 2 TryHackMe
tryhackme.com/room/vulnversity
Applications Places System
Mon 27 Oct, 20:33
AttackBox IP:10.201.109.36
Problem loading page — Mozilla Firefox
Problem loading page
https://www.google.com/search?client=ubuntu&channel=fs&q=universidad+ean
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...
Learn > Vulnversity
Vulnversity
Learn about active recon, web app attacks and privilege escalation.
45 min 347.969
Save Lesson
9326 Recommend
Options
Room progress (0%)
Subscribe to watch a walkthrough video. Othe complete this room for free!
Try Again
Timed Out
THM AttackBox
21min 4s
Noticias para ust... Cometa 3I-Atlas:...
Buscar
3:33 p.m. 27/10/2025

The connection has timed out

An error occurred during a connection to www.google.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

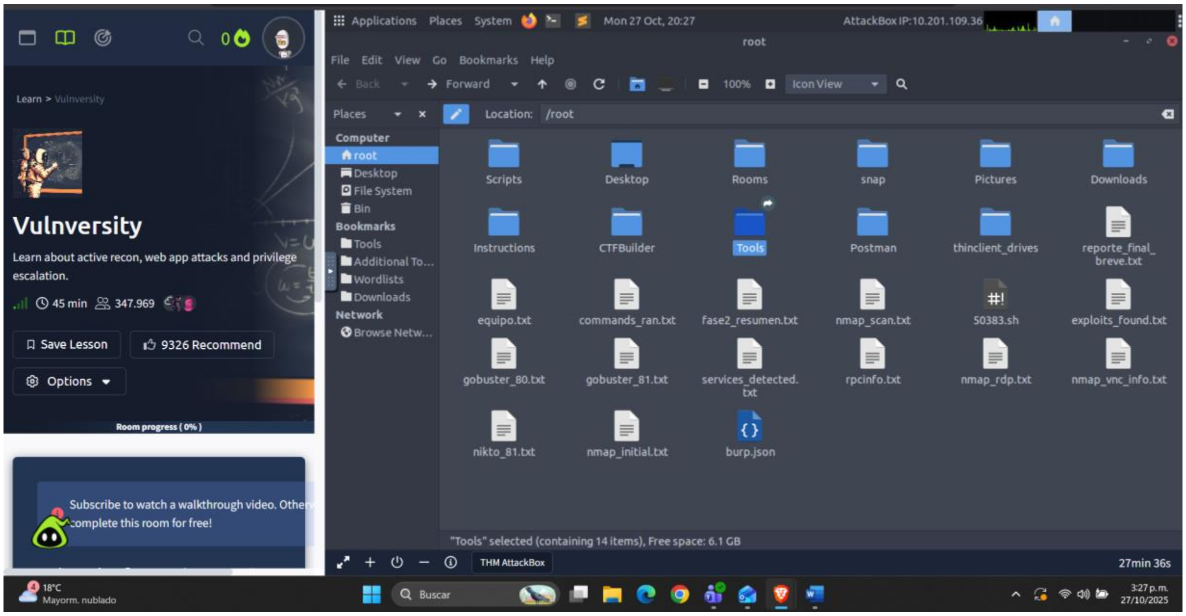
- commands_ran.txt (comandos ejecutados con breve explicación)



tryhackme.com/room/vulnversity
Applications Places System
Mon 27 Oct, 20:32
AttackBox IP:10.201.109.36
root
commands_ran.txt (~) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
commands_ran.txt
Plain Text Tab Width: 4 Ln 1, Col 1 INS
snap
Pictures
Downloa
Postman
thinclient_drives
reporte_final_breve.txt
nmap_scan.txt
50383.sh
exploits_fou
rpcinfo.txt
nmap_rdp.txt
nmap_vnc_info.txt
"commands_ran.txt" selected (281 bytes), Free space: 6.1 GB
Learn > Vulnversity
Vulnversity
Learn about active recon, web app attacks and privilege escalation.
45 min 347.969
Save Lesson
9326 Recommend
Options
Room progress (0%)
Subscribe to watch a walkthrough video. Othe complete this room for free!
THM AttackBox
22min 27s
18°C Mayorm. nublado
Buscar
3:32 p.m. 27/10/2025

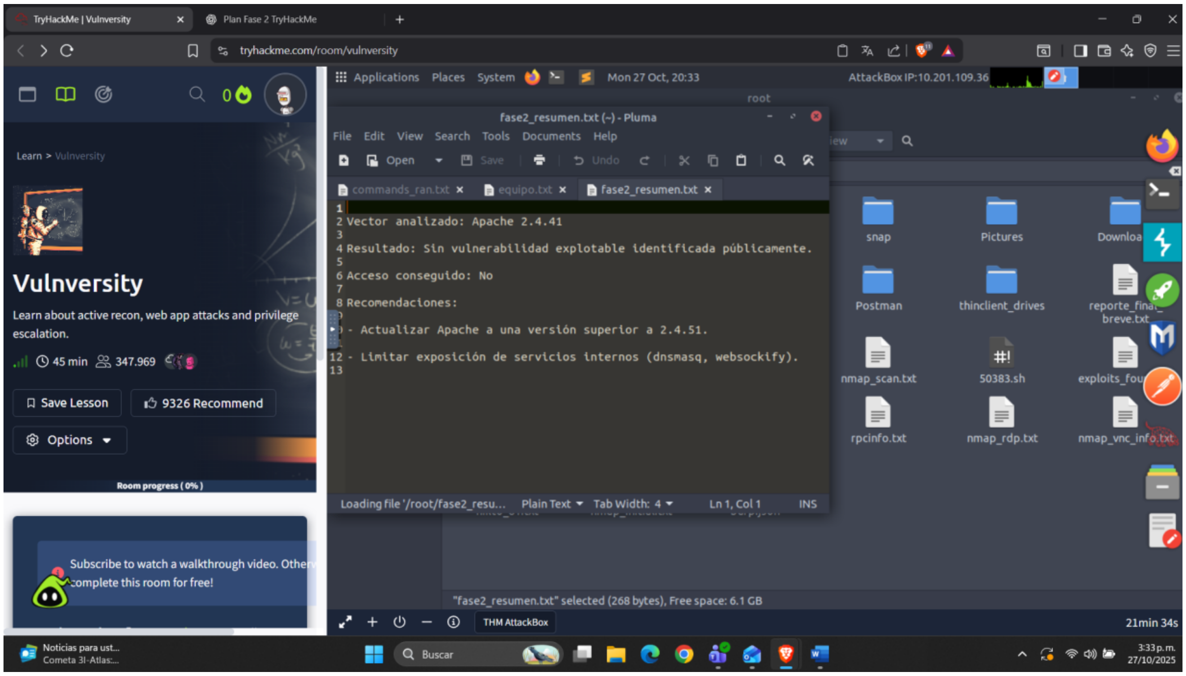
```

[00:00] nmap -sC -sV -p- -oN nmap_initial.txt --system-dns 10.201.109.36

[00:15] searchsploit "Apache 2.4.41"

[00:25] curl -I http://10.201.109.36

[00:35] Se evaluó exploit para Apache sin resultado funcional (solo DoS).

[00:50] Documentación y empaquetado de entregables.

```

- screenshot_shell.png



"Tools" selected (containing 14 items), Free space: 6.1 GB

- fase2_resumen.txt (vector explotado, acceso conseguido, recomendaciones)

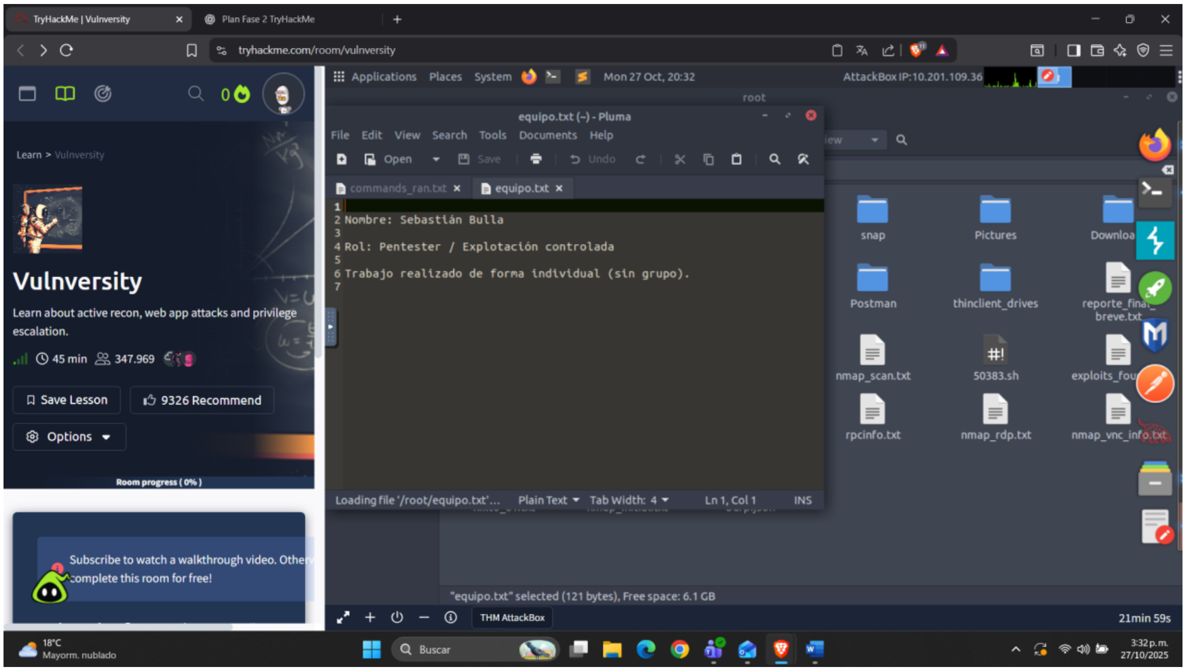


```

Vector analizado: Apache 2.4.41

Resultado: Sin vulnerabilidad explotable identificada públicamente.

Acceso conseguido: No

Recomendaciones:

- Actualizar Apache a una versión superior a 2.4.51.

- Limitar exposición de servicios internos (dnsmasq, websockify).

```

Loading file '/root/fase2_resu...

"fase2_resumen.txt" selected (268 bytes), Free space: 6.1 GB

- equipo.txt (nombres y roles)



Vulnversity

Learn about active recon, web app attacks and privilege escalation.

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

```
Nombre: Sebastián Bulla

Rol: Pentester / Explotación controlada

Trabajo realizado de forma individual (sin grupo).
```

Loading file '/root/equipo.txt'...

"equipo.txt" selected (121 bytes), Free space: 6.1 GB