

ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



BÁO CÁO AN AN TOÀN MẠNG

-&-

**ĐỀ TÀI: NGHIÊN CỨU VÀ TRIỂN KHAI CƠ CHẾ TẤN
CÔNG THU THẬP THÔNG TIN ENUMERATION**

Giảng viên hướng dẫn: **Nguyễn Duy**

Thực hiện bởi Nhóm 6, gồm:

- | | | |
|--------------------------------|-----------------|--------------------|
| • LẠI QUAN THIÊN | 22521385 | Trưởng nhóm |
| • MAI NGUYỄN NAM PHƯƠNG | 22521164 | Thành viên |
| • ĐẶNG ĐỨC TÀI | 22521270 | Thành viên |

Lớp: **NT140.P12.ANTT**

TP. Hồ Chí Minh, tháng 12 năm 2024

LỜI CẢM ƠN

Trước tiên, chúng em xin gửi lời cảm ơn sâu sắc đến thầy Nguyễn Duy - giảng viên hướng dẫn môn An Toàn Mạng, đã tận tình chỉ dẫn và chia sẻ những kinh nghiệm quý báu trong suốt quá trình thực hiện đề tài. Những ý kiến đóng góp và sự hướng dẫn của thầy đã giúp chúng em rất nhiều trong việc định hướng và hoàn thiện nội dung đồ án. Chúng em xin bày tỏ lòng biết ơn đến thầy đã hỗ trợ và động viên chúng em trong suốt quá trình thực hiện đề tài. Do giới hạn về kiến thức và thời gian, không thể tránh khỏi những thiếu sót trong đồ án, chúng em rất mong nhận được sự góp ý từ thầy để hoàn thiện hơn.

TP. Hồ Chí Minh, tháng 12 năm 2024

Nhóm 2, lớp NT140.P12.ANTT

MỤC LỤC

CHƯƠNG 1. TỔNG QUAN ĐỀ TÀI	1
CHƯƠNG 2. THỰC HIỆN ĐỀ TÀI.....	3
2.1. NetBIOS Enumeration Lab.....	3
2.1.1. NetBIOS là gì?	3
2.1.2. NetBIOS Enumeration	3
2.1.3. Công cụ và kịch bản triển khai.....	5
2.2. NFS Enumeration Lab.....	17
2.2.1. NFS là gì?.....	17
2.2.2. NFS Enumeration	18
2.2.3. Công cụ và kịch bản triển khai.....	18
2.3. DNS Enumeration Lab	28
2.3.1. DNS là gì?	28
2.3.2. DNS Enumeration	28
2.3.3. Công cụ và kịch bản triển khai.....	29
2.4. SMTP Enumeration Lab	50
2.4.1. SMTP là gì.....	50
2.4.2. SMTP Enumeration	50
2.4.3. Công cụ và kịch bản triển khai.....	50
2.5. Làm thêm: SNMP Enumeration – SNMPwalk Lab	55
2.6. Làm thêm: LDAP Enumeration Lab.....	60
PHẦN 3. KẾT LUẬN.....	65
3.1. Tầm quan trọng của Enumeration	65
3.2. Lợi ích thu được từ Enumeration	65

3.3. Những rủi ro và hạn chế của Enumeration	65
3.4. Ứng dụng thực tế.....	65
3.5. Tổng kết.....	66

CHƯƠNG 1. TỔNG QUAN ĐỀ TÀI

Enumeration là quá trình trích xuất username, hostname, tài nguyên mạng, dịch vụ từ một hệ thống hoặc mạng. Trong giai đoạn này, attacker tạo các kết nối và gửi các truy vấn trực tiếp để lấy thông tin về mục tiêu. Chúng sử dụng thông tin được thu thập bằng cách liệt kê để xác định các lỗ hổng trong bảo mật hệ thống, giúp khai thác hệ thống đích. Kỹ thuật liệt kê hoạt động trong môi trường mạng nội bộ.

Các phương pháp Enumeration tiêu biểu:

- **NetBIOS Enumeration:** Sử dụng giao thức NetBIOS để truy vấn tên máy, danh sách người dùng, và các thư mục chia sẻ trên hệ thống mạng Windows.
- **SNMP Enumeration:** Thu thập thông tin từ các thiết bị mạng (router, switch, firewall) sử dụng giao thức SNMP.
- **LDAP Enumeration:** Khai thác các dịch vụ thư mục như LDAP để thu thập thông tin người dùng và nhóm.
- **SMTP Enumeration:** Kiểm tra dịch vụ thư email để xác định các tài khoản email hợp lệ.
- **DNS Zone Transfer:** Khai thác DNS để lấy thông tin về cấu trúc của mạng, các tên miền con, và IP của từng tên miền.
- **NTP Enumeration:** NTP (Network Time Protocol) là giao thức được sử dụng để đồng bộ hóa thời gian giữa các máy tính và thiết bị trong một hệ thống mạng. Việc khai thác NTP có thể giúp thu thập thông tin về mạng, như danh sách các máy khách (clients) đang đồng bộ hóa thời gian với máy chủ NTP.
- **NFS Enumeration:** NFS (Network File System) là giao thức cho phép các máy tính chia sẻ tệp qua mạng. Việc khai thác NFS có thể giúp truy cập các thư mục hoặc tệp chia sẻ không được bảo vệ đúng cách.

Triển khai và phân tích các công cụ Enumeration: Một số công cụ như Nmap, Netcat, Metasploit, Enum4linux có thể được sử dụng để triển khai và thực hành Enumeration. Các công cụ này sẽ hỗ trợ bạn mô phỏng kỹ thuật Enumeration, giúp nhận diện được điểm yếu và hiểu rõ hơn về cách thức thực hiện Enumeration trong thực tế.

Giải pháp ngăn chặn Enumeration:

- **Quản lý dịch vụ và cổng mở:** Đảm bảo chỉ mở các cổng và dịch vụ cần thiết, chặn các dịch vụ không cần thiết.

- **Quản lý thông tin người dùng và quyền truy cập:** Hạn chế quyền truy cập và ẩn thông tin nhạy cảm từ các tài khoản người dùng.

- **Thiết lập tường lửa và IDS/IPS:** Tường lửa có thể chặn truy vấn từ các IP không xác định, trong khi hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) giúp phát hiện và ngăn chặn các hành động Enumeration.

- **Bảo mật SNMP và dịch vụ mạng:** Đảm bảo các dịch vụ SNMP, NetBIOS, LDAP được cấu hình bảo mật cao, và sử dụng các phiên bản giao thức bảo mật (như SNMPv3).

Phần tiếp theo sẽ đi vào chi tiết thực hiện đề tài, các kịch bản triển khai được dựa trên
CEH v12 - Module 4 - Enumeration

CHƯƠNG 2. THỰC HIỆN ĐỀ TÀI

2.1. NetBIOS Enumeration Lab

2.1.1. *NetBIOS là gì?*

NetBIOS ban đầu được phát triển như một API cho client truy cập tài nguyên mạng LAN. Tên NetBIOS là một chuỗi ASCII gồm 16 ký tự duy nhất được gán cho các hệ thống Windows để xác định các thiết bị mạng qua TCP/IP trong đó 15 ký tự được sử dụng cho tên thiết bị và ký tự thứ 16 được dành riêng cho loại dịch vụ hoặc bản ghi. NetBIOS thường được sử dụng trong các hệ thống Windows cũ hoặc mạng sử dụng SMB (Server Message Block) để chia sẻ tài nguyên như file và máy in. Trong mạng hiện đại, DNS đã dần thay thế NetBIOS, nhưng NetBIOS vẫn còn xuất hiện ở một số hệ thống legacy

2.1.2. *NetBIOS Enumeration*

NetBIOS Enumeration là quá trình thu thập thông tin về các thiết bị trong mạng sử dụng giao thức NetBIOS. Quá trình này nhằm liệt kê các tài nguyên được chia sẻ, nhóm làm việc, dịch vụ, và các thông tin liên quan khác của thiết bị trong mạng.

NetBIOS sử dụng port **UDP 137** (name services), port **UDP 138** (datagram services) và port **TCP 139** (session services). Attacker thường nhắm vào dịch vụ NetBIOS vì dễ khai thác và nó chạy trên Windows ngay cả khi không sử dụng. Việc Enumerate NetBIOS thường khai thác từ các cấu hình yếu hoặc không được bảo mật đúng cách trên các hệ thống cũ. Tuy nhiên, để liệt kê NetBIOS, hệ thống đích phải bật tính năng chia sẻ file và máy in và Microsoft không hỗ trợ NetBIOS name resolution cho IPv6

Bảng các thông tin có thể thu thập được từ hệ thống qua NetBIOS mã NetBIOS của dịch vụ:

Tên	Mã NetBIOS	Loại	Thông tin thu được
<host name>	00	UNIQUE	Tên máy tính (Hostname).
<domain>	00	GROUP	Tên miền hoặc nhóm làm việc (Domain name hoặc Workgroup).
<host name>	03	UNIQUE	Dịch vụ Messenger đang chạy trên máy.
<user name>	03	UNIQUE	Dịch vụ Messenger đang chạy cho người dùng đã đăng nhập.
<host name>	20	UNIQUE	Dịch vụ máy chủ (Server Service) đang hoạt động, thường là chia sẻ tệp tin.
<domain>	1D	GROUP	Tên Master Browser quản lý danh sách thiết bị trong subnet.
<domain>	1B	UNIQUE	Domain Master Browser, xác định máy chủ miền chính (PDC).
<domain>	1E	GROUP	Dịch vụ bầu chọn trình duyệt (Browser Service Elections).

2.1.3. Công cụ và kịch bản triển khai

a. Nbtstat

Nbtstat là một tiện ích Windows dùng để chẩn đoán và phân tích thông tin NetBIOS trên mạng TCP/IP. Nó hiển thị bảng tên NetBIOS, trạng thái phiên NetBIOS, và các thông tin liên quan đến thiết bị trong mạng

Những kẻ tấn công sử dụng Nbtstat để liệt kê thông tin chẳng hạn như thống kê giao thức NetBIOS qua TCP/IP (NetBT), bảng tên NetBIOS cho cả máy tính cục bộ và máy tính từ xa và bộ nhớ đệm tên NetBIOS

Nbtstat Parameter	Function
-a RemoteName	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer
-A IP Address	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
-c	Lists the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses
-n	Displays the names registered locally by NetBIOS applications such as the server and redirector
-r	Displays a count of all names resolved by a broadcast or WINS server
-R	Purges the name cache and reloads all #PRE-tagged entries from the Lmhosts file
-RR	Releases and re-registers all names with the name server
-s	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names
-S	Lists the current NetBIOS sessions and their status with the IP addresses
Interval	Re-displays selected statistics, pausing at each display for the number of seconds specified in Interval

nbtstat -A <IP>: Hiển thị bảng tên NetBIOS của máy tính từ xa, được chỉ định bởi IP địa chỉ của máy đó

```
C:\Users\Administrator>nbtstat -A 192.168.100.129

Ethernet0:
Node IpAddress: [192.168.100.128] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name                 Type                    Status
    -----
WORKGROUP                <00>   GROUP                Registered
LAB_CEH                  <00>   UNIQUE               Registered
LAB_CEH                  <20>   UNIQUE               Registered

MAC Address = 00-0C-29-37-94-B7
```

nbtstat -a <Name>: Hiển thị bảng tên NetBIOS của máy tính từ xa, trong đó RemoteName là tên NetBIOS của máy đó

```
C:\Users\Administrator>nbtstat -a LAB_CEH

Ethernet0:
Node IpAddress: [192.168.100.128] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name                 Type                    Status
    -----
WORKGROUP                <00>   GROUP                Registered
LAB_CEH                  <00>   UNIQUE               Registered
LAB_CEH                  <20>   UNIQUE               Registered

MAC Address = 00-0C-29-37-94-B7
```

nbtstat -c: Liệt kê nội dung của bộ đệm tên NetBIOS, bảng tên NetBIOS và địa chỉ IP đã được giải quyết

```
C:\Users\Administrator>nbtstat -c

Ethernet0:
Node IpAddress: [192.168.100.128] Scope Id: []

                NetBIOS Remote Cache Name Table

      Name                Type                Host Address        Life [sec]
-----
LAB_CEH                   <00>    UNIQUE                192.168.100.129      526
LAB_CEH                   <20>    UNIQUE                192.168.100.129      390

C:\Users\Administrator>
```

nbtstat -n: Hiện thị tên được đăng ký cục bộ bởi các ứng dụng NetBIOS như máy chủ

```
CA_ Command Prompt
C:\Users\namphuong>nbtstat -n

\Device\NetBT_Tcpip_{25069E9E-F642-4F63-B1C6-FA32E4D8A92E}:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Ethernet 3:
Node IpAddress: [192.168.56.1] Scope Id: []

                NetBIOS Local Name Table

      Name                Type                Status
-----
NAMPHUONGPC              <00>    UNIQUE                Registered
WORKGROUP                 <00>    GROUP                  Registered
NAMPHUONGPC              <20>    UNIQUE                Registered

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.18.1] Scope Id: []

                NetBIOS Local Name Table

      Name                Type                Status
-----
NAMPHUONGPC              <00>    UNIQUE                Registered
WORKGROUP                 <00>    GROUP                  Registered
NAMPHUONGPC              <20>    UNIQUE                Registered
```

```
VMware Network Adapter VMnet8:
Node IpAddress: [192.168.233.1] Scope Id: []

                NetBIOS Local Name Table

      Name                Type                Status
-----
NAMPHUONGPC              <00>    UNIQUE                Registered
WORKGROUP                 <00>    GROUP                  Registered
NAMPHUONGPC              <20>    UNIQUE                Registered

Ethernet:
Node IpAddress: [192.168.1.128] Scope Id: []

                NetBIOS Local Name Table

      Name                Type                Status
-----
NAMPHUONGPC              <00>    UNIQUE                Registered
WORKGROUP                 <00>    GROUP                  Registered
NAMPHUONGPC              <20>    UNIQUE                Registered

Wi-Fi:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

Nhận xét:

Ưu điểm	<ul style="list-style-type: none"> - Không cần cài đặt thêm công cụ. - Hiện thị chi tiết bảng tên NetBIOS.
Nhược điểm	<ul style="list-style-type: none"> - Chỉ hoạt động trên Windows. - Phải kiểm tra từng IP thủ công, không quét được phạm vi lớn.

b. NSE Script

NSE script (Nmap Scripting Engine script) là các tập lệnh được sử dụng trong công cụ quét mạng Nmap để thực hiện các tác vụ tự động hóa, từ việc phát hiện dịch vụ, thu thập thông tin hệ thống, đến kiểm tra bảo mật hoặc khai thác lỗ hổng

Sử dụng:

Lệnh	Ý nghĩa
<code>nmap --script nbstat <IP></code>	Thu thập thông tin NetBIOS từ địa chỉ IP cụ thể
<code>nmap --script nbstat <IP_RANGE></code>	Quét nhiều thiết bị trong một dải địa chỉ IP để thu thập thông tin NetBIOS
<code>nmap --script nbstat -p 137 <IP></code>	Chỉ định quét trên cổng 137 (NetBIOS Name Service)
<code>nmap --script nbstat --script-args nbstat.timeout=5 <IP></code>	Đặt thời gian chờ (timeout) cho tập lệnh
<code>nmap --script nbstat -p 137 --script-args newtargets <IP></code>	Tự động thêm các máy được phát hiện từ NetBIOS Name Service vào danh sách mục tiêu quét tiếp theo

Ví dụ:

```
nmap -sV -v --script nbstat.nse 192.168.100.128
```

- Quét dịch vụ NetBIOS trên máy 192.168.100.128
- Xác định chi tiết các thông tin về NetBIOS như tên máy, nhóm làm việc, địa chỉ MAC
- Hiển thị kết quả chi tiết (do có cờ -v).


```
nmap -sU -p 137 --script nbstat.nse 192.168.100.128
```

=> Quét cổng UDP 137 trên 192.168.100.128, sử dụng script nbstat.nse để thu thập các thông tin về tên máy, nhóm làm việc, và địa chỉ MAC của hệ thống NetBIOS

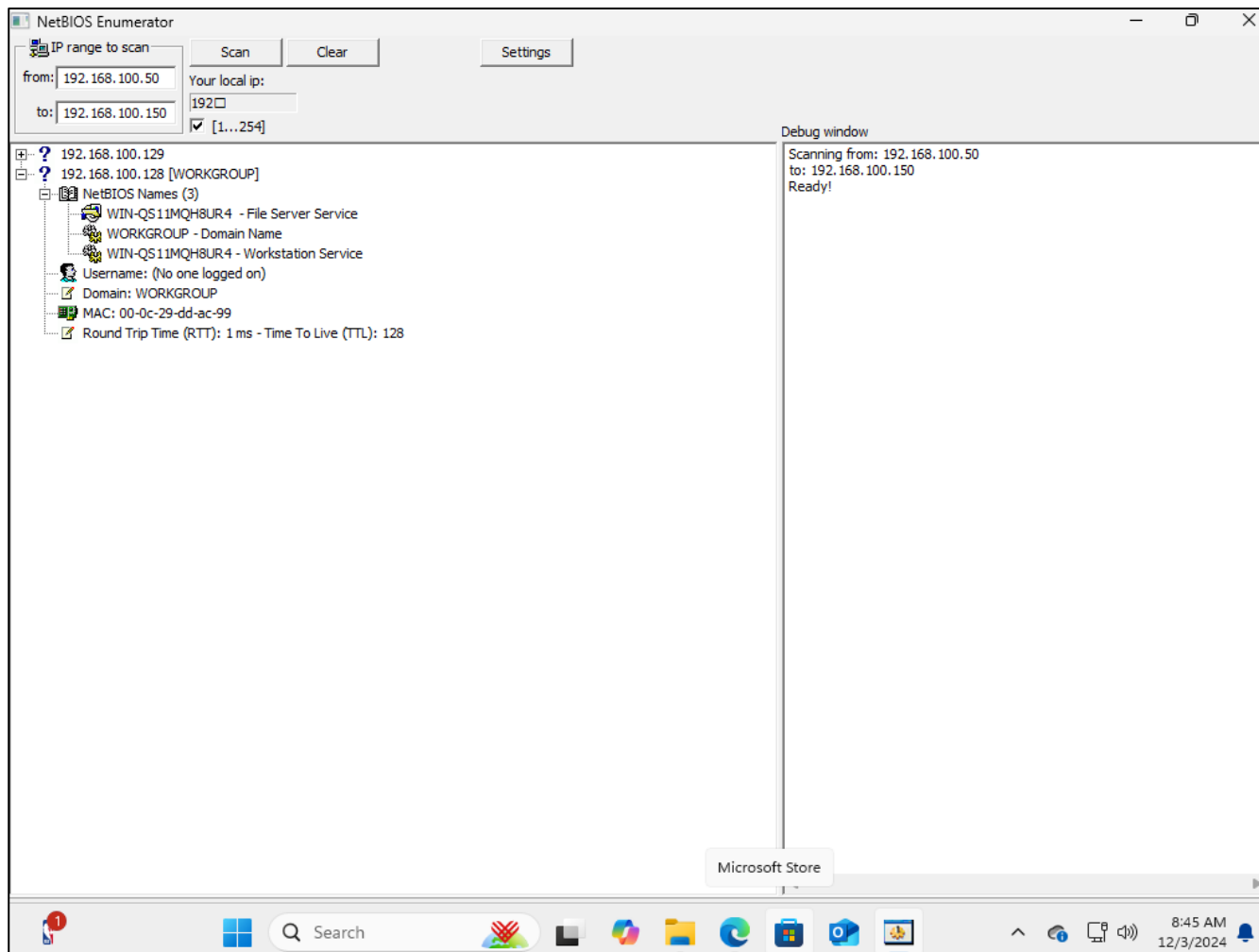
```
(kali㉿kali)-[~]  
└─$ nmap -sU -p 137 --script nbstat.nse 192.168.100.128  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 21:26 +07  
Nmap scan report for 192.168.100.128  
Host is up (0.00064s latency).  
  
PORT      STATE SERVICE  
137/udp   open  netbios-ns  
MAC Address: 00:0C:29:DD:AC:99 (VMware)  
  
Host script results:  
| nbstat: NetBIOS name: WIN-QS11MQH8UR4, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:dd:ac:99 (VMware)  
| Names:  
|   WORKGROUP<00>      Flags: <group><active>  
|   WIN-QS11MQH8UR4<00>  Flags: <unique><active>  
|_  WIN-QS11MQH8UR4<20>  Flags: <unique><active>  
  
Nmap done: 1 IP address (1 host up) scanned in 8.10 seconds
```

Nhận xét:

Ưu điểm	<ul style="list-style-type: none">- Tự động hóa quy trình.- Phân tích chi tiết và chính xác.- Khả năng mở rộng và quét hàng loạt dải địa chỉ
Nhược điểm	Tăng thời gian quét: Khi quét trên dải mạng lớn hoặc nhiều mục tiêu.

c. NetBios Enumerator

NetBIOS Enumerator là một công cụ cho phép sử dụng hỗ trợ mạng từ xa và một số các kỹ thuật khác như SMB (Khởi tin nhắn máy chủ). Nó được sử dụng để liệt kê các chi tiết như Tên NetBIOS, tên người dùng, tên miền và địa chỉ MAC cho một dải IP nhất định



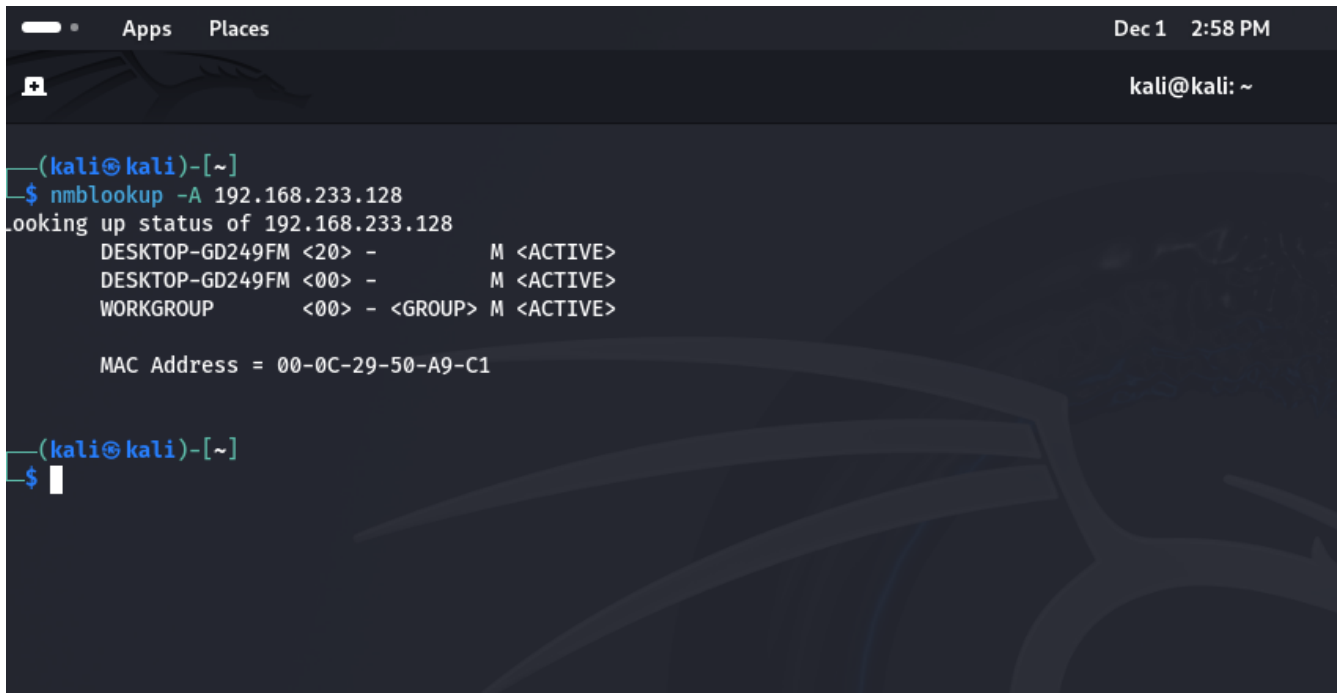
Ưu điểm	<ul style="list-style-type: none">- Tự động hóa quy trình.- Phân tích chi tiết và chính xác.- Quét đa mục tiêu- Đơn giản và dễ sử dụng vì có GUI
Nhược điểm	Giao diện chưa được hiện đại

d. Nmblookup

Là công cụ dòng lệnh trên Linux để truy vấn NetBIOS Name Service. Có thể dùng để tìm tên NetBIOS của một địa chỉ IP hoặc ngược lại

Ví dụ

```
nmblookup -a <IP>
```



```
(kali㉿kali)-[~]  
$ nmblookup -A 192.168.233.128  
Looking up status of 192.168.233.128  
DESKTOP-GD249FM <20> - M <ACTIVE>  
DESKTOP-GD249FM <00> - M <ACTIVE>  
WORKGROUP <00> - <GROUP> M <ACTIVE>  
  
MAC Address = 00-0C-29-50-A9-C1  
  
(kali㉿kali)-[~]  
$
```

```
nmblookup <hostname>
```

```
(kali㉿kali)-[~]  
$ nmblookup DESKTOP-GD249FM  
192.168.233.128 DESKTOP-GD249FM<00>
```

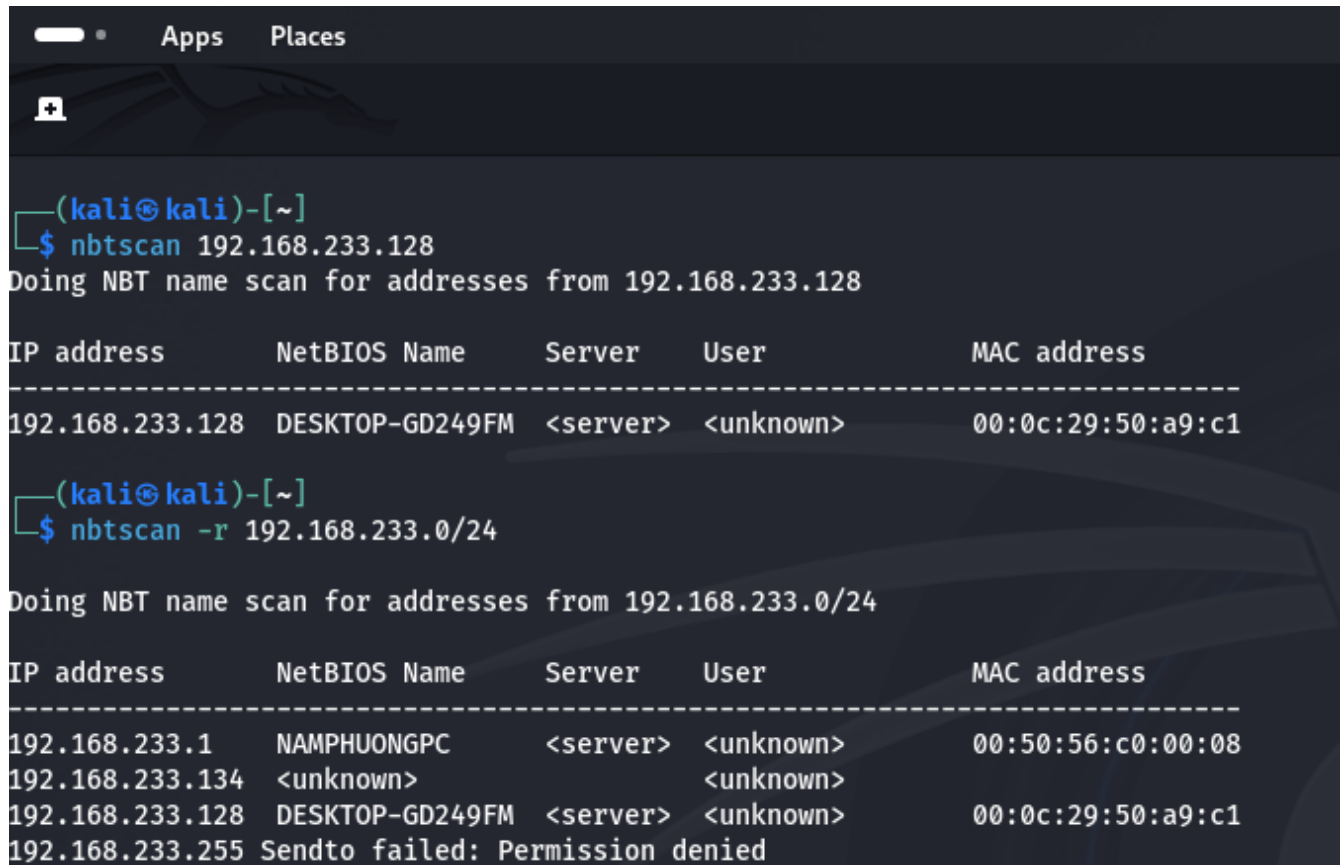
Ưu điểm	<ul style="list-style-type: none">- Linh hoạt, hỗ trợ tốt cho các mạng nhỏ.- Phù hợp để kiểm tra nhanh một địa chỉ IP cụ thể.
Nhược điểm	<ul style="list-style-type: none">- Không quét được phạm vi địa chỉ IP lớn.- Kết quả có thể giới hạn nếu máy đích không phản hồi.

e. Nbtscan

Dùng để quét phạm vi địa chỉ IP và liệt kê thông tin NetBIOS của các máy trong mạng. Hiện thị thông tin cơ bản như tên máy, nhóm làm việc và địa chỉ MAC

Ví dụ

```
nbtscan <IP>
```



```
(kali㉿kali)-[~]
$ nbtscan 192.168.233.128
Doing NBT name scan for addresses from 192.168.233.128

IP address      NetBIOS Name    Server    User      MAC address
-----
192.168.233.128  DESKTOP-GD249FM <server>  <unknown> 00:0c:29:50:a9:c1

(kali㉿kali)-[~]
$ nbtscan -r 192.168.233.0/24
Doing NBT name scan for addresses from 192.168.233.0/24

IP address      NetBIOS Name    Server    User      MAC address
-----
192.168.233.1    NAMPHUONGPC     <server>  <unknown> 00:50:56:c0:00:08
192.168.233.134  <unknown>       <unknown> <unknown> 
192.168.233.128  DESKTOP-GD249FM <server>  <unknown> 00:0c:29:50:a9:c1
192.168.233.255 Sendto failed: Permission denied
```

Ưu điểm	<ul style="list-style-type: none">- Dễ sử dụng.- Quét nhiều địa chỉ IP cùng lúc.- Tốc độ nhanh.
Nhược điểm	Chỉ tập trung vào việc liệt kê NetBIOS, không phân tích sâu

f. Net view

Net View là một công cụ dòng lệnh hiển thị danh sách các máy tính trong một workgroups hoặc các shared resource trên máy tính. Nó có thể được sử dụng theo những cách sau

Ví dụ:

```
net view \\<computername>
```

Trong lệnh trên, <computername> là tên hoặc IP của một máy tính cụ thể, các tài nguyên của máy tính đó sẽ được hiển thị

```
C:\Users\namphuong>net view \\192.168.1.128
Shared resources at \\192.168.1.128

Share name  Type  Used as  Comment
-----
Users       Disk
The command completed successfully.

C:\Users\namphuong>net view \\192.168.1.128 /ALL
Shared resources at \\192.168.1.128

Share name  Type  Used as  Comment
-----
ADMIN$      Disk      Remote Admin
C$          Disk      Default share
IPC$        IPC       Remote IPC
Users       Disk
Z$          Disk      Default share
The command completed successfully.

C:\Users\namphuong>
```

g. Ngăn chặn

1. Tắt NetBIOS nếu không cần thiết

Vấn đề: NetBIOS không còn cần thiết trong nhiều môi trường hiện đại, đặc biệt nếu sử dụng các giao thức mới như SMBv2/v3 hoặc DNS.

Giải pháp:

- Trên Windows:

1. Mở **Control Panel > Network and Sharing Center > Change adapter settings**.
2. Nhấp chuột phải vào kết nối mạng > **Properties**.
3. Chọn **Internet Protocol Version 4 (TCP/IPv4) > Properties**.
4. Nhấp **Advanced > Tab WINS**.
5. Chọn **Disable NetBIOS over TCP/IP > OK**.

- Tắt hoàn toàn dịch vụ NetBIOS trên máy chủ:

1. Mở **Services** (gõ services.msc).
2. Tìm dịch vụ **TCP/IP NetBIOS Helper**.
3. Nhấp chuột phải > **Properties > Startup type: Disabled > Stop**.

2. Chặn cổng NetBIOS trên tường lửa

Vấn đề: NetBIOS sử dụng các cổng mạng 137, 138 (UDP) và 139 (TCP) để liên lạc. Kẻ tấn công có thể khai thác các cổng này để thực hiện enumeration.

Giải pháp:

- Trên tường lửa Windows:

1. Mở **Windows Defender Firewall > Advanced Settings**.
2. Chọn **Inbound Rules > New Rule**.
3. Chọn **Port > Next**.
4. Chọn **TCP** và nhập các cổng: 139 > **Next**.
5. Chọn **Block the connection > Next > Đặt tên cho rule > Finish**.

- Trên tường lửa Linux (iptables):

```
iptables -A INPUT -p tcp --dport 139 -j DROP
iptables -A INPUT -p udp --dport 137 -j DROP
iptables -A INPUT -p udp --dport 138 -j DROP
```

3. Giới hạn quyền truy cập chia sẻ thư mục

Vấn đề: Chia sẻ thư mục công khai hoặc không kiểm soát quyền có thể dẫn đến rò rỉ thông tin.

Giải pháp:

- Chỉ chia sẻ thư mục khi cần thiết.
- Cấu hình quyền chia sẻ:
 1. Nhấp chuột phải vào thư mục > **Properties** > Tab **Sharing**.
 2. Chọn **Advanced Sharing > Permissions**.
 3. Chỉ cho phép quyền truy cập đối với người dùng cụ thể hoặc nhóm trong mạng nội bộ.
- Vô hiệu hóa chia sẻ ẩn danh:
 1. Mở **Local Security Policy** (gõ secpol.msc).
 2. Vào **Local Policies > Security Options**.
 3. Tìm **Network access: Sharing and security model for local accounts**.
 4. Đặt thành **Classic** để yêu cầu xác thực.

4. Sử dụng SMBv2 hoặc SMBv3 thay vì SMBv1

Vấn đề: SMBv1 là giao thức cũ và không an toàn, dễ bị khai thác.

Giải pháp:

- Tắt SMBv1 trên Windows:
 1. Mở **Control Panel > Programs and Features > Turn Windows features on or off**.
 2. Tìm **SMB 1.0/CIFS File Sharing Support** > Bỏ chọn > OK.
 3. Khởi động lại hệ thống.
- Bảo đảm rằng chỉ SMBv2 hoặc SMBv3 được sử dụng trong mạng nội bộ.

5. Sử dụng Group Policy để hạn chế truy cập

Vấn đề: Người dùng không được phân quyền rõ ràng có thể dẫn đến rủi ro bị enumeration.

Giải pháp: Tạo chính sách hạn chế qua Group Policy:

1. Mở **Group Policy Editor** (gõ gpedit.msc).
2. Vào **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
3. Tìm **Network access: Restrict anonymous access to named pipes and shares** > Bật chế độ **Enabled**.
4. Áp dụng chính sách qua Group Policy Management Console (GPMC) nếu quản lý domain.

2.2. NFS Enumeration Lab

2.2.1. NFS là gì?

NFS (Network File System) là một giao thức mạng cho phép các máy tính chia sẻ tệp và thư mục qua mạng. Nó được phát triển bởi Sun Microsystems vào năm 1984 và được thiết kế chủ yếu để sử dụng trên các hệ thống Unix/Linux, nhưng hiện nay cũng hỗ trợ trên nhiều hệ điều hành khác.

Cách hoạt động của NFS:

- **Máy chủ NFS (NFS Server):** Máy chủ cung cấp các thư mục hoặc tệp mà nó chia sẻ qua mạng.

- **Máy khách NFS (NFS Client):** Máy khách có thể truy cập và sử dụng các tệp/thư mục được chia sẻ từ máy chủ, như thể các tệp này nằm trong hệ thống file nội bộ của chính nó.

- **Giao thức RPC (Remote Procedure Call):** NFS sử dụng RPC để xử lý các yêu cầu từ máy khách.

Mục đích của NFS:

- Cho phép nhiều người dùng hoặc máy tính truy cập cùng một dữ liệu mà không cần sao chép cục bộ.

- Tăng hiệu quả sử dụng tài nguyên lưu trữ bằng cách tập trung hóa dữ liệu trên máy chủ.

- Thường được sử dụng trong môi trường doanh nghiệp, nơi nhiều người dùng cần truy cập dữ liệu chung trên các máy chủ.

2.2.2. NFS Enumeration

Thực hiện NFS Enumeration để xác định và trích xuất thông tin về:

- Các thư mục được export trên máy chủ NFS.
- Danh sách các client kết nối đến máy chủ, bao gồm địa chỉ IP và dữ liệu chia sẻ.
- Sử dụng các công cụ RPCScan và SuperEnum để thu thập thông tin chi tiết từ dịch vụ NFS.
- Phân tích kết quả và nhận diện lỗ hổng cấu hình có thể dẫn đến IP spoofing nhằm truy cập trái phép vào dữ liệu chia sẻ.

Lab này cung cấp các kỹ thuật thực hành **NFS Enumeration**, giúp nhận diện các lỗ hổng bảo mật từ cấu hình sai của dịch vụ NFS, bao gồm việc chia sẻ thư mục và quyền truy cập không an toàn. Đây là một phần quan trọng trong quy trình **thăm dò thông tin (Enumeration)** của CEH v12.

2.2.3. Công cụ và kịch bản triển khai

a. Một số kỹ thuật và công cụ dùng để khai thác

* Quét NFS Exported Directories

- Sử dụng lệnh showmount để liệt kê các thư mục được chia sẻ trên máy chủ NFS:
- Mục tiêu: Xác định danh sách các thư mục exported và kiểm tra quyền truy cập của các thư mục đó.

```
showmount -e <IP_Target>
```

* Quét RPC Service

- Dùng công cụ **RPCScan** hoặc **nmap** để phát hiện d/vụ **RPC** và NFS trên máy chủ:
- + Cổng 111: RPCbind – dịch vụ khởi tạo NFS.
- + Cổng 2049: Dịch vụ NFS chính.
- Mục tiêu: Xác định các cổng dịch vụ RPC đang hoạt động và thu thập phiên bản NFS.

```
nmap -sV -p 111,2049 <IP_Target>
```

*** Liệt kê và phân tích thông tin bằng SuperEnum**

SuperEnum được sử dụng để tự động liệt kê các:

- Exported directories (thư mục chia sẻ).
- Mount points (điểm gắn kết trên client).
- Danh sách các client đang kết nối.

- **Mục tiêu:** Tự động hóa quá trình thu thập và hiển thị thông tin chi tiết từ máy chủ NFS.

*** Mount thư mục NFS**

Sau khi thu thập thông tin, tiến hành **mount** thư mục chia sẻ để kiểm tra quyền truy cập:

```
mount -t nfs <IP_Target>:/exported_directory /mnt
```

Mục tiêu:

- Kiểm tra quyền đọc/ghi trên các thư mục.
- Xác định lỗ hổng nếu thư mục được cấu hình mở rộng cho mọi client.

*** Giả mạo IP (IP Spoofing)**

Sử dụng thông tin thu thập được để giả mạo địa chỉ IP hợp lệ nhằm truy cập trái phép vào dữ liệu chia sẻ (nếu cấu hình NFS sai).

Mục tiêu: Chứng minh lỗ hổng bảo mật khi không giới hạn IP client đáng tin cậy.

b. Thực hiện Task: Perform NFS Enumeration using RPCScan and SuperEnum

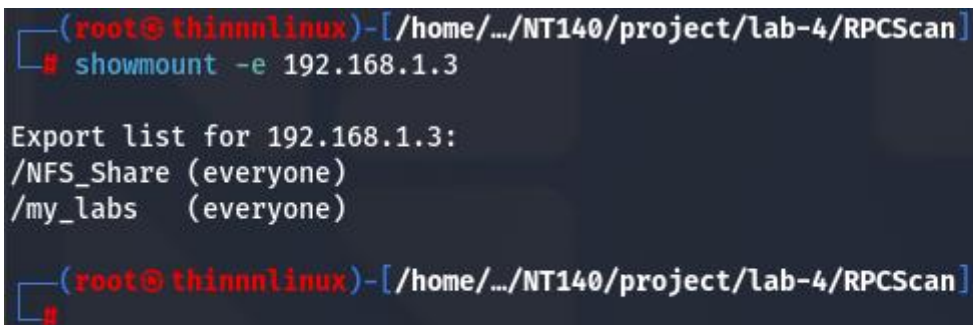
*** Mô tả:**

RPCScan: Công cụ này giao tiếp với các dịch vụ **RPC (Remote Procedure Call)** để kiểm tra cấu hình sai của **NFS shares**. Nó có thể:

- Liệt kê các dịch vụ **RPC** đang chạy.
- Hiển thị các **mountpoints** và thư mục có thể truy cập qua NFS.
- Liệt kê đệ quy các thư mục chia sẻ NFS.

SuperEnum: Là một công cụ hỗ trợ thực hiện **enumeration** cơ bản trên các cổng mở, bao gồm cổng **NFS (2049)**. SuperEnum giúp tự động hóa quá trình tìm kiếm các thông tin chia sẻ qua NFS và các dịch vụ đang chạy.

*** Thực hành**



```
(root@thinnlinux)-[/home/.../NT140/project/lab-4/RPCScan]
# showmount -e 192.168.1.3

Export list for 192.168.1.3:
/NFS_Share (everyone)
/my_labs   (everyone)

(root@thinnlinux)-[/home/.../NT140/project/lab-4/RPCScan]
#
```

Sử dụng Nmap để kiểm tra NFS:

```
(root@thinnlinux)-[/home/.../Documents/NT140/project/lab-4]
# nmap -p 2049 192.168.1.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 12:59 EST
Nmap scan report for 192.168.1.3
Host is up (0.00095s latency).
PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 00:0C:29:F7:31:FC (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Phân tích:

- Host is up (0.00095s latency): Máy đích **192.168.1.3** đang hoạt động, với độ trễ kết nối khoảng **0.95 ms**.

- PORT 2049/tcp:

- **STATE: open:** Cổng **2049** trên giao thức **TCP** đang mở.
- **SERVICE: nfs:** Dịch vụ **Network File System (NFS)** đang hoạt động trên cổng này.

- **MAC Address: 00:0C:29:F7:31:FC:** Đây là địa chỉ MAC của máy đích. Nó thuộc về **VMware**, cho thấy hệ thống đang chạy trên máy ảo VMware.

- **Dịch vụ NFS (Network File System):**

+ NFS là một dịch vụ chia sẻ file từ xa, cho phép máy trạm truy cập dữ liệu trên máy chủ qua mạng như truy cập thư mục cục bộ.

+ Cổng mặc định của NFS là **2049/tcp**.

- **Ý nghĩa:**

+ Việc cổng **2049** mở cho thấy dịch vụ NFS đang được cấu hình và sẵn sàng kết nối từ xa.

+ Đây có thể là mục tiêu tiềm năng để kiểm tra bảo mật, bao gồm:

- Liệt kê các share NFS.
- Kiểm tra quyền truy cập (đọc/ghi).
- Xác định các lỗ hổng cấu hình NFS.

Sử dụng SuperEnum

```
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:829: 'smbv2-enabled' did not match a category, filename, or directory
stack traceback:
  [C]: in function 'error' (1000000)  2      tcp      111
  /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts' 111
  /usr/share/nmap/nse_main.lua:1364: in main chunk      tcp      111
  [C]: in ?      nfs (100003)  2      tcp      2049
  /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts' 111
  /usr/share/nmap/nse_main.lua:1364: in main chunk      nfs (100003)  3      tcp      2049
  [C]: in ?      nfs (100003)  2      udp      2049
QUITTING!      nfs (100003)  2      udp      2049
Testing for 192.168.1.3: 137, Tool: nmap_smb-brute 3      udp      2049
  /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts' 111
  /usr/share/nmap/nse_main.lua:1364: in main chunk      nfs (100003)  4      tcp      2049
Testing for 192.168.1.3: 2049, Tool: nmap_nfs-ls 1      tcp      2049
Testing for 192.168.1.3: 2049, Tool: nmap_nfs-ls 2      tcp      2049
Testing for 192.168.1.3: 2049, Tool: nmap_nfs-statfs 3      tcp      2049
Testing for 192.168.1.3: 2049, Tool: showmount 1      udp      2049
  /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts' 111
  /usr/share/nmap/nse_main.lua:1364: in main chunk      nfs (100003)  2      udp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smb-brute 3      udp      2049
Testing for 192.168.1.3: 445, Tool: nbtscan (100021) 1      tcp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smb-enum-shares 1      tcp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smb-enum-users 1      tcp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smb-system-info 1      tcp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smb-os-discovery 1      udp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smb-security-mode 1      udp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smbv2-enabled 1      udp      2049
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:829: 'smbv2-enabled' did not match a category, filename, or directory
stack traceback:
  [C]: in function 'error' (1000000)  2      tcp      111
  /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts' 111
  /usr/share/nmap/nse_main.lua:1364: in main chunk      tcp      111
  [C]: in ?      nfs (100003)  2      tcp      2049
  /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts' 111
  /usr/share/nmap/nse_main.lua:1364: in main chunk      nfs (100003)  3      tcp      2049
  [C]: in ?      nfs (100003)  2      udp      2049
QUITTING!      nfs (100003)  2      udp      2049
Testing for 192.168.1.3: 445, Tool: nmap_smb-brute 3      udp      2049

Testing for 192.168.1.3: 49666

Testing for 192.168.1.3: 49668

Testing for 192.168.1.3: 49669

Testing for 192.168.1.3: 49677
```

```
Testing for 192.168.1.3: 53
Testing for 192.168.1.3: 53, Tool: nmap_dns-check-zone
Testing for 192.168.1.3: 53, Tool: nmap_dns-service-discovery
Testing for 192.168.1.3: 53, Tool: nmap_dns-srv-enum
Testing for 192.168.1.3: 53, Tool: nmap_dns-nsec3-enum
Testing for 192.168.1.3: 53, Tool: nmap_dns-nsec-enum

Testing for 192.168.1.3: 5985

0 IP/IPv6s left...

Scanning Complete!!!
Please check the folder : '/home/kali/Documents/NT140/project/lab-4/SuperEnum/17-12-2024'
```

Phân tích:

- Quét TCP/UDP trên IP 192.168.1.3:

+ SuperEnum thực hiện quét **TCP/UDP** để phát hiện các dịch vụ đang mở. Các cổng chính được quét bao gồm:

- **111**: RPC
- **135, 137, 445**: SMB (Windows File Sharing và RPC)
- **2049**: NFS (Network File System)
- **53**: DNS
- **5985, 49666, 49668, 49669, 49677**: Các cổng dịch vụ bổ sung.

- Công cụ sử dụng:

+ **nmap_rpcinfo** và **rpcinfo**: Kiểm tra các dịch vụ RPC trên cổng 111.

+ **nbtscan**: Quét NetBIOS Name Service trên cổng 135, 137, 445.

+ **nmap_smb- scripts***: Thực hiện các hoạt động enumeration trên SMB như:

- **smb-enum-shares**: Liệt kê các thư mục chia sẻ SMB.
- **smb-enum-users**: Liệt kê người dùng SMB.
- **smb-system-info**: Thu thập thông tin hệ thống SMB.
- **smb-os-discovery**: Phát hiện hệ điều hành qua SMB.
- **smb-security-mode**: Kiểm tra chế độ bảo mật SMB.

+ **nmap_nfs- scripts*** và **showmount**: Kiểm tra dịch vụ **NFS** trên cổng 2049.

+ **nmap_dns- scripts***: Kiểm tra các dịch vụ DNS trên cổng 53.

- Dịch vụ nổi bật

+ Cổng 2049 (NFS):

- Dịch vụ NFS được phát hiện và kiểm tra bằng **nmap_nfs-ls**, **nmap_nfs-statfs**, và **showmount**.
- Điều này cho thấy máy mục tiêu có thể đang chia sẻ thư mục qua **NFS**. Ta nên kiểm tra các thư mục được chia sẻ để xem xét quyền truy cập.

+ Cổng 135, 137, 445 (SMB):

- Quá trình quét SMB đã được thực hiện với nhiều script nhưng gặp lỗi với **nmap_smbv2-enabled**.

- Tuy nhiên, các script khác như smb-enum-shares, smb-enum-users, và smb-system-info vẫn chạy được và có thể cung cấp thông tin hữu ích.

+ **Cổng 53 (DNS):** Dịch vụ DNS được quét với các script như dns-check-zone, dns-service-discovery, dns-srv-enum.

- Kết luận

+ **Thành công:** SuperEnum đã quét thành công các cổng chính và sử dụng nhiều công cụ hỗ trợ như **nmap**, **rpcinfo**, và **nbtscan** để thu thập thông tin.

+ Dịch vụ cần chú ý:

- **NFS trên cổng 2049:** Kiểm tra quyền truy cập vào các thư mục chia sẻ.
- **SMB trên cổng 135, 137, 445:** Dịch vụ SMB có thể cung cấp thông tin người dùng hoặc các thư mục chia sẻ.

c. Ngăn chặn

Để ngăn chặn NFS Enumeration, ta có thể:

1. Giới hạn quyền truy cập: Cấu hình tệp exports chỉ cho phép IP đáng tin cậy.

Cấu hình tệp /etc/exports: Hạn chế quyền truy cập chỉ cho phép các địa chỉ IP đáng tin cậy. Trong tệp cấu hình, bạn có thể chỉ định quyền truy cập và các tùy chọn như chỉ cho phép truy cập từ một subnet hoặc máy chủ cụ thể.

```
/shared_directory 192.168.1.0/24(rw, sync, no_root_squash)
```

- **rw:** Chỉ định quyền đọc/ghi.

- **sync:** Đồng bộ hóa dữ liệu ngay lập tức để tăng tính nhất quán.

- **no_root_squash:** (Tránh sử dụng nếu không cần thiết) Quyền root của client được giữ nguyên trên server.

2. Sử dụng firewall: Chặn kết nối NFS từ các nguồn không xác định.

Cấu hình tường lửa (iptables hoặc firewalld):

- Chỉ cho phép các kết nối NFS từ các IP hoặc subnet đáng tin cậy.

- Với iptables:

```
iptables -A INPUT -p tcp --dport 2049 -s 192.168.1.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 2049 -j DROP
```

- Với firewalld:

```
firewall-cmd --zone=trusted --add-service=nfs --permanent  
firewall-cmd --reload
```

- **Đóng các cổng không cần thiết:** Các cổng liên quan đến NFS như 111 (rpcbind) cần được giám sát hoặc đóng nếu không cần sử dụng.

3. Dùng NFSv4 với Kerberos: Cung cấp bảo mật mạnh mẽ và xác thực.

Lý do sử dụng: NFSv4 cung cấp bảo mật tốt hơn NFSv3 nhờ hỗ trợ tích hợp với Kerberos để thực hiện xác thực, đảm bảo rằng chỉ những người dùng được phép mới truy cập được.

Cách triển khai:

- Cài đặt Kerberos trên cả server và client.
- Cấu hình NFS để sử dụng Kerberos

```
/shared_directory 192.168.1.0/24(sec=krb5p,rw, sync)
```

+ **sec=krb5:** Yêu cầu xác thực Kerberos.

+ **krb5p:** Bảo vệ tính toàn vẹn và mã hóa dữ liệu.

4. Cập nhật hệ thống thường xuyên: Vá lỗi bảo mật và theo dõi các cảnh báo.

5. Tắt showmount: Vô hiệu hóa việc liệt kê các thư mục chia sẻ.

Vấn đề: Lệnh showmount cho phép liệt kê các thư mục chia sẻ trên NFS server. Điều này có thể bị lợi dụng trong Enumeration.

Giải pháp: Chỉnh sửa cấu hình rpcbind để tắt dịch vụ showmount:

- Mở tệp /etc/sysconfig/nfs hoặc /etc/default/nfs-kernel-server.
- Thêm hoặc chỉnh sửa dòng và khởi động lại dịch vụ

```
RPCMOUNTDOPTS="--no-nfs-version 2 --no-nfs-version 3"
```

6. Sử dụng SELinux/AppArmor: Cấu hình bảo mật cho dịch vụ NFS.

Mục tiêu: Tăng cường bảo mật bằng cách giới hạn quyền truy cập của dịch vụ NFS.

Cách thực hiện:

- Với SELinux:

+ Đảm bảo SELinux được kích hoạt

```
sestatus
```

+ Thiết lập chính sách SELinux phù hợp cho NFS

```
setsebool -P nfs_export_all_rw 0  
setsebool -P nfs_export_all_ro 0
```

- Với AppArmor:

+ Đảm bảo AppArmor đang hoạt động

```
sudo aa-status
```

+ Áp dụng profile hạn chế cho NFS

```
sudo aa-enforce /etc/apparmor.d/usr.sbin.nfsd
```


2.3. DNS Enumeration Lab

2.3.1. DNS là gì?

DNS (Domain Name System) là một hệ thống phân giải tên miền thành địa chỉ IP và ngược lại, giúp các thiết bị trên mạng giao tiếp với nhau dễ dàng hơn. Nó được ví như một "danh bạ điện thoại" của Internet, nơi các tên miền dễ nhớ như `www.example.com` được ánh xạ tới địa chỉ IP thực tế mà máy tính cần để kết nối, ví dụ: `192.168.1.1`.

Vai trò của DNS

- **Phân giải tên miền:** Chuyển đổi tên miền thân thiện với con người (ví dụ: `google.com`) thành địa chỉ IP máy (ví dụ: `8.8.8.8`).
- **Cấu trúc phân tán:** DNS hoạt động theo mô hình phân tán và phân cấp, giúp nó có khả năng mở rộng và dễ quản lý trên quy mô toàn cầu.
- **Quản lý tài nguyên:** Lưu thông tin về máy chủ email (MX records), dịch vụ mạng (SRV records), hoặc các địa chỉ IP cụ thể (A/AAAA records).

2.3.2. DNS Enumeration

DNS Enumeration là quá trình thu thập thông tin từ hệ thống DNS để khám phá cấu trúc mạng và các tài nguyên liên quan. Quá trình này thường được thực hiện bởi các pentester hoặc hacker nhằm tìm kiếm các thông tin sau:

- Tên miền và địa chỉ IP tương ứng.
- Các bản ghi DNS (A, AAAA, MX, CNAME, NS, TXT, PTR, SRV).
- Máy chủ email, máy chủ web, hoặc các dịch vụ khác liên quan đến mục tiêu.
- Các tên miền con thông qua các truy vấn hoặc brute force.

Lab này giúp ta hiểu sâu hơn về cách hoạt động của DNS và các lỗ hổng có thể bị khai thác trong cấu hình DNS server. Thực hành các kỹ thuật này cung cấp kỹ năng thiết yếu cho việc kiểm tra và tăng cường bảo mật mạng.

2.3.3. Công cụ và kịch bản triển khai

a. Một số kỹ thuật và công cụ dùng để khai thác

Có ba kỹ thuật được sử dụng trong Lab này:

1. Zone Transfer

- **Mô tả:** Zone transfer (AXFR) là kỹ thuật yêu cầu DNS server cung cấp bản sao đầy đủ của vùng dữ liệu DNS. Nếu DNS server được cấu hình sai (cho phép zone transfer từ mọi IP), ta có thể lấy toàn bộ cơ sở dữ liệu DNS của mục tiêu.

- **Công cụ:**

- **Linux:**

```
dig @<DNS-server> <domain> axfr #Linux
```

- **Windows:**

```
nslookup  
  
server <DNS-server>  
  
set type=any  
  
ls -d <domain>
```

2. DNSSEC Zone Walking

- **Mô tả:** DNSSEC cung cấp bảo mật cho DNS, nhưng nếu được cấu hình không chuẩn, nó có thể lộ các thông tin trong zone file. Kỹ thuật zone walking khai thác DNSSEC để thu thập thông tin về các tên miền và subdomain.
- **Công cụ:** ldns-walk (Linux/Parrot Security)

```
ldns-walk <domain>
```

3. DNS Enumeration bằng Nmap

- **Mô tả:** Nmap có thể được sử dụng để quét và thu thập thông tin DNS bằng cách sử dụng các script tùy chỉnh.
- **Công cụ:**

```
nmap --script dns-brute -sn <domain>  
  
nmap --script dns-zone-transfer -p 53 <domain>
```

b. Thực hiện Task 1: Perform DNS Enumeration using Zone Transfer

*** Mô tả**

- Mục đích của Zone Transfer:

+ DNS server thường có một bản sao lưu hoặc server phụ. Server phụ này giữ toàn bộ dữ liệu của server chính để duy trì hoạt động nếu server chính gặp sự cố.

+ Zone transfer là cách mà server phụ lấy dữ liệu từ server chính.

- Ý nghĩa trong bảo mật:

+ Nếu một DNS server được **cấu hình sai** (cho phép zone transfer với bất kỳ yêu cầu nào), kẻ tấn công có thể thực hiện một yêu cầu zone transfer để **thu thập toàn bộ thông tin** từ hệ thống DNS của ta.

+ Các thông tin thu thập được có thể bao gồm:

- Hostnames (tên máy chủ)
- Địa chỉ IP
- Subdomains (tên miền con)
- Các thông tin cấu hình khác

- Kết quả khi thử Zone Transfer:

+ **Nếu thành công:** Kẻ tấn công có thể lấy toàn bộ zone file, chứa các thông tin nhạy cảm của DNS.

+ **Nếu thất bại:** Server sẽ từ chối yêu cầu zone transfer và báo lỗi (ví dụ: "Transfer failed" hoặc "Refused").

* Thực hiện

Trên máy ảo Kali Linux:

- Ta chạy lệnh: dig ns www.certifiedhacker.com được kết quả như hình bên dưới:
- + dig: Công cụ dòng lệnh để thực hiện các truy vấn DNS.
- + ns: Yêu cầu loại bản ghi DNS NS (Name Server), dùng để tìm các máy chủ DNS quản lý tên miền.
- + www.certifiedhacker.com: Tên miền mục tiêu.

```
root@thinnnlinux: /home/kali x + v

(root@thinnnlinux)-[/home/.../Documents/NT140/project/lab-5_task-1]
# ls

(root@thinnnlinux)-[/home/.../Documents/NT140/project/lab-5_task-1]
# dig ns www.certifiedhacker.com

; <<>> DiG 9.20.2-1-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9228
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    21600 IN      NS      ns2.bluehost.com.
certifiedhacker.com.    21600 IN      NS      ns1.bluehost.com.

;; Query time: 51 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Dec 01 05:22:39 EST 2024
;; MSG SIZE  rcvd: 111

(root@thinnnlinux)-[/home/.../Documents/NT140/project/lab-5_task-1]
# |
```

- Phân tích:

+ HEADER:

- **opcode:** QUERY - Đây là một truy vấn DNS.
- **status:** NOERROR - Truy vấn DNS thành công, không có lỗi.

- **id:** 9228 - Mã ID của truy vấn để nhận dạng phiên làm việc.

+ QUESTION SECTION

- Đây là phần **truy vấn** mà ta đã gửi.
- **Domain:** www.certifiedhacker.com
- **Loại bản ghi:** NS (Name Server)

+ ANSWER SECTION:

- www.certifiedhacker.com: Đây là một bản ghi **CNAME** (Canonical Name), nghĩa là www.certifiedhacker.com là bí danh của **certifiedhacker.com**. Bất kỳ truy vấn nào đến www.certifiedhacker.com sẽ được chuyển hướng đến **certifiedhacker.com**.
- **certifiedhacker.com**: Có hai bản ghi NS:
 - **ns2.bluehost.com.:** Đây là một máy chủ DNS thuộc dịch vụ Bluehost, chịu trách nhiệm quản lý tên miền.
 - **ns1.bluehost.com.:** Tương tự, đây là một máy chủ DNS khác của Bluehost.
- **TTL (Time To Live):**
 - 14400: Thời gian sống của bản ghi CNAME, tương đương 4 giờ.
 - 21600: Thời gian sống của các bản ghi NS, tương đương 6 giờ.

+ OPT PSEUDOSECTION:

- **EDNS:** Mở rộng DNS (Extension Mechanisms for DNS), phiên bản 0.
- **UDP size:** Gói tin DNS có kích thước tối đa là 512 byte.

+ **Query time:** Truy vấn mất **51 ms**, tương đối nhanh.

+ **SERVER:** Truy vấn được gửi đến DNS server 8.8.8.8 (DNS công cộng của Google), qua giao thức UDP.

+ **WHEN:** Thời điểm thực hiện truy vấn: Ngày 01/12/2024, lúc 05:22:39 (giờ EST).

+ **MSG SIZE rcvd:** Tổng kích thước thông điệp DNS nhận được: 111 byte.

- **Tiếp tục, ta thực hiện:** `dig @ns1.bluehost.com www.certifiedhacker.com axfr`

```
(root@thinnnlinux)-[/home/.../Documents/NT140/project/lab-5_task-1]
# dig @ns1.bluehost.com www.certifiedhacker.com axfr

; <<>> DiG 9.20.2-1-Debian <<>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

+ Lệnh trên cố gắng thực hiện **DNS Zone Transfer** từ máy chủ DNS ns1.bluehost.com cho tên miền www.certifiedhacker.com. Đây là kỹ thuật yêu cầu toàn bộ dữ liệu vùng DNS (zone file) từ máy chủ.

+ **Kết quả: "Transfer failed"** - Máy chủ DNS từ chối zone transfer. Điều này cho thấy:

- Máy chủ DNS đã được cấu hình an toàn, chỉ cho phép zone transfer với các máy chủ được ủy quyền.
- Kỹ thuật khai thác DNS zone transfer không thành công với mục tiêu này.

=> Máy chủ DNS ns1.bluehost.com không để lộ thông tin nhạy cảm thông qua zone transfer.

- **Kết luận:**

+ **CNAME Record:**

- www.certifiedhacker.com chỉ là bí danh của certifiedhacker.com.
- Tất cả yêu cầu DNS liên quan đến www.certifiedhacker.com sẽ được chuyển sang certifiedhacker.com.

+ **NS Records:**

- Tên miền certifiedhacker.com được quản lý bởi hai máy chủ DNS:
 - ns1.bluehost.com
 - ns2.bluehost.com
- Đây là máy chủ thuộc dịch vụ Bluehost, một nhà cung cấp dịch vụ hosting phổ biến.

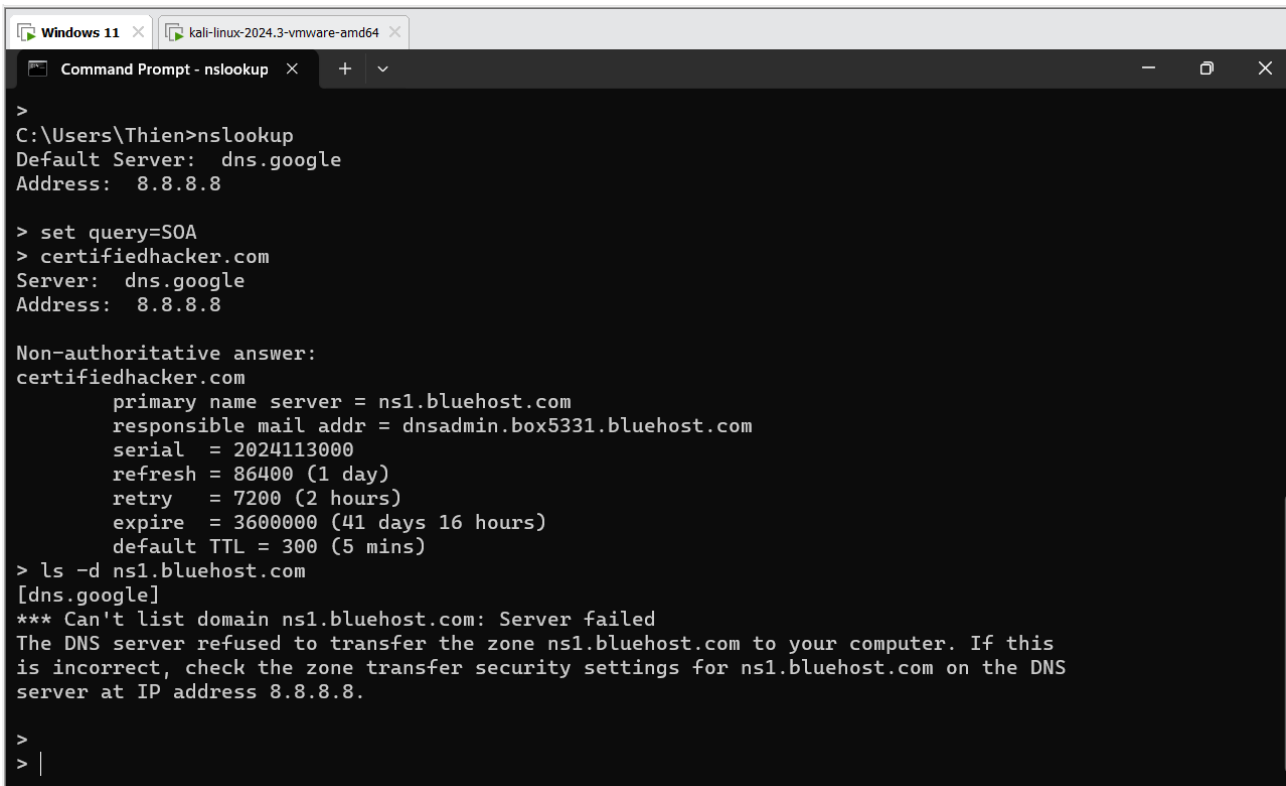
+ **Thông tin hữu ích:** Nếu mục tiêu của ta là thực hiện **DNS Enumeration**, ta có thể tiếp tục:

- Thực hiện zone transfer với hai máy chủ DNS trên (ns1.bluehost.com hoặc ns2.bluehost.com). [không thu thập được thông tin]
- Thử thu thập thêm subdomain, alias thông qua kỹ thuật khác như **DNSSEC zone walking** hoặc **Brute-force DNS**.

+ **Ứng dụng trong bảo mật:** Kết quả này có thể dùng để tìm hiểu cấu trúc DNS của mục tiêu và xác định các điểm yếu (nếu có).

Trên máy ảo Windows 11:

- Ta cũng thực hiện tương tự như bên Linux, tuy nhiên, câu lệnh sẽ khác đi đôi chút, nhưng kết quả trả về thì tương tự:



```
>
C:\Users\Thien>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set query=SOA
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024113000
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.

>
> |
```

- Phân tích:

+ Thông tin **SOA** cho thấy cấu hình DNS của certifiedhacker.com, với máy chủ DNS chính là ns1.bluehost.com.

+ **Lệnh** `ls -d ns1.bluehost.com`:

- Ta cố gắng liệt kê thông tin về tên miền ns1.bluehost.com với lệnh `ls -d`.
- Tuy nhiên, ta vẫn nhận được thông báo lỗi:
 - **"Can't list domain ns1.bluehost.com: Server failed"**.
 - Thông báo này cho thấy máy chủ DNS từ chối yêu cầu truy vấn zone transfer đối với tên miền ns1.bluehost.com.

+ Lỗi này xuất phát từ việc máy chủ DNS ns1.bluehost.com từ chối việc **zone transfer**. Điều này có thể là do máy chủ DNS đã được cấu hình để ngăn chặn các yêu cầu *zone transfer* từ bên ngoài vì lý do bảo mật. *Zone transfer* thường được dùng để sao chép toàn bộ bản ghi DNS của một miền, nhưng nếu không được bảo mật, có thể cung cấp thông tin nhạy cảm cho kẻ tấn công.

c. Thực hiện Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

*** Mô tả**

DNSSEC Zone Walking là một kỹ thuật trong DNS enumeration được sử dụng để thu thập các bản ghi DNS bên trong của máy chủ DNS mục tiêu nếu cấu hình của DNS zone không được bảo mật hoặc không đúng cách.

Mục tiêu của kỹ thuật này là truy cập vào các bản ghi DNS quan trọng mà không được công khai, giúp hacker có thể xây dựng bản đồ mạng của hệ thống mục tiêu.

DNSSEC là gì? DNSSEC (DNS Security Extensions) là một bộ mở rộng bảo mật cho DNS, nhằm ngăn chặn các cuộc tấn công như **DNS spoofing**. DNSSEC sử dụng chữ ký số để bảo vệ các bản ghi DNS và đảm bảo tính toàn vẹn của dữ liệu.

- Zone Walking:

+ **Zone Walking** là kỹ thuật đi qua tất cả các bản ghi DNS trong một zone bằng cách sử dụng DNSSEC. Các bản ghi DNSSEC bao gồm các chữ ký số (DNSKEY, RRSIG) và các bản ghi có thể giúp ta "đi bộ" qua toàn bộ zone, thu thập thông tin về các máy chủ DNS và các tên miền con mà không cần phải có quyền truy cập trực tiếp vào máy chủ chính.

+ Kỹ thuật này chỉ có thể hoạt động nếu máy chủ DNS cho phép việc truy vấn các bản ghi DNSSEC mà không yêu cầu xác thực hoặc nếu việc cấu hình không đúng cách.

- Lợi ích của Zone Walking:

+ **Thu thập thông tin:** Ta có thể thu thập thông tin về các bản ghi DNS, bao gồm máy chủ DNS, tên miền phụ, và các thông tin mạng khác.

+ **Tạo bản đồ mạng:** Các bản ghi DNS có thể giúp ta xác định các dịch vụ và máy chủ quan trọng trong mạng của mục tiêu, hỗ trợ trong việc vạch kế hoạch tấn công hoặc đánh giá bảo mật.

- **Công cụ sử dụng:** Có một số công cụ DNSSEC Zone Walking phổ biến giúp ta thực hiện kỹ thuật này, chẳng hạn như:

+ **Zonemaster:** Kiểm tra cấu hình DNSSEC của domain.

+ **DNSWalk:** Một công cụ thường được sử dụng để "đi bộ" qua các zone DNSSEC.

+ **dig:** Công cụ dòng lệnh có thể được sử dụng để thực hiện truy vấn DNSSEC.

* Thực hiện

```
root@thinnlinux: /home/kali x + v
(root@thinnlinux)-[/home/.../NT140/project/lab-5_task-2/dnsrecon-1.3.1]
# ./dnsrecon.py -d www.certifiedhacker.com -z
2024-12-01T06:48:15.705262-0500 INFO Starting enumeration for domain: www.certifiedhacker.com
2024-12-01T06:48:15.705663-0500 INFO std: Performing General Enumeration against: www.certifiedhacker.com...
2024-12-01T06:48:15.815549-0500 ERROR No answer for DNSSEC query for www.certifiedhacker.com
2024-12-01T06:48:15.944877-0500 INFO SOA ns1.bluehost.com 162.159.24.80
2024-12-01T06:48:16.154368-0500 INFO NS ns2.bluehost.com 162.159.25.175
2024-12-01T06:48:16.286440-0500 INFO NS ns1.bluehost.com 162.159.24.80
2024-12-01T06:48:16.716123-0500 INFO MX mail.certifiedhacker.com 162.241.216.11
2024-12-01T06:48:16.811865-0500 INFO CNAME www.certifiedhacker.com certifiedhacker.com
2024-12-01T06:48:16.812253-0500 INFO A certifiedhacker.com 162.241.216.11
2024-12-01T06:48:17.179241-0500 INFO TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
2024-12-01T06:48:17.277598-0500 INFO Enumerating SRV Records
2024-12-01T06:48:17.703769-0500 ERROR No SRV Records Found for www.certifiedhacker.com
2024-12-01T06:48:17.704049-0500 INFO Performing NSEC Zone Walk for www.certifiedhacker.com
2024-12-01T06:48:17.704168-0500 INFO Getting SOA record for www.certifiedhacker.com
2024-12-01T06:48:17.832121-0500 INFO Name Server 162.159.24.80 will be used
2024-12-01T06:48:18.145488-0500 INFO CNAME www.certifiedhacker.com certifiedhacker.com
2024-12-01T06:48:18.145799-0500 INFO A certifiedhacker.com 162.241.216.11
2024-12-01T06:48:19.853579-0500 INFO 2 records found
2024-12-01T06:48:19.853958-0500 INFO Completed enumeration for domain: www.certifiedhacker.com
(root@thinnlinux)-[/home/.../NT140/project/lab-5_task-2/dnsrecon-1.3.1]
#
```

Hình trên là kết quả từ việc sử dụng công cụ **dnsrecon** để thực hiện phân tích DNS đối với domain **www.certifiedhacker.com**. Dưới đây là một phân tích chi tiết về các kết quả thu được:

Các kết quả thu được:

- **SOA (Start of Authority):** **ns1.bluehost.com** (IP: 162.159.24.80) là máy chủ DNS chính của domain này.
- **NS (Name Servers):** Cả hai máy chủ DNS được liệt kê là **ns1.bluehost.com** (IP: 162.159.24.80) và **ns2.bluehost.com** (IP: 162.159.25.175). Đây là các máy chủ tên chính của domain.
- **MX (Mail Exchange):** Domain **mail.certifiedhacker.com** có địa chỉ IP là 162.241.216.11. Đây là máy chủ nhận thư cho domain này.
- **CNAME (Canonical Name):** **www.certifiedhacker.com** là một alias (biệt danh) cho domain **certifiedhacker.com**. Điều này có nghĩa là **www.certifiedhacker.com** và **certifiedhacker.com** đều trỏ tới cùng một địa chỉ.
- **A Record (Address Record):** **certifiedhacker.com** có địa chỉ IP là 162.241.216.11. Điều này cho biết máy chủ web của domain này có thể được truy cập qua địa chỉ IP này.
- **TXT (Text Record):** Một bản ghi TXT có giá trị **v=spf1 a mx ptr include:bluehost.com ?all**, liên quan đến cấu hình SPF (Sender Policy Framework) của domain, cho phép xác định các máy chủ nào có quyền gửi email thay cho domain này.

- **SRV (Service Record)**: Không tìm thấy bản ghi SRV cho domain này, có nghĩa là không có dịch vụ nào được chỉ định qua SRV record (thường dùng cho các dịch vụ như LDAP, SIP, v.v.).

- **DNSSEC**: Lỗi khi truy vấn DNSSEC, điều này có thể chỉ ra rằng DNSSEC chưa được cấu hình hoặc có vấn đề khi kiểm tra tính toàn vẹn của các bản ghi DNS.

- **NSEC Zone Walk**: Kết quả của việc đi bộ qua các NSEC (Next Secure) record cho thấy rằng chỉ có 2 bản ghi được tìm thấy: CNAME và A record. NSEC là một kỹ thuật để bảo vệ và chứng minh sự tồn tại hoặc không tồn tại của các bản ghi trong một zone DNS, nhưng kết quả ở đây khá đơn giản.

Tổng kết:

- Domain này được lưu trữ trên dịch vụ Bluehost với các bản ghi DNS cơ bản (SOA, NS, A, CNAME, MX, TXT).

- Không có các bản ghi dịch vụ (SRV) hoặc DNSSEC.

- Cổng 5061 đang mở, có thể liên quan đến dịch vụ SIP qua TLS như đã phân tích trước đó.

d. Thực hiện Task 3: Perform DNS Enumeration using Nmap

*** Mô tả**

Nmap là một công cụ mạnh mẽ được sử dụng chủ yếu để quét và phát hiện các thiết bị, cổng, dịch vụ trên mạng. Tuy nhiên, Nmap cũng có thể được sử dụng để thực hiện **DNS Enumeration** (thu thập thông tin DNS), giúp thu thập các bản ghi DNS của một domain như danh sách các subdomain, địa chỉ IP, bản ghi A, MX, CNAME, NS, TXT, và nhiều thông tin khác từ máy chủ DNS của domain mục tiêu.

Việc sử dụng **Nmap** trong DNS Enumeration có thể giúp người tấn công hoặc người kiểm tra bảo mật thu thập thông tin về cấu trúc DNS của một tổ chức hoặc dịch vụ mà không cần phải thực hiện các cuộc tấn công trực tiếp. Đây là bước quan trọng trong quá trình **OSINT** (Open-Source Intelligence) để tìm hiểu về cơ sở hạ tầng của đối tượng mà không cần xâm nhập.

Cụ thể hơn, khi sử dụng Nmap để thực hiện DNS Enumeration, ta có thể:

- **Xác định các bản ghi DNS:** Nmap có thể phát hiện các bản ghi DNS quan trọng như A, MX, CNAME, NS, TXT, giúp ta hiểu rõ hơn về cách domain được cấu hình.
- **Tìm kiếm subdomains:** Với Nmap, ta có thể sử dụng các script tùy chỉnh để tìm kiếm các subdomain liên quan đến domain mục tiêu.
- **Phát hiện các dịch vụ DNS:** Ta có thể xác định các dịch vụ DNS đang chạy trên các cổng như 53 (DNS mặc định), hoặc các cổng khác được cấu hình cho DNS tùy chỉnh.
- **Thu thập thông tin về mạng:** Bằng cách quét các máy chủ DNS của domain mục tiêu, ta có thể thu thập được các IP và các máy chủ tên (name servers) liên quan đến domain đó.

```
(root@thinnlinux)-[/home/_/NT140/project/lab-5_task-2/testssl.sh-3.2rc3]
# nmap -h
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

* Thực hiện

* Kịch bản quét 1:

```
nmap --script=broadcast-dns-service-discovery certifiedhacker.com
```

```
(wanthinnn@wanthinnn)-[~]
$ nmap --script=broadcast-dns-service-discovery certifiedhacker.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 04:50 PST
Pre-scan script results:
| broadcast-dns-service-discovery:
| 224.0.0.251
| 47989/tcp nvstream_dbd
|_ Address=192.168.1.201 2405:4803:b177:7aa0:dc09:905f:e0d0:7faa
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.35s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 984 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    filtered  smtp
26/tcp    open      rsftp
53/tcp    open      domain
80/tcp    open      http
110/tcp   open      pop3
143/tcp   open      imap
443/tcp   open      https
465/tcp   open      smtps
587/tcp   open      submission
993/tcp   open      imaps
995/tcp   open      pop3s
2222/tcp  open      EtherNetIP-1
3306/tcp  open      mysql
5432/tcp  open      postgresql

Nmap done: 1 IP address (1 host up) scanned in 21.46 seconds
```

Lệnh nmap --script=broadcast-dns-service-discovery certifiedhacker.com:

- --script=broadcast-dns-service-discovery: Sử dụng script phát hiện các dịch vụ DNS-SD (DNS Service Discovery) trong mạng.

- certifiedhacker.com: Là tên miền mục tiêu cần quét.

Script này giúp liệt kê các dịch vụ mạng khả dụng như máy in, dịch vụ chia sẻ tệp, v.v.

Kết quả sử dụng Nmap với script broadcast-dns-service-discovery cung cấp thêm thông tin liên quan đến việc phát hiện dịch vụ DNS qua broadcast trong mạng và dữ liệu từ mục tiêu certifiedhacker.com.

- **Phát hiện qua broadcast-dns-service-discovery**

+ **Broadcast address:** 224.0.0.251

- Đây là địa chỉ multicast mặc định cho mDNS (Multicast DNS).
- Dịch vụ mDNS có thể được dùng để tìm kiếm và khám phá thiết bị trong mạng cục bộ (như máy in, camera, hoặc các thiết bị IoT).

+ **Port dịch vụ được phát hiện => Port:** 47989/tcp

- **Service:** nvstream_dbd
- Đây là dịch vụ liên quan đến NVIDIA GameStream hoặc Desktop Broadcasting. Máy chủ 192.168.1.201 và địa chỉ IPv6 2405:4803:b177:7aa0:dc09:905f:e0d0:7faa có thể đang phát tệp hoặc cung cấp dịch vụ streaming.

- **Thông tin bổ sung từ mục tiêu** certifiedhacker.com

+ **IP mục tiêu:** 162.241.216.11.

+ **Reverse DNS:** box5331.bluehost.com.

+ Các cổng mở từ kết quả trước đó vẫn giữ nguyên và được xác nhận:

- **Dịch vụ FTP, SSH, Email (SMTP, POP3, IMAP).**
- **Web hosting (HTTP, HTTPS).**
- **Cơ sở dữ liệu MySQL và PostgreSQL.**

- **Nhận định về kết quả** broadcast-dns-service-discovery

+ **Ý nghĩa dịch vụ** nvstream_dbd **trên mạng cục bộ:**

- Máy chủ hoặc thiết bị 192.168.1.201 có khả năng là một thiết bị cục bộ trong mạng, không liên quan trực tiếp đến certifiedhacker.com.
- Dịch vụ này thường được sử dụng để streaming từ các thiết bị chạy NVIDIA, như PC hoặc Shield TV.

+ **Kết hợp với** certifiedhacker.com:

- Script broadcast-dns-service-discovery phù hợp để quét các dịch vụ phát hiện tự động trong mạng LAN, không nhắm trực tiếp vào mục tiêu từ xa.
- Kết quả trên có thể do ta đang quét từ một mạng nội bộ có nhiều thiết bị khác.

- **Phân tích bảo mật**

+ **Mạng nội bộ:**

- Dịch vụ nvstream_dbd thường không phải là mối đe dọa, nhưng ta cần kiểm tra cài đặt bảo mật của thiết bị liên quan nếu không sử dụng tính năng này.
- Có thể khóa hoặc hạn chế multicast DNS (mDNS) nếu không cần thiết.

+ **Mục tiêu từ xa** certifiedhacker.com:

- Không có thông tin mới về các lỗ hổng từ script này.

- Dữ liệu cũ vẫn cho thấy các cổng dịch vụ (như DNS, MySQL, và Email) cần kiểm tra thêm để đảm bảo không có cấu hình sai hoặc lỗi bảo mật.

* Kịch bản quét 2:

```
nmap -T4 -p 53 --script dns-brute certifiedhacker.com
```

```
(root@thinnlinux)~/home/kali
# nmap -T4 -p 53 --script dns-brute certifiedhacker.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 07:12 EST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.00062s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE      SERVICE
53/tcp    filtered  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|   news.certifiedhacker.com - 162.241.216.11
|   blog.certifiedhacker.com - 162.241.216.11
|   mail.certifiedhacker.com - 162.241.216.11
|   www.certifiedhacker.com - 162.241.216.11
|   ftp.certifiedhacker.com - 162.241.216.11
|   smtp.certifiedhacker.com - 162.241.216.11
|_  demo.certifiedhacker.com - 162.241.216.11

Nmap done: 1 IP address (1 host up) scanned in 5.39 seconds
```

Kết quả từ lệnh `nmap -T4 -p 53 --script dns-brute certifiedhacker.com` cho thấy quá trình quét DNS brute-force đối với domain `certifiedhacker.com` đã hoàn tất. Dưới đây là phân tích chi tiết kết quả:

- Thông tin về host:

+ **Host is up (0.00062s latency):** Máy chủ với IP 162.241.216.11 đang hoạt động và có độ trễ rất thấp (0.00062 giây).

+ **rDNS record for 162.241.216.11: box5331.bluehost.com:** Máy chủ này có một bản ghi rDNS (reverse DNS), chỉ ra rằng địa chỉ IP này được gán cho máy chủ `box5331.bluehost.com`.

- **Cổng 53 (DNS): PORT 53/tcp filtered domain:** Cổng 53 (dùng cho dịch vụ DNS) bị **filtered**, có nghĩa là không thể kết nối hoặc quét cổng này thành công do có tường lửa hoặc các cơ chế bảo mật ngăn chặn các yêu cầu từ bên ngoài.

- **Kết quả từ script dns-brute:** Script dns-brute thực hiện brute-force trên các tên miền con (subdomains) của certifiedhacker.com để tìm các tên miền có thể tồn tại. Dưới đây là các subdomains được phát hiện:

+ news.certifiedhacker.com

+ blog.certifiedhacker.com

+ mail.certifiedhacker.com

+ www.certifiedhacker.com

+ [ftp.certifiedhacker.com](ftp://ftp.certifiedhacker.com)

+ smtp.certifiedhacker.com

+ demo.certifiedhacker.com

=> Tất cả các subdomains này đều có địa chỉ IP 162.241.216.11.

- **Tóm tắt:**

+ **Cổng 53 bị filtered:** Mặc dù script thực hiện quét cổng DNS nhưng kết quả cho thấy cổng này không thể truy cập trực tiếp, có thể bị tường lửa hoặc các thiết lập bảo mật khác ngăn chặn.

+ **Kết quả từ brute-force:** Dù cổng bị filtered, nhưng script dns-brute đã thành công trong việc phát hiện một số subdomains của certifiedhacker.com. Các subdomains này đều được ánh xạ đến một địa chỉ IP duy nhất, cho thấy có thể tất cả các subdomains này đều nằm trên cùng một máy chủ.

+ Các subdomains có thể cung cấp thông tin hữu ích để thực hiện các bước tấn công tiếp theo, chẳng hạn như khai thác các dịch vụ SMTP, FTP, hay thậm chí thử tiếp cận các ứng dụng web tại www.certifiedhacker.com.

* Kịch bản quét 3:

```
nmap --script dns-srv-enum --script-args "dns-srv-enum.domain=certifiedhacker.com" certifiedhacker.com
```

```
(root@wanthin) ~/[home/wanthin]
# nmap --script dns-srv-enum --script-args "dns-srv-enum.domain=certifiedhacker.com" certifiedhacker.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 04:40 PST
Pre-scan script results:
| dns-srv-enum:
|   Exchange Autodiscovery
|   service prio weight host
|_  443/tcp 0 0 autodiscover.bluehost.com
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.31s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filtered smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2222/tcp  open  EtherNetIP-1
3306/tcp  open  mysql
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 47.26 seconds
```

Kết quả quét Nmap hiển thị một số thông tin quan trọng từ mục tiêu certifiedhacker.com:

- DNS Service Enumeration

Dịch vụ phát hiện: Exchange Autodiscovery.

- **Service:** 443/tcp (HTTPS).
- **Host:** autodiscover.bluehost.com.
- **Priority (prio):** 0.
- **Weight:** 0.

=> Dịch vụ Autodiscovery được sử dụng để cấu hình email tự động. Việc này cho thấy certifiedhacker.com đang được lưu trữ trên nền tảng **Bluehost**, một nhà cung cấp hosting phổ biến.

- Reverse DNS

+ Địa chỉ IP: 162.241.216.11.

+ Tên miền ngược (rDNS): box5331.bluehost.com.

=> Tên máy chủ (box5331) cũng xác nhận mục tiêu đang chạy trên Bluehost.

- Các cổng mở (Open Ports)

Nmap phát hiện các cổng sau đang mở, cung cấp thông tin về các dịch vụ đang chạy:

Port	State	Service	Ý nghĩa
21	Open	FTP	Máy chủ hỗ trợ FTP, có thể phục vụ việc chuyển tệp.
22	Open	SSH	Dịch vụ SSH (Secure Shell), có thể dùng để truy cập máy chủ từ xa một cách an toàn.
25	Filtered	SMTP	Máy chủ thư điện tử, nhưng bị lọc (filtered), có thể bị tường lửa chặn.
26	Open	RSFTP	Dịch vụ FTP qua cổng 26 (thường là cấu hình thay thế cho cổng 21 để bảo mật hơn).
53	Open	DNS	Hỗ trợ dịch vụ DNS. Có thể cung cấp thông tin tên miền hoặc thực hiện zone transfer nếu không được bảo vệ.
80	Open	HTTP	Máy chủ web HTTP.
110	Open	POP3	Dịch vụ email hỗ trợ giao thức POP3 (Post Office Protocol).
143	Open	IMAP	Hỗ trợ giao thức IMAP để truy xuất email.
443	Open	HTTPS	Máy chủ web qua HTTPS.
465	Open	SMTPS	Dịch vụ SMTP qua SSL.
587	Open	Submission	SMTP sử dụng cổng này để gửi thư an toàn.
993	Open	IMAPS	Giao thức IMAP qua SSL.
995	Open	POP3S	Giao thức POP3 qua SSL.

2222	Open	EtherNetIP-1	Có thể là dịch vụ quản lý từ xa hoặc backup qua SSH.
3306	Open	MySQL	Dịch vụ cơ sở dữ liệu MySQL.
5432	Open	PostgreSQL	Dịch vụ cơ sở dữ liệu PostgreSQL.

- Nhận định

+ Mục tiêu cung cấp nhiều dịch vụ liên quan đến:

- **Web hosting:** Cổng 80 (HTTP), 443 (HTTPS).
- **Email:** Cổng SMTP (25, 465, 587), POP3 (110, 995), IMAP (143, 993).
- **Dịch vụ cơ sở dữ liệu:** MySQL (3306), PostgreSQL (5432).
- **Quản lý từ xa:** SSH (22), FTP (21/26), RSFTP (26).

+ **Lỗ hổng tiềm ẩn:**

- Dịch vụ DNS (cổng 53) có thể bị khai thác nếu không cấu hình chặt chẽ.
- Các cổng dịch vụ email có thể bị kiểm tra để phát hiện thông tin rò rỉ hoặc brute force.
- Dịch vụ cơ sở dữ liệu mở trên mạng công khai là một điểm yếu bảo mật cần được kiểm tra.

- Kết luận:

+ Máy chủ được thiết lập trên nền tảng Bluehost với nhiều dịch vụ đang hoạt động.

+ Nên tiếp tục kiểm tra cụ thể hơn từng dịch vụ để xác định các lỗ hổng bảo mật tiềm tàng.

e. Ngăn chặn

1. Giới hạn truy cập DNS: Chỉ cho phép IP đáng tin cậy truy cập DNS.

Vấn đề: DNS thường được cấu hình để phản hồi mọi truy vấn, điều này khiến hệ thống dễ bị Enumeration từ các IP không đáng tin cậy.

Giải pháp:

- Cấu hình DNS server chỉ cho phép truy vấn từ các IP hoặc subnet đáng tin cậy.
- Ví dụ với BIND DNS Server:
 - + Mở tệp cấu hình `/etc/named.conf`.
 - + Thêm quy tắc và khởi động lại dịch vụ:

```
acl "trusted" {  
    192.168.1.0/24;  
    localhost;  
};  
  
options {  
    allow-query { trusted; };  
};
```

2. Vô hiệu hóa zone transfer: Cấm zone transfer từ các nguồn không xác định.

Vấn đề: Zone transfer (AXFR) cho phép lấy toàn bộ dữ liệu trong file zone của DNS server. Điều này có thể bị kẻ tấn công lợi dụng để thu thập danh sách tên miền con và IP.

Giải pháp:

- Chỉ cho phép zone transfer với các DNS server đáng tin cậy.
- Với BIND: Trong tệp cấu hình zone (ví dụ: `/etc/named.conf`)

```
zone "example.com" {  
    type master;  
    file "/var/named/example.com.db";  
    allow-transfer { 192.168.1.10; }; # Chỉ cho phép IP 192.168.1.10  
};
```

- Đối với Microsoft DNS:
 - + Vào **DNS Manager** > Zone Properties > Tab **Zone Transfers**.
 - + Chọn **Only to servers listed on the Name Servers tab**.

3. Sử dụng DNSSEC: Bảo vệ tính toàn vẹn dữ liệu DNS.

Vấn đề: DNSSEC (DNS Security Extensions) giúp bảo vệ tính toàn vẹn của dữ liệu DNS và ngăn chặn các tấn công giả mạo.

Giải pháp:

- Triển khai DNSSEC trên DNS server:

- + Tạo các cặp khóa DNSSEC (ZSK và KSK).
- + Ký zone file bằng các khóa này.
- + Cấu hình DNS server để phản hồi các truy vấn DNSSEC.

- Với BIND:

- + Thêm dòng sau vào cấu hình:

```
dnssec-enable yes;  
dnssec-validation yes;
```

- + Ký zone:

```
dnssec-signzone -A -3 RANDOM -N INCREMENT -o example.com -t  
/var/named/example.com.db
```

4. Giới hạn thông tin phản hồi DNS: Tắt tính năng ANY và hạn chế thông tin trả về.

Vấn đề: Các truy vấn DNS kiểu ANY trả về quá nhiều thông tin, tạo cơ hội cho kẻ tấn công thu thập dữ liệu DNS.

Giải pháp:

- Tắt tính năng phản hồi truy vấn ANY:

- + Với BIND:

```
options {  
    response-policy { zone "rpz-block"; };  
    minimal-responses yes;  
};
```

- + Hoặc sử dụng công cụ DNS firewall để lọc các truy vấn nguy hiểm.

- Giới hạn thông tin trả về chỉ trong phạm vi cần thiết, chẳng hạn bằng cách sử dụng chế độ **split-horizon DNS** (phân chia vùng trả lời theo nhóm IP).

5. Cấu hình tường lửa: Kiểm soát và giám sát truy vấn DNS.

Vấn đề: Tường lửa không được cấu hình đúng có thể để lọt các truy vấn DNS không hợp lệ.

Giải pháp:

- Chỉ cho phép truy vấn DNS từ các nguồn đáng tin cậy:

+ Với iptables:

```
iptables -A INPUT -p udp --dport 53 -s 192.168.1.0/24 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -j DROP
```

+ Firewallld:

```
firewall-cmd --add-service=dns --zone=trusted --permanent
firewall-cmd --reload
```

- Thường xuyên theo dõi log tường lửa để phát hiện các truy vấn bất thường

6. Kiểm soát subdomains: Đảm bảo các subdomains có chính sách bảo mật rõ ràng.

Vấn đề: Các subdomains không được quản lý chặt chẽ có thể làm lộ dữ liệu nhạy cảm.

Giải pháp:

- Triển khai **split-horizon DNS** để phân tách truy vấn nội bộ và truy vấn bên ngoài.

- Giới hạn subdomain công khai: Đảm bảo chỉ các subdomain cần thiết được công khai trên Internet.

- Kiểm tra định kỳ các subdomain bằng công cụ như:

+ **dnsenum:**

```
dnsenum example.com
```

+ **sublist3r:**

```
python3 sublist3r.py -d example.com
```

2.4. SMTP Enumeration Lab

2.4.1. SMTP là gì

SMTP (Simple Mail Transfer Protocol) là một giao thức mạng dùng để gửi email và không chịu trách nhiệm về việc **nhận email**. Đây là một giao thức quan trọng trong bộ giao thức **TCP/IP** và là một phần không thể thiếu trong việc truyền tải email. Khi gửi một email từ một ứng dụng hoặc dịch vụ email SMTP sẽ được sử dụng để truyền tải email đó từ client đến server của người nhận hoặc đến các server trung gian. Các cổng SMTP phổ biến: 25, 587, 465

2.4.2. SMTP Enumeration

Là một kỹ thuật tấn công mà kẻ xâm nhập sử dụng để **liệt kê** (enumerate) các **tài khoản người dùng hợp lệ** trên một máy chủ SMTP. Mục tiêu: thu thập thông tin về những tài khoản email hợp lệ trên hệ thống đích, điều này có thể được sử dụng cho các cuộc tấn công sau, chẳng hạn như **brute force** hoặc **phishing**.

Các công cụ và kỹ thuật phổ biến mà kẻ tấn công sử dụng trong SMTP Enumeration bao gồm:

- **VERFY (Verify)**: Kiểm tra xem một địa chỉ email có tồn tại trên máy chủ hay không
- **EXPN (Expand)**: Liệt kê các tên người dùng trong một danh sách phân phối (Distribution List) hoặc alias.
- **RCPT TO**: Chỉ định người nhận trong một email để xác minh liệu địa chỉ email đó có hợp lệ hay không.

2.4.3. Công cụ và kịch bản triển khai

a. Enumerate by using NMAP

Attacker có thể liệt kê SMTP server bằng cách sử dụng các lệnh SMTP khác nhau có sẵn tích hợp trong Nmap Scripting Engine (NSE).

- Liệt kê tất cả các lệnh hỗ trợ trong Nmap directory:

```
nmap -p 25, 365,587 -script=smtp-commands 192.168.153.129
```

```
(dducktai@kali)-[~]
$ nmap -p 25,365,587 --script=smtp-commands 192.168.153.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:35 CET
Nmap scan report for 192.168.153.129
Host is up (0.00079s latency).

PORT      STATE      SERVICE
25/tcp    open      smtp
| smtp-commands: WIN-L38JU79NS24 Hello [192.168.153.128], TURN, SIZE 2097152, ETRN, PIPELINING
, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HE
LP AUTH TURN ETRN BDAT VRFY
365/tcp   filtered  dtk
587/tcp   filtered  submission

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

- Xác định SMTP server có open relays không (cho phép gửi email từ bất kỳ máy khách nào mà không yêu cầu xác thực, không phân biệt người gửi):

```
nmap -p 25,365,587 -script=smtp-open-relay 192.168.153.129
```

```
(dducktai@kali)-[~/smtp-user-enum]
$ nmap -p 25,365,587 -script=smtp-open-relay 192.168.153.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 17:08 CET
Nmap scan report for 192.168.153.129
Host is up (0.00083s latency).

PORT      STATE      SERVICE
25/tcp    open      smtp
| smtp-open-relay: Server is an open relay (14/16 tests)
365/tcp   filtered  dtk
587/tcp   filtered  submission

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```

- Liệt kê tất cả người dùng trên máy chủ SMTP:

```
nmap -p 25 -script=smtp-enum-users 192.168.153.129
```

```
(dducktai@kali)-[~]
$ nmap -p 25 -script=smtp-enum-users 192.168.153.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:47 CET
Nmap scan report for 192.168.153.129
Host is up (0.0010s latency).

PORT      STATE      SERVICE
25/tcp    open      smtp
| smtp-enum-users:
|_ root
|_ admin
|_ administrator
|_ webadmin
|_ sysadmin
|_ netadmin
|_ guest
|_ user
|_ web
|_ test

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```


b. Enumerate by using smtp-user-enum:

smtp-user-enum là một công cụ để liệt kê các tài khoản người dùng ở mức hệ điều hành (OS-level) trên Solaris thông qua dịch vụ SMTP (sendmail). Nó liệt kê bằng cách kiểm tra các phản hồi đối với các lệnh VRFY, EXPN và RCPT TO. **smtp-user-enum** cần được chuyển vào danh sách người dùng và ít nhất một mục tiêu đang chạy dịch vụ SMTP.

Cú pháp:

smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)

Trong đó:

- m n:** Số tiến trình tối đa (mặc định là 5)
- M mode:** Chỉ định lệnh SMTP sẽ sử dụng để đoán tên người dùng trong số EXPN, VRFY và RCPT TO (mặc định: VRFY)
- u user:** Kiểm tra xem người dùng có tồn tại trên hệ thống đích hay không?
- f addr:** Chỉ định địa chỉ email gửi để sử dụng cho việc đoán “RCPT TO” (mặc định: user@example.com)
- D dom:** Chỉ định domain để thêm vào danh sách người dùng được cung cấp để tạo địa chỉ email (mặc định: không có)
- U file:** Chọn file chứa tên đăng nhập để kiểm tra qua dịch vụ SMTP
- t host:** Chỉ định server host đang chạy dịch vụ SMTP
- T file:** Chọn file chứa hostname chạy dịch vụ SMTP
- p port:** Chỉ định port TCP mà dịch vụ SMTP chạy trên đó (mặc định: 25)
- d:** Bật debug
- t n:** Đợi tối đa n giây để trả lời (mặc định: 5)
- v:** Chế độ đầu ra chi tiết
- h:** Trợ giúp

perl smtp-user-enum.pl -u root -t 192.168.153.129 -p 25

```
(dducktai@kali)-[~/smtp-user-enum]
$ perl smtp-user-enum.pl -u root -t 192.168.153.129 -p 25

Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
|                               Scan Information                               |
-----

Mode ..... VRFY
Worker Processes ..... 5
Target count ..... 1
Username count ..... 1
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....

##### Scan started at Tue Dec 17 14:05:21 2024 #####
192.168.153.129: root exists
##### Scan completed at Tue Dec 17 14:05:21 2024 #####
1 results.

1 queries in 1 seconds (1.0 queries / sec)
```

- Chạy lệnh sau để kiểm tra trong wordlist (Seclist) những danh sách người dùng phổ thông:

perl smtp-user-enum.pl -U userlist.txt -t 192.168.153.129 -p 25

```
(dducktai@kali)-[~/smtp-user-enum]
$ perl smtp-user-enum.pl -U userlist.txt -t 192.168.153.129 -p 25

Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
|                               Scan Information                               |
-----

Mode ..... VRFY
Worker Processes ..... 5
Usernames file ..... userlist.txt
Target count ..... 1
Username count ..... 17
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....

##### Scan started at Tue Dec 17 15:29:30 2024 #####
192.168.153.129: admin exists
192.168.153.129: info exists
192.168.153.129: guest exists
192.168.153.129: test exists
192.168.153.129: root exists
192.168.153.129: adm exists
192.168.153.129: mysql exists
192.168.153.129: administrator exists
192.168.153.129: user exists
192.168.153.129: ftp exists
192.168.153.129: oracle exists
192.168.153.129: pi exists
192.168.153.129: ec2-user exists
192.168.153.129: ansible exists
192.168.153.129: puppet exists
192.168.153.129: azureuser exists
192.168.153.129: vagrant exists
##### Scan completed at Tue Dec 17 15:29:30 2024 #####
17 results.
```

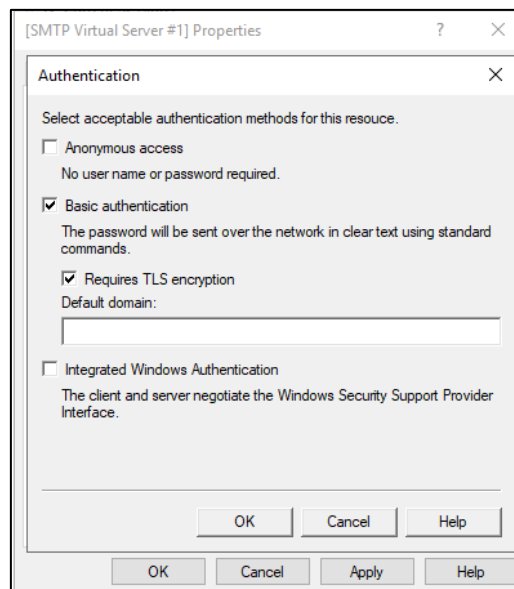
c. Ngăn chặn

1. Yêu cầu xác thực SMTP (SMTP Authentication)

Kích hoạt **SMTP Authentication** để đảm bảo chỉ người dùng đã xác thực mới được phép kết nối và gửi email.

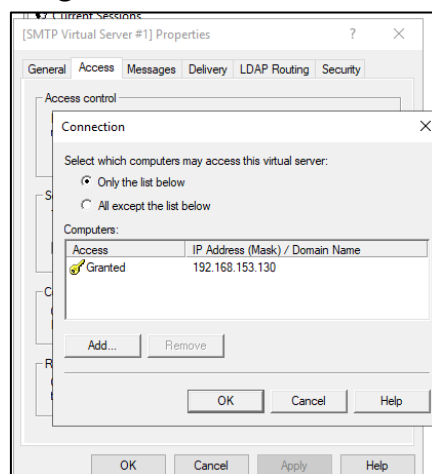
Thực hiện:

- Trong tab Access Chọn Authentication:
 - Tick vào Basic Authentication hoặc Integrated Windows Authentication.
 - Bỏ chọn Anonymous Access.
- Lưu cấu hình và khởi động lại SMTP Service.



2. Kích hoạt IP Restriction:

- Trong tab Access, chọn Connection và Relay Restrictions: Chỉ định IP hoặc dải IP được phép kết nối với SMTP Server.
- Lưu cấu hình và khởi động lại SMTP Service.



2.5. Làm thêm: SNMP Enumeration – SNMPwalk Lab

(Phần này không nằm trong phân công giữa 2 nhóm thực hiện đề tài)

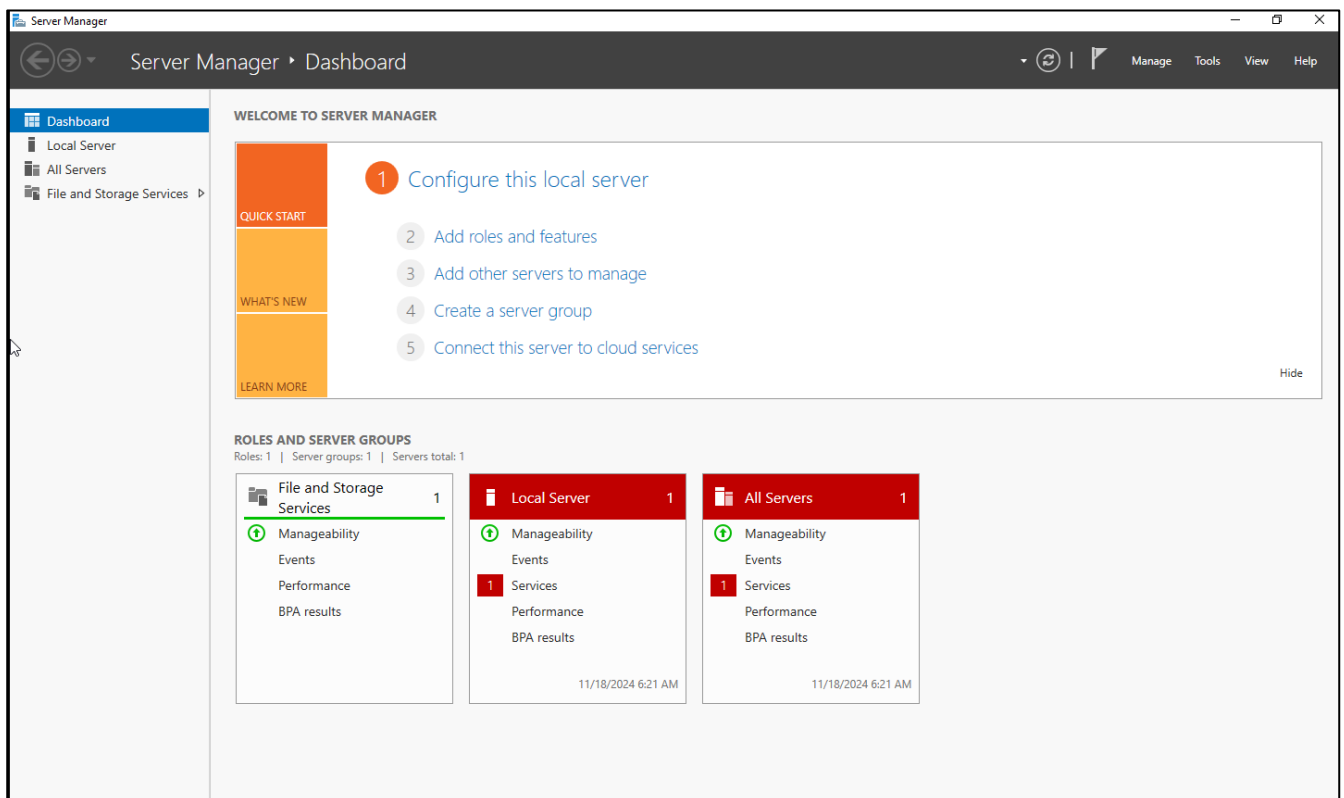
Ở kịch bản này ta sẽ sử dụng 2 OS như sau:

- Parrot Security: máy chính dùng để khai thác SNMP Enumeration
- Window Server 2022: máy bị khai thác SNMP Enumeration

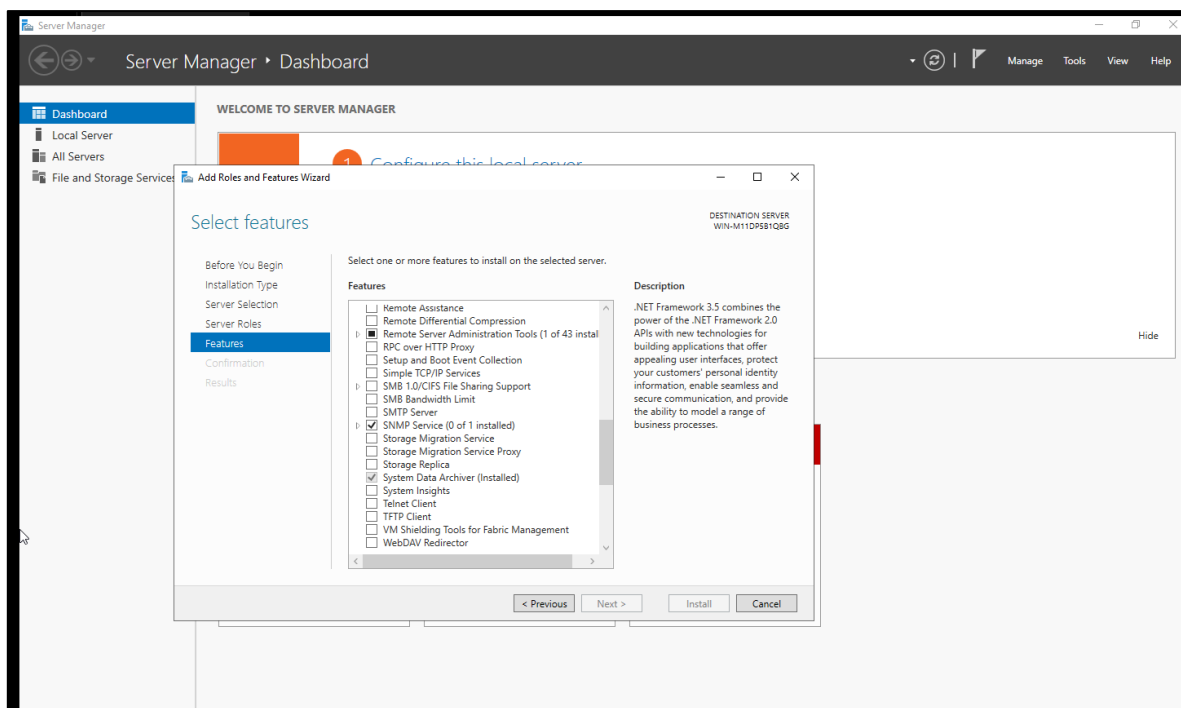
* Thực hiện setting trong Window Server 2022 để phù hợp với yêu cầu Enumeration:

- Vào Server Manager:

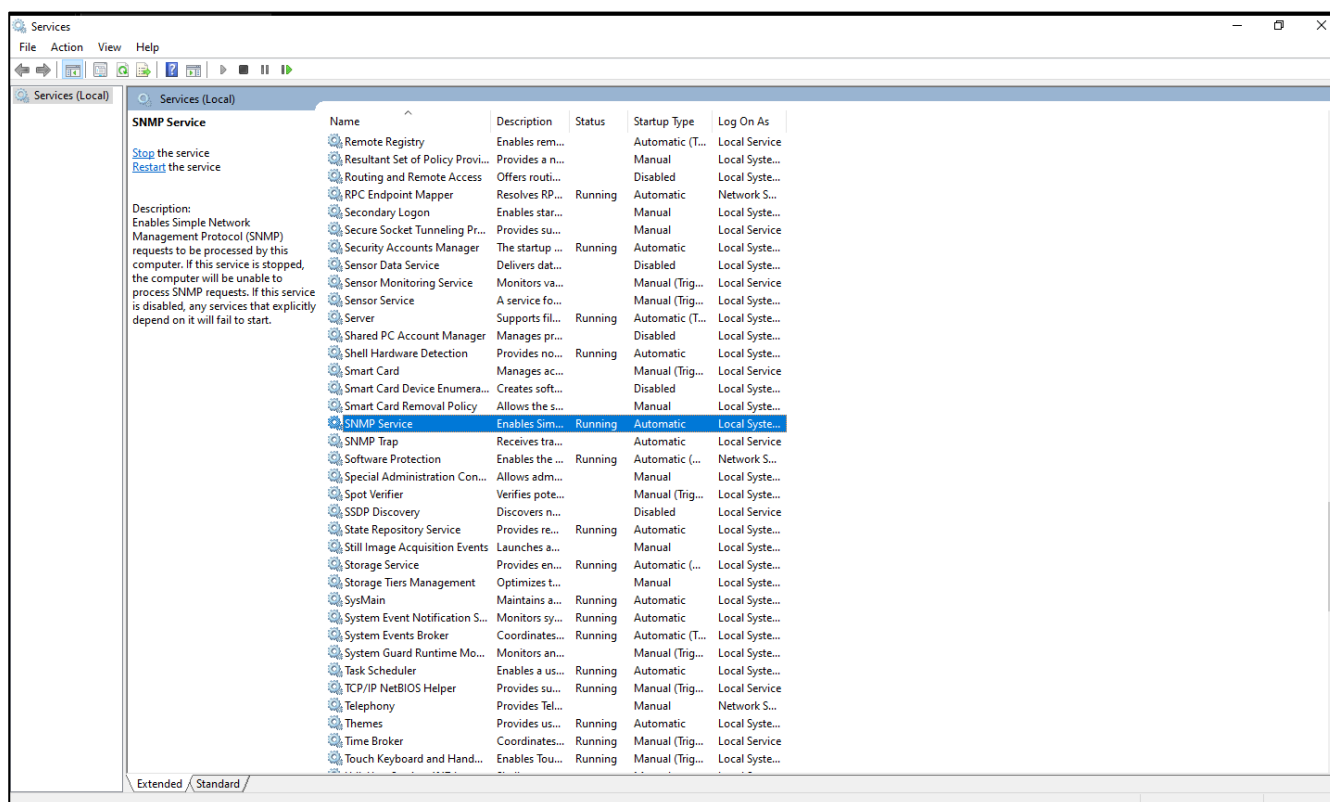
+ Add role and feature:



+ Vào tab Features -> tick chọn SNMP Service -> Install => để kích hoạt SNMP trên Window Server

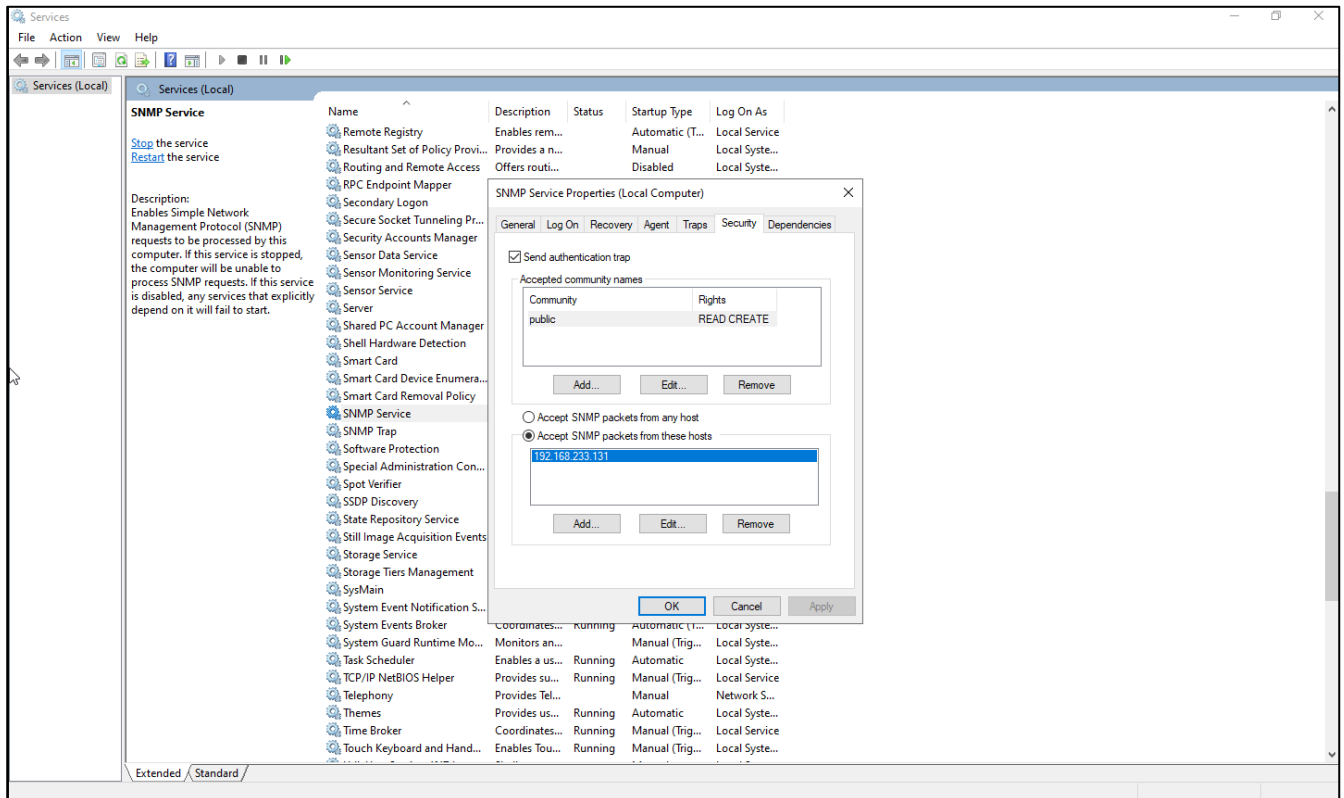


+ Vào Services -> tìm SNMP Services



+ Mở properties của SNMP Service rồi chọn vào tab Security setting như sau

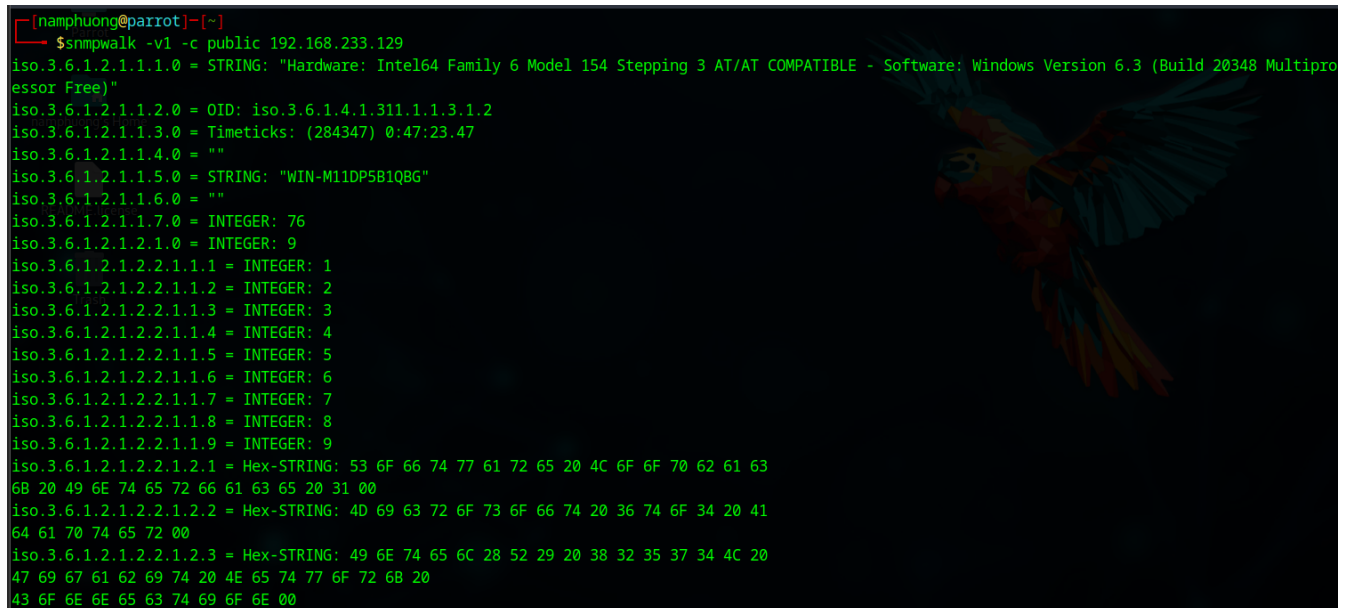
- Tạo 1 community mới tên là public và cấp quyền bất kì cho nó (ở đây mình cấp quyền READ CREATE)
- Có thể chọn nhận gói tin SNMP từ tất cả địa chỉ hoặc chỉ những địa chỉ mình cho phép (ở đây mình sử dụng option 2 và đưa địa chỉ của Parrot OS là 192.168.233.131 vào)



+ Ngoài ra ta cần cho phép lưu lượng qua các cổng 161 (UDP) và 162 (UDP) nếu chưa có

* Thực hiện khai thác trên Parrot

- snmpwalk -v1 -c public 192.168.233.129 (ip của Window Server 2022)



```
[namphuong@parrot]~$ snmpwalk -v1 -c public 192.168.233.129
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 154 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.2
iso.3.6.1.2.1.1.3.0 = Timeticks: (284347) 0:47:23.47
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "WIN-M11DP5B1QBG"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.2.1 = Hex-STRING: 53 6F 66 74 77 61 72 65 20 4C 6F 6F 70 62 61 63
6B 20 49 6E 74 65 72 66 61 63 65 20 31 00
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 4D 69 63 72 6F 73 6F 66 74 20 36 74 6F 34 20 41
64 61 70 74 65 72 00
iso.3.6.1.2.1.2.2.1.2.3 = Hex-STRING: 49 6E 74 65 6C 28 52 29 20 38 32 35 37 34 4C 20
47 69 67 61 62 69 74 20 4E 65 74 77 6F 72 6B 20
43 6F 6E 6E 65 63 74 69 6F 6E 00
```

+ iso.3.6.1.2.1.1.1.0: là một hệ thống Windows Server hoặc tương tự, phiên bản 6.3 (Windows Server 2012 R2 hoặc Windows 8.1)

+ iso.3.6.1.2.1.1.3.0: hệ thống đã hoạt động được 47 phút 23 giây

+ iso.3.6.1.2.1.1.5.0: là tên máy tính hoặc hostname

+ iso.3.6.1.2.1.2.7.0: là số dịch vụ được hỗ trợ bởi thiết bị

+ iso.3.6.1.2.1.2.2.1.X: chứa thông tin chi tiết về các giao diện mạng (interfaces)

-snmpwalk -v2c -c public 192.168.233.129 (ip của Window Server 2022)

```
[namphuong@parrot]~$  
$snmpwalk -v2c -c public 192.168.233.129  
iso.3.6.1.2.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 154 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.2  
iso.3.6.1.2.1.1.3.0 = Timeticks: (361395) 1:00:13.95  
iso.3.6.1.2.1.1.4.0 = ""  
iso.3.6.1.2.1.1.5.0 = STRING: "WIN-M11DP5B1QBG"  
iso.3.6.1.2.1.1.6.0 = ""  
iso.3.6.1.2.1.1.7.0 = INTEGER: 76  
iso.3.6.1.2.1.2.1.0 = INTEGER: 9  
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1  
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2  
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3  
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4  
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5  
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6  
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7  
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8  
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9  
iso.3.6.1.2.1.2.2.1.2.1 = Hex-STRING: 53 6F 66 74 77 61 72 65 20 4C 6F 6F 70 62 61 63 68 20 49 6E 74 65 72 66 61 63 65 20 31 00  
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 4D 69 63 72 6F 73 6F 66 74 20 36 74 6F 34 20 41 64 61 70 74 65 72 00  
iso.3.6.1.2.1.2.2.1.2.3 = Hex-STRING: 49 6E 74 65 6C 28 52 29 20 38 32 35 37 34 4C 20 47 69 67 61 62 69 74 20 4E 65 74 77 6F 72 68 20 43 6F 6E 6E 65 63 74 69 6F 6E 00  
iso.3.6.1.2.1.2.2.1.2.4 = Hex-STRING: 4D 69 63 72 6F 73 6F 66 74 20 49 50 2D 48 54 54 50 53 20 50 6C 61 74 66 6F 72 6D 20 41 64 61 70
```

+ iso.3.6.1.2.1.1.0: là một hệ thống Windows Server hoặc tương tự, phiên bản 6.3 (Windows Server 2012 R2 hoặc Windows 8.1)

+ iso.3.6.1.2.1.1.3.0: hệ thống đã hoạt động được 1 tiếng 13 giây

+ iso.3.6.1.2.1.1.5.0: là tên máy tính hoặc hostname

+ iso.3.6.1.2.1.2.7.0: là số dịch vụ được hỗ trợ bởi thiết bị

+ iso.3.6.1.2.1.2.2.1.X: chứa thông tin chi tiết về các giao diện mạng (interfaces)

=> Về cơ bản thì snmp v1 và v2c cũng khá là tương đồng nhau về kết quả trả về, nhưng v2c có một số ưu điểm như sau:

+ v2c hỗ trợ lệnh GetBulk, cho phép lấy nhiều giá trị dữ liệu trong một lần yêu cầu. Điều này giảm bớt số lượng yêu cầu (request) cần thiết để lấy nhiều thông tin, đặc biệt là khi làm việc với bảng (như Interface Table) trong khi v1 không có tính năng này, phải sử dụng nhiều lệnh GetNext để duyệt qua các OID

+ Về cơ bản, thông tin có thể truy cập được giống nhau giữa v1 và v2c, miễn là bạn có quyền (community string) phù hợp và thiết bị hỗ trợ các OID tương ứng (không đáng kể)

+ v2c giúp lấy thông tin hiệu quả hơn nhờ khả năng truy xuất dữ liệu hàng loạt

- + v2c hỗ trợ Counter64, phù hợp thiết bị hiện đại, v1 sử dụng Counter32
- + v2c cung cấp cơ chế xử lý lỗi tốt hơn: bao gồm mã lỗi chi tiết và mô tả lỗi

2.6. Làm thêm: LDAP Enumeration Lab

(Phần này không nằm trong phân công giữa 2 nhóm thực hiện đề tài)

Đối tượng:

- Attacker: Máy ảo Ubuntu 20.04.6
- Server: Máy ảo Ubuntu 20.04.6

Kịch bản 1: LDAP Enumeration bằng NMAP và Python

Server:

- Đang sử dụng dịch vụ LDAP Server.
- Thông tin trên Server như sau:

```
dducktai@ubuntu:~$ ldapsearch -x -b "" -s base "(objectClass=*)" namingContexts
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectClass=*)
# requesting: namingContexts
#
#
dn:
namingContexts: dc=domain,dc=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
dducktai@ubuntu:~$ ldapsearch -x -b "" -s base "(objectClass=*)" supportedLDAPVersion
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectClass=*)
# requesting: supportedLDAPVersion
#
#
dn:
supportedLDAPVersion: 3

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

```
dducktai@ubuntu:~$ 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
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:cf:fe:71 brd ff:ff:ff:ff:ff:ff
    altnam enp2s1
    inet 192.168.159.15/24 brd 192.168.159.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::a407:2dec:8401:f0d4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Attacker:

- Attacker có thể liệt kê LDAP thủ công bằng Python. Sử dụng Nmap, kiểm tra xem máy chủ LDAP có đang lắng nghe port 389 đối với LDAP và cổng 636 đối với secure LDAP hay không:

```
dducktai@ubuntu:~$ nmap -p 389 192.168.159.15
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-19 07:50 PST
Nmap scan report for 192.168.159.15
Host is up (0.0019s latency).

PORT      STATE SERVICE
389/tcp   open  ldap

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
dducktai@ubuntu:~$ nmap -p 636 192.168.159.15
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-19 07:51 PST
Nmap scan report for 192.168.159.15
Host is up (0.0010s latency).

PORT      STATE SERVICE
636/tcp   filtered ldapssl

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

- Kết quả từ Nmap cho thấy cổng 636 (LDAP over SSL) bị "filtered," có nghĩa là không thể kết nối được qua cổng này, có thể do tường lửa hoặc các biện pháp bảo mật khác chặn kết nối. Tuy nhiên, cổng 389 (LDAP) đang mở và có thể kết nối được. Ta có thể tiếp tục thực hiện enumeration với cổng 389.
- Ta mở python3 và bắt đầu thực hiện kết nối với một máy chủ LDAP:

```
dducktai@ubuntu:~$ python3
Python 3.8.10 (default, Sep 11 2024, 16:02:53)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>> server = ldap3.Server('192.168.159.15', get_info=ldap3.ALL, port=389)
>>> connection = ldap3.Connection(server)
>>> connection.bind()
True
>>> █
```

- + **ldap3.Server:** Tạo một đối tượng đại diện cho máy chủ LDAP.
- + **'192.168.159.15':** Địa chỉ IP của máy chủ LDAP.
- + **get_info=ldap3.ALL:** Yêu cầu tất cả thông tin về máy chủ, bao gồm các thông tin cấu hình và schema.
- + **port=389:** Sử dụng cổng 389 (mặc định của LDAP).

- + **ldap3.Connection**: Tạo một kết nối đến máy chủ LDAP thông qua đối tượng server.
- + **connection.bind()**: Thực hiện quá trình xác thực (bind) để kết nối với máy chủ LDAP.
- Nếu kết quả trả về là “True” như trên thì kết nối thành công. Sau đó ta có thể tìm nạp thông tin như domain name cách gõ **server.info**

```
>>> server.info
DSA info (from DSE):
Supported LDAP versions: 3
Naming contexts:
dc=domain,dc=local
Supported controls:
1.2.826.0.1.3344810.2.3 - Matched Values - Control - RFC3876
1.2.840.113556.1.4.319 - LDAP Simple Paged Results - Control - RFC2696
1.3.6.1.1.12 - Assertion - Control - RFC4528
1.3.6.1.1.13.1 - LDAP Pre-read - Control - RFC4527
1.3.6.1.1.13.2 - LDAP Post-read - Control - RFC4527
1.3.6.1.1.22 - LDAP Don't Use Copy - Control - RFC6171
1.3.6.1.4.1.4203.1.10.1 - Subentries - Control - RFC3672
2.16.840.1.113730.3.4.18 - Proxy Authorization Control - Control - RFC6171
2.16.840.1.113730.3.4.2 - ManageDsaIT - Control - RFC3296
Supported extensions:
1.3.6.1.1.8 - Cancel Operation - Extension - RFC3909
1.3.6.1.4.1.4203.1.11.1 - Modify Password - Extension - RFC3062
1.3.6.1.4.1.4203.1.11.3 - Who am I - Extension - RFC4532
Supported features:
1.3.6.1.1.14 - Modify-Increment - Feature - RFC4525
1.3.6.1.4.1.4203.1.5.1 - All Op Attrs - Feature - RFC3673
1.3.6.1.4.1.4203.1.5.2 - OC AD Lists - Feature - RFC4529
1.3.6.1.4.1.4203.1.5.3 - True/False filters - Feature - RFC4526
1.3.6.1.4.1.4203.1.5.4 - Language Tag Options - Feature - RFC3866
1.3.6.1.4.1.4203.1.5.5 - Language Range Options - Feature - RFC3866
Supported SASL mechanisms:
DIGEST-MD5, NTLM, CRAM-MD5
Schema entry:
cn=Subschema
Other:
objectClass:
top
OpenLDAPRootDSE
structuralObjectClass:
OpenLDAPRootDSE
configContext:
cn=config
entryDN:
```

- Biết được thông tin domain là **domain.local**. Sau khi có naming context, ta truy xuất tất cả các đối tượng thư mục:

```
>>> connection.search(search_base='dc=domain,dc=local', search_filter='(&(objectClass=person))', search_scope='SUBTREE', attributes=['userPassword'])
True
```

- + **search_base='dc=domain,dc=local'**: Định nghĩa điểm gốc (base DN) để bắt đầu tìm kiếm trong cây thư mục LDAP.
- + **search_filter='(&(objectClass=person))'**: Áp dụng bộ lọc tìm kiếm để chỉ tìm kiếm các đối tượng có thuộc tính objectClass=person.
- + **search_scope='SUBTREE'**: Chỉ định phạm vi tìm kiếm trong toàn bộ cây thư mục, bao gồm cả điểm gốc và các cấp con.
- + **attributes=['userPassword']**: Chỉ yêu cầu truy xuất giá trị của thuộc tính userPassword từ các mục phù hợp với bộ lọc.
- Nếu tìm thấy đối tượng phù hợp, dữ liệu sẽ được lưu trong connection.entries. Nếu không tìm thấy, kết quả trả về là False. Vì kết quả là “True”. Ta tiếp tục mở connection.entries để xem kết quả:

```
>>> connection.entries
[DN: uid=jdoe,ou=users,dc=domain,dc=local - STATUS: Read - READ TIME: 2024-11-19T08:05:21.499446
]
```

- Kết quả trùng khớp với phía Server:

```
ducktai@ubuntu:~$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/systemd/system/slapd.service; Drop-In: /usr/lib/systemd/system/slapd.service.d
          └─slapd-remain-after-exit.conf
   Active: active (running) since Tue 2024-11-19 05:22:06 PST; 2h 45min ago
     Docs: man:systemd-sys-generator(8)
    Tasks: 4 (limit: 4572)
   Memory: 5.0M
    CGroup: /system.slice/slapd.service
            └─8529 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -f /etc/ldap/slapd.d

Nov 19 05:22:06 ubuntu systemd[1]: Starting LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)...
Nov 19 05:22:06 ubuntu slapd[8522]: * Starting OpenLDAP slapd
Nov 19 05:22:06 ubuntu slapd[8528]: @(#) SuperLDAP: slapd (Ubuntu) (Jan 25 2024 18:43:43) $
Nov 19 05:22:06 ubuntu slapd[8529]: slapd starting
Nov 19 05:22:06 ubuntu slapd[8522]: ...done.
Nov 19 05:22:06 ubuntu systemd[1]: Started LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol).
Nov 19 05:48:03 ubuntu slapd[8529]: Entry (uid=jdoe,ou=users,dc=domain,dc=local), attribute 'uid' not allowed
ducktai@ubuntu:~$ ldapsearch -x -b "dc=domain,dc=local" "(objectclass=person)"
# extended LDIF
#
# LDAPv3
# base <dc=domain,dc=local> with scope subtree
# filter: (objectclass=person)
# requesting: ALL
#
# jdoe, users, domain.local
dn: uid=jdoe,ou=users,dc=domain,dc=local
objectclass: inetOrgPerson
uid: jdoe
cn: John Doe
sn: Doe
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
```

Kịch bản 2: LDAP Enumeration bằng NMAP và Python

- sudo su để thực hiện các lệnh tiếp theo bằng quyền root. Tìm nạp thông tin domain của server:

```
root@ubuntu:/home/dducktai# ldapsearch -h 192.168.159.15 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#
#
dn:
namingContexts: dc=domain,dc=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

- + **-h 192.168.159.15**: Kết nối đến máy chủ LDAP tại địa chỉ IP này.
- + **-x**: Sử dụng xác thực đơn giản.
- + **-s base**: Giới hạn tìm kiếm chỉ tại điểm gốc (baseObject).
- + **namingcontexts**: Thuộc tính hiển thị các cơ sở dữ liệu gốc (Base DN) trên máy chủ.
- Sau khi xác định được domain, ta tiếp tục tấn công để hiển thị toàn bộ dữ liệu trong cây LDAP tại "dc=domain,dc=local":

```
root@ubuntu:/home/dducktai# ldapsearch -h 192.168.159.15 -x -b "dc=domain,dc=local"
# extended LDIF
#
# LDAPv3
# base <dc=domain,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# domain.local
dn: dc=domain,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: UIT
dc: domain

# admin, domain.local
dn: cn=admin,dc=domain,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# users, domain.local
dn: ou=users,dc=domain,dc=local
objectClass: organizationalUnit
ou: users

# jdoe, users, domain.local
dn: uid=jdoe,ou=users,dc=domain,dc=local
objectClass: inetOrgPerson
uid: jdoe
cn: John Doe
sn: Doe

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

PHẦN 3. KẾT LUẬN

3.1. Tầm quan trọng của Enumeration

Enumeration là một giai đoạn quan trọng trong kiểm tra bảo mật và đánh giá hệ thống. Thông qua các kỹ thuật này, ta có thể thu thập thông tin chi tiết về hệ thống mục tiêu, bao gồm tài khoản người dùng, cấu hình dịch vụ, tài nguyên chia sẻ, và các lỗ hổng tiềm ẩn. Đây là bước nối tiếp quan trọng từ việc quét ban đầu (scanning) và tạo cơ sở để thực hiện tấn công hoặc đề xuất cải tiến bảo mật. Đây là giai đoạn **active information gathering**, đòi hỏi sự tương tác trực tiếp với hệ thống mục tiêu

3.2. Lợi ích thu được từ Enumeration

Thu thập thông tin chi tiết: Xác định người dùng, nhóm, cấu hình dịch vụ, chia sẻ mạng, và thông tin DNS giúp hiểu rõ cách hệ thống vận hành

Xác định lỗ hổng tiềm năng: Các điểm yếu trong cấu hình (như chia sẻ không bảo mật hoặc dịch vụ công khai) có thể dễ dàng bị khai thác

Hỗ trợ cho giai đoạn tấn công: Cung cấp dữ liệu nền tảng cần thiết để thiết kế và triển khai các chiến lược tấn công cụ thể, như brute-force, privilege escalation, hoặc tấn công ứng dụng

Đề xuất cải tiến: Giúp quản trị viên hệ thống nhận diện các cấu hình không an toàn để thực hiện biện pháp phòng thủ hiệu quả hơn

3.3. Những rủi ro và hạn chế của Enumeration

Bị phát hiện: Nhiều hoạt động enumeration dễ bị giám sát bởi các hệ thống IDS/IPS hoặc nhật ký sự kiện

Tính hợp pháp: Nếu không có sự cho phép rõ ràng, hoạt động enumeration có thể vi phạm quy định pháp luật

3.4. Ứng dụng thực tế

Pentesting: Sử dụng thông tin từ enumeration để thực hiện các giai đoạn sau như tấn công ứng dụng, khai thác lỗ hổng, hoặc kiểm tra quyền truy cập

Cải thiện bảo mật: Nhận diện các dịch vụ không cần thiết hoặc các cấu hình không an toàn và loại bỏ chúng

3.5. Tổng kết

Enumeration cung cấp thông tin quan trọng để hiểu rõ cấu hình và hoạt động của hệ thống, từ đó giúp phát hiện lỗ hổng và cải thiện an ninh mạng. Tuy nhiên, quá trình này đòi hỏi sự cẩn thận để tránh gây ảnh hưởng đến hệ thống mục tiêu và tuân thủ nghiêm ngặt các quy định pháp lý. Đây là một kỹ năng cần thiết không chỉ cho pentesters mà còn cho các quản trị viên hệ thống nhằm đảm bảo tính toàn vẹn và bảo mật của hạ tầng mạng.

----- **HẾT** -----