Lab 4: Network Discovery and Nmap Scanning

In this lab, you will learn how to discover hosts on your network, identify their IP addresses, and use **nmap** to scan for open ports and services. This will help you understand the network topology and identify potential vulnerabilities in the target machine (Metasploitable).

Step 1: Discover Hosts on the Network

1.1 Use arp Command

- The **arp** command displays the ARP (Address Resolution Protocol) table, which maps IP addresses to MAC addresses.

```
arp --help
```

- To view the ARP table:

```
arp -a
```

  - If you only see the router's IP address, you may need to update the ARP table by pinging other devices on the network.

arp -a : Shows the ARP (Address Resolution Protocol) table, which maps IP addresses to MAC addresses. This helps you see devices that your machine has recently communicated with.

If the ARP table is incomplete : You can update it by pinging other devices on the network

1.2 Ping the Metasploitable Machine

- If the ARP table is incomplete, you can ping the Metasploitable machine to populate it:

```
ping <Metasploitable_IP>
```

  - Replace **<Metasploitable_IP>** with the actual IP address of the Metasploitable machine.
  - ping <Metasploitable_IP> : Sends ICMP echo requests to the Metasploitable machine to check if it's reachable. Replace <Metasploitable_IP> with the actual IP address of the Metasploitable machine. This also updates the ARP table with the target machine's IP and MAC address.

1.3 Use netdiscover for Network Discovery

- A better way to discover all hosts on the network is to use **netdiscover**. This tool scans the network and lists all active devices.

```
sudo netdiscover
```

  - You do not need to ping anything manually; **netdiscover** will automatically detect all active hosts on the network.

1.4 Identify Your Router's IP Address

- To check which IP address belongs to your router, use the **netstat** command:

```
netstat -nr
```

  - The "Gateway" column shows the IP address of your router.

Step 2: Start Nmap Scanning

2.1 Basic Nmap Scan

- **nmap** is an essential tool for network scanning. First, check the available options:
- **Note: use sudo su**

```
nmap --help
```

- Perform a basic scan on the Metasploitable machine to discover open ports:

```
nmap <Metasploitable_IP>
```

  - This will show you which ports are open (e.g., port 80 for HTTP, port 22 for SSH).
  - Note: By default, **nmap** scans the top 1,000 most common ports, not all 65,535 ports.

2.2 Check if Port 80 is Open

- If port 80 is open, you can try accessing it via a web browser to see if there is a web server running:

```
firefox http://<Metasploitable_IP>
```

  - Other open ports may be vulnerable to exploitation.

2.3 Scan the Entire Network

- To scan all devices on your local network (e.g., **192.168.1.0/24**), use:

```
nmap 192.168.1.1/24
```

  - This will scan all IPs in the range **192.168.1.1** to **192.168.1.254**.

Step 3: Different Types of Nmap Scans

3.1 TCP SYN Scan (-sS)

- A SYN scan is a stealthy way to check if ports are open without completing the TCP handshake: This is useful for avoiding detection by intrusion detection systems (IDS).

```
nmap -sS <Metasploitable_IP>
```

3.2 TCP Connect Scan (-sT)

- A TCP connect scan completes the full TCP handshake, making it less stealthy but more reliable: This is the default scan type if you don't have root privileges.
- **3.3 UDP Scan (-sU)**

```
nmap -sT <Metasploitable_IP>
```

3.3 UDP Scan (-sU)

Checks for open UDP ports. UDP scans are slower because they rely on timeouts to determine if a port is open.

```
nmap -sU <Metasploitable_IP>
```

Step 4: Advanced Nmap Options

4.1 Operating System Detection (-O)

- To determine the operating system running on the target machine:

```
nmap -O <Metasploitable_IP>
```

  - Example: It might detect that the target is running Windows 7 or Linux.

4.2 Service Version Detection (-sV)

- To check the version of services running on open ports:

```
nmap -sV <Metasploitable_IP>
```

  - You can increase the intensity of version detection using the **--version-intensity** option:

```
nmap -sV --version-intensity 9 <Metasploitable_IP>
```

4.3 Aggressive Scan (-A)

- An aggressive scan combines OS detection, version detection, script scanning, and traceroute:

```
nmap -A <Metasploitable_IP>
```

4.4 Host Discovery (-sn)

- To check which hosts are up on the network without scanning ports:

```
nmap -sn 192.168.1.1-255
```

Step 5: Scanning Specific Ports

5.1 Scan Specific Ports

- To scan specific ports (e.g., port 80 and 22):

  ```
  nmap -p 80,22 <Metasploitable_IP>
  ```

5.2 Scan All Ports

- To scan all 65,535 ports:

  ```
  nmap -p 1-65535 <Metasploitable_IP>
  ```

Step 6: Save Nmap Output to a File

6.1 Redirect Output to a File

- You can save the output of an **nmap** scan to a file for later analysis:

  ```
  nmap -sS <Metasploitable_IP> >> output.txt
  ```

- Check the contents of the file:

```
cat output.txt
```

- Alternatively, list the files in the current directory:

  ```
  ls
  ```

Step 7: Explore Nmap Manual Page

- For more detailed information about **nmap**, you can refer to the manual page:

  ```
  man nmap
  ```