Task 1: Scan Your Local Network for Open Ports

Description:

This project focuses on scanning a local network to discover active devices, open ports, and running services. Using Nmap, a powerful network scanning tool, the project demonstrates how to identify the IP addresses of devices on the network and the services they are running. Optionally, Wireshark is used to capture and analyze network traffic, giving insights into the communication patterns within the network.

The purpose of this project is to understand network behavior, identify potential vulnerabilities, and learn practical cybersecurity techniques in a controlled, educational environment. By documenting discovered devices, open ports, and associated services, the project helps in assessing potential security risks and gaining hands-on experience in network scanning and analysis.

Objectives:

1.Install and configure Nmap to perform network scanning effectively.

2. Identify the local network IP range to target for scanning.

3. Perform TCP SYN scans to discover active hosts and open ports on the network.

4. Document all discovered IP addresses and open ports for analysis.

5. Optionally capture and analyze network traffic using Wireshark to understand packet flow.

6. Research common services running on open ports to gain insight into network behavior.

7. Identify potential security risks associated with open ports and exposed services.

Expected Outcome:

1. A clear list of devices on the local network.
2. Open ports for each device with their associated services.
3. Saved outputs in text format or screenshots.
4. A professional project document combining description, code, and outputs for submission.

Notes:

1. This project is for educational purposes only.
2. Scanning networks without permission is illegal. Always use your own network.

Commands/Code Used:

Ipconfig

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:9027:9566:793b:6f0a:8ec0:708c
   Temporary IPv6 Address. . . . . . : 2401:4900:9027:9566:bc3b:4de1:8852:f29d
   Link-local IPv6 Address . . . . . : fe80::f57:37b8:af89:1f67%12
   IPv4 Address. . . . . . . . . . . : 10.44.226.157
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::60d8:9fff:feb3:5270%12
                                       10.44.226.239

C:\Users\User>
```

Nmap -sn 192.168.43.136

```
C:\Users\User>nmap -sn 192.168.43.136
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 15:41 +0530
Nmap scan report for DESKTOP-OAGIO88 (192.168.43.136)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Nmap -sT 192.168.43.136

The Nmap command nmap -sT performs a TCP Connect Scan on the target host. In this scan, Nmap attempts to establish a full TCP connection with each port on the target machine using the standard three-way handshake (SYN → SYN-ACK → ACK). By doing this, it can determine which ports are open, closed, or filtered. This type of scan is the most basic and reliable method of scanning because it uses normal operating system networking functions, and it does not require administrative privileges. While it is slower than some stealth scans and easier for firewalls or intrusion detection systems to notice, it is ideal for beginners to safely discover active services on a network.

1. MSRPC (Microsoft Remote Procedure Call)

Port: Usually 135/tcp

Purpose: Allows programs on different computers in a network to communicate and request services from each other.

Simple Example: If one computer wants another computer to perform a task, MSRPC handles the communication.

2. NetBIOS-SSN (NetBIOS Session Service)

Port: 139/tcp

Purpose: Used for sharing files, printers, and other resources over a Windows network using the older NetBIOS protocol.

Simple Example: If you access a shared folder on another Windows computer, this service manages the connection.

3. Microsoft-DS (Microsoft Directory Services)

Port: 445/tcp

Purpose: Used for modern Windows file sharing and Active Directory services. It replaced NetBIOS for most file/printer sharing tasks.

Simple Example: Accessing shared folders or printers in a modern Windows network uses this port.

4. WSDAPI (Web Services on Devices API)

Port: 5357/tcp (typically)

Purpose: Allows discovery and communication with network devices like printers, scanners, and cameras using Web Services.

Simple Example: When your PC automatically detects a network printer, WSDAPI is the protocol that helps your computer talk to it.

```
C:\Users\User>nmap -sT 192.168.43.136
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 15:43 +0530
Nmap scan report for DESKTOP-OAGIO88 (192.168.43.136)
Host is up (0.0013s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
```

Nmap -sS 192.168.43.136

The Nmap command nmap -sS performs a TCP SYN scan, also known as a “half-open” scan. In this scan, Nmap sends a SYN packet to the target port and waits for a response. If the port responds with a SYN-ACK, Nmap knows the port is open, but it does not complete the full TCP handshake, immediately sending a RST (reset) to close the connection. If there is no response or a RST is received, the port is considered closed or filtered. This scan is faster and stealthier than a full TCP connect scan (-sT) because it avoids fully opening connections, making it harder

for firewalls or intrusion detection systems to detect. It is widely used for safely discovering open ports on a network.

```
C:\Users\User>nmap -sS 192.168.43.136
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 15:44 +0530
Nmap scan report for DESKTOP-OAGIO88 (192.168.43.136)
Host is up (0.00012s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

23	72.319329	192.168.43.136	4.1.82.186	TCP	54 7669 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
24	72.319425	192.168.43.136	4.1.82.186	TCP	54 7669 → 443 [RST] Seq=2 Win=0 Len=0
25	72.319544	185.201.3.104	192.168.43.136	TCP	58 443 → 8715 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1392
26	72.319627	192.168.43.136	185.201.3.104	TCP	54 8715 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
27	72.320304	185.201.3.104	192.168.43.136	TLSv1.2	85 Encrypted Alert
28	72.320405	192.168.43.136	185.201.3.104	TCP	54 7664 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
29	72.320502	185.201.3.104	192.168.43.136	TCP	54 443 → 7664 [FIN, ACK] Seq=32 Ack=2 Win=63883 Len=0
30	72.320521	192.168.43.136	185.201.3.104	TCP	54 7664 → 443 [RST] Seq=2 Win=0 Len=0

5	13.738323	192.168.43.136	4.1.82.185	TCP	66 8714 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6	13.953088	4.1.82.185	192.168.43.136	TCP	66 443 → 8714 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1392 SACK_PERM WS=128
7	13.953200	192.168.43.136	4.1.82.185	TCP	54 8714 → 443 [ACK] Seq=1 Ack=1 Win=66816 Len=0
8	13.953399	192.168.43.136	4.1.82.185	TCP	54 8714 → 443 [FIN, ACK] Seq=1 Ack=1 Win=66816 Len=0
9	14.157816	4.1.82.185	192.168.43.136	TCP	54 443 → 8714 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
10	14.157869	192.168.43.136	4.1.82.185	TCP	54 8714 → 443 [ACK] Seq=2 Ack=2 Win=66816 Len=0

Wireshark Packet Capture Notes:

Captured TCP SYN packets sent to scanned ports.

Observed handshake attempts for open ports.

Identified common services running (HTTP, SSH, FTP).

Nmap -O 192.168.43.136

The Nmap command nmap -O is used for OS detection on the target host. When this option is used, Nmap analyzes the responses from the target's network stack to try to determine which operating system it is running, such as Windows, Linux, or macOS. Nmap does this by sending specially crafted packets and comparing the responses with a database of known OS fingerprints. This helps in understanding the network environment and identifying potential vulnerabilities related to specific operating systems. OS detection is useful in cybersecurity assessments because it provides more context about the target beyond just open ports and services.

```
C:\Users\User>nmap -O 192.168.43.136
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 15:47 +0530
Nmap scan report for DESKTOP-OAGIO88 (192.168.43.136)
Host is up (0.00051s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

Nmap -A 192.168.43.136

The Nmap command nmap -A enables aggressive scanning, which combines several advanced features to gather detailed information about the target host. This includes OS detection, version detection of services, script scanning, and traceroute. By using -A, Nmap not only identifies which ports are open but also attempts to determine the software running on those ports, the operating system, and additional network information. This scan provides a comprehensive overview of the target, making it very useful for security assessments. However, because it generates more traffic and is more easily detected by firewalls or intrusion detection systems, it should be used carefully and only on networks you have permission to scan.

```
C:\Users\User>nmap -A 192.168.43.136
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 15:49 +0530
Nmap scan report for DESKTOP-OAGIO88 (192.168.43.136)
Host is up (0.0010s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-09-22T10:20:17
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.91 seconds
```

Conclusion / Observations:

1. All active devices and open ports were successfully discovered.
2. Common services identified include SSH (22), HTTP (80), HTTPS (443), FTP (21).
3. Open ports may present potential security risks if not properly secured.
4. This project provides hands-on understanding of network scanning, port discovery, and traffic analysis.