Task 1: Scan Your Local Network for Open Ports

The objective of this task is to understand **basic network reconnaissance** by scanning the local network for open ports. In cybersecurity, open ports can expose running services, which may become potential entry points for attackers. By identifying these ports, we can assess the level of network exposure and take steps to secure them.

For this task, we use **Nmap (Network Mapper)**, a free and open-source tool widely used for network scanning and security auditing. Nmap allows us to discover active devices, detect open ports, and identify services running on those ports. Additionally, **Wireshark** (optional) can be used to capture and analyze the packets generated during the scan, giving a deeper view of the network traffic.

Through this exercise, the aim is to build skills in port scanning, analyzing scan results, and understanding the importance of securing open ports in a network.

Tools Used

1. Nmap (Network Mapper)

- Nmap is a free and open-source tool for network discovery and security auditing.
- It is mainly used to:
  - Scan networks and discover active hosts.
  - Detect open ports and the services running on them.
  - Identify potential security risks from exposed services.
- In this task, Nmap was used to perform a TCP SYN scan across the local IP range to find devices and their open ports.

2. Wireshark (Optional)

- Wireshark is a free and open-source network protocol analyzer.
- It captures and inspects live network packets to show how devices communicate.
- It can be used to:
  - Monitor the traffic generated during Nmap scans.
  - Analyze TCP/UDP packets, handshakes, and responses.
- In this task, Wireshark was optional, but it can complement Nmap by providing deeper insights into the packets exchanged during the scan.

In this task, I am using **Nmap (Network Mapper)** as the primary tool to perform port scanning on my local network. Nmap helps me discover devices, detect open ports, and identify services running on those ports.

Network discovery and port scanning using namp:

1. Checking Nmap Installation and Version

- **Command Run:**

  ```
  nmap --version
  ```

- **Purpose:**
  The nmap --version command checks the currently installed version of Nmap and its associated compiled libraries. This confirms that Nmap is correctly installed and ready for use.
- **Output:**

  ```
  Nmap version 7.98 ( https://nmap.org )
  Platform: i686-pc-windows-windows
  Compiled with: nmap-liblua-5.4.8 openssl-3.0.17 nmap-libssh2-1.11.1 nmap-libz-1.3.1
  nmap-libpcre2-10.45 Npcap-1.83 nmap-libdnet-1.18.0 ipv6
  Compiled without:
  Available nsock engines: iocp poll select
  ```

- **Explanation:**
  This output shows the version (7.98), platform (Windows), the libraries Nmap was compiled with, and available networking engines. Documenting this step is good security practice, ensuring the tool environment matches assignment requirements and enabling reviewers to verify your environment.

2. Local Network IP Configuration

- **Command Run:**

  ```
  ipconfig
  ```

- **Purpose:**
  This command displays the current network configuration of the system, including all network adapters with their IP addresses, subnet masks, and default gateways.
- **Output (Redacted for Security):**

  ```
  Windows IP Configuration

  Wireless LAN adapter Wi-Fi:
    Link-local IPv6 Address . . . . . : fe80::53b7:7503:f6c:2d00%19
    IPv4 Address. . . . . . . . . . . : 192.168.1.xx
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : fe80::1%19
                                        192.168.1.xx
  ```

- **Explanation:**
  The IPv4 address 192.168.1.xx denotes the local IP address assigned to the Wi-Fi network adapter, redacted for security reasons. The subnet mask of 255.255.255.0

indicates the size of the local network, and the default gateway 192.168.1.xx is the local IP address of the router. The other network adapters are not connected and are therefore showing "Media disconnected".

3.Network Scan Results Using Nmap

- **Command Run:**

  nmap -sS 192.168.1.0/24

- **Purpose:**
  To perform a TCP SYN scan across the entire local subnet (192.168.1.0/24) to identify live hosts and discover open TCP ports and associated services.
- **Output**

  Nmap scan report for 192.168.1.x

  Host is up (0.00xxs latency).
  Not shown: 997 filtered tcp ports (no-response)
  PORT STATE SERVICE
  53/tcp open domain
  80/tcp open http
  443/tcp open https
  MAC Address: 20:0C:86:xx:xx:xx (GX India Pvt)

  Nmap scan report for 192.168.1.x
  Host is up (0.00xxs latency).
  Not shown: 996 closed tcp ports (reset)
  PORT STATE SERVICE
  7000/tcp open afs3-fileserver
  8001/tcp open vcom-tunnel
  8002/tcp open teradataordbms
  8080/tcp open http-proxy
  MAC Address: 4C:57:39:xx:xx:xx (Samsung Electronics)

  Nmap scan report for 192.168.1.x
  Host is up (0.00xxs latency).
  All 1000 scanned ports on 192.168.1.x are in ignored states.
  Not shown: 1000 closed tcp ports (reset)
  MAC Address: B4:C4:FC:xx:xx:xx (Xiaomi Communications)

  Nmap scan report for 192.168.1.x
  Host is up (0.00xxs latency).
  All 1000 scanned ports on 192.168.1.x are in ignored states.
  Not shown: 1000 closed tcp ports (reset)
  MAC Address: 62:35:0A:xx:xx:xx (Unknown)

  Nmap scan report for host.docker.internal (192.168.1.x)
  Host is up (0.00xxs latency).
  Not shown: 992 closed tcp ports (reset)

```
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3580/tcp open  nati-svrloc
6646/tcp open  unknown
7070/tcp open  realserver
8080/tcp open  http-proxy
```

- **Explanation:**
  - The scan identified 5 hosts active on the local network with various open ports and associated services.
  - IP addresses and MAC addresses have been partially redacted for security to prevent revealing exact network details that could aid malicious actors.
  - Typical services such as web servers (http, https, http-proxy), database (mysql), and Windows networking (msrpc, netbios-ssn) are identified.
  - Closed and filtered ports indicate unresponsive or protected services.
  - This information helps assess the network exposure and security posture of devices on the subnet.

Nmap scan report for 192.168.1.x

Host is up (0.013s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT   STATE SERVICE

53/tcp open domain

80/tcp open http

443/tcp open https

MAC Address: 20:0C:86:xx:xx:xx (GX India Pvt)

Nmap scan report for 192.168.1.x

Host is up (0.0082s latency).

Not shown: 996 closed tcp ports (reset)

PORT   STATE SERVICE

7000/tcp open afs3-fileserver

8001/tcp open vcom-tunnel

8002/tcp open teradataordbms

8080/tcp open http-proxy

MAC Address: 4C:57:39:xx:xx:xx (Samsung Electronics)

Nmap scan report for 192.168.1.x

Host is up (0.018s latency).

All 1000 scanned ports on 192.168.1.x are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: B4:C4:FC:xx:xx:xx (Xiaomi Communications)

Nmap scan report for 192.168.1.x

Host is up (0.014s latency).

All 1000 scanned ports on 192.168.1.x are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: 62:35:0A:xx:xx:xx (Unknown)

Nmap scan report for host.docker.internal (192.168.1.x)

Host is up (0.0012s latency).

Not shown: 993 closed tcp ports (reset)

PORT   STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3306/tcp open mysql

3580/tcp open nati-svrloc

7070/tcp open realserver

8080/tcp open http-proxy"

This Nmap scan results show the active devices on the local network along with their open TCP ports and related services. Sensitive IP and MAC address details have been redacted to protect network security while preserving the scan's analytical value."

Research on Common Services Running on Open Ports

The Nmap scan revealed several open ports, each typically associated with standard network services widely used in networks:

- **Port 53 (DNS):** Domain Name System responsible for translating domain names into IP addresses.
- **Ports 80 (HTTP) and 443 (HTTPS):** Web services for unencrypted and encrypted web browsing respectively.
- **Port 3306 (MySQL):** Database service commonly used to manage and store data.
- **Ports 135, 139, 445:** Windows networking ports supporting file sharing and remote procedure calls.
- **Ports 7000, 8001, 8080:** Often used by application-specific services such as media servers, proxies, and web interfaces.

These services enable normal network operations but also represent key points of interaction between devices.

Identification of Potential Security Risks from Open Ports

Open ports can represent potential attack vectors if the associated services are not properly secured:

- **Database Port 3306:** Exposes data to unauthorized users if default passwords or weak authentication are used.
- **Windows Networking Ports (135, 139, 445):** Historically targeted by malware and ransomware attacks exploiting vulnerabilities like EternalBlue.
- **Web Ports (80, 443, 8080):** Vulnerable to web-based attacks such as SQL injection, cross-site scripting, or unpatched server exploits.
- **Other Open Ports:** Services on ports 7000 and 8001 could be custom applications that require configuration and monitoring to avoid exposure to attackers.

Mitigation includes closing unnecessary ports, enforcing strong authentication, applying patches, and continuous monitoring.