**Day-1 (22/9/25)**

**Task 1:** Scan Your Local Network for Open Ports

**Objective:** Learn to discover open ports on devices in your local network to understand network exposure.

**Tools & Environment**

 OS**:** Windows 10

 Tool**:** Nmap 7.98

 Network **Range:** 192.168.X.0/24 (private lab network)

 Optional**:** Wireshark for packet analysis

## Process ( step – by – step walkthrough)

## Step 1: Install Nmap

* **What:** Nmap is a network scanner. It “knocks” on device doors (ports) to see what services are listening.
* **Why:** To know which devices and services are reachable in your network.
* **How (Windows):**
  + Download the installer from nmap.org and run it (include “Nmap” and “Npcap” when asked).
  + Open Command Prompt as Administrator to avoid permission issues.

**Step 2: Find your IP range:**

* Open Command Prompt. Run:
  + ipconfig
  + Note your IPv4 address (e.g., 192.168.1.23) and Subnet Mask (e.g., 255.255.255.0).
  + With 255.255.255.0, your range is usually 192.168.1.0/24.

**Step 3: Perform a TCP SYN Scan with Nmap**

* Command : nmap -sS 192.168.X.X/24 -oN scan-results.txt
*  -sS triggers a stealthy SYN scan.
*  -oN saves output in normal text format.
* My Findings :

Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 17:57 +0530

Nmap scan report for 192.168.X.X

Host is up (0.00090s latency).

Not shown: 992 closed tcp ports (reset)

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

1521/tcp open oracle

8080/tcp open http-proxy

Nmap done: 256 IP addresses (1 host up) scanned in 13.00 seconds

**Step 4:** Note down IP addresses and open ports found.

* From my scan:

|  |  |
| --- | --- |
| IP Address | Open Ports & Services |
| 192.168.X.X | 80 (http), 135 (msrpc), 139 (netbios-ssn), 445 (microsoft-ds), 902 (iss-realsecure), 912 (apex-mesh), 1521 (oracle), 8080 (http-proxy) |

**Step 6** : Research common services on those ports

|  |  |  |
| --- | --- | --- |
| **Port** | **Service** | **Typical Use** |
| 80 | HTTP | Websites (unsecured) |
| 135 | MSRPC | Microsoft Remote Procedure Call (Windows services) |
| 139 | NetBIOS-SSN | Windows file/printer sharing (legacy) |
| 445 | Microsoft-DS | SMB file sharing (modern) |
| 902 | ISS RealSecure | VMware/remote management |
| 912 | Apex-Mesh | VMware/remote management |
| 1521 | Oracle DB | Oracle database listener |
| 8080 | HTTP-Proxy | Web service or proxy server |

**Step 7 – Identify potential security risks**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | Port | Risk | Mitigation | | 80 (HTTP) | Unencrypted traffic; data can be intercepted | Use HTTPS or restrict access | | 135 (MSRPC) | Can be abused for Windows exploits | Restrict to trusted hosts, firewall block externally | | 139 (NetBIOS) | Legacy protocol, vulnerable to enumeration | Disable if not needed | | 445 (SMB) | Common ransomware target | Disable if unused, patch regularly, restrict access | | 902/912 (VMware) | Could allow remote control if exposed | Restrict to admin network, strong credentials | | 1521 (Oracle) | Database exposure risk | Restrict to internal use, strong creds, patch | | 8080 (HTTP-Proxy) | May host admin panels or apps | Secure with auth, use HTTPS, restrict access | |