**Project Report: Local Network Reconnaissance using Nmap**

**📌 Objective**

To discover open ports on devices within the local network using Nmap and optionally analyze traffic with Wireshark. This helps in understanding network exposure and identifying potential security risks.

**🧰 Tools Used**

* **Nmap** – for network scanning and port discovery
* **Wireshark** – for packet capture and traffic analysis (optional)

**🧠 Key Concepts**

* **Port Scanning**
* **TCP SYN Scan**
* **IP Ranges and Subnets**
* **Network Reconnaissance**
* **Open Ports and Common Services**
* **Network Security Basics**

**📝 Methodology**

**1. Installation**

Installed Nmap and Wireshark from official sources.

**2. Identifying the IP Range**

Used ipconfig (Windows) / ip a (Linux) to find:

* IPv4 Address: 192.168.29.21
* Subnet: 255.255.255.0

=> Network Range: 192.168.1.0/24

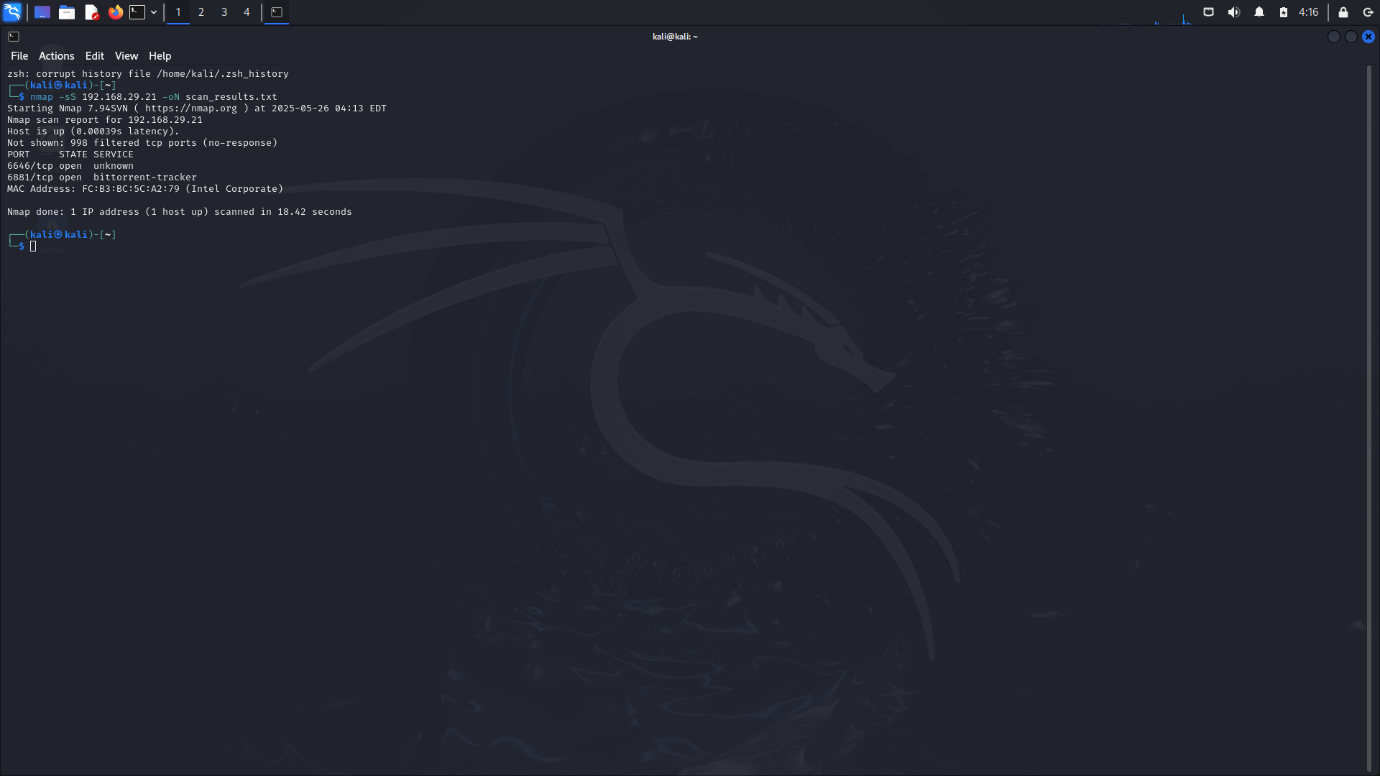
**3. Scanning the Network**

Executed the following command to perform a TCP SYN scan:

nmap -sS 192.168.29.21

This scanned all devices on the local subnet and listed open TCP ports.

**4. Analyzing Scan Results**

****

|  |  |  |
| --- | --- | --- |
| **Port** | **State** | **Service** |
| **6881** | **Open** | **BitTorrent Tracker** |

**🔍 Findings & Analysis**

* **Common Services Detected:**
  + **Port 6881 (BITTORRENT TRACKER):** Tracker or peer exchange traffic
* **Potential Security Risks:**
  + Port **6881 TCP** is most famously used by **BitTorrent** and similar peer-to-peer (P2P) file-sharing applications. While the port itself isn't inherently dangerous, **leaving it open** or **exposed to the internet** can introduce several **security risks**.

**✅ Outcome**

* Gained practical experience in using Nmap for reconnaissance.
* Learned to interpret scan results and relate open ports to real-world services.
* Understood how attackers might probe networks to identify vulnerabilities.
* Explored packet-level traffic using Wireshark.

**🛡️ Recommendations**

* Disable unused services and ports on local devices.
* Use firewalls to block unnecessary inbound connections.
* Keep firmware and OS updated to patch known vulnerabilities.
* Replace insecure protocols (e.g., Telnet) with secure alternatives (e.g., SSH).

**📚 References**

* https://nmap.org/book/
* https://www.wireshark.org/docs/
* https://www.speedguide.net/ports.php

| **Observation** | **Description:** |
| --- | --- |
| Target Port | TCP 6881 |
| Source IP | 192.168.1.10 |
| Protocol | BitTorrent |
| TCP Flags | SYN, ACK observed |
| Notes | Peer-to-peer communication detected, indicating BitTorrent client activity. |