Network Scanning Report: Task 1 – Scan Your Local Network for Open Ports

Task: Task 1 – Network Reconnaissance with Nmap

Objective

The objective of this task was to discover open ports on devices within my local network using Nmap. This helped me understand basic network reconnaissance and how open ports can indicate exposed or vulnerable services on the network.

Tools Used

- Nmap (Network Mapper)
- Wireshark (optional, not used in this task)

Steps Performed

1. Installed Nmap from the official website.
2. Identified my local IP range using ipconfig (on Windows) and found it to be 192.168.1.0/24.
3. Performed a TCP SYN scan using the command:

   nmap -sS 192.168.1.0/24

4. Noted the IP addresses of active devices and listed their open ports.
5. Looked up the services running on these open ports (e.g., HTTP, SSH, Telnet).
6. Evaluated the risks based on the services found, such as Telnet and FTP.
7. Saved the scan results to a text file using:

   nmap -sS 192.168.1.0/24 -oN open_ports.txt

Findings

IP Address	Open Ports	Notes
192.168.1.1	80, 443	Router web interface (normal)

IP Address	Open Ports	Notes
192.168.1.5	22, 23	SSH is okay, Telnet is insecure
192.168.1.10	21, 139, 445	FTP and SMB present, possible risks

I noticed that some devices had ports open that could be dangerous, such as Telnet (port 23) and FTP (port 21). These services are known for lacking encryption and can be exploited by attackers if not secured.

Security Recommendations

- Disable or replace insecure services like Telnet and anonymous FTP.
- Use a firewall to restrict unnecessary incoming and outgoing connections.
- Keep all systems updated with the latest patches.
- Regularly monitor network traffic and perform periodic scans.