Task 1

Scanned Local Network for Open Ports

Name: Ananya N
Date: 20/10/2025
Environment: **Kali Linux**

Tools used:

1)Nmap:

Nmap is a tool used to scan networks. It shows which devices are online and which ports are open. It also tells what services are running on those ports. Nmap helps to find weaknesses in a network.

2)Wireshark:

Wireshark is a tool used to capture network traffic. It shows all the data moving on the network. You can see which devices are talking and what information is sent. Wireshark helps to check scans and understand network activity**.**

Commands I ran during scanning using Nmap

I ran these commands from Kali terminal during the task.

1)TCP SYN scan (subnet)

Command
sudo nmap -sS <ip address>

this is a TCP SYN (half-open) scan of the subnet. I used it because it is fast and effective for finding open TCP ports on many hosts while leaving less trace than a full connect scan.

2) Full TCP port scan on a host (all ports, faster)

Command
sudo nmap -sS -p- -T4 <ip address>

this scans all 65,535 TCP ports on a single host with faster timing. I used it to find services on non-standard ports when a host looked interesting, but I used -T4 cautiously since it is noisier and may trigger security devices.

3) UDP top 50 ports (network scan)

Command
sudo nmap -sU --top-ports 50 <ip address>

this is a UDP scan that checks the 50 most common UDP ports across the whole subnet. I used it to quickly find common UDP services (like DNS or SNMP) that TCP scans can miss.

Wireshark: how I captured and verified packets

1. Started Wireshark capture on my active network interface before running the Nmap scans.
2. Ran the Nmap scans while Wireshark was capturing.
3. Used these display filters to check scan packets in real time:

SYN packets (scan probes): tcp.flags.syn==1 && tcp.flags.ack==0
SYN-ACK packets (open port replies): tcp.flags.syn==1 && tcp.flags.ack==1
Closed port (RST): tcp.flags.rst==1
ARP (to map MAC addresses): arp

OUTPUT:

I learned to use Nmap to perform TCP SYN scans, full port scans, and UDP top-port scans to discover hosts and services on my local network. I learned to capture and inspect network traffic in Wireshark to confirm scan results. I also learned to identify common services and understand potential risks from open ports.