TASK 01: LOCAL NETWORK PORT SCANNING

Objective: To discover open ports on devices within the local network using Nmap and analyze the network traffic using Wireshark to understand exposure risks in a basic internal environment.

Tools Used

Nmap – Network scanner to detect hosts and open ports

Wireshark – Packet analyzer for traffic inspection

OS: Kali Linux

Steps Performed

1. Checked Local IP Address

Command used:

“ifconfig”
IP address found: 10.0.2.15

This IP is within the 10.0.2.0/24 subnet, which means there may be up to 254 hosts.

2. Performed Nmap TCP SYN Scan

Command used:

“nmap -sS 10.0.2.0/24 -oN scan.txt”
This command performed a stealth scan (TCP SYN scan) on all devices in the 10.0.2.0/24 subnet.

Results were saved to scan.txt.

3. Devices Found

Nmap discovered 4 active hosts:

10.0.2.2

10.0.2.3

10.0.2.4

10.0.2.15

📊 Open Ports Discovered

IP Address, Open Ports, Services, MAC Address

10.0.2.2, 135, 445, 8090, msrpc, microsoft-ds, opsmessaging, 52:54:00:12:35:02

10.0.2.3, 135, 445, 8090, Same as above, 52:54:00:12:35:03

10.0.2.4, 135, 445, 8090, Same as above, 52:54:00:12:35:04

10.0.2.15, None, All ports closed, —

Wireshark Analysis

Started Wireshark before Nmap scan to capture packets.

Applied filter: tcp

Observed:

SYN packets being sent from 10.0.2.15 to other hosts.

SYN-ACK responses from IPs like 10.0.2.2 (indicates open port).

Reset (RST) packets where ports were closed.

This confirmed the scan behavior and service responses.

⚠ Potential Risks Identified

Port, Risk Description

135, Used by Microsoft RPC. Vulnerable to remote code execution if not patched.

445, SMB port. Historically targeted by ransomware like WannaCry (EternalBlue exploit).

8090, Likely running a web or messaging service. If unpatched or weakly configured, could be exploited.