# TASK 1: LOCAL NETWORK PORT SCANNING & SECURITY ANALYSIS

## Objective

The objective of this task is to analyze the local network environment by identifying active devices and detecting open TCP ports. This helps in understanding network exposure, running services, and potential security vulnerabilities.

## Tools Used

- Kali Linux
- Nmap (Network Mapper)

## Network Environment

- System IP Address: 10.141.123.92
- Network Range: 10.141.123.0/24
- Scan Method: TCP SYN Scan
- Total Active Hosts Identified: 3

## Scanning Methodology

A TCP SYN scan was performed using Nmap to identify open ports across the local network. This scanning technique is efficient and minimally intrusive, sending SYN packets to determine port states without establishing full connections.

## Nmap Command Executed

```
sudo nmap -sS -O 10.141.123.0/24 -oN detailed_scan.txt
```

## Scan Results Summary

| Target IP | Open Port | Service | Risk Level |
|---|---|---|---|
| 10.141.123.244 | 3306/TCP | MySQL Database | High |
| 10.141.123.244 | 7070/TCP | RealServer / Web Service | Medium |

## Security Risk Analysis

Port 3306 (MySQL): An open database service increases the risk of unauthorized access, data breaches, and credential attacks if weak authentication is used.

Port 7070: Often associated with web or administrative services. Exposure without proper security controls may lead to information disclosure or exploitation.

## Firewall & Security Considerations

Firewalls play a critical role in restricting unauthorized access by filtering incoming and outgoing traffic. Only essential services should be exposed, and unused ports must be closed to reduce attack surface.

## Use of Wireshark

Wireshark was optional for this task. Since Nmap provided sufficient information to identify services and port states, packet capture analysis was not required for successful task completion.

## Conclusion

This task successfully demonstrated local network reconnaissance using Nmap. The identification of open ports highlights the importance of proper network hardening and regular security assessments to prevent potential threats.