

CYBER SECURITY INTERNSHIP

Day 1

Date : 23/06/2025

Task 1: Scan Your Local Network for Open Ports:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:00:01:dd brd ff:ff:ff:ff:ff:ff  
    inet 192.168.170.128/24 brd 192.168.170.255 scope global dynamic noprefixroute eth0  
        valid_lft 1541sec preferred_lft 1541sec  
    inet6 fe80::abac:de16:c044:7aa8/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(kali@kali)-[~]  
$
```

```
(kali@kali)-[~]  
$ nmap -sS 192.168.170.128/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 11:17 EDT  
Nmap scan report for 192.168.170.1  
Host is up (0.00080s latency).  
Not shown: 995 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3306/tcp  open  mysql  
MAC Address: 00:50:56:C0:00:08 (VMware)  
  
Nmap scan report for 192.168.170.2  
Host is up (0.00044s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp    filtered domain  
MAC Address: 00:50:56:F4:9A:70 (VMware)  
  
Nmap scan report for 192.168.170.254  
Host is up (0.00052s latency).  
All 1000 scanned ports on 192.168.170.254 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 00:50:56:FC:BD:3B (VMware)  
  
Nmap scan report for 192.168.170.128  
Host is up (0.000018s latency).  
All 1000 scanned ports on 192.168.170.128 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.60 seconds
```

OPEN PORTS (80,135,139,445,3306):

This task was a valuable hands-on experience that helped me understand how network scanning works in real-world environments. By using Nmap, I was able to identify active devices in my local network and examine which ports were open, what services were running on those ports, and what risks those services might pose.

My Opinion that includes **details about the open ports (80, 135, 139, 445, 3306)** you discovered during the scan — making it more personal and relevant to your task:

Port 80 (HTTP):

This port is used to show websites. In my scan, it showed that a website is running. But the problem is — it is using **HTTP without encryption**, which means if someone logs in or sends data, **a hacker can see that information easily**. This is not safe. It is better to use **HTTPS (secure version)** instead.

Port 135 (MSRPC):

This port is used by Windows to allow programs to talk to each other remotely. But it is **often targeted by attackers** to run harmful code from far away (called remote code execution). So, **keeping this port open is risky**, especially if the computer is connected to the internet.

Port 139 (NetBIOS) and Port 445 (SMB):

These ports are used for **file sharing in Windows**. If they are open, an attacker can find out **what folders are shared, usernames**, or even access files without permission. Port 445 is very dangerous — it was used in a real attack called **WannaCry ransomware**. These ports should be closed unless we really need file sharing in a private network.

Port 3306 (MySQL):

This port is used by the **MySQL database**. It helps websites or apps store and use data. If this port is open to the internet, someone could try to **guess the password** or **steal the data** using attacks like **SQL injection**. It is better to keep this port open only inside the system (not public) and use a strong password.