

Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools Used : Nmap , ChatGPT (research purpose), VMware

Scan Results :

```
(sangini@kali)~$ ip addr show
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:c4:cd:68 brd ff:ff:ff:ff:ff:ff
   inet 192.168.87.128/24 brd 192.168.87.255 scope global dynamic noprefixroute eth0
       valid_lft 1690sec preferred_lft 1690sec
   inet6 fe80::20c:29ff:fc06:64 scope link noprefixroute
       valid_lft forever preferred_lft forever
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
   link/none
   inet 10.10.10.23 scope global tun0
       valid_lft forever preferred_lft forever
   inet6 dead:beef:4::1000/64 scope global
       valid_lft forever preferred_lft forever
   inet6 fe80::3900:f06:1e0:d57e/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever

(sangini@kali)~$ 
(sangini@kali)~$ 
(sangini@kali)~$ 
$ nmap -sS 192.168.87.128/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 04:57 EST
Nmap scan report for 192.168.87.1
Host is up (0.00044s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.87.254
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.87.254 are in ignored states.
```

IP address found : [192.168.87.128/24](#)

Open port after scanning through Nmap : [3306/tcp](#)

Common service for open port : [MySQL](#)

Identified potential risk for open port :

1. Unauthorized Access to the Database

If MySQL is exposed without proper access controls:

- Attackers can attempt **brute-force attacks** on MySQL credentials.
- Weak usernames/passwords (e.g., root/root) can give full DB access.
- If a default user exists with no password → complete compromise.

2. SQL Injection (Remote Exploitation)

If MySQL accepts external connections:

- If any application queries this DB improperly, attackers can inject malicious SQL remotely.
- Privilege escalation inside the DB server.

3. Remote Code Execution (RCE) Vulnerabilities

Historically, MySQL and MariaDB have had vulnerabilities allowing:

- Remote code execution (via UDFs)
- Privilege escalation
- Remote takeover of the database server

So, attackers can:

- Upload malicious libraries
- Execute OS-level commands

- Gain root access to the machine running MySQL

6. Buffer Overflow / Zero-day Exploits

Attackers can scan for MySQL version → check for public CVEs.

Known critical vulnerabilities include:

- CVE-2021 variants
- CVE-2020 MySQL privilege escalation
- CVE-2016 MySQL auth bypass
- Older CVEs allowing remote manipulation

7. Lateral Movement in the Network

Once an attacker gains DB access, they may:

- Steal credentials stored in the DB
- Use compromised accounts to pivot
- Move deeper into the network
- Reach application servers, web servers, or internal services