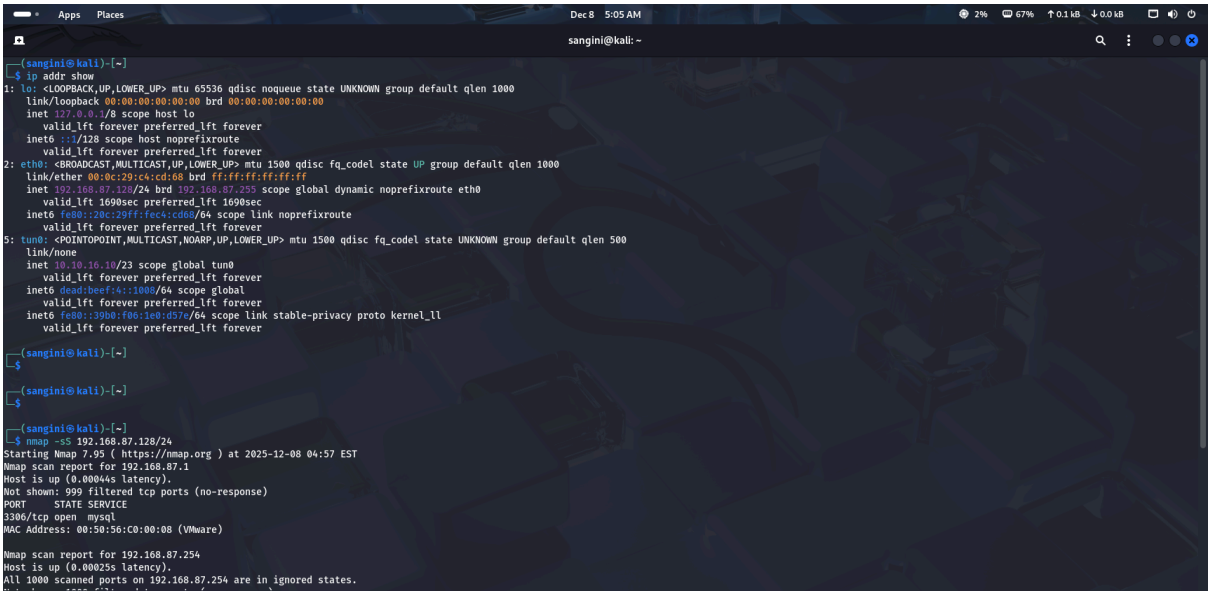
Task 1: Scan Your Local Network for Open Ports

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 :



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