VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

MySQL attack using Metasploit

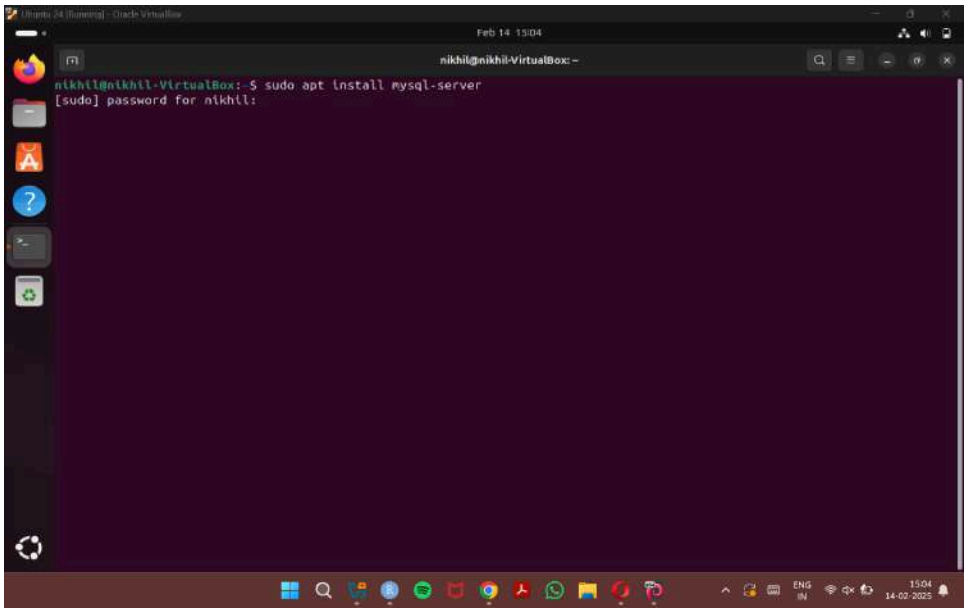
NAME: DHEVATHA S P
REG NO.: 22BCE0826

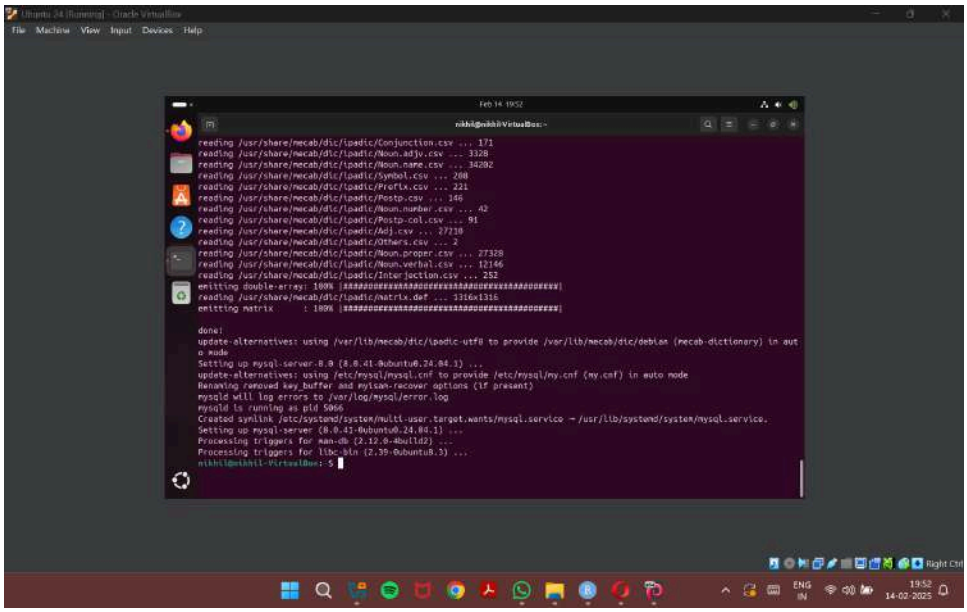
NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

Dhevatha S P
22BCE0826

Ubuntu - Setting the MySQL environment

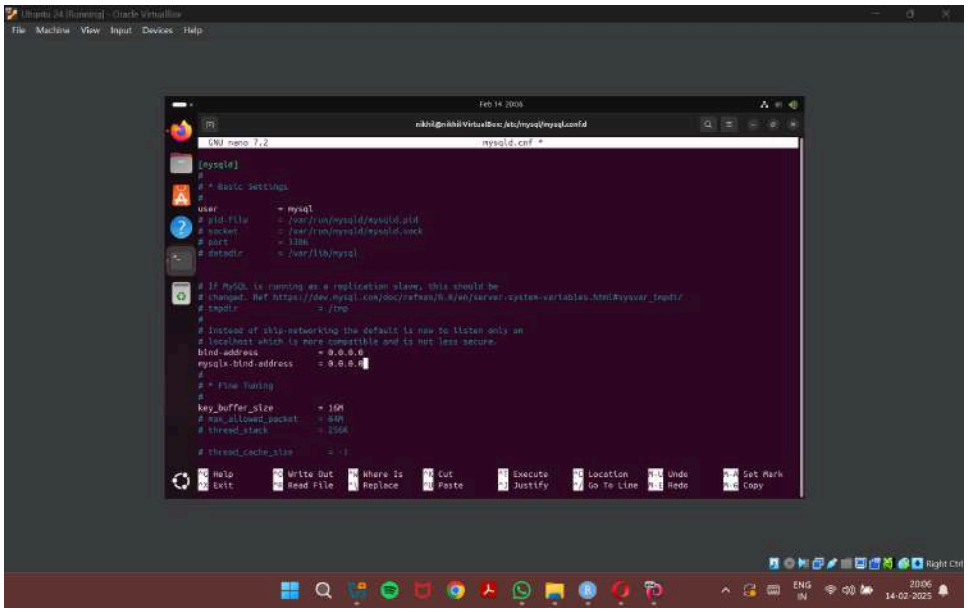
1. Installing MySQL in Ubuntu



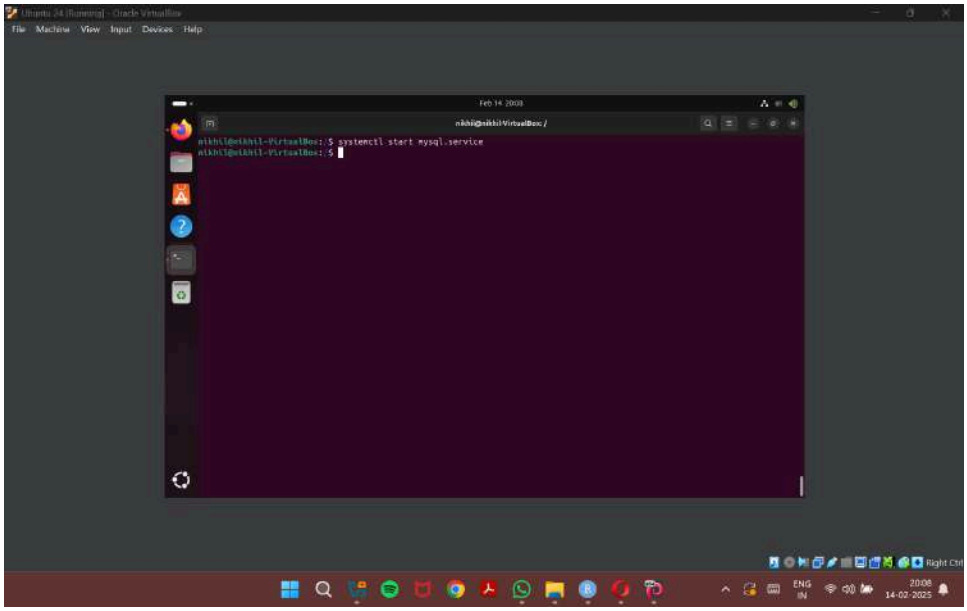


Dhevatha S P
22BCE0826

2. Locating mysqld.cnf in /etc/mysql/mysql.conf.d and change accordingly.

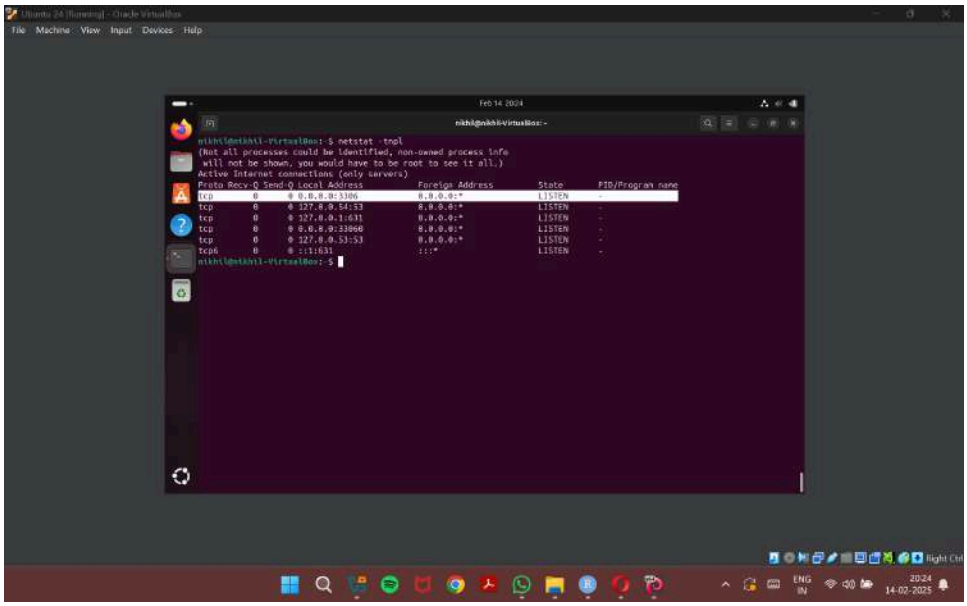


3. Starting MySQL server

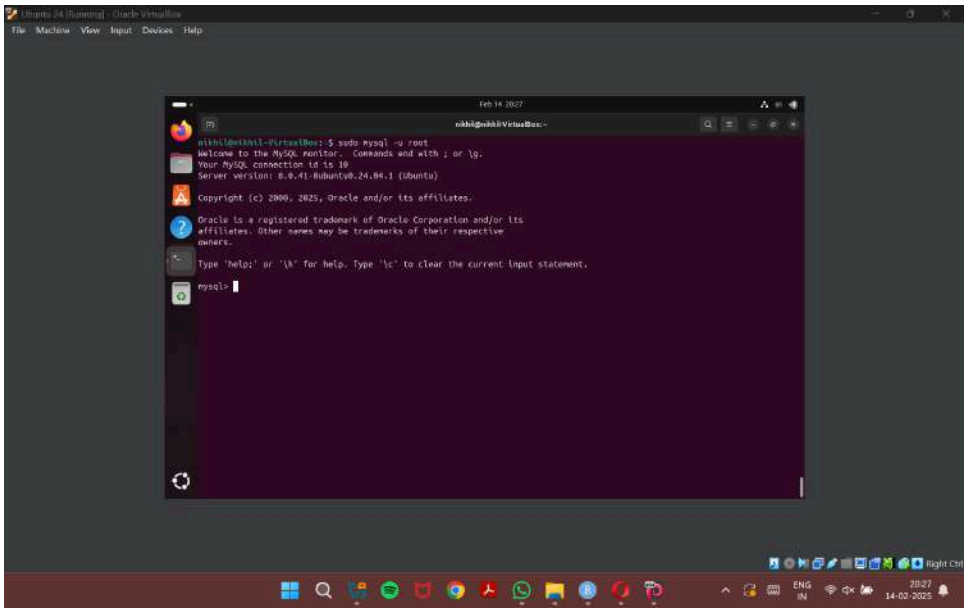


Dhevatha S P
22BCE0826

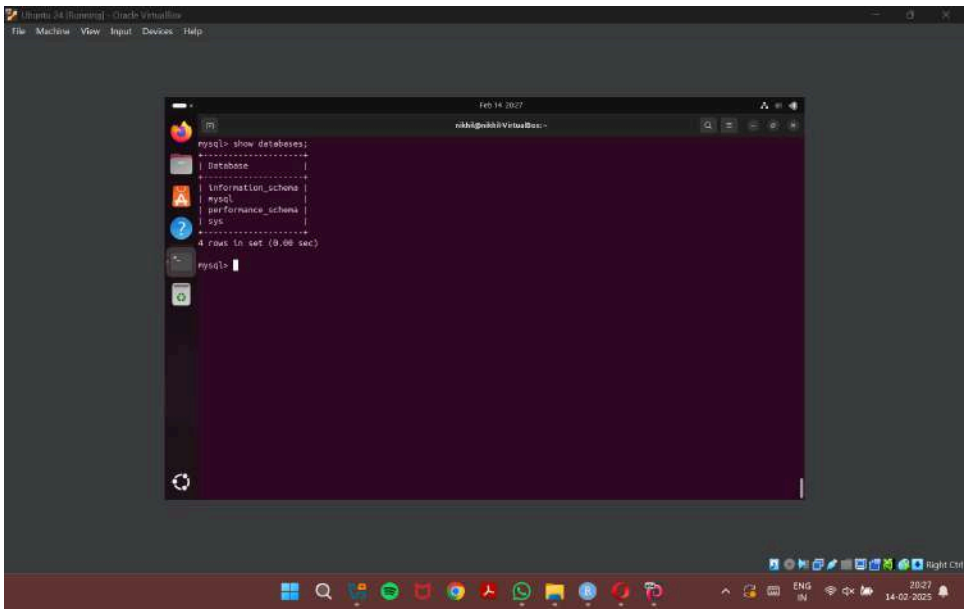
4. Checking the network status



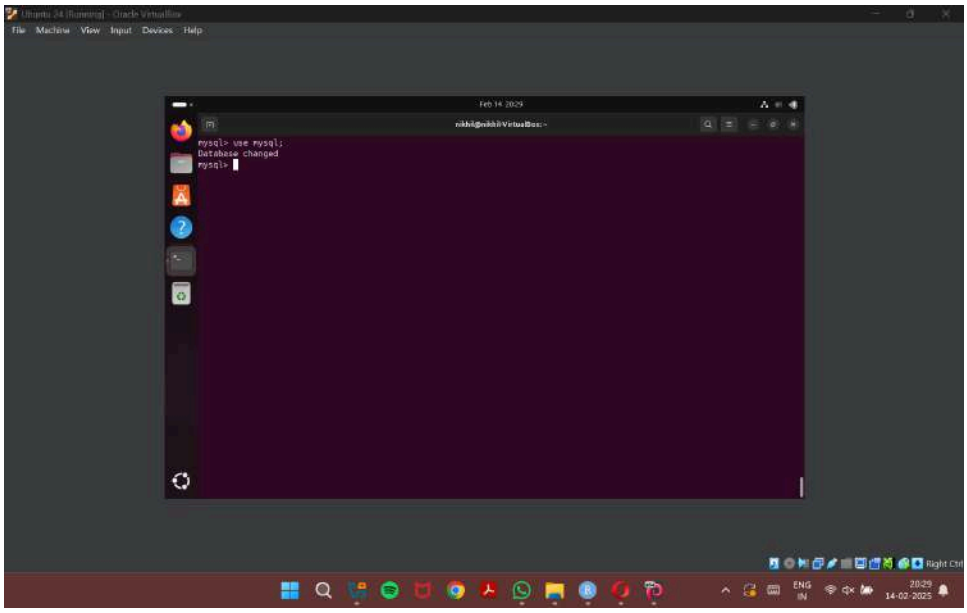
5. Logging into the MySQL database



6. Checking databases in MySQL in Ubuntu

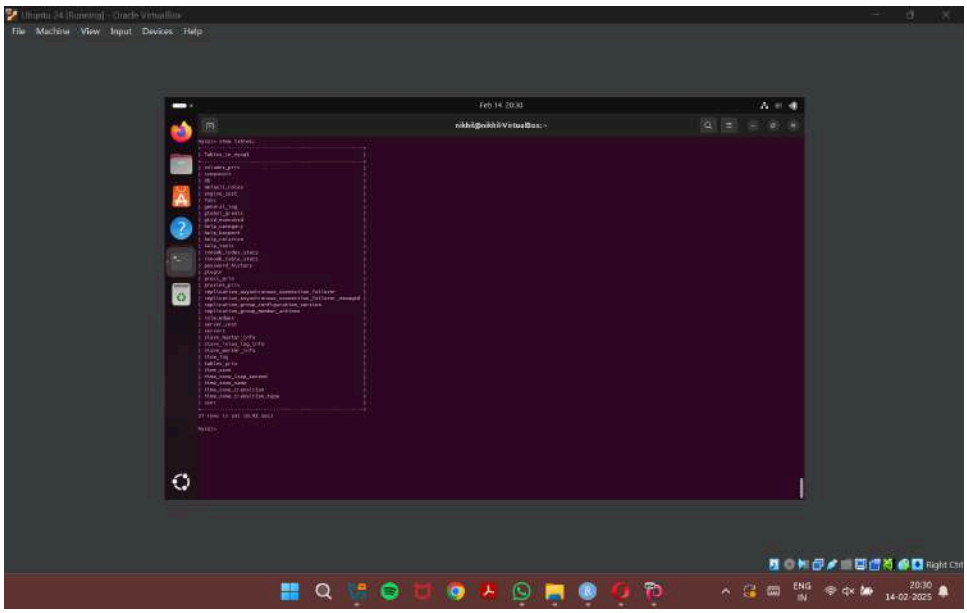


7. Using the mysql database

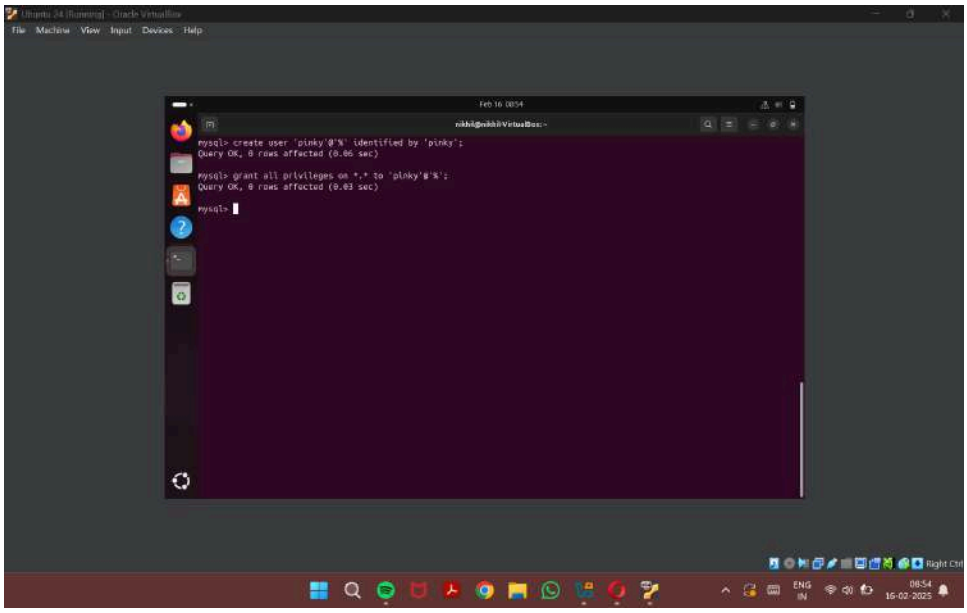


Dhevatha S P
22BCE0826

8. Checking the tables in the mysql database



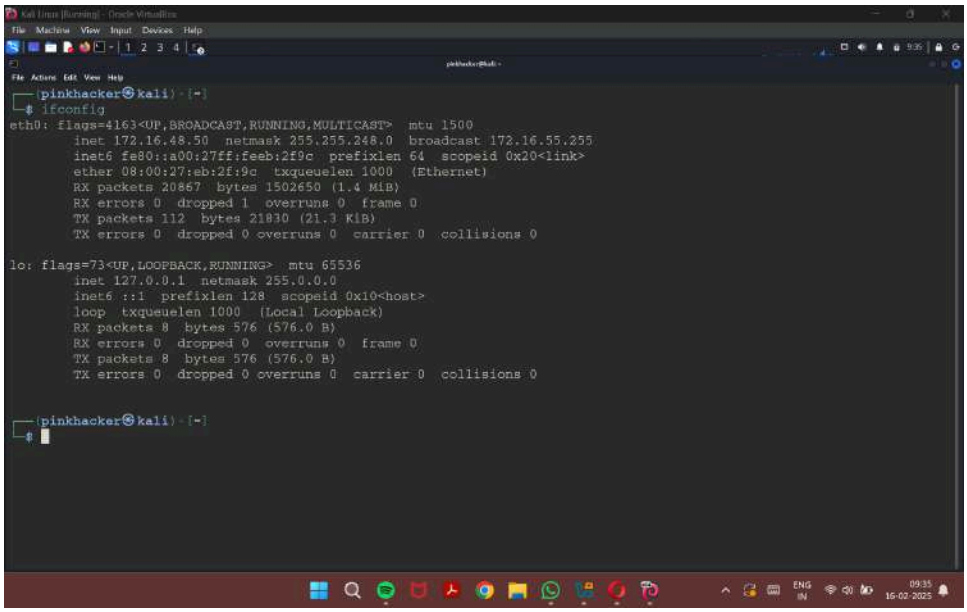
9. Creating a new user (pinky) and granting all privileges to this user

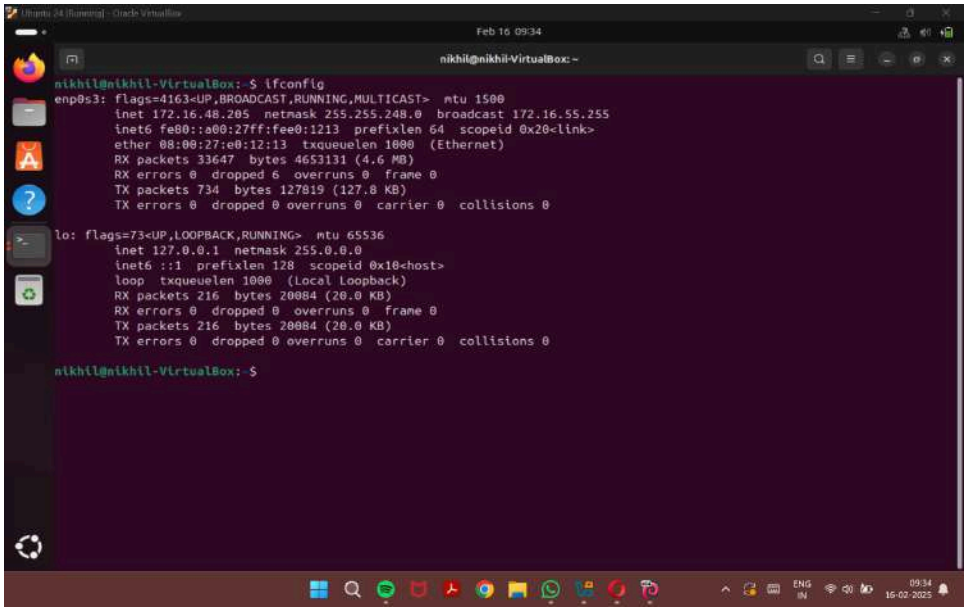


Dhevatha S P
22BCE0826

Exploitation using Kali Linux

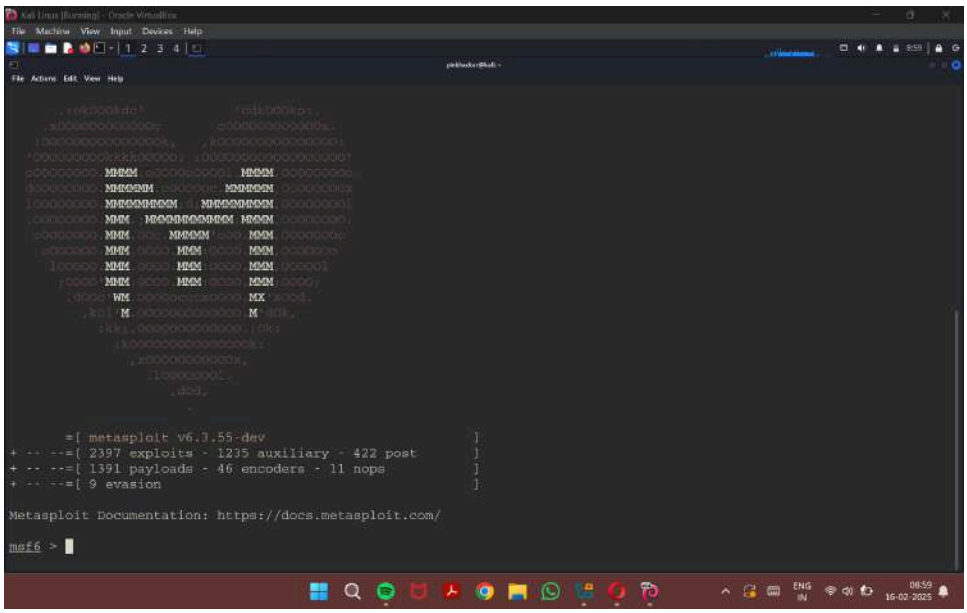
1. IP addresses of Kali Linux and Ubuntu





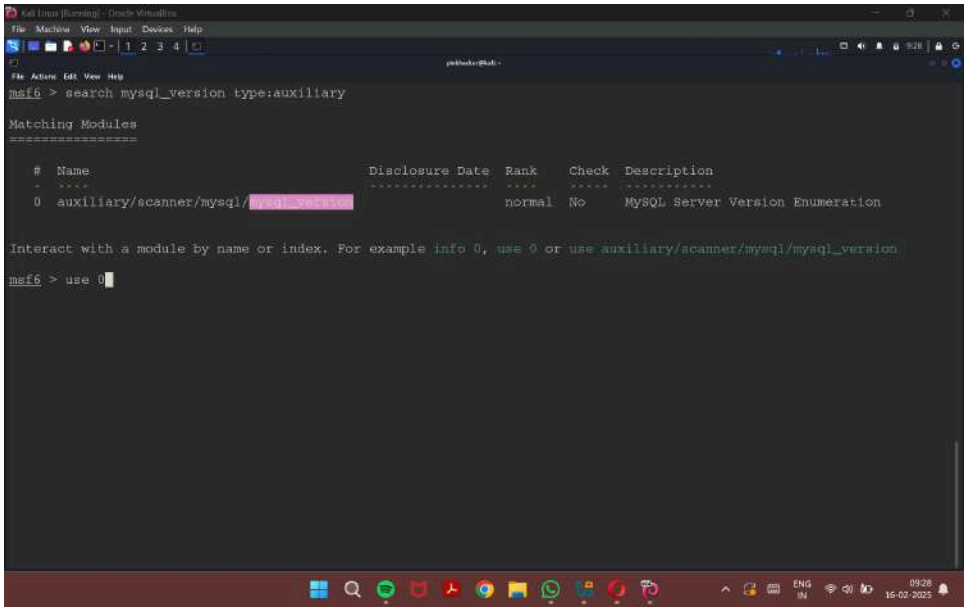
Dhevatha S P
22BCE0826

2. Starting MSFConsole in Kali Linux



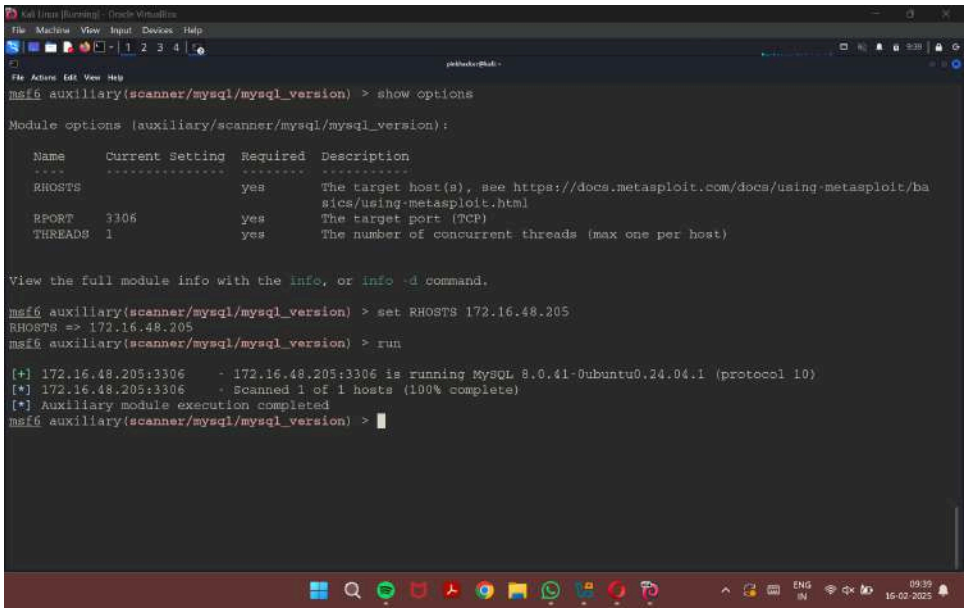
MySQL Version

3. Searching for mysql_version under type auxiliary and use the tool



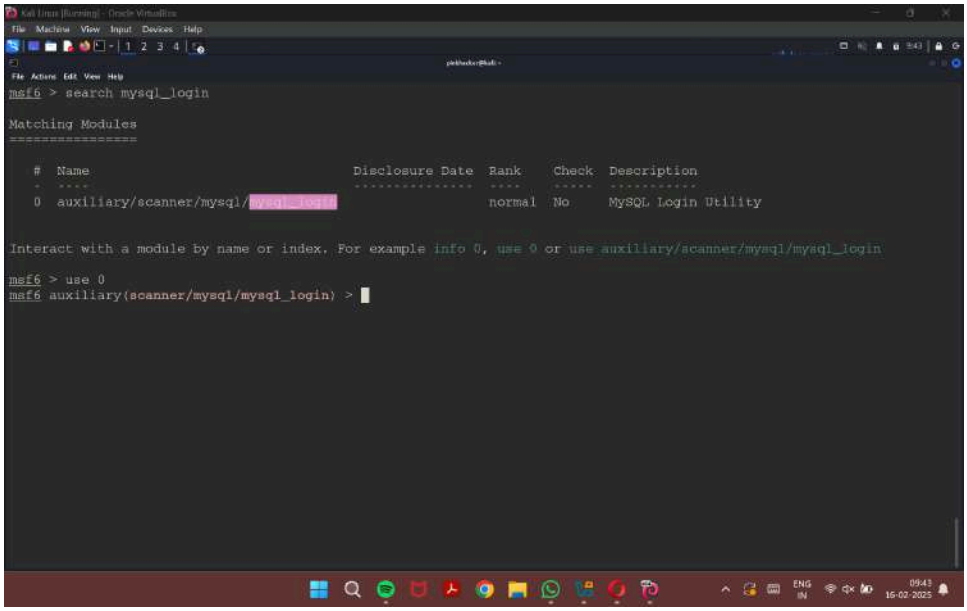
Dhevatha S P
22BCE0826

4. Setting the RHOST to the IP address of the Ubuntu and run the exploit

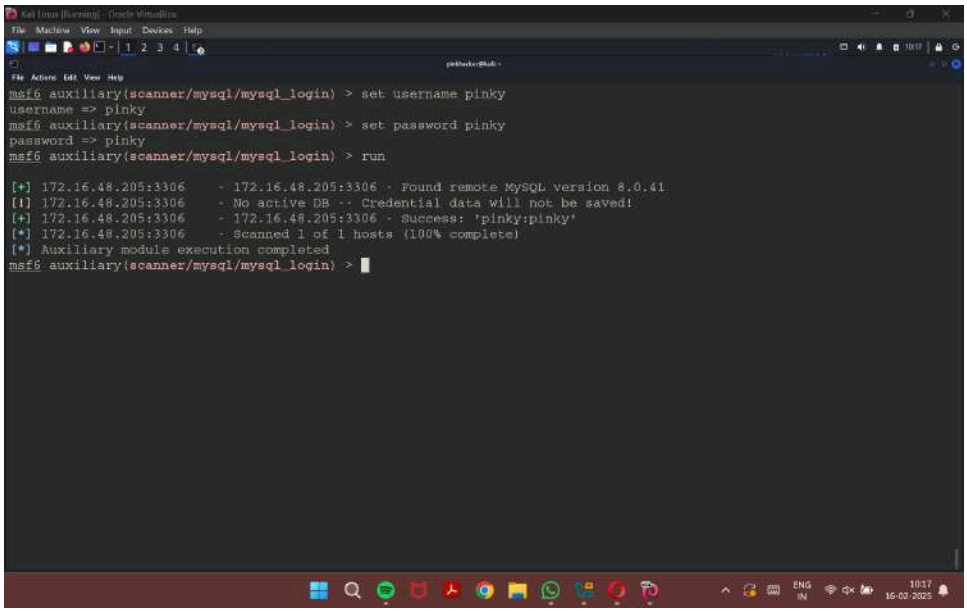


MySQL Login

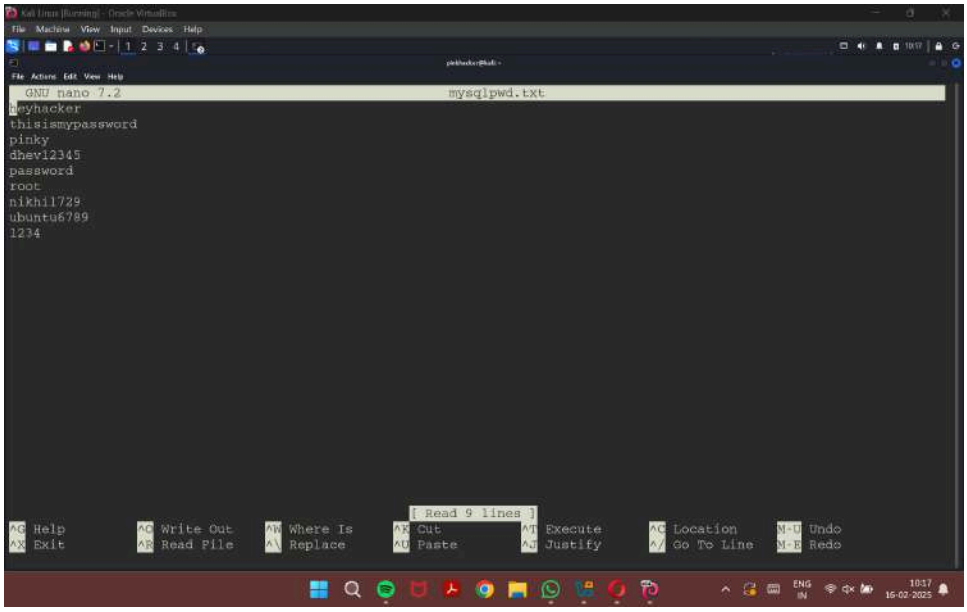
5. Search for mysql_login and use it



6. Setting the RHOSTS to IP address of the Ubuntu and username to ‘pinky’ and password to ‘pinky’ and run it

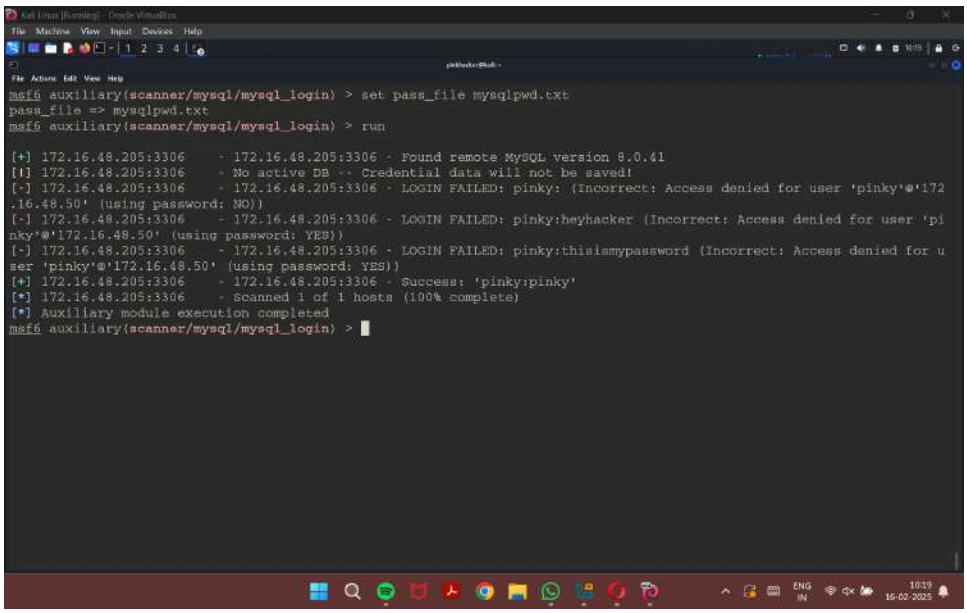


7. Create mysqlpwd.txt



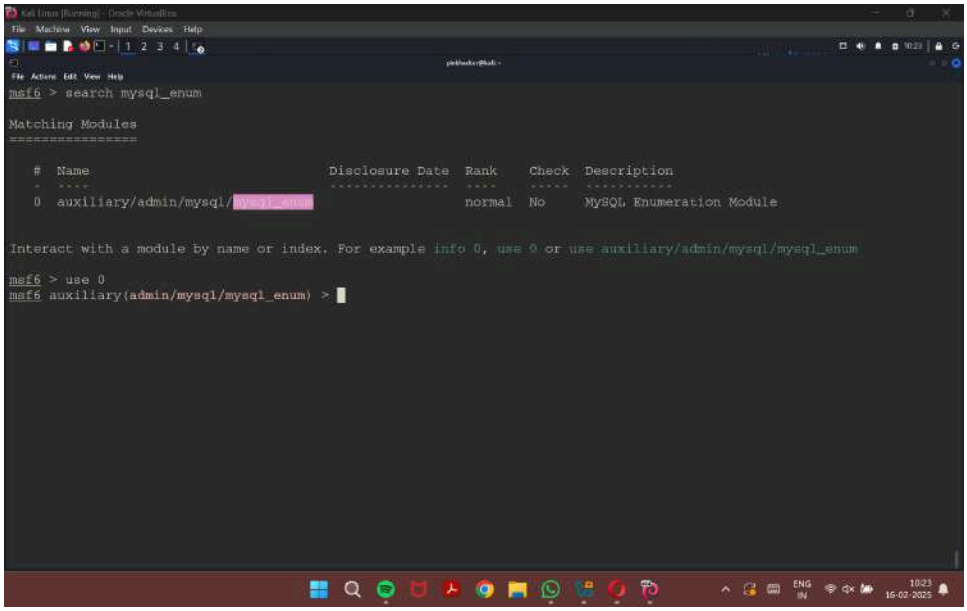
Dhevatha S P
22BCE0826

8. Set pass_file as mysqlpwd.txt and run it

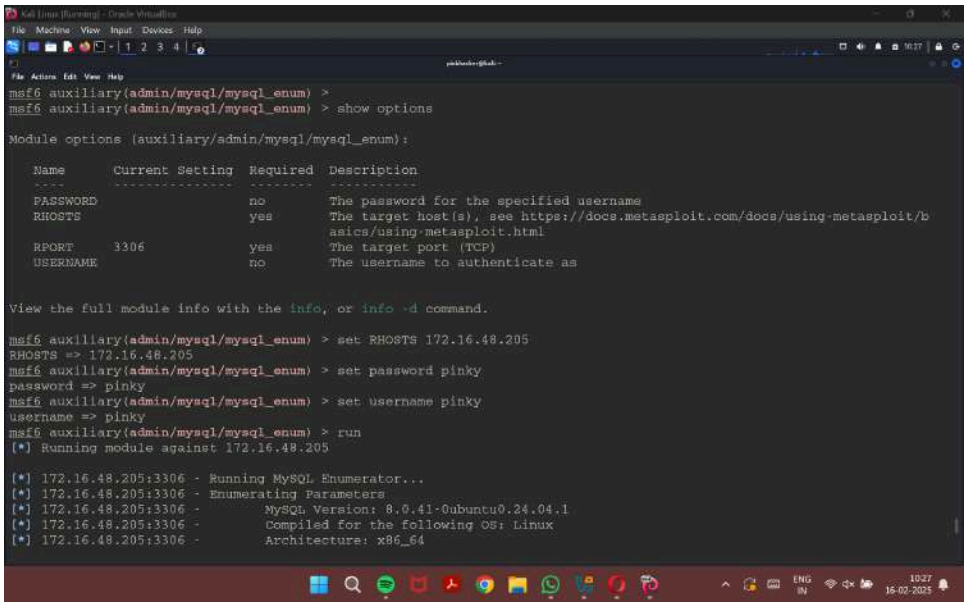


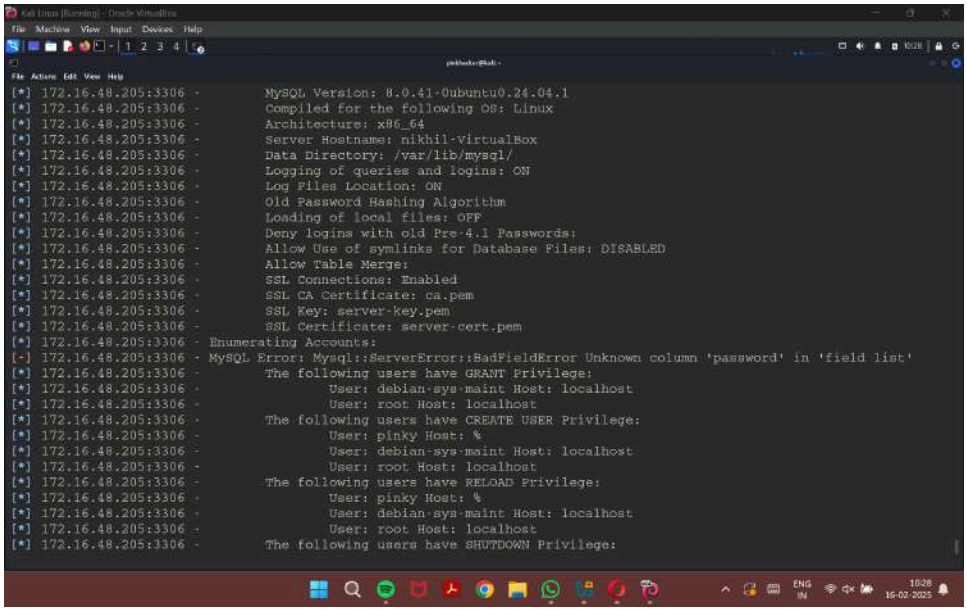
MySQL Enumerate

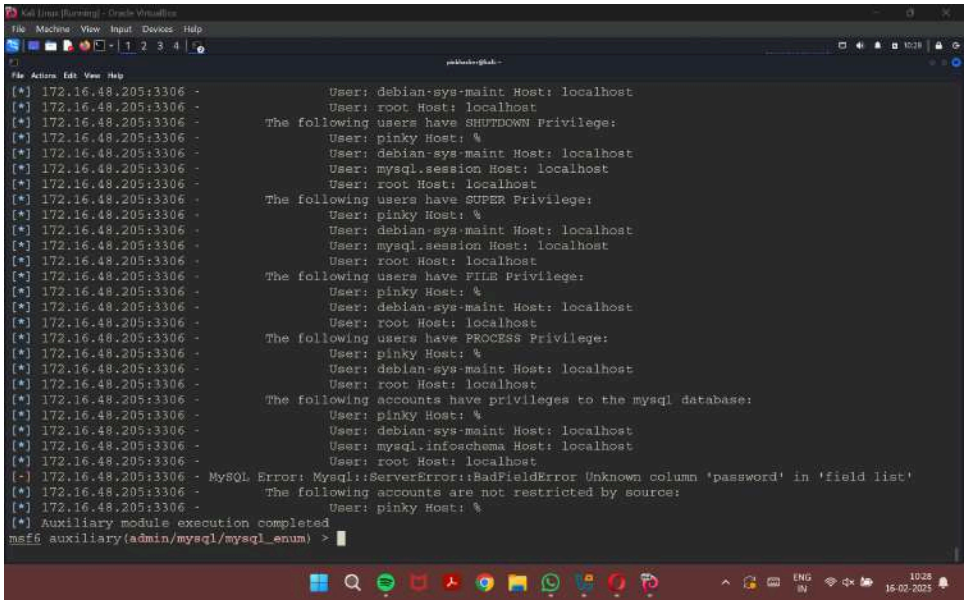
9. Search for mysql_enum and use it



10. Set the RHOSTS to the IP address of Ubuntu and username to ‘pinky’ and password to ‘pinky’ and run it.

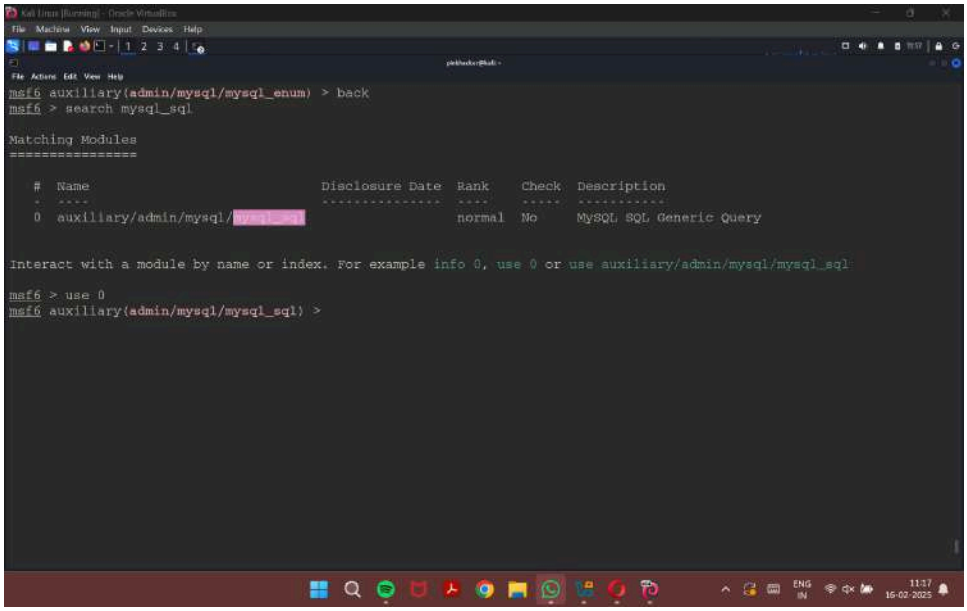




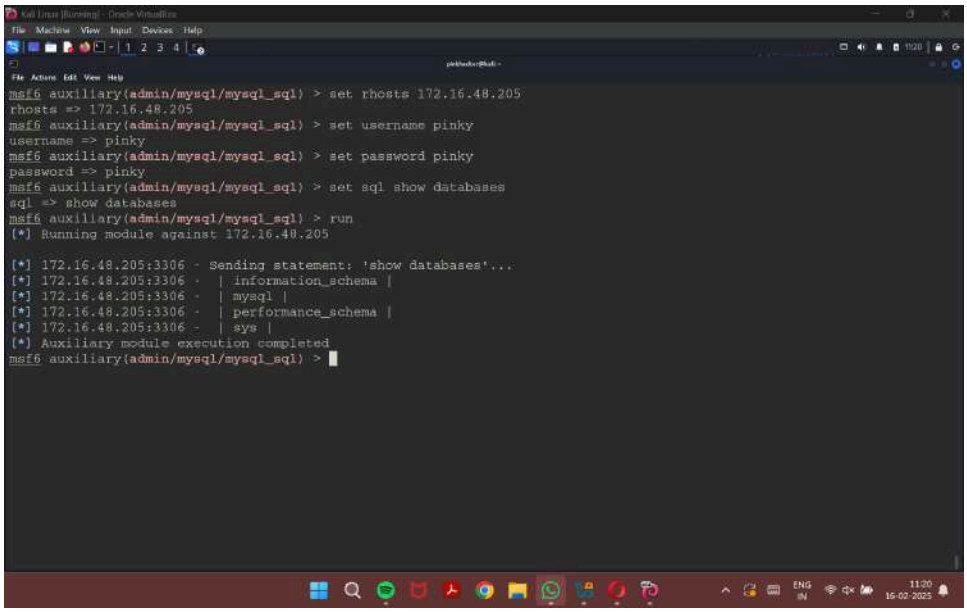


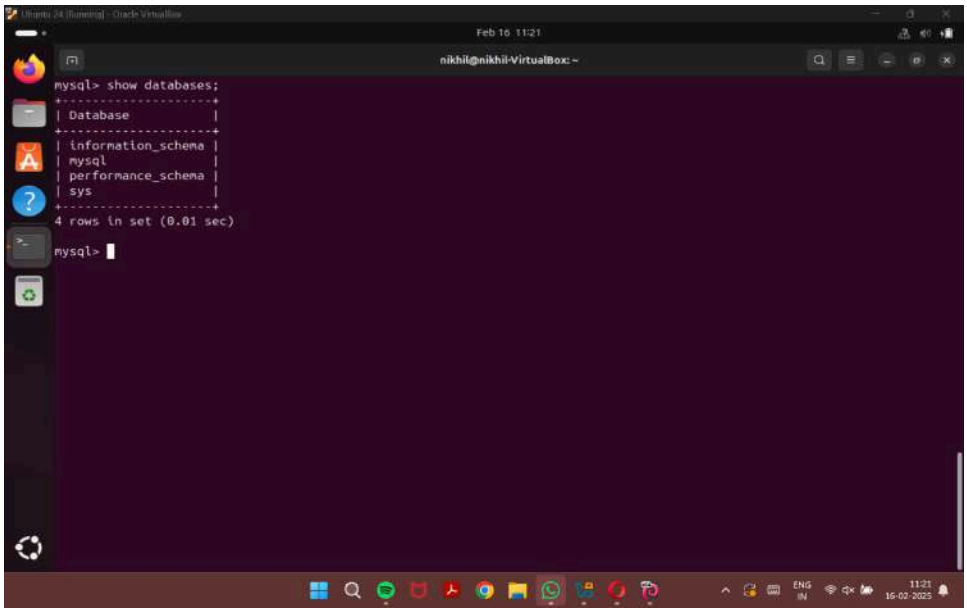
MySQL SQL

11. Search for mysql_sql and use it



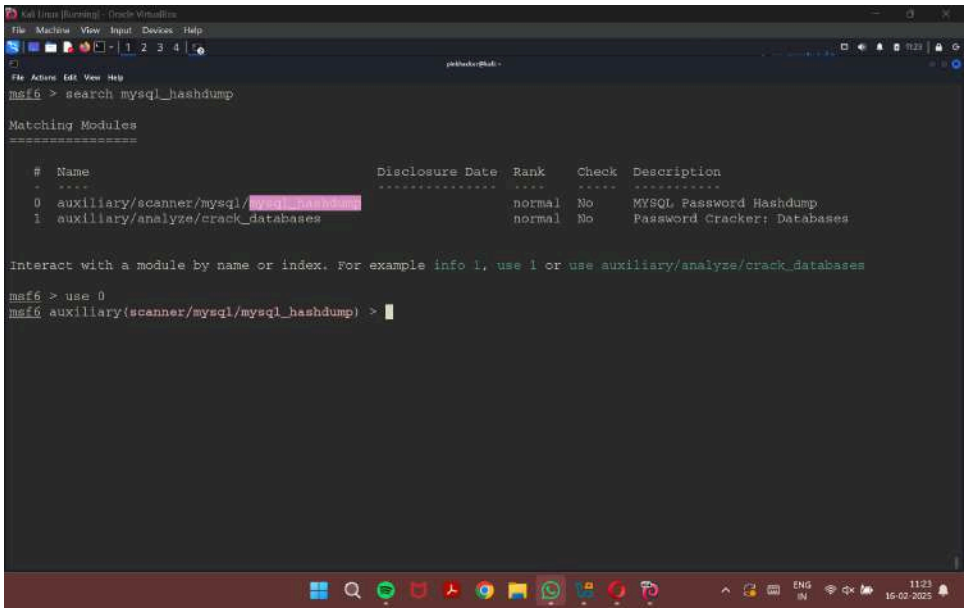
12. Set rhost to IP address of ubuntu, username to pinky, password to pinky and sql to the sql command (here ‘show databases’) and run it



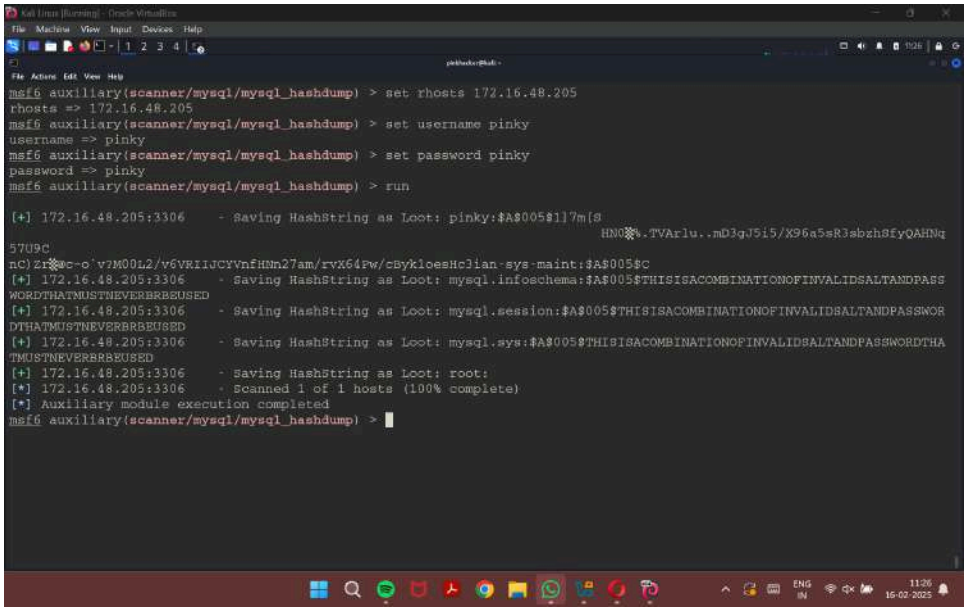


MySQL Hashdump

13. Search for mysql_hashdump and use it

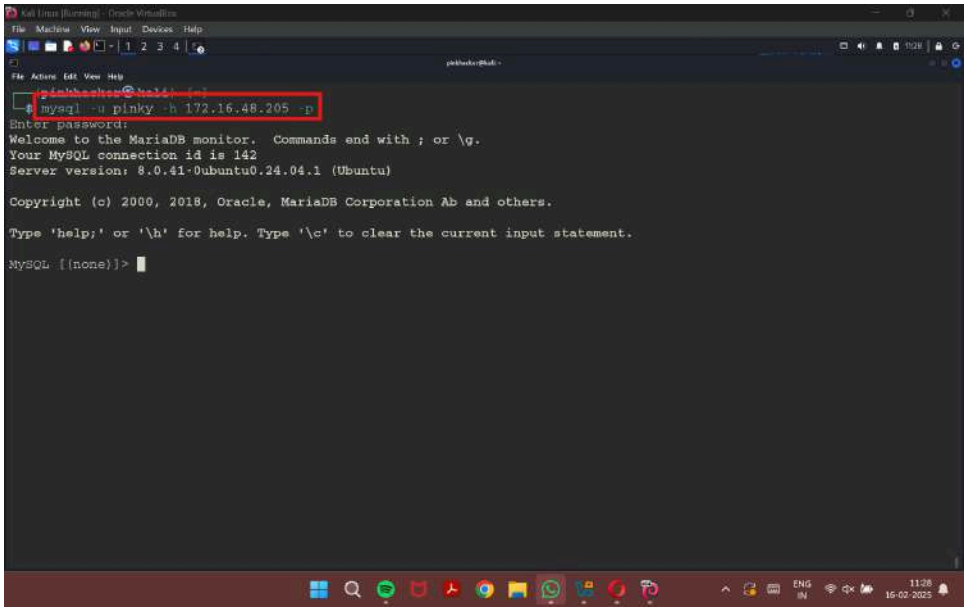


14. Set as below and run

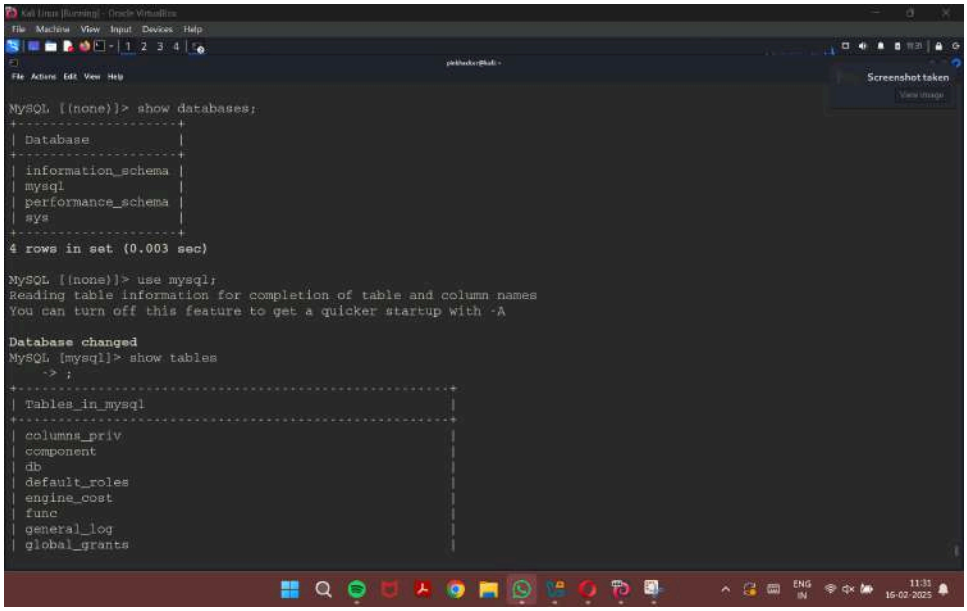


MySQL Login (of Ubuntu) from Kali Linux

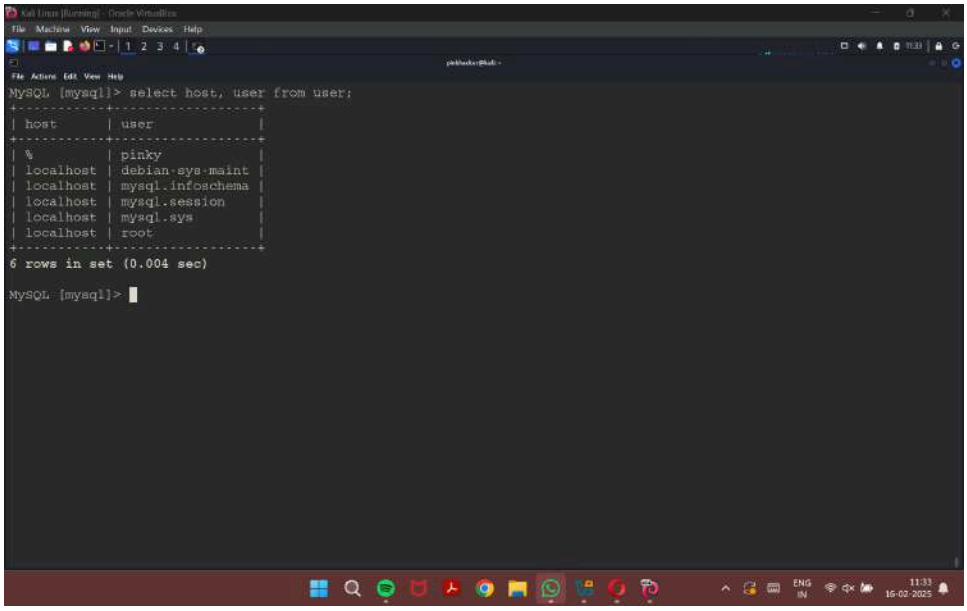
15. Open a terminal and run the following command (with ubuntu's IP address) and enter the password



16. With this access you can look into any MySQL databases in Ubuntu machine



Dhevatha S P
22BCE0826



Dhevatha S P
22BCE0826