Project – MySQL Pen Testing

Group Members: Dalen Wimsatt, Ethan Epperson, Stephen Stine

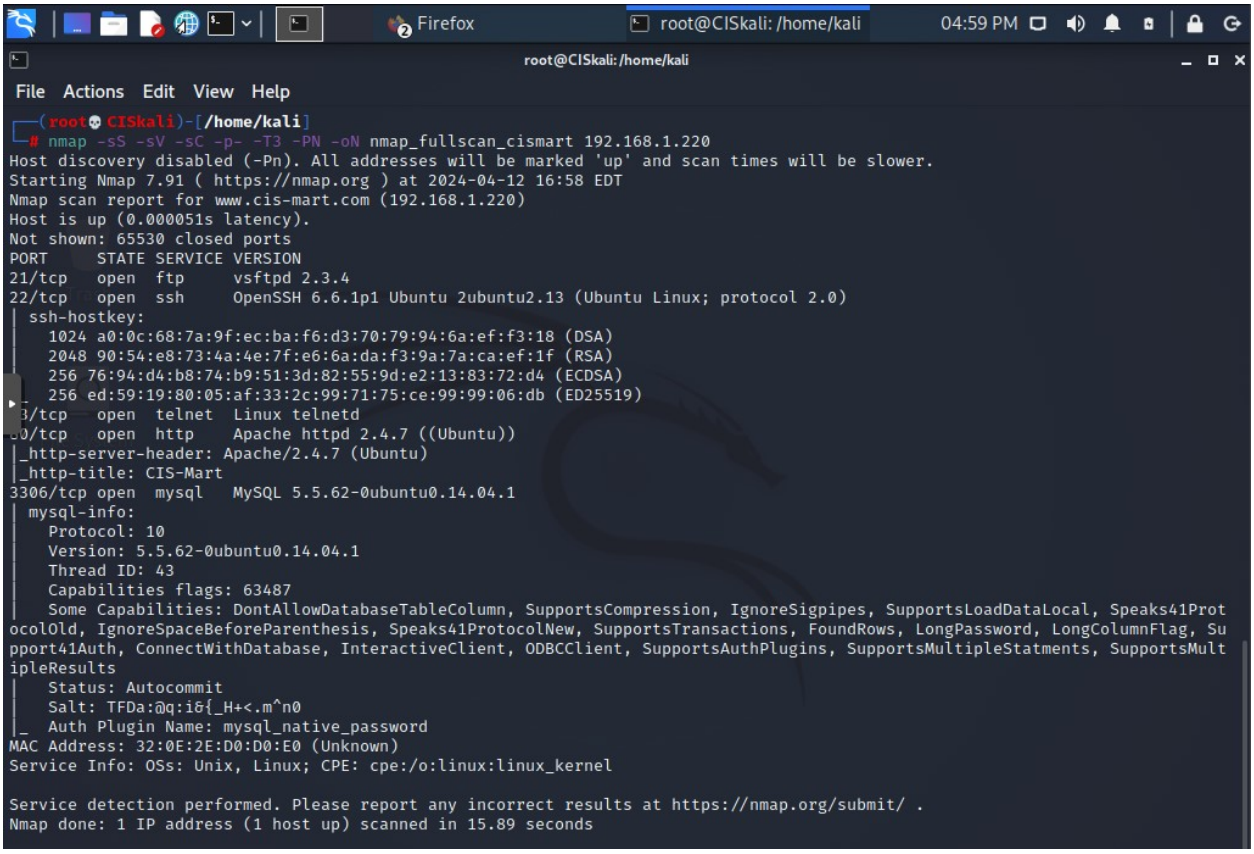
Guidelines

1) For submission, follow the naming convention: CIS483PenTest-TeamX.docx, where X is your team ID on the team roster.

Tasks

Task 1. Nmap scan of the server

- Take a screenshot of the outcome.



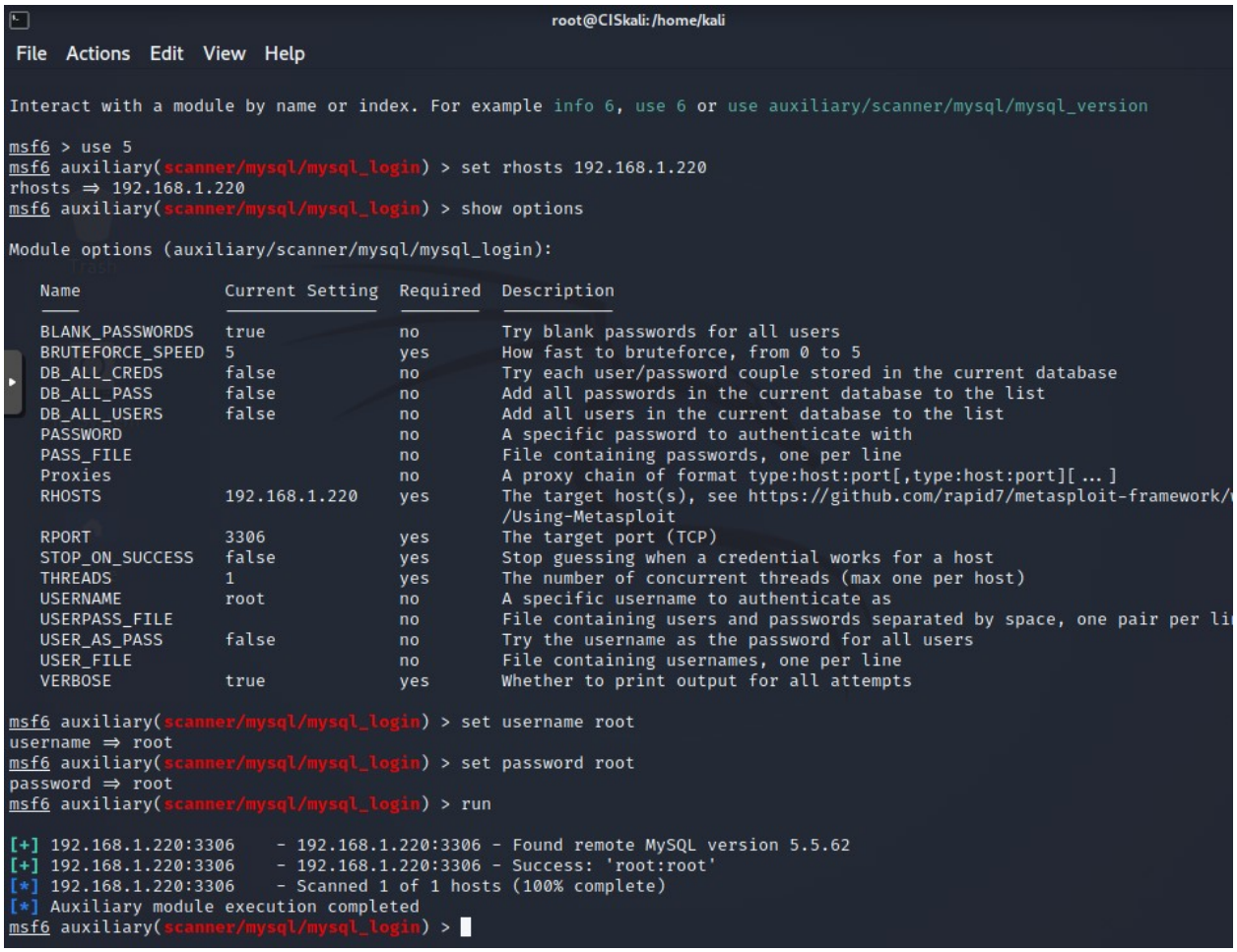
- Describe your observation after a nmap scan.

We ran a full Nmap scan that performs a SYN scan for faster scanning, service version detection, script scan, full port scan, sets the timing option to moderate for enhanced scan speed, skips host discovery (we already know the target is up), and then outputs to the specified file "nmap_fullscan_cismart". From the scan we were able to see that several service ports are open at 21, 22, 23, 80, and most importantly 3306. 3306 is the default MySQL port and we were able

to determine several key insights into the service such as protocol, version, thread ID, capabilities flags, the capabilities themselves, and more.

Task 2. Brute-forcing logins

- Take a screenshot of the outcome.

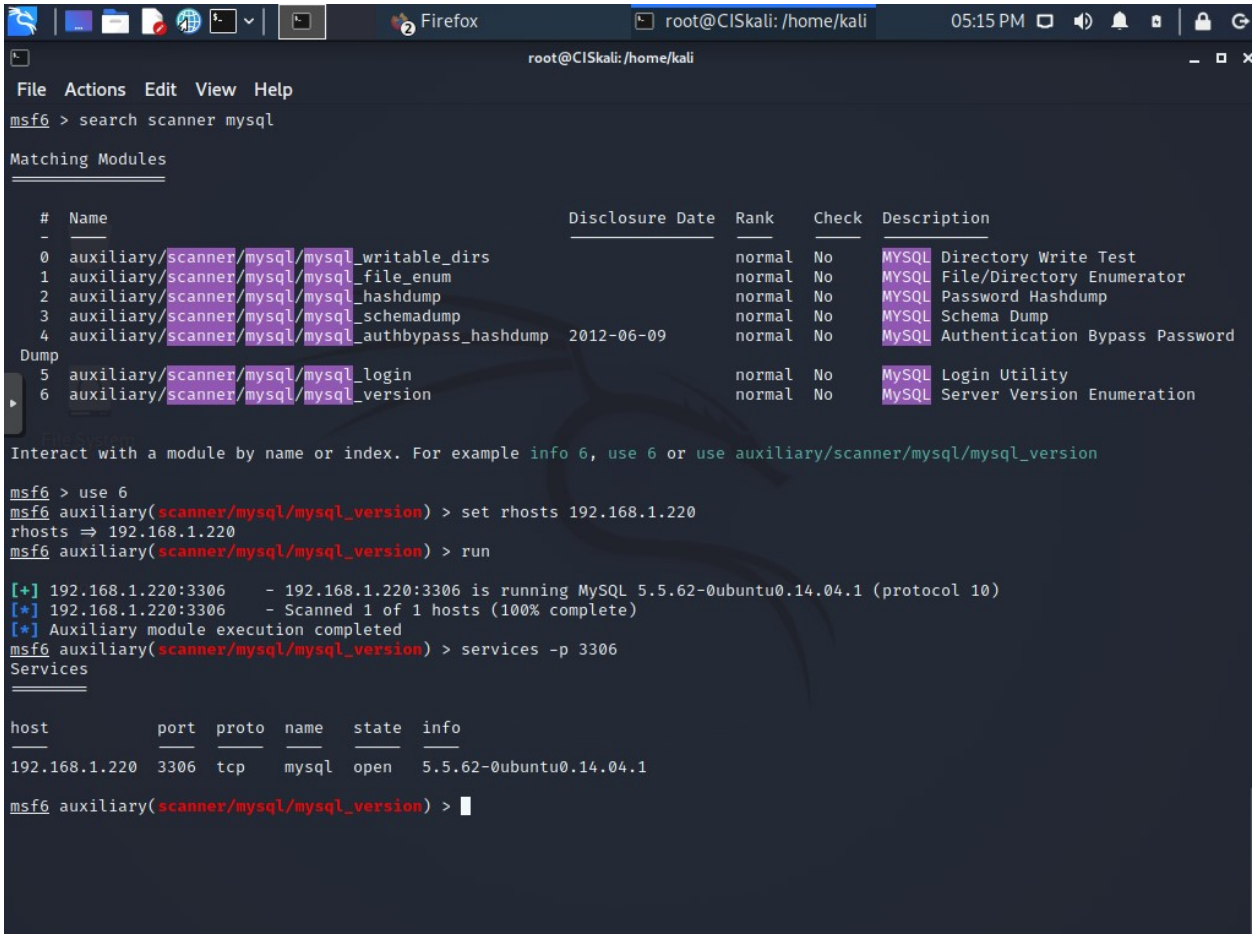


- Explain what you have accomplished.

We used the auxiliary MySQL login utility module to brute force logins. We set rhosts to the address for the e-commerce server and then set the username/password to “root” respectively. We ran it and were successful.

Task 3. Obtaining MySQL version

- Take a screenshot of the outcome.

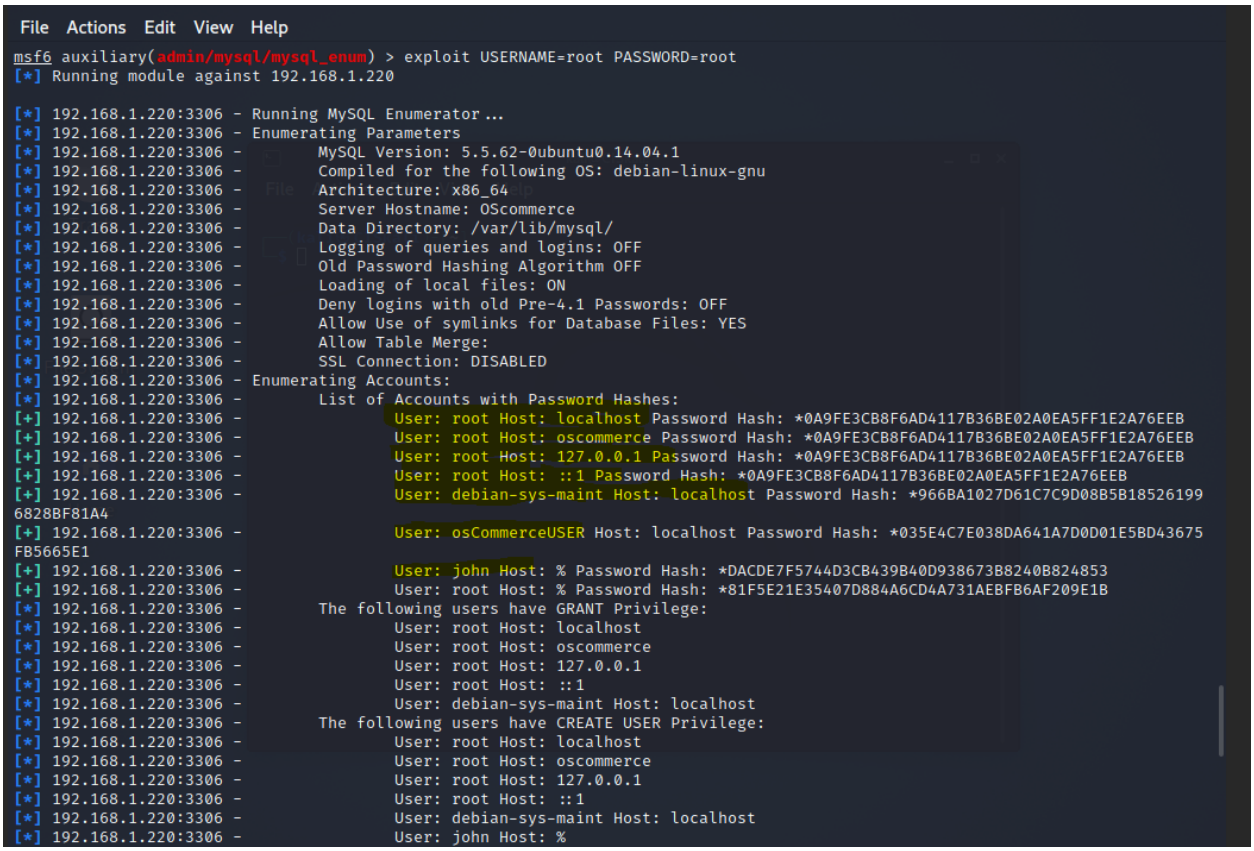


- Describe explicitly the version of MySQL.

To get a second source of validation that port 3306 is open with MySQL service running besides Nmap, we ran an auxiliary module for MySQL server version enumeration. Through this module we were able to determine information about MySQL version. The host using the default MySQL port at 3306 over TCP, it's currently open, and the version is 5.5.62-0ubuntu0.14.04.1. 5.5.62 is the specific major (5.5) and minor version of mysql (.62). The first 0 indicates the build number. 'Ubuntu0' represents the distribution-specific changes and packaging. It's built for Ubuntu. 14.04.1 is the release version of Ubuntu being used for the MySQL package.

Task 4. Enumerating MySQL Users

- Take a screenshot of the outcome.

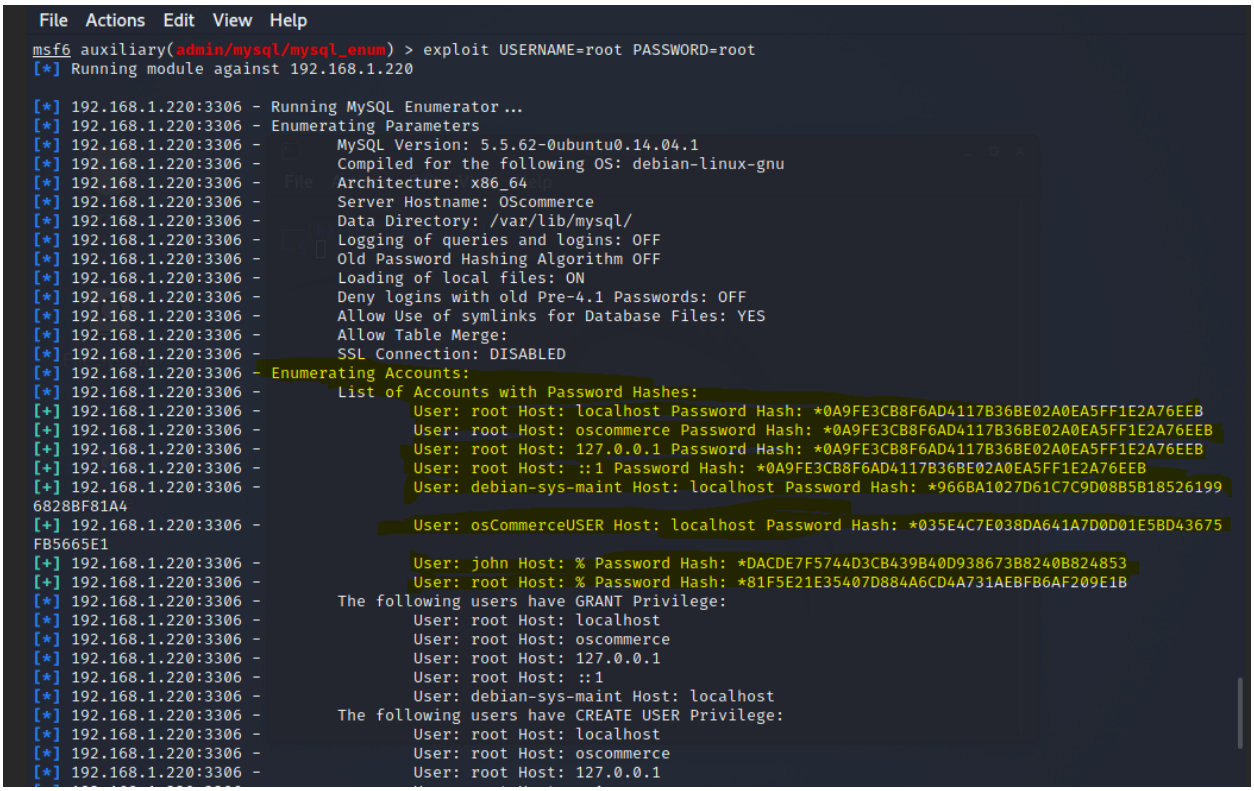


- Describe explicitly MySQL users you've extracted.

Using mysql_enum we enumerated the users on the sql server targeting both the port 3360 and the IP 192.168.1.220. We were able to gather information on 7 users including system maintenace and root accounts from several different hosts. Among the data collected was password hashes and rights for each of the users.

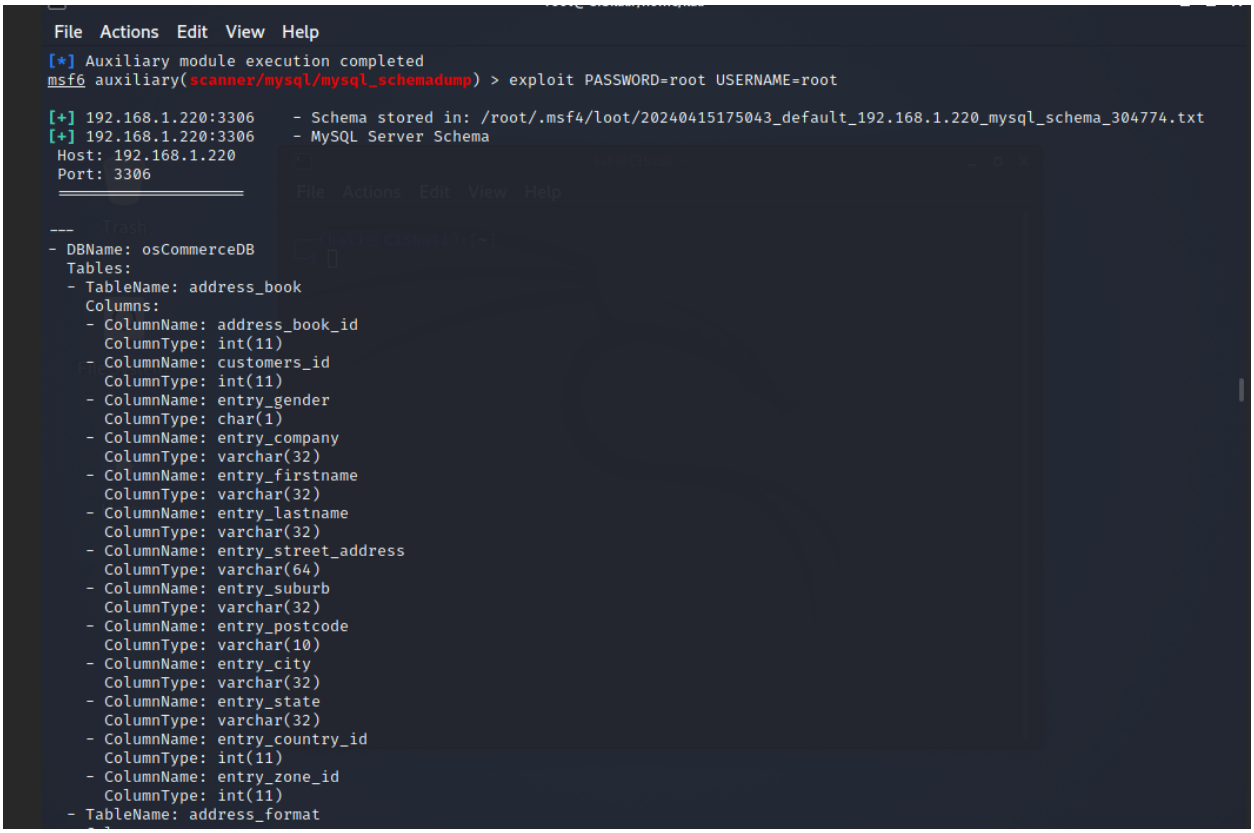
Task 5. Dump password hashes of MySQL Users

- Take a screenshot of the outcome to report the password hashes you've extracted.



Task 6. Dump database schema

- Take a screenshot of the outcome.



- How many tables did you find?

We found 46 tables ranging from customer information to address books to product information and order information.