جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Computer Data Security and Privacy Project

G3

Team Members

Name	ID
Shahad Emad Aljiaan	2200003861
Amal Mohammed Alotaibi	2200001746
Wadha Nayef Alsheddi	2200003246
Asma Zaher Alshehri	2200000484

Supervisor: Dr. Azza Abdo Ali

Table of contents

Table of figures

1. Introduction

This project aims on discovering and using various Kali Linux tools which is an operating system used to conduct penetration tests that is most widely used for security reasons [1]. Tools which will be discussed are Namp, SQLmap and Hydra. For each of these tools a detailed description about its definition, features, implementation and countermeasures using the Kali Linux will be conducted.

2. Network Mapper ("Nmap"):

Nmap is an open-source security auditing tool that can be used for preventative security auditing of all networks, list all ports, determine whether or not they are open and detect all vulnerabilities on all types of devices. It can also be used to audit servers, routers, and mobile devices. Nmap can be run under all operating systems, including Linux, Windows, and Mac OS [2].

2.1 Features:

- Flexible: Detects IP filtering, routers, firewalls, and other obstacles on networks, including TCP and UDP port scanning. Also detects operating systems, versions, pings, and more.
- Easy: Nmap is available as a command-line as well as a graphical user interface (GUI) version for the convenience of those who do not wish to compile Nmap from source.
- Powerful: It has been used to perform massive network scans on networks with literally hundreds of thousands of devices using Nmap.

2.2 Nmap Commands:

There are various commands that Nmap establish to users, the figure below shows commonly used commands with illustration of its usage

Command	Usage	Written as
-p	Used to scan set of ports whether it is on a local or remote servers.	nmap -p
-sT	It is used to scan open ports and has the ability to work	nmap -sT

	with the TCP protocol without any problems.	
-p -n	Used to disable DNS to speed up scans.	nmap –p -n
-sp	It is used to scan ping command.	nmap -sp

Table: Nmap commands

2.2.1 Command to scan nmap ports

by using this command, a port, or a set of ports can be scanned whether it is on a local or remote servers depending on your configuration. As we can see from the image below, we have scanned 20 ports on the local host computer.

Nmap -p 1-65535 localhost

2.2.2 Nmap Ping Scan

When you want to perform a ping scan on any existing network with a purpose of discovering the host, this command is the most commonly used and popular command to do so.

Nmap –sp 192.168.5.0/24

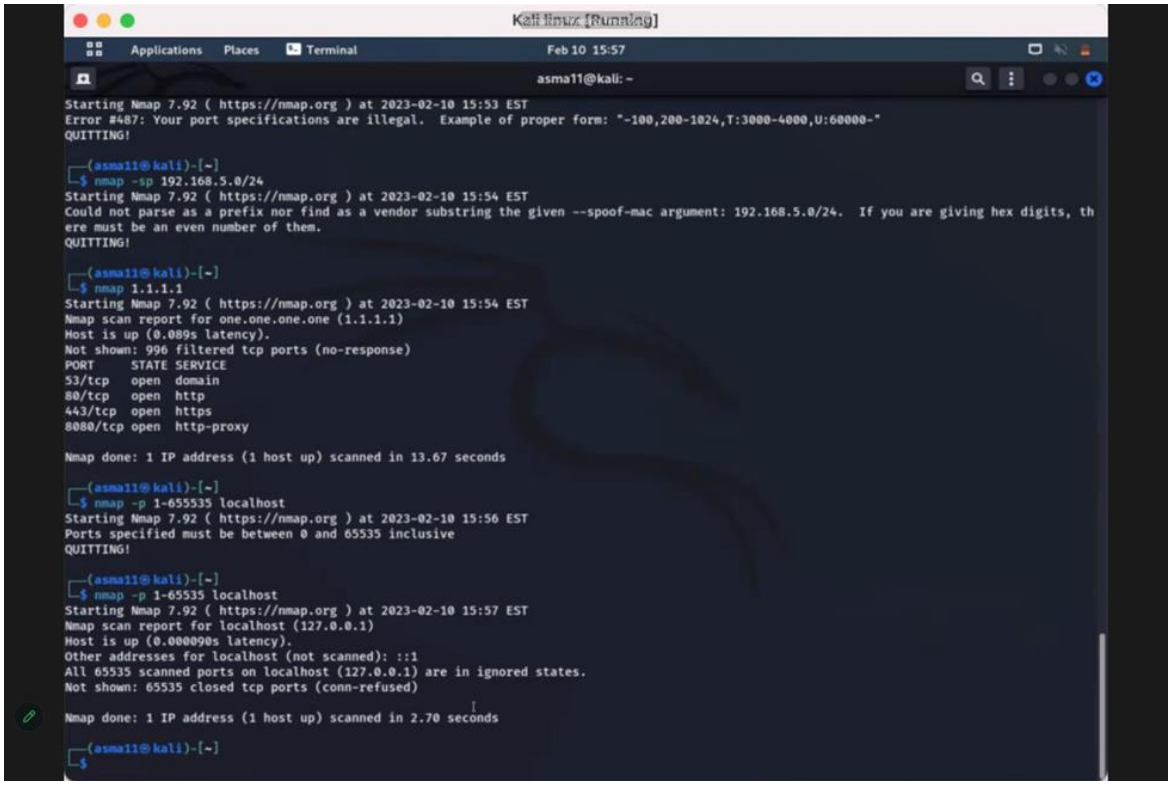

Figure 1 scan nmap ports & ping

2.2.3 Host and IP address scan with Nmap

Nmap Scan Against Host and Ip Address We used this command as a method of scanning either the IP address or host name, as shown in the picture below.

nmap 1.1.1.1

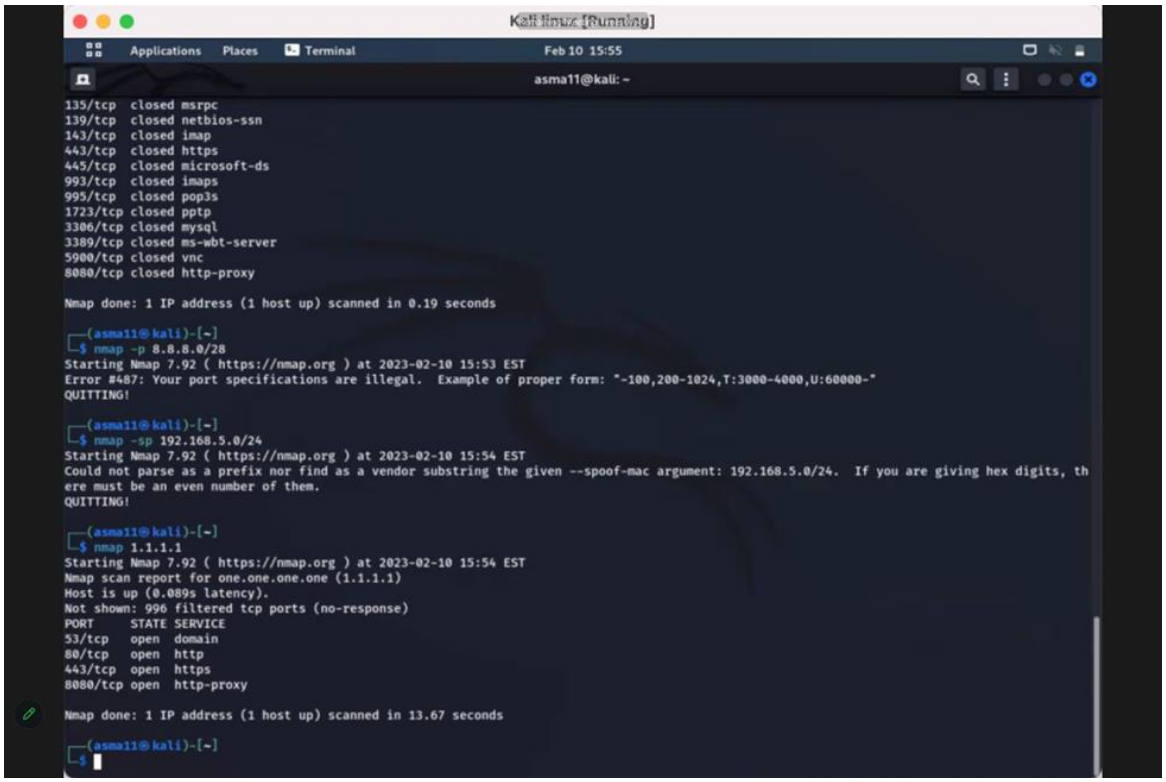

Figure 2 Host and IP address scanning

2.2.4 Nmap scan of multiple IP addresses

Multiple Ip Address Scan Using this command, we can scan multiple IP addresses simultaneously, which is a very useful feature when scanning multiple addresses at once.

nmap 1.1.1.1 8.8.8.8

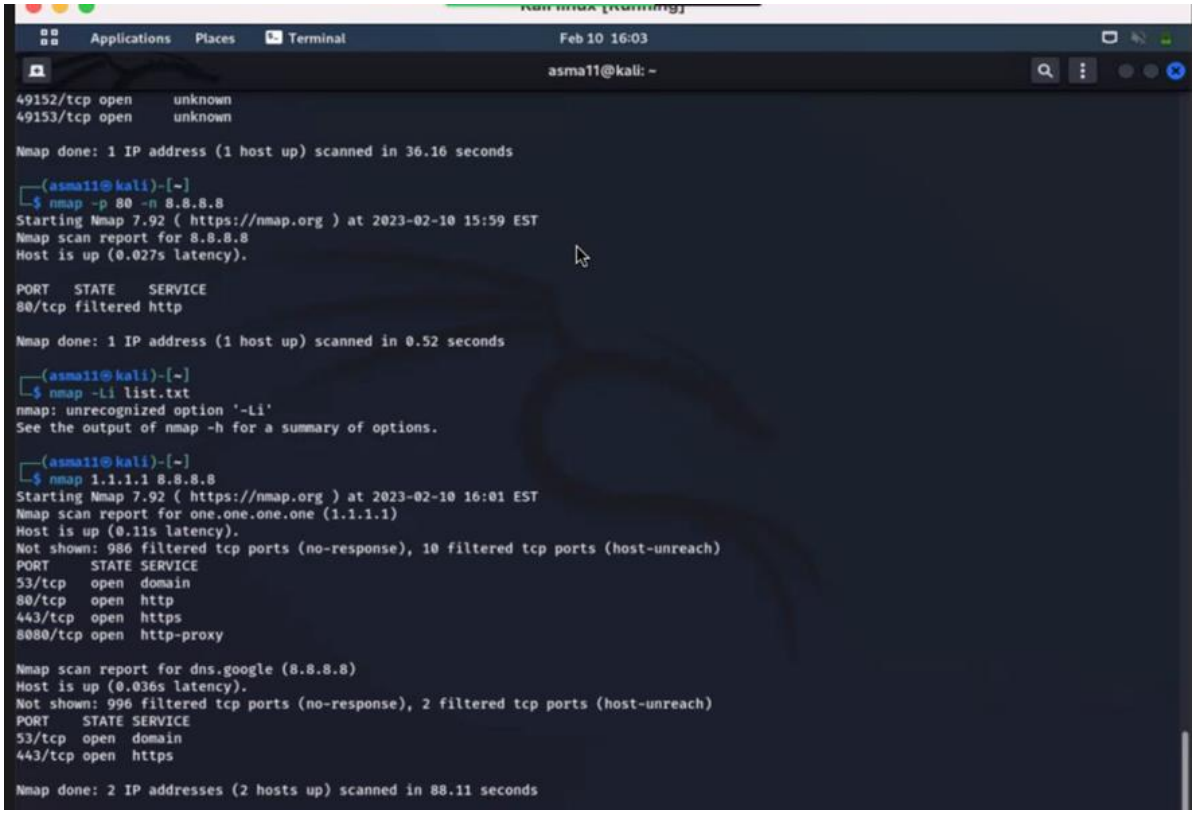

Figure 3 Sscan of multiple IP addresses

2.2.5 DNS Name Resolution Disabled Using Nmap

Disabling DNS Name Resolution, the aim of this command is to speed up the scans, if there are a lot of scans that need to be performed. To achieve this, we had to disable the reverse DNS in order to speed up the scans. The SSH port was filtered.

map -p 80 -n 8.8.8.8

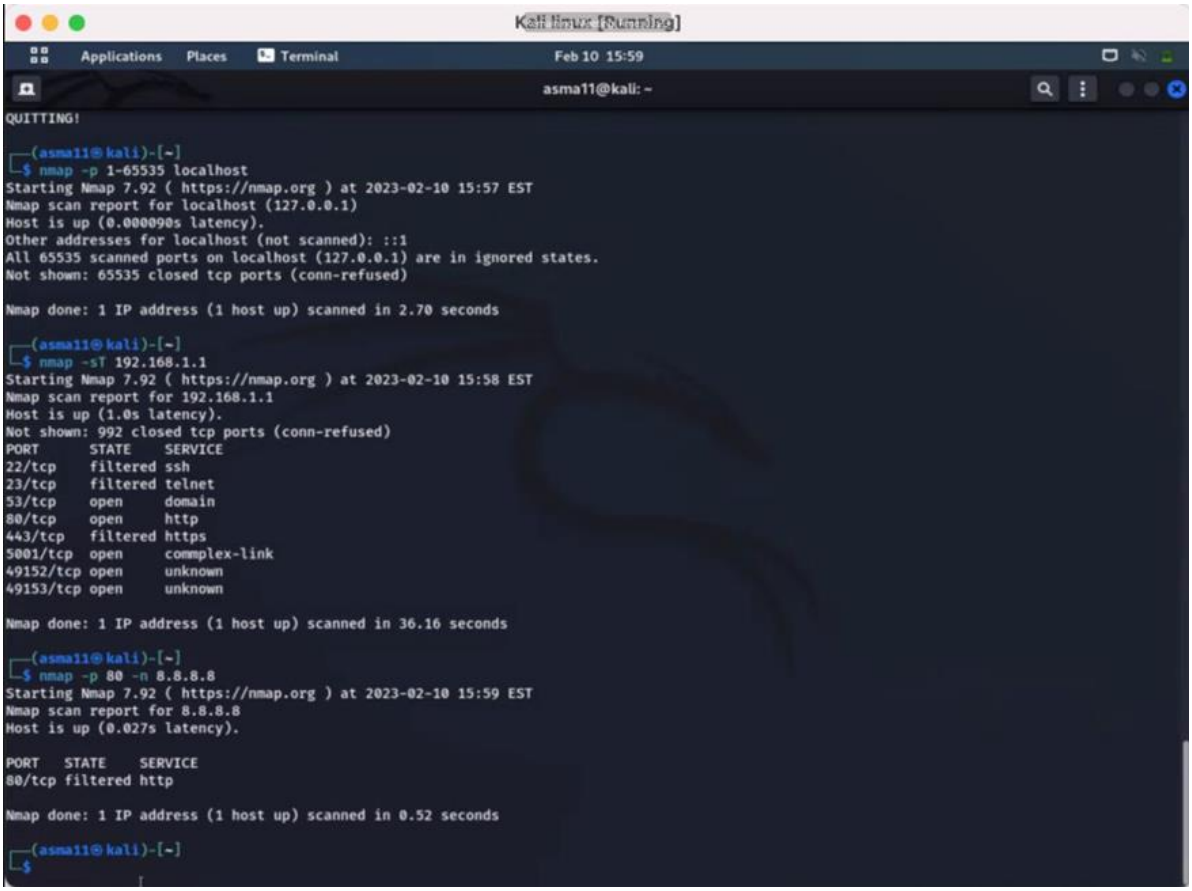

Figure 4 DNS Name Resolution Disabled

2.2.6 Using TCP for scanning

Nmap can scan open ports and has the ability to work with the TCP protocol without any issues, so when we used this command as shown in the picture, here was the output that we got when using standard TCP to scan ports.

map-sT 192.168.1.1

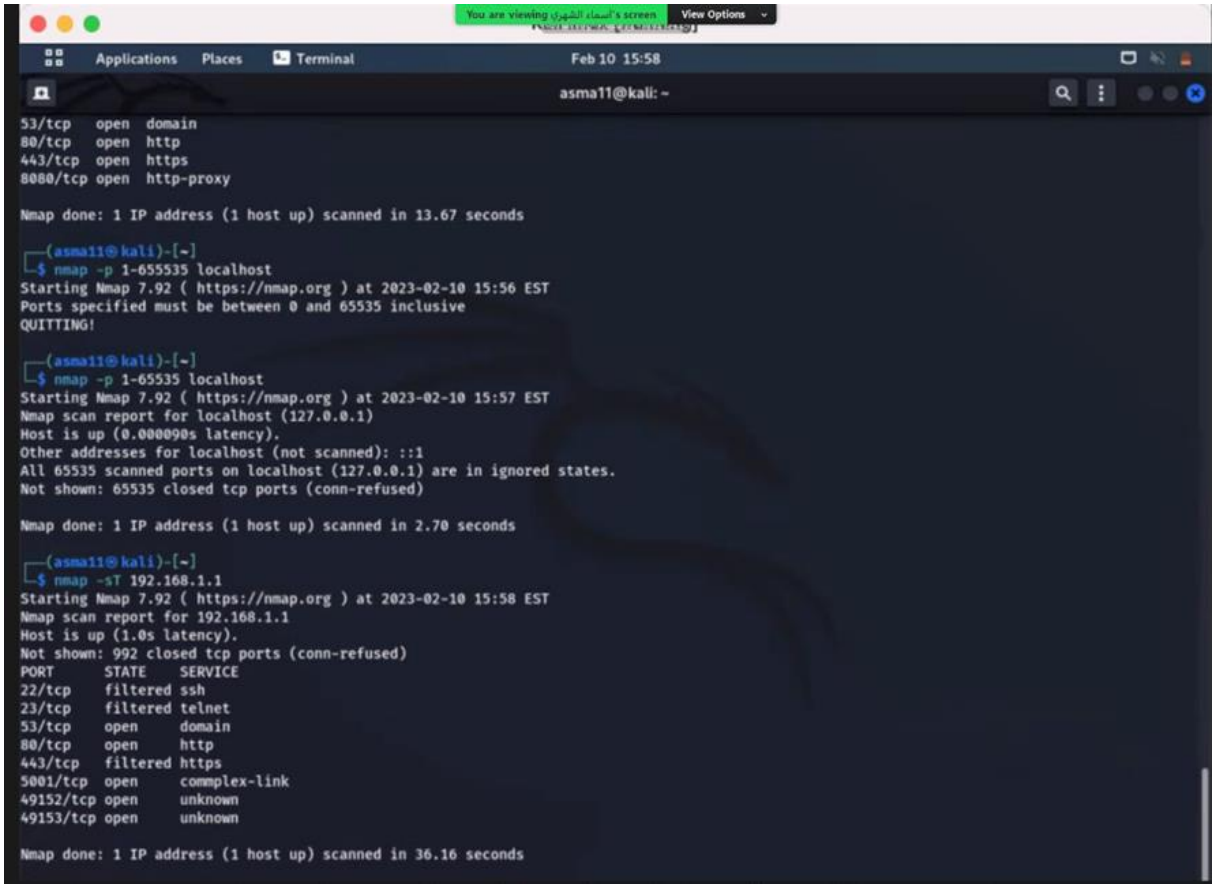

Figure 5 TCP scanning

2.3 Nmap results and analysis:

- Scanning ports (open and close).

- Opening of a closed port to open port.

- Detecting vulnerabilities across all devices and networks through preventive security auditing, listing all ports, determining whether they are open or not, and finding all open ports on all networks.

2.4 Nmap countermeasures:

Several measures can be taken to prevent attackers from scanning your network using Namap, such as the following:

1. Firewall installation is one of the most effective means of preventing unauthorized access, since it controls and inspects the ports, and it can also scan and close them.
2. Discover network holes, make sure to check your internal ports until you are able to determine if there are more open ports than needed in your system. You can also scan your system periodically to find out if there are any vulnerabilities that can be exploited by attackers.
3. Intrusion detection systems monitor traffic, it will be able to discover and detect Nmap scans that block traffic that is deemed malicious [3].

3. SQLmap:

SQLmap is an open-source penetration testing tool used to detect and exploit SQL injection flaws, as well as gaining access to database servers. The tool includes an efficient detection engine, various features for penetration testers, and numerous switches that allow gives access to database, fetch data, access the underlying file system, and execute commands on the operating system using out-of-band connections, the process is from database fingerprinting to database retrieval [4].

3.1 Features:

- Support many database management systems such as: MySQL, Microsoft access and MySQL
- Enable the direct connection to the database without having to go through any SQL injections by providing the database management system credentials, database name and IP address which can directly allow to connect to the database.
- Provide time arrival estimation by displaying the amount of time it will take to retrieve the queries' result and it will display for each query in real time to give users a clear vision about what is happening.
- Queries and their results (even in the case of partial retrieving) will be automatically saved in the form of a text file, which is parsed to resume injections.
- can detect and exploit five types of the SQL injections which are: Boolean based blind, stacked queries, Union query, Time based blind and Error based.

3.2 SQLmap Commands

There are various commands that SQLmap establish to users, the table low shows commonly used commands with illustration of its usage

Command	Usage	Written as
--wizard	Help new users by providing an interface to help to get familiar with the tool	sqlmap –wizard
-u	Include vulnerable query parameters in the target URL	sqlmap -u
--purge	Used to clear the entire database folder	sqlmap -purge
--dependencies	Used to detect any missing dependencies	sqlmap--dependencies
-d direct	Used for the direct connection with the database	sqlmap-d

Table: SQLnap commands

3.3 SQLmap using procedure

Step 1:

For SQLmap tool to be used, it must be installed in Kali Linux. After installing it, the tool will appear at the database assessment section as it shown in the following figure

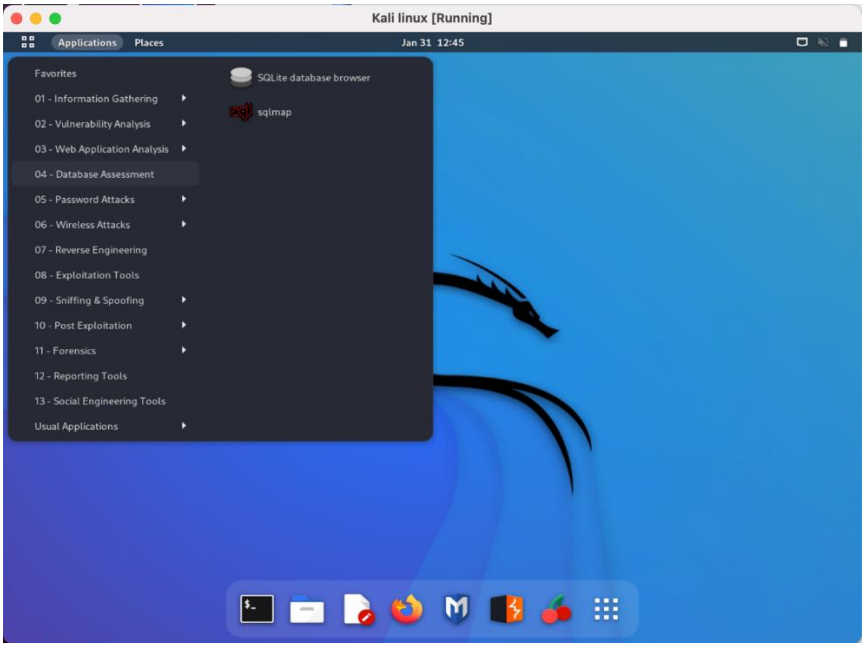

Figure 6 showing SQLmap tool

Step 2:

The wizard command was used which will help in getting familiar with the tool implementation requirements as shown in the following figure

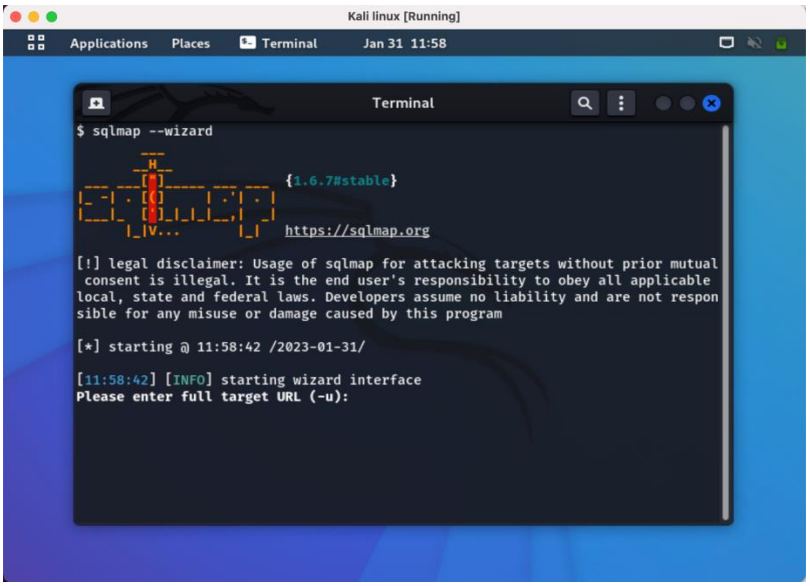

Figure 7 wizard command

Step 3:

using Acuart from vulnweb website

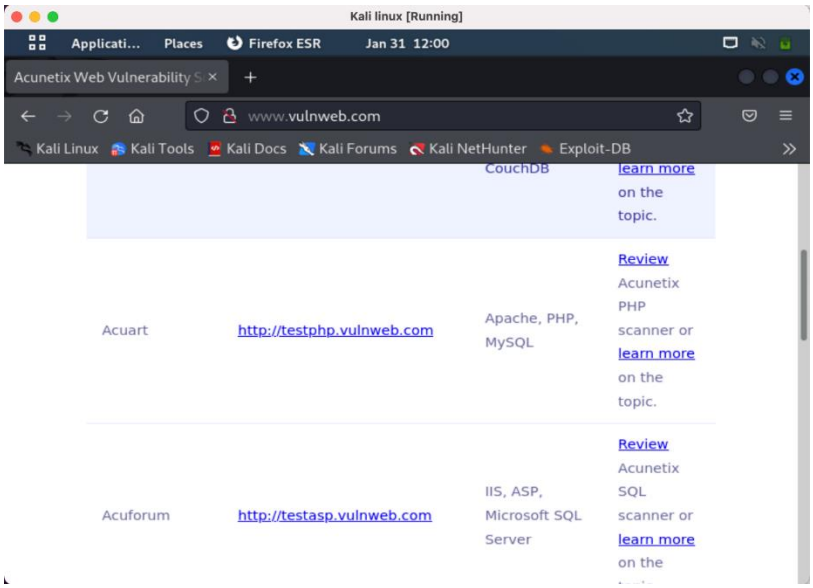

Figure 8 vulnweb website

Step 4:

The following command will be used to display the tables of database as shown in the figure "-u http://testphp.vulweb.com/artists.php?artist=1 -D acuart –tables"

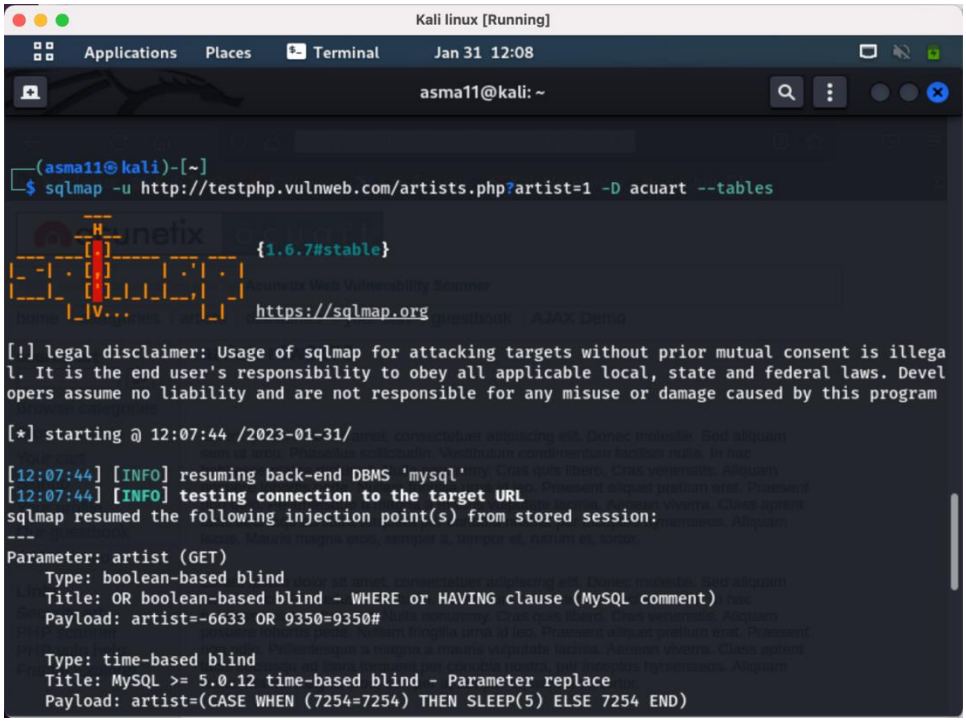

Figure 9 showing tables commands

Step 5:

The following command will be used to display the columns of database as shown in the figure "-u http://testphp.vulweb.com/artists.php?artist=1 -D acuart -T users –columns"

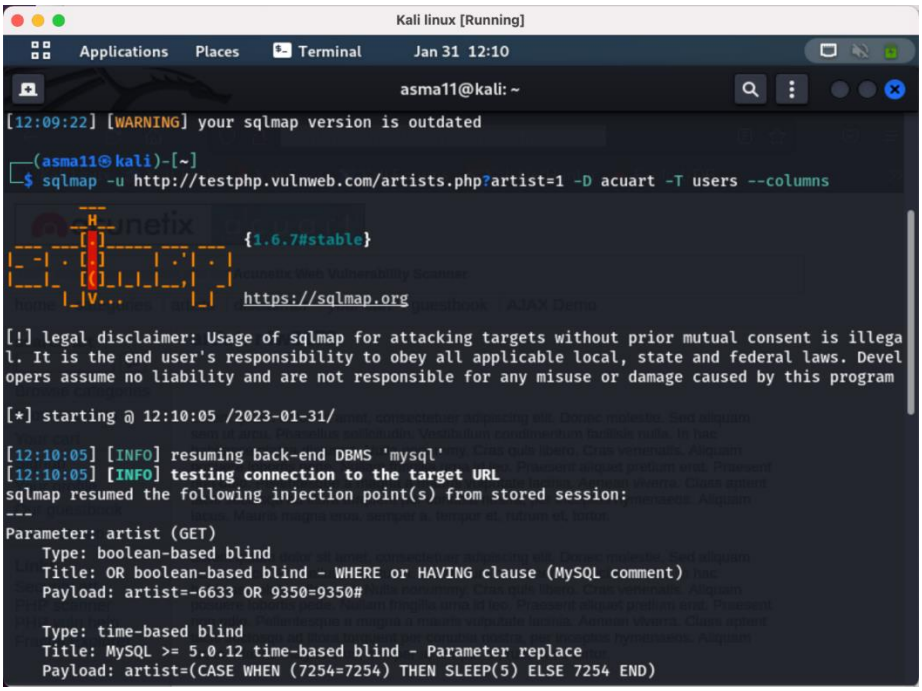

Figure 10 showing columns commands

Step 6:

The following command will be used to display the username as shown in the figure

-u http://testphp.vulweb.com/artists.php?artist=1 -D acuart -T users -C uname—dump

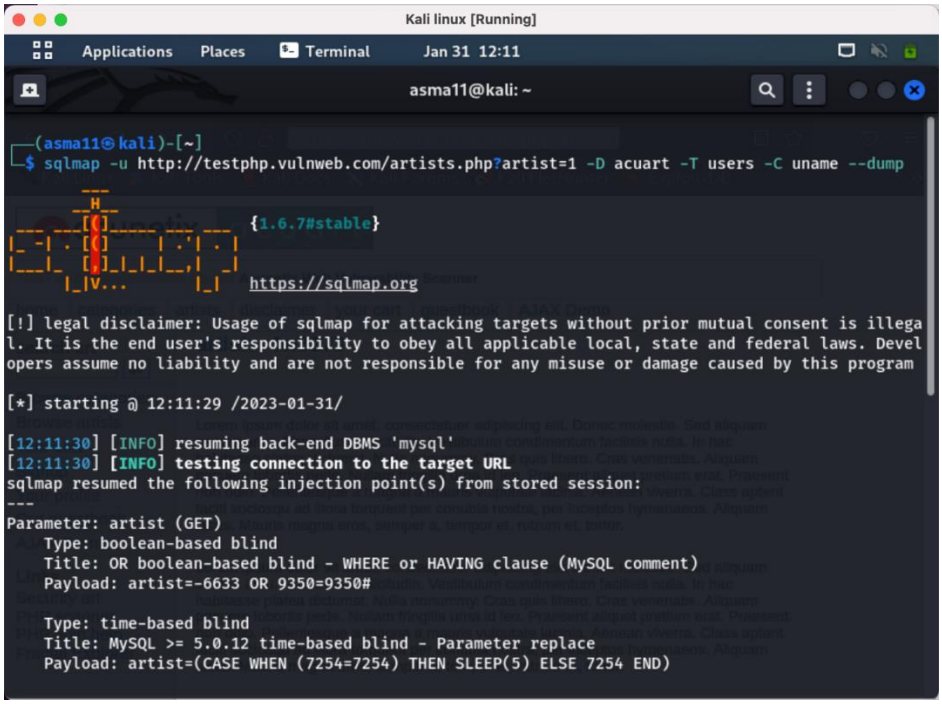

Figure 11 Display username command

Step 7:

The following command will be used to display the password as shown in the figure

-u http://testphp.vulweb.com/artists.php?artist=1 -D acuart -T users -C pass—dump

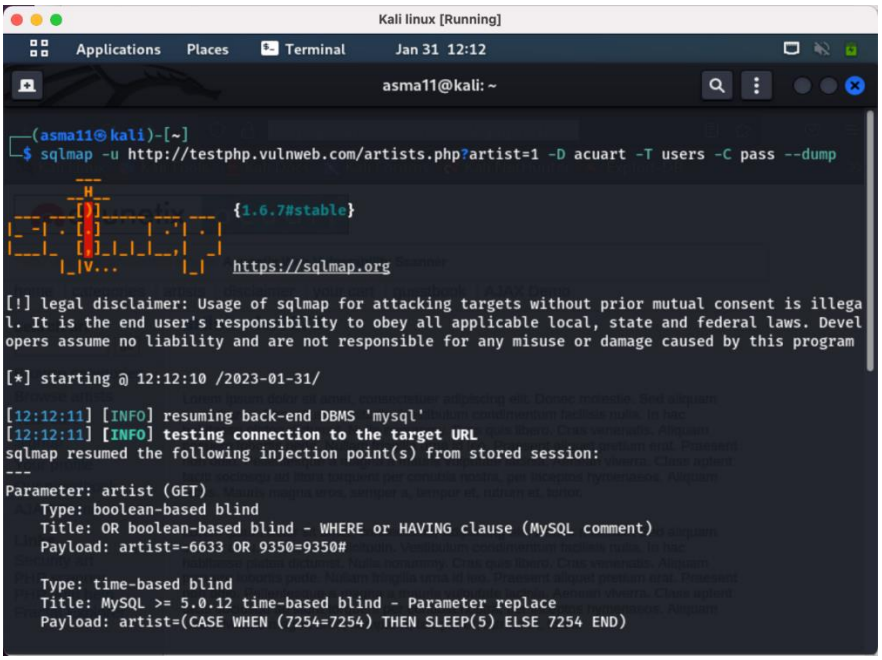

Figure 12 Display password command

3.4 SQlmap Result and Analysis

- The result of executing displaying the table command is shown in the figure below

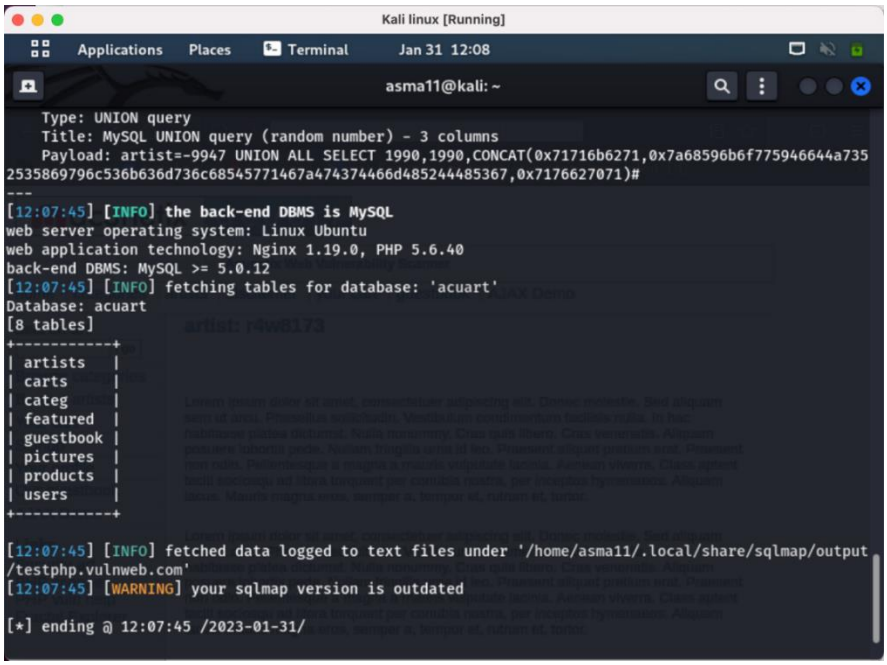

Figure 13 table command results

- The result of executing displaying the column command

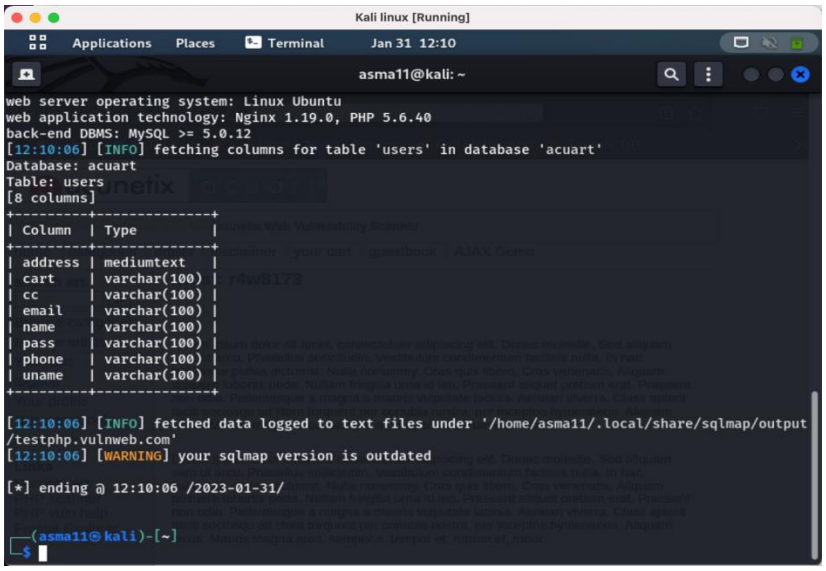

Figure 14 column command results

- The result of executing displaying the username command

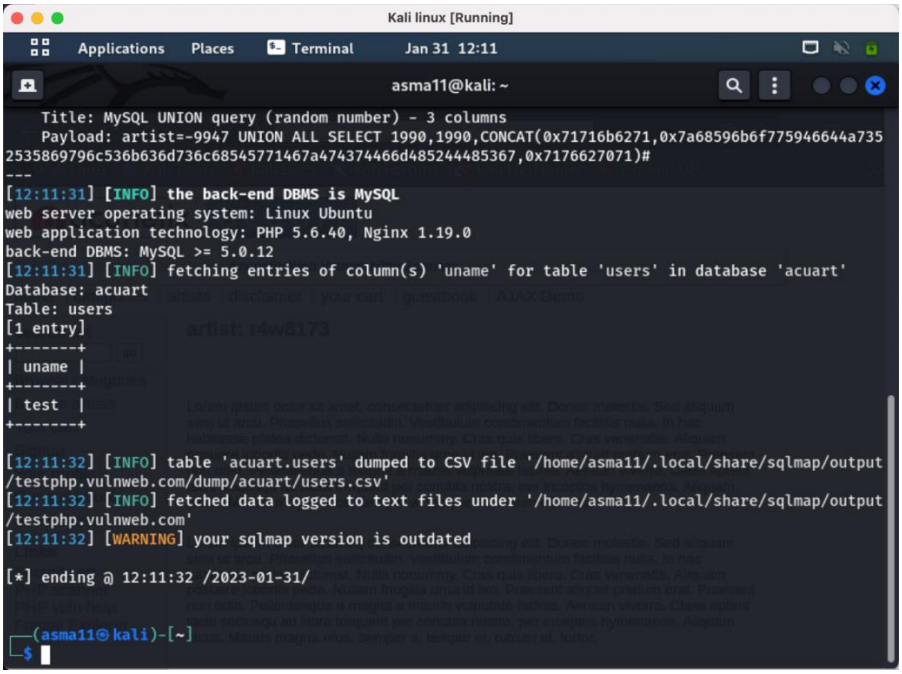

Figure 15 username command results

- The result of executing displaying the password command

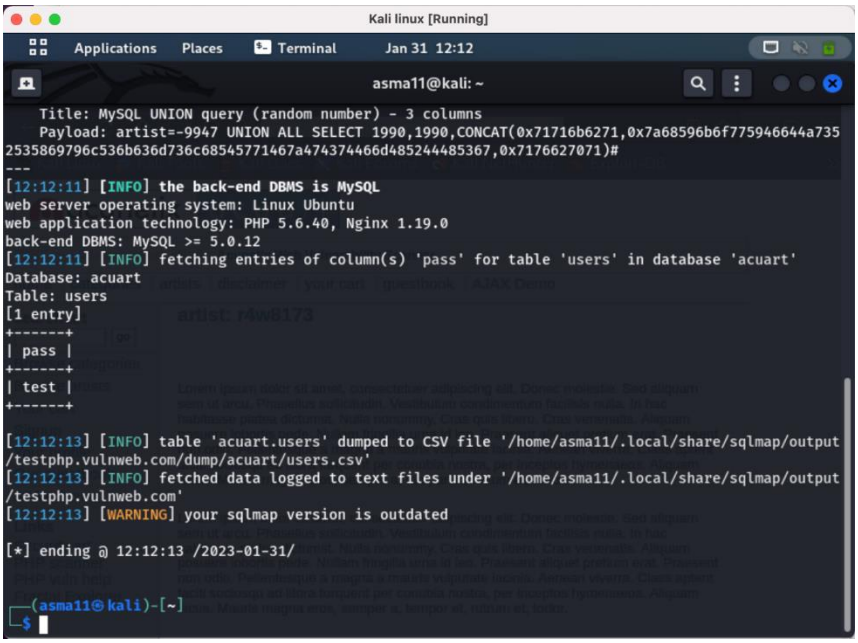

Figure 16 password command results

- the login through the website using the username and password that has been found by executing the commands as it shown in the figure which are:

username: test

password: test

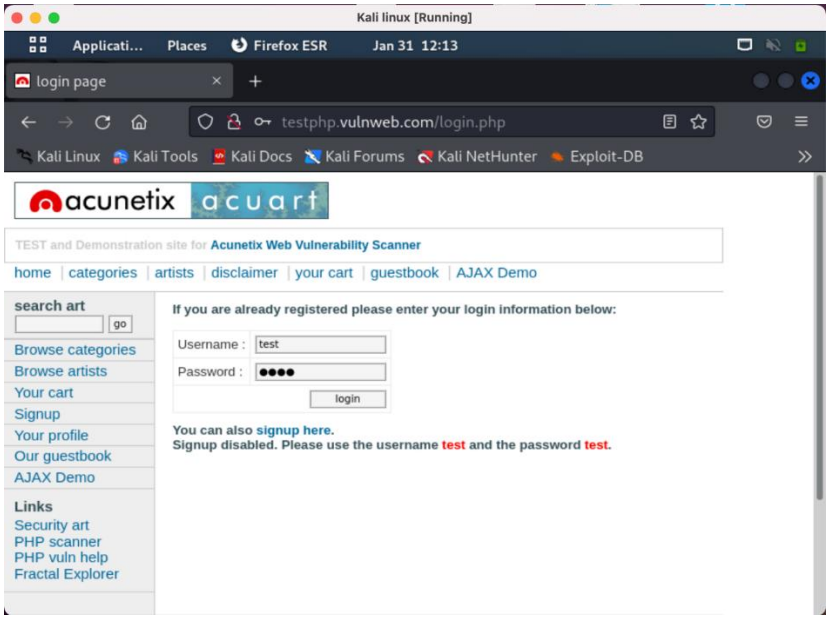

Figure 17 Entering username and password

- The following figure shows that the entered username and password initiated a successful login to the website

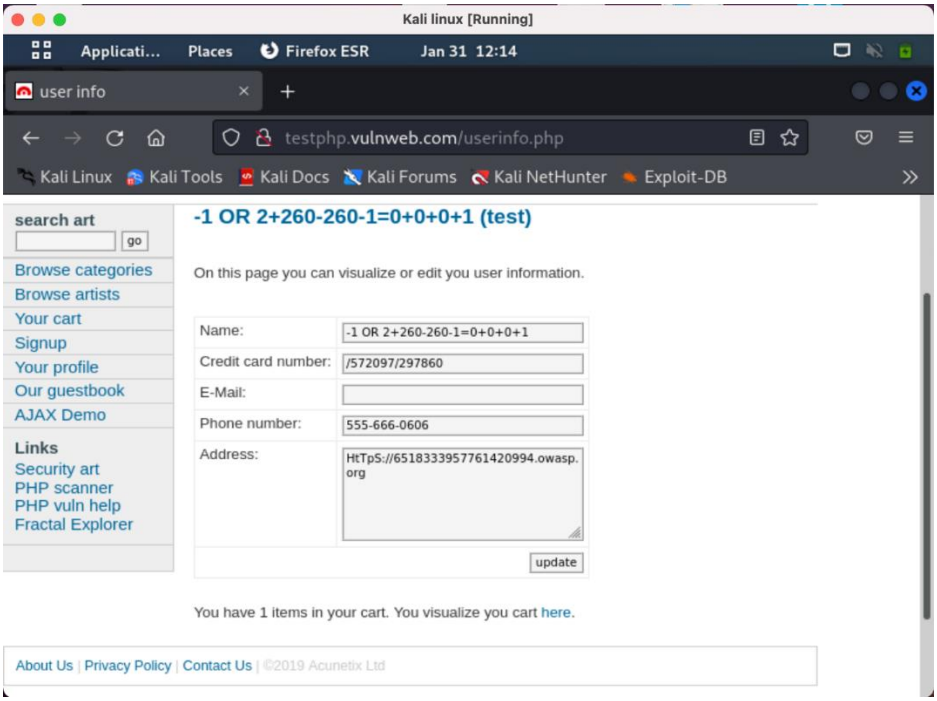

Figure 18 Website successful login

3.5 SQLmap Countermeasures

There are various ways which can be used to avoid for any vulnerates to be discovered and exploit by the SQLmap such as [5]:

- Using the Least privilege concept when giving the programmer the credential to run the SQL commands to communicate with the database such as insert, delete, and update where the programmer should only be giving minimal privileges to perform the tasks which is assigned to complete to minimize the occurrence of the sql injection.

- Using a web application firewalls to protect against any SQl injections and cross site scripting that can be exploited by SQLmap.

- Allowing programmers to use the object relationak mapping to conduct operations on the database table in a seucre way avoiding any SQLinjections.

4. Hydra:

Hydra is a powerful password cracker used by penetration testers who operate under the pseudonym of "ethical hackers" and can be used with other Kali Linux tools such as nmap to conduct brutal force attacks using trial and error methods. We use it to guess passwords and usernames with the use of large amount of guess list made in order to perform the guessing, with files ending in ssh, telnet and ftp. It's also used to test the system against any malicious attack to the information.[6]

4.1 Features:

- Supports a variety of protocols that can be attacked.
- The tool is considered to be flexible and fast.
- The security administrator can use this tool to easily clarify the possibility of unauthorized access to the system using this tool.
- Hydra tool is designed to evolve over time as wide services will be supported.

4.1.1

Brutal force attack was used in this tool

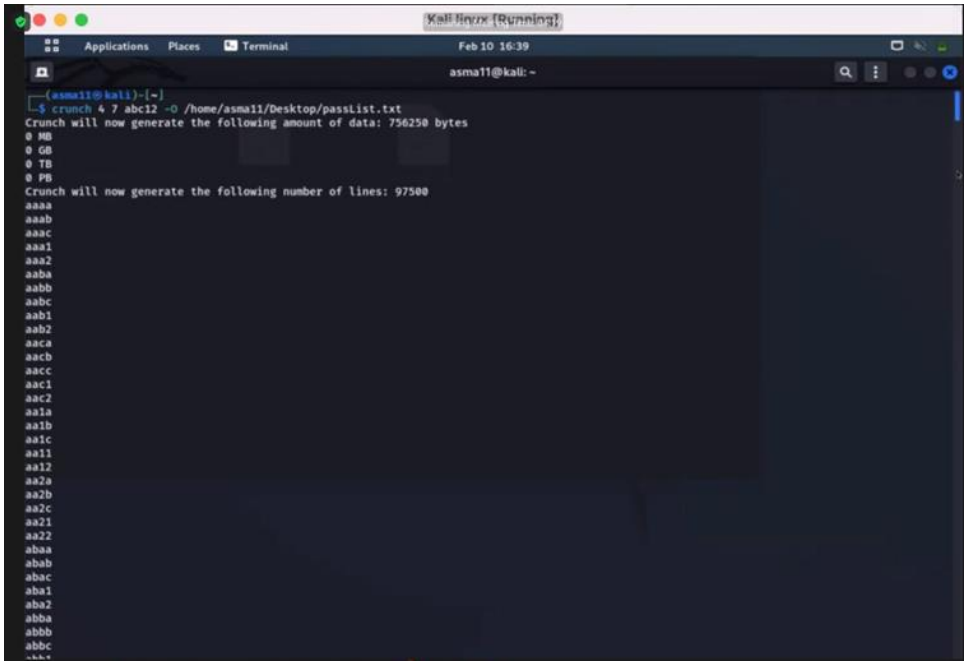

Figure 19 User.text

User.text

File contains usernames that we have created.

4.1.2

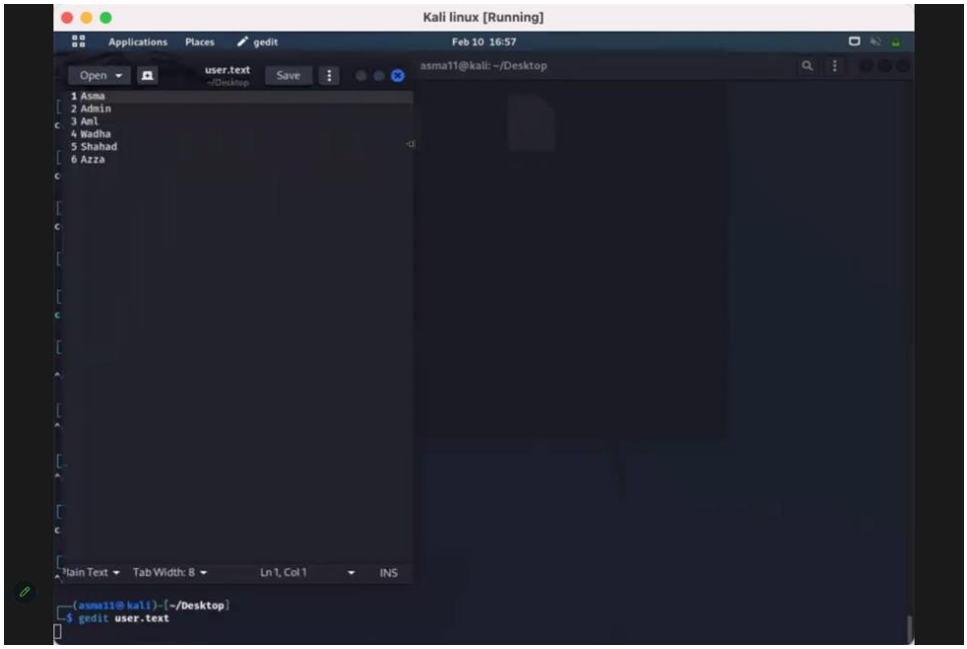

Figure 20 Password.text

Password.text

File continues passwords that we have created.

4.1.3

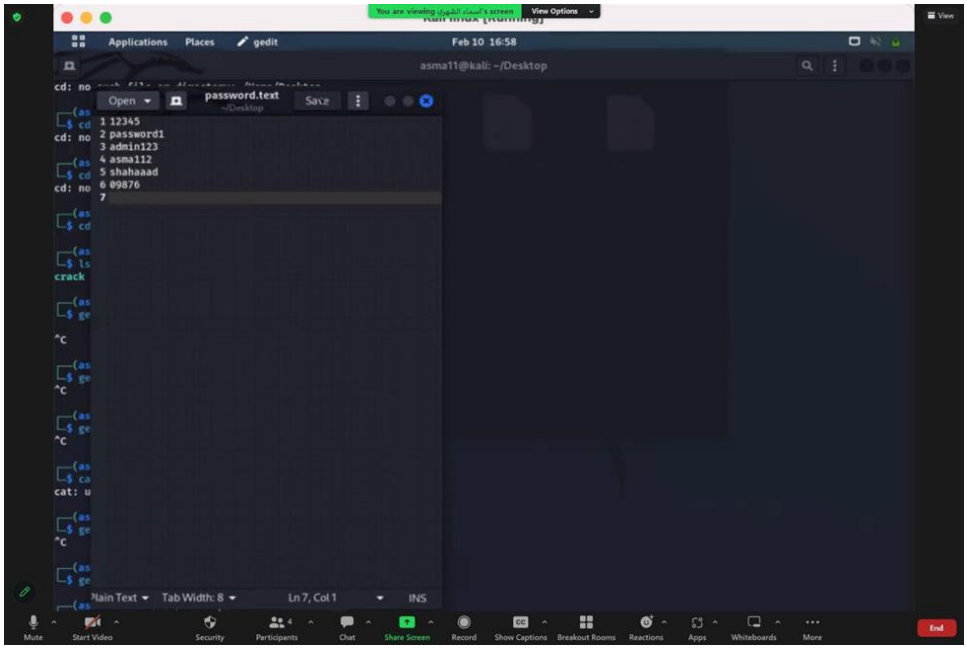

Figure 21

Here we have attacked the files

4.1.4

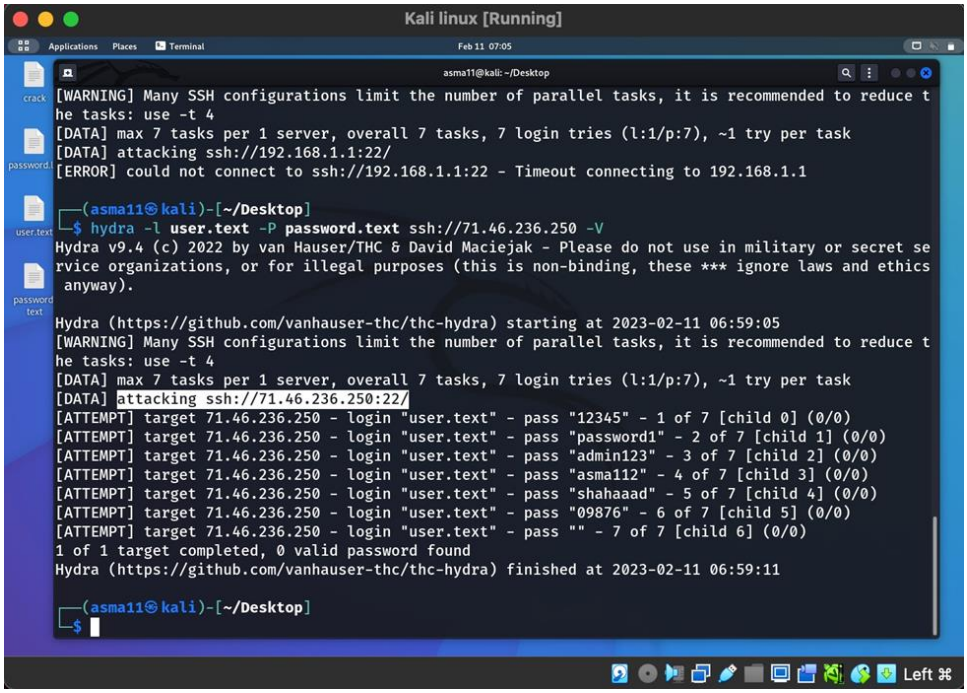

Figure 22

We selected User.text and Password.text and the chosen target which is ssh//71.46.236.250 which is the port of a server that we initially took form Nmap. When we used the tool nmap and saw what ports are closed and which are open . the address was closed but we have opened it in Nmap, then we contained to hydra and we started the attack which is the command bellow.

The attack succeeded and we successfully have password that are inside the server ssh//71.46.236.250 .

We tried to enter a username “asma112” and used the file Password.text and then hydra started guessing the password of “asma112”. hydray test the possibility of the password being “asma112” same as the username . also the possibility of the password being in reveres “211amsa” ” until a match is found .

Hydra -l user.text -p password.text ssh//71.46.236.250 -v

Here we have opened the close port ssh//71.46.236.250 successfully

4.1.5

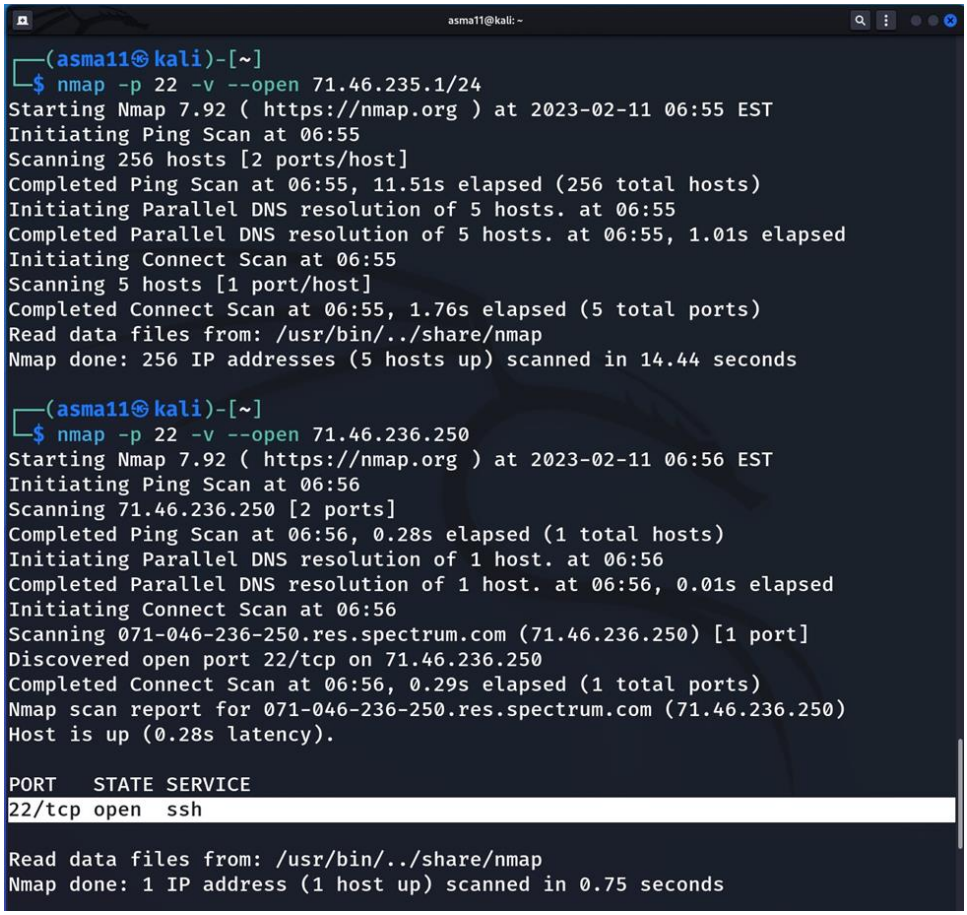

Figure 23

4.2 Hydra Commands

There are various commands that Hydra establish to users, the table low shows commonly used commands with illustration of its usage

Command	Usage	Written as
crunch	Generator used to specify the number of characters that will be used	$ crunch
-p	Used as a password list	-p
-l	Used as login	-l

Table: Hydra commands

4.3 Hydra Results and analysis

-Showcase a username and password from a test file we've created.

-use of Brutal force attack on a file.

-guessing the password of a creature file.

4.4 Hydra Countermeasures

- Enforcment of complex password policy on the system, so password can't be easily guessed .
- No use of personal information as a password like name, birthday to avoid hacking.
- If leaks happened, then user must be informed that the password used is a leaky password.
- No unsegment of the same password across different systems, so if one got leaked all other systems can be easily hacked.
- Provent the use of popular password like "123" in critical systems like a bank
- Change of the password frequently every three months.
- Usage of long password can minimize the brutal force attack on the system.
- Limitation of password attempt and logout of the account after many unsuccessful attempts.

5. Conclusion

The project aimed on discovering and analyzing the performance of Kali Linux tools which are Namp, SQLmap and Hydra. Each of these tool falls in a specific category, Nmap which is a tool used for information gathering, SQLmap which is a tool used in databases and Hydra, a password cracking tool. Each of these tools were defined and discussed by its features and countermeasures. The tools were also tested for its use using different commands.

6. References

[1]: S. Ali, L. Allen, and T. Heriyanto, *Kali Linux assuring security by Penetration Testing: Mastering the art of penetration testing with Kali Linux*. Birmingham: Packt Publishing, 2014.

[2]: *https://nmap.org/*. [Online]. Available: https://nmap.org/

[3]: *Firewall/IDS Evasion and Spoofing | Nmap Network Scanning*. [Online]. Available: https://nmap.org/book/man-bypass-firewalls-ids.html

[4] :"Sqlmap®," *sqlmap*. [Online]. Available: https://sqlmap.org/. [Accessed: 11-Feb-2023].

[5]: "How to defend your business against SQL Injections," *Logz.io*, 01-Nov-2021. [Online]. Available: https://logz.io/blog/defend-against-sql-injections/. [Accessed: 11-Feb-2023].

[6] "Kali Linux - password cracking tools," *TutorialsPoint*, 28-Jul-2021. [Online]. Available: https://www.tutorialspoint.com/kali_linux/kali_linux_password_cracking_tools.htm. [Accessed: 11-Feb-2023].