



Comp Data Security & Privacy Course Project

"Academic Year (2022-2023) – Second Semester"

Team Members:

Fida M. Alelou

Ghala M. Alkhaldi

May M. AlOtaibi

Supervised by:

Dr. Azza Abdo Ali

TABLE OF CONTENT

● Introduction	4
1. Nmap	4
1. Nmap Used procedure.	5
2. Nmap Result and Analysis	7
3. Nmap Countermeasures	7
2. John	8
1. John Used procedure.	12
2. John Result and Analysis	12
3. John Countermeasures	13
3. Nikto	
1. Nikto Used procedure.	
2. Nikto Result and Analysis	
3. Nikto Countermeasures	
● Conclusion	
● References	

TABLE OF FIGURES

Figure 1: Information gathering-Nmap	5
Figure 2: IP address	6
Figure 3: Devices in network	6
Figure 4: Scanning google.com	7
Figure 5: hash-identifier icon	8
Figure 6: hash type of first password	8
Figure 7: create text file	9
Figure 8: hash of the first password	9
Figure 9: crack result of the first password	9
Figure 10: hash type of second password	10
Figure 11: hash of the second password	10
Figure 12: crack result of the second password	11
Figure 13: hash type of third password	11
Figure 14: hash of the third password	12
Figure 15: crack result of the third password	12
Figure 16: crack result of the first password	12
Figure 17: crack result of the second password	13
Figure 18: crack result of the third password	13
Figure 19: Nikto Command	15
Figure 20 Opening Nikto Tool	16
Figure 21 Testing Website	17
Figure 22: Saving the result	17
Figure 23: Vulnerabilities Report	18
Figure 24: 'X-XSS-Protection' Header	18
Figure25: Missing anti-clickjacking	18

Introduction

An operating system was required to evaluate penetrations because modern hacking techniques have advanced and improved with the advancement of technology. Kali Linux was made available in 2013. For security-related needs, Kali Linux is the most popular operating system. The operating system Kali Linux, which is based on Ubuntu, was created for penetration testing. The user can test the infiltration of a collection of devices and networks using a set of tools that are included. Three tools, namely John, Nmap, and Nikto, have been examined and applied in this project.

Information gathering:

Information gathering is a stage taken by a hacker or penetration tester in conducting penetration tests. In this stage, hackers are required to find information about the victim.

1. Nmap

Network Mapper is referred to as Nmap. Nmap in Kali Linux refers to an open-source tool that penetration testers frequently utilize for network discovery and system security assessments. Nmap can be used by users for a variety of tasks, such as network inventory, service availability monitoring, schedule management, and host monitoring. The hosts on a network, the services they offer, the operating systems they are running on, the types of packets or firewalls they utilize, and many other features are all determined by Nmap using new techniques^[1].

NMAP features [2]:

- The ability to easily identify every device on single or several networks, including servers, routers, switches, and mobile devices.
- Determine the network's security vulnerabilities.
- Host discovery.
- OS detection.
- Can find details about the operating system that is present on a device. During a penetration test, it can provide specific details like OS versions, making it simpler to prepare additional strategies.

There are various commands in Nmap that are commonly used, such as:

1. # basic command nmap
sudo nmap <ip target>
2. # basic command nmap for scanning port
sudo nmap -P <ip target>
3. # basic command nmap for scanning operating system
sudo nmap -O <ip target>
4. # basic command nmap for fast scanning port
sudo nmap -sS <ip target>

1.1 Nmap Used procedure

Step 1:

You can find the list of tools by entering the virtual box and starting Kali Linux. will find the Nmap tool under the section for information gathering, as shown in figure 1.

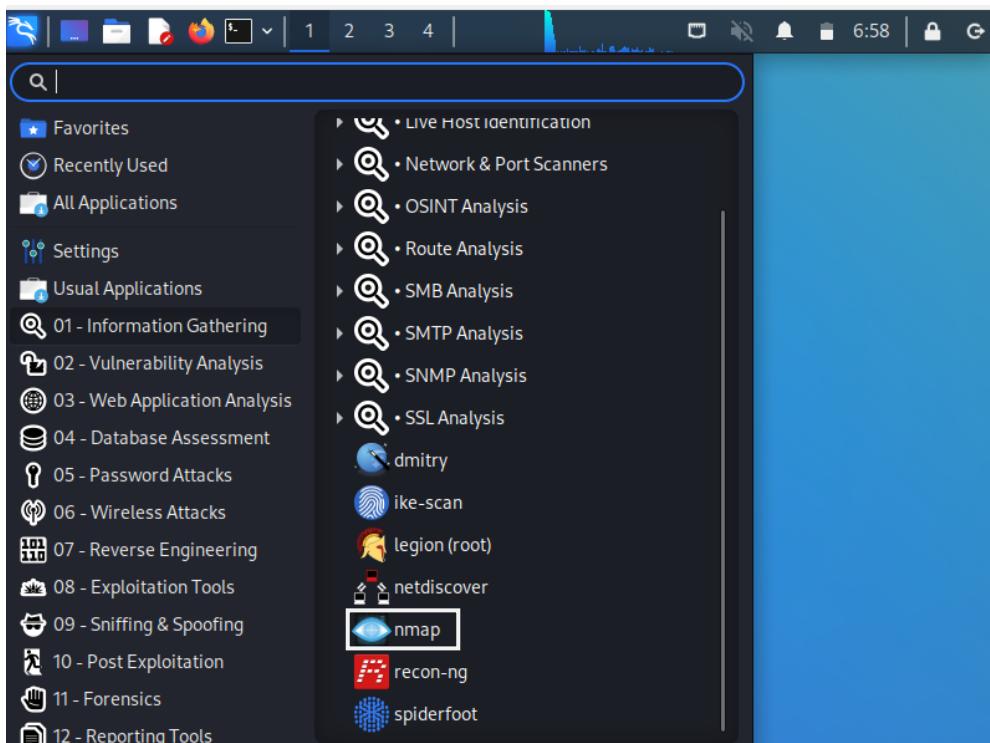
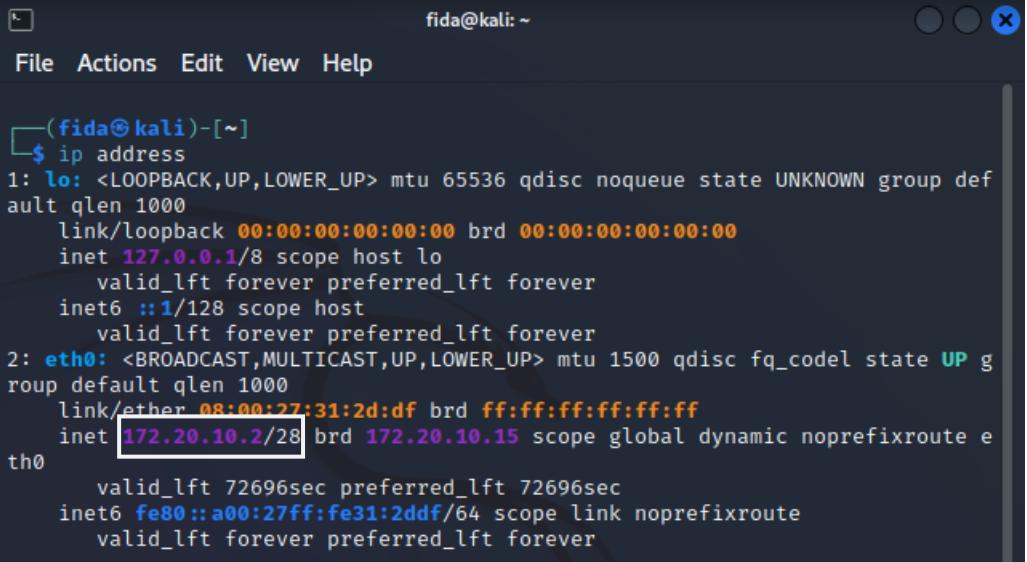


Figure 1: Information gathering-Nmap.

Step 2:

To determine the network's IP address, then determine how many devices are connected to it and show more details about these. Go to the computer's terminal, and then execute the command (IP address) as shown in figure 2. Therefore, the network's devices will be discovered using the IP address 172.20.10.2/28.

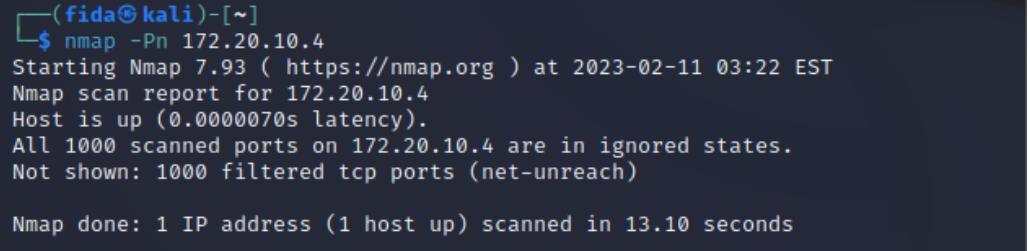


```
(fida㉿kali)-[~]
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:31:2d:df brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.2/28 brd 172.20.10.15 scope global dynamic noprefixroute eth0
        valid_lft 72696sec preferred_lft 72696sec
    inet6 fe80::a00:27ff:fe31:2ddf/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Figure 2: IP address

Step 3:

Now, will use a command that shows more details about devices that connect to the network and ports (nmap 172.20.10.4) However, here simply require to know how many active devices there are and their IP addresses as shown in figure 3.



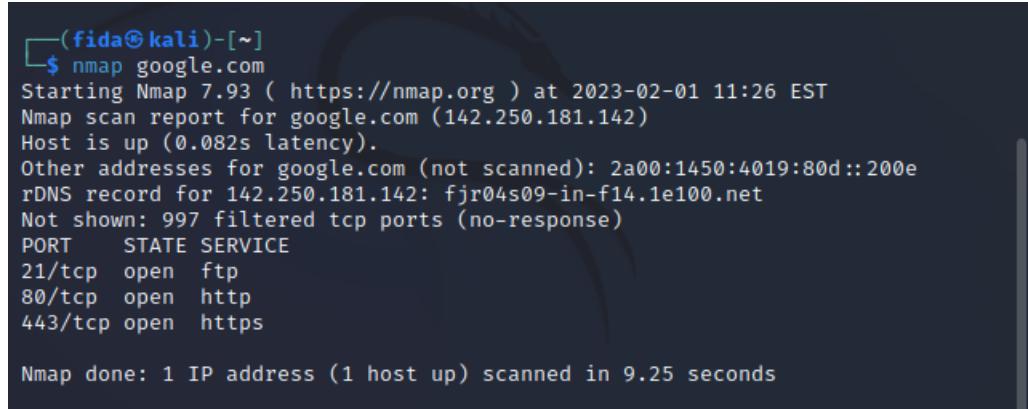
```
(fida㉿kali)-[~]
$ nmap -Pn 172.20.10.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 03:22 EST
Nmap scan report for 172.20.10.4
Host is up (0.0000070s latency).
All 1000 scanned ports on 172.20.10.4 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

Figure 3: Devices in network

1.2 Nmap Result and Analysis

Google.com will be scanned using Nmap in figure 4. Use the command to achieve that (nmap google.com). All host information, including the reverse DNS name (rDNS), and the ports with service names, will be provided by the scan. Notice that each port has a state.



```
(fida㉿kali)-[~]
$ nmap google.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-01 11:26 EST
Nmap scan report for google.com (142.250.181.142)
Host is up (0.082s latency).
Other addresses for google.com (not scanned): 2a00:1450:4019:80d::200e
rDNS record for 142.250.181.142: fjr04s09-in-f14.1e100.net
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

Figure 4: Scanning google.com.

Nmap categorizes ports into different states [3]:

As shown in the picture, the state of ports is **open**, which means that the service is currently active and ready to connect.

closed: means that no services were active on this port.

Unfiltered: The port is reachable, but nmap cannot determine if it is open or closed.

Filtered: This shows that a firewall or packet filter is preventing nmap from determining whether the port is open.

1.3 Nmap Countermeasures

One of the most common methods of research before a hack is port scanning, which enables attackers to identify the ports that are most vulnerable. A hacker could gain access to your network or steal confidential information by using port scanning. There are various things you can take to minimize being scanned to prevent attackers from using Nmap to scan your network, such as:

1. Perform the port scan before the attacker: Running frequent port scans on your network to detect susceptible ports and block them is the first step in preventing bad actors from entering your network through a port scan assault.
2. One of the strongest defenses against scanning is installing a firewall. Unauthorized access to your private network is helped by a firewall. controls the visibility and exposure of the ports as well. Additionally, firewalls have the ability to recognize and stop active port scans.

2. John

John the Ripper is an open-source software that combines several cracking programs into one tool that runs both brute force and dictionary attack. Initially released for UNIX-based systems, but it has now been ported to a variety of operating systems by means of a CML (Command Line Interface). Additionally, Enterprises often use John the Ripper to detect weak passwords, which could compromise network security, as well as other administrative purposes. This software can crack passwords on a variety of operating systems and can be scripted to execute locally or remotely.

Features:

- Support a wide range of password hashes
 - Uses the password hash rather than the file itself
 - Various platforms are available for cracker to continue their cracking session
 - Particularly efficient when combined with open-source wordlists such as seclists

2.1 John Used Procedure

First password

Step 1:

Check the type of hash from “hash-identifier”. As shown in **Figure 6**, the hash is MD5.

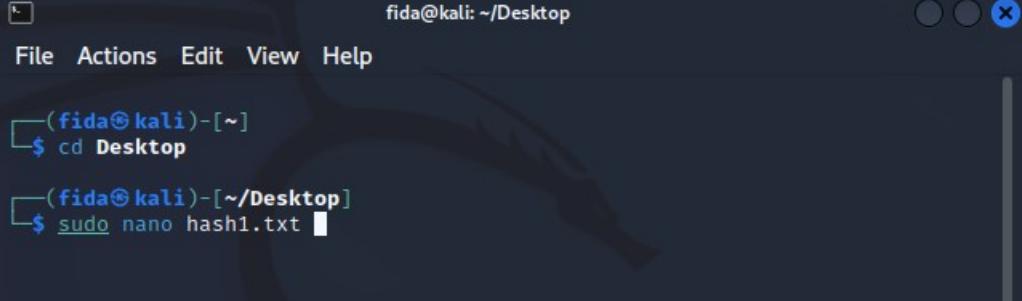


Figure 5: hash-identifier icon

Figure 6: hash type of first password

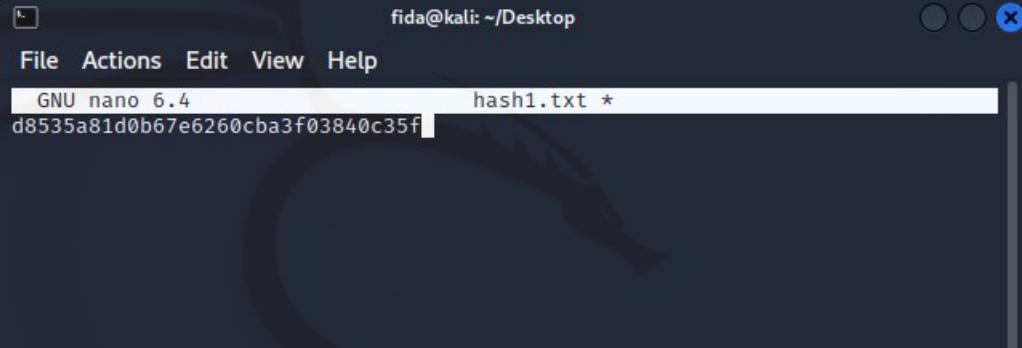
Step 2:

Create a text file and store the hash in it. As shown in **Figure 7**, file created on the desktop with the name "hash1.txt".



```
fida@kali: ~/Desktop
File Actions Edit View Help
(fida@kali)-[~]
$ cd Desktop
(fida@kali)-[~/Desktop]
$ sudo nano hash1.txt
```

Figure 7: create text file

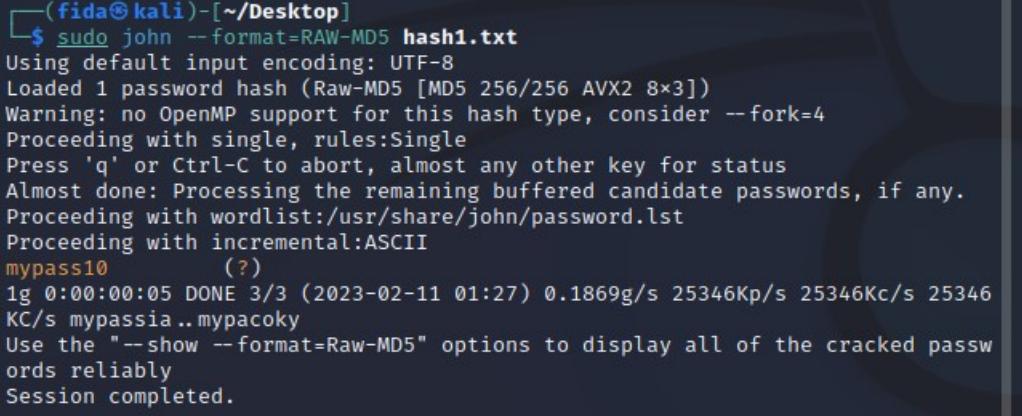


```
fida@kali: ~/Desktop
File Actions Edit View Help
GNU nano 6.4          hash1.txt *
d8535a81d0b67e6260cba3f03840c35f
```

Figure 8: hash of the first password

Step 3:

To crack the hash, we use the command “sudo john –format=RAW-MD5 hash1.txt”. As shown in **Figure 9**.



```
(fida@kali)-[~/Desktop]
$ sudo john --format=RAW-MD5 hash1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
mypass10      (?)
1g 0:00:00:05 DONE 3/3 (2023-02-11 01:27) 0.1869g/s 25346Kp/s 25346Kc/s 25346
KC/s mypassia..mypacoky
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Figure 9: crack result of first password

Second password

Step 1:

Check the type of hash from “hash-identifier”. As shown in **Figure 10**, the hash is MD5.

Figure 10: hash type of second password

Step 2:

Create a text file and store the hash in it. As shown in **Figure 11**, file created on the desktop with the name "hash2.txt".

```
fida@kali: ~/Desktop
File Actions Edit View Help
GNU nano 6.4          hash2.txt *
8b1a9953c4611296a827abf8c47804d7
```

Figure 11: hash of the second password

Step 3:

To crack the hash, we use the command “`sudo john –format=RAW-MD5 hash2.txt`”. As shown in **Figure 12**.

```
[fida㉿kali)-[~/Desktop]
$ sudo john --format=RAW-MD5 hash2.txt.save
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Hello          (?)
1g 0:00:00:00 DONE 2/3 (2023-02-11 04:44) 100.0g/s 345600p/s 345600c/s 345600
C/s modem..OU812
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.
```

Figure 12: crack result of second password

Third password

Step 1:

Check the type of hash from “hash-identifier”. As shown in **Figure 13**, the hash is MD5.

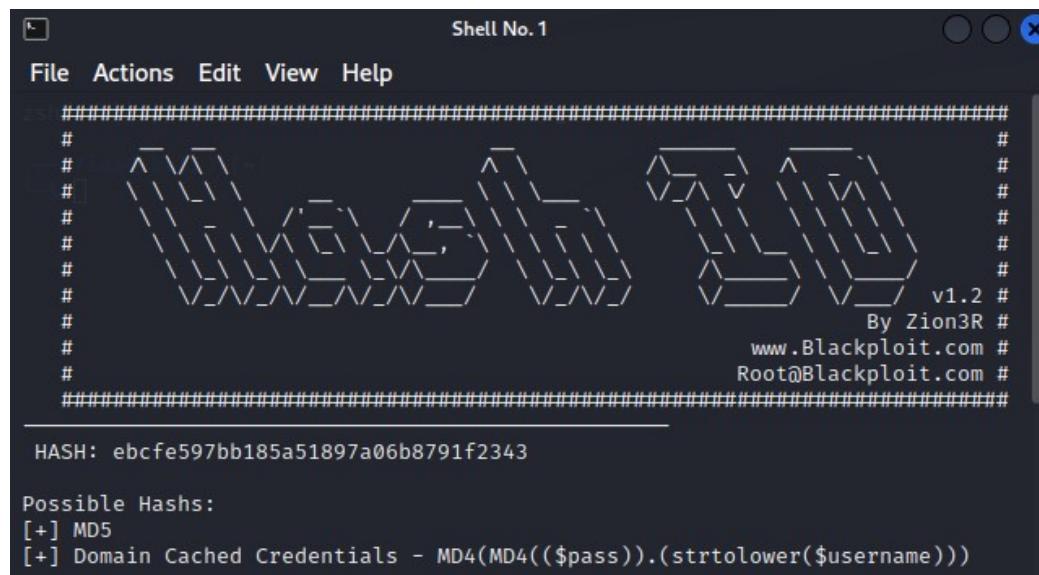
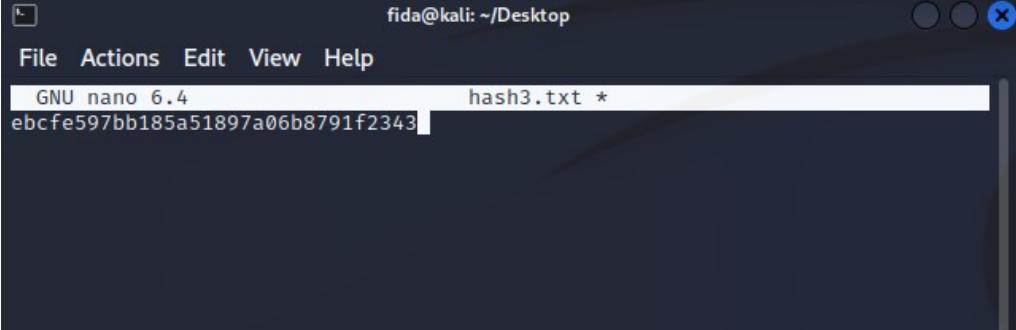


Figure 13: hash type of third password

Step 2:

Create a text file and store the hash in it. As shown in **Figure 14**, file created on the desktop with the name "hash3.txt".

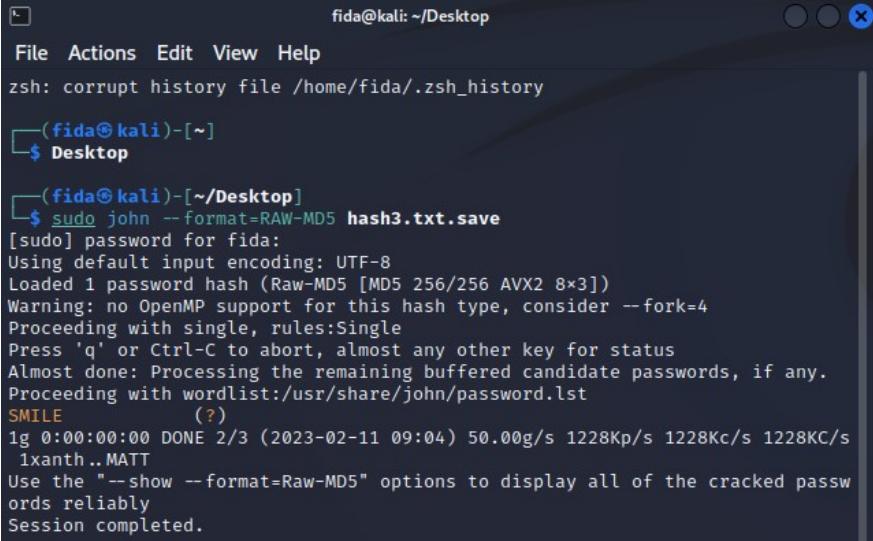


```
fida@kali: ~/Desktop
File Actions Edit View Help
GNU nano 6.4          hash3.txt *
ebcfe597bb185a51897a06b8791f2343
```

Figure 14: hash of the third password

Step 3:

To crack the hash, we use the command “sudo john –format=RAW-MD5 hash3.txt”. As shown in **Figure 15**.



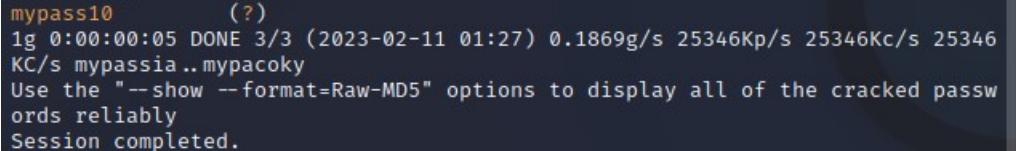
```
fida@kali: ~/Desktop
File Actions Edit View Help
zsh: corrupt history file /home/fida/.zsh_history
[(fida㉿kali)-[~]
$ Desktop
[(fida㉿kali)-[~/Desktop]
$ sudo john --format=RAW-MD5 hash3.txt.save
[sudo] password for fida:
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
SMILE      (?)
1g 0:00:00:00 DONE 2/3 (2023-02-11 09:04) 50.00g/s 1228Kp/s 1228Kc/s 1228KC/s
  ixanth..MATT
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Figure 15: crack result of third password

2.2 John Result and Analysis

First password

As shown in **Figure 16**, John the ripper cracks the first password which is mypass10 at 25346Kp/s.



```
mypass10      (?)
1g 0:00:00:05 DONE 3/3 (2023-02-11 01:27) 0.1869g/s 25346Kp/s 25346Kc/s 25346
KC/s mypassia..mypacoky
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Figure 16: crack result of first password

Second password

As shown in **Figure 17**, John the ripper cracks the first password which is **Hello** at 345600p/s.

```
Hello          (?)
1g 0:00:00:00 DONE 2/3 (2023-02-11 04:44) 100.0g/s 345600p/s 345600c/s 345600
C/s modem..OU812
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Figure 17: crack result of second password

Third password

As shown in **Figure 18**, John the ripper cracks the first password which is **SMILE** at 1228Kp/s.

```
SMILE          (?)
1g 0:00:00:00 DONE 2/3 (2023-02-11 09:04) 50.00g/s 1228Kp/s 1228Kc/s 1228KC/s
1xanth..MATT
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Figure 18: crack result of third password

Based on the previous results, Jhon the ripper took longer to crack the passwords as the difficulty increased.

2.3 John Countermeasures

To prevent attackers from cracking the password using john the ripper, the user must make sure of the following:

- Use password that has more than 12 characters
- Use a combination of numbers, capital and lowercase letters, and special character like #, _, \$, @
- Don't use your personal information (name/birth date/phone number) in the password
- Don't share your password
- Don't use the same password in different application
- Change the password regularly

For developers:

- Ensure that users do not use simple and guessable passwords.
- The password hash should include salt.

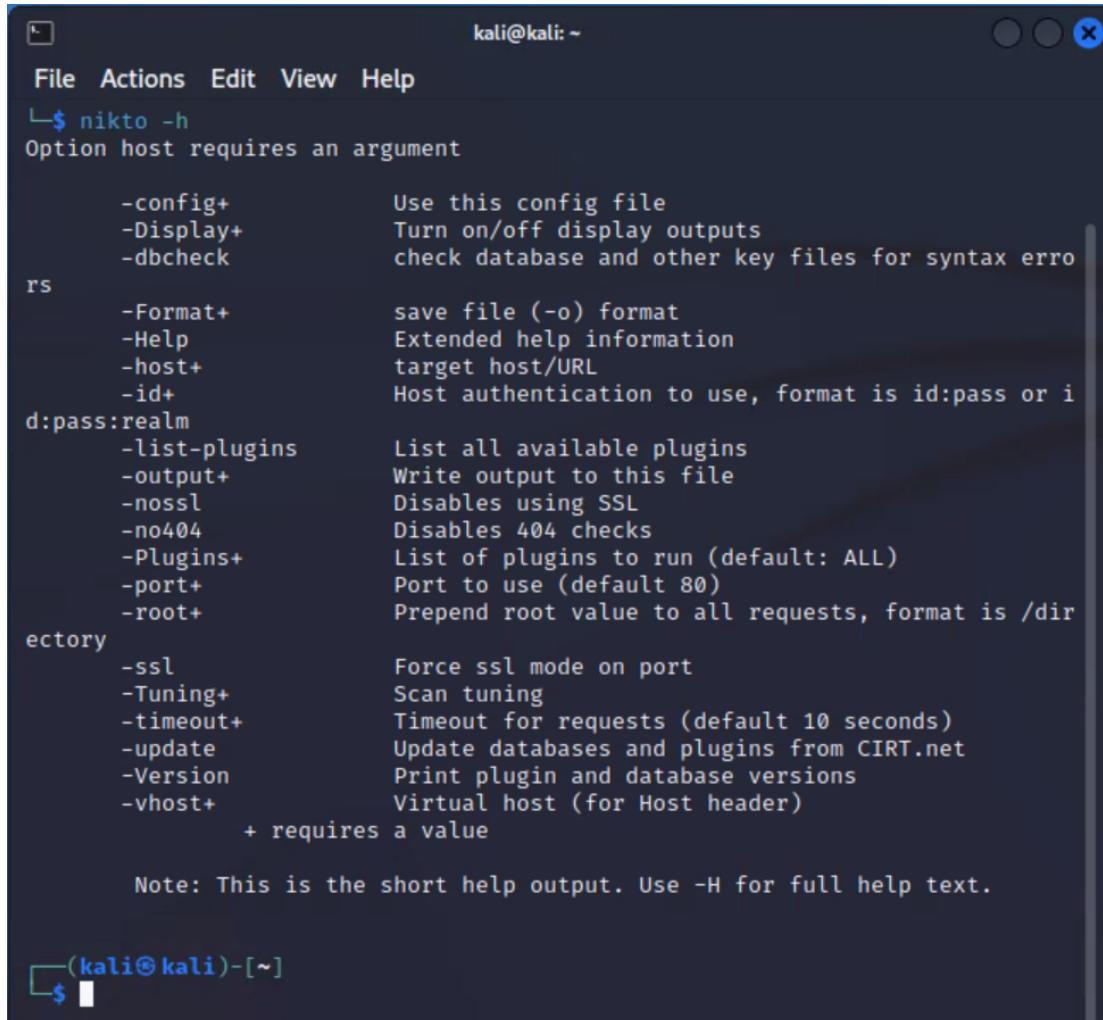
3. Nikto

An exploitable vulnerability on a website can be found using this tool, which is written in the Perl language. It scans and examines websites and web apps, reporting any vulnerabilities that can be exploited to exploit the site. Additionally, it can detect faults with specific version information on more than 200 servers and check for vulnerabilities with outdated version details on 1200 servers.

Features:

- Full support for SSL
- Gives details of installed software
- Supports full HTTP Proxy
- Updated easily
- Result saved in multiple format

Nikto tool is installed when we are dealing with Kali Linux, and we can run the tool from the device as shown in the figure below:



```

kali@kali: ~
File Actions Edit View Help
└$ nikto -h
Option host requires an argument

      -config+          Use this config file
      -Display+         Turn on/off display outputs
      -dbcheck          check database and other key files for syntax errors
      -Format+          save file (-o) format
      -Help              Extended help information
      -host+             target host/URL
      -id+               Host authentication to use, format is id:pass or id:pass:realm
      -list-plugins     List all available plugins
      -output+           Write output to this file
      -noSSL            Disables using SSL
      -no404            Disables 404 checks
      -Plugins+          List of plugins to run (default: ALL)
      -port+             Port to use (default 80)
      -root+             Prepend root value to all requests, format is /directory
      -ssl               Force ssl mode on port
      -Tuning+           Scan tuning
      -timeout+          Timeout for requests (default 10 seconds)
      -update             Update databases and plugins from CIRT.net
      -Version            Print plugin and database versions
      -vhost+             Virtual host (for Host header)
      + requires a value

      Note: This is the short help output. Use -H for full help text.

(kali㉿kali)-[~]
└$ 

```

Figure 19: Nikto Command

3.1 Nikto Used Procedure

With the following steps, we will explain how to use the Nikto tool to scan websites for vulnerabilities:

Step 1:

We download Kali Linux on the device so that we can open the tool through the steps shown in Figure 20.

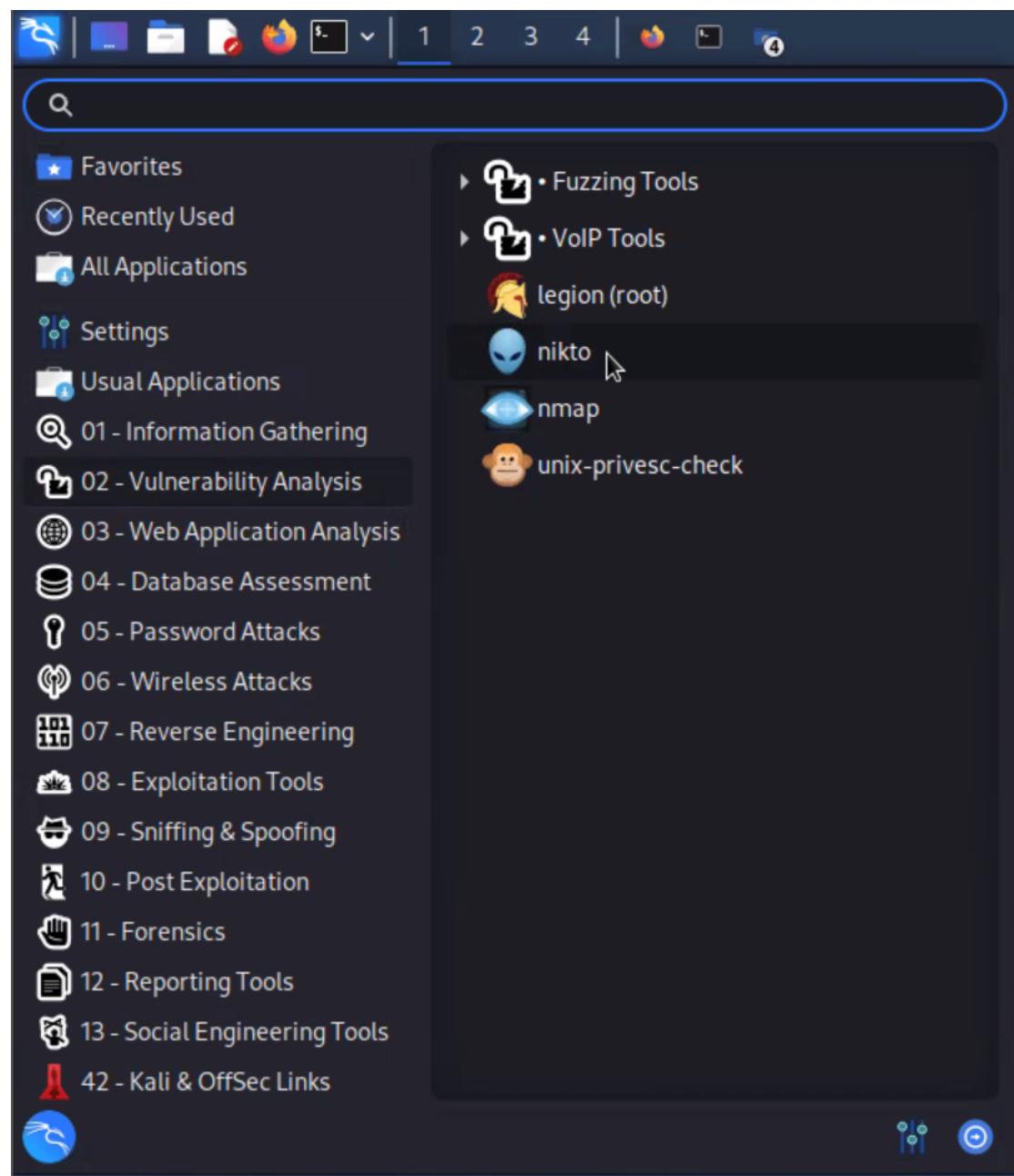


Figure 20: Opening Nikto Tool

Step 2:

In this step, the vulnerabilities encountered by testphp.vulnweb.com will be tested using the command shown in Figure 21.

By using this command:(nikto -h <IP or hostname>).

```
(kali㉿kali)-[~]
└─$ nikto -h testphp.vulnweb.com
- Nikto v2.1.6

+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2023-02-11 10:39:43 (GMT-5)

+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ /clientaccesspolicy.xml contains a full wildcard entry. See http://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 7 item(s) reported on remote host
+ End Time:         2023-02-11 10:42:16 (GMT-5) (153 seconds)

+ 1 host(s) tested

(kali㉿kali)-[~]
└─$
```

Figure 21: Testing Website

Step 3:

In this step, as shown in Figure 22, we will save the results to a file (html) on the desktop so that we can analyze the results.

```
(kali㉿kali)-[~]
└─$ nikto -h testphp.vulnweb.com -o Desktop/TestNikto.html
- Nikto v2.1.6
```

Figure 22: Saving the result

3.2 Nikto Result and Analysis

testphp.vulnweb.com / 44.228.249.3 port 80	
Target IP	44.228.249.3
Target hostname	testphp.vulnweb.com
Target Port	80
HTTP Server	nginx/1.19.0
Site Link (Name)	http://testshop.vulnweb.com:80/
Site Link (IP)	http://44.228.249.3:80/
URI	/
HTTP Method	GET
Description	Received x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Test Links	http://testshop.vulnweb.com:80/ http://44.228.249.3:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://testshop.vulnweb.com:80/ http://44.228.249.3:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://testshop.vulnweb.com:80/ http://44.228.249.3:80/
OSVDB Entries	OSVDB-0
URI	/clientaccesspolicy.xml
HTTP Method	GET

Figure 23: Vulnerabilities Report

We opened the vulnerability report on the site testphp.vulnweb.com a vulnerability in the image below caught our attention.

URI	/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://testshop.vulnweb.com:80/ http://44.228.249.3:80/
OSVDB Entries	OSVDB-0

Figure 24: 'X-XSS-Protection' Header

Synopsis: Missing 'X-XSS-Protection' Header.

Description: As a result, any pages on this website could be vulnerable to Cross-Site Scripting (XSS) attacks since the server does not return a 'X-XSS-Protection' header.

Also, there is another vulnerability is that the website's header does not have an anti-clickjacking X-Frame option.

URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://testshop.vulnweb.com:80/ http://44.228.249.3:80/
OSVDB Entries	OSVDB-0

Figure 24: Missing anti-clickjacking

Synopsis: Missing anti-clickjacking X-Frame option.

Description: This website could be vulnerable to clickjacking attacks because X-Frame-Options is missing. In HTTP header field X-Frame-Options, the browser specifies whether a frame or an iframe should be used for rendering the transmitted resource.

3.3 Nikto Countermeasures

To avoid clickjacking attacks, developers can add the X-frame option to the header and specify one of the following three options:

- Deny which means when the user clicks on the frame, they cannot go to anywhere.
- Sameorigin means that if the website that has been specified in the code from the same origin of the website that the user clicks on, it will immediately go to the desired page.
- Allow-From means the developer can specify a certain URL, so when the user clicks on the frame, it will go to that website.

References

- Nmap Commands in Kali Linux - javatpoint* (no date) [www.javatpoint.com](http://www.javatpoint.com/nmap-commands-in-kali-linux#:~:text=In%20Kali%20Linux%2C%20Nmap%20means,schedules%2C%20host%20monitoring%2C%20etc). Available at: <https://www.javatpoint.com/nmap-commands-in-kali-linux#:~:text=In%20Kali%20Linux%2C%20Nmap%20means,schedules%2C%20host%20monitoring%2C%20etc> (Accessed: February 1, 2023).
- Shea, S. (2022) *How to use nmap to scan for Open Ports*: TechTarget, Security. TechTarget. Available at: <https://www.techtarget.com/searchsecurity/feature/How-to-use-Nmap-to-scan-for-open-ports> (Accessed: February 1, 2023).
- Shivanandhan, M. (2020) *What is nmap and how to use it – a tutorial for the greatest scanning tool of all time*, freeCodeCamp.org. freeCodeCamp.org. Available at: <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/> (Accessed: February 1, 2023).