|  |
| --- |
| Kingdom of Saudi Arabia  Ministry of Education  Imam Abdulrahman bin Faisal University  Computer Science department  College of Science and Humanities |



**CIS425- Comp Data Security & Privacy Project**

CIS Year 4, G2

Dr. Azza Abdo Ali

*11 February 2023*

**Content:**

[**List of figures:** 3](#_Toc127036984)

[**List of tabels:** 3](#_Toc127036985)

[**Introduction:** 5](#_Toc127036986)

[**1.** **Nmap** 5](#_Toc127036987)

[**1.1** **Nmap Used procedure** 6](#_Toc127036988)

[**1.2 Nmap Result and Analysis** 7](#_Toc127036989)

[**1.3** **Nmap Countermeasures** 8](#_Toc127036990)

[**2.** **Hydra** 9](#_Toc127036991)

[**2.1 Hydra Used procedure** 9](#_Toc127036992)

[**2.2 Hydra Result and Analysis** 14](#_Toc127036993)

[**2.3** **Hydra Countermeasures** 14](#_Toc127036994)

[**3.** **Nikto** 15](#_Toc127036995)

[**3.1 Nikto Used procedure** 16](#_Toc127036996)

[**3.2 Nikto Result and Analysis** 19](#_Toc127036997)

[**3.3 Nikto Countermeasures** 21](#_Toc127036998)

[**Conclusion:** 22](#_Toc127036999)

[**Reference:** 23](#_Toc127037000)

# **List of figures:**

[Figure 1:Opening Nmap in Kali Linux 6](#_Toc127037001)

[Figure 2: Finding the Ip address 6](#_Toc127037002)

[Figure 3: Finding all the devices in the network 7](#_Toc127037003)

[Figure 4: Scanning scanme.nmap.org website 7](#_Toc127037004)

[Figure 5: Downloading DVWA web server 9](#_Toc127037005)

[Figure 6: DVWA configuration file 9](#_Toc127037006)

[Figure 7: Activating DVWA database 10](#_Toc127037007)

[Figure 8: DVWA login page 10](#_Toc127037008)

[Figure 9: Login error 11](#_Toc127037009)

[Figure 10: Login page source view 11](#_Toc127037010)

[Figure 11: Usernames file 12](#_Toc127037011)

[Figure 12: Password file 12](#_Toc127037012)

[Figure 13: Hydra command execution 12](#_Toc127037013)

[Figure 14: Hydra command result 13](#_Toc127037014)

[Figure 15: Login attempt 13](#_Toc127037015)

[Figure 16: Launching the website successfully 13](#_Toc127037016)

[Figure 17: Nikto commands 15](#_Toc127037017)

[Figure 18: How to open Nikto 16](#_Toc127037018)

[Figure 19: Testing tastphp.Vulnweb.com website 17](#_Toc127037019)

[Figure 20: How to save result file as HTML document 18](#_Toc127037020)

[Figure 21: Opening HTML file 18](#_Toc127037021)

[Figure 22: The vulnerabilities report 19](#_Toc127037022)

[Figure 23: Anti-clickjacking X-Frame-Option vulnerability 19](#_Toc127037023)

[Figure 24: X-Content-Type-Option vulnerability 20](#_Toc127037024)

[Figure 25: How to set X-frame option to the header 21](#_Toc127037025)

[Figure 26: How to set X-frame option to the header 21](#_Toc127037026)

[Figure 27: Set the content type header 22](#_Toc127037027)

[Figure 28: Set the X-content-type option header 22](#_Toc127037028)

# **List of tabels:**

[Team members table 4](#_Toc127037031)

[Nmap commands table 5](#_Toc127037032)

**Team Members:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Leader** | **ID** | **Member Name** | **Email Address** |
| € | 2200004242 | Bushra Alshehri | 2200004242@iau.edu.sa |
| € | 2200006257 | Albandari Alsanhani | 2200006257@iau.edu.sa |
| € | 2200005678 | Dana Kurdi | 2200005678@iau.edu.sa |
| € | 2200006269 | Jumana Aljassim | 2200006269@iau.edu.sa |

### Team members table

# **Introduction:**

The Kali Linux operating system was released in 2013. In terms of security, Kali Linux is the most commonly used operating system. Ubuntu is the basis for Kali Linux. It was designed to be used for penetration testing. Various tools are provided so that the user can test a group of devices and networks. Nmap, Hydra, and Nikto are the tools used in this project. Also virtual box application is used to run Kili Linux.

# **Nmap**

Nmap is one of the tools used for information gathering, as it is free and open source. By using Nmap, you can determine which hosts are on your network, see what kind of firewalls are in place, find and exploit vulnerabilities, and identify operating systems. It is designed to scan large networks but also works with single hosts. Furthermore, Nmap comes with Zenmap, which is the same tool as Nmap, but uses a GUI instead of a command line.

**Nmap features [1]:**

* Without any advanced commands or configuration, Nmap can map out your network quickly.
* Recognize all the devices including servers, routers, etc on single / multiple networks.
* Support command line and GUI.
* Scan huge networks.
* Information about the device's operating system can Nmap found.
* Identify network vulnerabilities.

Common commands in Nmap [2]:

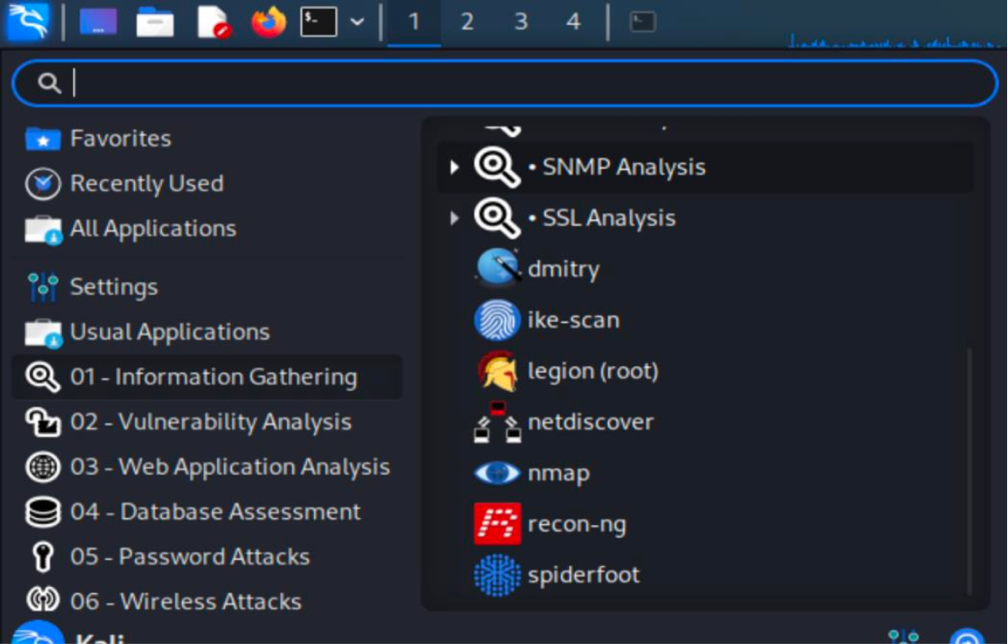
|  |  |  |
| --- | --- | --- |
| Goal | Command | Example |
| Scan a Single Target | nmap [target] | nmap 10.0.2.15 |
| OS Detection | nmap -O [target] | nmap -O 10.0.2.15 |
| Open Ports | nmap –open [target] | nmap –open 10.0.2.15 |
| Help | nmap -h | nmap -h |
| Nmap Version | nmap -V | nmap -V |

### Nmap commands table

# **Nmap Used procedure**

Step 1:

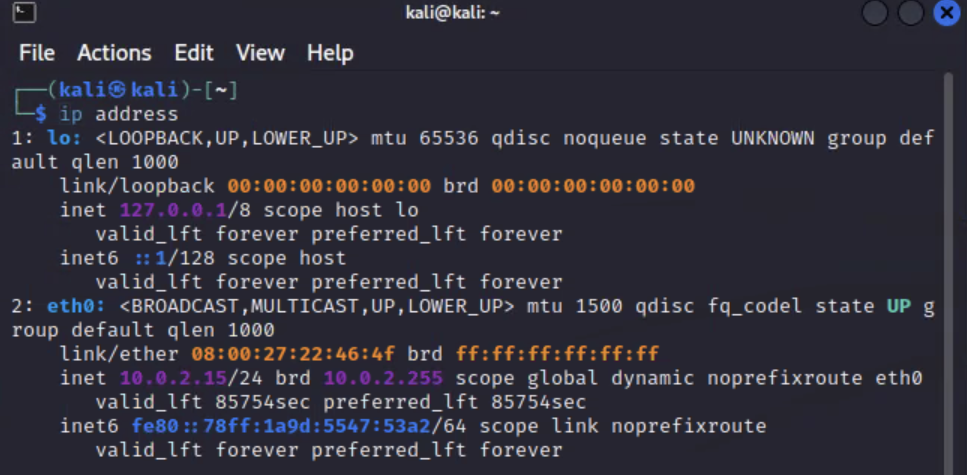
Firstly, we opened the Virtual box and running Kali Linux then from the application icon we found the list of tools. On figure (1) it shows the Nmap tool in the information gathering section.



## Figure 1:Opening Nmap in Kali Linux

Step 2:

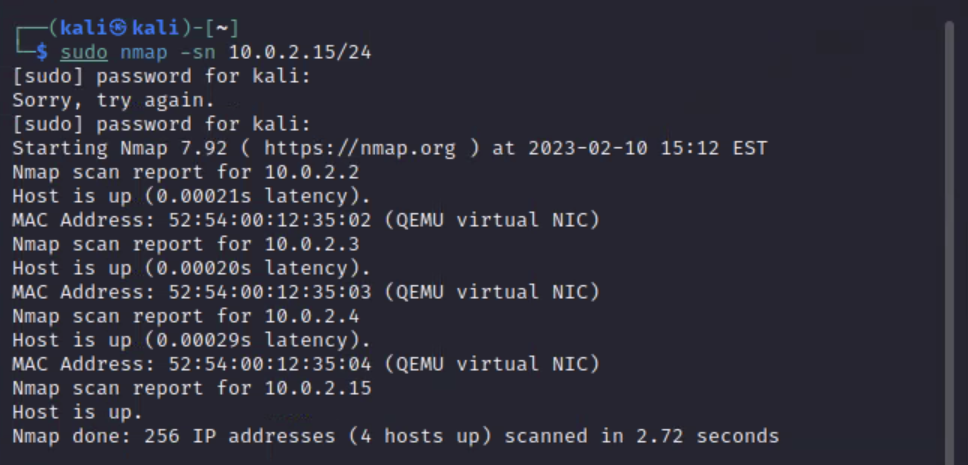
Discover how many devices run on the network and show more information about them based on the IP address of the network. Start by writing the command (ip address) in the terminal of the Kali Linux as shown in figure (2). In order to discover devices on the network, we used 10.0.2.15/24 as the IP address.



## Figure 2: Finding the Ip address

Step 3:

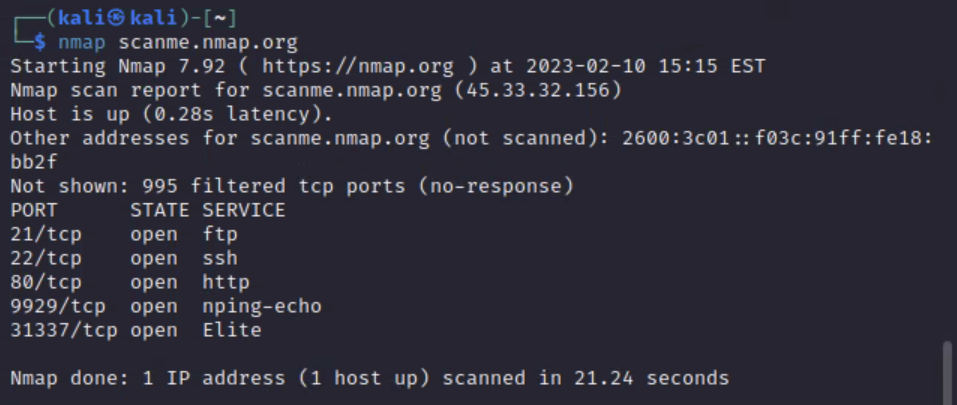
In this step we wrote the nmap -sn 10.0.2.15/24 command. This command shows more details about targets and ports. But as shown in figure (3) we just want to know how many devices are running and the Ip address of these devices.



## Figure 3: Finding all the devices in the network

# **1.2 Nmap Result and Analysis**

In figure (4) we used Nmap to scan the “scanme.nmap.org” website by using nmap target command. This command will provide all hosts data that include the IPv4 addresses, service names of the ports and revers DNS name. each port that displayed has its own state [3].



## Figure 4: Scanning scanme.nmap.org website

* **Open:** Open ports indicate an active service that is ready for connection.
* **Closed:** There was no service running on this port after the probes were received, so the port was closed.
* **Filtered:** In this case, nmap is unable to determine whether the port is open since packet filters and firewalls are blocking it.
* **Unfiltered:** Probes are unfiltered when they are received but the state cannot be determined.
* **Open/Filtered:** It indicates that the port was either filtered or open, but there could be no indication of its state.
* **Closed/Filtered:** It indicates that the port was either filtered or closed, but there could be no indication of its state.

# **Nmap Countermeasures**

The following methods can help you limit the number of times your network is scanned by attackers using nmap [4]:

* Firewall: The installation of a firewall can prevent unauthorized access to your private network. Visibility and exposure of exposed ports are controlled by it. It is also possible for firewalls to detect and shut down port scans in progress.
* TCP Wrappers: With TCP wrappers, administrators can restrict or allow IP addresses or domain names from accessing the servers.
* Uncover Holes in the Network: Check your internal ports for open ports beyond what is needed in order to uncover network holes. Identify existing weak points in your system and check them periodically.

# **Hydra**

Hydra is a parallel login cracker tool that supports multiple attack protocols. It is very fast and flexible, and new modules can be easily added.Using this tool, researchers and security consultants can demonstrate how easy it is to gain unauthorized access to systems remotely.[1][10]

Hydra is a brute force tool that helps penetration testers and ethical hackers crack passwords to web services.

Hydra can perform quick dictionary attacks against more than 50 protocols.

In a dictionary attack, we have one/multiple usernames and provide Hydra with a dictionary of passwords. Hydra then tests all of these passwords against each user in the list.[9]

# **2.1 Hydra Used procedure**

Text

Description automatically generated

## Figure 5: Downloading DVWA web server

**Step 2:** Save DVWA database configuration

Text

Description automatically generated

## Figure 6: DVWA configuration file

**Step 3:** Activate the DVWA database using the configuration information

Text

Description automatically generated

## Figure 7: Activating DVWA database

**Step 4:** Successfully launching the site login page in kali using the machine IP address

Graphical user interface, text, application

Description automatically generated

## Figure 8: DVWA login page

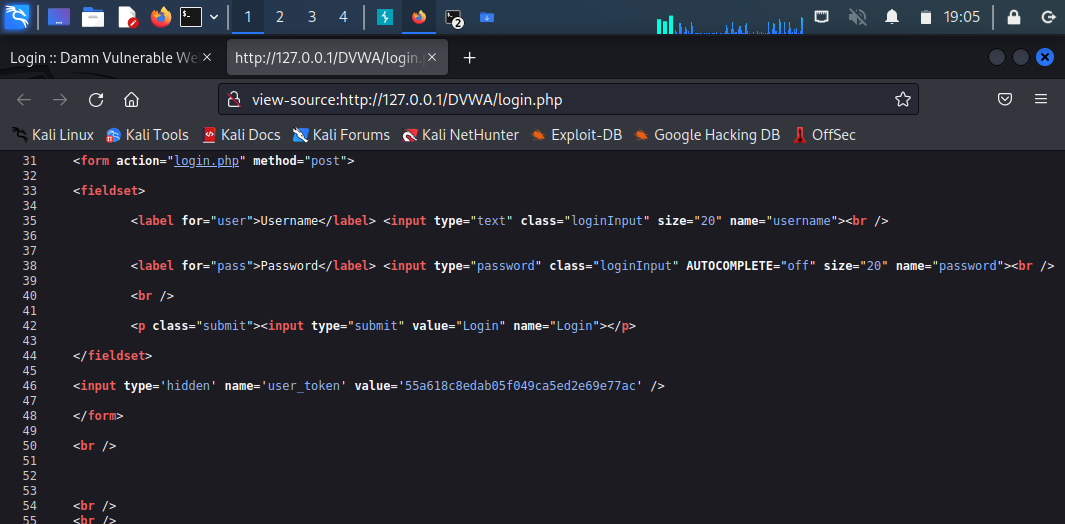
**Step 5:** Trying to log in with a random username and password

Graphical user interface, text, application, website

Description automatically generated

## Figure 9: Login error

**Step 6:** Opening the source page view for the login webpage which provides more information about the form. We can see the fields names of the inputs “username”,”password”, and “Login”



## Figure 10: Login page source view

**Step 7:** Create a file containing usernames and a file containing passwords

A screenshot of a computer

Description automatically generated with medium confidence

## Figure 11: Usernames file

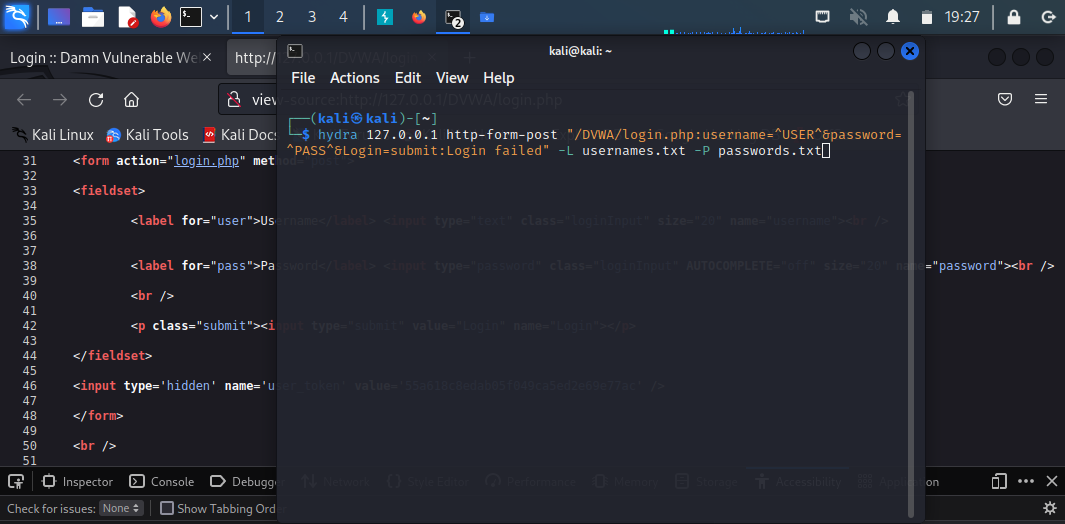
Graphical user interface, text, application

Description automatically generated

## Figure 12: Password file

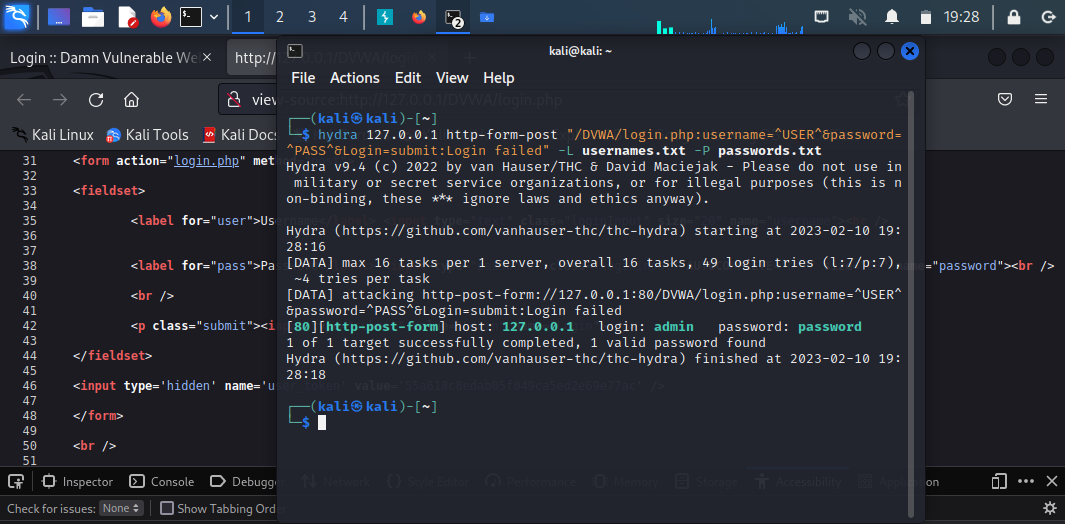
**Step 8:** Writing the hydra command using these parameters:

* The IP address
* URL path
* The failure message
* Usernames list
* Password list



## Figure 13: Hydra command execution

**Step 9:** The output of hydra with the valid username and password



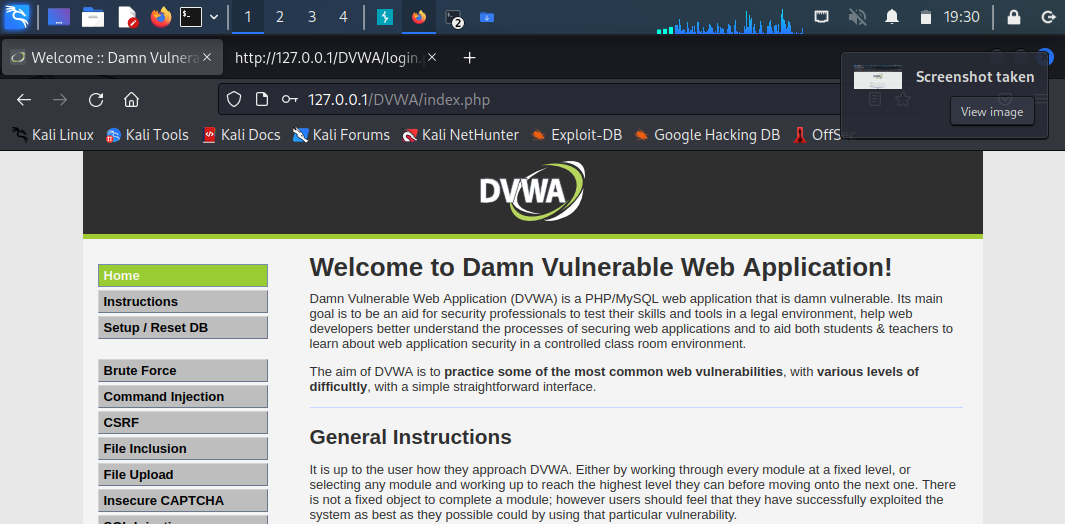
## Figure 14: Hydra command result

**Step 10**: Successful login to the website using the username and password

Graphical user interface, text, application

Description automatically generated

## Figure 15: Login attempt



## Figure 16: Launching the website successfully

# **2.2 Hydra Result and Analysis**

We used Hydra tool to dictionary attack against the web application DVWA (Damn Vulnerable Web Application) login page. DVWA contains different vulnerabilities than dictionary attack such as brute force, SQL injection, XSS, and more. The optained information from web page source view helped us to collect information about the login form to use it with Hydra commaned. As Hydra the most popular password guessing tool, we provided two files contains usernames and passwords and the error message, so Hydra can walkthroug the list and recognize the valid username and password.

In Hydra tool, the tool was able to successfully find the right username and password with 49 login tries.

# **Hydra Countermeasures**

* Implementing an intrusion prevention system (IPS) which adds protection against different types of brute-force attacks. With an IPS you can apply security on certain ports or services in your server (e.g. apache, ssh, ftp).
* Prevent attackers from gaining access to password storage.
* Do not store passwords in plaintext.
* Store passwords using a strong, industry-vetted algorithm (e.g. bcrypt).
* Prevent users from setting passwords on common attacker lists.
* Password policies: compelling users to create and maintain dependable, safe passwords.

# **Nikto**

Nikto is a free and open source, the nikto tool is written in Perl and has a GNU license. Chris Sullo programmed it to scan web servers. Since this tool scans more than 6,700 files for potential security vulnerabilities, it is very effective at scanning websites. Nikto has only one drawback that website security measures are more likely to detect the tool because it is not obvious.[7][8]

The default installation is available on the Kali Linux penetration testing system, It can also be run directly from the terminal as shown below[8]:



## Figure 17: Nikto commands

Here are some of the most used commands in Nikto[8]:

**1-config**

Replace config.txt in the install directory with an alternative configuration file.

**2-dbchech**

Make sure there are no syntax errors in the scan databases.

**3-host**

The host(s) to target. IP addresses, hostnames, or text files of hosts can be used. Stdout may be indicated with a single dash (-).

**4-Format**

Choose the type of file that will be used to save the results

**5- h or H (help)**

h- Commands are represented as a short list.

H- All commands are represented as a list.

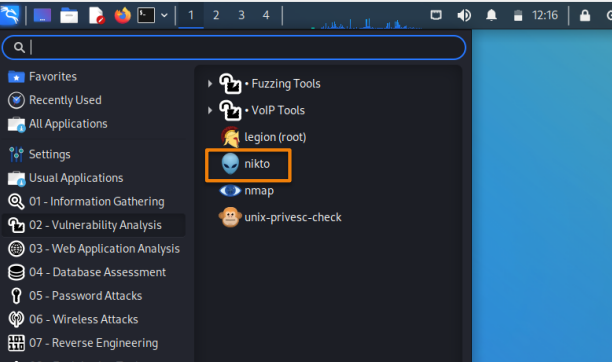
**6-Port**

Scan host to targeting specific ports.

# **3.1 Nikto Used procedure**

Using this tool requires installation of Kali Linux in virtual box or Windows, as well as the tool itself[7][8].

Step1:

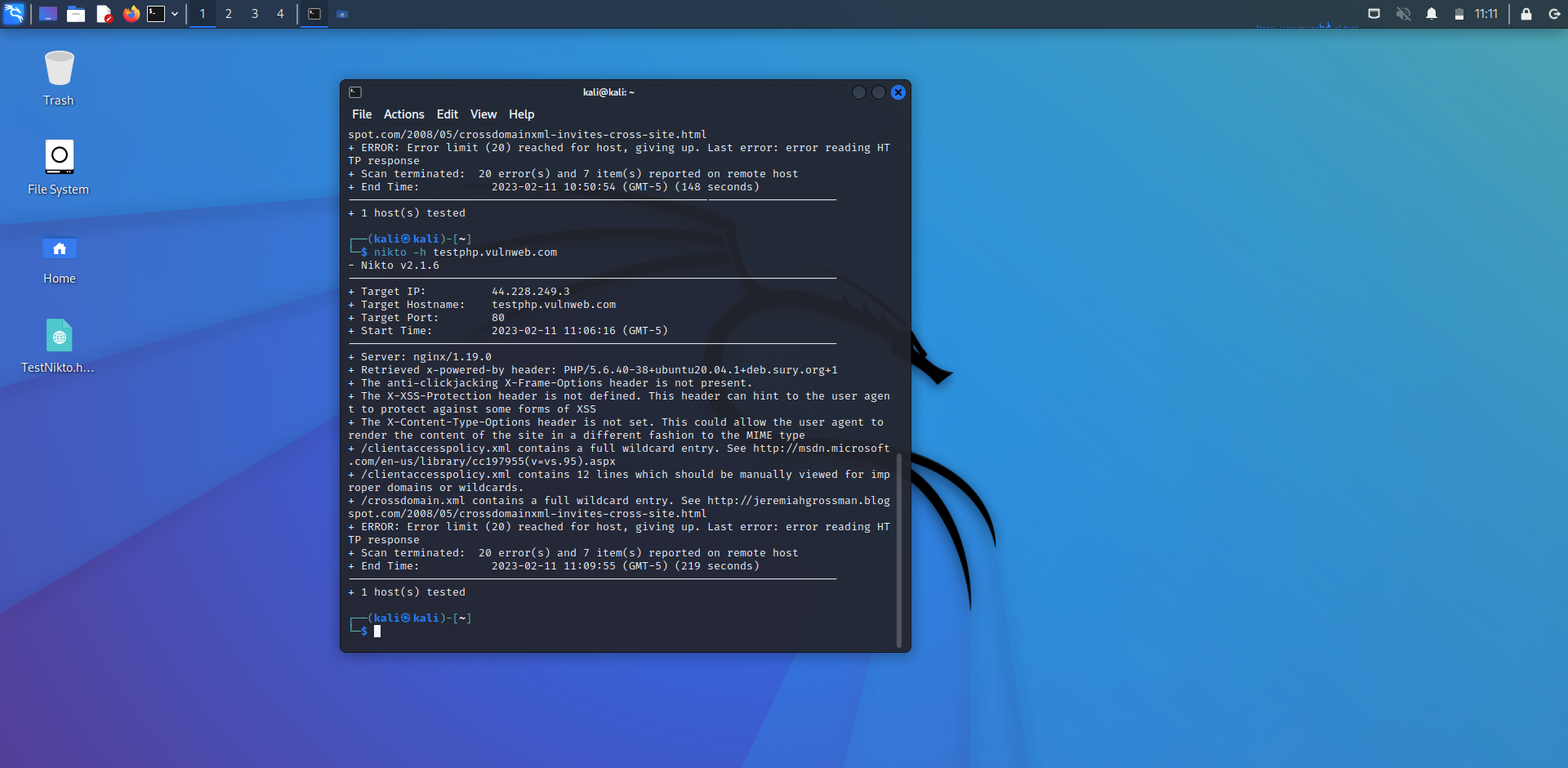


## Figure 18: How to open Nikto

Kali Linux will be running in a virtual box once you start it, then you will find a list of tools under the application menu. Nikto comes from vulnerability crack tools, so click on it and then Nikto will appear.

Step2:

This command can be used to test and examine any website (nikto -h). as shown in the figure below:

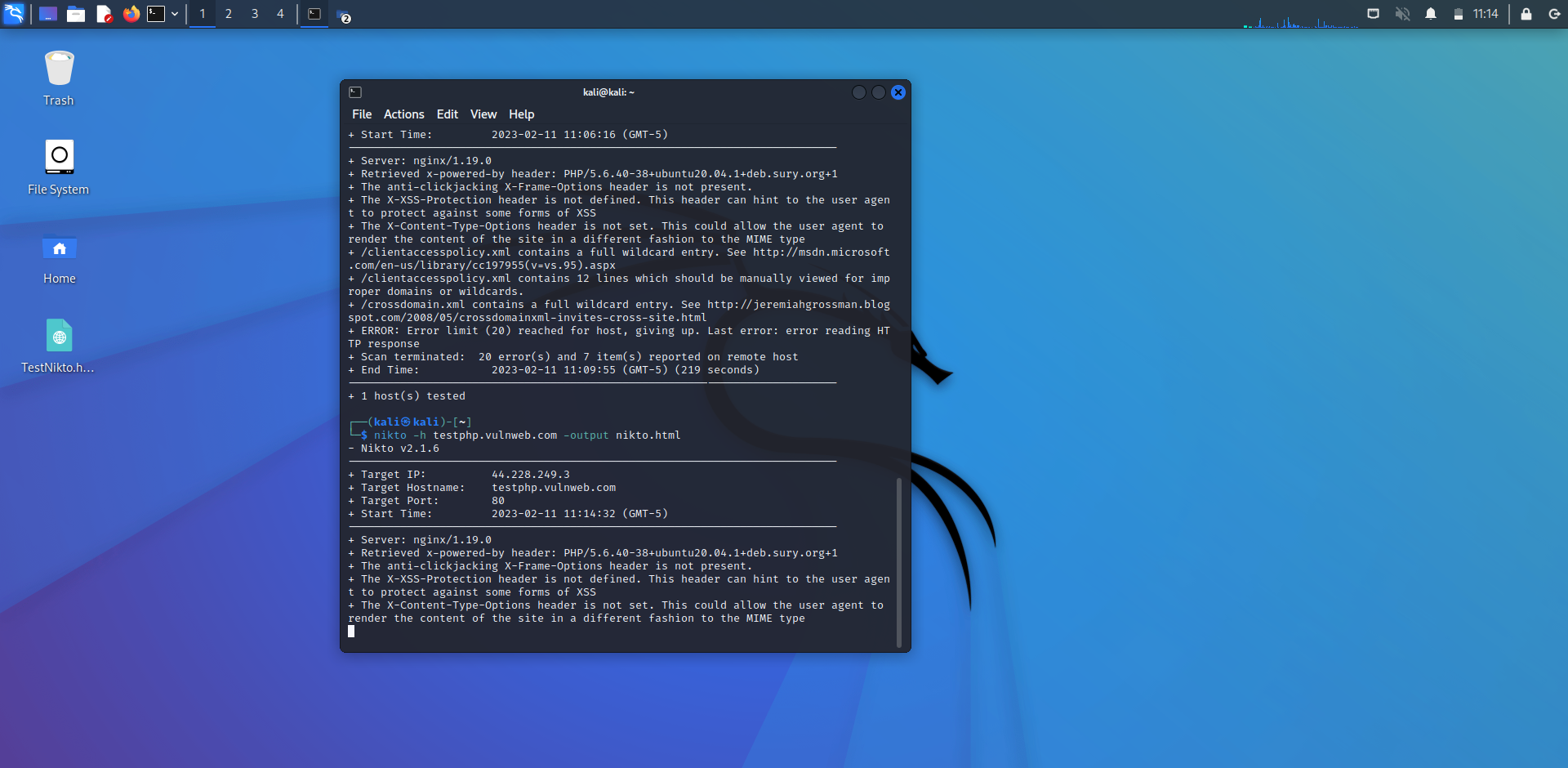


## Figure 19: Testing tastphp.Vulnweb.com website

Also, you can specify a port number (nikto -h -p 80).

Step3:

use this command (nikto -h <IP or hostname> -output nikto.html) To save the result as HTML



## Figure 20: How to save result file as HTML document

Graphical user interface, text, application, email

Description automatically generated

## Figure 21: Opening HTML file

# **3.2 Nikto Result and Analysis**

Graphical user interface, text, application, email

Description automatically generated

## Figure 22: The vulnerabilities report

Taking a look at the above figure, here is the full report of the tested website with all the vulnerabilities. A vulnerability on the website is its lack of an anticlickjacking X-Frame option in the header. See figure below[6]:

Graphical user interface, text, application, email

Description automatically generated

## Figure 23: Anti-clickjacking X-Frame-Option vulnerability

This point in the report shows that the website may be at risk of a click hack. Users who click on images on the site will see a different URL than they expect, or they will see ads instead of the video if they click on a video.

Graphical user interface, text, application, email

Description automatically generated

## Figure 24: X-Content-Type-Option vulnerability

X-Content-Type-Option is not set as shown in the figure above, which leads to another vulnerability.

The MIME-type sniffer in the browser is a method of finding an appropriate way to present and render data. In cases of missing content types, the browser adds appropriate types. This could cause problems because the browser may change the MIME type from jpg to php, thereby converting a non-executable file into an executable one.

# **3.3 Nikto Countermeasures**

**1-Avoid clickjacking**

developer can avoid **clickjacking** attacks by adding the X-Frame Option to the header and specifying either of these three options [5]:

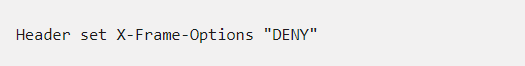
1. Deny: It is not possible to display the page in a frame, regardless of what the site tries to do.
2. Sameorigin: It is necessary that all ancestor frames on the page have the same origin as the page itself in order to display it.
3. Allow-From: By setting a URL, the developer can link to a certain website when the user clicks on the frame.

This is the configuration you need to add to your site's configuration to send the X-Frame-Options header to all pages:

**Logo

Description automatically generated with low confidence**

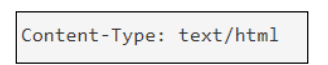
## Figure 25: How to set X-frame option to the header



## Figure 26: How to set X-frame option to the header

**2- Avoid MIME-sniffing attacks**

The developer must send the appropriate content-type header when serving HTML pages, for example, using HTTP headers if serving HTML pages. Then a "nosniff" value should be added to the X-Content-Type-Options header, telling the browser that the content-type is appropriate and not for sniffing.



## Figure 27: Set the content type header

A picture containing shape

Description automatically generated

## Figure 28: Set the X-content-type option header

# **Conclusion:**

In this project we interduces some tools in Kali Linux OS which are Nmap, Hydra and Nikto. On each tool we present some points like the tool used procedure, result and analysis and the countermeasures of each tool. In Nmap tool we used to gather information about the network.

In addition to Hydra tool, we used it to crack the site login form. On the last tool Nikto we used to discover the websites vulnerabilities. Our project has test different targets such as websites and the Ip addresses

# **Reference:**

[1]F. Lyon, *Nmap*, 2017. [Online]. Available: https://nmap.org/. [Accessed: 11-Feb-2022].

[2] *Nmap cheat sheet* (2020) *TutorialsPoint*. TutorialsPoint. Available at: https://www.tutorialspoint.com/nmap-cheat-sheet (Accessed: February 11, 2023).

[3] S. Shea, “How to use nmap to scan for open ports,” *SearchSecurity*, 27- Jan-2022. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/How-to-use-Nmap-to- scan-for-open-ports. [Accessed: 14-May-2022].

[4] T. Mesevage, “What is Port Scanning?,” *Datto Networking*, 2019. [Online]. Available: https://www.datto.com/blog/what-is-port-scanning. [Accessed: 12-May-2022].

[5] *X-Frame-Options - http: MDN* (no date) *HTTP | MDN*. Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options (Accessed: February 11, 2023).

[6] *【clickjacking prevention 】what is this attack and examples* (2022) *Crashtest Security*. Available at: https://crashtest-security.com/clickjacking-attack/ (Accessed: February 11, 2023).

[7] Obbayi, L. (2021) *Introduction to the nikto web application vulnerability scanner*, *Infosec Resources*. Infosec Resources. Available at: https://resources.infosecinstitute.com/topic/introduction-nikto-web-application-vulnerability-scanner/ (Accessed: February 11, 2023).

[8] *Nikto: Kali linux tools* (2022) *Kali Linux*. Available at: https://www.kali.org/tools/nikto/#:~:text=root%40kali%3A~%23%20nikto,pass%3Arealm%20%2Dlist%2Dplugins (Accessed: February 11, 2023).

[9] D. Czagan, “Online dictionary attack with Hydra,” Infosec Resources, 13-Sep-2013. [Online].

[10] M. Shivanandhan, “How to use hydra to hack passwords – penetration testing tutorial,” freecodecamp.org, 18-Nov-2022. [Online].