College of Computer Science & Engineering
Cybersecurity Department

CCCY 323 Network Security

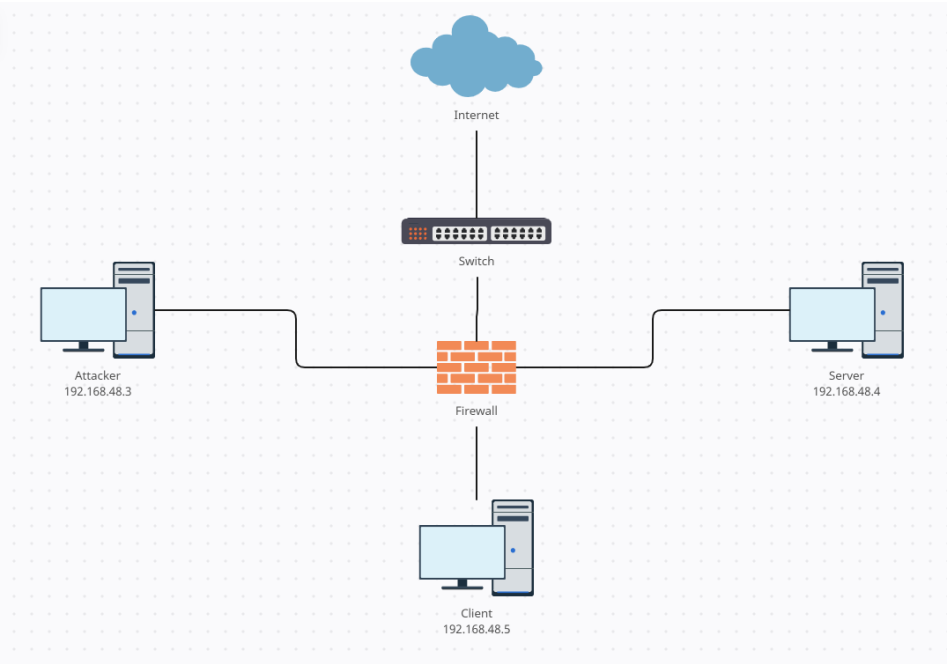
Group members:

Waleed Badran | 1945350

Saud Alghamdi | 2040176

Mohammed Aljayzani | 2041075

Figure 1: Network Diagram



As shown above the Network Diagram of our projects with the IP Addresses of the machines (Client, Server, Attacker).

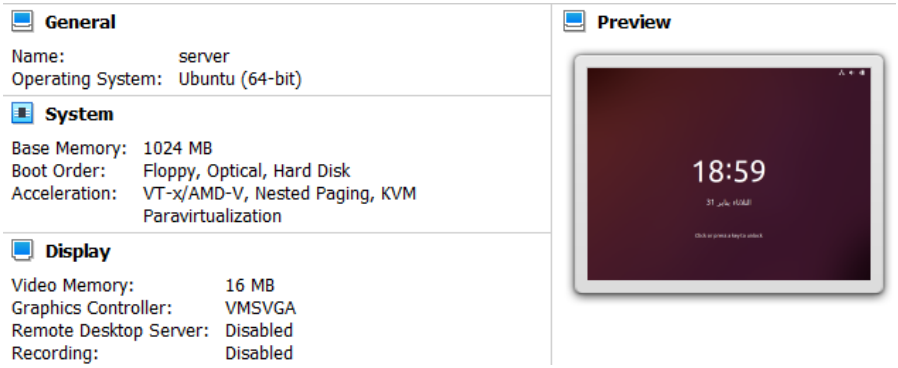
List of Software's and Tools

1. XAMPP
2. NMAP
3. HPING3
4. WIRESHARK
5. Golden EYE
6. IPTABLES
7. SNORT

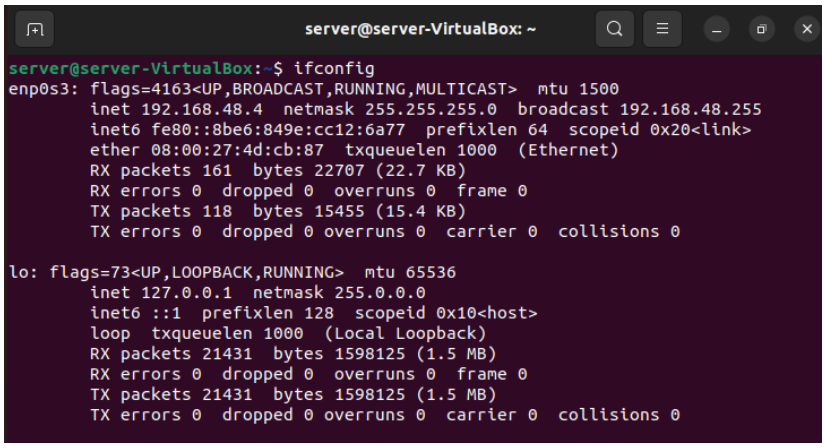
Part 1: Network Setup

Task 1: Server setting

- Operating system: Linux (Ubuntu)

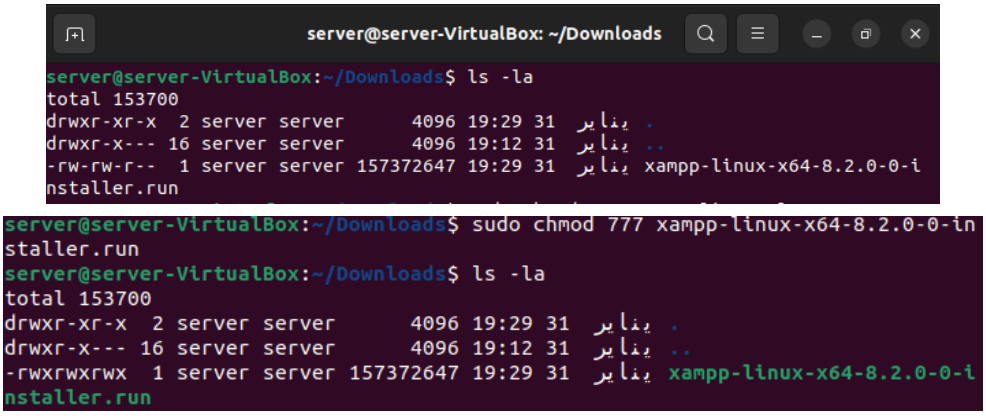


Configuration of Server machine

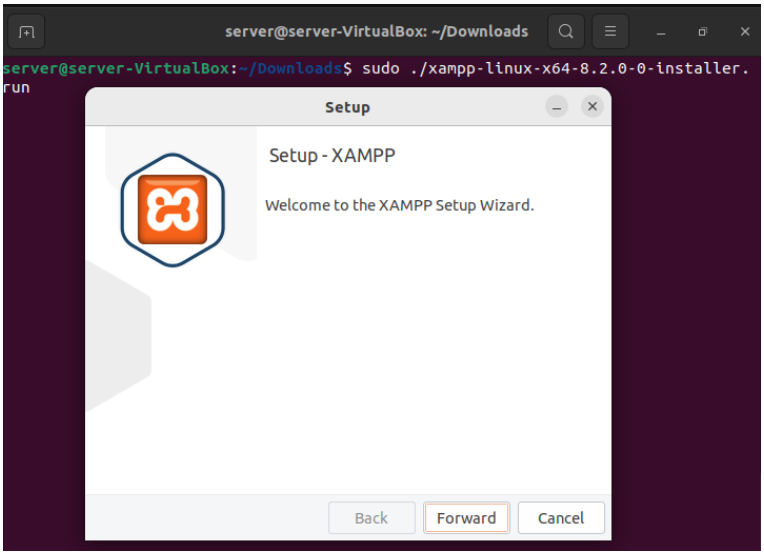


IP address of the server machine: 192.168.48.4

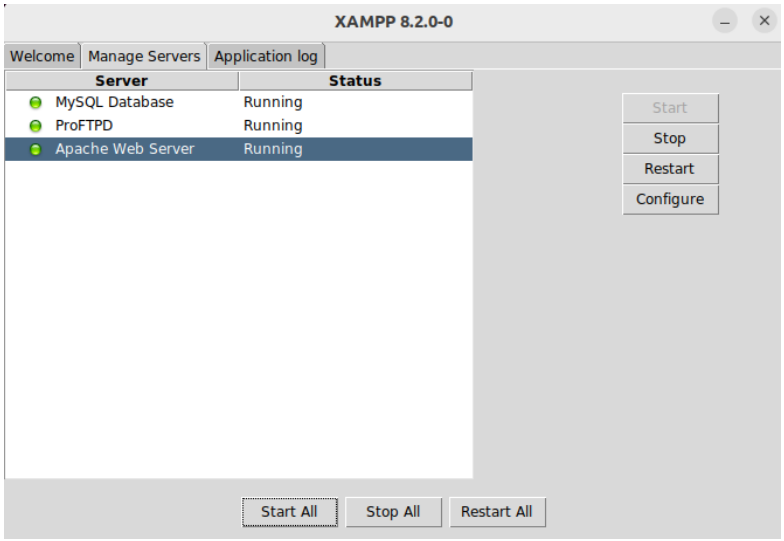
- You need to setup Apache server (on the server VM) **with a sample webpage**, such as "hello world".



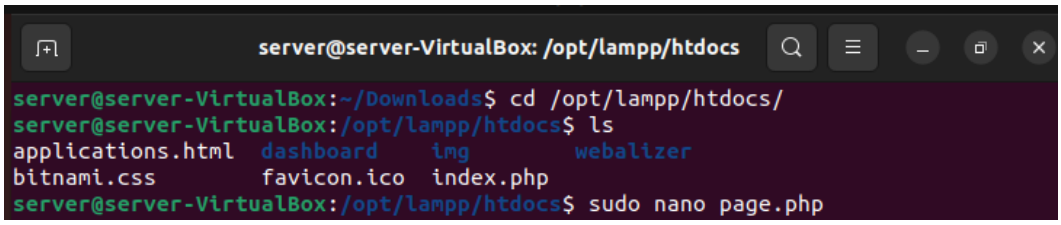
After we install XAMPP, we changed their permission.



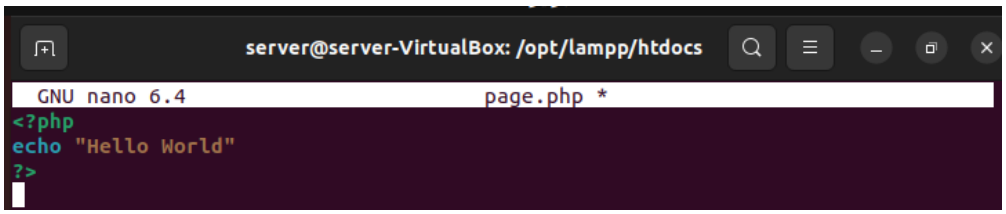
Here we start setup XAMPP.



After installation is completed, we start all servers.



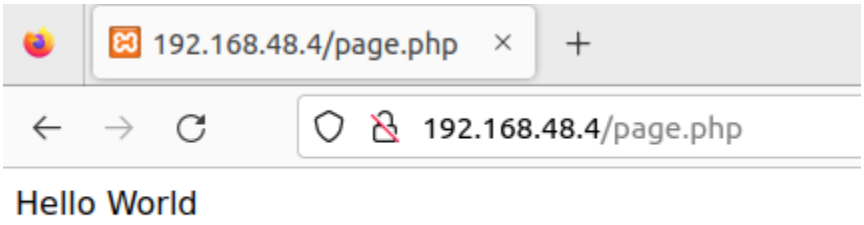
We creat PHP file inside htdocs and we will write PHP code on it.



This is the PHP code for printing "Hello World"

```
server@server-VirtualBox: /opt/lampp/htdocs
server@server-VirtualBox:/opt/lampp/htdocs$ ls -ls
total 60
 4 -rw-r--r--  1 root   root    3607 2022  15  يونيو applications.html
 4 -rw-r--r--  1 root   root     177 2022  15  يونيو bitnami.css
 4 drwxr-xr-x 20 root   root    4096 17:22 1  فبراير dashboard
32 -rw-r--r--  1 root   root   30894 2007  11   مايو favicon.ico
 4 drwxr-xr-x  2 root   root    4096 17:22 1  فبراير img
 4 -rw-r--r--  1 root   root     260 2015  9   يوليو index.php
 4 -rw-r--r--  1 root   root      29 18:17 1  فبراير page.php
 4 drwxr-xr-x  2 daemon daemon  4096 17:22 1  فبراير webalizer
server@server-VirtualBox:/opt/lampp/htdocs$ sudo chmod 777 page.php
server@server-VirtualBox:/opt/lampp/htdocs$ ls -la
total 68
drwxr-xr-x  5 root   root    4096 18:17 1  فبراير .
drwxr-xr-x 30 root   root    4096 18:08 1  فبراير ..
-rw-r--r--  1 root   root    3607 2022  15  يونيو applications.html
-rw-r--r--  1 root   root     177 2022  15  يونيو bitnami.css
drwxr-xr-x 20 root   root    4096 17:22 1  فبراير dashboard
-rw-r--r--  1 root   root   30894 2007  11   مايو favicon.ico
drwxr-xr-x  2 root   root    4096 17:22 1  فبراير img
-rw-r--r--  1 root   root     260 2015  9   يوليو index.php
-rwxrwxrwx  1 root   root      29 18:17 1  فبراير page.php
drwxr-xr-x  2 daemon daemon  4096 17:22 1  فبراير webalizer
```

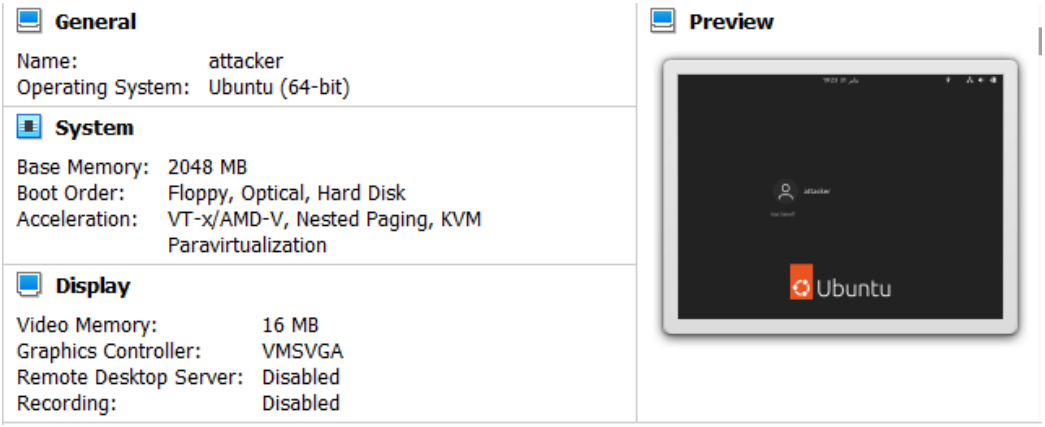
After we creat the PHP file, we changed the permission to be executed.



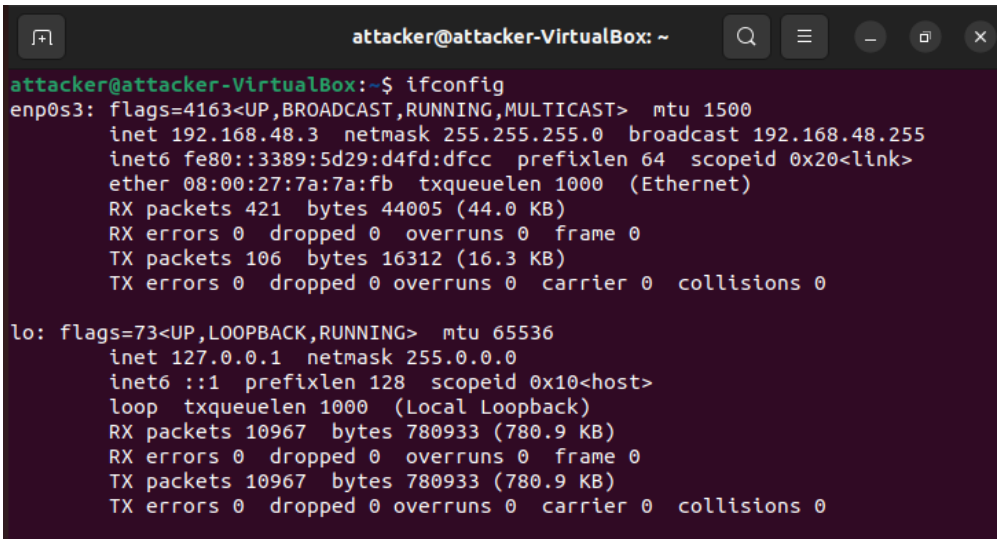
Here we can see the "Hello World" that we are printed

Task 2: Attacker VM

- Operating system: Linux (Ubuntu)

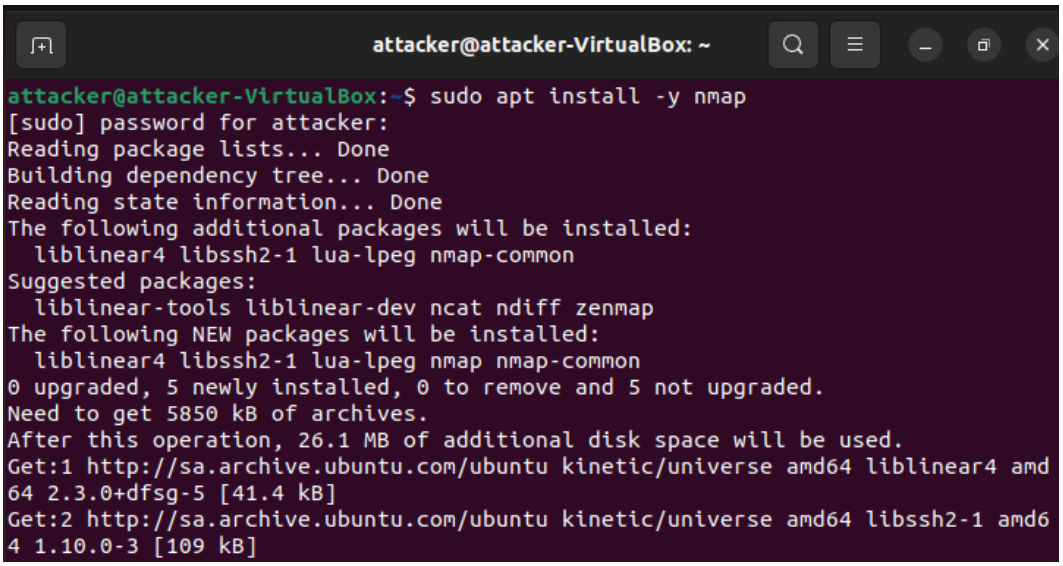


Configuration of Attacker machine



IP address of the Attacker machine: 192.168.48.3

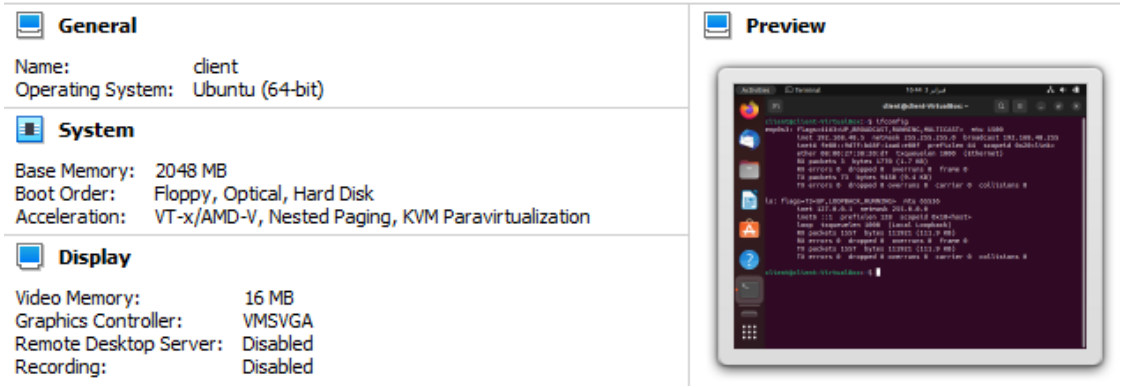
- In this project, you need to perform two types of attacks using **nmap** tool.
    - Network Scanning Attack
    - Dos Attack



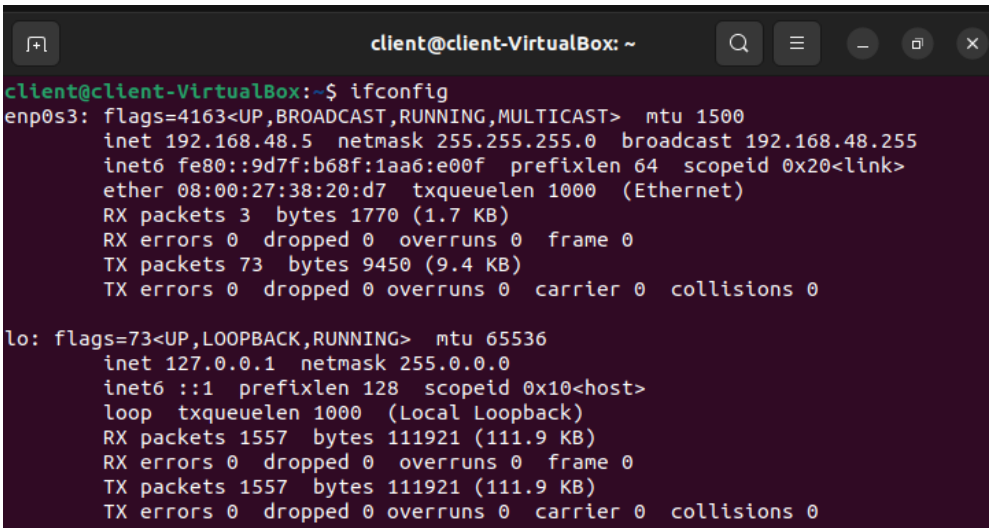
Nmap tool installation

Task 3: Client

- Operating system: Linux (Ubuntu)



Configuration of Client machine



IP address of the Attacker machine: 192.168.48.5

Part 2: Performing passive and active attack

Task1: Perform network scanning attack from the attacker machine to the server VM.

- Perform TCP Connect Scan

```
attacker@attacker-VirtualBox:~$ nmap -sT 192.168.48.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 14:12 +03
Nmap scan report for 192.168.48.4
Host is up (0.00051s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
```

We used Nmap tool with option -sT to scan the network of Server and establishing a full connection

- Perform Stealth Scan

```
attacker@attacker-VirtualBox:~$ sudo nmap -sS 192.168.48.4
[sudo] password for attacker:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 14:27 +03
Nmap scan report for 192.168.48.4
Host is up (0.0017s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 08:00:27:4D:CB:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

We used Nmap tool with option -sS to scan the network of Server and scanning the port that doesn't have firewalls.

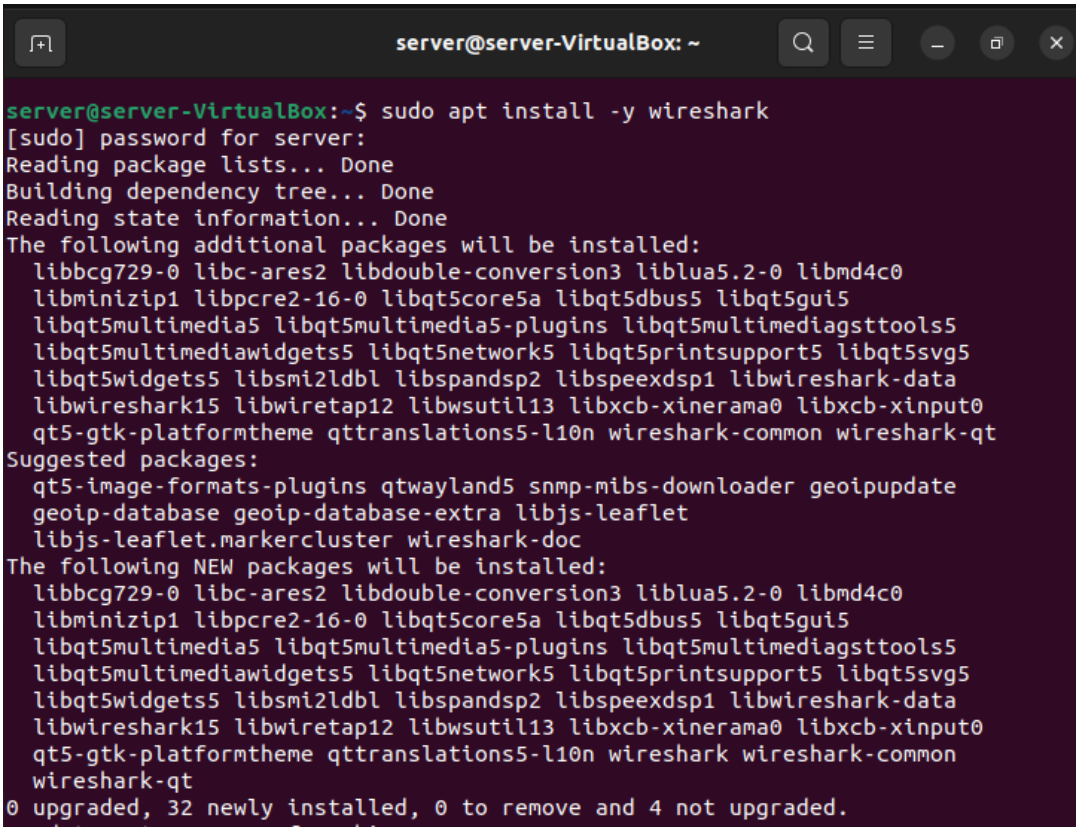
- Perform a scan that enables OS detection, version detection, script scanning, and traceroute

```
attacker@attacker-VirtualBox:~$ sudo nmap -A 192.168.48.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 14:35 +03
Nmap scan report for 192.168.48.4
Host is up (0.00032s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD
80/tcp   open  http     Apache httpd 2.4.54 ((Unix) OpenSSL/1.1.1s PHP/8.2.0 mod_perl/2.0.12 Perl/v5.34.1)
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.48.4/dashboard/
|_http-server-header: Apache/2.4.54 (Unix) OpenSSL/1.1.1s PHP/8.2.0 mod_perl/2.0.12 Perl/v5.34.1
443/tcp  open  ssl/http Apache httpd 2.4.54 ((Unix) OpenSSL/1.1.1s PHP/8.2.0 mod_perl/2.0.12 Perl/v5.34.1)
| http-title: Welcome to XAMPP
|_Requested resource was https://192.168.48.4/dashboard/
|_http-server-header: Apache/2.4.54 (Unix) OpenSSL/1.1.1s PHP/8.2.0 mod_perl/2.0.12 Perl/v5.34.1
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE
| Not valid before: 2004-10-01T09:10:30
|_Not valid after:  2010-09-30T09:10:30
|_ssl-date: TLS randomness does not represent time
3306/tcp open  mysql    MariaDB (unauthorized)
MAC Address: 08:00:27:4D:CB:87 (Oracle VirtualBox virtual NIC)
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 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.48.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.75 seconds
```

We used Nmap tool with option -A to scan the network of Server and enabling version detection, OS detection, traceroute and script scanning.

Part 3: Wireshark

Install Wireshark tool on the server VM and use it to capture:



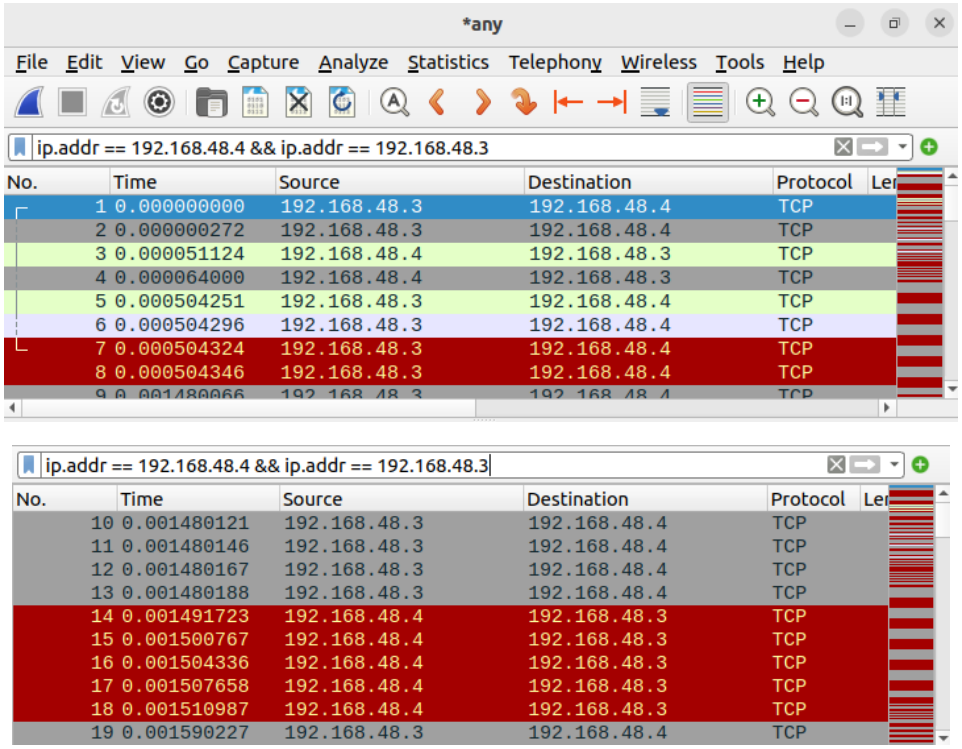
```
server@server-VirtualBox: ~

server@server-VirtualBox:~$ sudo apt install -y wireshark
[sudo] password for server:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libspeexdsp1 libwireshark-data
  libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libspeexdsp1 libwireshark-data
  libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
  wireshark-qt
0 upgraded, 32 newly installed, 0 to remove and 4 not upgraded.
```

Wireshark installation

- The TCP connect scan

```
attacker@attacker-VirtualBox: ~
attacker@attacker-VirtualBox:~$ nmap -sT 192.168.48.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 15:10 +03
Nmap scan report for 192.168.48.4
Host is up (0.00067s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

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

We used Nmap tool with option -sT to scan the network of Server and establishing a full connection

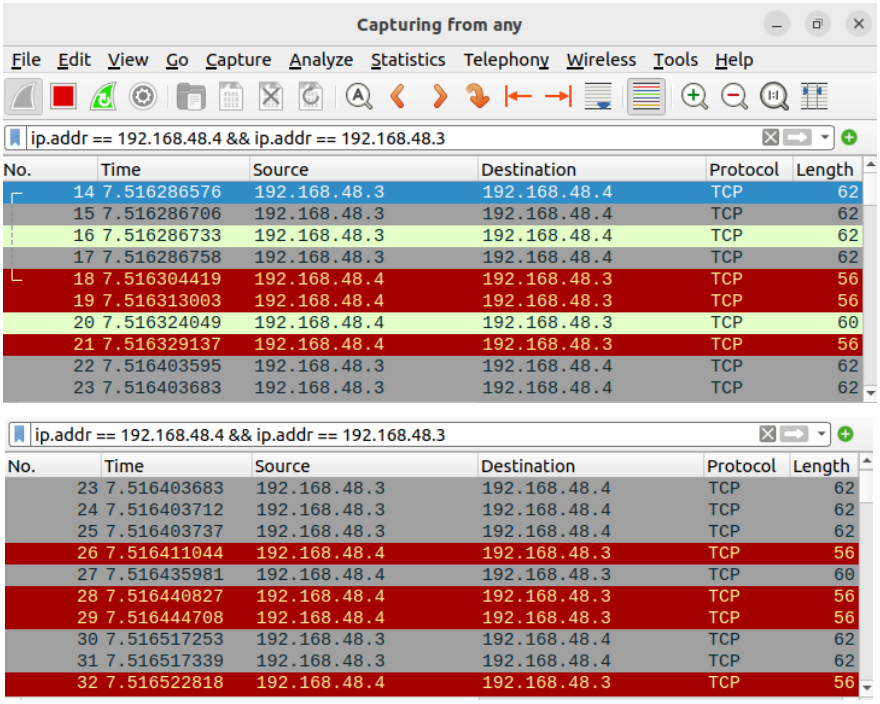


Wireshark of the packets that comes from 192.168.48.4 or going to 192.168.48.4

- The Stealth Scan.

```
attacker@attacker-VirtualBox:~$ sudo nmap -sS 192.168.48.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 18:40 +03
Nmap scan report for 192.168.48.4
Host is up (0.0014s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 08:00:27:4D:CB:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

We used Nmap tool with option -sS to scan the network of Server and scanning the port that doesn't have firewalls.



The stealth scan is the attacker machine send SYN flag to the server machine when the server response SYN/ACK the attacker send RST so the port is open, but when the server response RST rather than SYN/ACK here we know the port is closed, and when there is no response from the server the attacker will send SYN again and again so the port will be filtered.

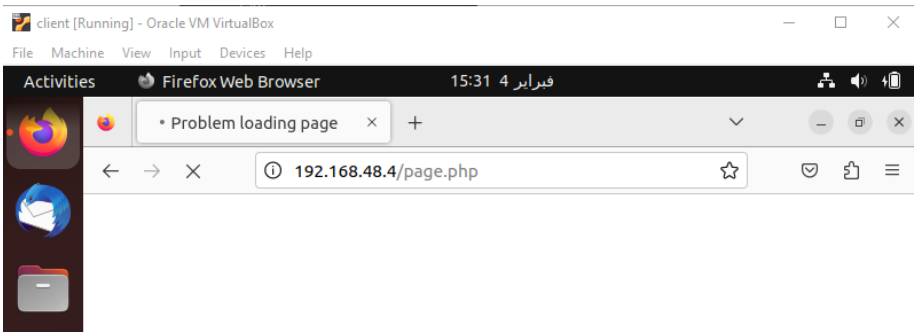
\

- The malicious packets coming from attacker VM (Capture **only** 500 packets)

```
attacker@attacker-VirtualBox:~$ sudo git clone https://github.com/jseidl/Golden
Eye.git
Cloning into 'GoldenEye'...
remote: Enumerating objects: 102, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 102 (delta 0), reused 2 (delta 0), pack-reused 99
Receiving objects: 100% (102/102), 121.64 KiB | 793.00 KiB/s, done.
Resolving deltas: 100% (36/36), done.
```

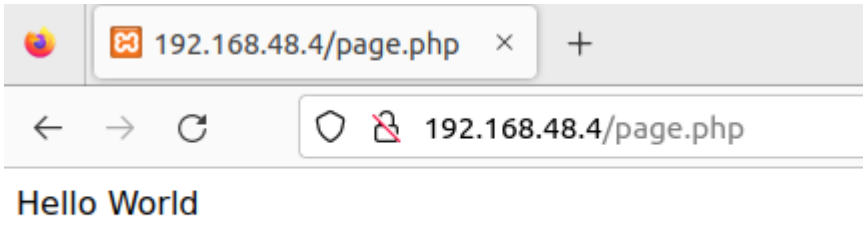
```
attacker@attacker-VirtualBox: ~/GoldenEye
attacker@attacker-VirtualBox:~/GoldenEye$ ./goldeneye.py http://192.168.48.4/pa
ge.php -s 500

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. H
it CTRL+C to cancel.
```

We used GoldenEye tool to do a DoS attack from the attacker machine to 192.168.48.4/page.php website and we captured 500 packets.

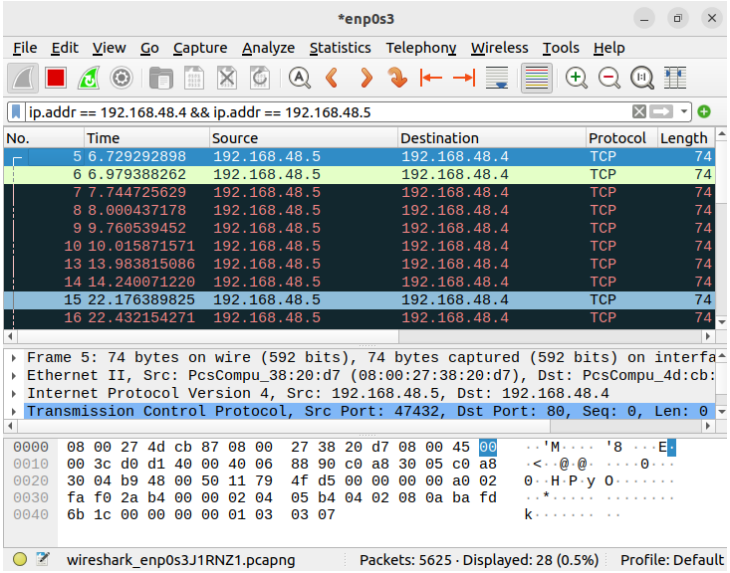


And we try to reach to 192.168.48.4/page.php website from the client machine but we cannot access to it

- Capture both the incoming and outgoing packets between **the client VM and the server.**



we visited 192.168.48.4/page.php from the client browser and we captured the traffic between the client and server

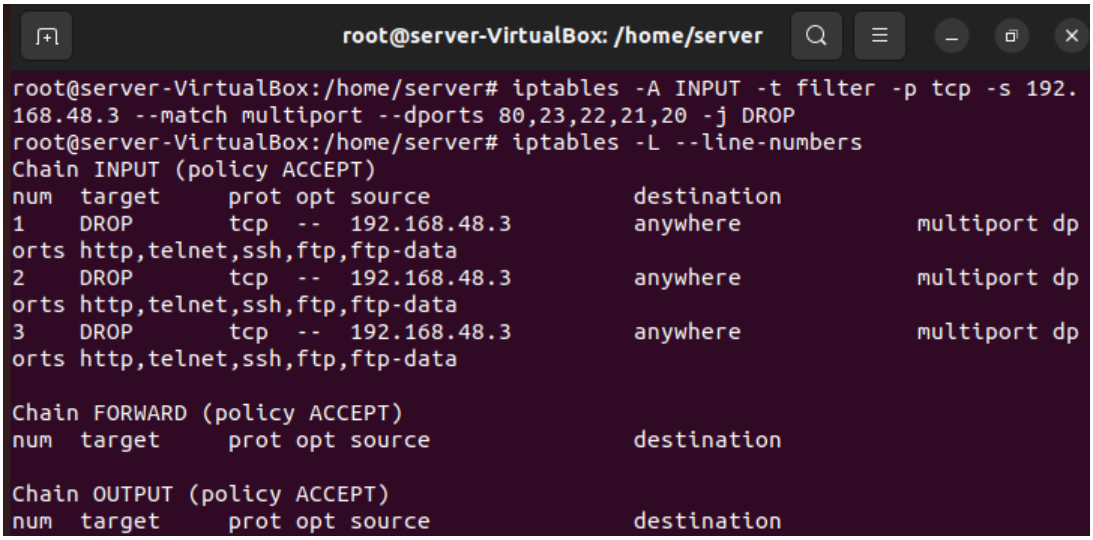


Part 4: Firewall

(5 marks)

Task 1: After you successfully complete **Part 2 and 3**, write the following iptables on the server to **block** the following traffic types originated from the attacker to the server:

1. HTTP connection request from the attacker to the server.
2. SSH connection request from the attacker to the server.
3. FTP and Telnet requests (Use single rule to block these multiple ports).



```
root@server-VirtualBox: /home/server
root@server-VirtualBox:/home/server# iptables -A INPUT -t filter -p tcp -s 192.
168.48.3 --match multiport --dports 80,23,22,21,20 -j DROP
root@server-VirtualBox:/home/server# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  192.168.48.3         anywhere             multiport dp
orts http,telnet,ssh,ftp,ftp-data
2    DROP       tcp  --  192.168.48.3         anywhere             multiport dp
orts http,telnet,ssh,ftp,ftp-data
3    DROP       tcp  --  192.168.48.3         anywhere             multiport dp
orts http,telnet,ssh,ftp,ftp-data

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

we will block multi ports using iptables command, -A option used for append to the chain rule in the INPUT, -t option will manipulate table and we mentioned a specific table while applying rules which is filter, -p option used to specific protocol, -s option we wrote the attacker IP: 192.168.48.3 , --match option we wrote multiport to wrote lots of ports, --dport option which we wrote the requested ports, port 80 for HTTP, port 23 for telnet, port 22for ssh and ports 21 and 20 for ftp, also we used -j option for DROP the any packets come from the attacker IP to these ports.

Task 2: Configure the iptables to log dropped packets (enable logging in iptables) and then show the log messages.

```
root@server-VirtualBox:/home/server# iptables -A INPUT -t filter -p tcp -s 192.
168.48.3 --match multiport --dports 80,23,22,21,20 -j LOG --log-prefix "iptable
s: "
```

Here we create a rule for logging from 80,23,22,21,20 ports to the attacker IP: 192.168.250.4

```
root@server-VirtualBox: /home/server
root@server-VirtualBox:/home/server# iptables -N LOGGING
iptables: Chain already exists.
root@server-VirtualBox:/home/server# iptables -A INPUT -j LOGGING
root@server-VirtualBox:/home/server# iptables -A INPUT -j LOG --log-prefix "ipt
ables: " --log-level 4
root@server-VirtualBox:/home/server# iptables -A INPUT -j DROP
root@server-VirtualBox:/home/server#
```

In the first command, we create a new chain "LOGGING".

in the second command, the option -A to append the chain with INPUT, Option -j the target chain "LOGGING".

in the third command, the option -A to append with the chain "LOGGING", option -j the target: LOG, we choose the prefix that we want it in the option –log-prefix which is "iptables:", and we will generate warning option –log-level 4.

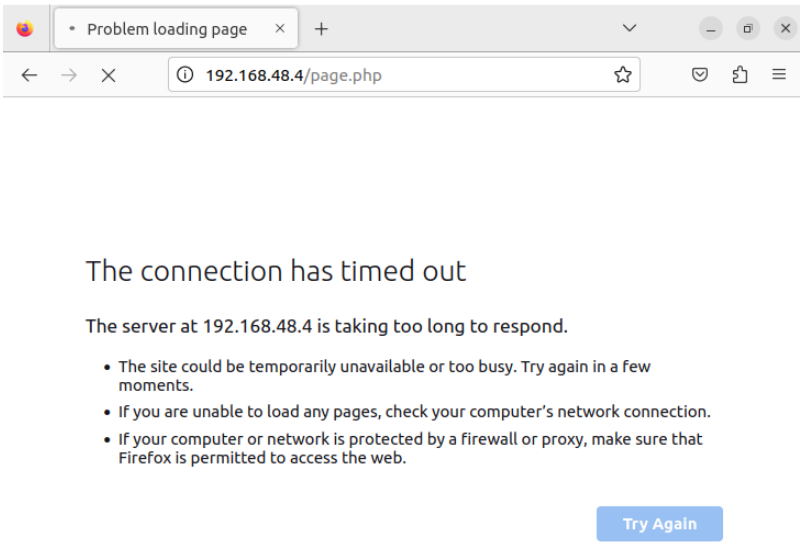
in the last command we used the chain "LOGGING" with option -A, option -j the target is DROP.

```
attacker@attacker-VirtualBox: ~
attacker@attacker-VirtualBox:~$ telnet 192.168.48.4
Trying 192.168.48.4...
```

Here we use telnet with the Server IP: 192.168.48.4 to open a telnet session between the attacker machine and the server machine but we couldn't because we are applied rule in the Server

```
Feb  3 16:54:07 server-VirtualBox kernel: [63407.074792] iptables: IN=enp0s3 OUT= MAC=08:00:27:4d:cb:87:08:00:27:fe:f6:
d7:08:00 SRC=192.168.48.3 DST=192.168.48.4 LEN=576 TOS=0x00 PREC=0x00 TTL=255 ID=440 PROTO=TCP SPT=67 DPT=68 LEN=556
```

we read the logs file, and the destination port is 23 which is for the telnet, and we can see the attacker IP 192.168.48.3



we tried to access the webpage that we are created before which is 192.168.48.4/page.php, but we could not because we applied the rule

```
Feb  3 16:54:07 server-VirtualBox kernel: [63407.074792] iptables: IN=enp0s3 OUT= MAC=08:00:27:4d:cb:87:08:00:27:fe:f6:
d7:08:00 SRC=192.168.48.3 DST=192.168.48.4 LEN=576 TOS=0x00 PREC=0x00 TTL=255 ID=440 PROTO=UDP SPT=67 DPT=68 LEN=556
Feb  3 16:54:07 server-VirtualBox kernel: [63407.074792] iptables: IN=enp0s3 OUT= MAC=08:00:27:4d:cb:87:08:00:27:fe:f6:
d7:08:00 SRC=192.168.48.2 DST=192.168.48.4 LEN=576 TOS=0x00 PREC=0x00 TTL=255 ID=440 PROTO=UDP SPT=67 DPT=68 LEN=556
```

After the attacker tried to access the website, we read the file that contains the logs, and we see the destination port was 80 which is for the http, and we can see the attacker IP 192.168.48.3

Part 5: IDS

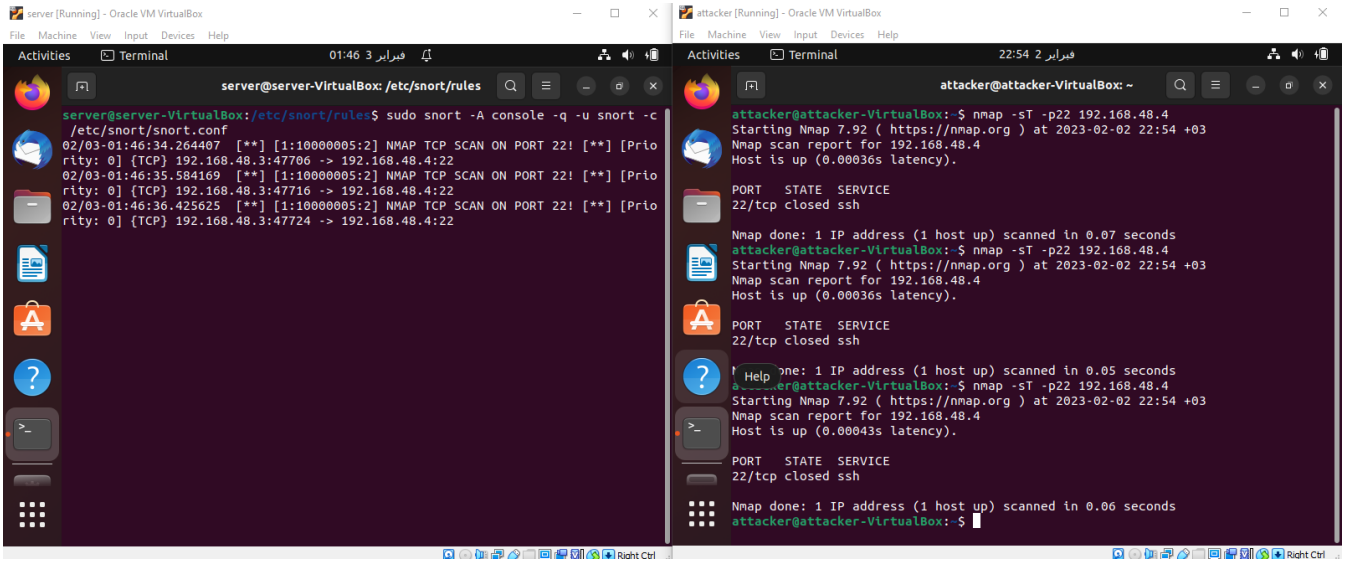
Install and configure snort on server VM to alert on TCP connect scan on port 22 from the attacker VM.

```
server@server-VirtualBox: ~
server@server-VirtualBox:~$ sudo apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.15.1-6build1).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
```

Installation of Snort tool

```
Open    local.rules
        /etc/snort/rules    Save
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # ----------------
3 # LOCAL RULES
4 # ----------------
5 # This file intentionally does not come with signatures.  Put your local
6 # additions here.
7
8
9 alert tcp 192.168.48.3 any -> 192.168.48.4 22 (msg: "NMAP TCP SCAN ON PORT
  22!"; sid:10000005; rev:2; )
```

we wrote in local.rules file the rule that applied with snort.
The rule will alert with TCP protocol from Attacker IP and any port, to port 22 to the Server IP, with the message: “NMAP TCP SCAN ON PORT 22 !”



we run snort tool with option -A to send alerts, and option -q to be quit without any banner, the option -u to run snort with snort user, the option -g for run snort with snort group, the option -c for choose the configuration snort file.
after we run snort we run Nmap to scan the port 22 with option -sT for TCP scan on the server machine with that IP 192.168.48.3
when we are scanning with nmap the alerts shows in server machine

Conclusion

In conclusion, we have applied the projects with the given requirement, and we learned a lot of how to implement a virtual machines, setup the network and the web pages, then we have done demonstrating DoS attack with showing the effectiveness of firewall in time of before the attack, during the attack, and after the attack. The attack was using tools such as hping3, Nmap, and golden eye. We have learned how to use Wireshark to inspect the traffics also we applied IDS and wrote a rule that gives an alerts when the attacker tries to use Nmap to scan TCP with port number 22.