

College of Computer Science & Engineering
Cybersecurity Department

CCCY 323 Network Security

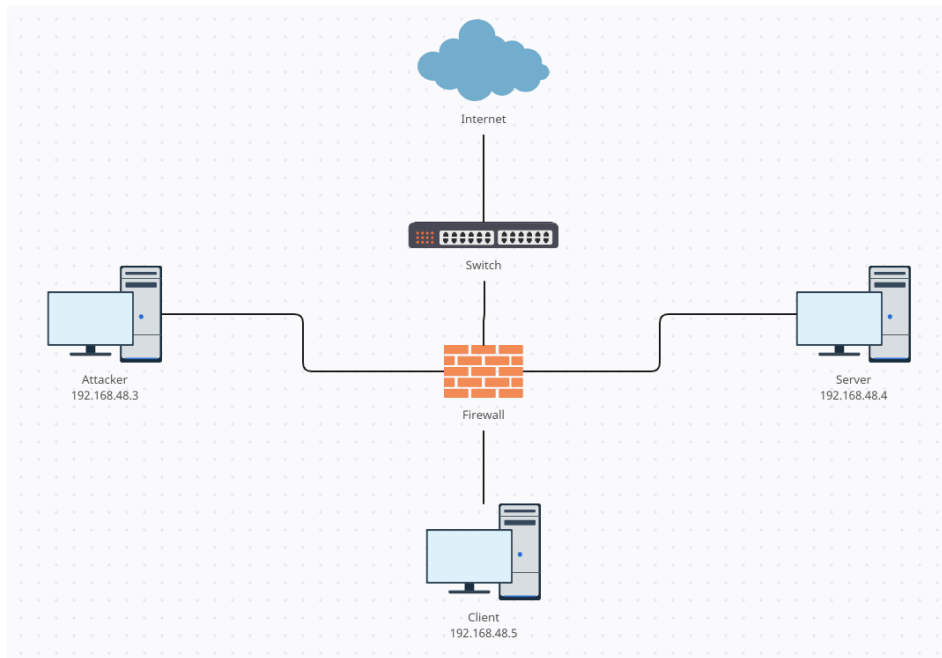
Group members:

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).

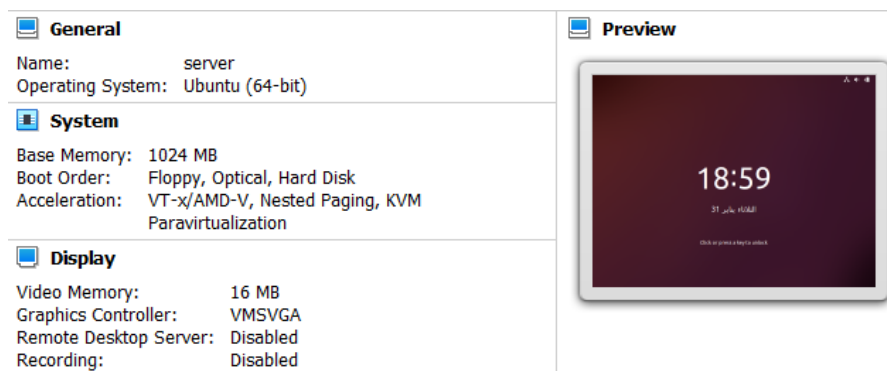
List of Software's and Tools

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

```
server@server-VirtualBox: ~  
server@server-VirtualBox:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.48.4 netmask 255.255.255.0 broadcast 192.168.48.255  
    inet6 fe80::8be6:849e:cc12:6a77 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:4d:cb:87 txqueuelen 1000 (Ethernet)  
    RX packets 161 bytes 22707 (22.7 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 118 bytes 15455 (15.4 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 21431 bytes 1598125 (1.5 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 21431 bytes 1598125 (1.5 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

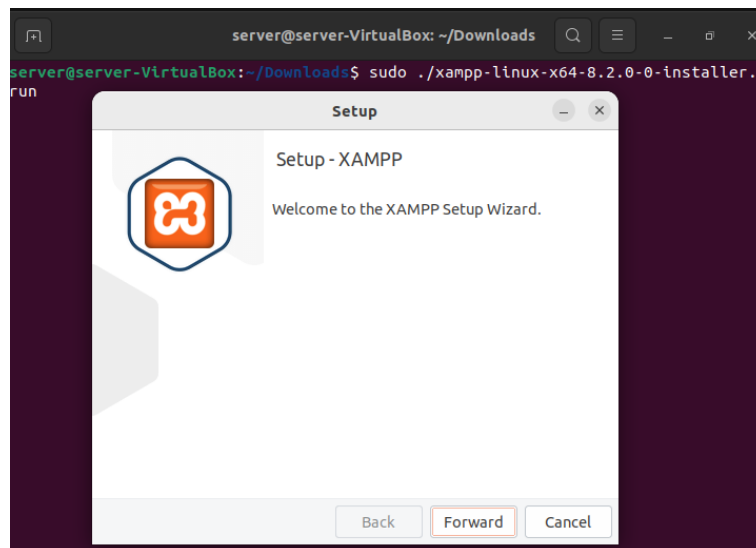
IP address of the server machine: 192.168.48.4

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

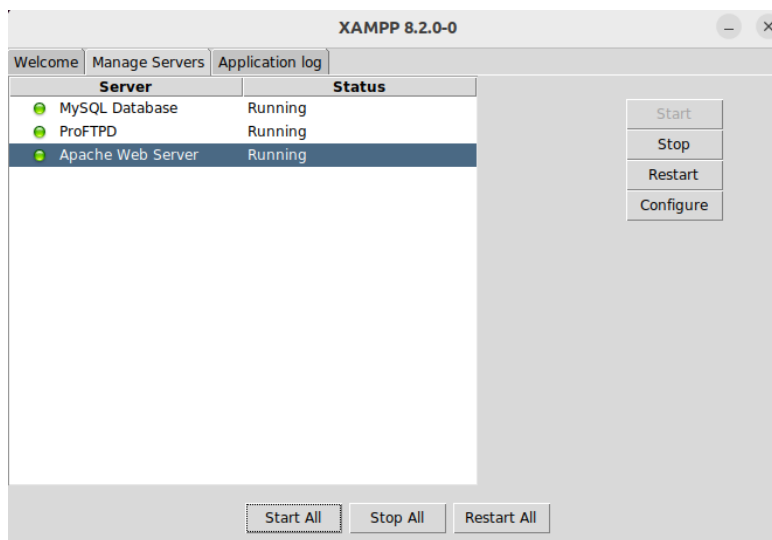
```
server@server-VirtualBox: ~/Downloads
server@server-VirtualBox:~/Downloads$ ls -la
total 153700
drwxr-xr-x  2 server server    4096 19:29 31  .
drwxr-xr-x 16 server server    4096 19:12 31  ..
-rw-rw-r--  1 server server 157372647 19:29 31  xampp-linux-x64-8.2.0-0-i
nstaller.run

server@server-VirtualBox:~/Downloads$ sudo chmod 777 xampp-linux-x64-8.2.0-0-i
nstaller.run
server@server-VirtualBox:~/Downloads$ ls -la
total 153700
drwxr-xr-x  2 server server    4096 19:29 31  .
drwxr-xr-x 16 server server    4096 19:12 31  ..
-rwxrwxrwx  1 server server 157372647 19:29 31  xampp-linux-x64-8.2.0-0-i
nstaller.run
```

After we install XAMPP, we changed their permission.



Here we start setup XAMPP.



After installation is completed, we start all servers.

```
server@server-VirtualBox: /opt/lampp/htdocs
server@server-VirtualBox:~/Downloads$ cd /opt/lampp/htdocs/
server@server-VirtualBox:/opt/lampp/htdocs$ ls
applications.html  dashboard  img        webalizer
bitnami.css       favicon.ico index.php
server@server-VirtualBox:/opt/lampp/htdocs$ sudo nano page.php
```

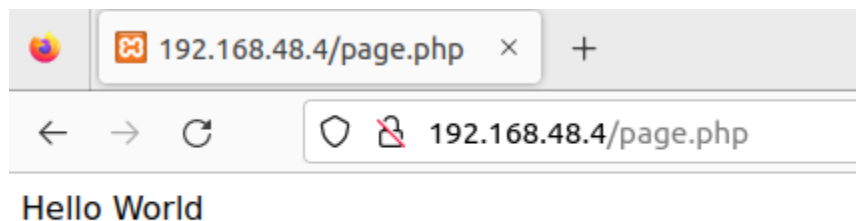
We creat PHP file inside htdocs and we will write PHP code on it.

```
GNU nano 6.4 page.php *
<?php
echo "Hello World"
?>
```

This is the PHP code for printing "Hello World"

```
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
```

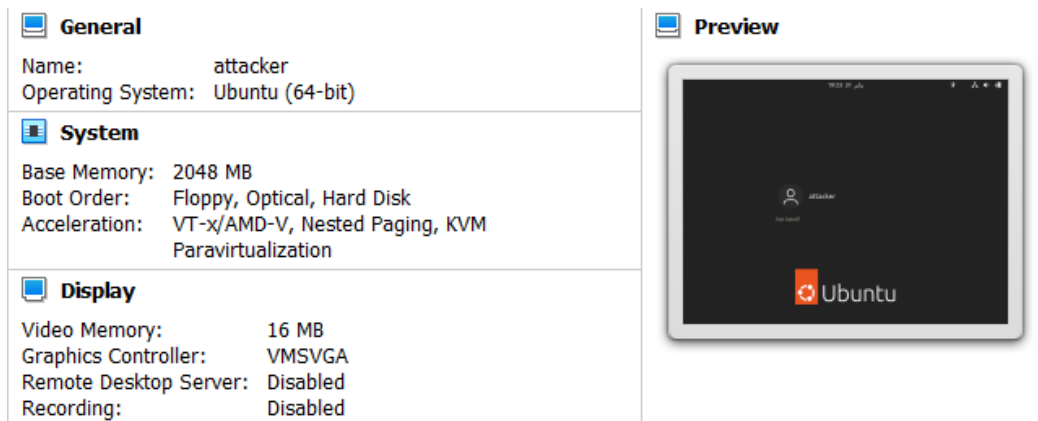
After we creat the PHP file, we changed the permission to be executed.



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

Task 2: Attacker VM

- Operating system: Linux (Ubuntu)



Configuration of Attacker machine

```
attacker@attacker-VirtualBox: ~  
attacker@attacker-VirtualBox:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.48.3 netmask 255.255.255.0 broadcast 192.168.48.255  
inet6 fe80::3389:5d29:d4fd:dfcc prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:7a:7a:fb txqueuelen 1000 (Ethernet)  
RX packets 421 bytes 44005 (44.0 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 106 bytes 16312 (16.3 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 10967 bytes 780933 (780.9 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 10967 bytes 780933 (780.9 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

IP address of the Attacker machine: 192.168.48.3

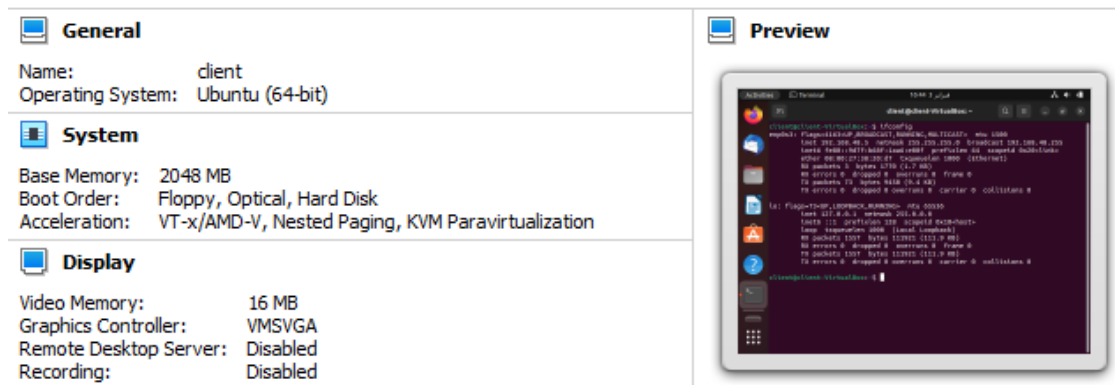
- In this project, you need to perform two types of attacks using nmap tool.
 - Network Scanning Attack
 - Dos Attack

```
attacker@attacker-VirtualBox: ~  
attacker@attacker-VirtualBox:~$ sudo apt install -y nmap  
[sudo] password for attacker:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  liblinear4 libssh2-1 lua-lpeg nmap-common  
Suggested packages:  
  liblinear-tools liblinear-dev ncat ndiff zenmap  
The following NEW packages will be installed:  
  liblinear4 libssh2-1 lua-lpeg nmap nmap-common  
0 upgraded, 5 newly installed, 0 to remove and 5 not upgraded.  
Need to get 5850 kB of archives.  
After this operation, 26.1 MB of additional disk space will be used.  
Get:1 http://sa.archive.ubuntu.com/ubuntu kinetic/universe amd64 liblinear4 amd  
64 2.3.0+dfsg-5 [41.4 kB]  
Get:2 http://sa.archive.ubuntu.com/ubuntu kinetic/universe amd64 libssh2-1 amd6  
4 1.10.0-3 [109 kB]
```

Nmap tool installation

Task 3: Client

- Operating system: Linux (Ubuntu)



Configuration of Client machine

```
client@client-VirtualBox: ~  
client@client-VirtualBox:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.48.5 netmask 255.255.255.0 broadcast 192.168.48.255  
inet6 fe80::9d7f:b68f:1aa6:e00f prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:38:20:d7 txqueuelen 1000 (Ethernet)  
RX packets 3 bytes 1770 (1.7 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 73 bytes 9450 (9.4 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 1557 bytes 111921 (111.9 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 1557 bytes 111921 (111.9 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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:  
  libbcb729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0  
  libminizip1 libpcr2-16-0 libqt5core5a libqt5dbus5 libqt5gui5  
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediastools5  
  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 geopipupdate  
  geoip-database geoip-database-extra libjs-leaflet  
  libjs-leaflet.markercluster wireshark-doc  
The following NEW packages will be installed:  
  libbcb729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0  
  libminizip1 libpcr2-16-0 libqt5core5a libqt5dbus5 libqt5gui5  
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediastools5  
  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 Packet Capture 1

Filter: ip.addr == 192.168.48.4 && ip.addr == 192.168.48.3

No.	Time	Source	Destination	Protocol	Length
1	0.000000000	192.168.48.3	192.168.48.4	TCP	60
2	0.000000272	192.168.48.3	192.168.48.4	TCP	60
3	0.000051124	192.168.48.4	192.168.48.3	TCP	60
4	0.000064000	192.168.48.4	192.168.48.3	TCP	60
5	0.000504251	192.168.48.3	192.168.48.4	TCP	60
6	0.000504296	192.168.48.3	192.168.48.4	TCP	60
7	0.000504324	192.168.48.3	192.168.48.4	TCP	60
8	0.000504346	192.168.48.3	192.168.48.4	TCP	60
9	0.001480666	192.168.48.3	192.168.48.4	TCP	60

Wireshark Packet Capture 2

Filter: ip.addr == 192.168.48.4 && ip.addr == 192.168.48.3

No.	Time	Source	Destination	Protocol	Length
10	0.001480121	192.168.48.3	192.168.48.4	TCP	60
11	0.001480146	192.168.48.3	192.168.48.4	TCP	60
12	0.001480167	192.168.48.3	192.168.48.4	TCP	60
13	0.001480188	192.168.48.3	192.168.48.4	TCP	60
14	0.001491723	192.168.48.4	192.168.48.3	TCP	60
15	0.001500767	192.168.48.4	192.168.48.3	TCP	60
16	0.001504336	192.168.48.4	192.168.48.3	TCP	60
17	0.001507658	192.168.48.4	192.168.48.3	TCP	60
18	0.001510987	192.168.48.4	192.168.48.3	TCP	60
19	0.001590227	192.168.48.3	192.168.48.4	TCP	60

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.

Capturing from any					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
ip.addr == 192.168.48.4 && ip.addr == 192.168.48.3					
No.	Time	Source	Destination	Protocol	Length
14	7.516286576	192.168.48.3	192.168.48.4	TCP	62
15	7.516286706	192.168.48.3	192.168.48.4	TCP	62
16	7.516286733	192.168.48.3	192.168.48.4	TCP	62
17	7.516286758	192.168.48.3	192.168.48.4	TCP	62
18	7.516304419	192.168.48.4	192.168.48.3	TCP	56
19	7.516313003	192.168.48.4	192.168.48.3	TCP	56
20	7.516324049	192.168.48.4	192.168.48.3	TCP	60
21	7.516329137	192.168.48.4	192.168.48.3	TCP	56
22	7.516403595	192.168.48.3	192.168.48.4	TCP	62
23	7.516403683	192.168.48.3	192.168.48.4	TCP	62
ip.addr == 192.168.48.4 && ip.addr == 192.168.48.3					
No.	Time	Source	Destination	Protocol	Length
23	7.516403683	192.168.48.3	192.168.48.4	TCP	62
24	7.516403712	192.168.48.3	192.168.48.4	TCP	62
25	7.516403737	192.168.48.3	192.168.48.4	TCP	62
26	7.516411044	192.168.48.4	192.168.48.3	TCP	56
27	7.516435981	192.168.48.4	192.168.48.3	TCP	60
28	7.516440827	192.168.48.4	192.168.48.3	TCP	56
29	7.516444708	192.168.48.4	192.168.48.3	TCP	56
30	7.516517253	192.168.48.3	192.168.48.4	TCP	62
31	7.516517339	192.168.48.3	192.168.48.4	TCP	62
32	7.516522818	192.168.48.4	192.168.48.3	TCP	56

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)

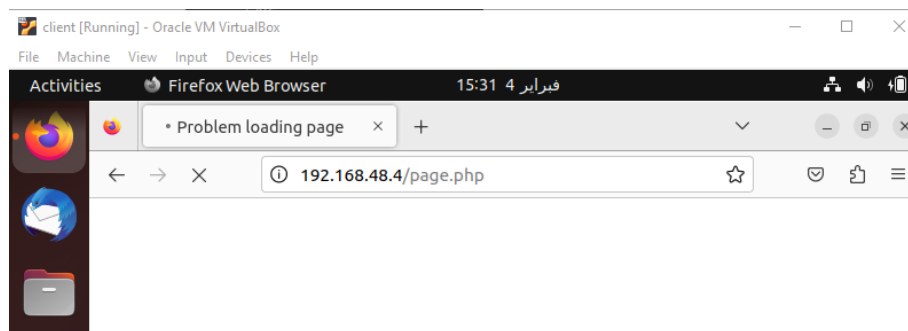
```
attacker@attacker-VirtualBox:~$ sudo git clone https://github.com/jseidl/GoldenEye.git
Cloning into 'GoldenEye'...
remote: Enumerating objects: 102, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 102 (delta 0), reused 2 (delta 0), pack-reused 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/page.php -s 500

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

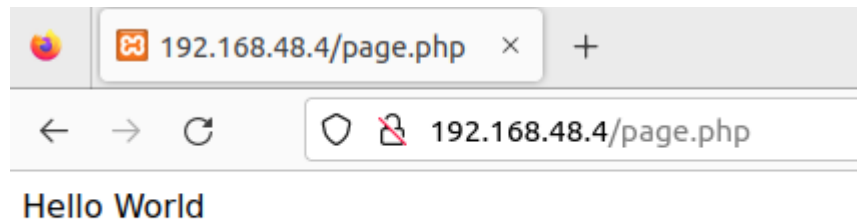
Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
```

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.

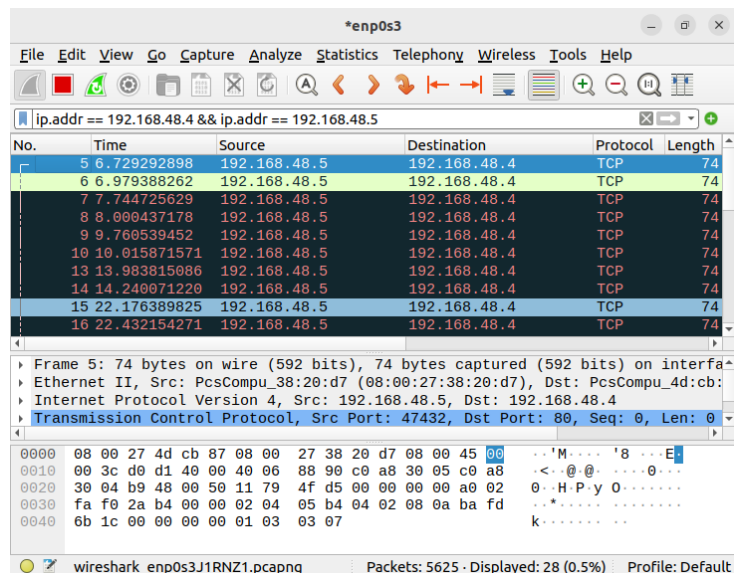


And we try to reach to 192.168.48.4/page.php website from the client machine but we cannot access to it

- 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            multiport dp
1  DROP          tcp  --  192.168.48.3          anywhere               multiport dp
  ports http,telnet,ssh,ftp,ftp-data
2  DROP          tcp  --  192.168.48.3          anywhere               multiport dp
  ports http,telnet,ssh,ftp,ftp-data
3  DROP          tcp  --  192.168.48.3          anywhere               multiport dp
  ports http,telnet,ssh,ftp,ftp-data

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

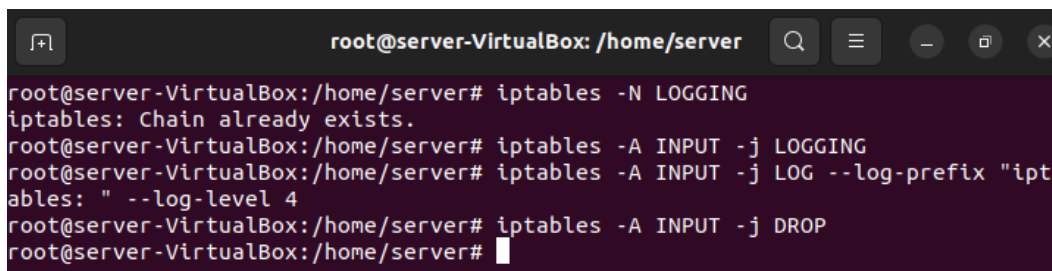
Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination
```

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 "iptables: " --log-level 4
```

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 "iptables: " --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.

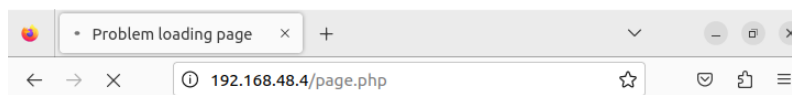
in the last command we used the chain "LOGGING" with option -A, option -j the target is DROP.

```
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



The connection has timed out

The server at 192.168.48.4 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

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

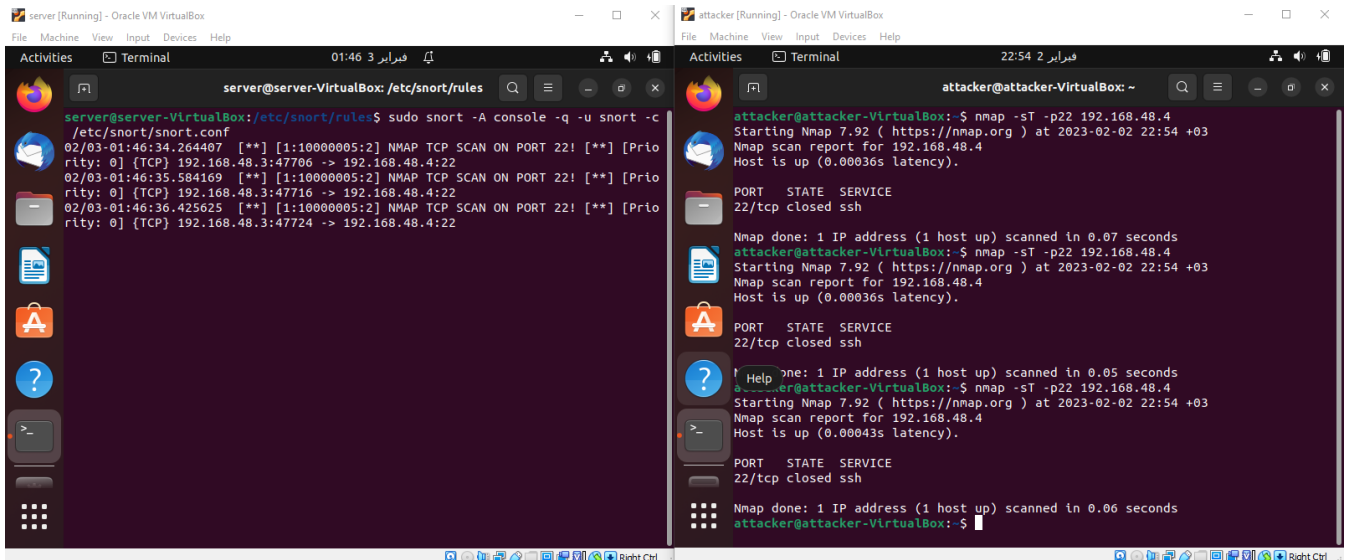
Install and configure snort on server VM to alert on TCP connect scan on port 22 from the attacker VM.

```
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

```
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 !"



```
server@server-VirtualBox: /etc/snort/rules$ sudo snort -A console -q -u snort -c /etc/snort/snort.conf
02/03-01:46:34.264407  [**] [1:10000005:2] NMAP TCP SCAN ON PORT 22! [**] [Priority: 0] [TCP] 192.168.48.3:47706 -> 192.168.48.4:22
02/03-01:46:35.584169  [**] [1:10000005:2] NMAP TCP SCAN ON PORT 22! [**] [Priority: 0] [TCP] 192.168.48.3:47716 -> 192.168.48.4:22
02/03-01:46:36.425625  [**] [1:10000005:2] NMAP TCP SCAN ON PORT 22! [**] [Priority: 0] [TCP] 192.168.48.3:47724 -> 192.168.48.4:22

attacker@attacker-VirtualBox: ~$ nmap -sT -p22 192.168.48.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 22:54 +03
Nmap scan report for 192.168.48.4
Host is up (0.00036s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
attacker@attacker-VirtualBox: ~$ nmap -sT -p22 192.168.48.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 22:54 +03
Nmap scan report for 192.168.48.4
Host is up (0.00036s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
attacker@attacker-VirtualBox: ~$ nmap -sT -p22 192.168.48.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-02 22:54 +03
Nmap scan report for 192.168.48.4
Host is up (0.00043s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
attacker@attacker-VirtualBox: ~$
```

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.