CS 437 / SEC 537 - Lab 1

In this lab, you are asked to obtain a local Kali Linux virtual machine as well as **remote** Ubuntu Linux server and make small scans to familiarize with Nmap, a free network security scanner.

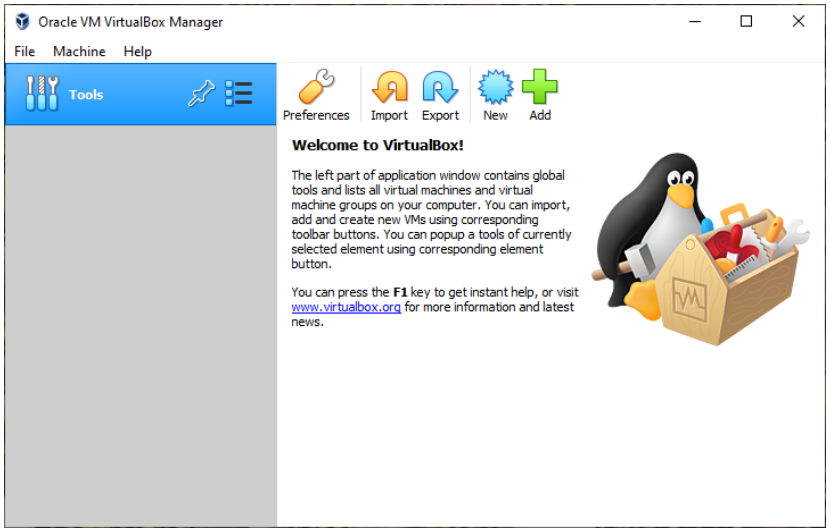
Aims of the lab is the following:

1) Learn how to download and import Kali Linux & Get familiar with Kali Linux
2) How to get free or paid hosting
3) How to deploy a web server to a remote server
4) Get Familiar with Nmap

Part 1 : Learn how to download and import Kali Linux & Get familiar with Kali Linux

Step 1 – Download Kali Linux ISO image
You will need a virtualization platform for opening a virtual machine. So go to https://www.virtualbox.org/ and install free virtualization software virtualbox. Default instructions are easy. Download the exe from the website and enable installation by double-clicking the exe. After that follow the default installation settings.

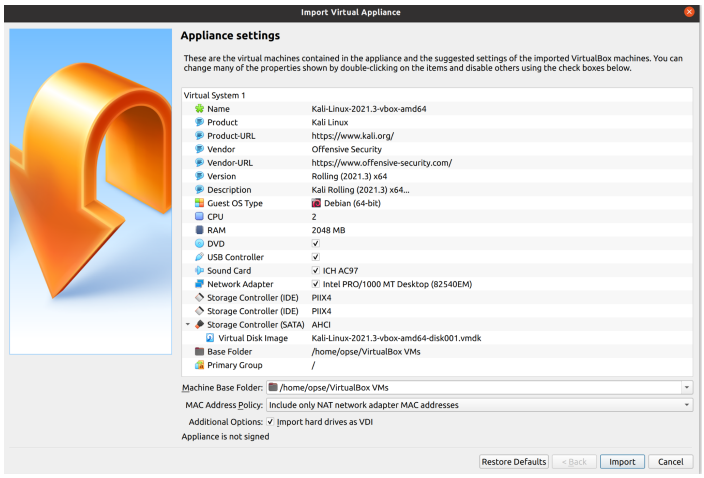
Once installed you will have the following view:



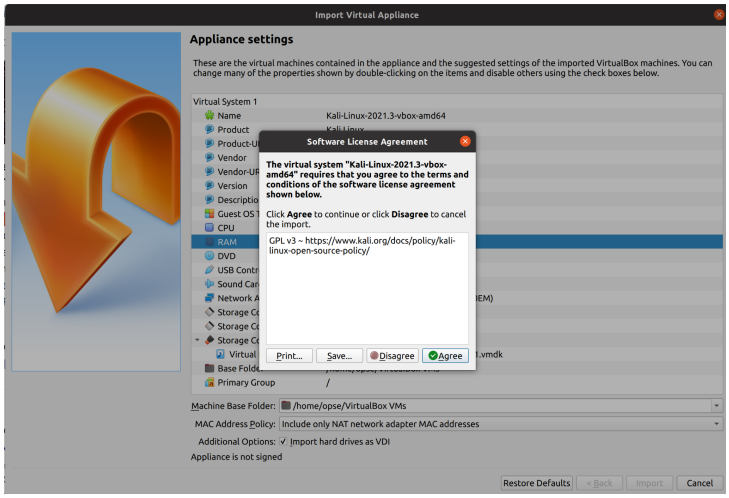
Now it is time to populate the VirtualBox with Kali VM. To install the Kali Linux, you will need an ISO image file. Download Kali Linux ISO from here: https://www.kali.org/get-kali/. Please download the 64 bit or 32 bit image depending on the system you have.

Once downloaded you will get an ISO file in your file system. Following installation is performed in Ubuntu 20.04.3 LTS (VirtualBox on Ubuntu). If you are using Windows, this guide can help you: https://www.shaileshjha.com/how-to-install-kali-linux-2017-in-virtualbox/

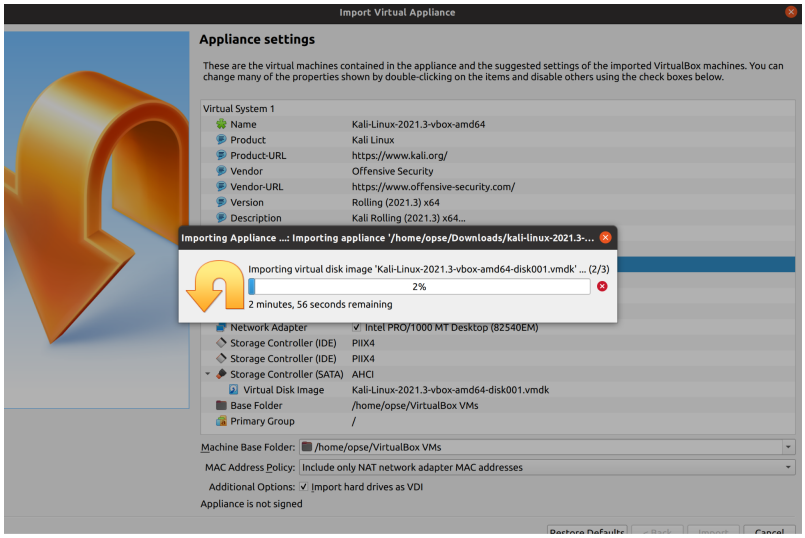
Double click on the ISO. Then you will see the following screen. Change the CPU and RAM according to your PC settings. Minimum setting should be 2GB RAM and 2 CPU. You can give more to make your VM run faster. Mine is 8GB RAM and 4 CPU.



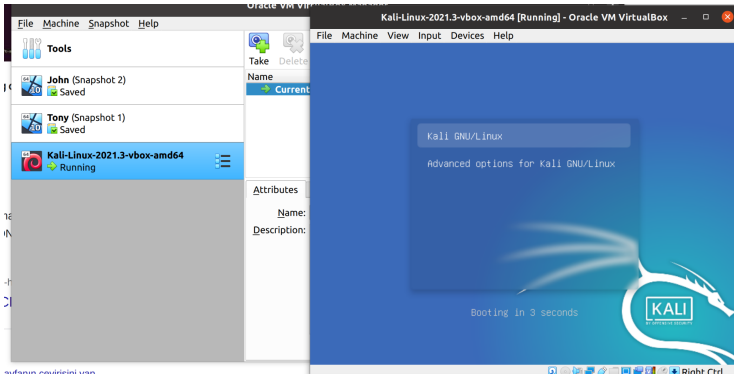
Then click on Import. After that, agree on the software license agreement.

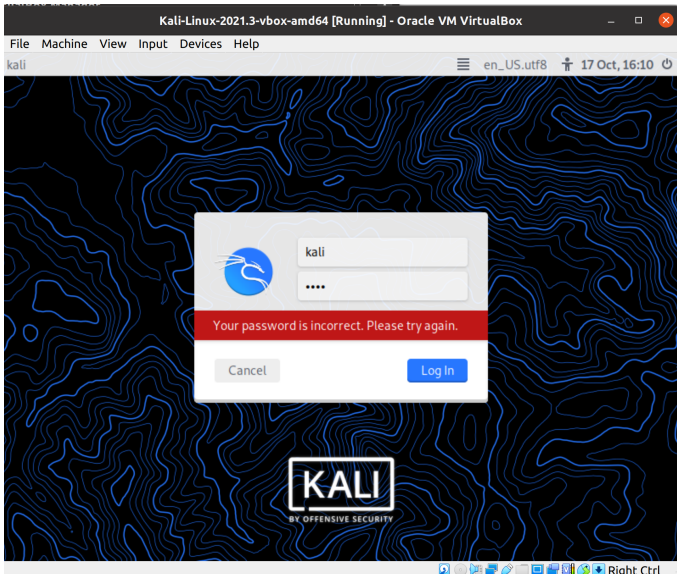


After that the system will import the disk. You will see a similar page.



Once import is over, you will start to see the Kali screen.
ID/Password combınation is kali/kali

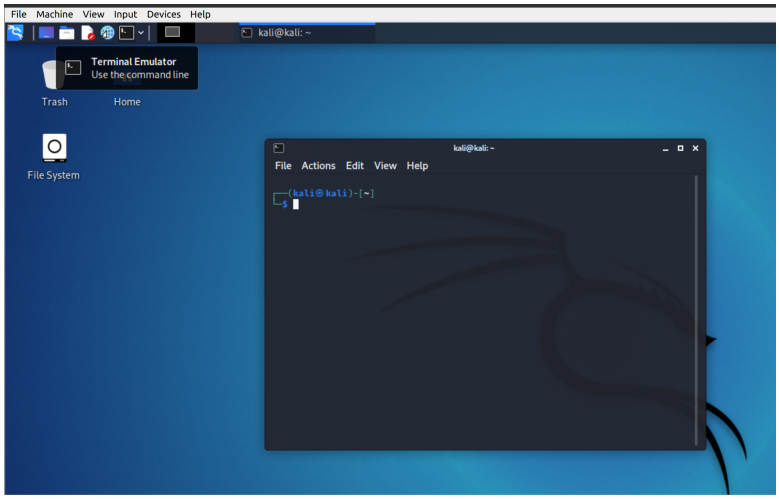




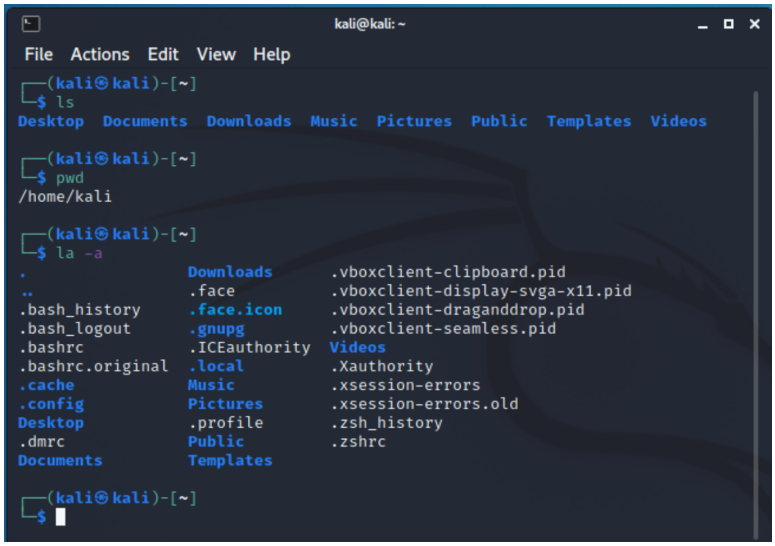
kali/kali

Desktop Kali Linux view

Open Terminal by clicking on the Terminal Emulator button. Once opened, you will get the terminal window greeting you with the kali@kali line.



Now you can try some commands to help you understand where you are.



You can also try other commands you learned from lectures.
Now let's see some security tools on the command line.

Part 2

Get yourself a hosting account to create your remote server.
There 2 hosting options :

1) **Free hosting**

   Big companies offer free hosting for a limited time (typically 2 months).
   These companies includes:

   a) DigitalOcean
   b) Google cloud
   c) Alibaba
   d) Linode (Not sure anymore)

A guide is provided for how to get started with Digitalocean. You can also try Google Cloud or AliBaba. In order to get these accounts you will need a credit card or virtual card (sanal kart). If you don't have it, get it from your bank as soon as possible. Without these you won't be able to get your hosting account. Once get your hosting, get a small server with following :

1 CPU & **1 GB** Memory

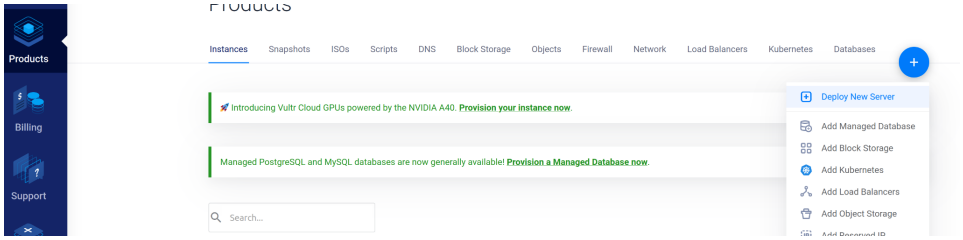
Or higher.
Once your server is ready, find its ID and password and then SSH time.

Then SSH through your server! Follow the video
For windows :
How to Use Putty to SSH on Windows
https://www.youtube.com/watch?v=pWDHUlvcAsg
MAC :
https://www.servermania.com/kb/articles/ssh-mac/

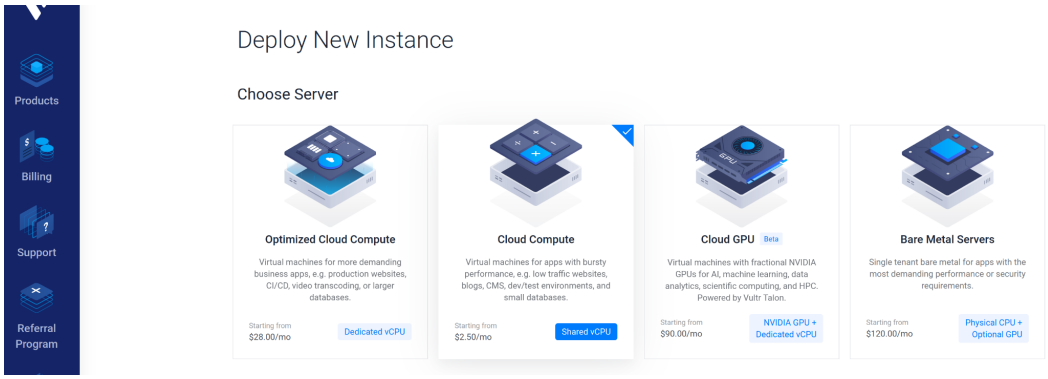
If you have linux:
ssh root@IP address

2) **Paid hosting**

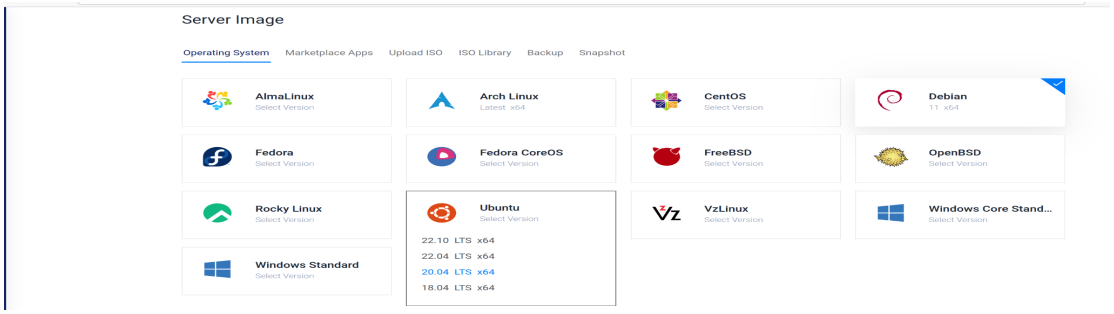
   Of Course here credit card or virtual card is necessary.
   You can get it from Vultr.
   Per month you need to pay 6 dollars.
   Once you get it follow the below:
   Go to products and select 'Deploy New server'



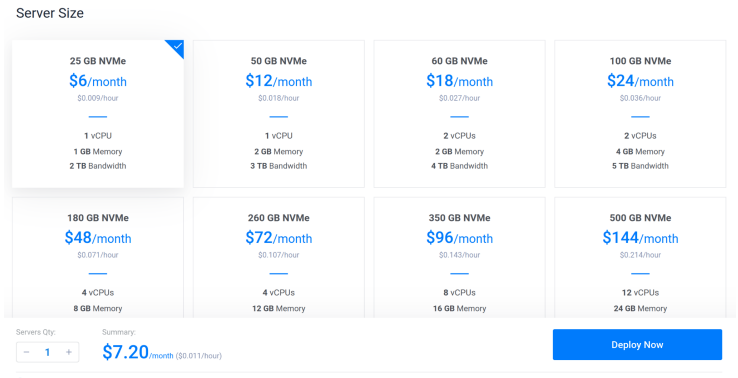
After that select ‘Cloud Compute’



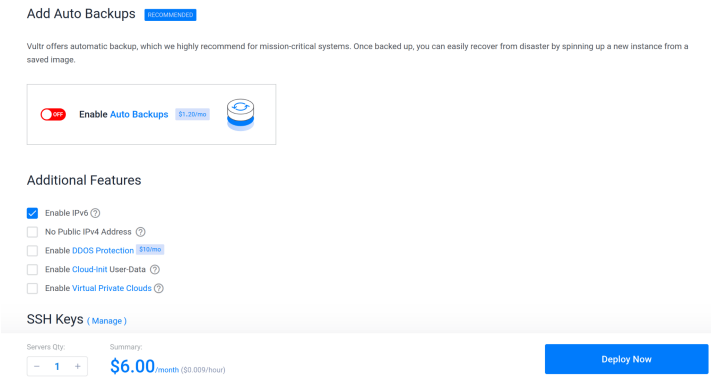
Then pick any country that you want. My advice is to select a country close to Turkey. After that select the operating system. Your options are UBUNTU 20.04 and UBUNTU 18.04. Other versions of Ubuntu are fine.



After that, pick the server.
$6 dollar one 1 vCPU and 1 GB memory



Get rid of Auto Backups protection and deploy the server. MAKE SURE THAT ‘AUTO BACKUPS’ İS OFF!!. Now you save money!



Then SSH through your server! Follow the video
For windows :
How to Use Putty to SSH on Windows
https://www.youtube.com/watch?v=pWDHUlvcAsg
MAC :
https://www.servermania.com/kb/articles/ssh-mac/

If you have linux:
ssh root@IP address

Part 3 : How to deploy a web server to a remote server

Make sure your system is up to date and patched.
To do that, type the following:

sudo apt update
sudo apt upgrade

```
root@vultr:~# sudo apt update
Hit:1 https://apprepo.vultr.com/ubuntu universal InRelease
Hit:2 http://de.clouds.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:4 http://de.clouds.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:5 http://de.clouds.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:6 http://de.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [600 B]
Get:7 http://de.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [664 B]
Fetched 337 kB in 1s (429 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
root@vultr:~# sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
Try Ubuntu Pro beta with a free personal subscription on up to 5 machines.
Learn more at https://ubuntu.com/pro
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@vultr:~#
```

Install Apache 2 software:

sudo apt install apache2

```
root@vultr:~#
root@vultr:~# ls
snap
root@vultr:~# sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 1606 kB of archives.
After this operation, 7125 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://de.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-4ubuntu2 [10.5 kB]
Get:2 http://de.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-ldap amd64 1.6.1-4ubuntu2 [8736 B]
Get:3 http://de.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libjansson4 amd64 2.12-1build1 [28.9 kB]
Get:4 http://de.clouds.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.2-0 amd64 5.2.4-1.1build3 [106 kB]
Get:5 http://de.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-bin amd64 2.4.41-4ubuntu3.12 [1181 kB]
Get:6 http://de.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-data all 2.4.41-4ubuntu3.12 [159 kB]
Get:7 http://de.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2 amd64 2.4.41-4ubuntu3.12 [95.6 kB]
Get:8 http://de.clouds.archive.ubuntu.com/ubuntu focal/main amd64 ssl-cert all 1.0.39 [17.0 kB]
Fetched 1606 kB in 0s (8373 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
(Reading database ... 118805 files and directories currently installed.)
Preparing to unpack .../0-libaprutil1-dbd-sqlite3_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.1-4ubuntu2) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
Preparing to unpack .../1-libaprutil1-ldap_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1-ldap:amd64 (1.6.1-4ubuntu2) ...
Selecting previously unselected package libjansson4:amd64.
Preparing to unpack .../2-libjansson4_2.12-1build1_amd64.deb ...
Unpacking libjansson4:amd64 (2.12-1build1) ...
Selecting previously unselected package liblua5.2-0:amd64.
Preparing to unpack .../3-liblua5.2-0_5.2.4-1.1build3_amd64.deb ...
Unpacking liblua5.2-0:amd64 (5.2.4-1.1build3) ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../4-apache2-bin_2.4.41-4ubuntu3.12_amd64.deb ...
Unpacking apache2-bin (2.4.41-4ubuntu3.12) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../5-apache2-data_2.4.41-4ubuntu3.12_all.deb ...
Unpacking apache2-data (2.4.41-4ubuntu3.12) ...
Selecting previously unselected package apache2.
Preparing to unpack .../6-apache2_2.4.41-4ubuntu3.12_amd64.deb ...
Unpacking apache2 (2.4.41-4ubuntu3.12) ...
```

Make sure Apache service started on boot

We are going to use the systemctl command as follows to enable the apache2.service:

sudo systemctl is-enabled apache2.service

If not enabled, enable it, run:

sudo systemctl enable apache2.service

```
root@vultr:~#  sudo systemctl is-enabled apache2.service
enabled
root@vultr:~#  sudo systemctl enable apache2.service
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@vultr:~#
```

Check your version :

apache2 -version

```
root@vultr:~# apache2 -version
Server version: Apache/2.4.41 (Ubuntu)
Server built:   2022-06-14T13:30:55
```

Firewall configuration

First, let's list the application profiles that we need to give Apache access to. Run the following command to do so:

sudo ufw app list

```
tin@ubuntu:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
```

We will use the highly restrictive profile 'Apache' to enable network ctivity on port 80.

sudo ufw allow 'Apache'

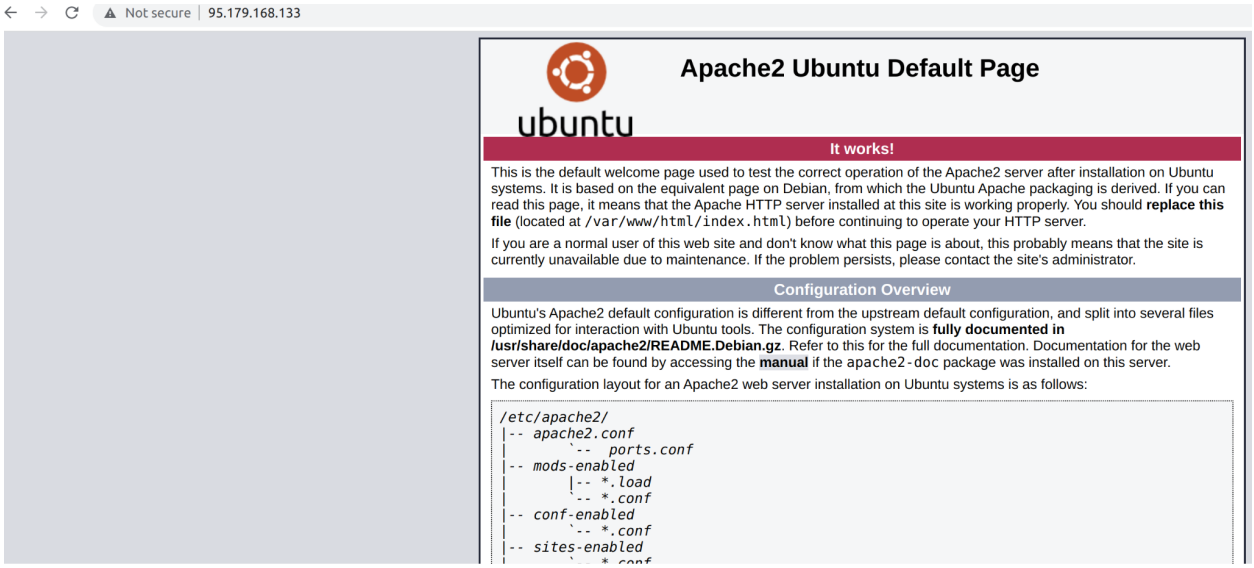
```
root@vultr:~# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)

root@vultr:~# hostname -I
hostname: the specified hostname is invalid
root@vultr:~# sudo ufw allow 'Apache'
ERROR: Bad port
root@vultr:~# sudo ufw allow 'Apache'
Rule added
Rule added (v6)
root@vultr:~# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
Apache                     ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
Apache (v6)                ALLOW       Anywhere (v6)
```

Find the status of apache2 server

sudo systemctl status apache2.service

```
root@vultr:~# sudo systemctl status apache2.service
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2022-10-24 09:13:32 UTC; 11min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 28807 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 28821 (apache2)
      Tasks: 55 (limit: 1066)
     Memory: 5.3M
     CGroup: /system.slice/apache2.service
             ├─28821 /usr/sbin/apache2 -k start
             ├─28822 /usr/sbin/apache2 -k start
             └─28823 /usr/sbin/apache2 -k start

Oct 24 09:13:32 vultr systemd[1]: apache2.service: Succeeded.
Oct 24 09:13:32 vultr systemd[1]: Stopped The Apache HTTP Server.
Oct 24 09:13:32 vultr systemd[1]: Starting The Apache HTTP Server...
Oct 24 09:13:32 vultr systemd[1]: Started The Apache HTTP Server.
```

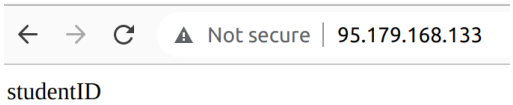
Check your IP on the browser :
Now you must be seen default Apache page



Apache server change default page:
Default page is in :**/var/www/html**

```
root@vultr:/var/www/html# ls
index.html
root@vultr:/var/www/html# cat index.html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2016-11-16
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }
```

Remove index.html
Use nano : https://linuxize.com/post/how-to-use-nano-text-editor/
Create new index.html
Put your student ID. Your STUDENT ID!



studentID

Part 4

Networks can be easily scanned and classified with various tools.
Most notable one is NMAP.

Nmap (Network Mapper)

Nmap or Network Mapper is a free and open source network scanner created by Gordon Lyon. Typically Nmap is used to discover hosts and services on the Internet by sending network packets and analyzing the responses.
Website : https://nmap.org/
Download : https://nmap.org/download.html
Explanation for installation: https://www.priviasecurity.com/nmap-nedir-part-1-3/

Nmap features include:

- Host discovery – Identifying hosts on a network.
    - IoT devices
        - Cameras, DVRs, Modems, Routers, Switches
    - SCADA systems
    - Databases
        - Elasticsearch
        - MongoDB
        - Redis
        - MySQL
- Port scanning
    - FTP
    - Telnet
    - DNS
- Version detection
    - Elasticsearch version
    - Apache 2.1
- OS detection
    - Windows
    - Linux
- Scriptable interaction with the target
    - using Nmap Scripting Engine(NSE)

Let’s turn back to Kali. You can use nmap in Kali’s terminal screen. Typing nmap would show you what can be done using nmap.

Query examples:

EXAMPLES:

nmap -v -A scanme.nmap.org

nmap -v -sn 192.168.0.0/16 10.0.0.0/8

nmap -v -iR 10000 -Pn -p 80

SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

Application Version Detection

Nmap version detection is activated using the -sV option. Also, there are some additional options that are available that begin with -- version, which help you determine the intensity of the scan. Once a Nmap scan is run with the version detection flag, the tool will list its output with the:

1) port
2) port state
3) service

4) version that it detects

Let’s take a look at it.

Well, version detection is performed using the -sV flag.
Now let’ take a look what happens:
1) Nmap conducts a port scan and then obtains the results and looks for open ports that it can use to find service and application versions running on the target.
2) When open ports are detected, the tool is going to first try to do a TCP connection to the open port on the target.
3) If the connection is successful, Nmap will try to capture any information coming from the target.
Looks for :
Banners

Banner information for an IoT device is above.

If a banner is not available / sent, and some other type of response is sent by the targeted host, Nmap can then evaluate output to detect the service and version. After this port, other ports will receive the same treatment. If no results are found, UDP probes will be made. If still no results come out, Nmap may then move on to try and detect it by sending SSL probes. Here, Nmap is still looking for responses and something to help with application detection. If the SSL probes are successful and the target responds to the probe, it will send an SSL connection to the target port. Again if a successful connection is established, Nmap will listen to the target and look for clues to help with identification. Next, Nmap will move on and attempt an RPC or SMB probe. Once it obtains a response from the targeted host, it will start an RPC or SMB brute force against the target to try to get any information it can. If still unable to match it to a particular version, then Nmap will produce a fingerprint of the version and output it to the screen. In this case, you can take that fingerprint and send it to Nmap along with the application version so that they can improve their detection methods in the future.

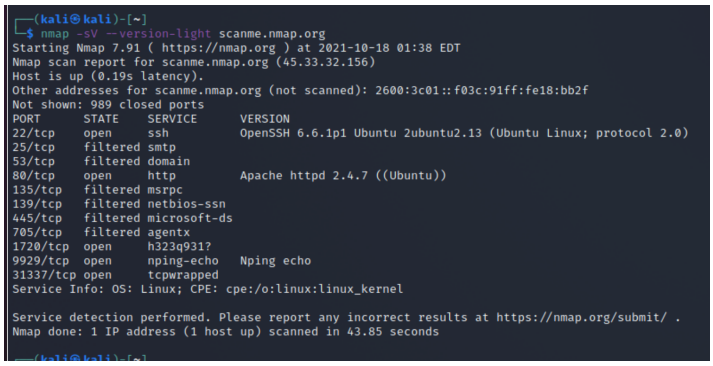
Options for version detection

Version detection has four options to establish the ***intensity*** of the scan.
Version intensity just controls:
a) how many probes are sent
b) how many different types of probes are sent to each port to try to determine the version
Version intensity can be between 0 to 9.
Also changes time and stealthiness required.

--version-light actually is just a shortcut for --version- intensity level 2
--version-all is a shortcut for --version-intensity level 9.
--version- trace is going to output the process that Nmap is following when it's conducting the version scan and show you the steps along the way so that you can see how it's actually going about detecting it.

Example:

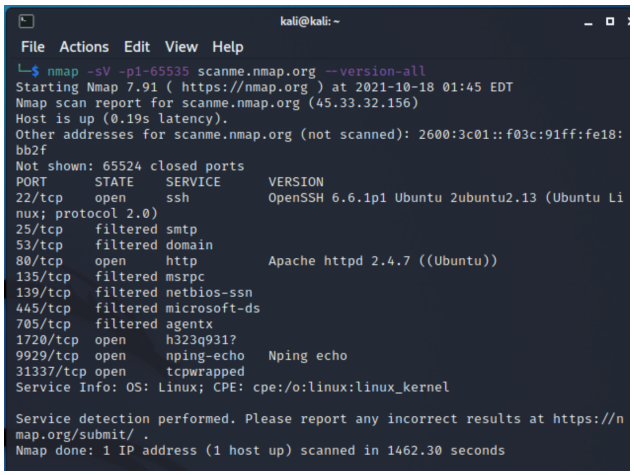
nmap -sV --version-light scanme.nmap.org



You manage to find the underlying OS (Linux). You discover the SSH application name and version. Also you found Apache 2.4.7 is there. Lastly, a Nping Echo service.

Try other queries like :

nmap -sV -p1-65535 scanme.nmap.org --version-all



More queries:

nmap -p0- -v -A -T4 scanme.nmap.org

Nmap scan is modified with four options. -p0- asks Nmap to scan every possible TCP port, -v asks Nmap to be verbose about it, -A enables aggressive tests such as remote OS detection, service/version detection, and the Nmap Scripting Engine (NSE). Finally, -T4 enables a more aggressive timing policy to speed up the scan.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p0- -v -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-18 01:50 EDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:50
Completed NSE at 01:50, 0.00s elapsed
Initiating NSE at 01:50
Completed NSE at 01:50, 0.00s elapsed
Initiating NSE at 01:50
Completed NSE at 01:50, 0.00s elapsed
Initiating Ping Scan at 01:50
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 01:50, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:50
Completed Parallel DNS resolution of 1 host. at 01:50, 0.00s elapsed
Initiating Connect Scan at 01:50
Scanning scanme.nmap.org (45.33.32.156) [65536 ports]
Discovered open port 1720/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Connect Scan Timing: About 5.60% done; ETC: 01:59 (0:08:42 remaining)
Connect Scan Timing: About 12.93% done; ETC: 01:59 (0:08:11 remaining)
Connect Scan Timing: About 18.23% done; ETC: 01:59 (0:07:42 remaining)
Connect Scan Timing: About 24.69% done; ETC: 01:59 (0:06:46 remaining)
Connect Scan Timing: About 30.60% done; ETC: 01:59 (0:06:10 remaining)
Discovered open port 31337/tcp on 45.33.32.156
Connect Scan Timing: About 37.25% done; ETC: 01:59 (0:05:40 remaining)
Connect Scan Timing: About 44.35% done; ETC: 01:59 (0:05:10 remaining)
Connect Scan Timing: About 51.10% done; ETC: 01:59 (0:04:25 remaining)
Connect Scan Timing: About 56.73% done; ETC: 01:59 (0:03:54 remaining)
Connect Scan Timing: About 62.61% done; ETC: 01:59 (0:03:27 remaining)
Connect Scan Timing: About 68.08% done; ETC: 01:59 (0:02:58 remaining)
Connect Scan Timing: About 73.16% done; ETC: 01:59 (0:02:30 remaining)
Connect Scan Timing: About 78.59% done; ETC: 01:59 (0:02:00 remaining)
Connect Scan Timing: About 84.23% done; ETC: 01:59 (0:01:28 remaining)
Connect Scan Timing: About 89.66% done; ETC: 01:59 (0:00:58 remaining)
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 01:59, 566.92s elapsed (65536 total ports)
Initiating Service scan at 01:59
Scanning 5 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 02:02, 156.34s elapsed (5 services on 1 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 02:02
Completed NSE at 02:02, 14.21s elapsed
Initiating NSE at 02:02
Completed NSE at 02:02, 1.23s elapsed
Initiating NSE at 02:02
Completed NSE at 02:02, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
```

```
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 65524 closed ports
PORT      STATE    SERVICE      VERSION
0/tcp     filtered unknown
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Li
nux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
705/tcp   filtered agentx
1720/tcp  open     h323q931?
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 02:02
Completed NSE at 02:02, 0.00s elapsed
Initiating NSE at 02:02
Completed NSE at 02:02, 0.00s elapsed
Initiating NSE at 02:02
Completed NSE at 02:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 739.38 seconds
```

OS Detection

Now let’s run the stealth SYN scan (-sS).
Run version detection (-sV)
Operating system detection with -O

Include the --osscan- guess to more aggressively guess the operating systems

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -O --osscan-guess scanme.nmap.org                1 ×

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-18 01:59 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 989 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Li
nux; protocol 2.0)
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
705/tcp   filtered agentx
1720/tcp  open     h323q931?
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: QEMU user mode network gateway (96%), Bay Networks Bay
Stack 450 switch (software version 3.1.0.22) (89%), Konica Minolta 7035 print
er (88%), Allied Telesyn AT-9006SX/SC switch (88%), Linux 2.6.18 (CentOS 5, x
86_64, SMP) (87%), Bay Networks BayStack 450 switch (software version 4.2.0.1
6) (87%), HP 9100c Digital Sender printer (J3113A) (87%), GNU Hurd 0.3 (87%),
 Minolta Di550 laser printer (86%), NEC SuperScript printer (86%)
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=10/18%OT=22%CT=1%CU=42427%PV=N%DS=2%DC=I%G=Y%TM=616D0D
OS:ED%P=x86_64-pc-linux-gnu)SEQ(SP=12%GCD=FA00%ISR=9C%TI=I%CI=RD%II=I%TS=U)
OS:SEQ(SP=30%GCD=FA00%ISR=AB%CI=RD%TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4
OS:%O5=M5B4%O6=M5B4)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN
OS:(R=Y%DF=N%T=41%W=FFFF%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%T=41%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%
OS:S=Z%A=S+%F=AR%O=%RD=0%Q=)T4(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=100%W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%D
OS:F=N%T=3C%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=3
OS:9%CD=S)

Network Distance: 2 hops
```

```
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.05 seconds
```

Install it on your UBUNTU:

Opening up the terminal and executing the following command:

```
sudo apt install nmap
```

```
root@vultr:/var/www/html# sudo apt install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  liblinear4 liblua5.3-0 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  liblinear4 liblua5.3-0 lua-lpeg nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 5528 kB of archives.
After this operation, 26.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://de.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64 2.3.0+dfsg-3build1 [41.7 kB]
Get:2 http://de.clouds.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.3-0 amd64 5.3.3-1.1ubuntu2 [116 kB]
Get:3 http://de.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:4 http://de.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 nmap-common all 7.80+dfsg1-2build1 [3676 kB]
Get:5 http://de.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 nmap amd64 7.80+dfsg1-2build1 [1662 kB]
Fetched 5528 kB in 0s (25.4 MB/s)
Selecting previously unselected package liblinear4:amd64.
(Reading database ... 119482 files and directories currently installed.)
Preparing to unpack .../liblinear4_2.3.0+dfsg-3build1_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Selecting previously unselected package liblua5.3-0:amd64.
Preparing to unpack .../liblua5.3-0_5.3.3-1.1ubuntu2_amd64.deb ...
Unpacking liblua5.3-0:amd64 (5.3.3-1.1ubuntu2) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.80+dfsg1-2build1_all.deb ...
Unpacking nmap-common (7.80+dfsg1-2build1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.80+dfsg1-2build1_amd64.deb ...
```

Then ready to go :

```
root@vultr:/var/www/html# nmap -p0- -v -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-24 09:48 UTC
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:48
Completed NSE at 09:48, 0.00s elapsed
Initiating NSE at 09:48
Completed NSE at 09:48, 0.00s elapsed
Initiating NSE at 09:48
Completed NSE at 09:48, 0.00s elapsed
Initiating Ping Scan at 09:48
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 09:48, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:48
Completed Parallel DNS resolution of 1 host. at 09:48, 0.21s elapsed
Initiating SYN Stealth Scan at 09:48
Scanning scanme.nmap.org (45.33.32.156) [65536 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 14.16% done; ETC: 09:52 (0:03:08 remaining)
SYN Stealth Scan Timing: About 27.93% done; ETC: 09:52 (0:02:37 remaining)
SYN Stealth Scan Timing: About 42.37% done; ETC: 09:52 (0:02:04 remaining)
SYN Stealth Scan Timing: About 59.19% done; ETC: 09:51 (0:01:23 remaining)
Discovered open port 31337/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 73.73% done; ETC: 09:51 (0:00:54 remaining)
```

Lab Questions

1) Now that you have KALI linux installed! Please take a screenshot of your Kali machine's CPU info
   (First use: cat /proc/cpuinfo | grep 'core id'
   Then: cat /proc/cpuinfo)
   Entire screenshot is needed! Whole page including queries and the whole responses!
   Screenshots of all processor info as well as query is needed! Processor information must be clearly shown after the query! Don't copy paste responses! Screenshot is needed!

2) Now that you have a remote server, you are asked to follow the procedure and deploy an Apache 2 server. After that change the main page with your studentID. Required: Take a screenshot of the page.
   After the submission, **don't have apache or page down (Do not stop your server since we will check it)!!**
   We will make sure that this task is done by scanning your page
   Web Server must be on port 80!! With your student ID!
   Points Will be given based on : All or nothing policy!

   Your server IP's address must be sent to the following email addresses:

   cs437help@gmail.com

Email format must be :
Title:
'CS437/SEC537 IP address'
Body:
'You can find my IP address and info related below'
'IP address: xx.xx.xx.xxYourIPGoesHere'
'Provider : Digital Ocean'
'Student ID : xxxxxx-YourIDGoesHere'
'Student name: YourNameGoesHere'
'Thank you''

3) Now you are asked to scan the following hosts with Nmap and try to determine what kind of services are behind it! **Using your remote server.** You will use other Nmap queries to gather more information from the hosts. *You cannot use other security tools to scan the system. If we see any inconsistency or other tool scans you will immediately get 0.* So explain the results very well and how you

obtain them. Additionally, we require a screenshot of every query used (**You need to include time in your screenshot otherwise you will get PENALTY.**).
Lastly, IP addresses used in the analysis should be put in a txt file
(Your remote Ubuntu server's IP address).
This file should contain your name and .txt extension
Format yourName_yourSurname.txt
So for Orçun Yılmaz, IP file name would be orcun_yilmaz.txt.
No screenshot and IP file no points.

Requirements:

1) Screenshots of queries used to identify services
2) Screenshots of queries used to determine OS type
3) Explanation for both
4) Any online source used (URLs) to make decisions
5) Results found !(Services, applications, versions and also OS type (Linux? Windows?)) and their explanation
6) IP addresses used (while probing) should be in a txt file with the given format. Also get evidence from the Internet (for instance: https://whatismyipaddress.com/tr/ip-im). Screenshot will be enough.

Target hosts:

1) 64.176.188.181
2) 45.63.99.102

Not: Timestamps are very important for us. Because one service is designed to dynamically change its port number. So even if a screenshot is taken, explain your results with Timestamps!

Things to consider:

1)You will submit your report via su course plus
You **might** be given a time slot to demonstrate your work. If we find issues with your report this could be implemented.
2) You need to submit a zip file that includes the .txt file explained above and a pdf that includes all your answers. An answer for the question should include the explanation, the screenshot which includes the necessary information (such as time) as it's explained before in the document. Do NOT put screenshots in the end or any irrelevant place in your document in other words put them with corresponding question and explanation.
3) In the case of plagiarism, both parties will get 0 for this assignment and receive additional grade penalty (10% overall) for the overall course.-> So, the current assignment will be marked "0" and a 10% overall grade penalty will be applied.