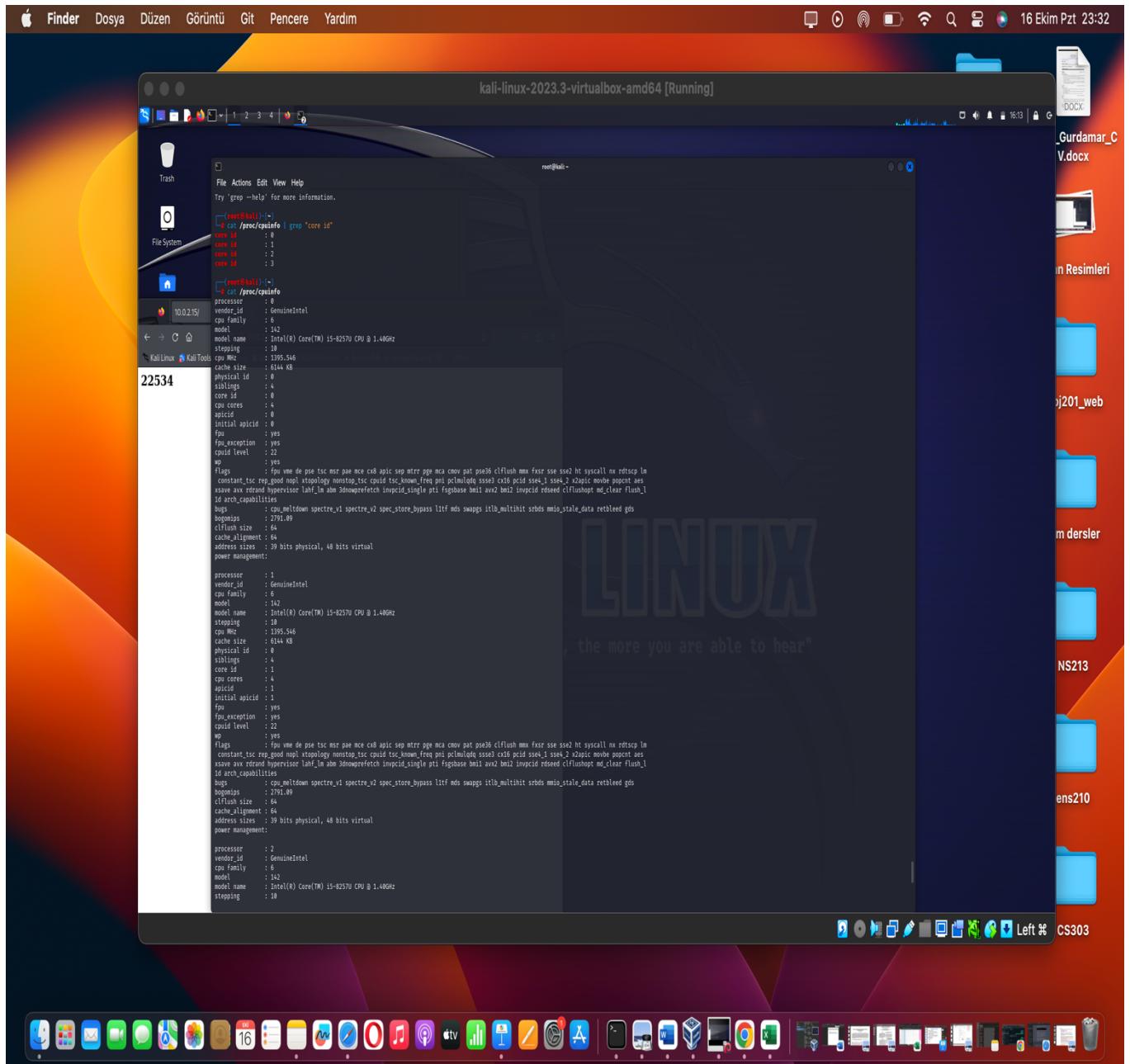


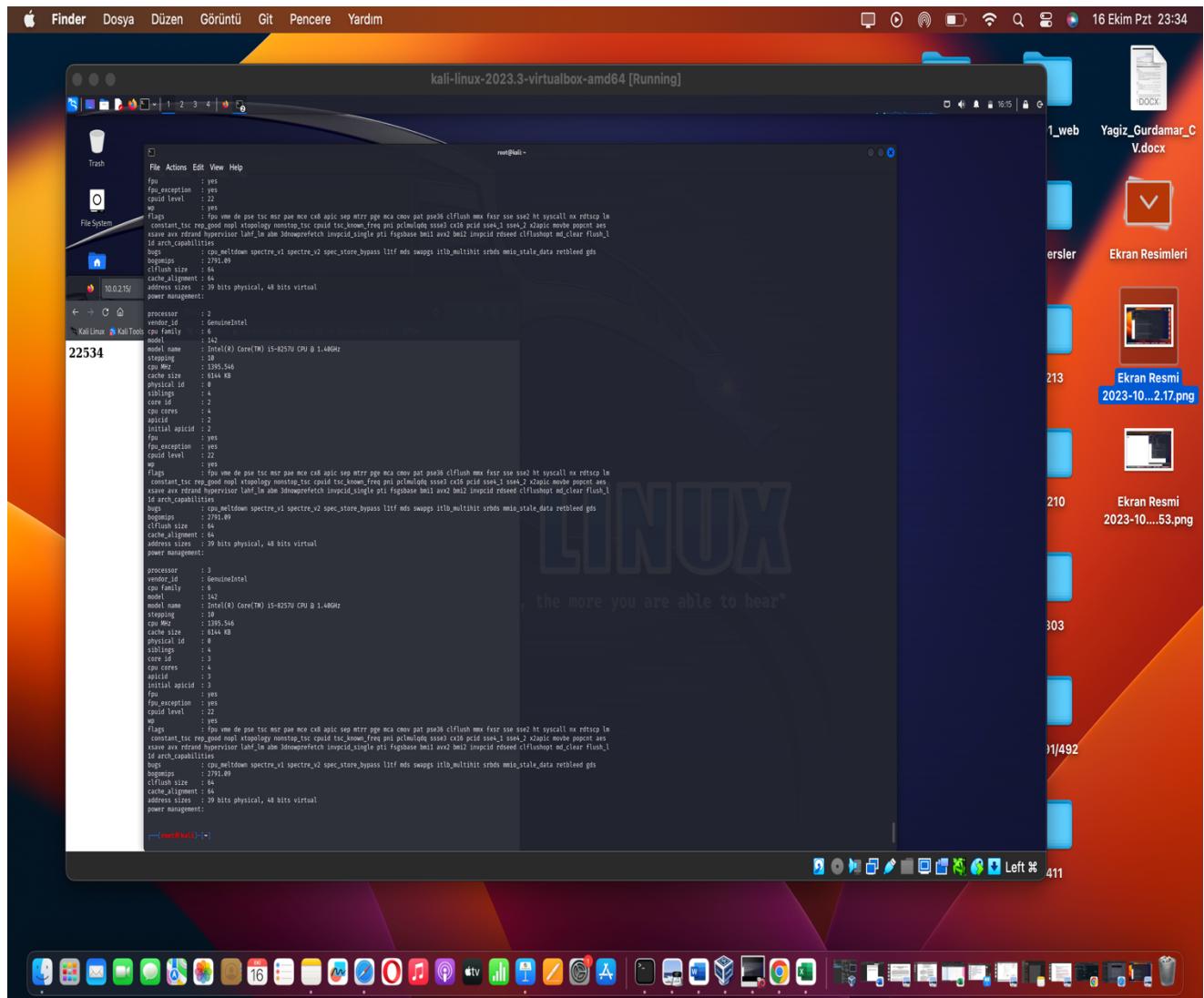
CS437 LAB1 REPORT

Part 1:

1. After I started my kali linux first I used `cat /proc/cpuinfo | grep 'core id'`
2. Then I runned `cat/proc/cpuinfo`



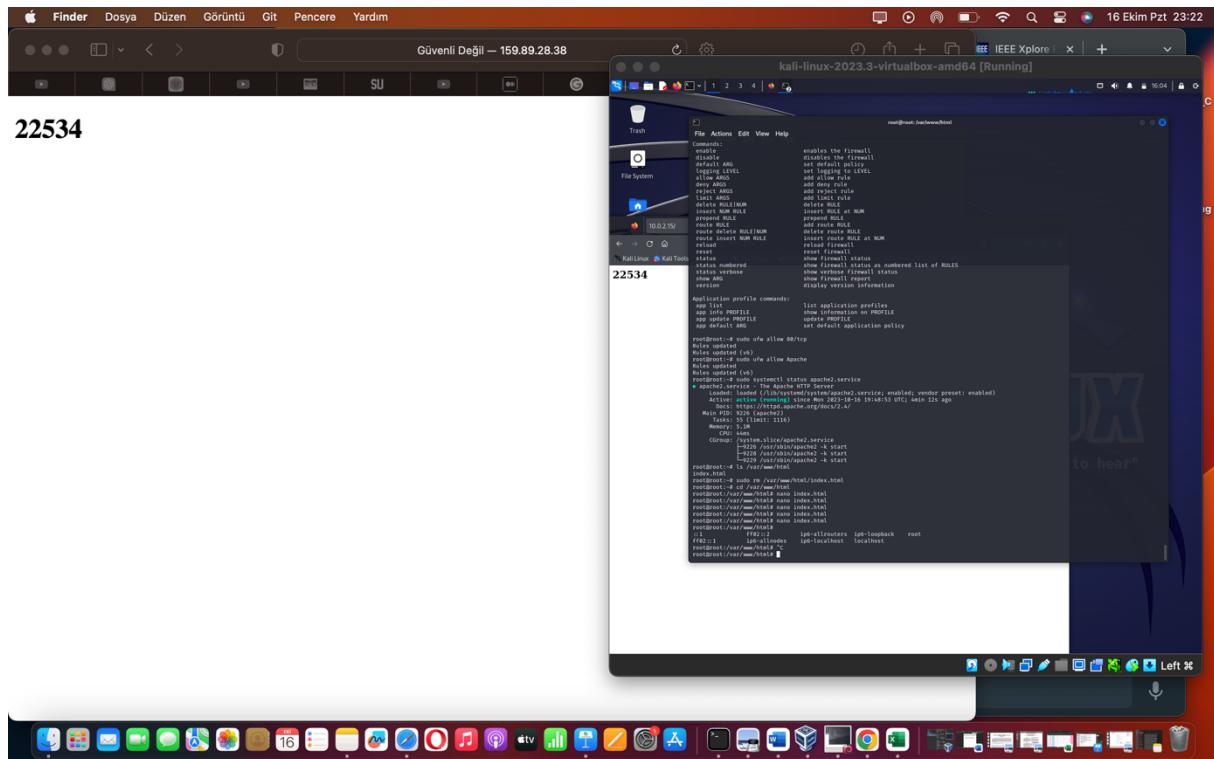
Second part of screenshot:



Part 2:

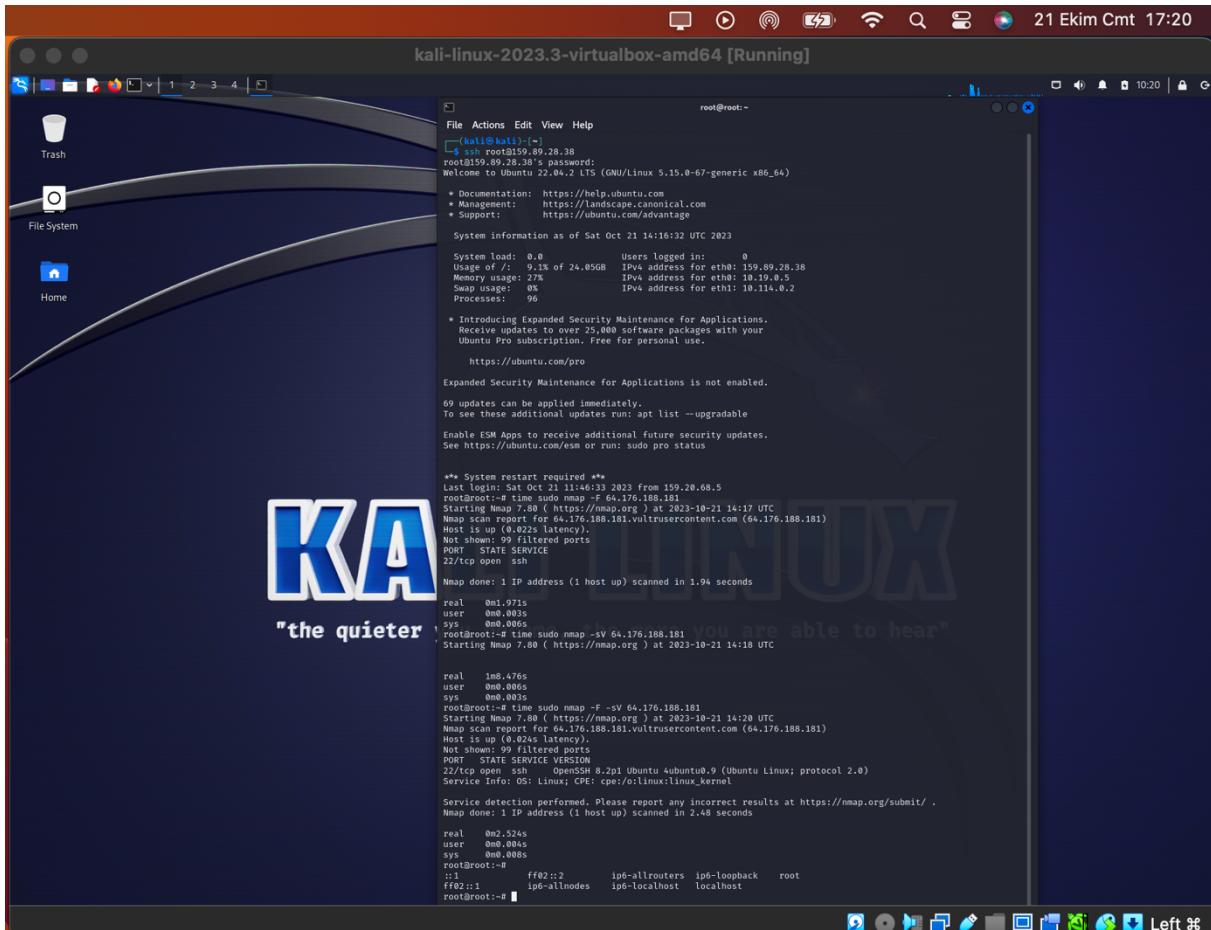
So for part2 I runned the commands that you wrote for my server, which I created from Digital Ocean. I installed Apache2 and then allowed. I already sent my ip address but here it is: 159.89.28.38

After re-wrote html page my server looks like this, also you can see some of my commands:



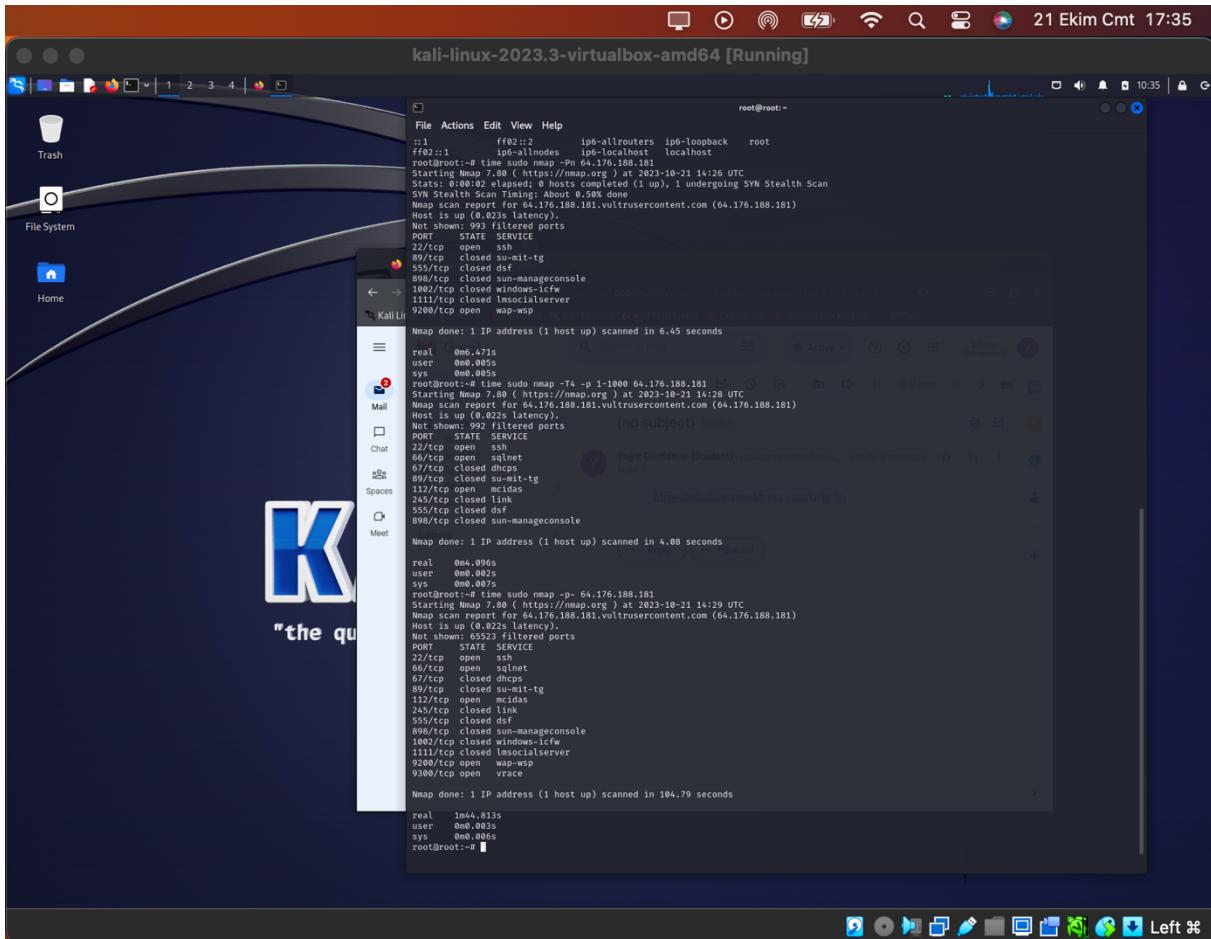
Part 3:

So for part 3 first I installed nmap to my server. When I was searching for commands I used nmap.org. After installation of nmap I started with small steps. Firstly I checked first 100 ports with sudo nmap -F 64.176.188.181. Also for finding version we can add -sV command :



As you can see here port 22/tcp is open and running the SSH service, which is identified as "OpenSSH 8.2p1 Ubuntu 4ubuntu0.9" on an Ubuntu Linux system. The protocol version is 2.0.

After that, I expanded my search and looked for all ports. As you can see, the **-Pn** command is used to avoid sending pings, which means I did not check whether the systems were responding or not for a quicker search. The **-T4** option is for search speed. When I first tried the **-p-** command (which is for checking all ports), it took a long time. I looked for this command, and it was faster.



- **`sudo nmap -Pn 64.176.188.181:`**

The scan was performed without sending any ping probes (`-Pn`), which means it didn't check if the host was up or not.

The host is detected as up with a latency of 0.023 seconds.

The scan detected that port 22/tcp (SSH) is open and responsive.

Several other ports are closed.

This scan took 6.45 seconds to complete.

- **`sudo nmap -T4 -p 1-1000 64.176.188.181:`**

This scan focused on scanning the first 1000 ports (ports 1 to 1000).

It detected that port 22/tcp (SSH) and port 66/tcp (SQLNet) are open and responsive.

Port 112/tcp (McIDAS) is also open.

Other ports are closed.

The scan took 4.08 seconds to complete.

- **sudo nmap -p- 64.176.188.181:**

This scan attempted to scan all 65535 possible ports.

It detected that port 22/tcp (SSH), port 66/tcp (SQLNet), port 112/tcp (McIDAS), port 9200/tcp (wap-wsp), and port 9300/tcp (vrace) are open and responsive.

Many ports are filtered, which means they didn't respond to the scan.

This scan took 104.79 seconds to complete.

So I specifically looked for ports where I tried port 22 and checked its version:

```
root@root:~# time sudo nmap -p 22 64.176.188.181
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 14:38 UTC
Nmap scan report for 64.176.188.181.vultrusercontent.com (64.176.188.181)
Host is up (0.022s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

real    0m0.105s
user    0m0.010s
sys     0m0.000s
root@root:~#
```

Last thing to do is for OS type, first I runned nmap -O which brings me just OS types:

The screenshot shows a terminal window titled "kali-linux-2023.3-virtualbox-amd64 [Running]" running on a Kali Linux desktop environment. The terminal displays the results of an nmap scan against a target host at 64.176.188.181. The output includes three separate nmap runs:

- The first run shows a single closed port (898/tcp) for "sun-manageconsole".
- The second run shows multiple open ports: 22/tcp (ssh), 66/tcp (sqlnet), 67/tcp (closed dhcps), 89/tcp (closed su-mit-tg), 112/tcp (open mcidas), 245/tcp (closed link), 555/tcp (closed dsf), 898/tcp (closed sun-manageconsole), 1002/tcp (closed windows-icfw), 1111/tcp (closed lmsocialserver), 9200/tcp (open wap-wsp), and 9300/tcp (open vrace). It also shows a message about a mail inbox.
- The third run shows a single open port (22/tcp) for ssh.

At the bottom of the terminal, the Aggressive OS guesses section lists various Linux distributions and devices as potential matches:

```
Aggressive OS guesses: Linux 3.10 - 4.11 (93%), Linux 3.2 - 4.9 (92%), Linux 2.6.32 - 3.10 (92%), HP P2000 G3 NAS device (91%), Oracle VM Server 3.4.2 (Linux 4.1) (91%), Infomir MAG-250 set-top box (91%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (91%), Ubiquiti Pico S station WAP (AirOS 5.2.6) (90%), Linux 2.6.32 - 3.13 (90%), Linux 2.6.32 (90%)
```

No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds

In summary, the scan results indicate that the target host is running a Linux-based operating system.

For advanced search we can try nmap -AO --osscan-guess command. This command enables OS fingerprint guessing. Nmap will make educated guesses about the operating system even when it's unable to make a conclusive identification.

-The scan (**sudo nmap -AO --osscan-guess 64.176.188.181**) was performed with aggressive OS detection enabled (**-AO**), aiming to identify the operating system running on the target host.

-The target host (64.176.188.181) was detected as up with a latency of 0.022 seconds.

-Port 22/tcp (SSH) is open and running OpenSSH 8.2p1 on Ubuntu 4ubuntu0.9, which is an Ubuntu Linux system.

-Several other ports are closed, including ports 89/tcp, 555/tcp, 898/tcp, 1002/tcp, and 1111/tcp. Port 9200/tcp is open but returns some HTTP-related data, indicating a web service, potentially related to Elasticsearch.

-Aggressive OS detection was performed, and the results suggest that the most likely operating system on the target host is a version of Linux. It provides some OS version guesses based on the scan, ranging from Linux 3.2 to Linux 4.11.

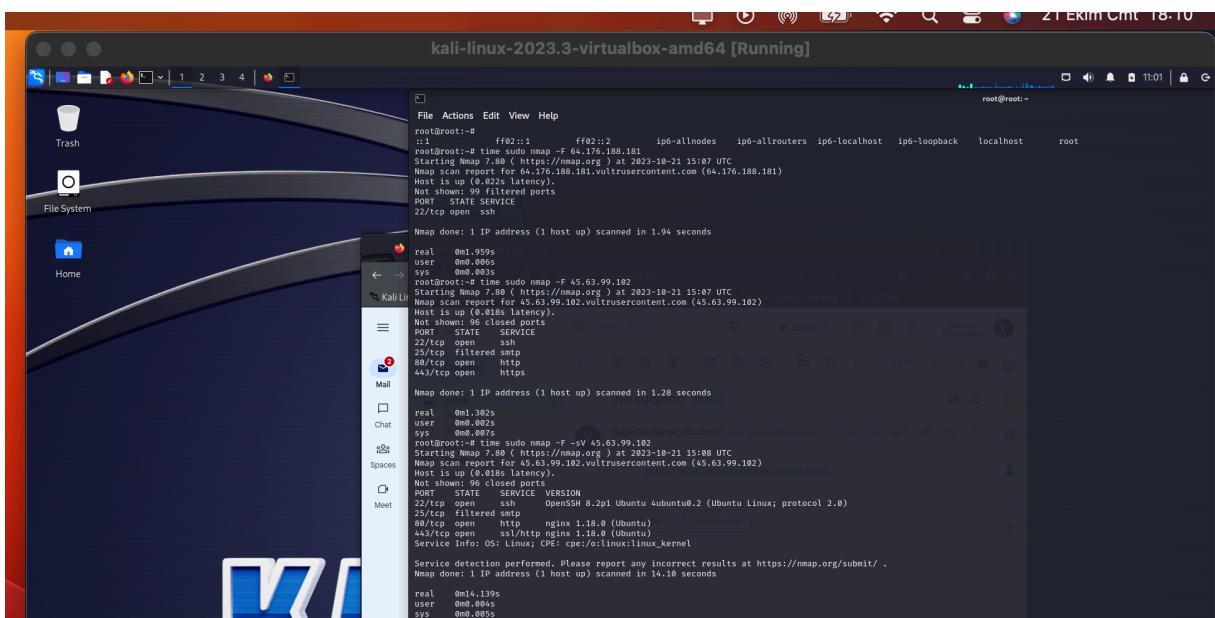
- The traceroute (using port 1002/tcp) shows the network path taken to reach the target host.

-The scan took 103.57 seconds to complete.

In summary, the scan results, along with aggressive OS detection, indicate that the target host is running an Ubuntu Linux system with OpenSSH.

From now you can see same commands for other IP address which is 45.63.99.102:

-F and -F -sV commands



The screenshot shows a Kali Linux desktop environment with two terminal windows open. The top terminal window shows the output of an Nmap scan for the IP address 64.176.188.181. The bottom terminal window shows the output of an Nmap scan for the IP address 45.63.99.102. Both scans were run with the command `sudo nmap -F`. The results show various open ports and their services, including SSH (port 22), SMTP (port 25), HTTP (port 80), and HTTPS (port 443). The desktop interface includes a dock with icons for File System, Home, Mail, Chat, Spaces, and Meet, and a taskbar at the bottom.

```
root@kali:~# sudo nmap -F 64.176.188.181
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:07 UTC
Nmap scan report for 64.176.188.181.vultrusercontent.com (64.176.188.181)
Host is up (0.018s latency).
Not shown: 99 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds

root@kali:~# sudo nmap -F 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:07 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.018s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

root@kali:~# sudo nmap -sV 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:08 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.018s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http    nginx 1.18.0 (Ubuntu)
443/tcp   open  ssl/http nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.10 seconds
```

As you can see here port 22,80,443 are open and with -sV we can see their version

-Pn -p- and -p 22 search commands:

```
File Actions Edit View Help
See https://ubuntu.com/esm or run: sudo pro status

** System restart required **
Last login: Sat Oct 21 14:16:33 2023 from 159.20.68.5
root@root:~# time sudo nmap -Pn 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:16 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.018s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    filtered sasl
25/tcp    filtered smtp
80/tcp    open     http
443/tcp   open     https
5001/tcp  open     complex-link

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds

real    0m1.383s
user    0m0.008s
sys     0m0.008s
root@root:~# time sudo nmap -T4 -p- 1-1000 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:17 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.018s latency).
Not shown: 65529 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    filtered sasl
25/tcp    filtered smtp
80/tcp    open     http
443/tcp   open     https
5001/tcp  open     complex-link
12321/tcp filtered memcache

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds

real    0m1.412s
user    0m0.002s
sys     0m0.004s
root@root:~# time sudo nmap -p- 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:17 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.018s latency).
Not shown: 65529 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    filtered sasl
80/tcp    open     http
443/tcp   open     https
5001/tcp  open     complex-link
12321/tcp filtered memcache

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

real    0m0.508s
user    0m0.003s
sys     0m0.004s
root@root:~# time sudo nmap -p- -V 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:17 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.017s latency).
Not shown: 65529 closed ports
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
23/tcp    filtered sasl
80/tcp    open     http    nginx 1.18.0 (Ubuntu)
443/tcp   open     ssl/http nginx 1.18.0 (Ubuntu)
5001/tcp  open     http    nginx 1.18.0
8080/tcp  open     http    nginx 1.18.0
12321/tcp filtered memcache
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.47 seconds

real    0m21.496s
user    0m0.007s
sys     0m0.006s
root@root:~#
```

As we can see here same ports are open, also with -p- -sV command we can see ports service and also their version. For example port 22s service type is ssh and its version openSSH 4ubuntu0.2

And also OS commands:

```
File Actions Edit View Help
kali-linux-2023.3-virtualbox-amd64 [Running]
root@root:~# time sudo nmap -O 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:21 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.017s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    filtered sasl
80/tcp    open     http
443/tcp   open     https
5001/tcp  open     complex-link

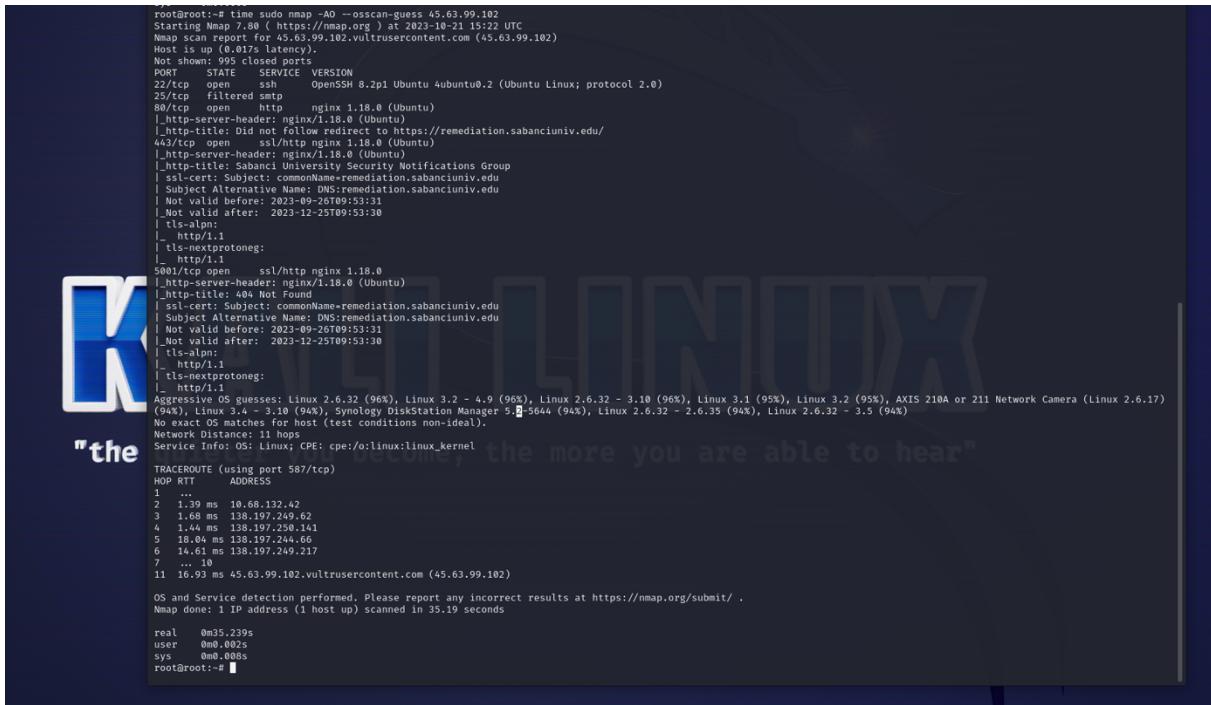
Aggressive OS guesses: Linux 2.6.32 (90%), Linux 3.2 - 4.0 (90%), Linux 2.6.32 - 3.10 (90%), Linux 3.4 - 3.10 (90%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).

Network Distance: 10 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 5.01 seconds

real    0m5.048s
user    0m0.003s
sys     0m0.006s
```



```

root@root:~# time sudo nmap -AO --oscan-guess 45.63.99.102
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-21 15:22 UTC
Nmap scan report for 45.63.99.102.vultrusercontent.com (45.63.99.102)
Host is up (0.017s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http  nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to https://remediation.sabanciuniv.edu/
443/tcp   open  ssl/http nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Sabanci University Security Notifications Group
|ssl-cert: Subject: commonName=remediation.sabanciuniv.edu
|Subject Alternative Name: DNS:remediation.sabanciuniv.edu
|_Not valid before: 2023-09-26T09:53:31
|_Not valid after:  2023-12-25T09:53:30
|_tls-alpn: h2
|_tls-ecdh-curve: P-256
|_tls-nextprotoneg:
|_http/1.1
5001/tcp  open  ssl/http nginx 1.18.0
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: 404 Not Found
|ssl-cert: Subject: commonName=remediation.sabanciuniv.edu
|Subject Alternative Name: DNS:remediation.sabanciuniv.edu
|_Not valid before: 2023-09-26T09:53:31
|_Not valid after:  2023-12-25T09:53:30
|_tls-alpn: h2
|_tls-ecdh-curve: P-256
|_tls-nextprotoneg:
|_http/1.1
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 3.4 - 3.10 (94%), Synology DiskStation Manager 5.2-5644 (94%), Linux 2.6.32 - 2.6.35 (94%), Linux 2.6.32 - 3.5 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 587/tcp)
HOST RTT ADDRESS
2  1.39 ms  10.68.132.42
3  1.68 ms  138.197.249.62
4  1.44 ms  138.197.250.141
5  18.04 ms 138.197.244.66
6  14.61 ms 138.197.249.217
7  ... 18
11  16.93 ms 45.63.99.102.vultrusercontent.com (45.63.99.102)

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 35.19 seconds

real    0m35.239s
user    0m0.002s
sys     0m0.008s
root@root:~# 

```

First Scan (sudo nmap -O 45.63.99.102):

- The scan was performed without aggressive OS detection (-O), focusing on identifying open ports and services.
- The target host (45.63.99.102) was detected as up with a latency of 0.017 seconds.
- Several ports are open:
 - Port 22/tcp (SSH)
 - Port 80/tcp (HTTP)
 - Port 443/tcp (HTTPS)
 - Port 5001/tcp (Complex-link)
- Port 25/tcp (SMTP) is filtered, indicating that the SMTP service is not directly accessible.
- The OS detection did not yield an exact match, but it provided aggressive OS guesses that suggest a high probability of the target host running a version of Linux.
- The scan also reports the network distance (number of hops) to reach the target host.

Second Scan (sudo nmap -AO --oscan-guess 45.63.99.102)

- This scan was performed with aggressive OS detection enabled (-AO), aiming to identify the operating system and provide more detailed information about services.
- Similar to the previous scan, it identified the target host (45.63.99.102) as up with a latency of 0.017 seconds.
- The following services were identified:
 - Port 22/tcp (SSH) running OpenSSH 8.2p1 on Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0).
 - Port 25/tcp (SMTP) is still filtered.
 - Port 80/tcp (HTTP) running nginx 1.18.0 on Ubuntu.

- Port 443/tcp (HTTPS) running nginx 1.18.0 on Ubuntu with SSL certificates for "remediation.sabanciuniv.edu."
- Port 5001/tcp (Commplex-link) running nginx 1.18.0.
- Aggressive OS detection results are consistent with the previous scan, suggesting the target host is running a version of Linux.
- The network distance is reported, and traceroute data is provided.

In summary, these scans indicate that the target host is likely running a version of Linux (Ubuntu) and provides information about open ports and services. It also provides details about the web server and SSL certificates. The exact OS version was not determined due to non-ideal test conditions. The host appears to be related to Sabanci University based on the hostname and SSL certificate.

As final step here is my IP addressed used while probing

My Ifconfig:

```
root@root:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 159.89.28.38 netmask 255.255.240.0 broadcast 159.89.31.255
                inet6 fe80::18c3:75ff:fe8f:418d prefixlen 64 scopeid 0x20<link>
                ether lac:3:75:8f:41:8d txqueuelen 1000 (Ethernet)
                RX packets 659332 bytes 335213235 (335.2 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 913894 bytes 890776880 (89.0 MB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.114.0.2 netmask 255.255.240.0 broadcast 10.114.15.255
                inet6 fe80::f871:97ff:fed3:7af3 prefixlen 64 scopeid 0x20<link>
                ether fa:71:97:3d:7a:f3 txqueuelen 1000 (Ethernet)
                RX packets 126 bytes 8896 (8.8 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 744 bytes 35332 (35.3 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 14501 bytes 1224146 (1.2 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 14501 bytes 1224146 (1.2 MB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

real    0m0.002s
user    0m0.002s
sys     0m0.000s
root@root:~#
```

