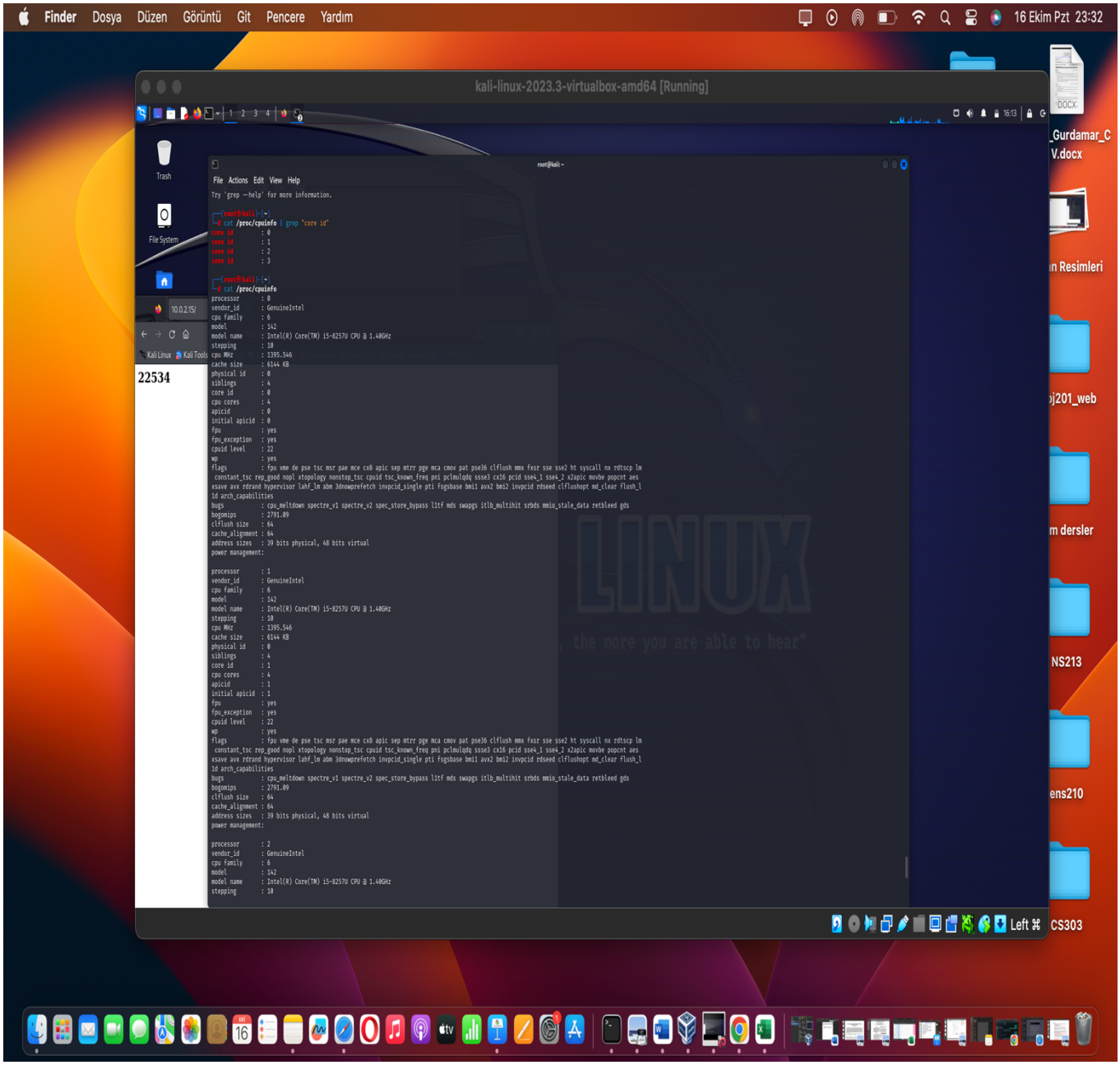
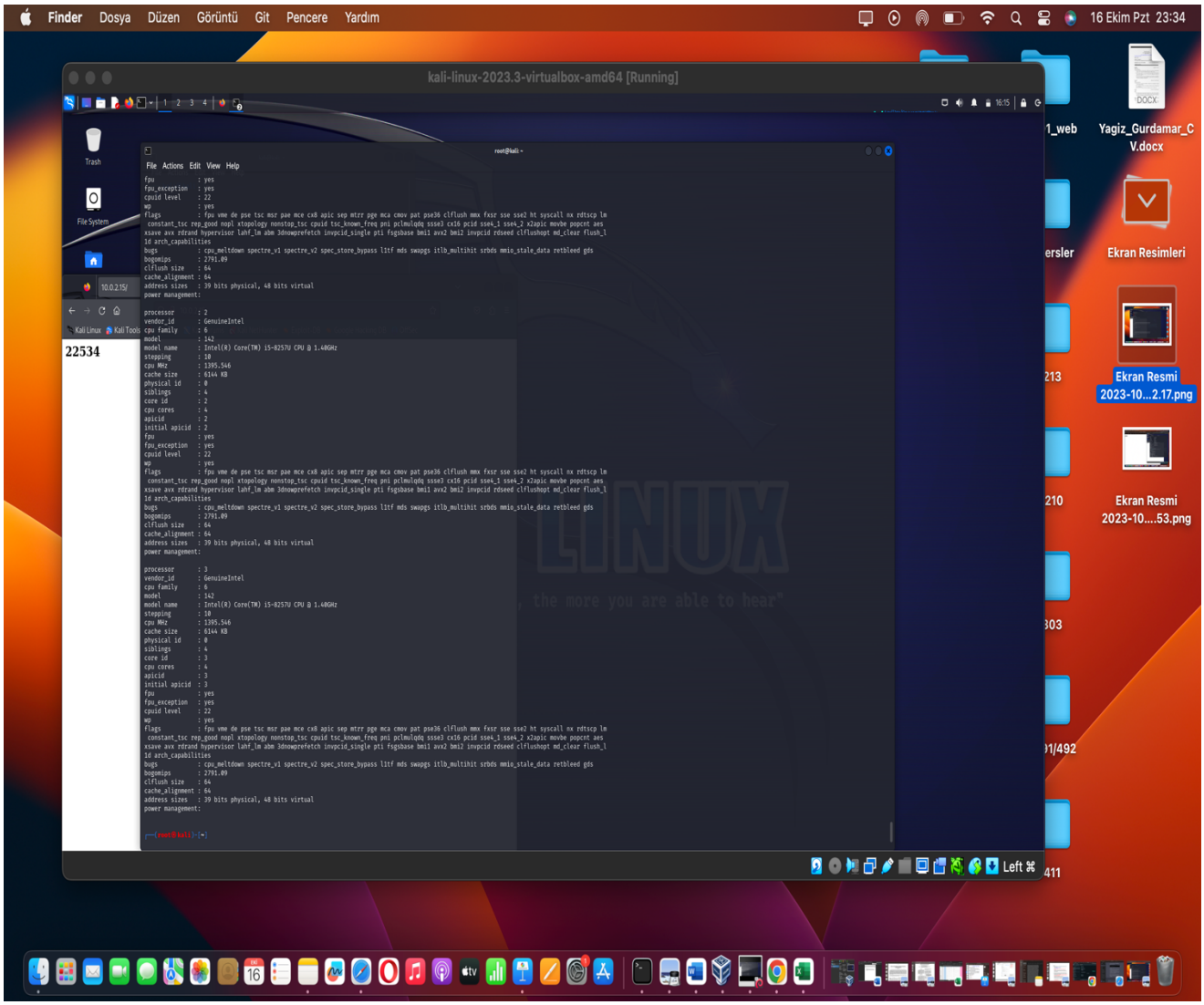
CS437 LAB1 REPORT

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



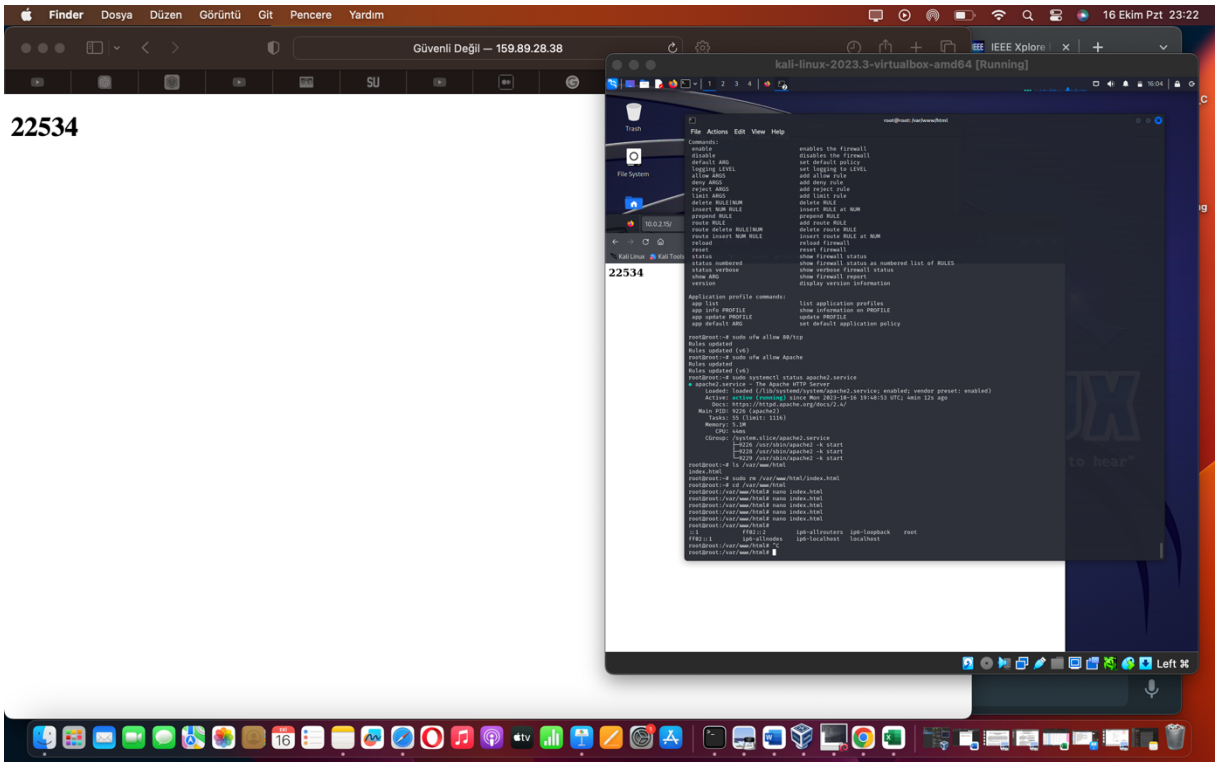
Second part of screenshot:



Part 2:

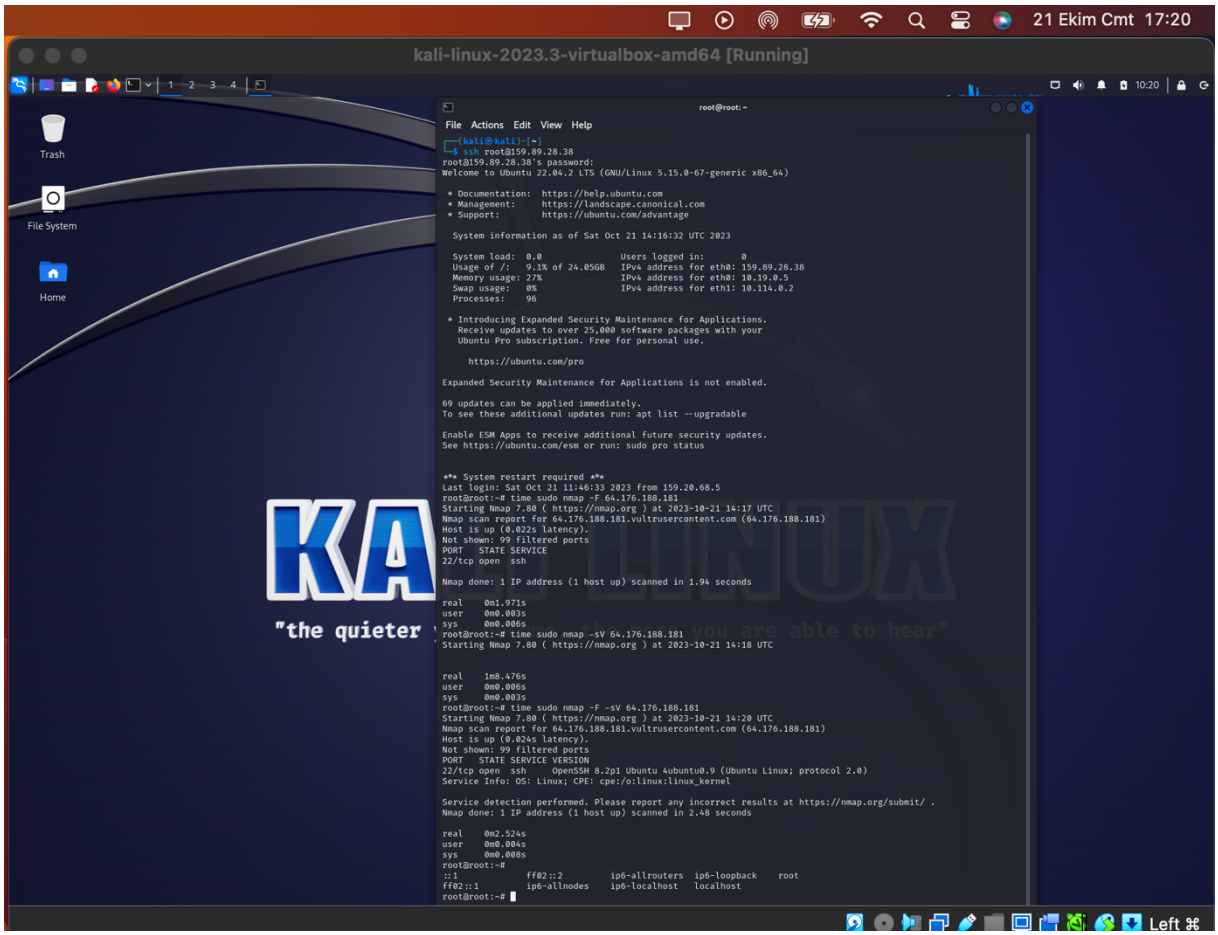
So for part2 I runned the commands that you wrote for my server, which I created from Digital Ocean. I installed Apache2 and then allowed. I already sent my ip address but here it is: 159.89.28.38

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



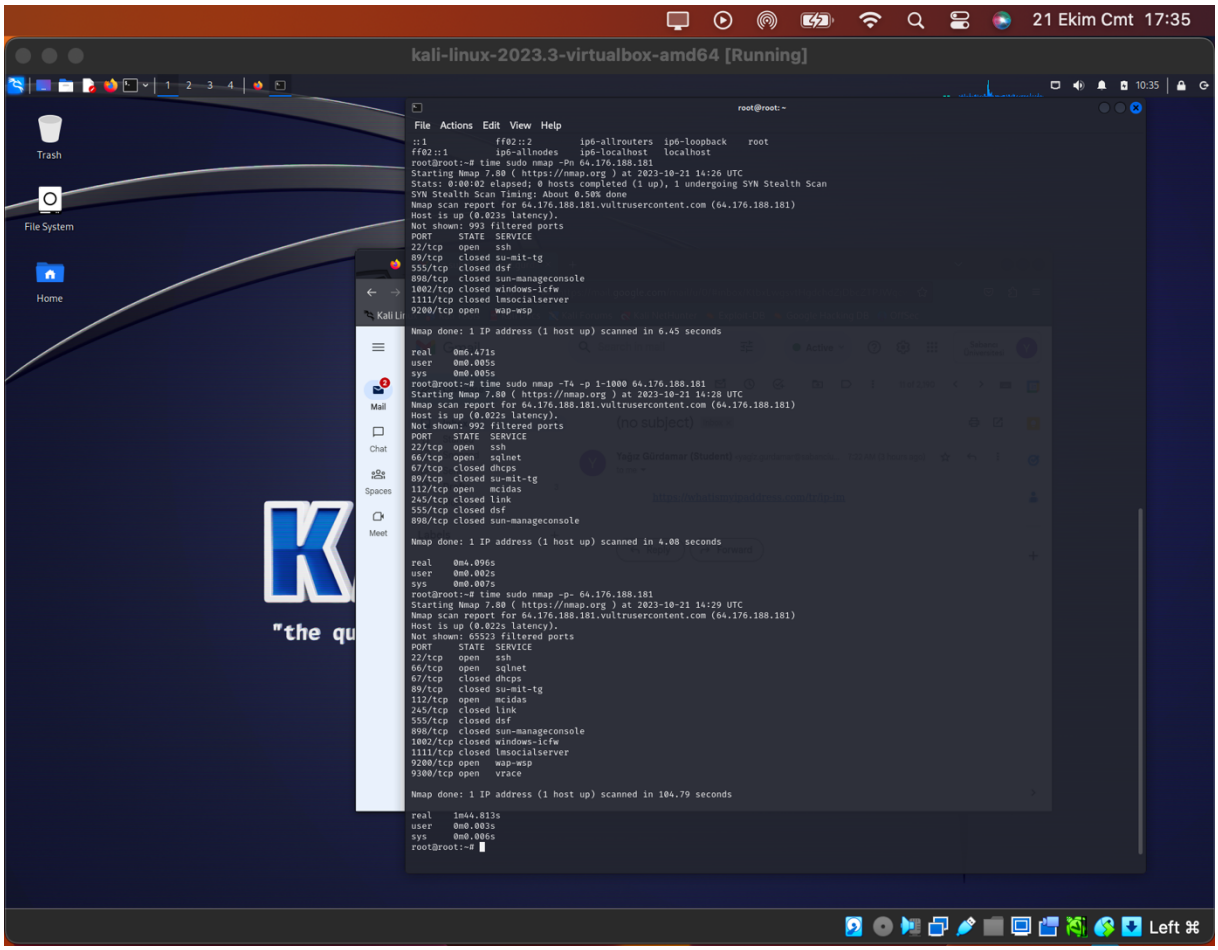
Part 3:

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.

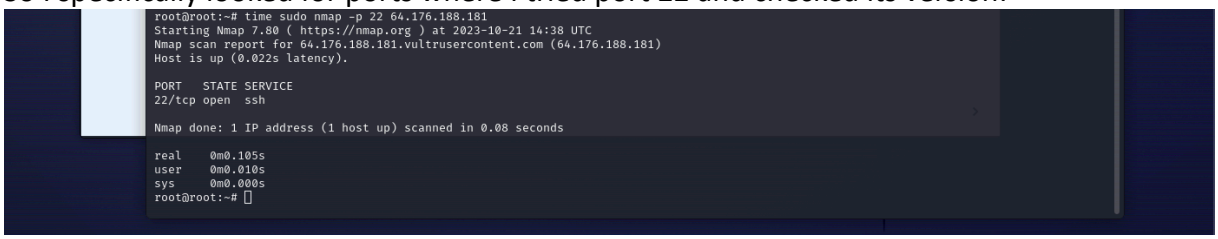
- **sudo nmap -T4 -p 1-1000 64.176.188.181**:

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.

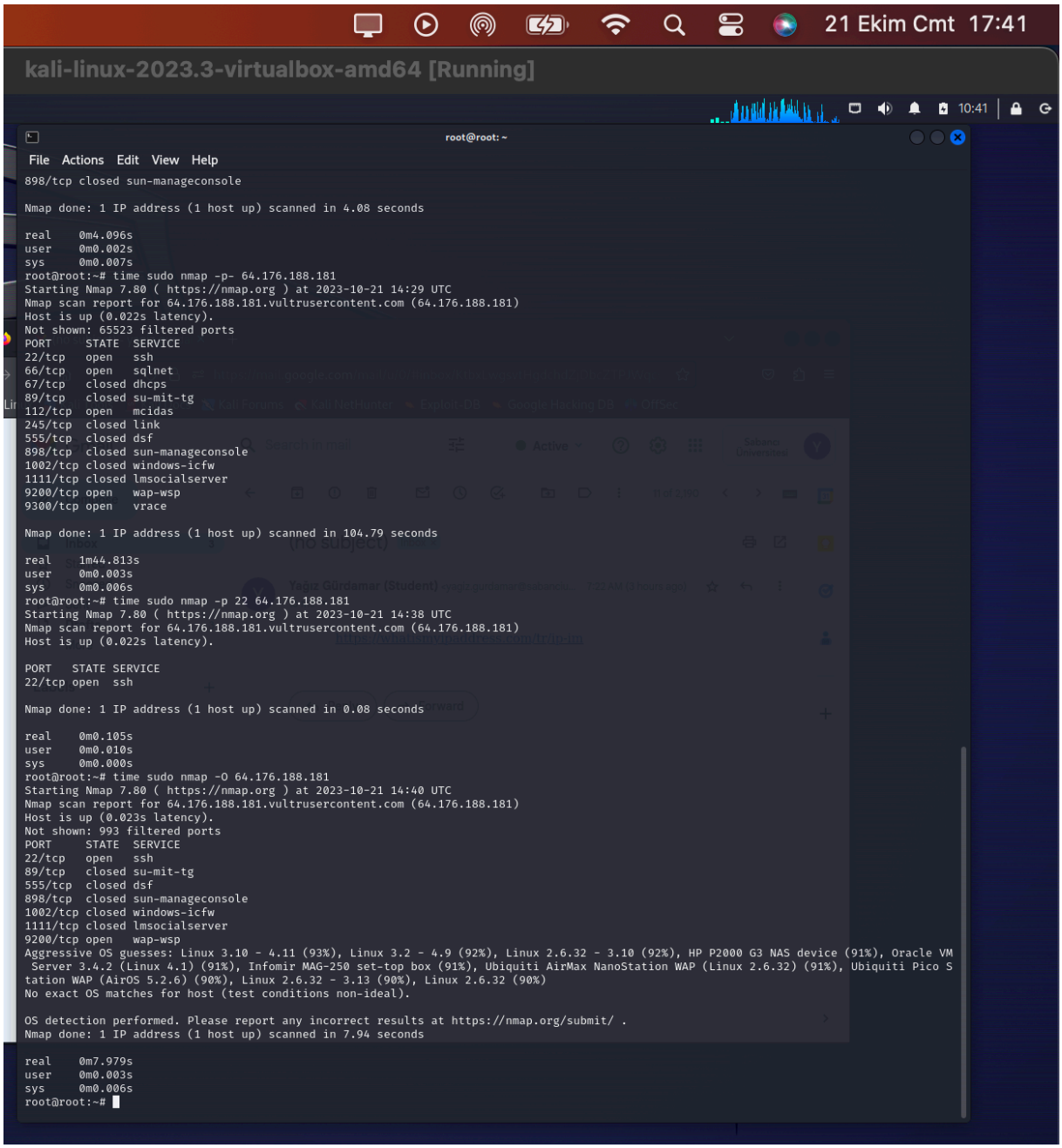
- **sudo nmap -p- 64.176.188.181**:

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:

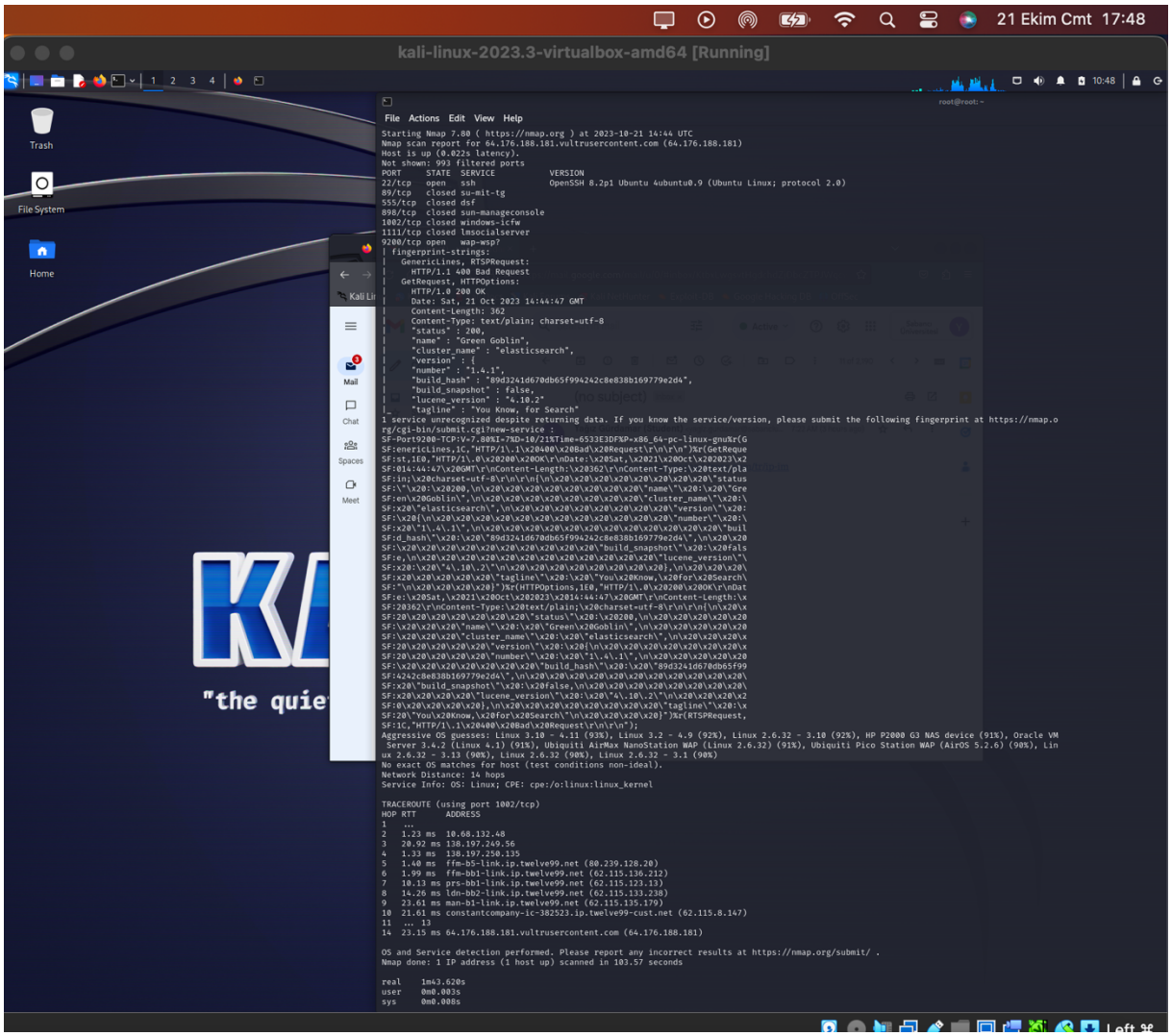


Last thing to do is for OS type, first I runned nmap -O which brings me just OS types:



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.

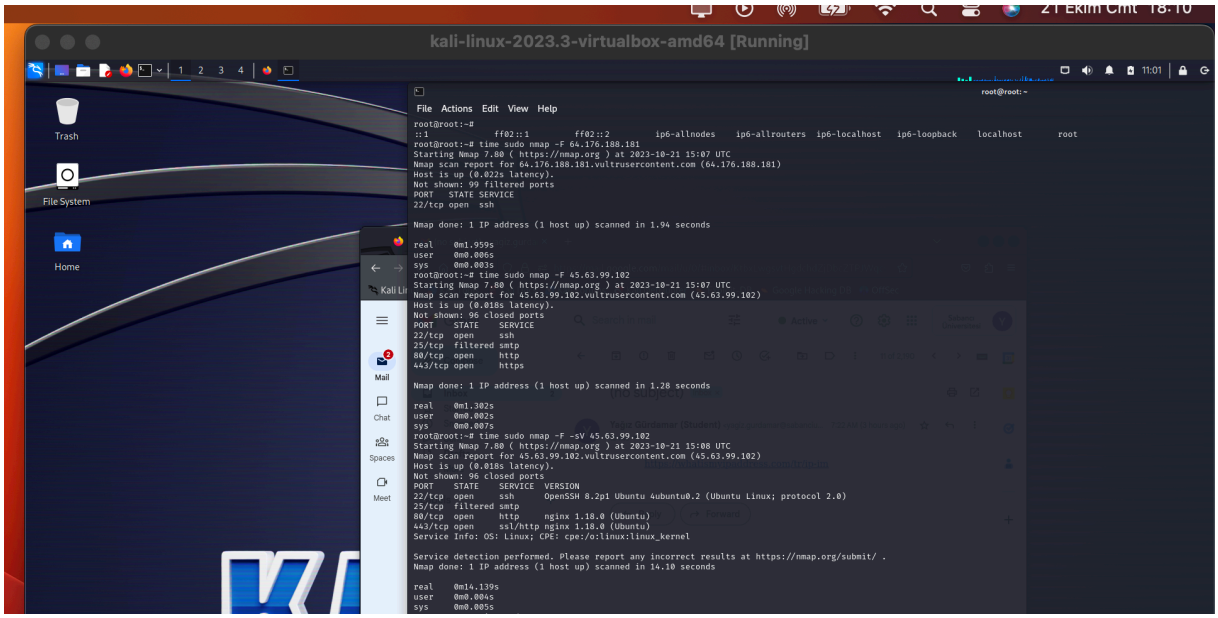


-The scan (**sudo nmap -AO --osscan-guess 64.176.188.181**) was performed with aggressive OS detection enabled (**-AO**), aiming to identify the operating system running on the target host.
-The target host (64.176.188.181) was detected as up with a latency of 0.022 seconds.
-Port 22/tcp (SSH) is open 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.

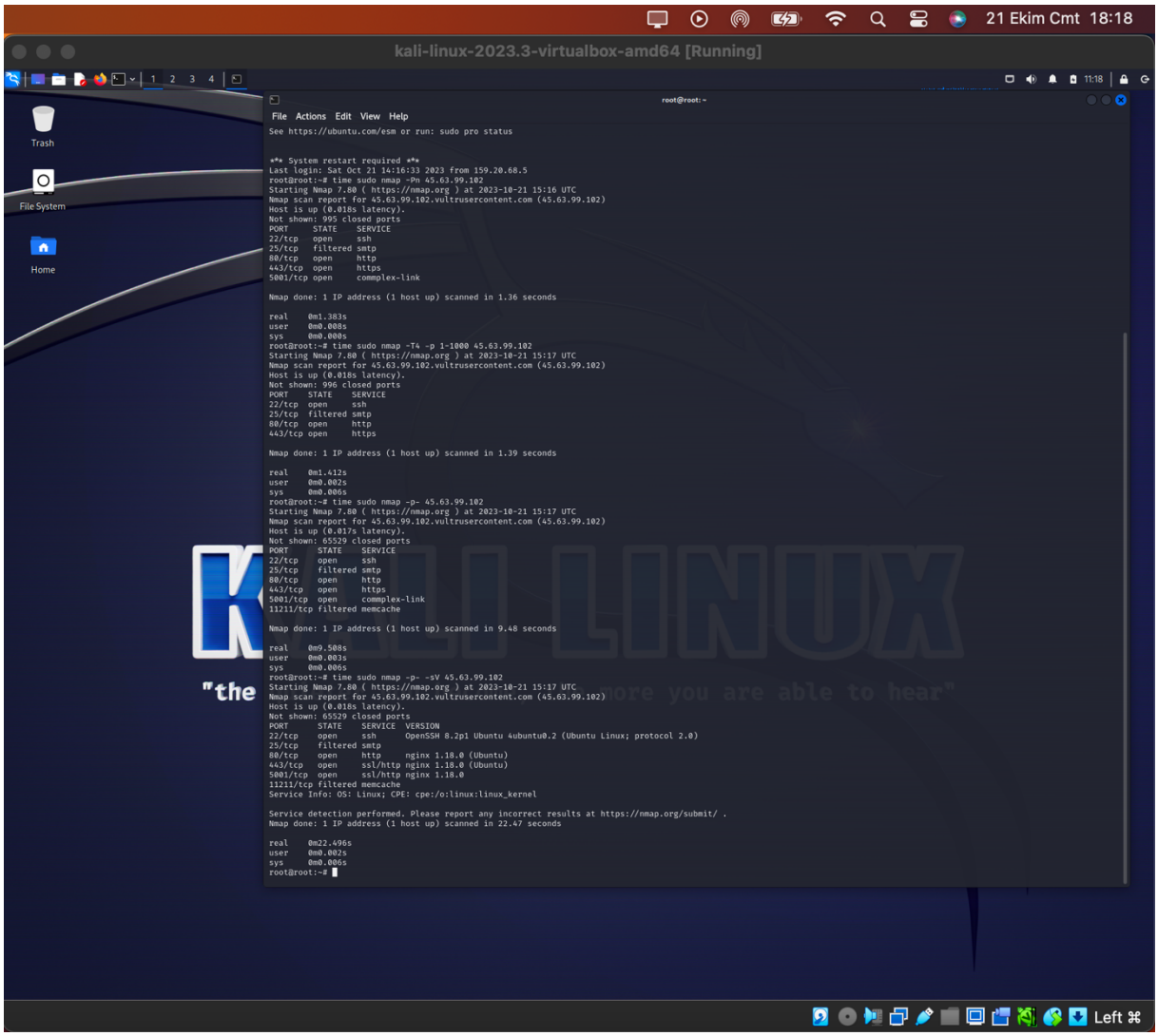
From now you can see same commands for other IP adress which is 45.63.99.102:

-F and -F -sV commands



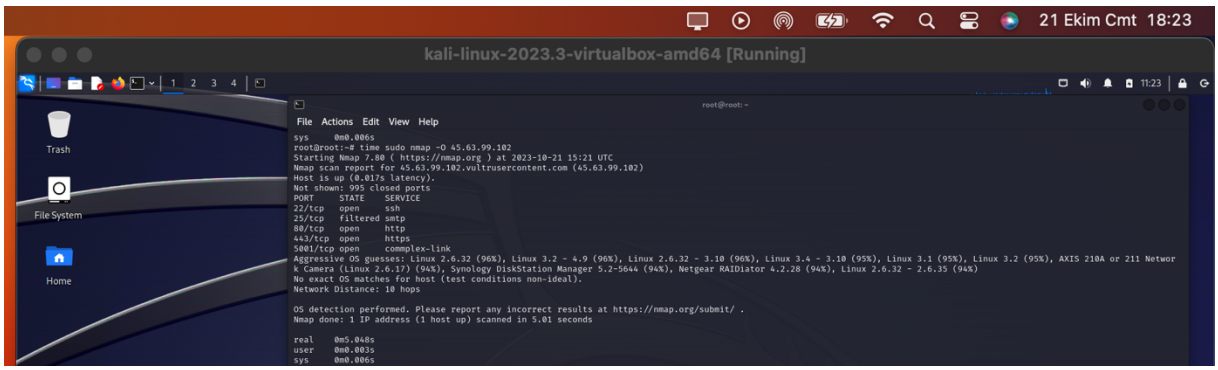
As you can see here port 22,80,443 are open and with -sV we can see their version

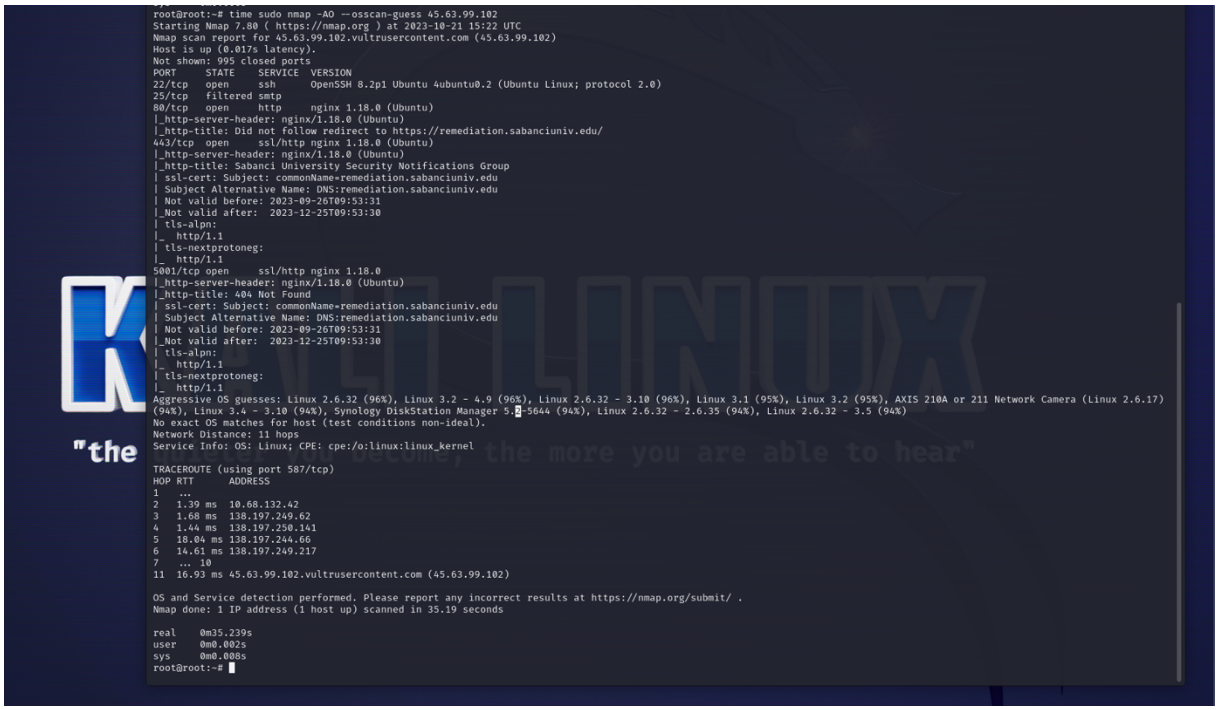
-Pn -p- and -p 22 search commands:



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:





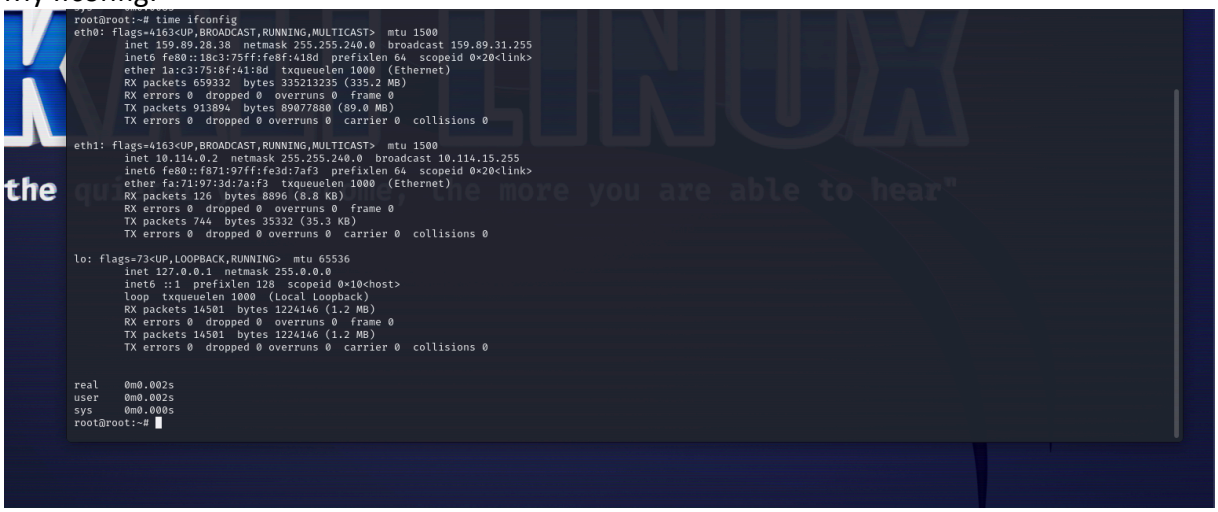
First Scan (sudo nmap -O 45.63.99.102):
- The scan was performed without aggressive OS detection (-O), focusing on identifying open ports and services.
- The target host (45.63.99.102) was detected as up with a latency of 0.017 seconds.
- Several ports are open:
 - Port 22/tcp (SSH)
 - Port 80/tcp (HTTP)
  - Port 443/tcp (HTTPS)
 - Port 5001/tcp (Commplex-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.

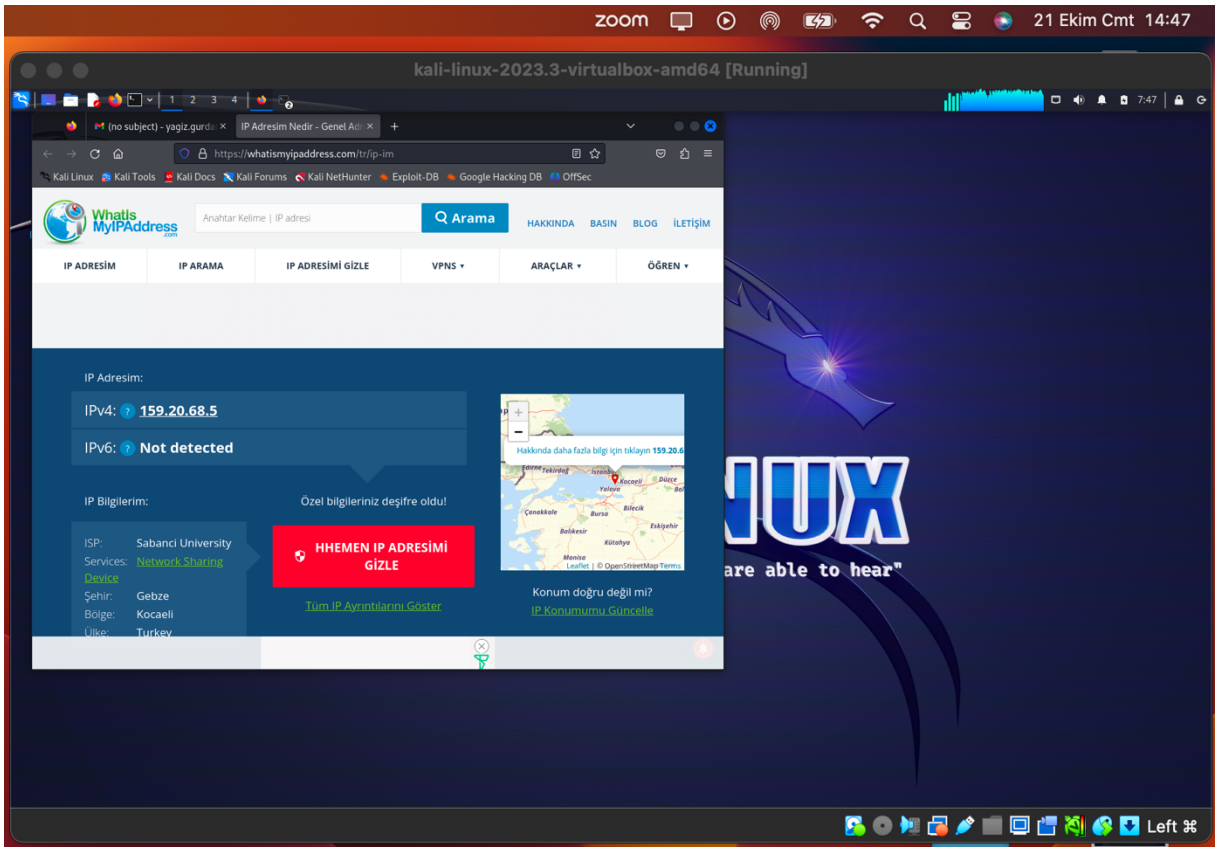
Second Scan (sudo nmap -AO --osscan-guess 45.63.99.102)
- This scan was performed with aggressive OS detection enabled (-AO), aiming to identify the operating system and provide more detailed information about services.
- Similar to the previous scan, it identified the target host (45.63.99.102) as up 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:




zoom
21 Ekim Cmt 14:47
kali-linux-2023.3-virtualbox-amd64 [Running]
(no subject) - yagiz.gurda
IP Adresim Nedir - Genel Adı
https://whatismyipaddress.com/tr/ip-im
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
WhatIsMyIPAddress.com
Anahtar Kelime | IP adresi
Arama
HAKKINDA
BASIN
BLOG
İLETİŞİM
IP ADRESİM
IP ARAMA
IP ADRESİMİ GİZLE
VPNS
ARAÇLAR
ÖĞREN
IP Adresim:
IPv4: 159.20.68.5
IPv6: Not detected
IP Bilgilerim:
Özel bilgileriniz deşifre oldu!
ISP: Sabanci University
Services: Network Sharing Device
Şehir: Gebze
Bölge: Kocaeli
Ülke: Turkey
HHEMEN IP ADRESİMİ GİZLE
Tüm IP Ayrıntılarını Göster
Konum doğru değil mi?
IP Konumumu Güncelle
Left ⌘