CMP020X305S: Cyber Security

Portfolio 02: Asset Updates, Reconnaissance and Monitoring

Set Date:	**10th February 2023**
Deadline:	3rd March 2023 by 17:00 hours
Submission Points:	Upload via Moodle
Submission Format:	Screen Captures Saved to a Document. Upload to Moodle
Feedback and Marks:	Via Moodle
Marking Scale (Lab):	Maximum 10.00 marks for Lab completion
Marking Scale (Wow Factor):	Maximum 6.66 marks for Lab completion
Learning Outcomes:	LO2: Investigate measures that can be taken by both individuals and organizations including governments to prevent or mitigate the undesirable effects of computer crimes and identity theft. LO4: Evaluate risks to privacy and anonymity in commonly used applications.

IMPORTANT: This is a living document and will be subject to changes and updates during the life cycle of the lab portfolio. Therefore, it is imperative that you check this document regularly!!

How will this portfolio be marked?

This portfolio will be marked in accordance with the following rubrics:

Portfolio Requirement A: Host Name Updates & Resolution	Maximum Mark
Not attempted	0
Evidence of a very limited level of completion in accordance with the requirement description.	1.0 - 2.1
Evidence of a limited level of completion in accordance with the requirement description.	2.1 - 2.5
Evidence of an adequate level of completion in accordance with the requirement description.	2.6 - 3.0
Evidence of a good level of completion in accordance with the requirement description.	3.1 - 3.5
Evidence of full completion in accordance with the requirement description.	3.6 - 5.0

Portfolio Requirement B: Exploring NMAP Commands	Maximum Mark
Not attempted	0
Evidence of a very limited level of completion in accordance with the requirement description.	1.0 - 2.1
Evidence of a limited level of completion in accordance with the requirement description.	2.1 - 2.5
Evidence of an adequate level of completion in accordance with the requirement description.	2.6 - 3.0
Evidence of a good level of completion in accordance with the requirement description.	3.1 - 3.5
Evidence of full completion in accordance with the requirement description.	3.6 - 5.0

Portfolio (Optional): Wow factor!!	Maximum Mark
Not attempted	0
Evidence of a very limited attempt that is not directly relevant to the portfolio.	1.0 - 2.6
Evidence of a limited attempt that is somewhat relevant to the portfolio.	2.7 - 3.2
Evidence of an adequate attempt that is mostly relevant to the portfolio.	3.3 - 3.9
Evidence of a good attempt that is relevant to the portfolio.	4.0 - 4.6
Evidence of a very good attempt that is relevant to the portfolio.	4.7 - 5.2
Evidence of an excellent attempt that is relevant to the portfolio.	5.3 - 6.6

The **maximum mark for this lab portfolio is 10**. An **additional maximum mark of 6.66** can be awarded for "**Wow Factor**" that evidences appropriate, relevant and additional learning. Typically, wow factor demonstrates a self-study contribution that extends or advances the core technical requirements of a lab portfolio.

To receive a mark for this portfolio lab, you will need to submit a screencast that clearly evidences the requirements described in this document. If you are not sure how to capture and present screencast evidence, **ASK**!!

Late Portfolio Submissions

For each week that a portfolio is late, two marks will be deducted from the portfolio score that is awarded.

ACADEMIC MISCONDUCT

Your submission for this coursework will be scrutinised for plagiarism, collusion, and other forms of academic misconduct. Please ensure that the work that you submit is your own, and that you have cited and referenced appropriately, to avoid having to attend an academic misconduct hearing.

Host Name Updates & Resolution

1. Change the host name for Ubuntu Server 22.04 (Zabbix)

You will notice that this server has a host name of `router` or `student`.

```
student@student:~$
```

OR

```
student@router:~:
```

From an asset monitoring perspective, this is not particularly helpful. Therefore, you will need to change the host name to something more relevant. As this is a Zabbix server, change the hostname to `zabbix`. Type:

```
sudo nano /etc/hostname
```

The following screen will be displayed:

Amend the hostname so that it is `zabbix` and save the open *hostname* file by typing `Ctrl x`, followed by `y`, then press `Enter` .

Restart the server to reflect the update and once the server has been rebooted, login. The hostname should now have been updated and should appear as follows:

```
student@zabbix:~$
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

2. Change the host name for Ubuntu Server 14.04 (WordPress)

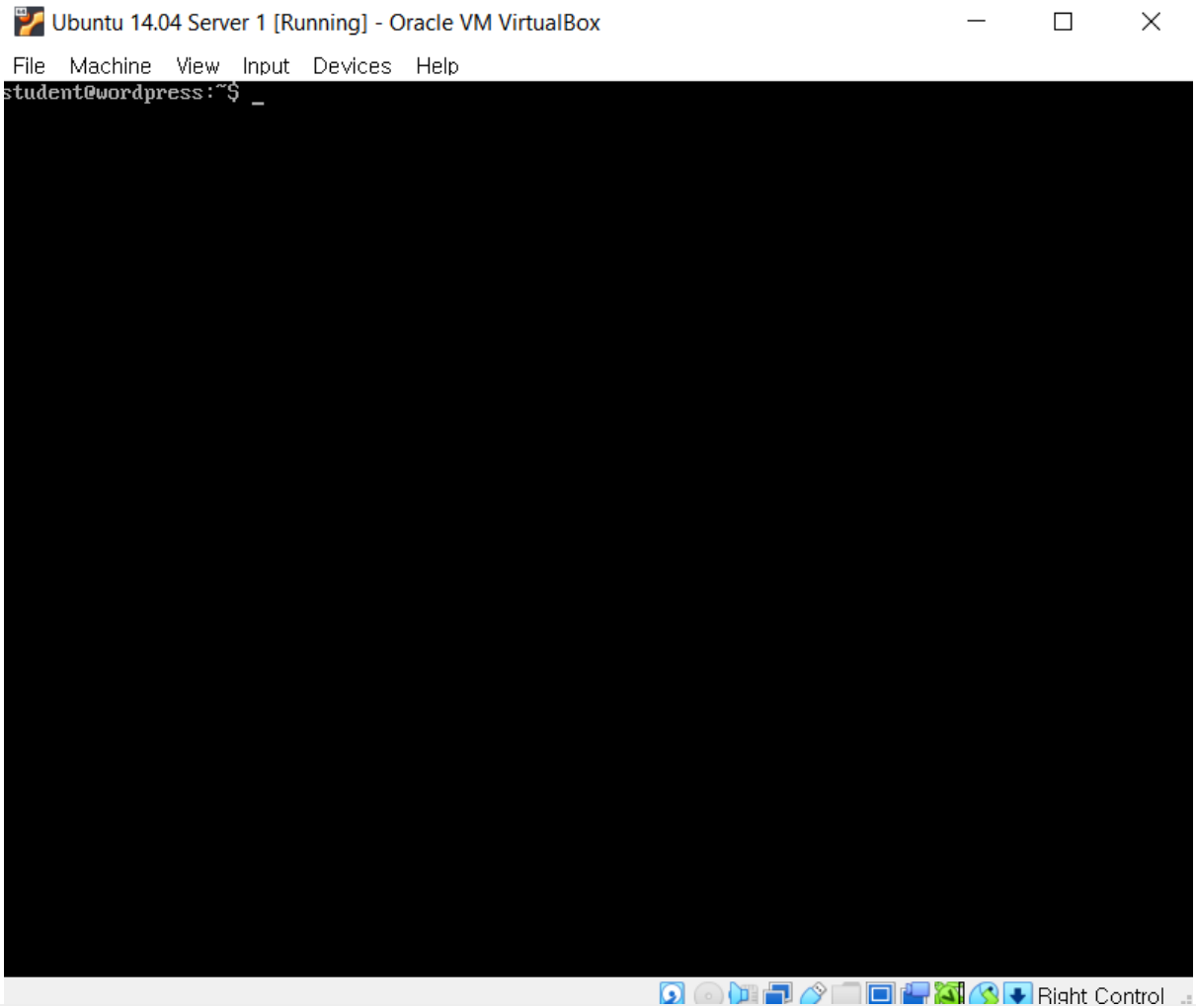
As this is also a WordPress server change the hostname to `wordpress`. Type:

```
sudo nano /etc/hostname
```

Amend the hostname so that it is `wordpress` and save the open *hostname* file by typing `Ctrl x`, followed by `y`, then press `Enter` .

Restart the server to reflect the update and once the server has been rebooted, login. The hostname should now have been updated and should appear as follows:

```
student@wordpress:~$
```



3. Change the host name for Ubuntu Server 22.04 (Gateway)

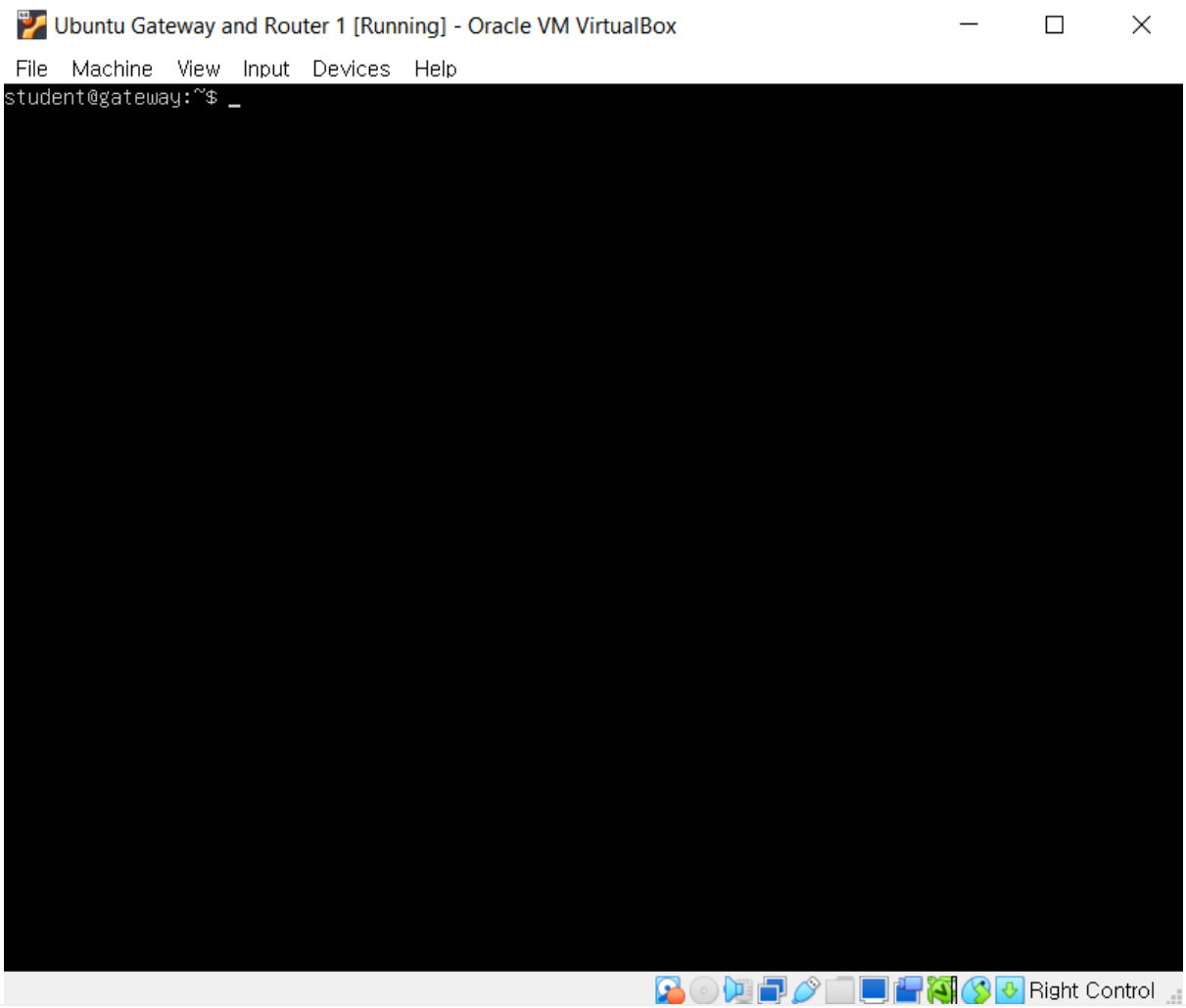
As this is a gateway server, change the hostname to `gateway`. Type:

```
sudo nano /etc/hostname
```

Amend the hostname so that it is `gateway` and save the open *hostname* file by typing `Ctrl x`, followed by `y`, then press `Enter` .

Restart the server to reflect the update and once the server has been rebooted, login. The hostname should now have been updated and should appear as follows:

```
student@gateway:~$
```



4. Change the host name for Bitnami-elk

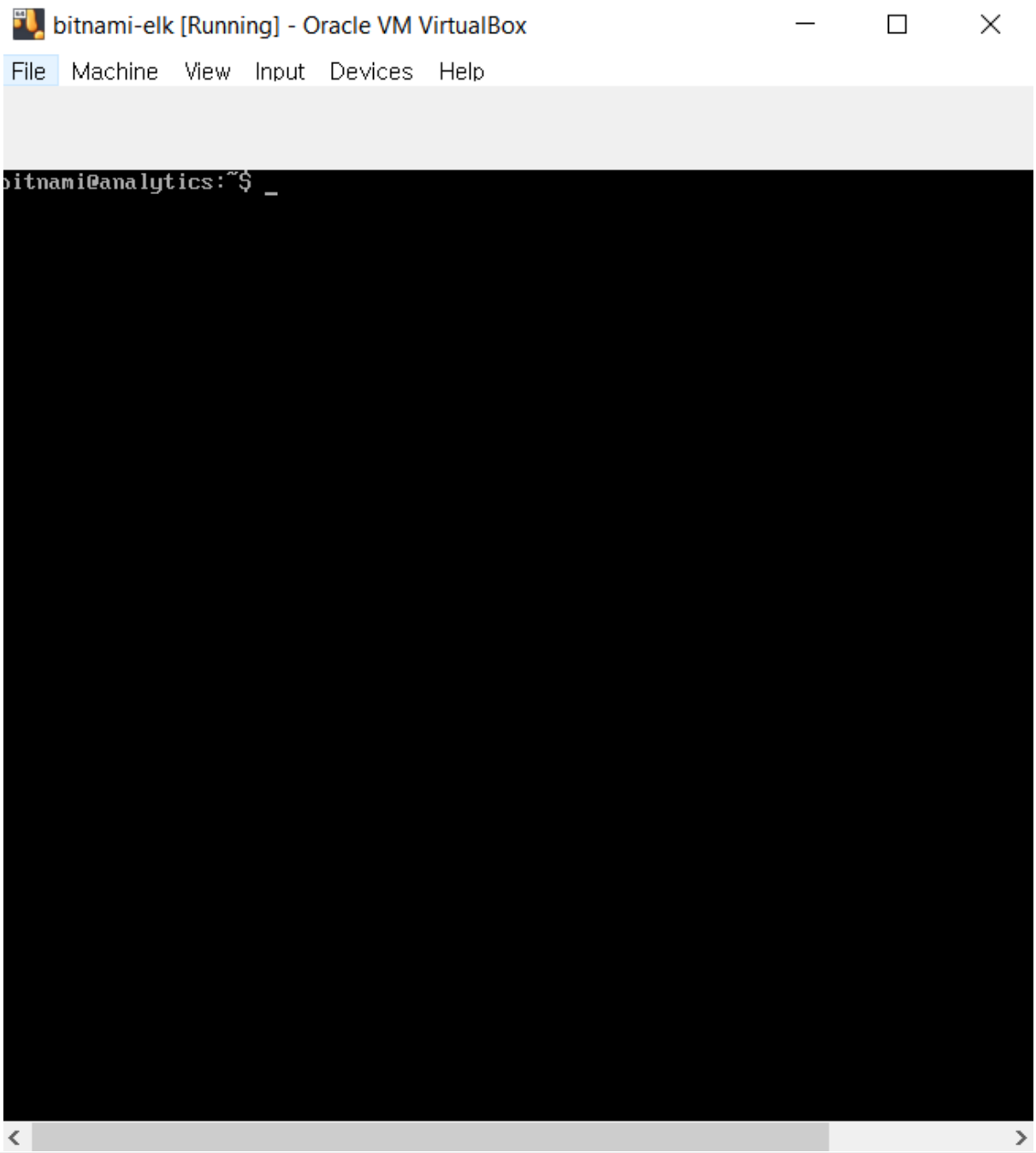
As this is an Elastic Search server (ELK Stack) change the hostname to `analytics`. Type:

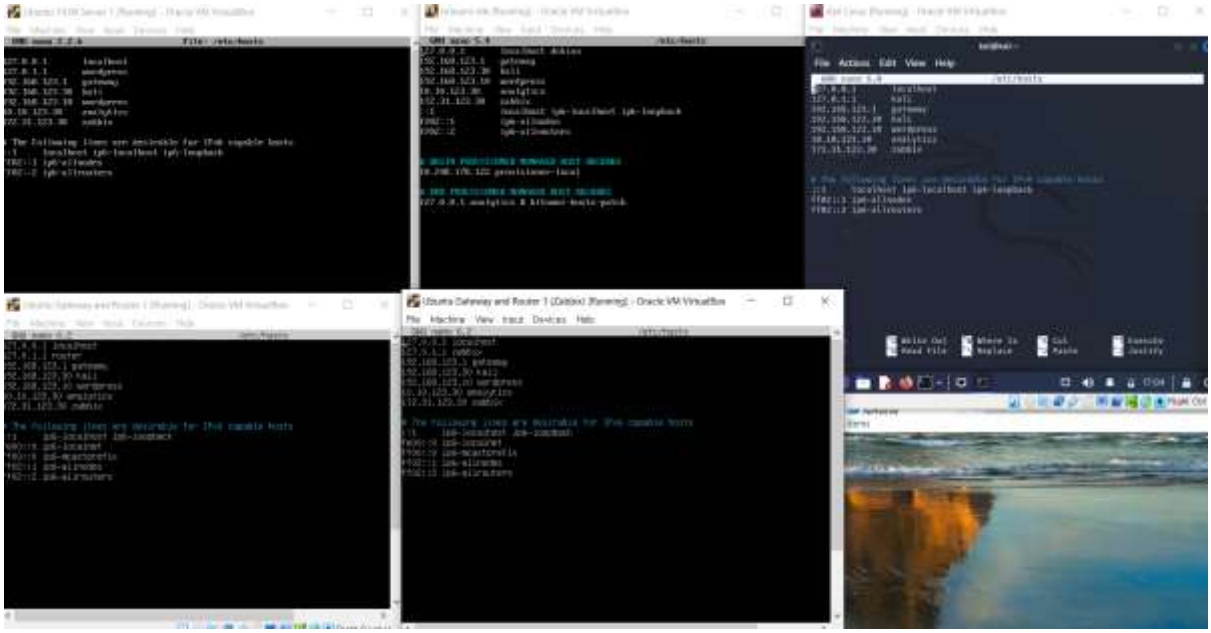
```
sudo nano /etc/hostname
```

Amend the hostname so that it is `analytics` and save the open *hostname* file by typing `Ctrl x`, followed by `y`, then press `Enter` .

Restart the server to reflect the update and once the server has been rebooted, login. The hostname should now have been updated and should appear as follows:

```
student@analytics:~$
```





4. Do not Amend Kali Linux

5. Make the host name for each virtual machine, resolve to its IP address

On your Kali Linux virtual machine, open a terminal and type

```
sudo nano /etc/hosts
```

The following screen should be displayed:

You will need to add entries in this file, so that each machine can be accessed via a host name, rather than an ip address. Amend the file as shown in the image below.

IN EACH CASE, DO NOT MODIFY THE FIRST TWO LINES!

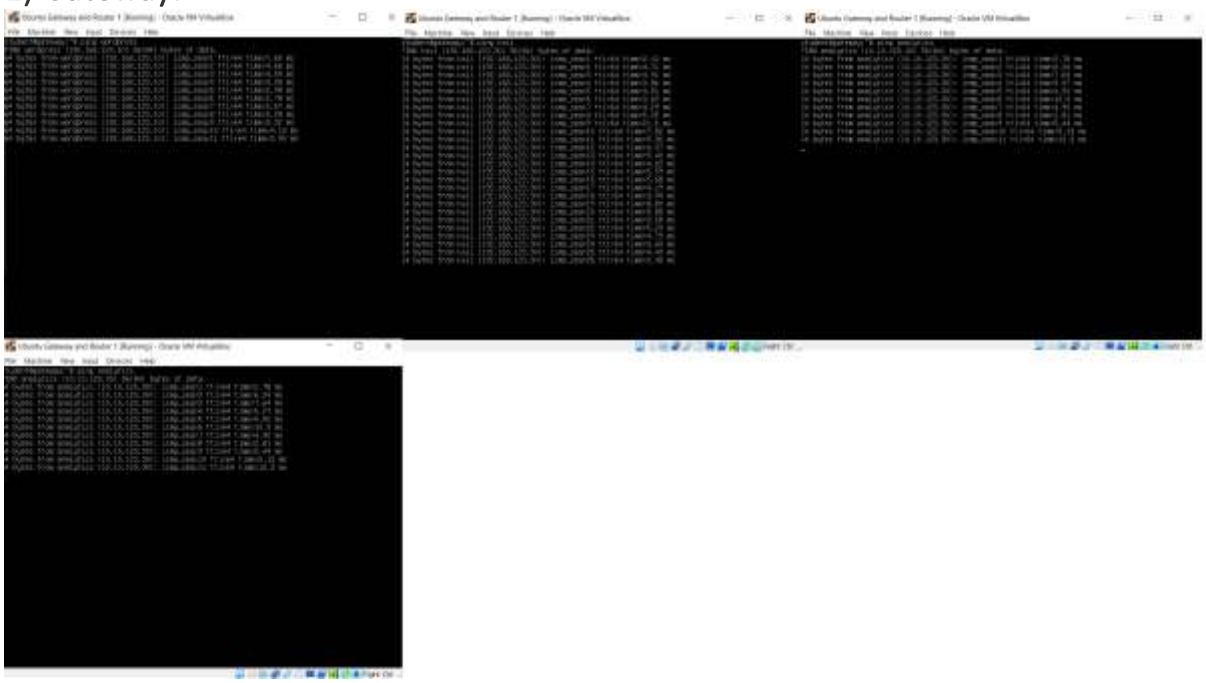
Save the open *hosts* file by typing `Ctrl x`, followed by `y`, then press `Enter` . From your kali terminal, test that you can `ping` the host names.

6. Repeat the steps in task 5 for the other virtual machines on your network.
Amend the `hosts` file for `wordpress`, `analytics`, `zabbix` and `gateway` . Once completed, you should be able to ping any of the configured host names on any of the virtual machines and resolve each host name to its respective IP address.

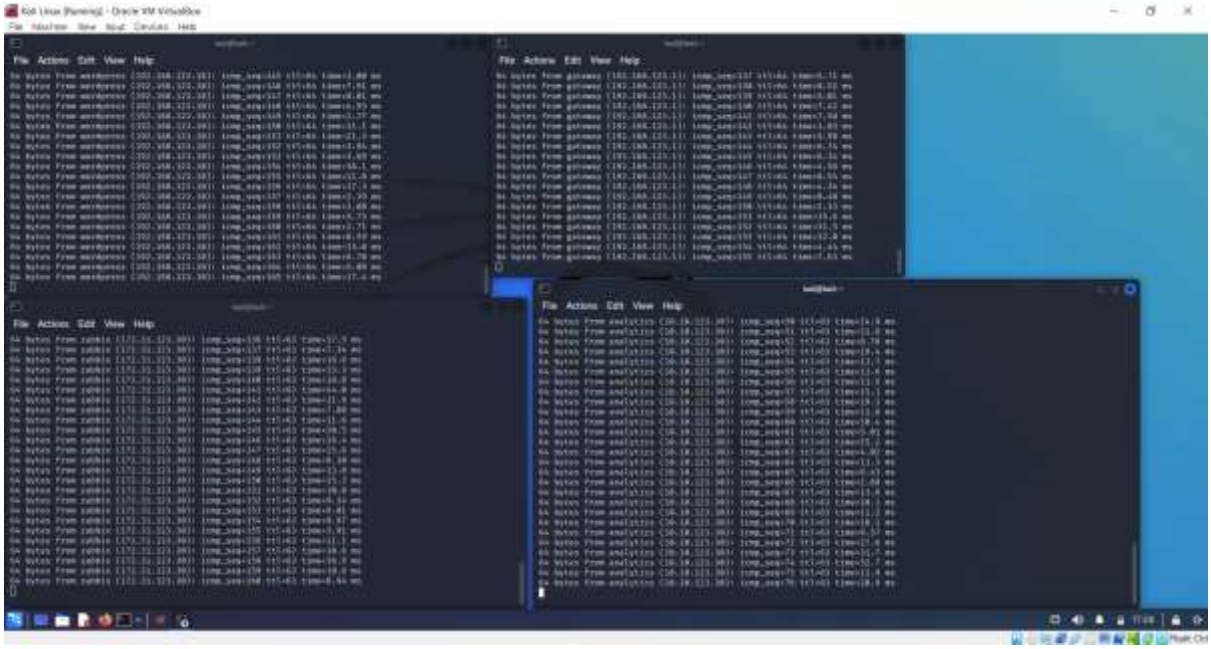
Requirement A: Demonstration Tasks

1. From the **gateway**, demonstrate that you can successfully ping the `kali`, `wordpress`, `analytics` and `zabbix` host names.
2. From the **kali**, demonstrate that you can successfully ping the `gateway`, `wordpress`, `analytics` and `zabbix` host names.
3. From the **wordpress**, demonstrate that you can successfully ping the `gateway`, `kali`, `analytics` and `zabbix` host names.
4. From the **analytics**, demonstrate that you can successfully ping the `gateway`, `kali`, `wordpress` and `zabbix` host names.
5. From the **zabbix**, demonstrate that you can successfully ping the `gateway`, `kali`, `wordpress` and `analytics` host names.
6. From `kali`, open a browser, connect to the `zabbix` home page and log in.
7. While logged in to `zabbix` from the `kali` browser, demonstrate that `zabbix`, `gateway`, `kali`, `wordpress` and `analytics` are being monitored in real-time. Take `gateway`, `wordpress` or `analytics` offline. This should prompt an alert.

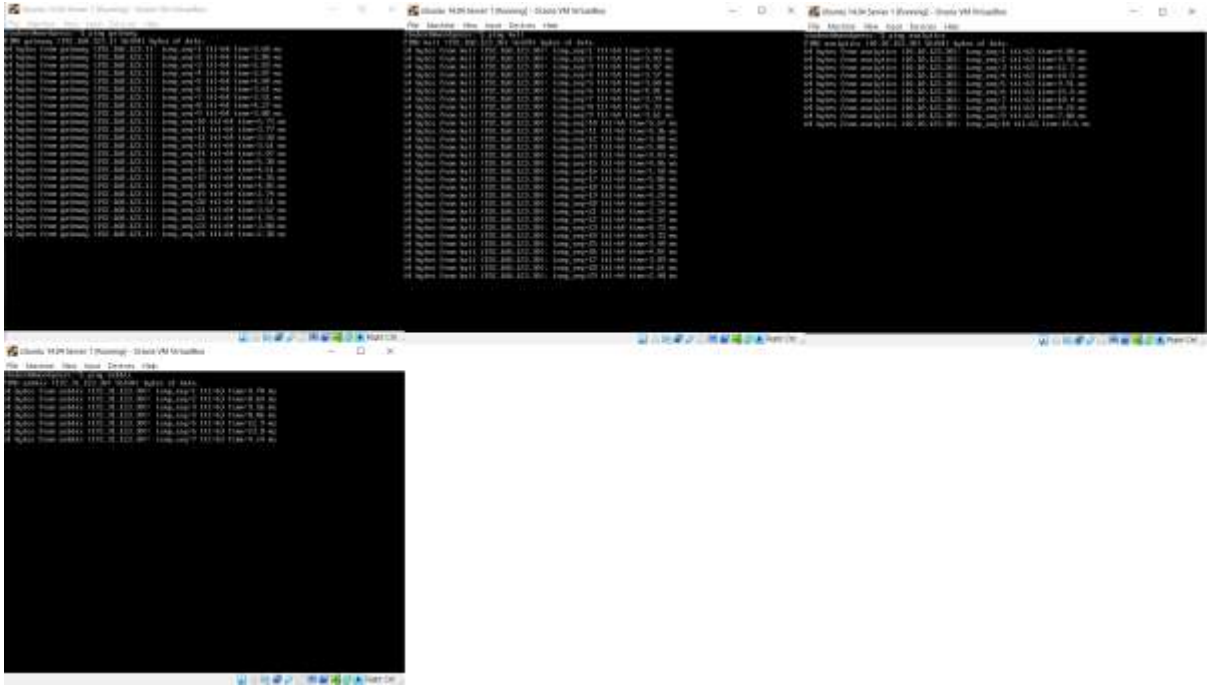
1) Gateway:



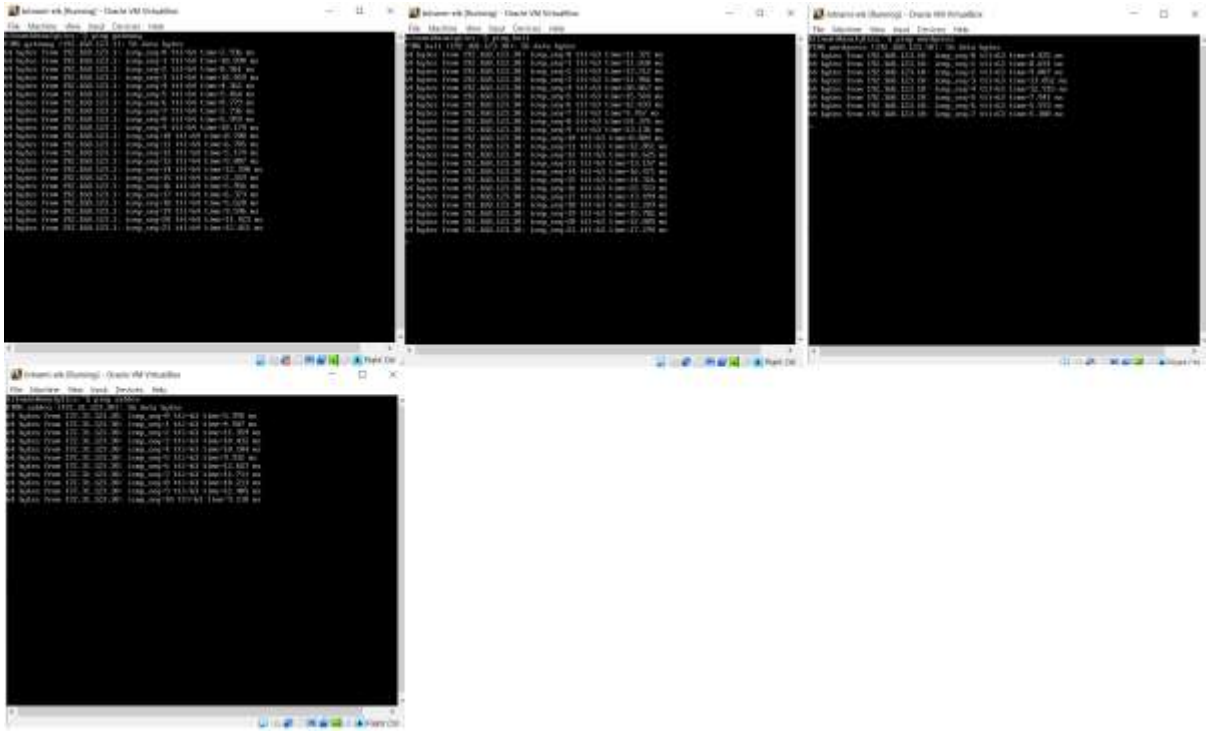
2) Kali:



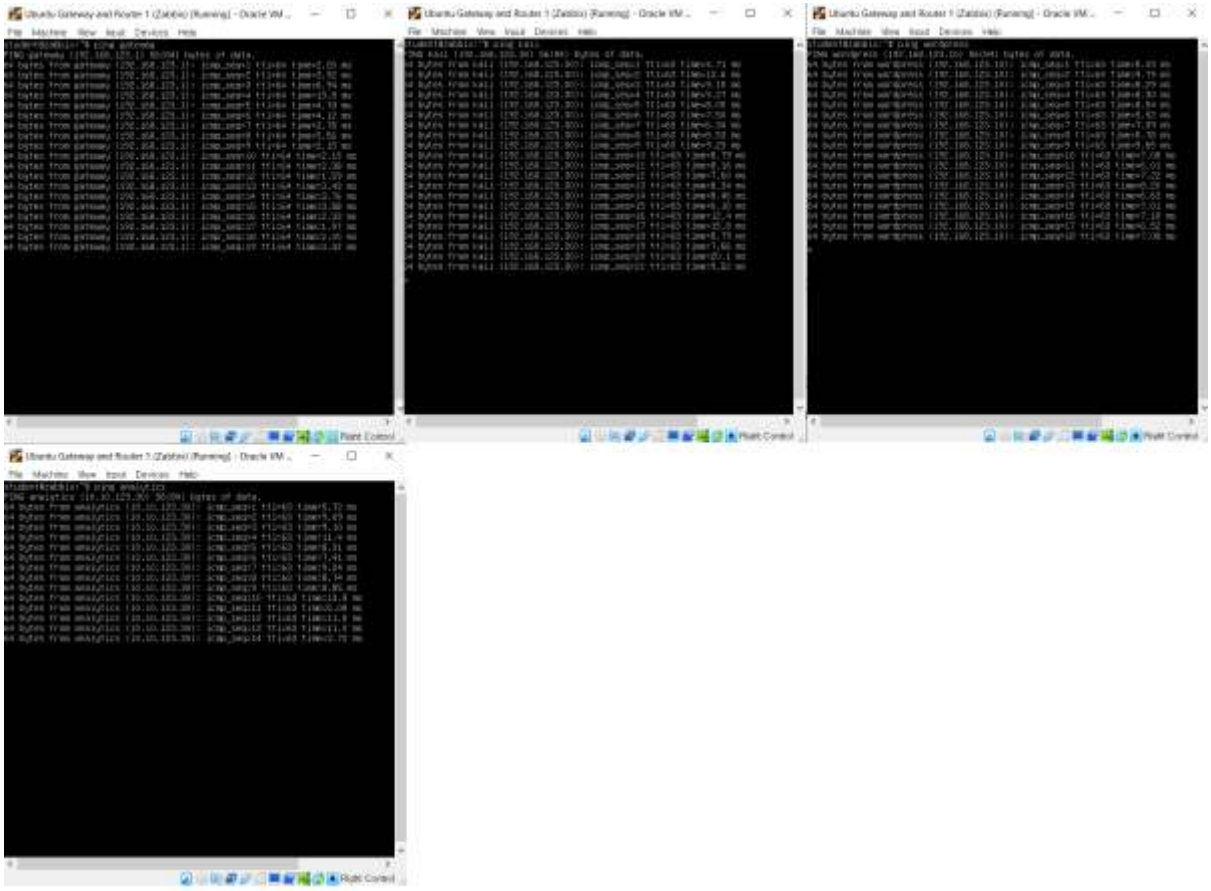
3) Wordpress:



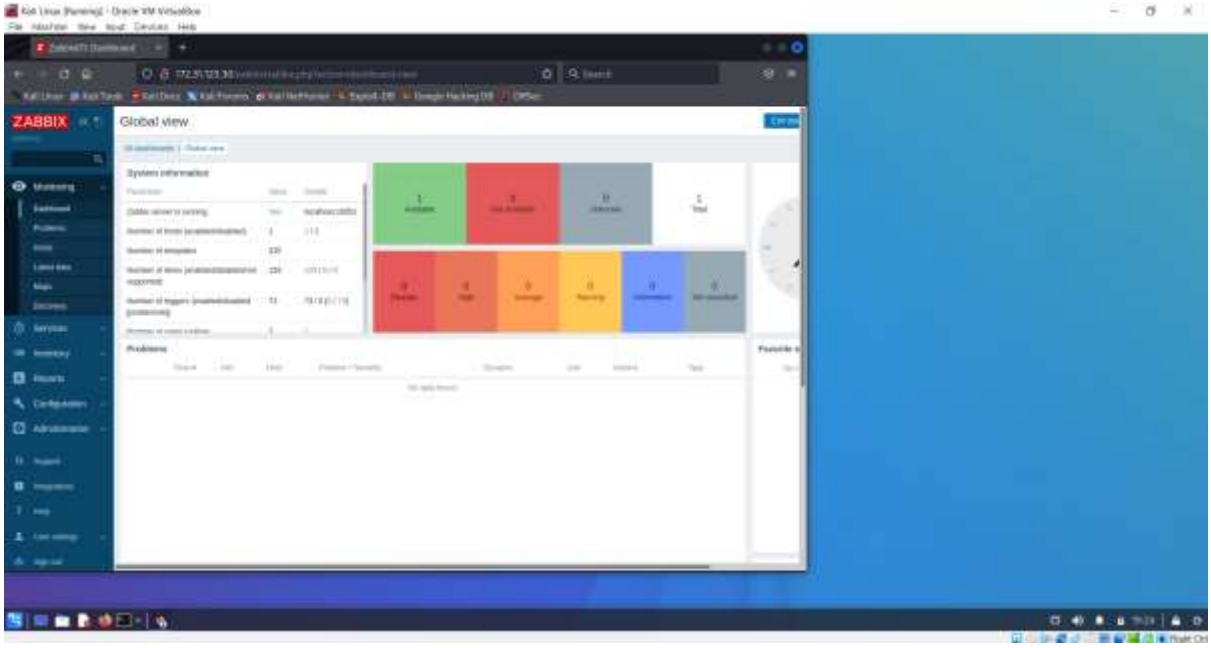
4) Analytics:



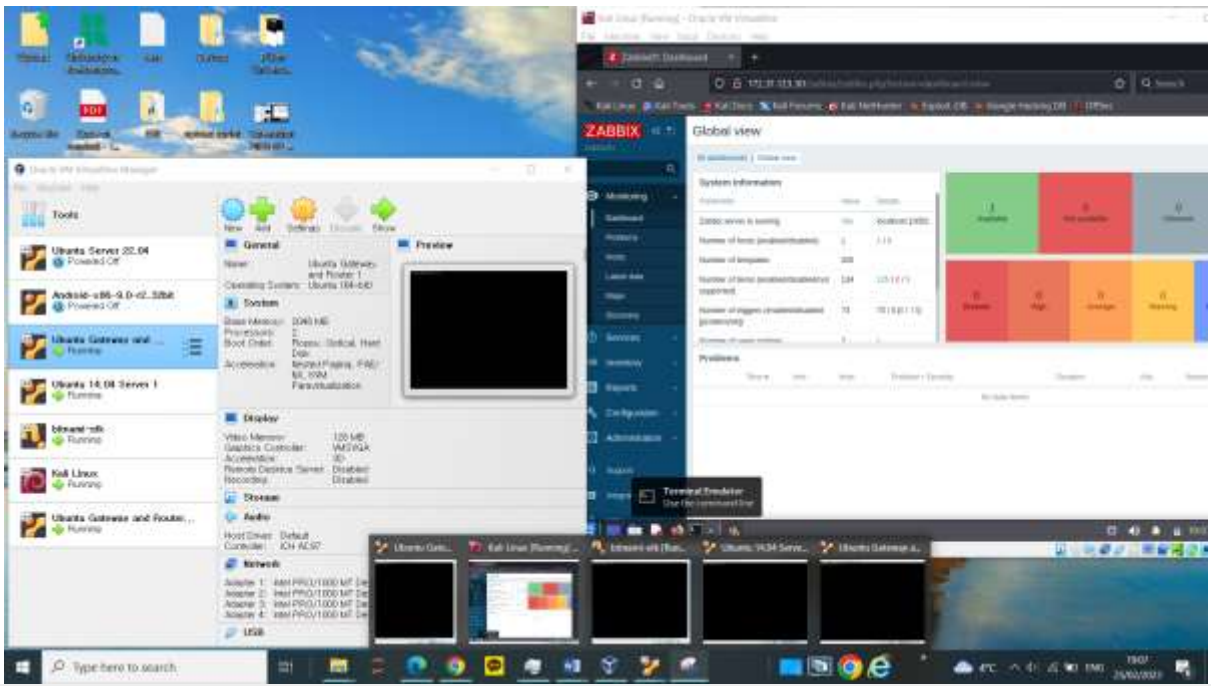
5) Zabbix:



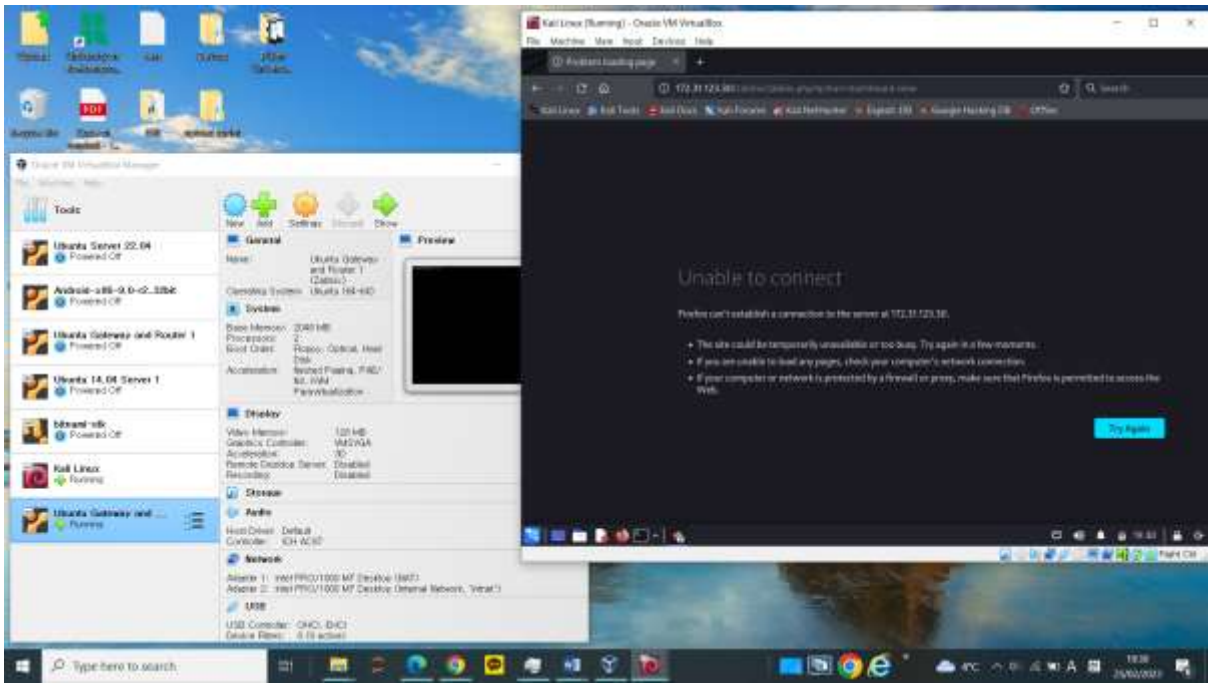
6) This is the image of logging in to the zabbix page with the Kali virtual machine.



7) This shows that zabbix, gateway, kali, wordpress, and analysis are monitored in real time while logging into zabbix in a kali browser.



This shows that the connection to the Zabbix site in the Kali browser is disconnected when Wordpress, analytics , and Gateway virtual machines are turned off.



Portfolio Requirement B: Exploring NMAP Commands

From your Kali virtual machine, test the following **nmap** commands on your sandboxed network.

What is nmap?

"Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime".
Definition Source: https://nmap.org/ (Accessed 29th October 2022)

Nmap is also a useful tool for conducting preliminary port scans of assets on a network. Port scanning activities are part of the reconnaissance and scanning stages of pen testing, during which the aim is to detect potential vulnerabilities. Particularly where a vulnerability has a known threat that poses a tangible risk to an asset.

What is a vulnerability?

"A software vulnerability is a bug or error found in a cybersecurity system and is a point of weakness which can be exploited by cybercriminals. These bad actors gain unauthorized access through network vulnerabilities and carry out cyberattacks.
Definition Source: https://www.malwarebytes.com/glossary (Accessed 29th October 2022)

What is a threat?

*A potential means of exploiting a target (e.g. computer, mobile device, network) through a **vulnerability**, putting the target at **risk** of being **exploited**.*

What is a risk?

*A risk occurs where a **threat** is matched to a known vulnerability (e.g. a network **port** left "open".).*

What is a port?

"A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection."
Definition Source: https://nmap.org/ (Accessed 29th October 2022)

Why are ports an important factor in cyber security?

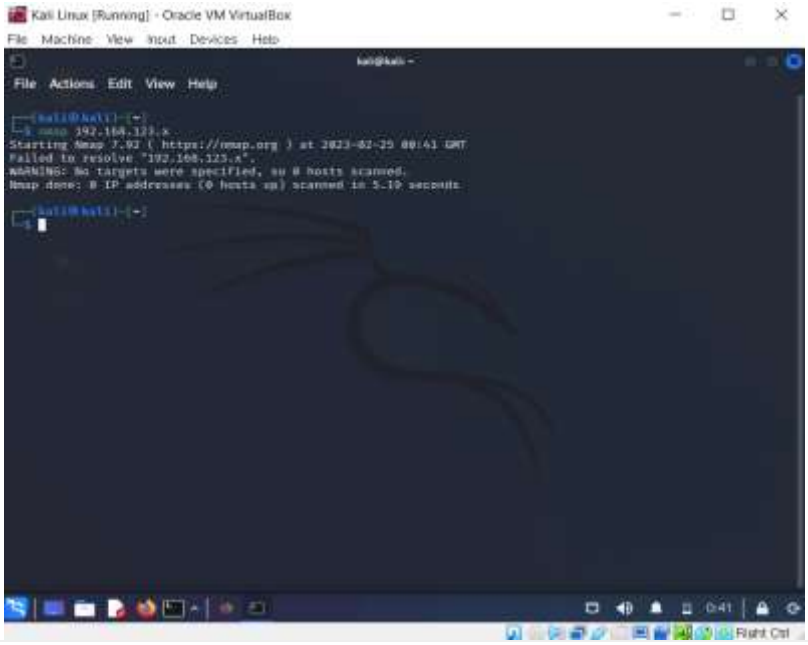
**"A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.*
When hackers send a message to a port, the response they receive determines whether the port is being used and if there are any potential weaknesses that could be exploited.

*Businesses can also use the port scanning technique to send packets to specific ports and analyze responses for any potential vulnerability. They can then use tools like IP scanning, network mapper (**Nmap**), and Netcat to ensure their network and systems are secure."*
Definition Source: https://www.fortinet.com/resources/cyberglossary/what-is-port-scan (Accessed 29th October 2022)

1. Scan a Single Host or an IP Address

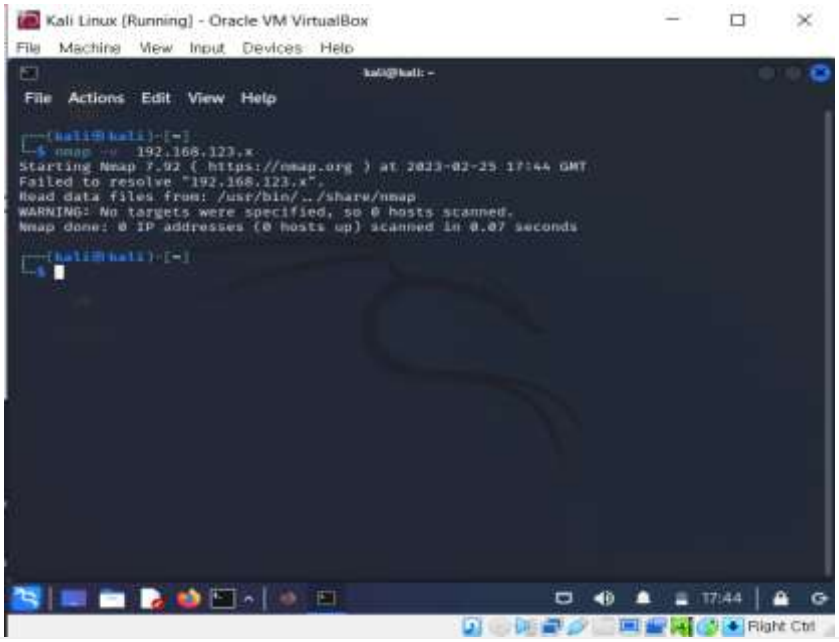
Scan a **Single IP Address**:

```
$ nmap 192.168.123.x
```

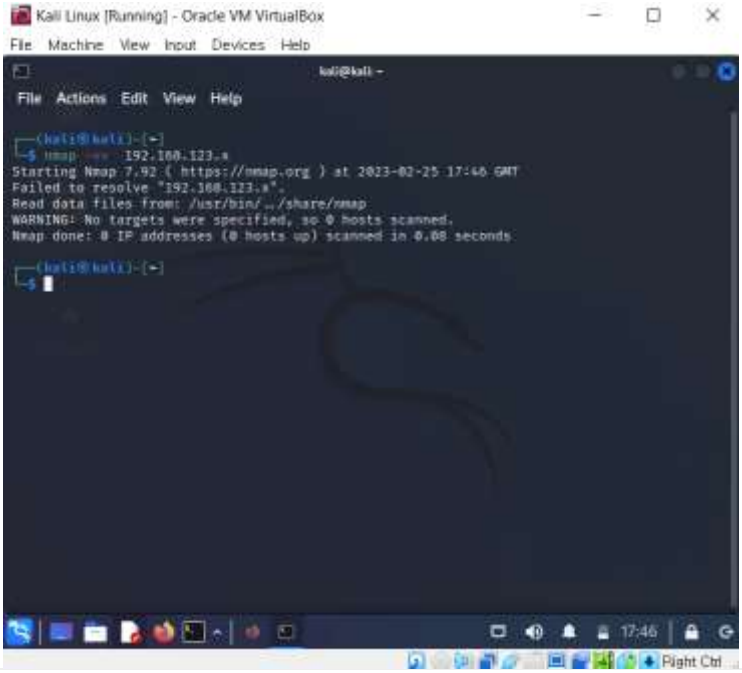


The verbosity of feedback from a command can be used by including the `-v` and `-vv` options.

```
$ nmap -v 192.168.123.x
```




```
$ nmap -vv 192.168.123.x
```



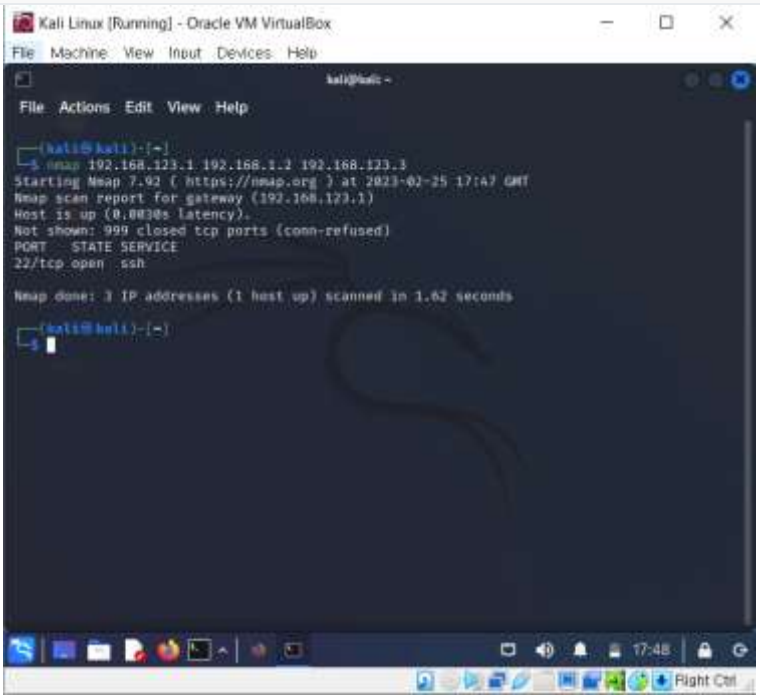
2. Scan Multiple IP Addresses

Scan **Multiple IP Addresses**:

```
$ nmap 192.168.123.1 192.168.1.2 192.168.123.3
```

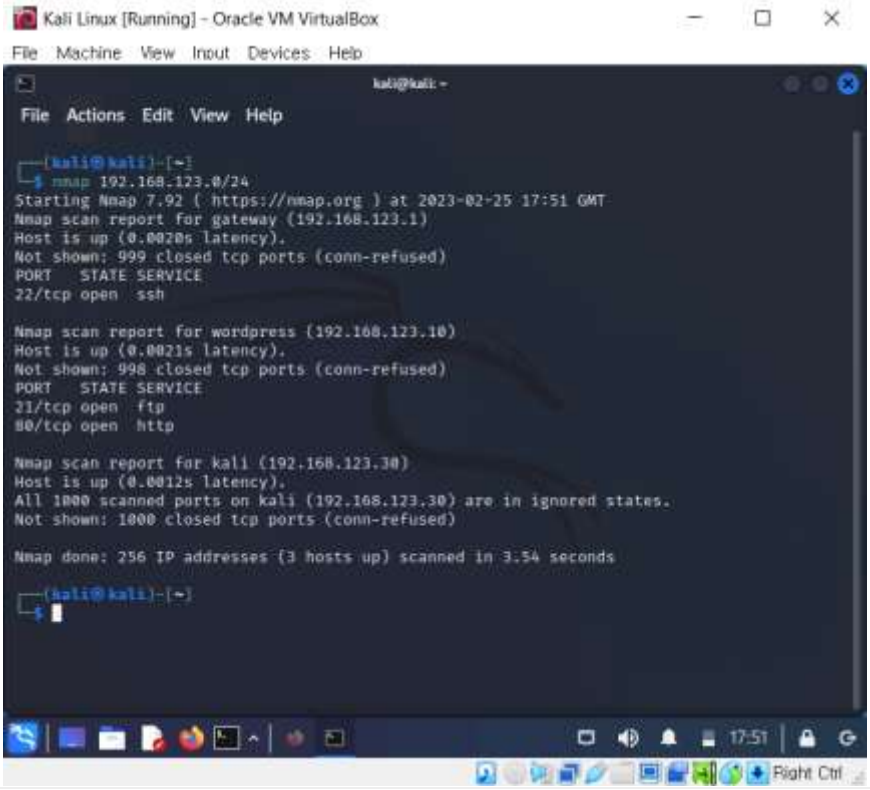
or

```
$ nmap 192.168.123.1,2,3
```

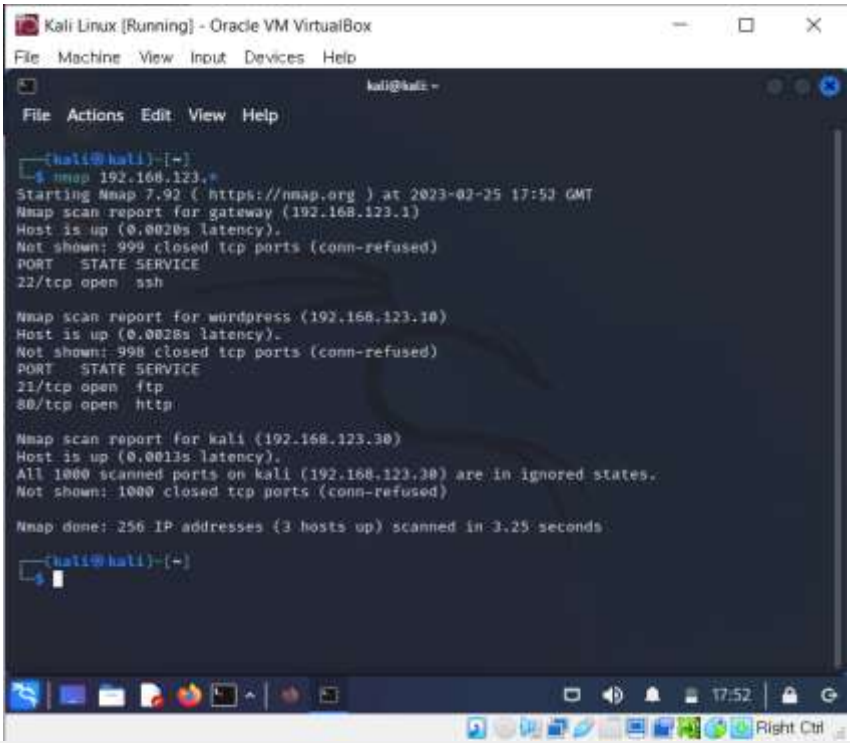


3. Scan a Subnet:

```
$ nmap 192.168.123.0/24
```

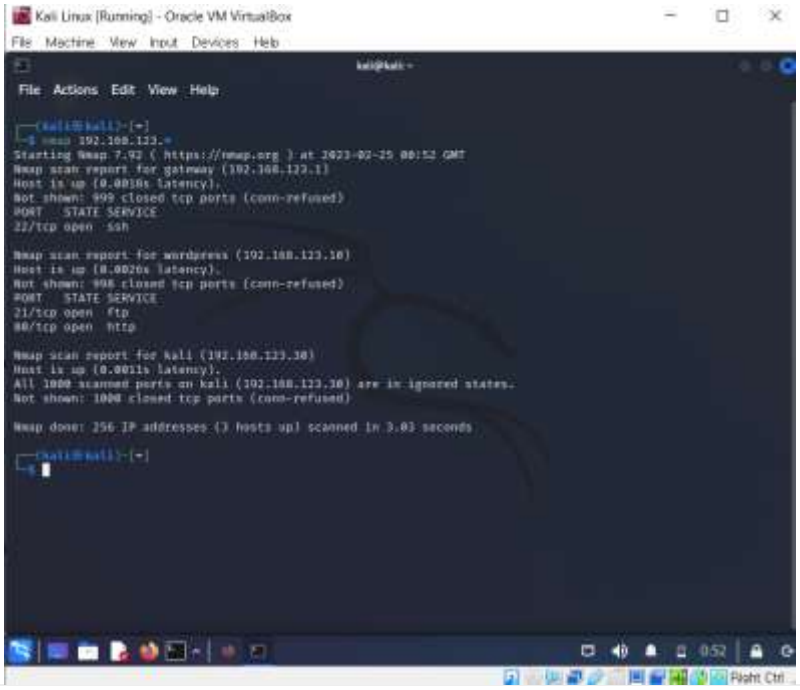



```
$ nmap 192.168.123.*
```



4. Scan a Range of IP Addresses (192.168.1.0 – 192.168.1.200):

```
$ nmap 192.168.123.0-200
```

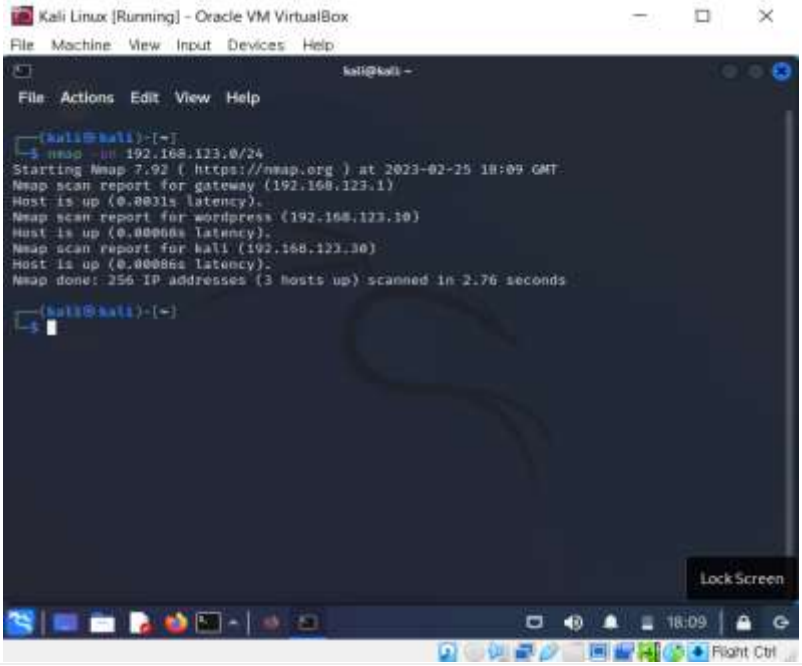


5. Scan a Network for Active Computers

Tip: Scan the network with the `ping` command only! Discover all the active computers in your LAN! [Read more →]

Scan for **Active Hosts** on a network:

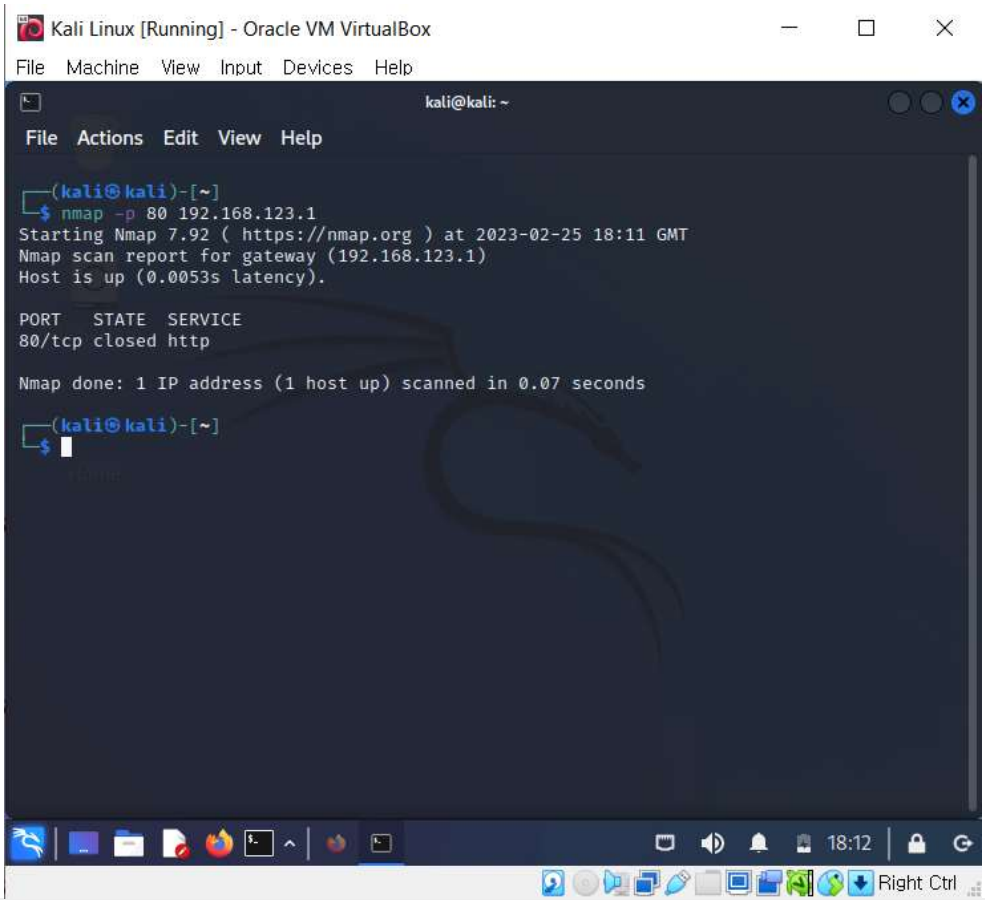
```
$ nmap -sn 192.168.123.0/24
```



6. Scan For Specific Ports

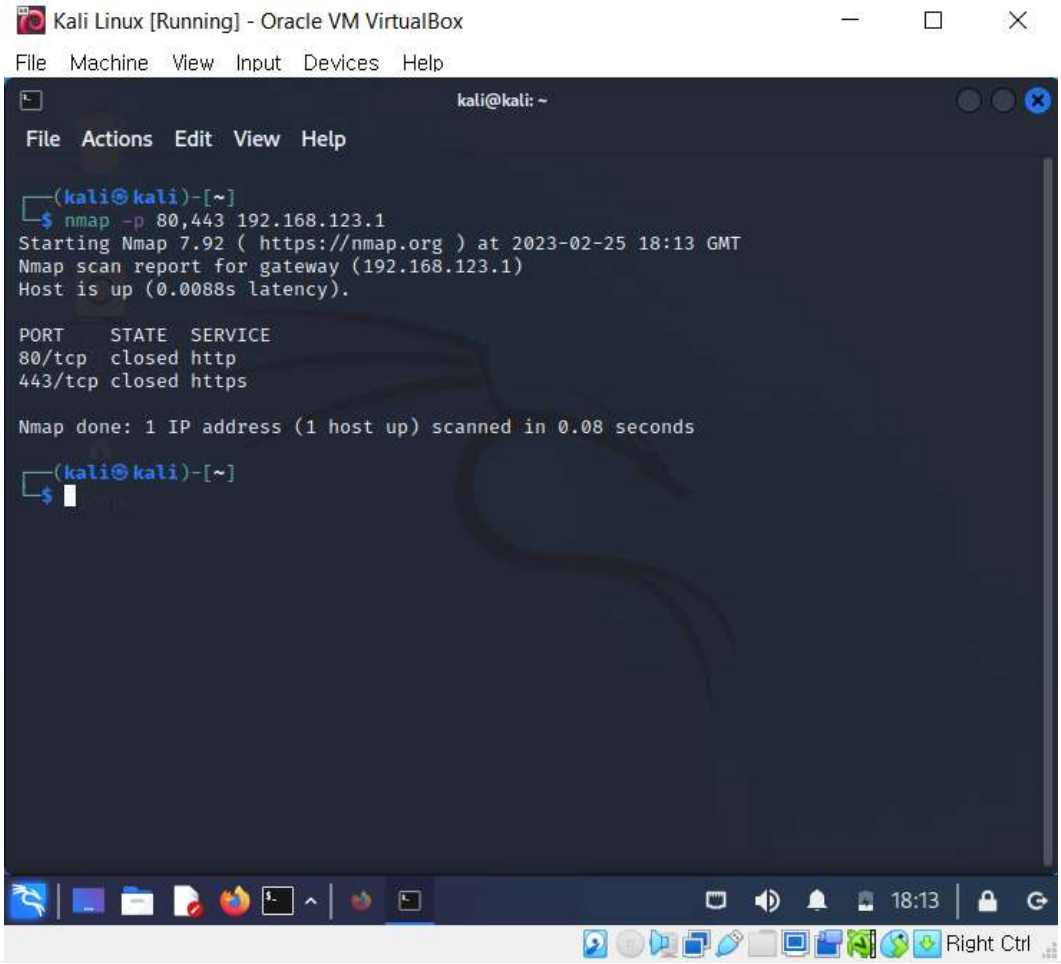
Scan for a **Single Port**:

```
$ nmap -p 80 192.168.123.1
```



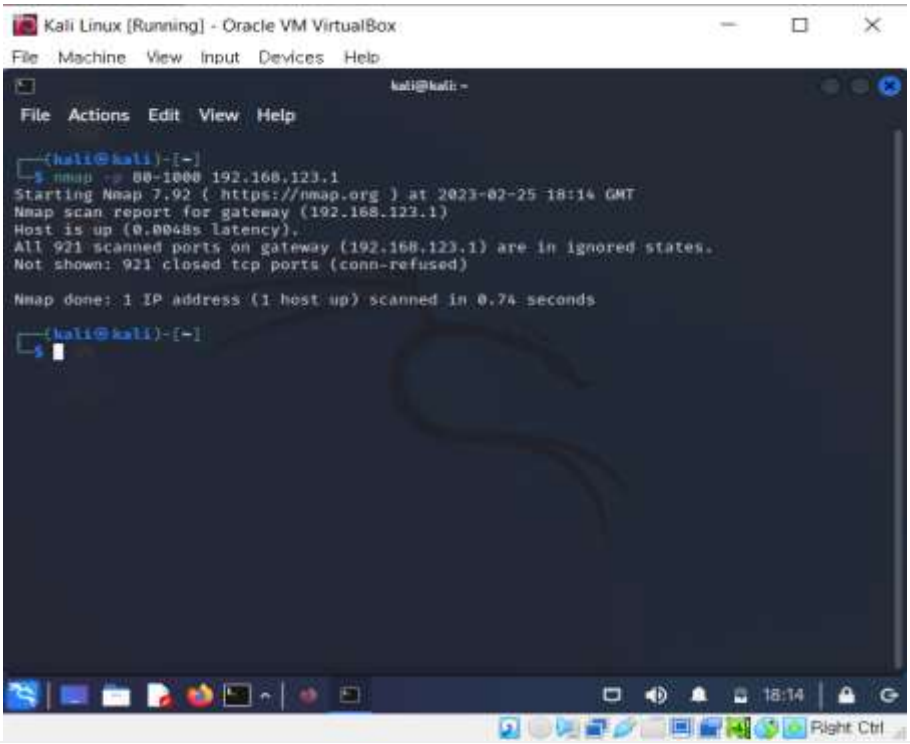
Scan for **Several Ports**:

```
$ nmap -p 80,443 192.168.123.1
```



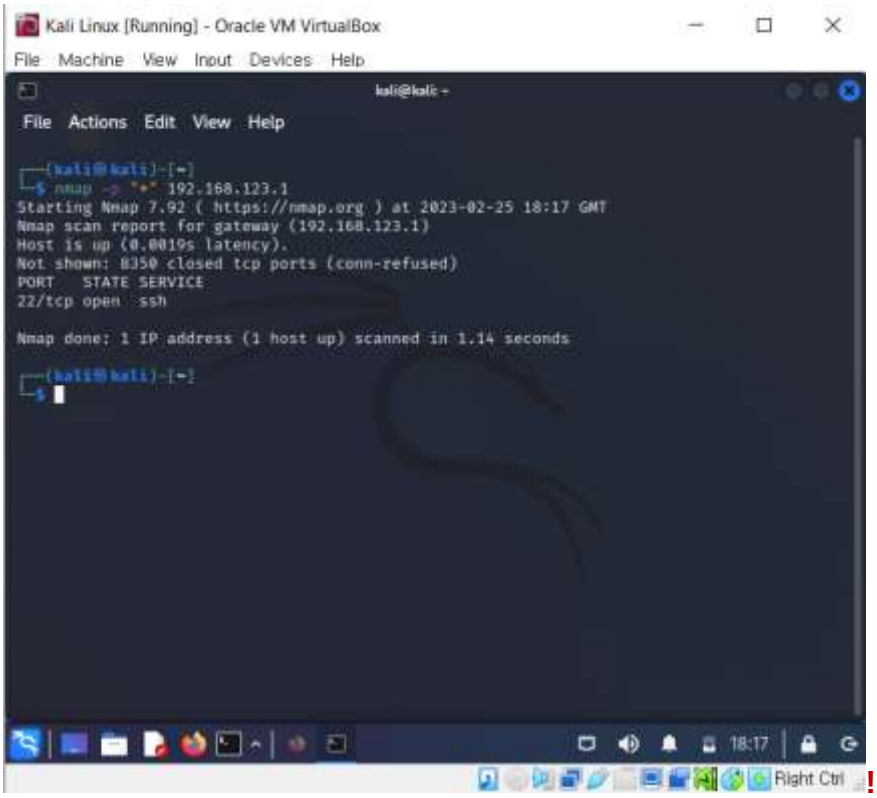
Scan for a **Port Range**:

```
$ nmap -p 80-1000 192.168.123.1
```



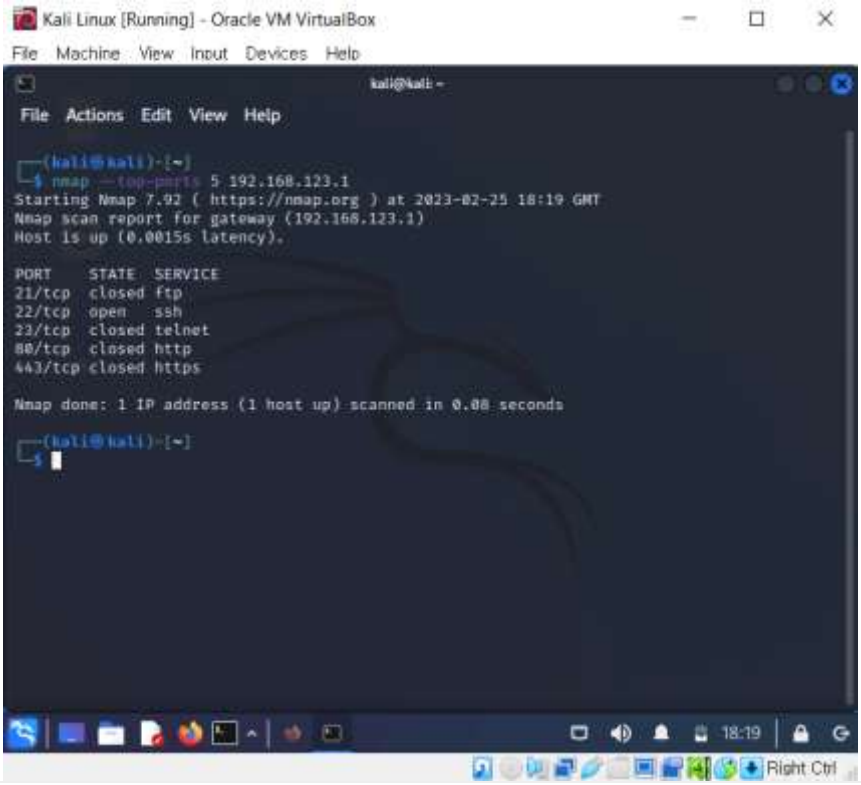
Scan for **All Ports**:

```
$ nmap -p "*" 192.168.123.1
```

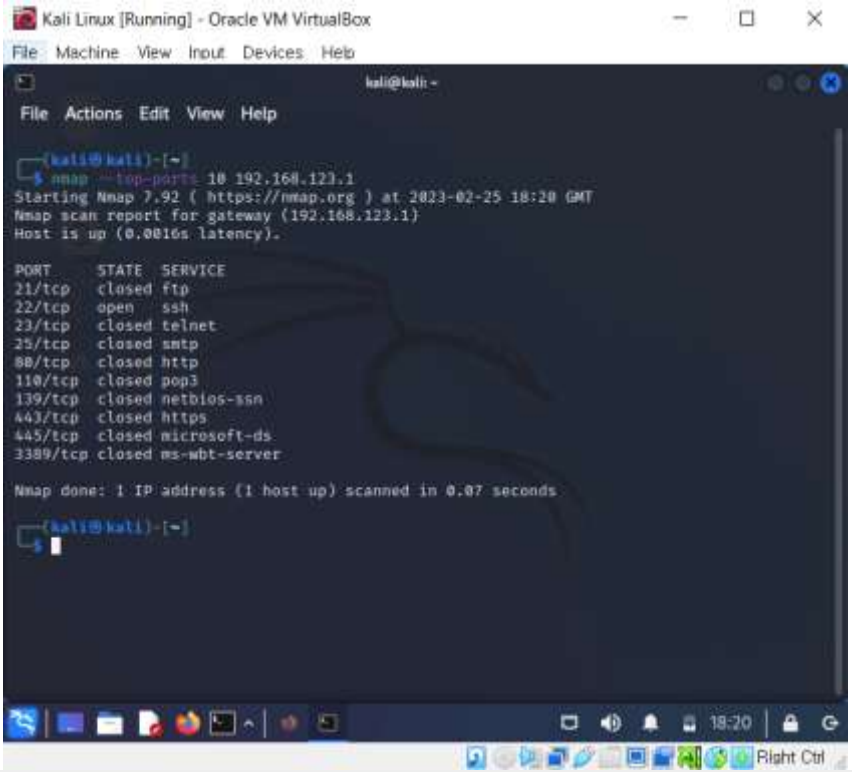


Scan for top most **Common Ports**:

```
$ nmap --top-ports 5 192.168.123.1
```



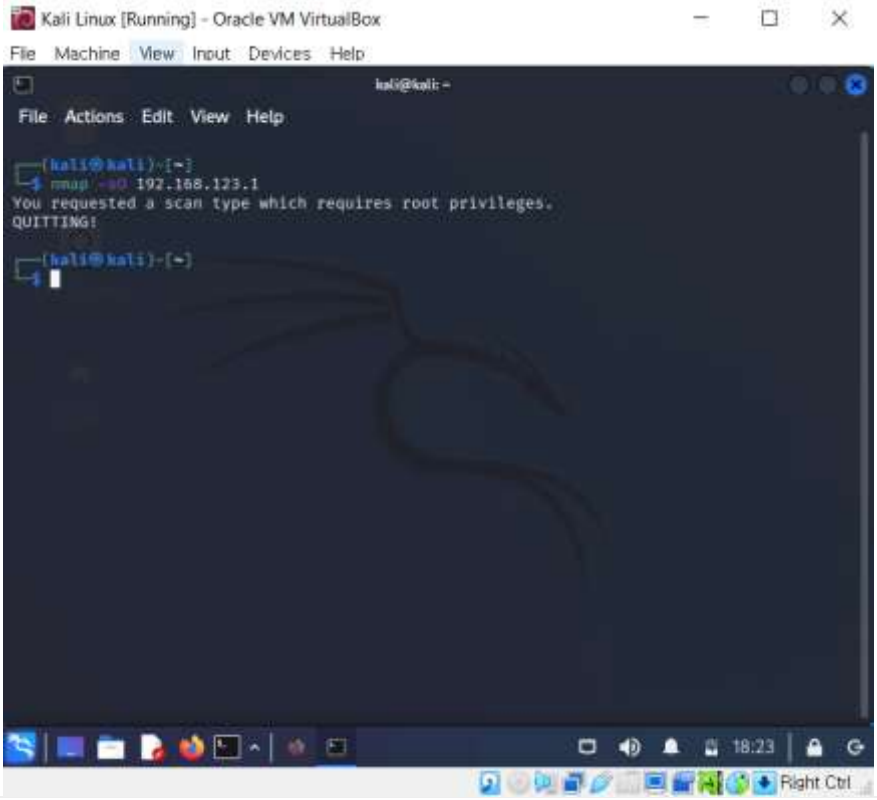

```
$ nmap --top-ports 10 192.168.123.1
```



7. Determine Supported IP Protocols

Determine which **IP Protocols** (TCP, UDP, ICMP, etc.) are supported by target host:

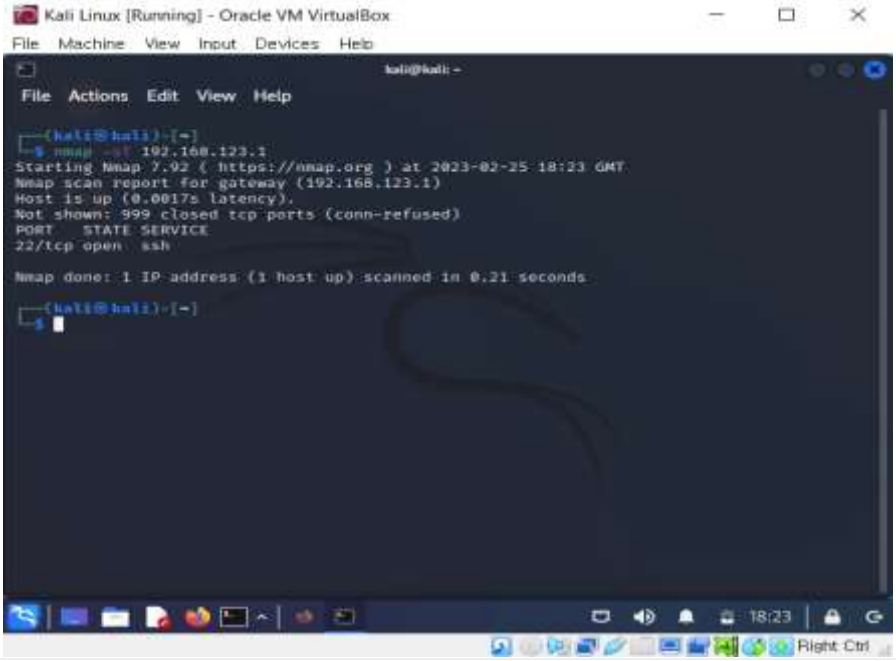
```
$ nmap -sO 192.168.123.1
```



8. Scan For TCP/UDP Ports

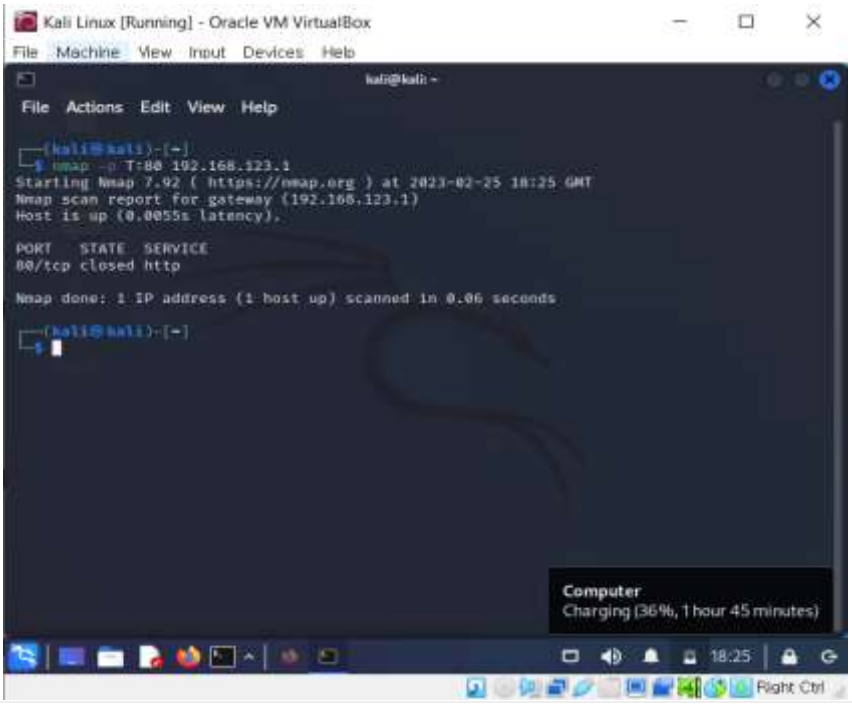
Scan for **All TCP Ports**:

```
$ nmap -sT 192.168.123.1
```



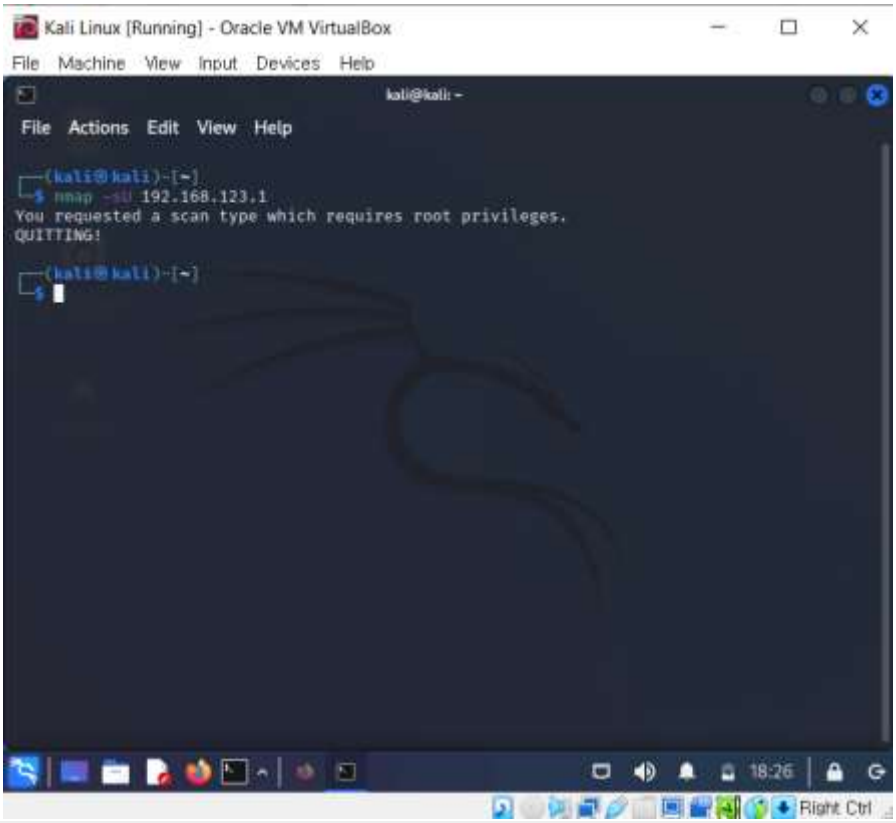
Scan for **Particular TCP Ports**:

```
$ nmap -p T:80 192.168.123.1
```



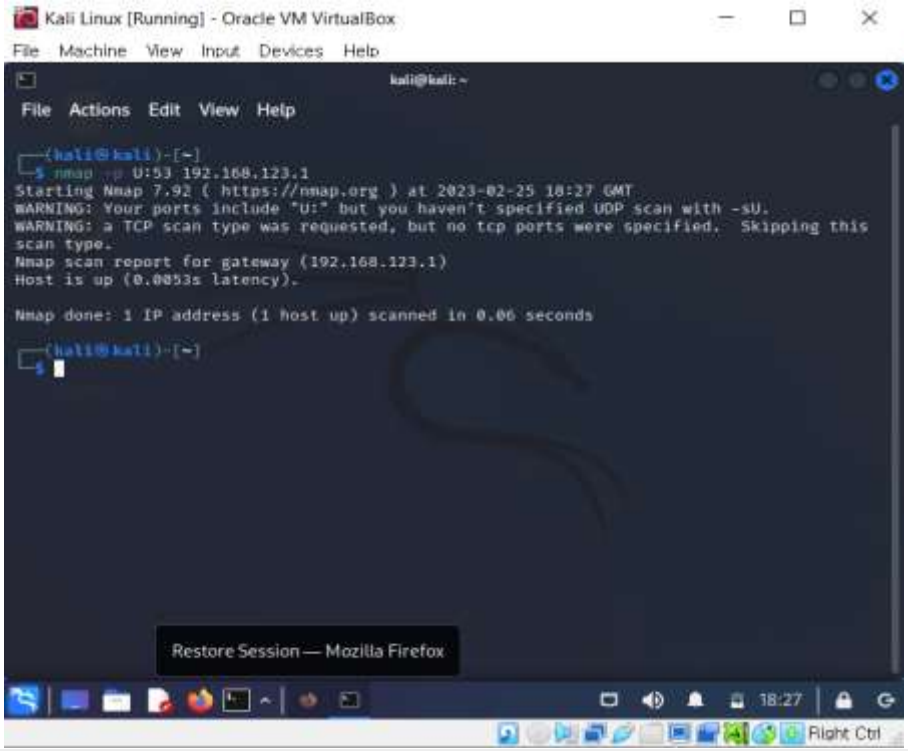
Scan for **All UDP Ports**:

```
$ nmap -sU 192.168.123.1
```



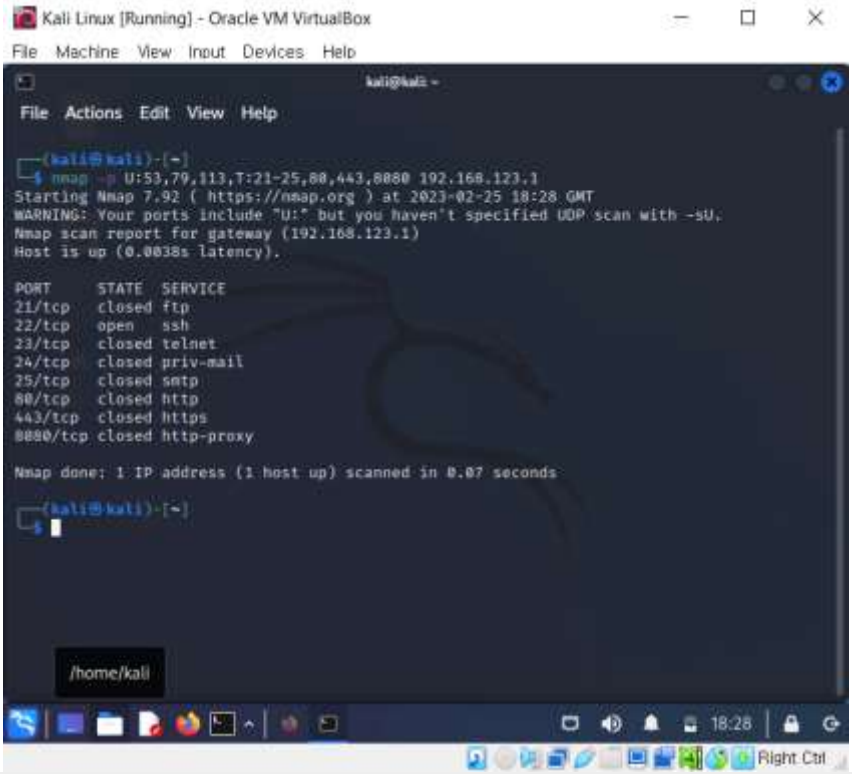
Scan for **Particular UDP Ports**:

```
$ nmap -p U:53 192.168.123.1
```



Combine scanning of different ports:

```
$ nmap -p U:53,79,113,T:21-25,80,443,8080 192.168.123.1
```

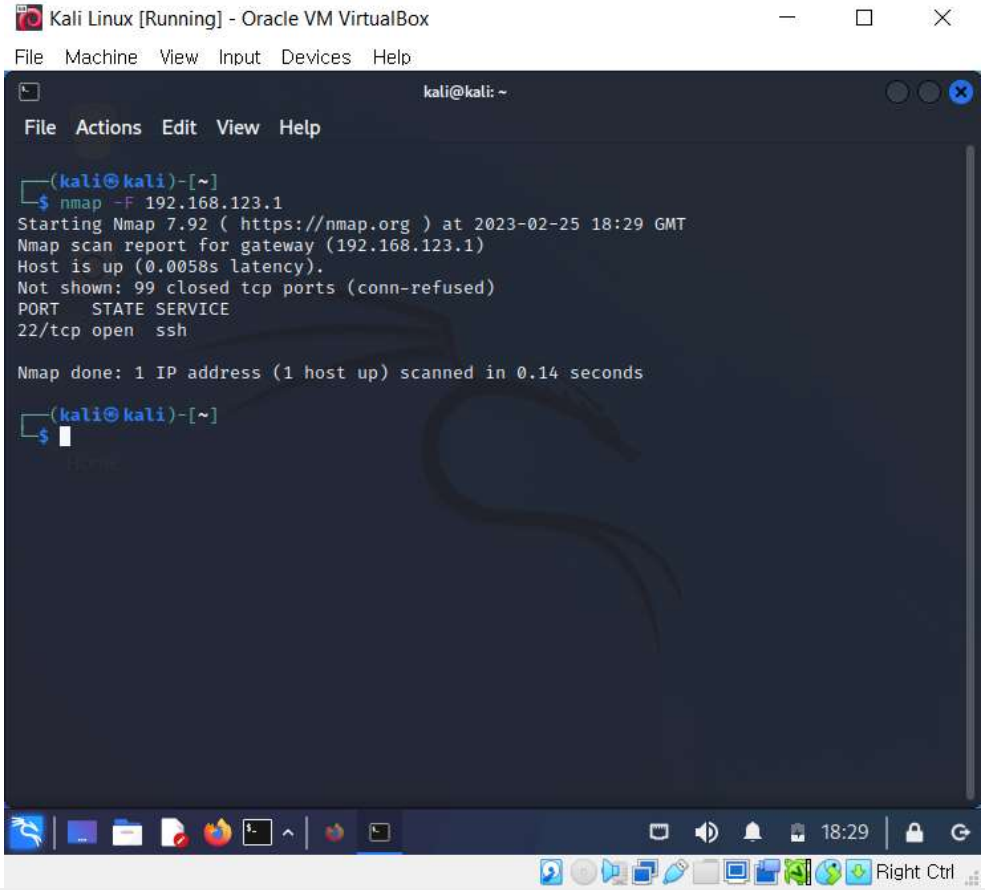


9. Perform a Fast Scan

Enable **Fast Mode**:

```
$ nmap -F 192.168.123.1
```

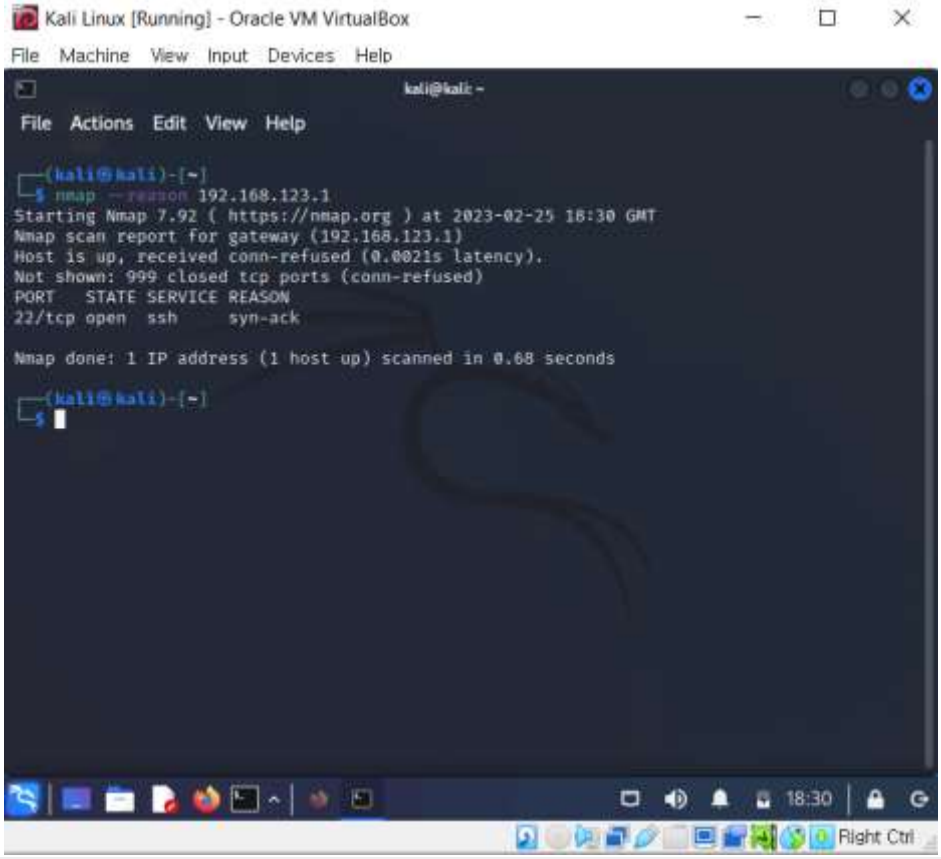
** Scan fewer ports than the default scan.*



10. Display the Reason a Port is in a Particular State

Display the **Reason** why Nmap thinks that a port is in a particular state:

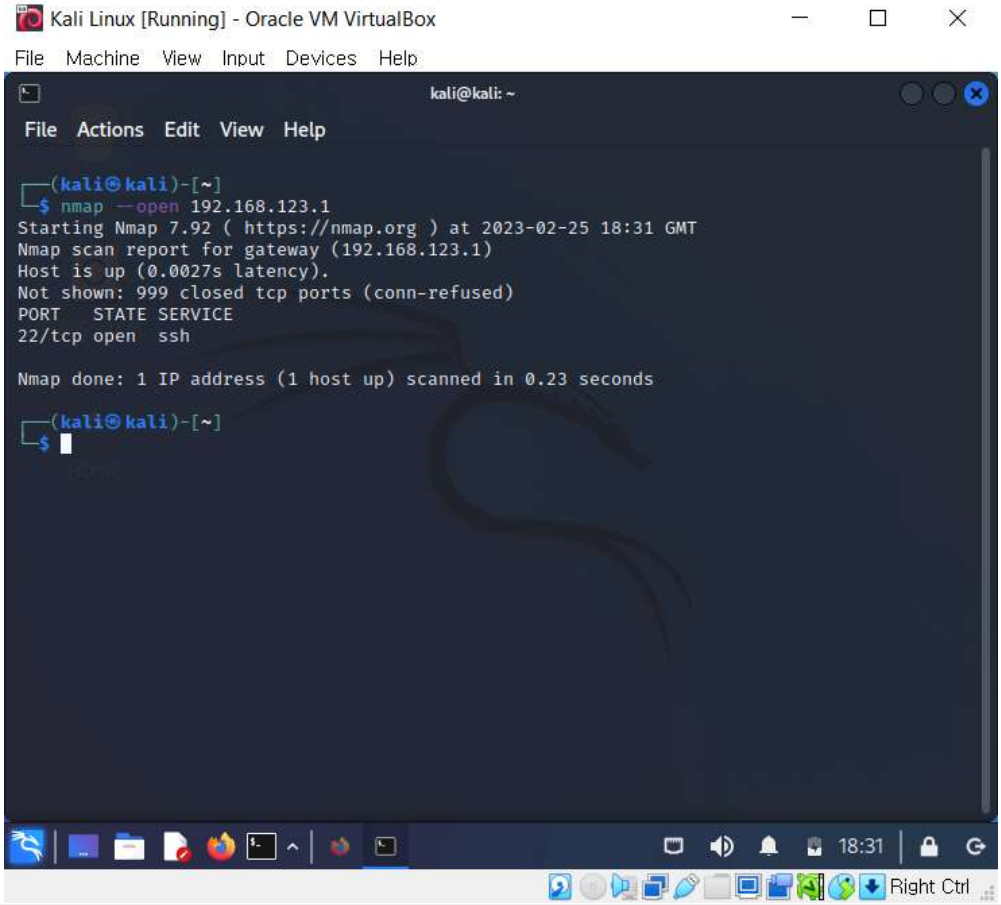
```
$ nmap --reason 192.168.123.1
```



11. Show Only Open Ports

Show **Only Open Ports** (or possibly open):

```
$ nmap --open 192.168.123.1
```

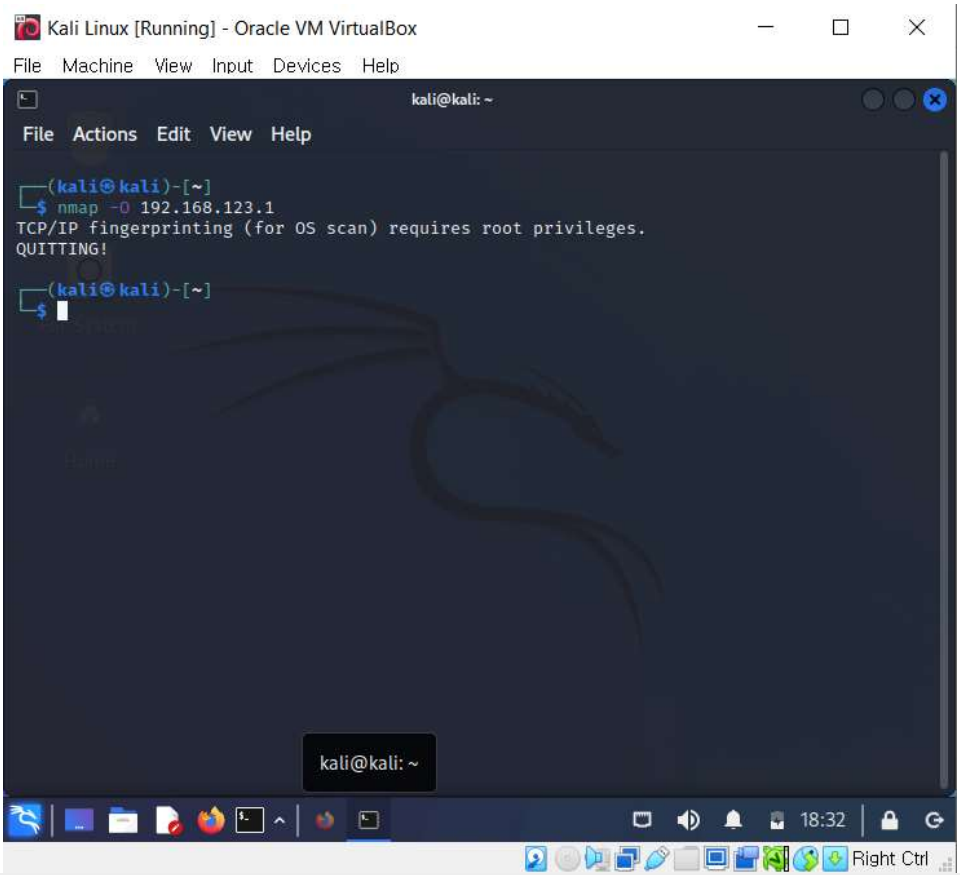


12. OS Detection

One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines the responses. After performing dozens of tests, Nmap compares the results to its database and prints out the OS details if there is a match.

Turn on **OS Detection**:

```
$ nmap -O 192.168.123.1
```

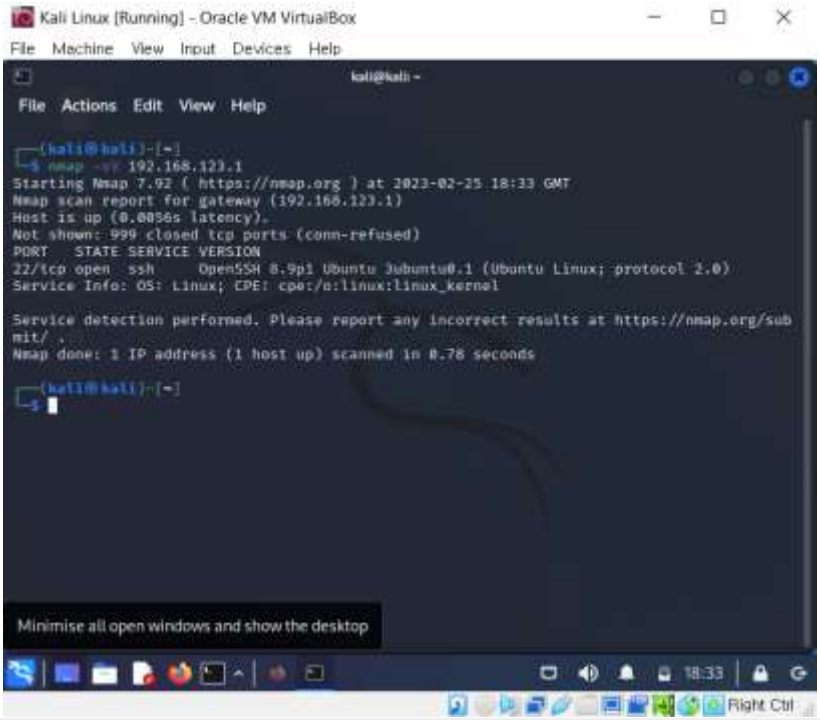


13. Service Version Detection

Turn on **Version Detection**:

```
$ nmap -sV 192.168.123.1
```

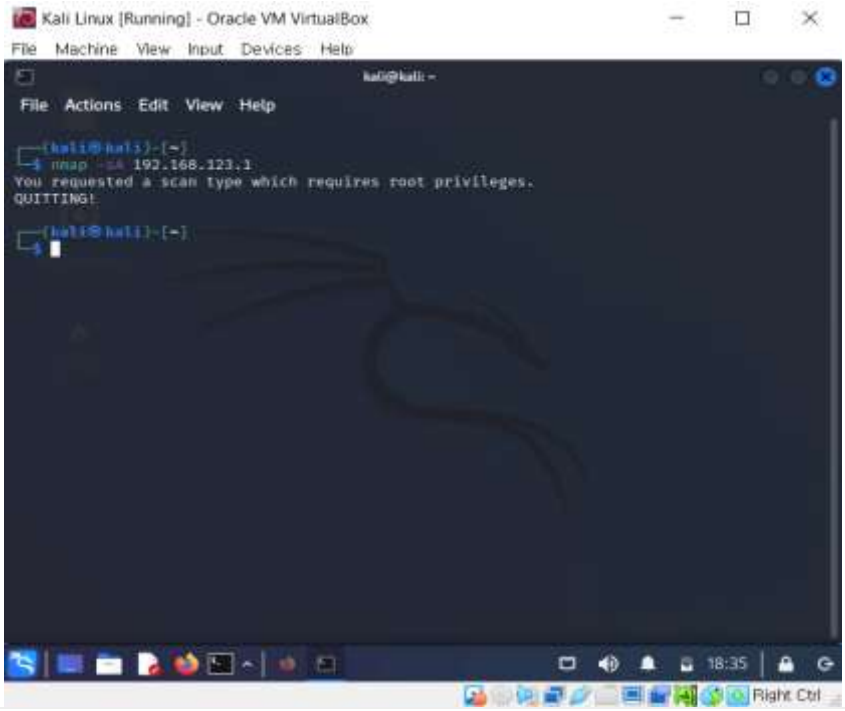
* *Discover what version of software is running on a remote host.*



14. Firewall Detection

Find out if a host is protected by any Packet Filters or Firewall:

```
$ nmap -sA 192.168.123.1
```



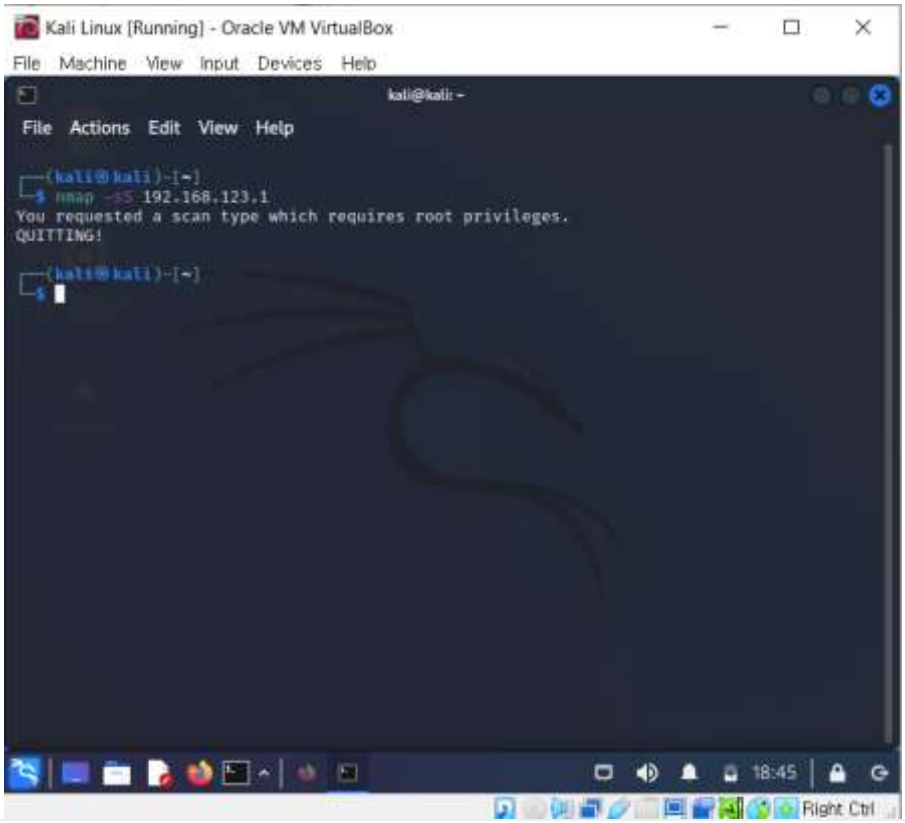
15. Stealthy Scan

Tip: Stay anonymous during port scanning! Use `Nmap` + `Tor` + `ProxyChains`! Safe and easy penetration testing! [Read more →]

TCP SYN Scan:

```
$ nmap -sS 192.168.123.1
```

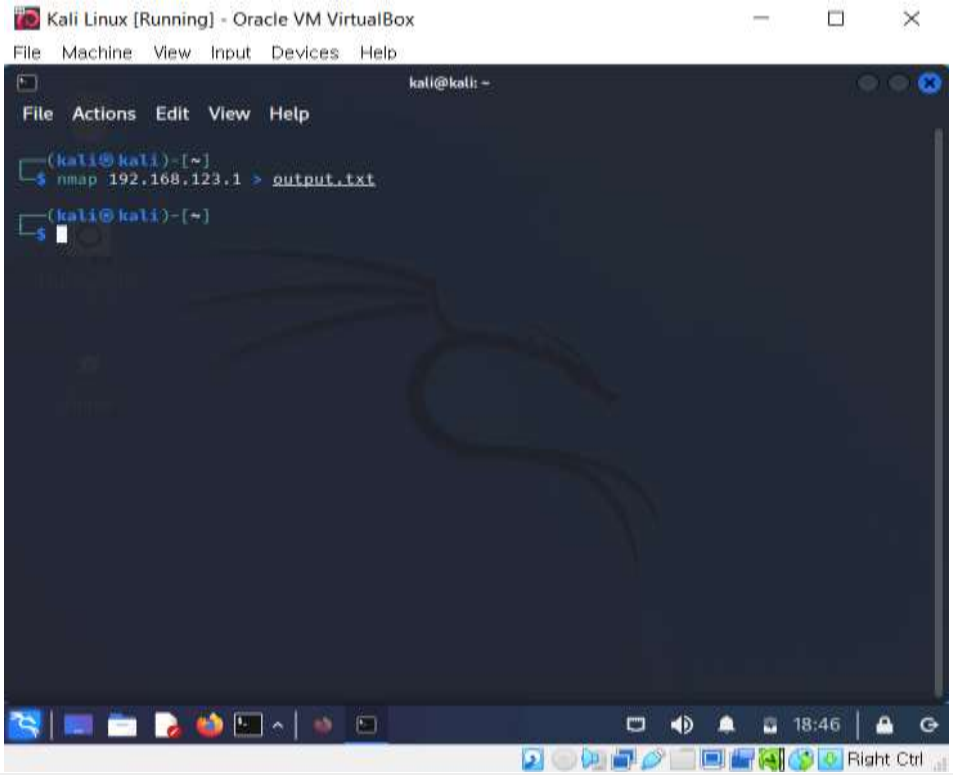
* *Well known as a half-open scanning, as it doesn't open a full TCP connection.*



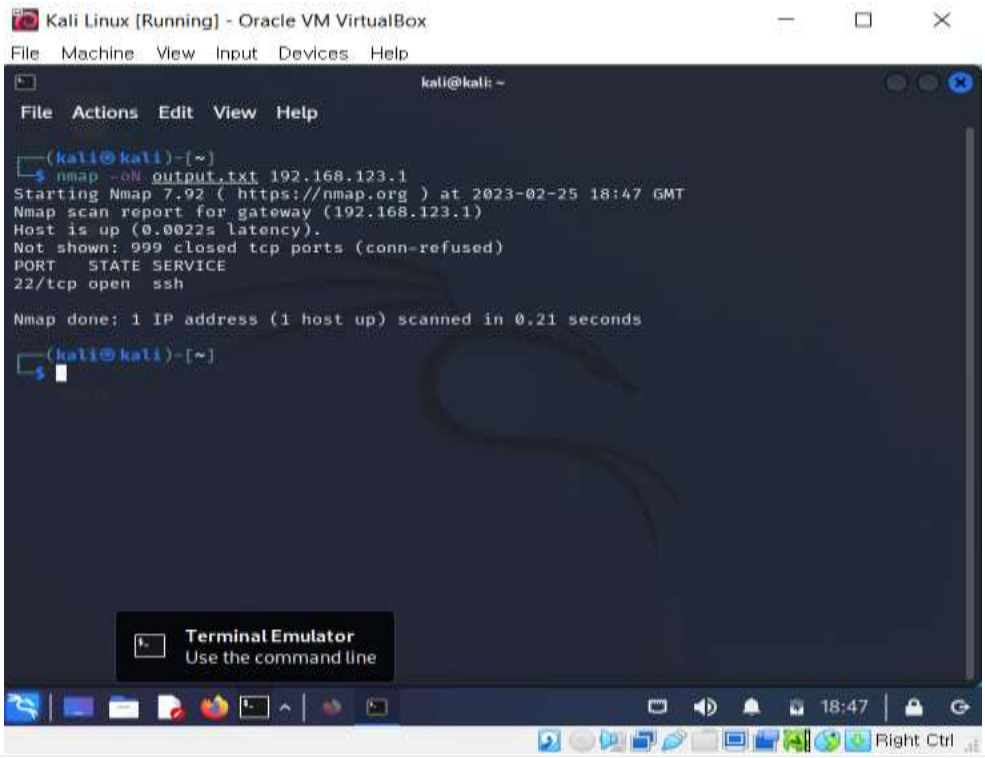
16. Save Output of Nmap Scan to a File

Save output of Nmap scan to a **TEXT File**:

```
$ nmap 192.168.123.1 > output.txt
```

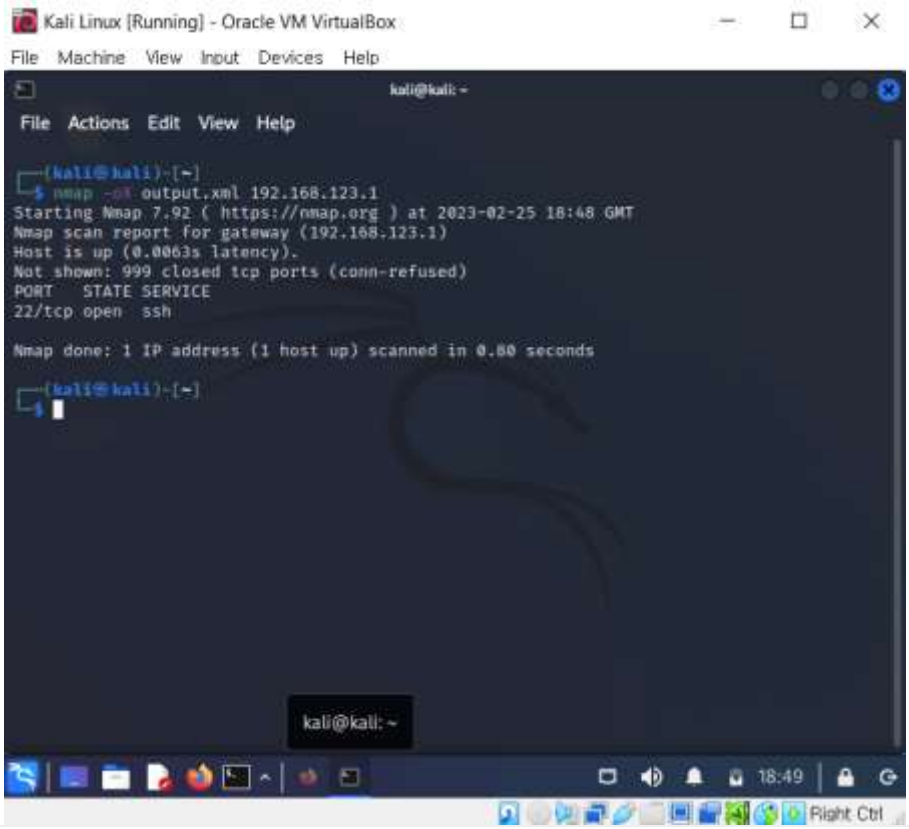



```
$ nmap -oN output.txt 192.168.123.1
```



Save output of Nmap scan to an **XML File**:

```
$ nmap -oX output.xml 192.168.123.1
```



SOURCE: https://www.shellhacks.com/20-nmap-examples/ (Accessed 29th October 2022)

Wow factor suggestions.

It is feasible to pass this portfolio without completing any "wow factor". However, if you decide to take on this additional learning opportunity, the choice of what to contribute is yours. Here are some examples to consider:

- Apply a sequence of selected nmap commands to other assets in your sandboxed network.
- Expand the functionality of nmap using `python3-nmap` (python3-nmap · PyPI)

PORTFOLIO SUBMISSION RECORD

To receive a mark for this work, you must demonstrate the extent to which you have completed the requirements and specifications of this portfolio to your instructor in the lab.

NOTE: In order to ensure that instructor assessment time fairly distributed, each student is permitted one formal demonstration period, after which, marks and an outcome will be added to your Portfolio logbook.

Please complete the following table and upload this document to Moodle.

Declaration	I certify that the work for this portfolio lab is my own work.
Demonstration Date and Time:	25/02/2023 19:35
Student Name:	Taejin Kim
Student ID:	KIM20480006
Date:	25/02/2023