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:

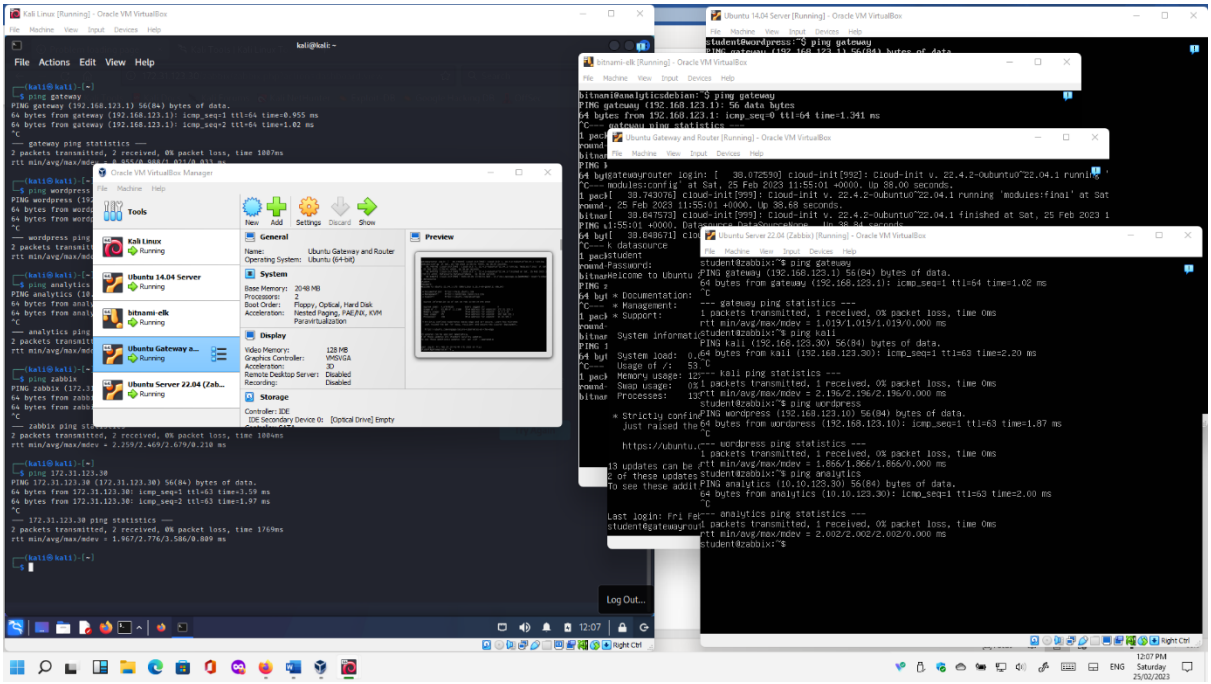
```
sudo nano /etc/hostname
```

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:~$
```



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

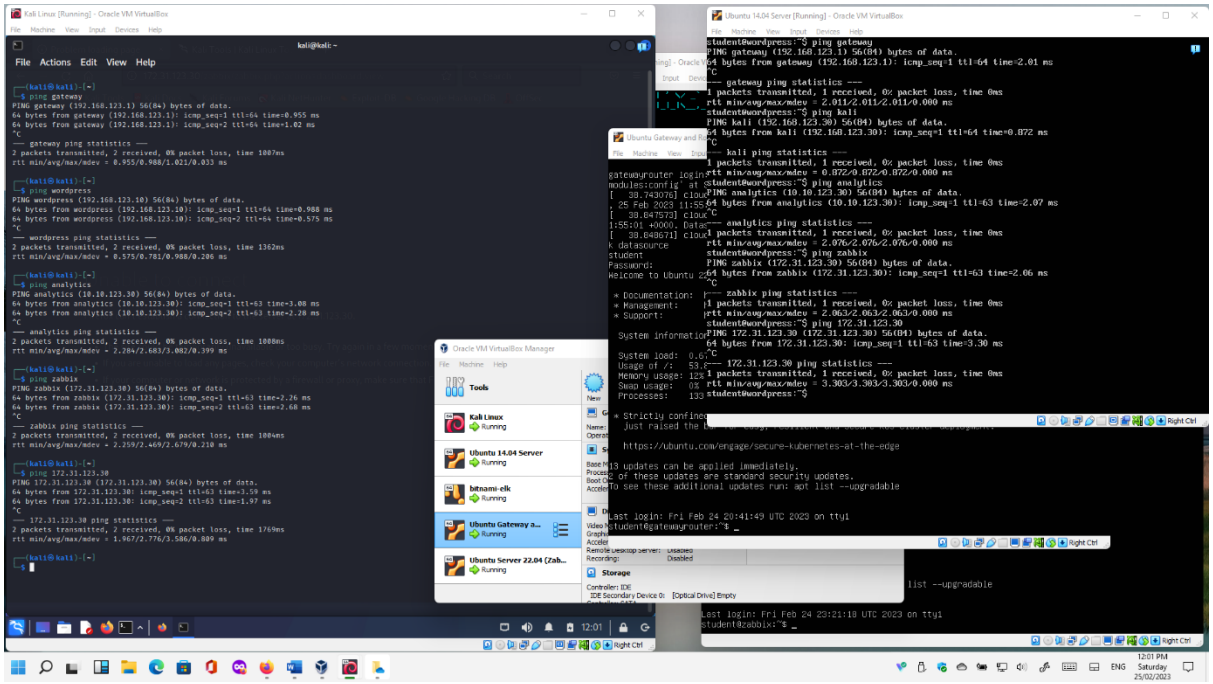
As this is also a WordPress server change the hostname to `wordpress`. Type:

```
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)

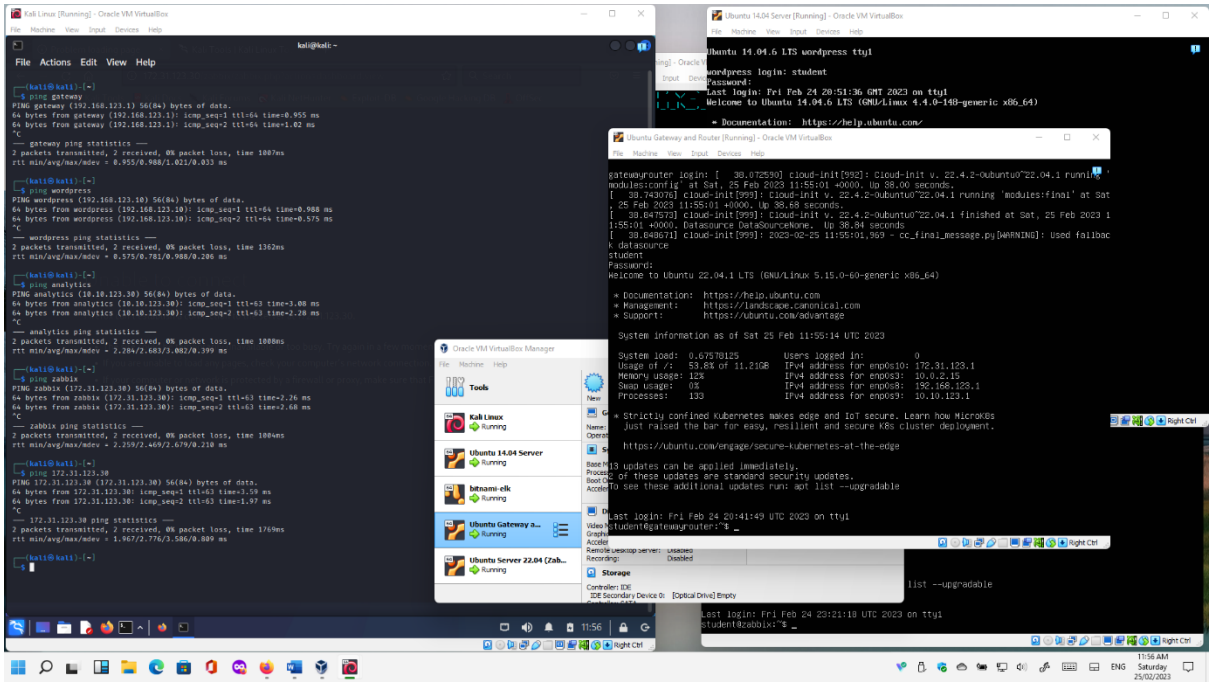
As this is a gateway server, change the hostname to `gateway`. Type:

```
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

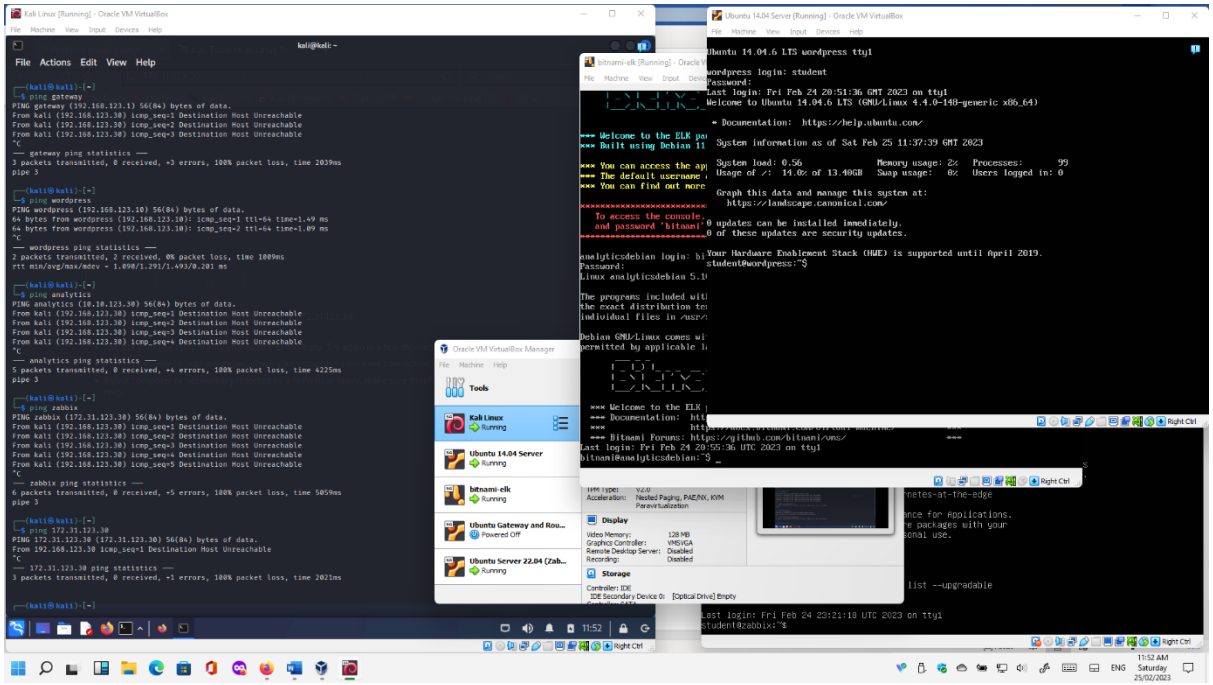
As this is an Elastic Search server (ELK Stack) change the hostname to `analytics`. Type:

```
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

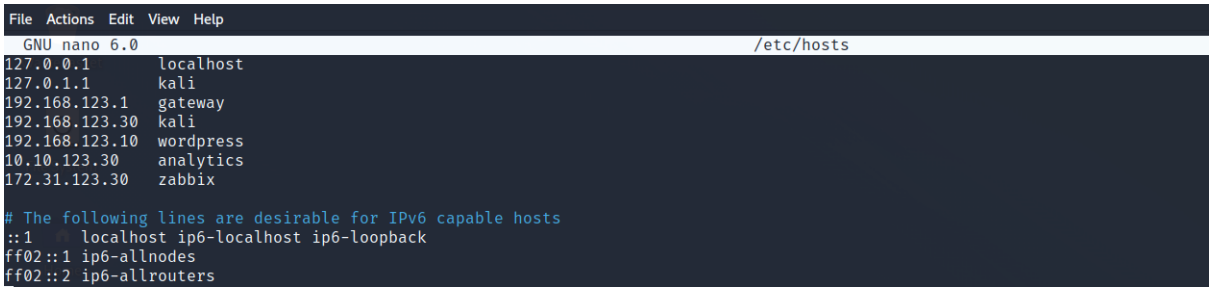
5. Make the host name for each virtual machine, resolve to its IP address

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!



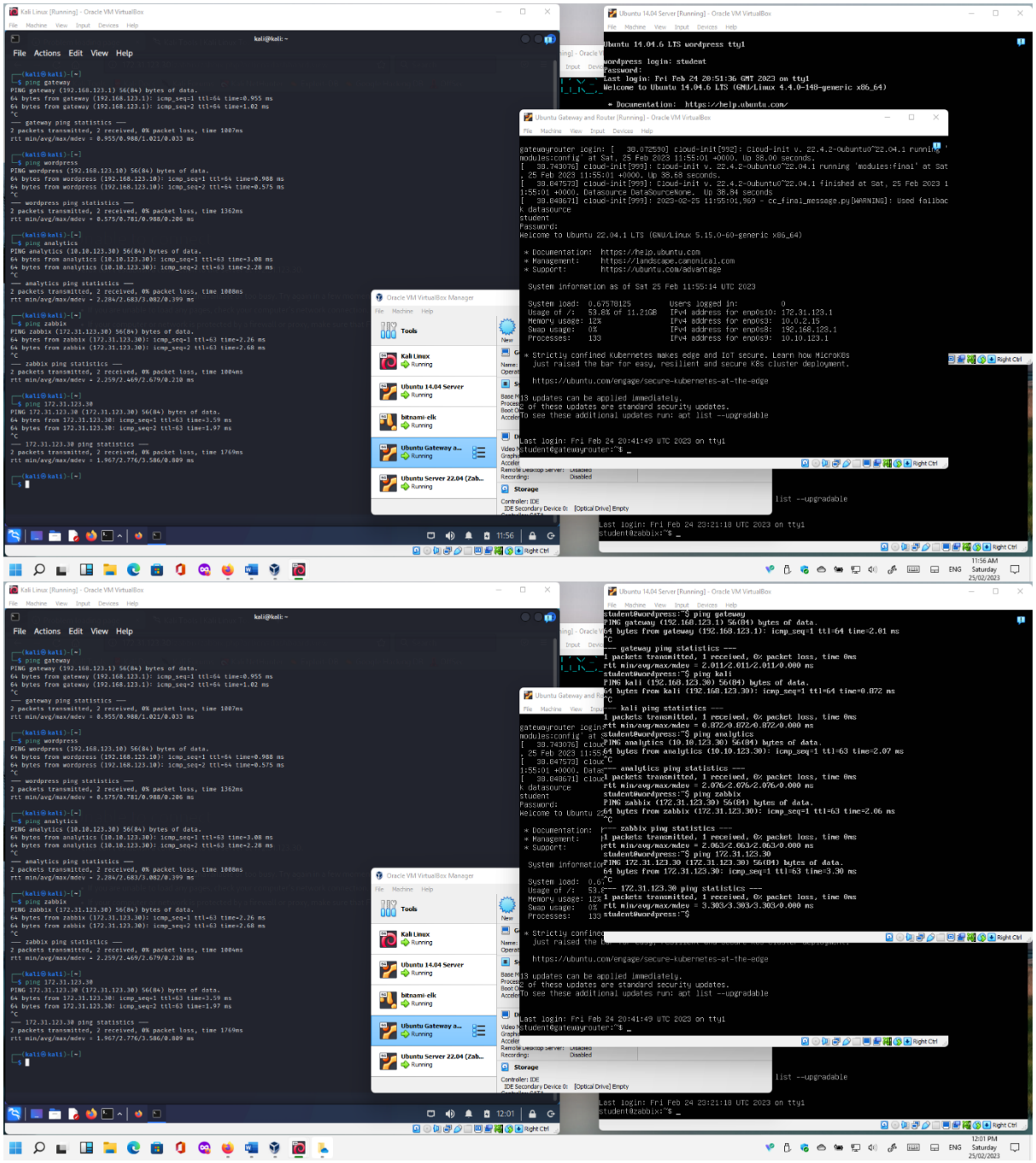
Save the open *hosts* file by typing Ctrl x, followed by y, then press Enter . From your kali terminal, test that you can ping the host names.

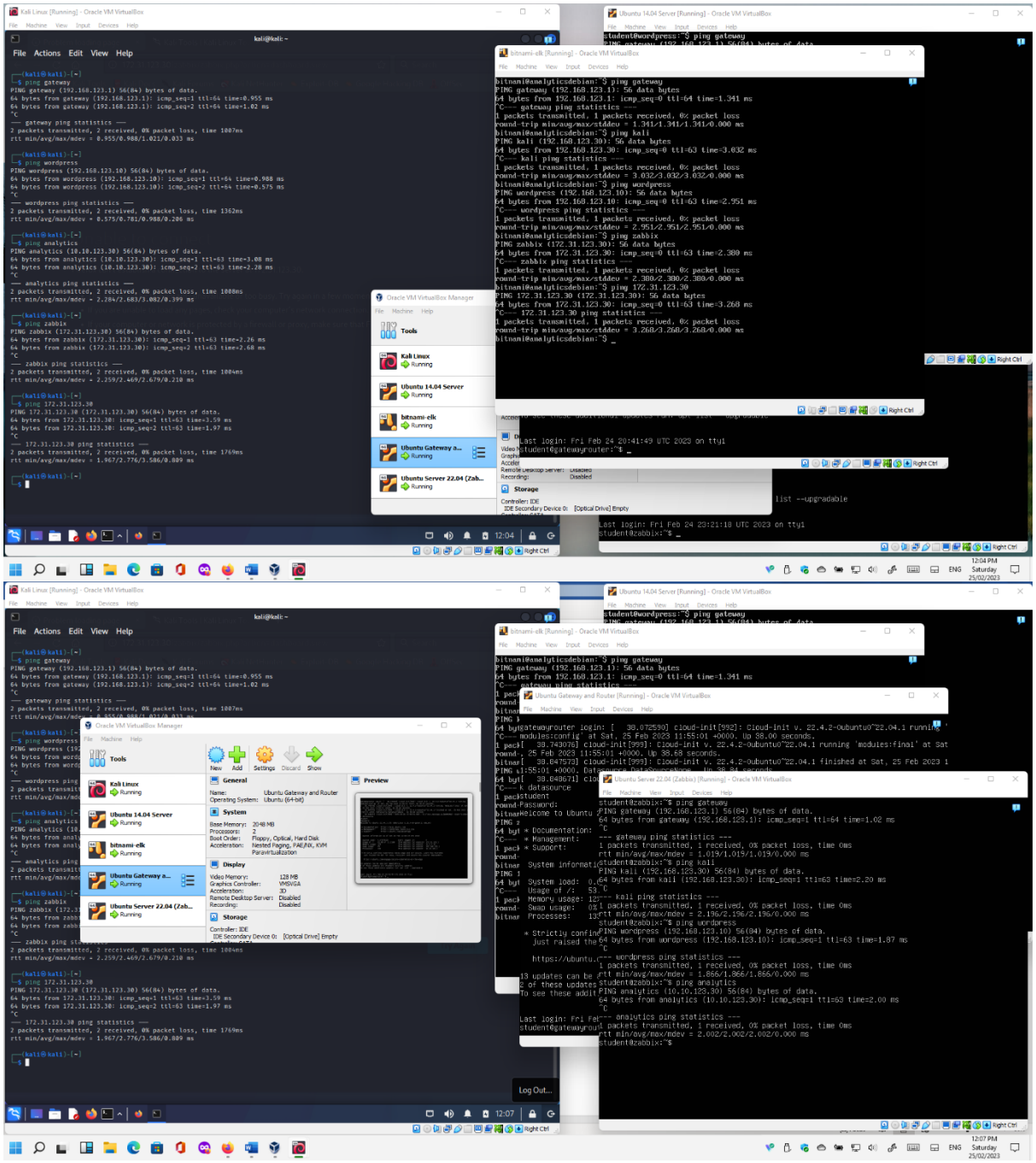
6. Repeat the steps in task 5 for the other virtual machines on your network.

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.

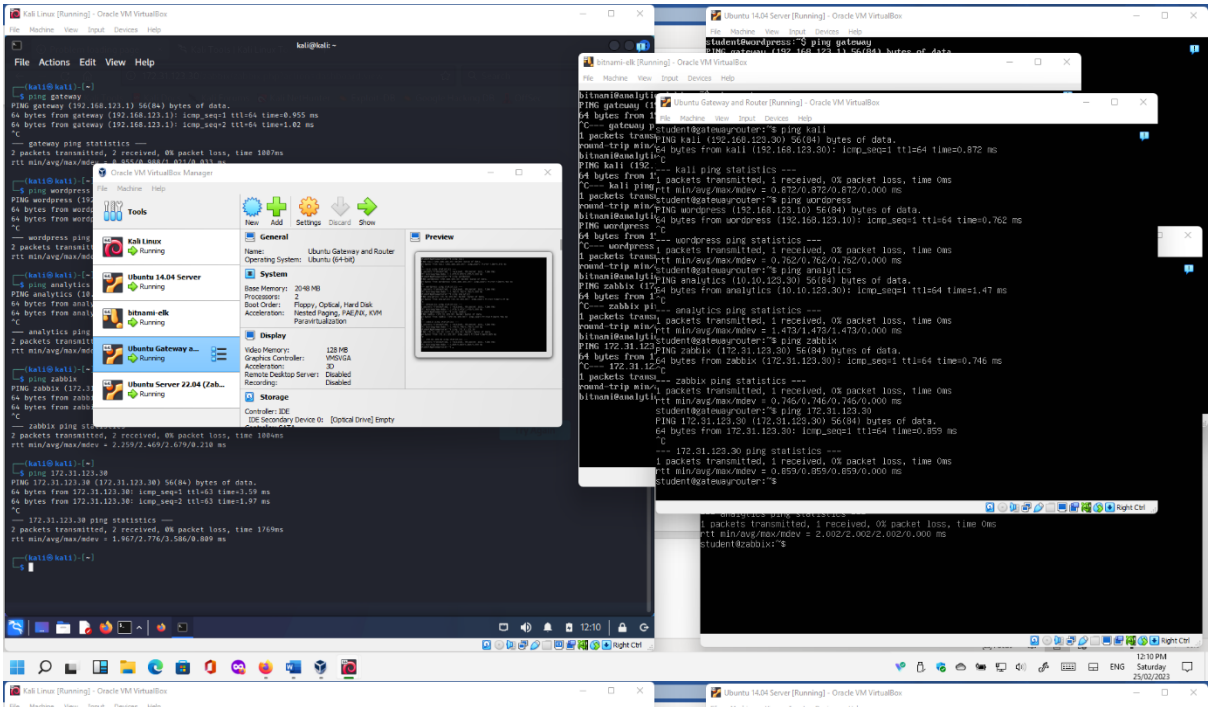
Requirement A: Demonstration Tasks

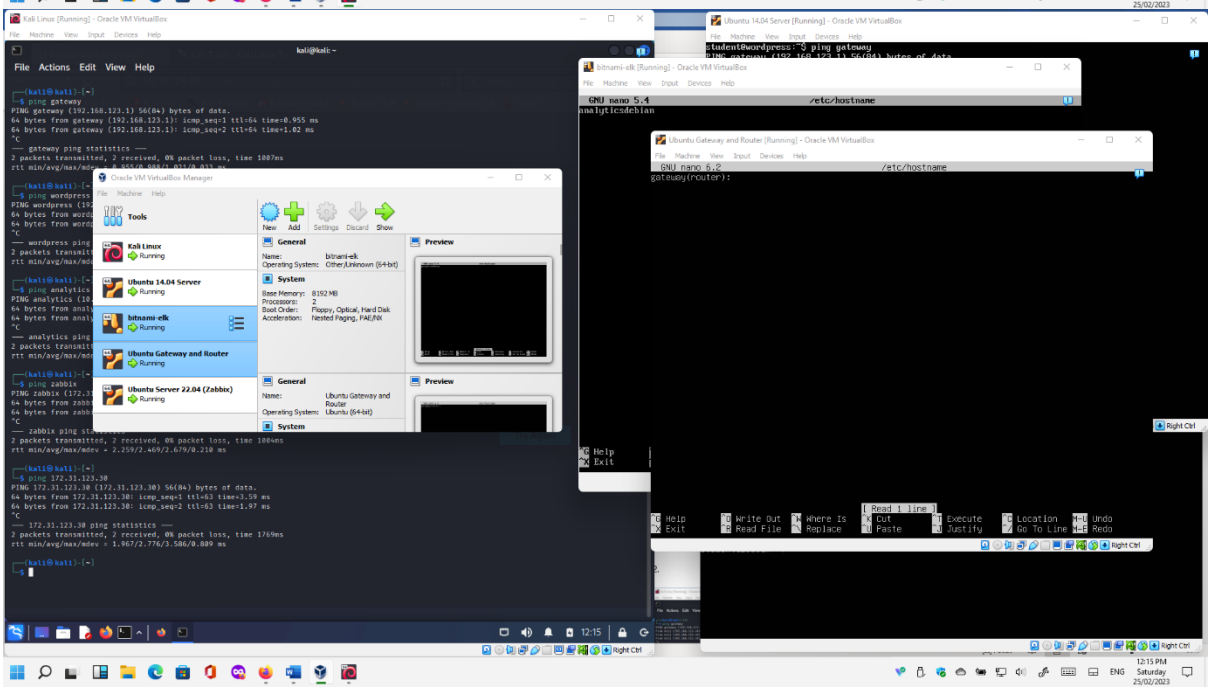
1. From the **gateway**, demonstrate that you can successfully ping the kali, wordpress, analytics and zabbix host names.
2. From the **kali**, demonstrate that you can successfully ping the gateway, wordpress, analytics and zabbix host names.
3. From the **wordpress**, demonstrate that you can successfully 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.

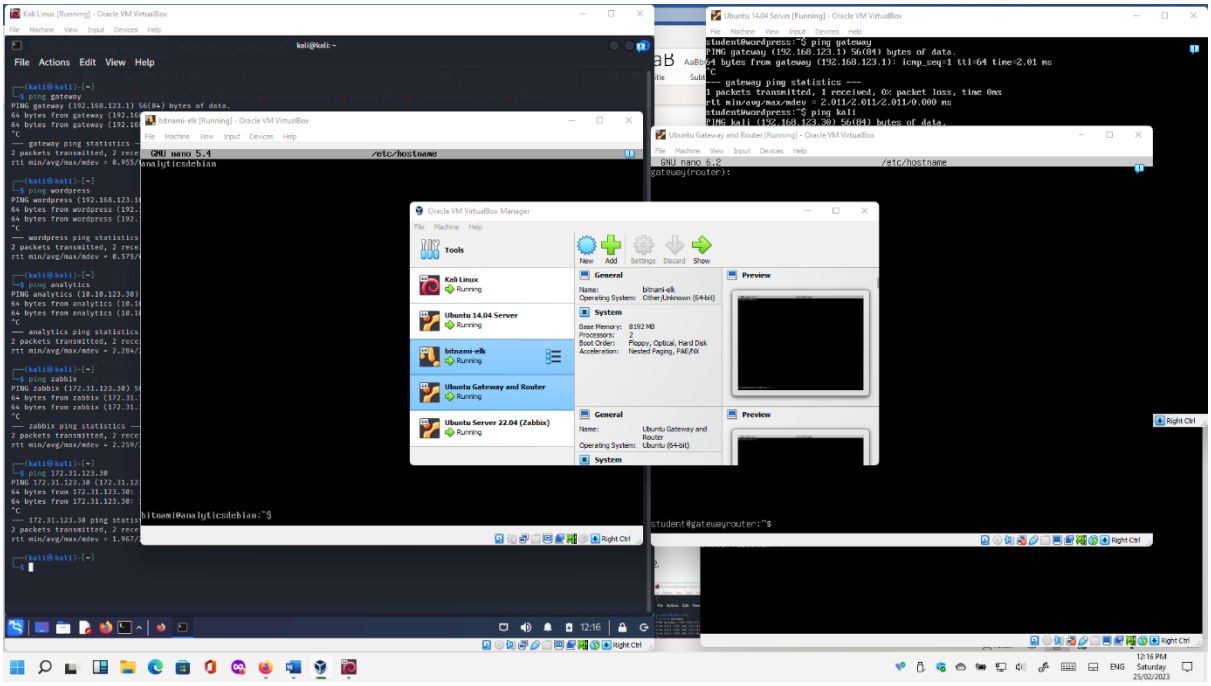



Kali Linux [Running] - Oracle VM VirtualBox
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
bitnami-elk [Running] - Oracle VM VirtualBox
Oracle VM VirtualBox Manager
Tools
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway a...
Running
Ubuntu Server 22.04 (Zab...
Running
File Actions Edit View Help
kali@kali: ~
Last login: Fri Feb 24 20:41:49 UTC 2023 on tty1
student@gatewayrouter:~$
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Last login: Fri Feb 24 23:21:18 UTC 2023 on tty1
student@zabbix:~$
12:04
ENG
Saturday
25/02/2023

Kali Linux [Running] - Oracle VM VirtualBox
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
bitnami-elk [Running] - Oracle VM VirtualBox
Ubuntu Gateway and Router [Running] - Oracle VM VirtualBox
Ubuntu Server 22.04 (Zabbix) [Running] - Oracle VM VirtualBox
Oracle VM VirtualBox Manager
Tools
New
Add
Settings
Discard
Show
General
Name: Ubuntu Gateway and Router
Operating System: Ubuntu (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM
Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Preview
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway a...
Running
Ubuntu Server 22.04 (Zab...
Running
Log Out...
12:07
ENG
Saturday
25/02/2023







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?

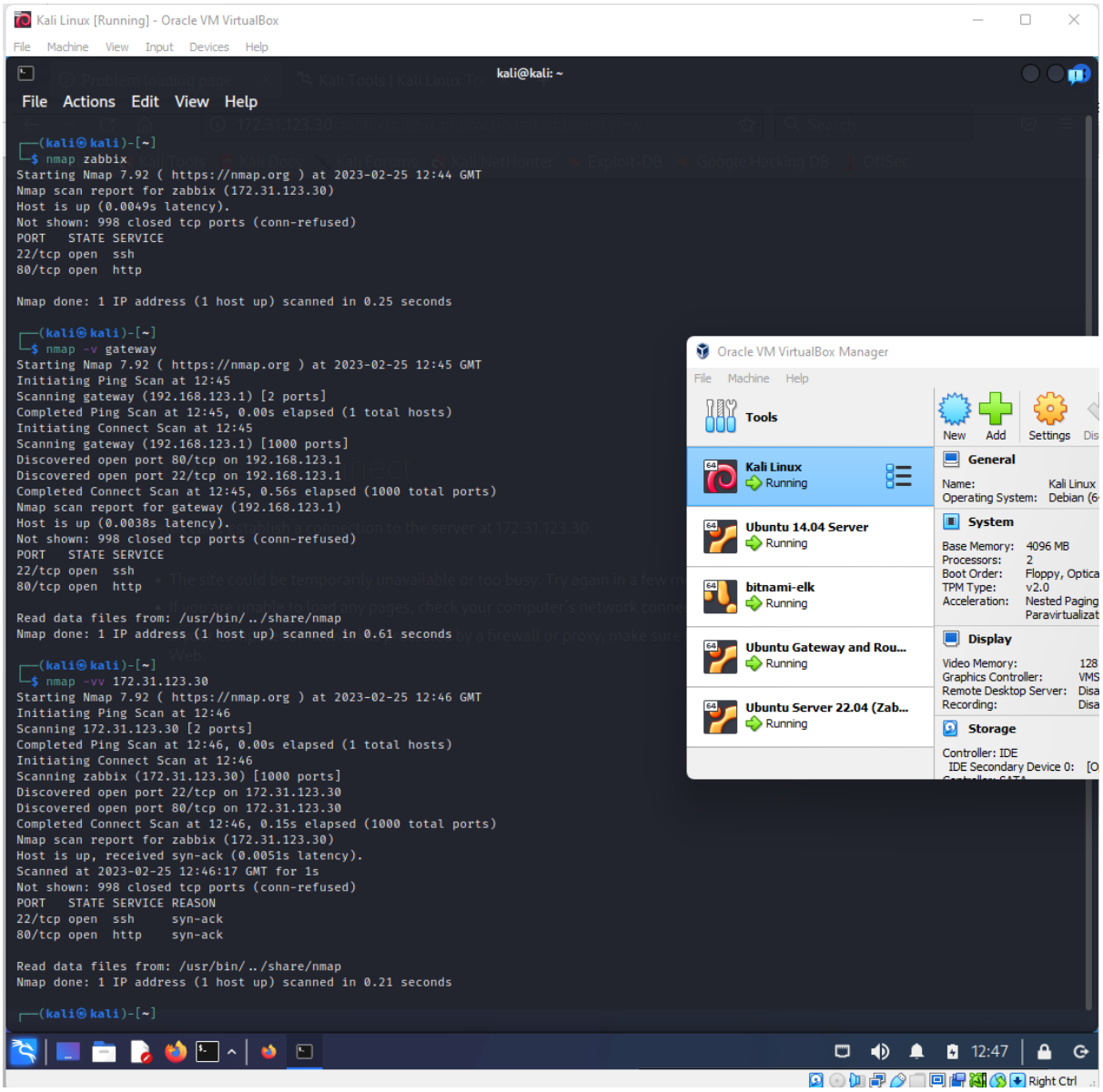
*"A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an 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
```

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

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

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

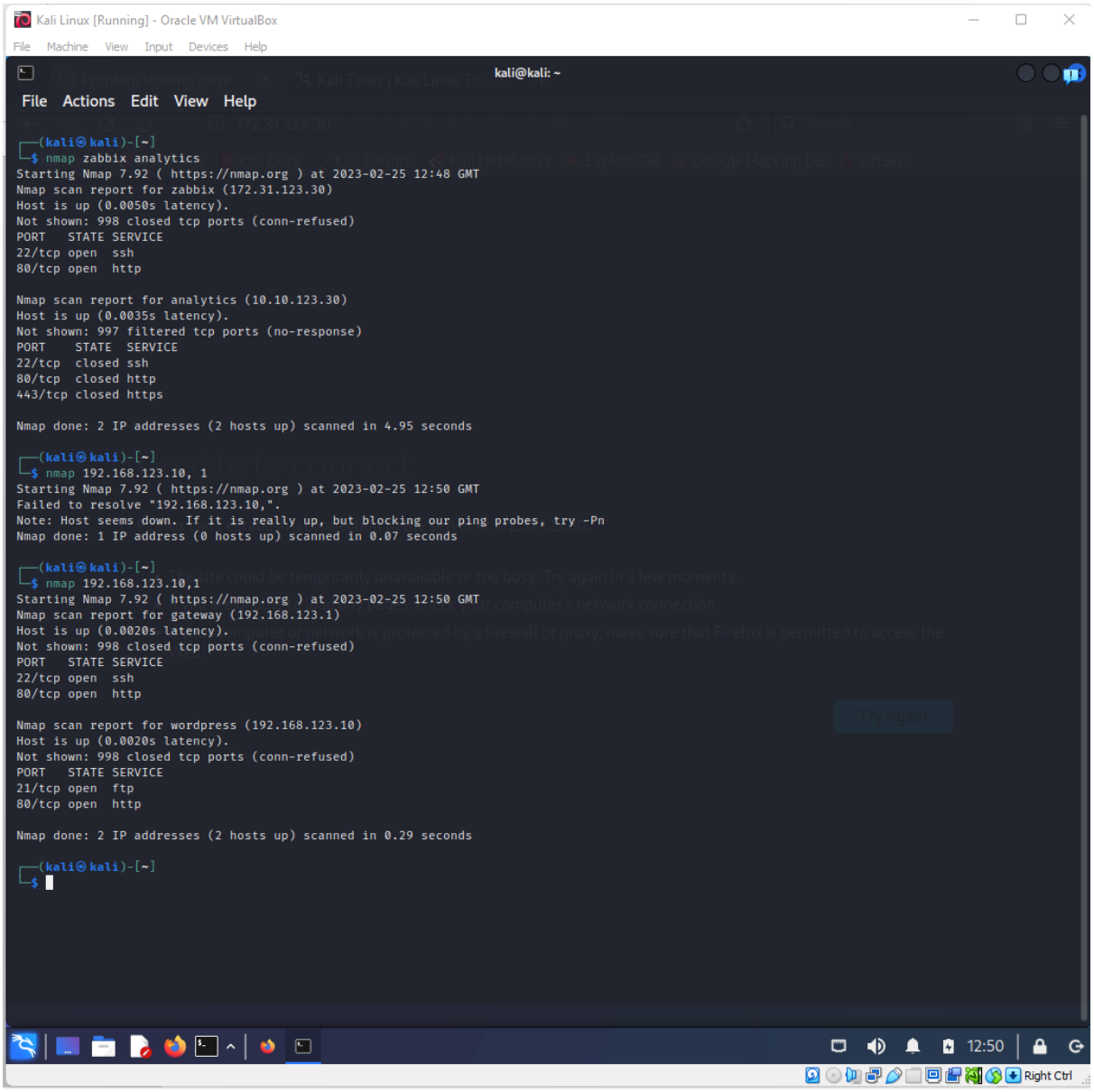
2. Scan Multiple IP Addresses

Scan **Multiple IP Addresses**:

```
$ nmap 192.168.123.1 192.168.1.2 192.168.123.3
```

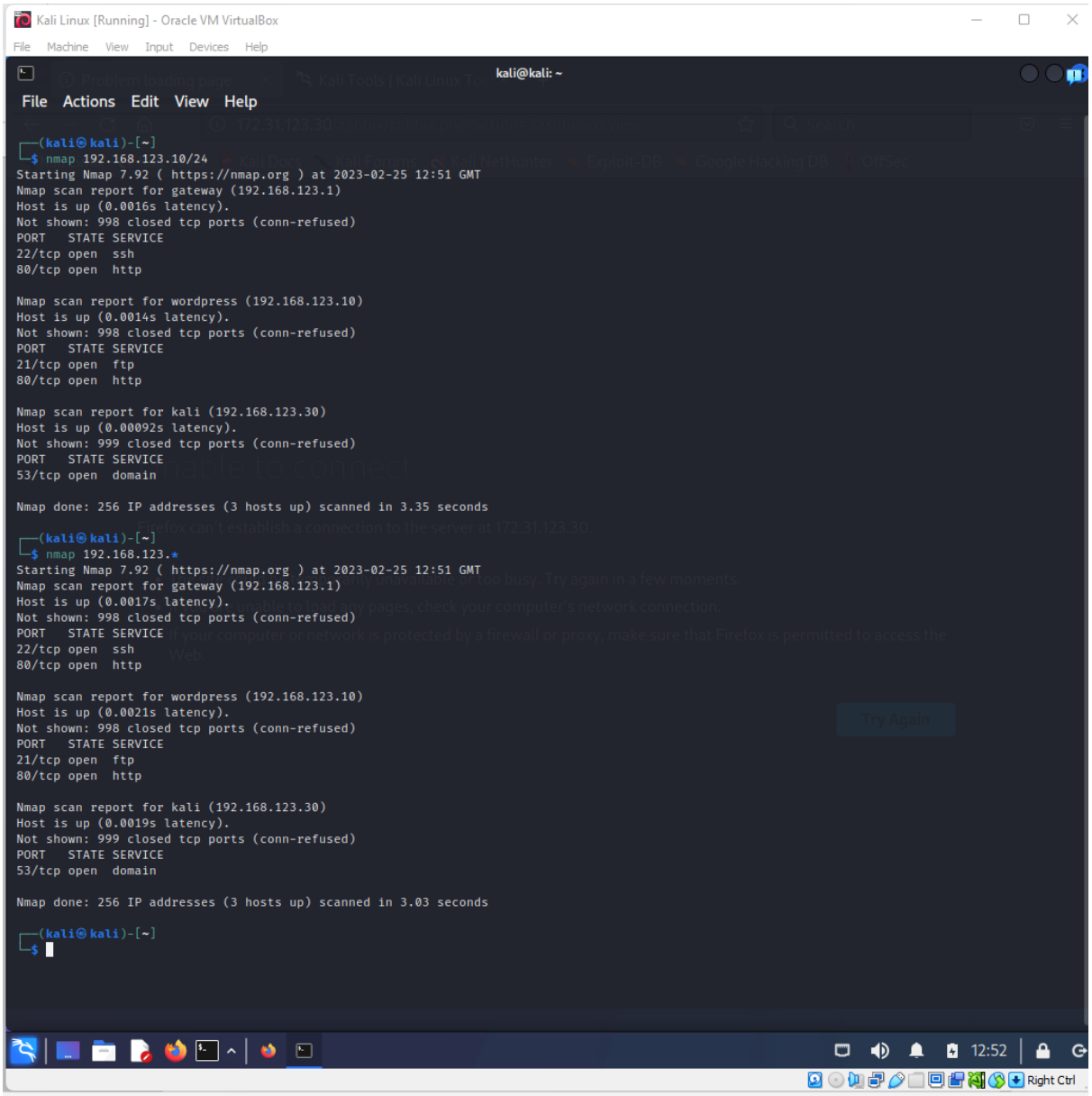
or

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

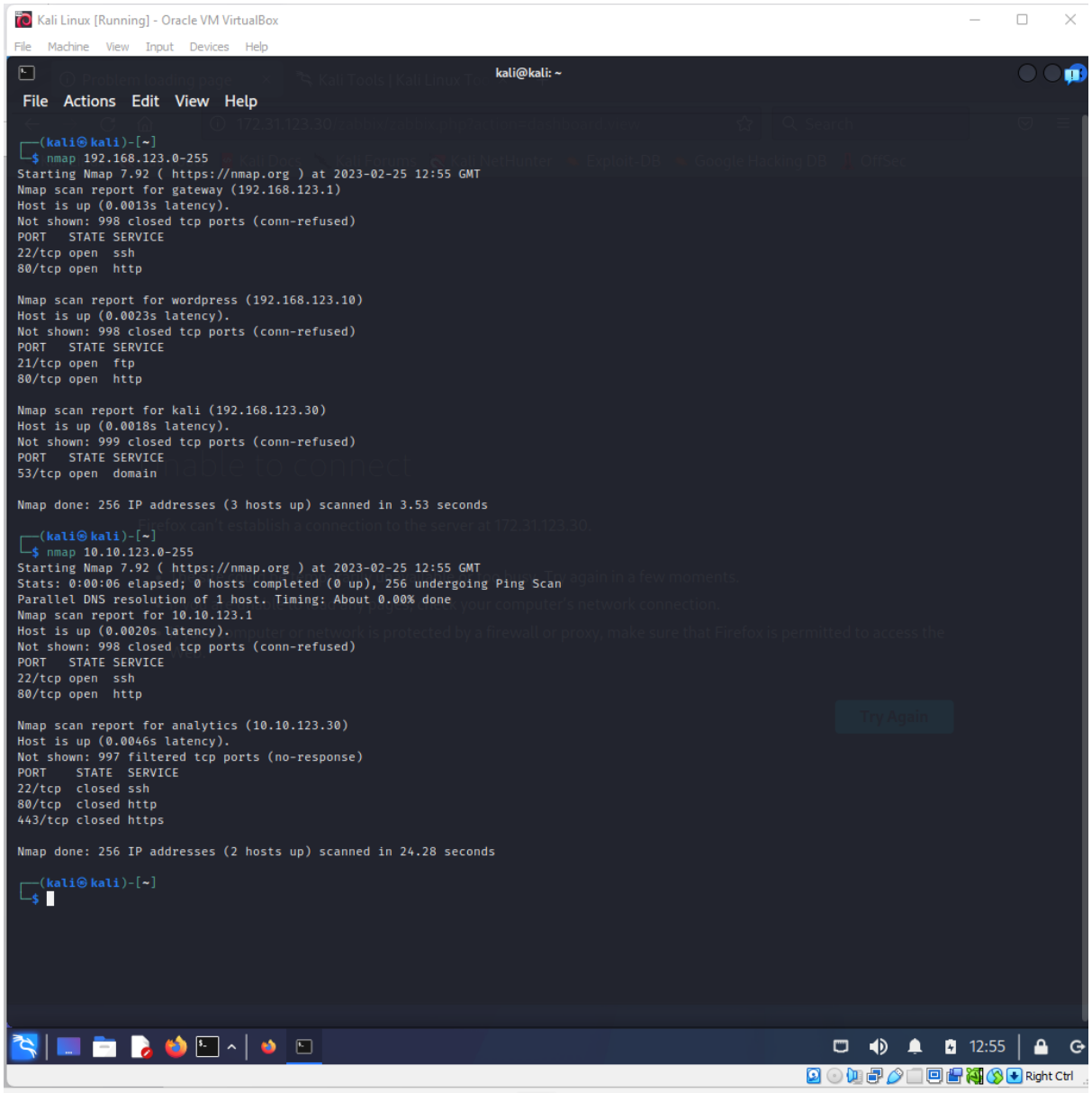


3. Scan a Subnet:

```
$ nmap 192.168.123.0/24
```

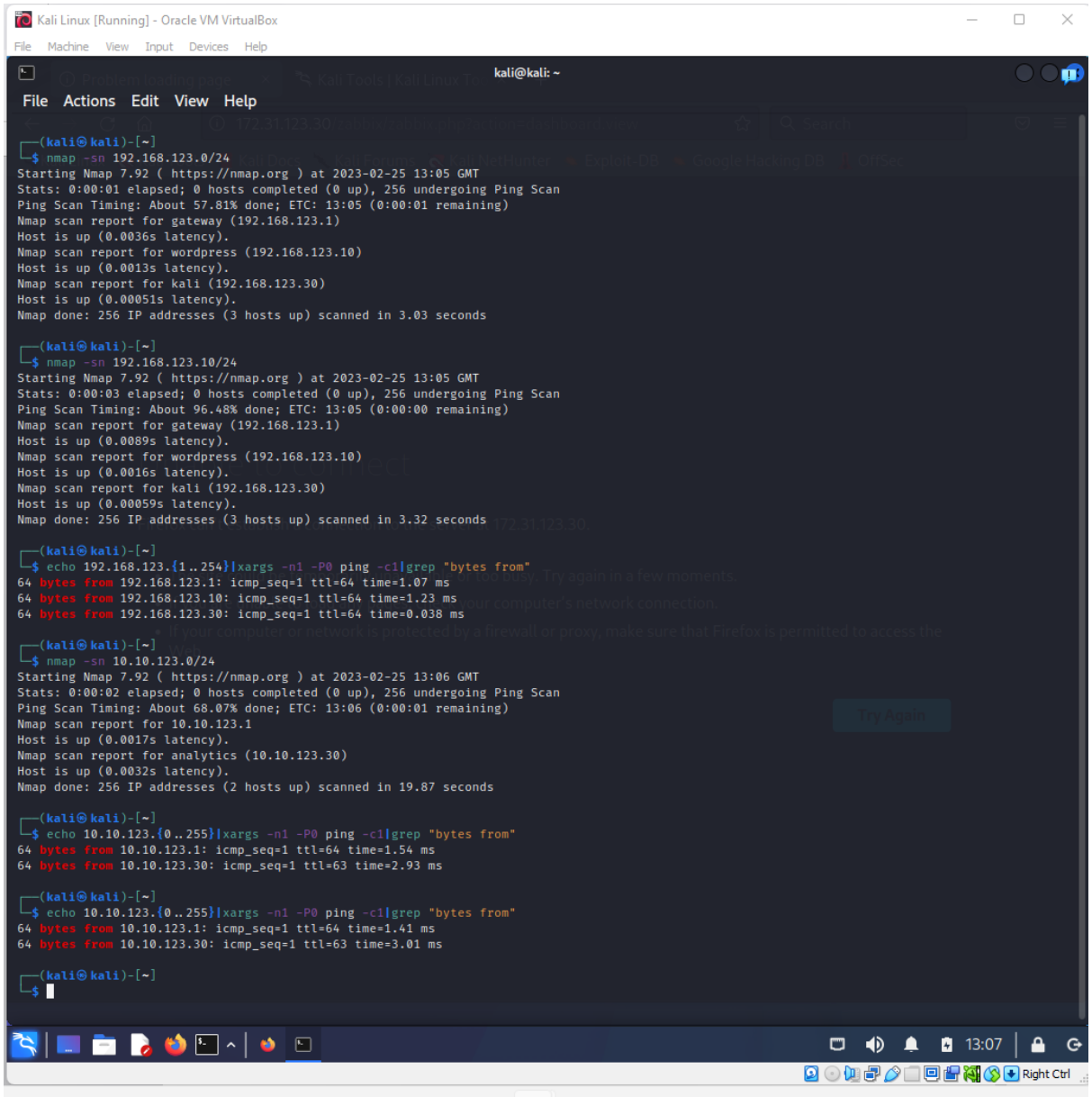



```
$ nmap 192.168.123.*
```



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

```
$ nmap 192.168.123.0-200
```

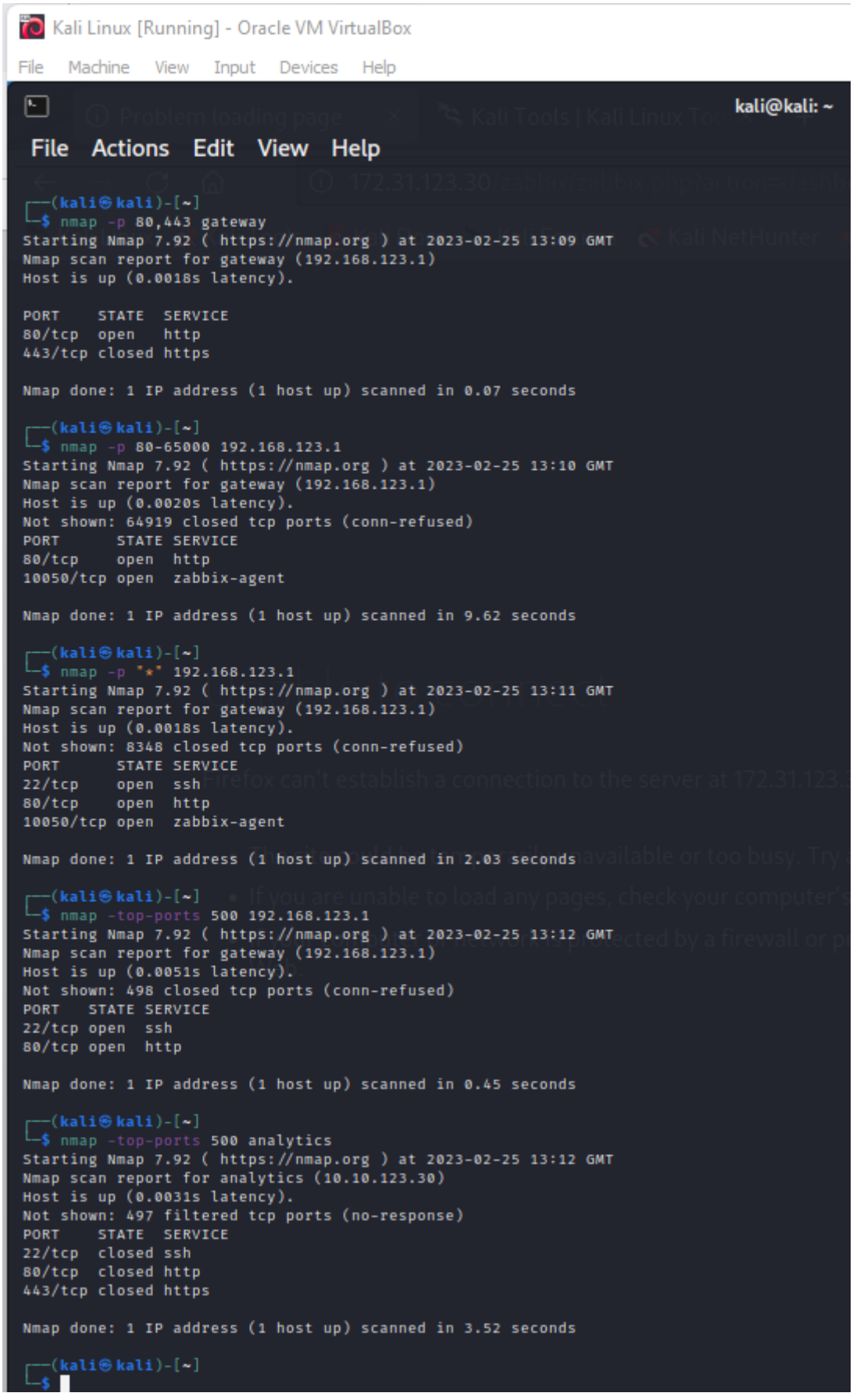


5. Scan a Network for Active Computers

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:

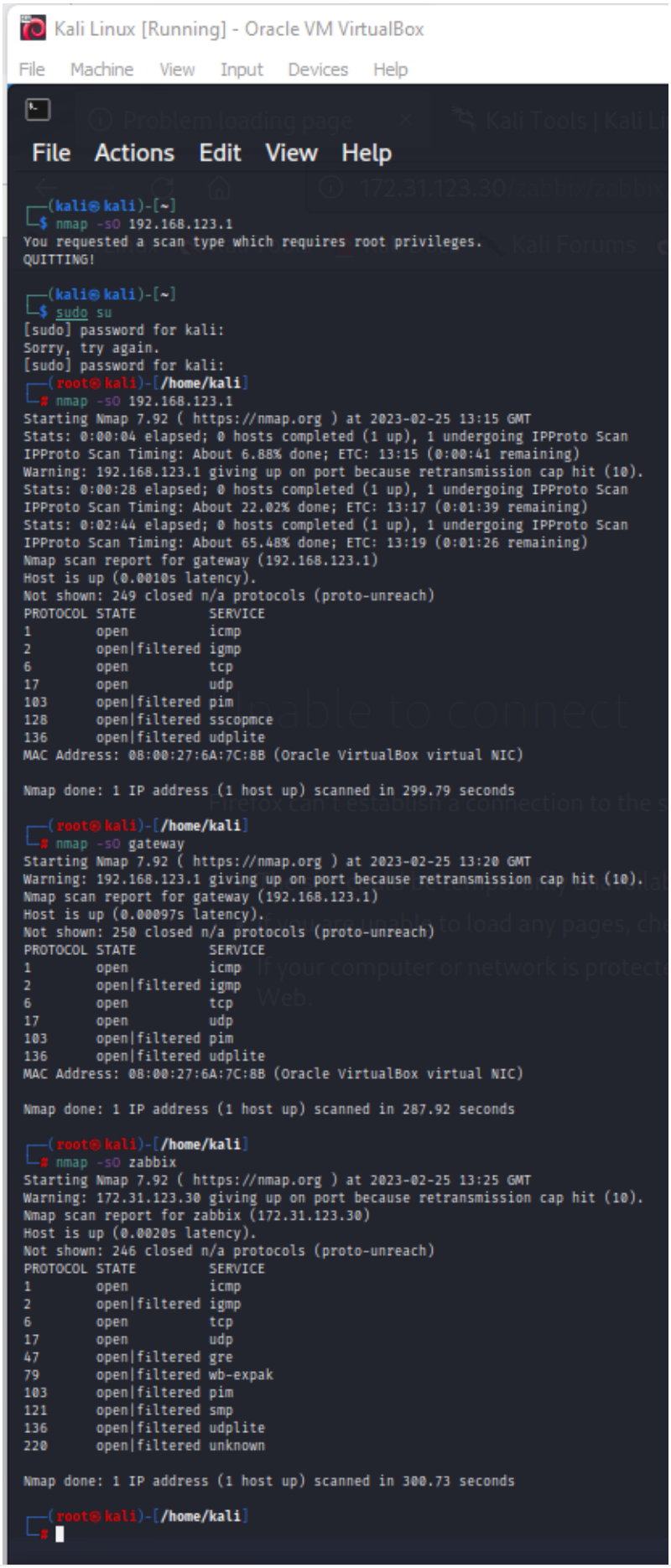
```
$ nmap -sn 192.168.123.0/24
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -p 80,443 gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:09 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0018s latency).
PORT STATE SERVICE
80/tcp open http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
(kali㉿kali)-[~]
$ nmap -p 80-65000 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:10 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0020s latency).
Not shown: 64919 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http
10050/tcp open zabbix-agent
Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds
(kali㉿kali)-[~]
$ nmap -p "*" 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:11 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0018s latency).
Not shown: 8348 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
10050/tcp open zabbix-agent
Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
(kali㉿kali)-[~]
$ nmap -top-ports 500 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:12 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0051s latency).
Not shown: 498 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
(kali㉿kali)-[~]
$ nmap -top-ports 500 analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:12 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0031s latency).
Not shown: 497 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 3.52 seconds
(kali㉿kali)-[~]
$

6. Scan For Specific Ports

Scan for a **Single Port**:

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


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sO 192.168.123.1
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sO 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:15 GMT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 6.88% done; ETC: 13:15 (0:00:41 remaining)
Warning: 192.168.123.1 giving up on port because retransmission cap hit (10).
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 22.02% done; ETC: 13:17 (0:01:39 remaining)
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 65.48% done; ETC: 13:19 (0:01:26 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0010s latency).
Not shown: 249 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
103 open|filtered pim
128 open|filtered sscopmce
136 open|filtered udplite
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 299.79 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sO gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:20 GMT
Warning: 192.168.123.1 giving up on port because retransmission cap hit (10).
Nmap scan report for gateway (192.168.123.1)
Host is up (0.00097s latency).
Not shown: 250 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
103 open|filtered pim
136 open|filtered udplite
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 287.92 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sO zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:25 GMT
Warning: 172.31.123.30 giving up on port because retransmission cap hit (10).
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0020s latency).
Not shown: 246 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
47 open|filtered gre
79 open|filtered wb-expak
103 open|filtered pim
121 open|filtered smp
136 open|filtered udplite
220 open|filtered unknown
Nmap done: 1 IP address (1 host up) scanned in 300.73 seconds
┌──(root㉿kali)-[/home/kali]
└─#

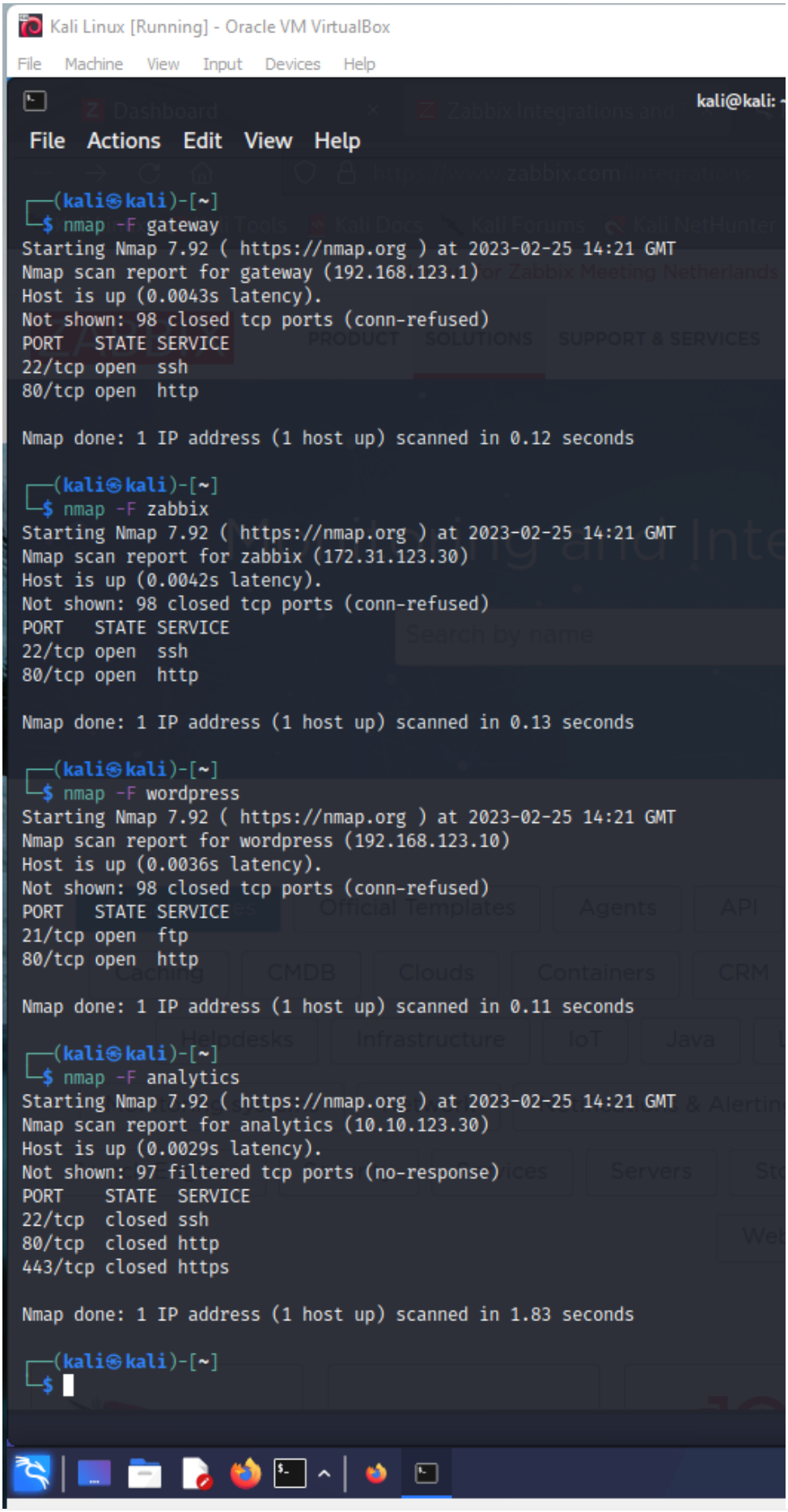
Scan for **Several Ports**:

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

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.123.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:57 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0039s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:66:0A:6D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p T:80 gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:57 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0020s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:57 GMT
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 2.04% done; ETC: 14:05 (0:07:59 remaining)
Stats: 0:10:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 57.64% done; ETC: 14:15 (0:07:23 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s latency).
All 1000 scanned ports on gateway (192.168.123.1) are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)
MAC Address: 08:00:27:C2:1A:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1087.05 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p U:53 gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:18 GMT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
WARNING: a TCP scan type was requested, but no tcp ports were specified.  Skipping this scan type.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0010s latency).
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p U:53,79,113,T:21-80,443,8080 zabbix
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:18 GMT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0069s latency).
Not shown: 60 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p U:53,79,113,T:21-80,443,8080 gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:18 GMT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0010s latency).
Not shown: 60 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

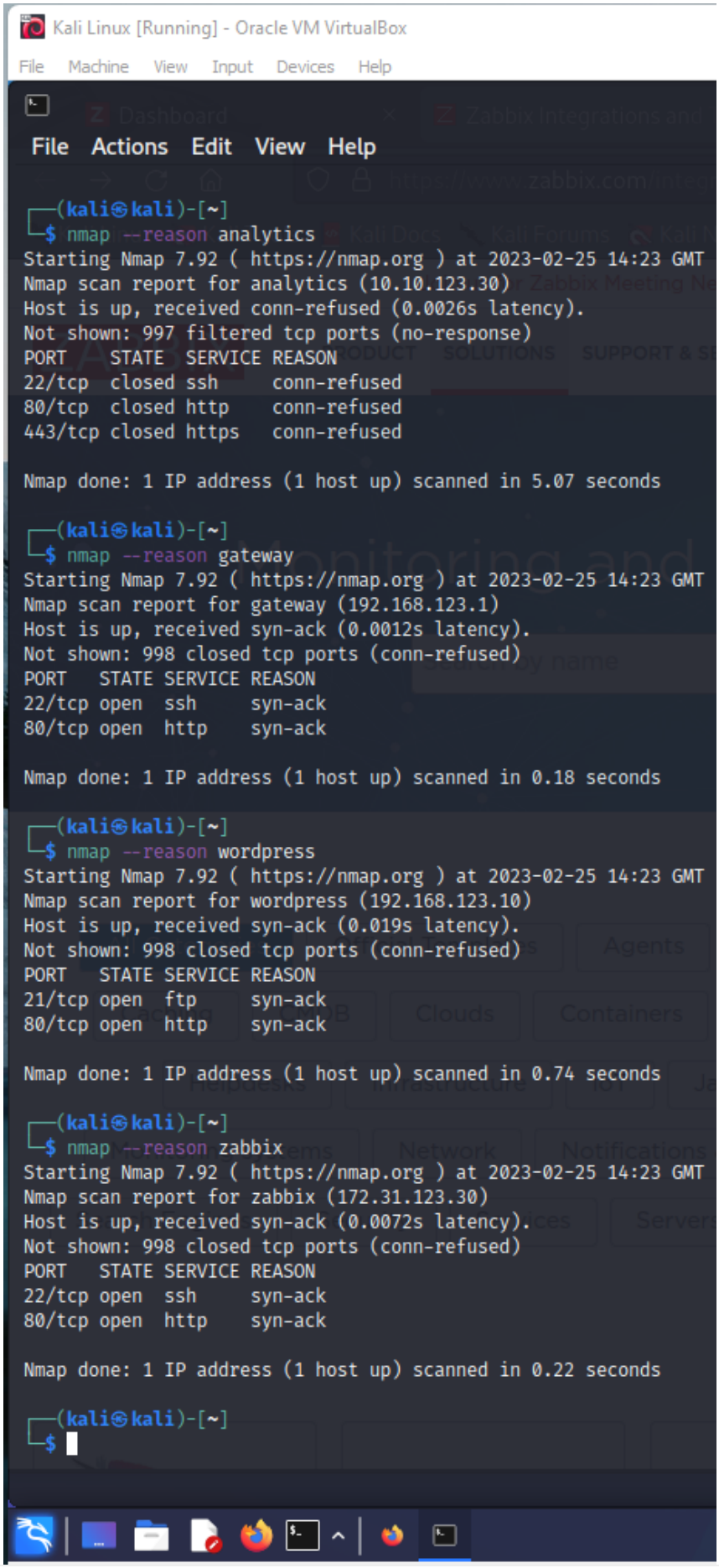
Scan for a **Port Range**:

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


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -F gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0043s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
(kali㉿kali)-[~]
$ nmap -F zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0042s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
(kali㉿kali)-[~]
$ nmap -F wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0036s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(kali㉿kali)-[~]
$ nmap -F analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0029s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
(kali㉿kali)-[~]
$

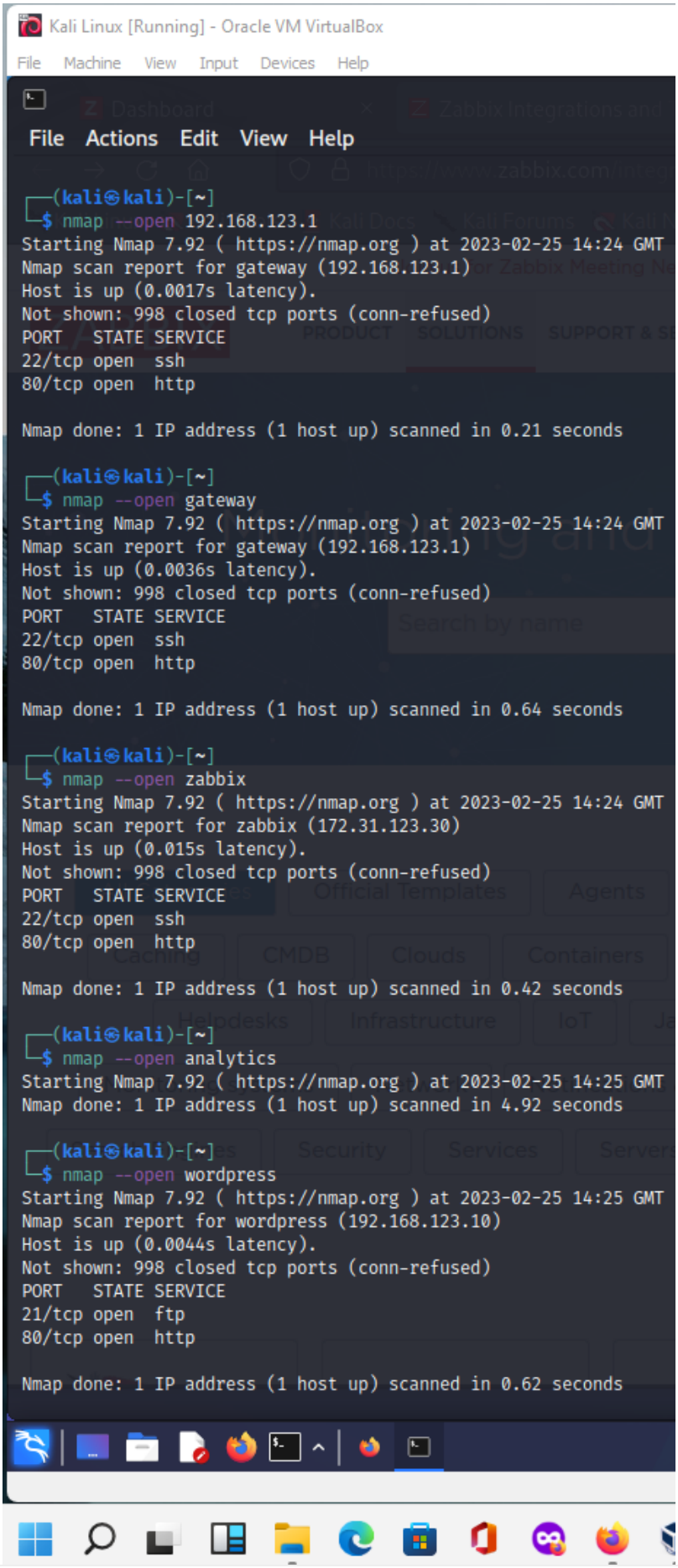
Scan for **All Ports**:

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

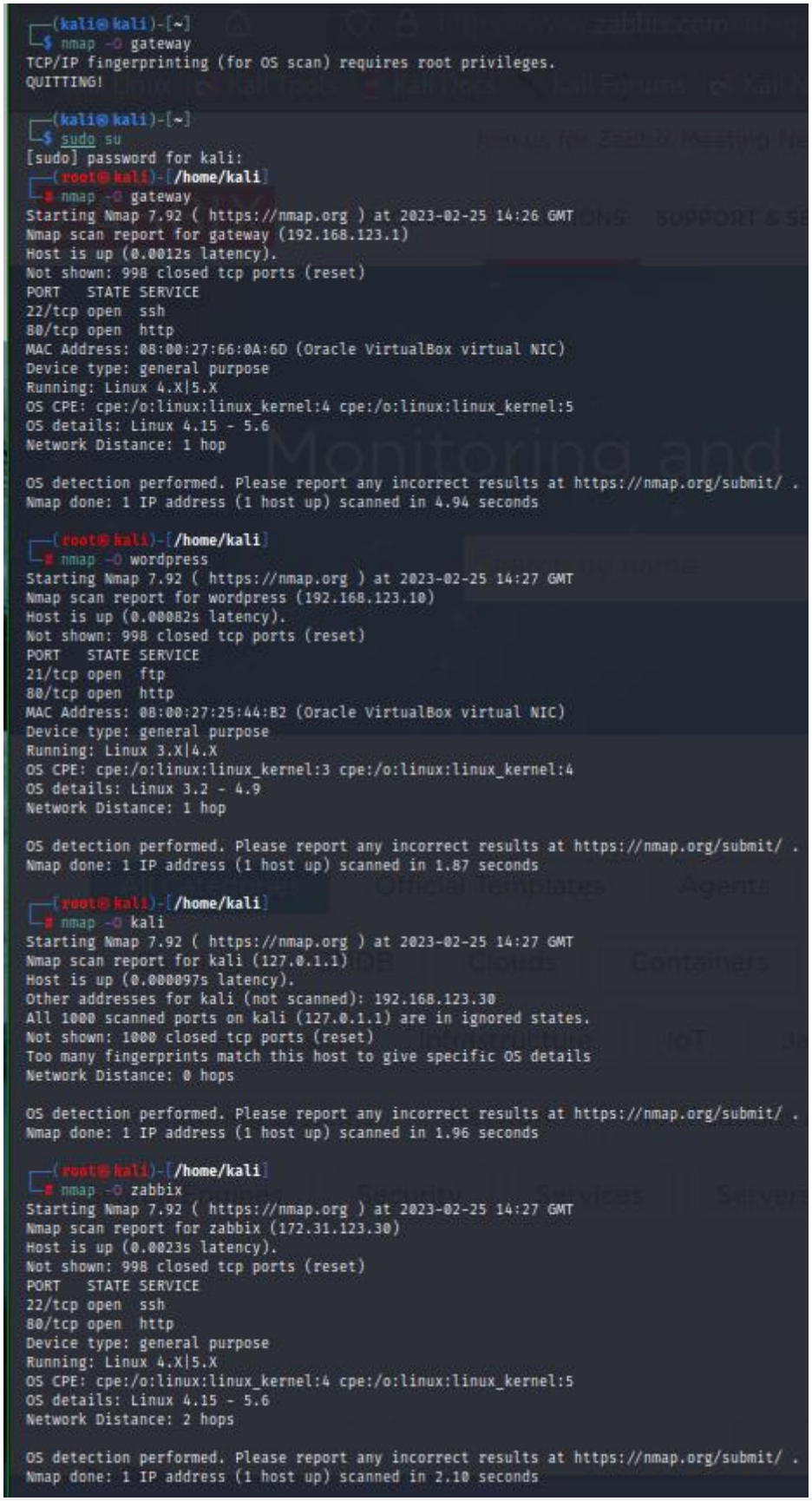

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap --reason analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up, received conn-refused (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE REASON
22/tcp closed ssh conn-refused
80/tcp closed http conn-refused
443/tcp closed https conn-refused
Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
(kali㉿kali)-[~]
$ nmap --reason gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up, received syn-ack (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
(kali㉿kali)-[~]
$ nmap --reason wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up, received syn-ack (0.019s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
80/tcp open http syn-ack
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
(kali㉿kali)-[~]
$ nmap --reason zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up, received syn-ack (0.0072s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
(kali㉿kali)-[~]
$

Scan for top most **Common Ports**:

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


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap --open 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:24 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0017s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:24 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0036s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:24 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.015s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:25 GMT
Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:25 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0044s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds

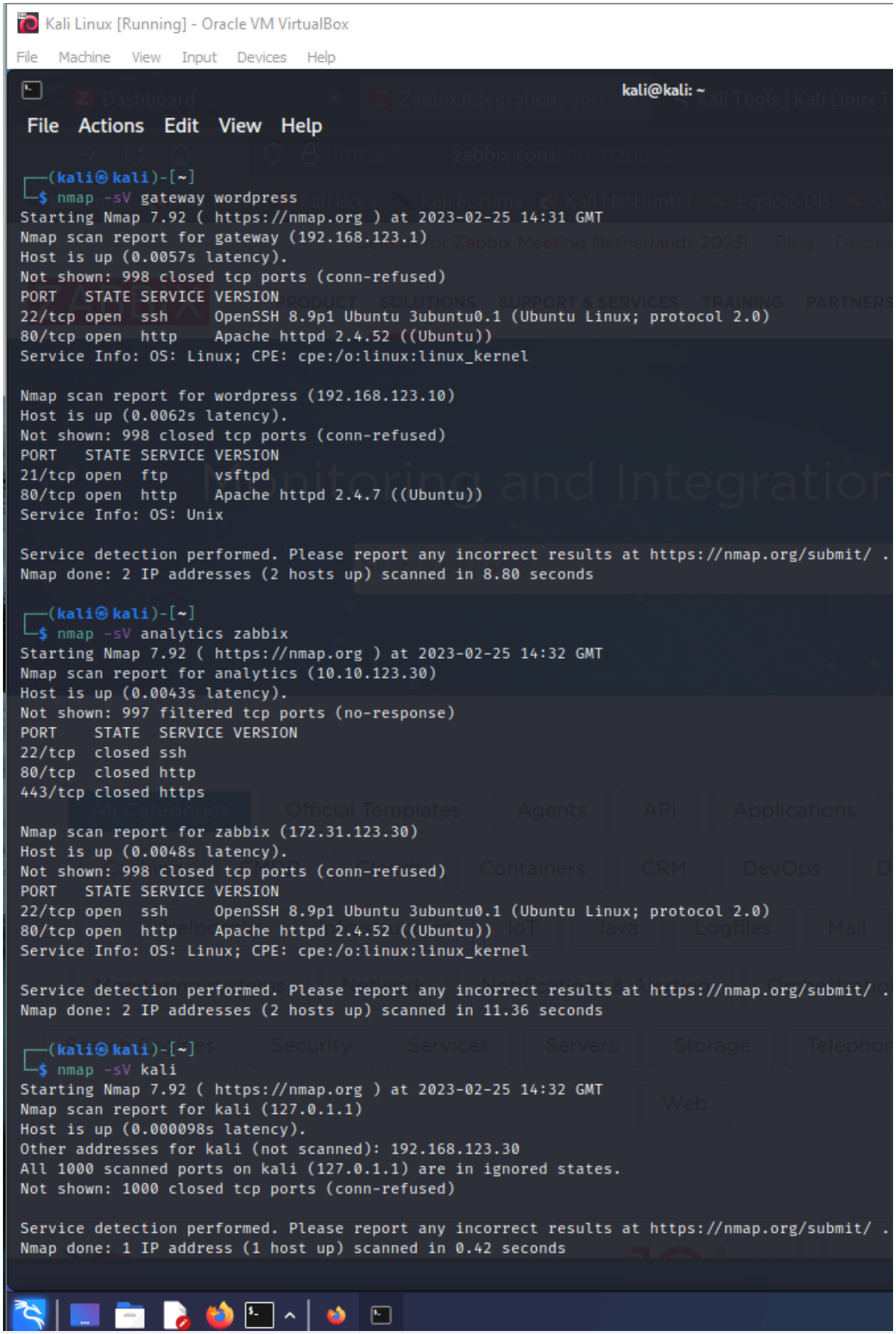
$ nmap --top-ports 10 192.168.123.1



7. Determine Supported IP Protocols

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

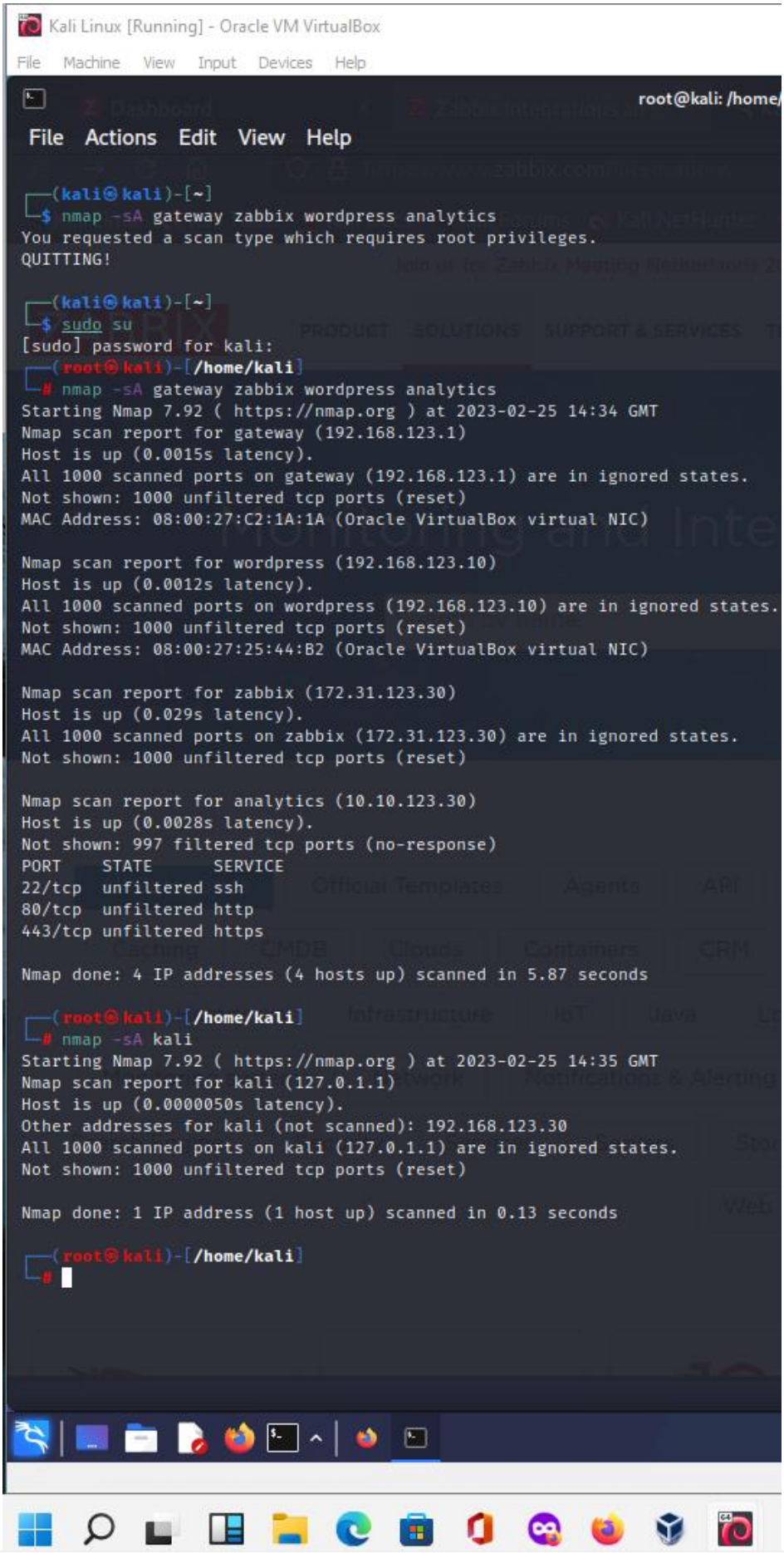
```
$ nmap -sO 192.168.123.1
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sV gateway wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:31 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0057s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0062s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 8.80 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sV analytics zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:32 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0043s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0048s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.52 ((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: 2 IP addresses (2 hosts up) scanned in 11.36 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sV kali
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:32 GMT
Nmap scan report for kali (127.0.1.1)
Host is up (0.000098s latency).
Other addresses for kali (not scanned): 192.168.123.30
All 1000 scanned ports on kali (127.0.1.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

8. Scan For TCP/UDP Ports

Scan for **All TCP Ports**:

```
$ nmap -sT 192.168.123.1
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sA gateway zabbix wordpress analytics
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA gateway zabbix wordpress analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:34 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0015s latency).
All 1000 scanned ports on gateway (192.168.123.1) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:C2:1A:1A (Oracle VirtualBox virtual NIC)
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0012s latency).
All 1000 scanned ports on wordpress (192.168.123.10) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:25:44:B2 (Oracle VirtualBox virtual NIC)
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.029s latency).
All 1000 scanned ports on zabbix (172.31.123.30) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp unfiltered ssh
80/tcp unfiltered http
443/tcp unfiltered https
Nmap done: 4 IP addresses (4 hosts up) scanned in 5.87 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA kali
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:35 GMT
Nmap scan report for kali (127.0.1.1)
Host is up (0.0000050s latency).
Other addresses for kali (not scanned): 192.168.123.30
All 1000 scanned ports on kali (127.0.1.1) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
┌──(root㉿kali)-[/home/kali]
└─#

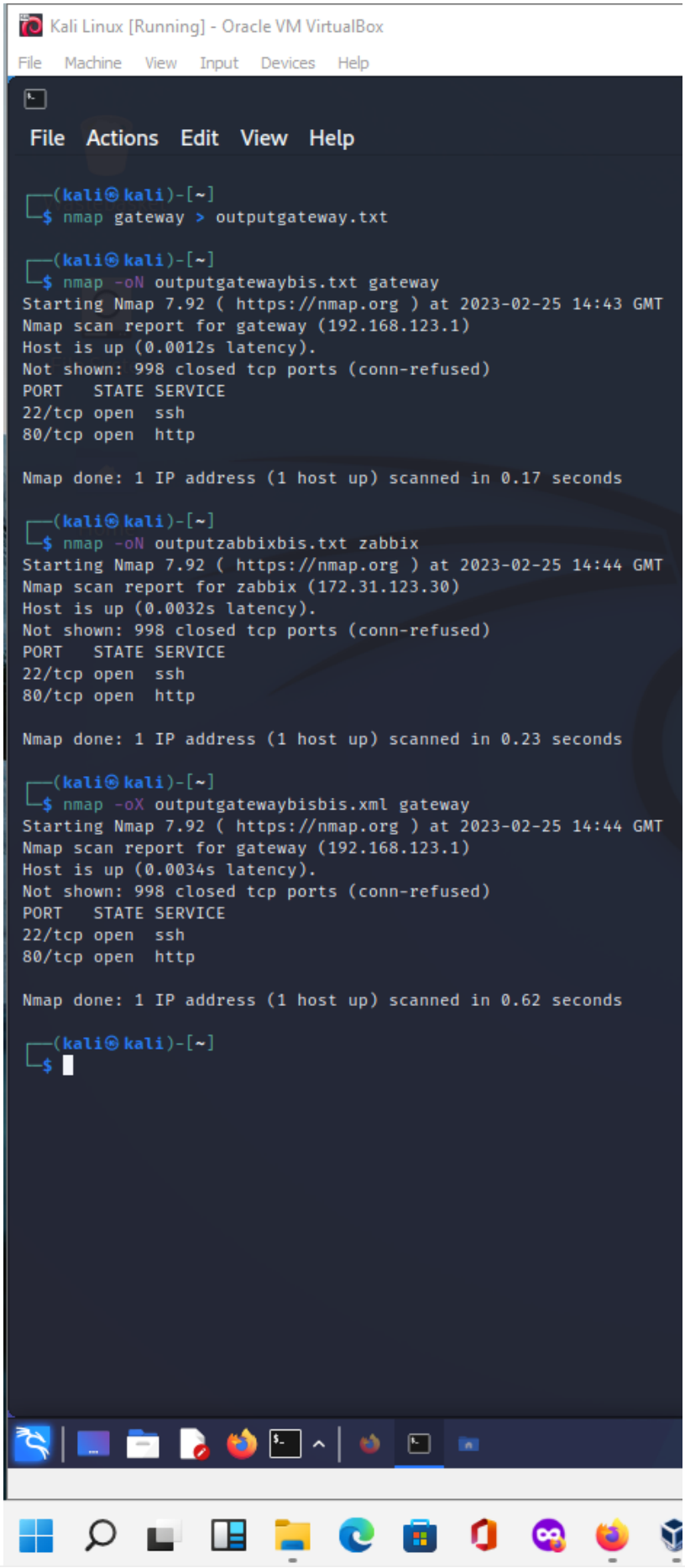
Scan for **Particular TCP Ports**:

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


root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:36 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
MAC Address: 08:00:27:66:0A:6D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS analytics zabbix wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:36 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0034s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.027s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
MAC Address: 08:00:27:25:44:B2 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (3 hosts up) scanned in 6.27 seconds
┌──(root㉿kali)-[/home/kali]
└─# tor-resolve google.com
Command 'tor-resolve' not found, but can be installed with:
apt install tor
Do you want to install it? (N/y)y
apt install tor
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Some packages could not be installed. This may mean that you have
requested an impossible situation or if you are using the unstable
distribution that some required packages have not yet been created
or been moved out of Incoming.
The following information may help to resolve the situation:
The following packages have unmet dependencies:
libc6-dev : Breaks: binutils (< 2.38) but 2.37-10.1 is to be installed
E: Error, pkgProblemResolver::Resolve generated breaks, this may be caused by held packages.
┌──(root㉿kali)-[/home/kali]
└─# tor-resolve google.com
Command 'tor-resolve' not found, but can be installed with:
apt install tor
Do you want to install it? (N/y)y
apt install tor
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Some packages could not be installed. This may mean that you have

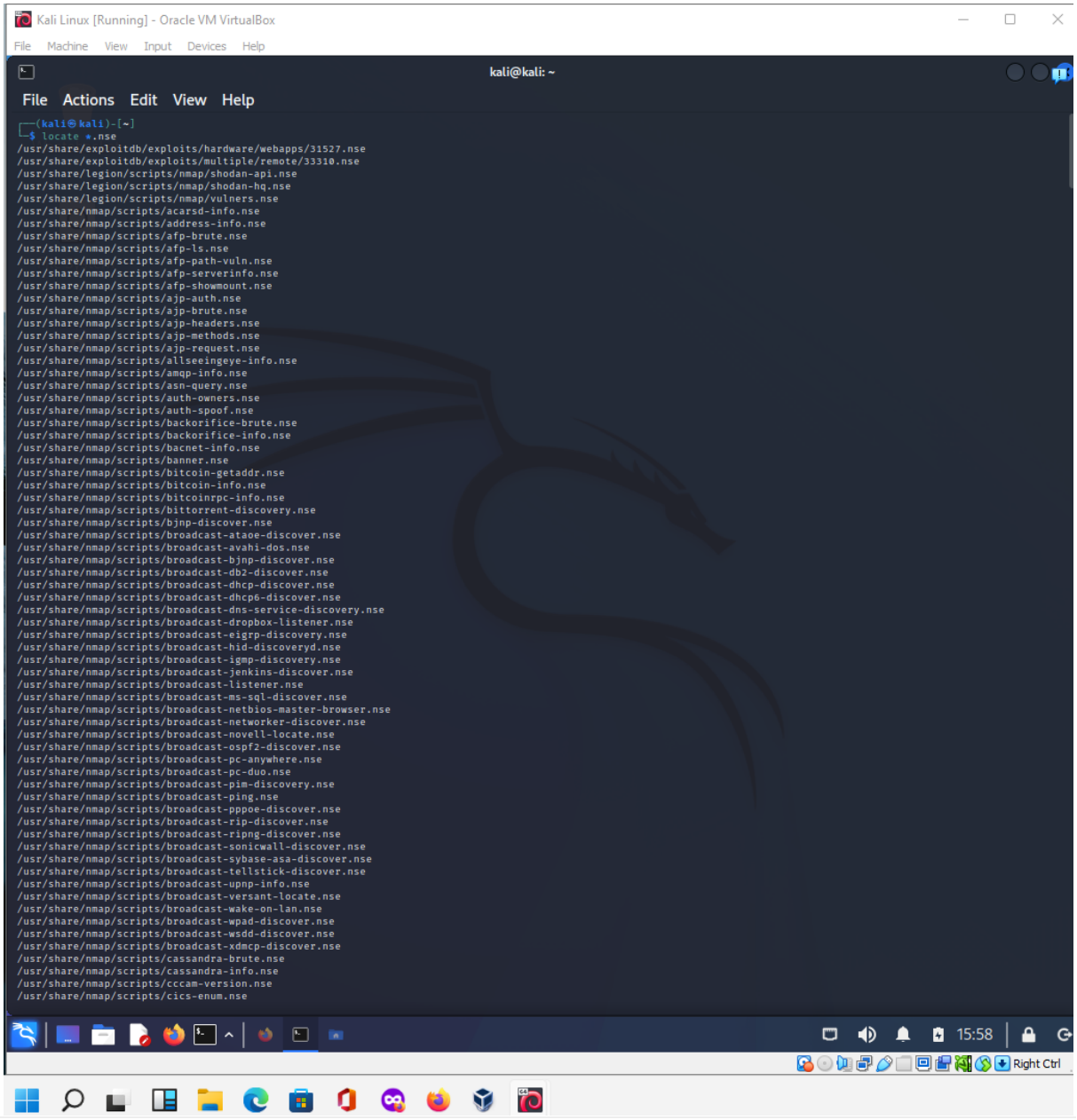
Scan for **All UDP Ports**:

```
$ nmap -sU 192.168.123.1
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap gateway > outputgateway.txt
┌──(kali㉿kali)-[~]
└─$ nmap -oN outputgatewaybis.txt gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:43 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -oN outputzabbixbis.txt zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:44 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0032s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -oX outputgatewaybisbis.xml gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:44 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0034s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
┌──(kali㉿kali)-[~]
└─$

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
```

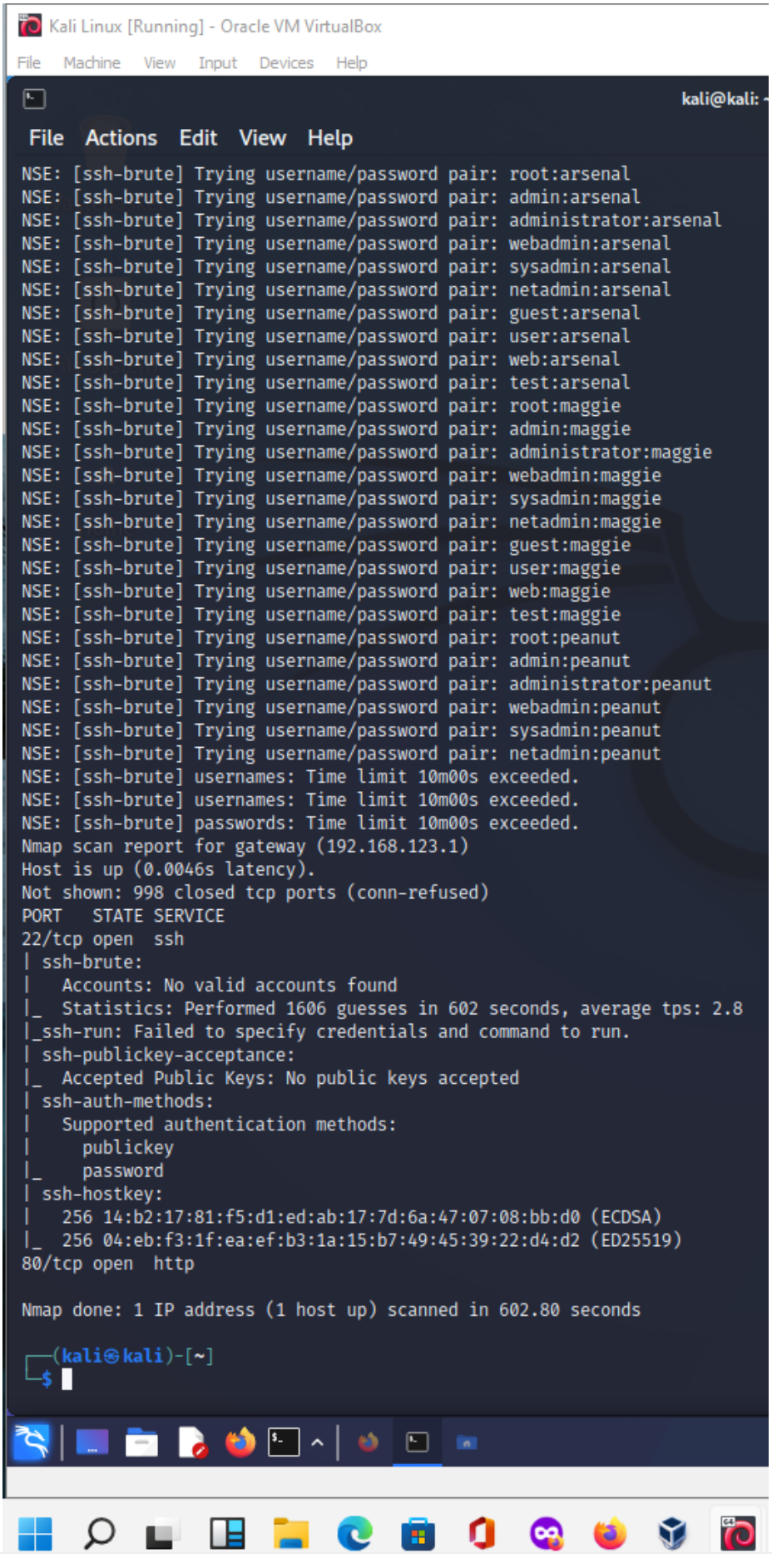

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sC gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 15:59 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
| ssh-hostkey:
| 256 14:b2:17:81:f5:d1:ed:ab:17:7d:6a:47:07:08:bb:d0 (ECDSA)
|_ 256 04:eb:f3:1f:ea:ef:b3:1a:15:b7:49:45:39:22:d4:d2 (ED25519)
80/tcp open http
|_http-title: Apache2 Ubuntu Default Page: It works
Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --script http-headers gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 16:00 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0014s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
| http-headers:
| Date: Sat, 25 Feb 2023 16:00:37 GMT
| Server: Apache/2.4.52 (Ubuntu)
| Last-Modified: Fri, 24 Feb 2023 14:35:39 GMT
| ETag: "29af-5f5730b170d83"
| Accept-Ranges: bytes
| Content-Length: 10671
| Vary: Accept-Encoding
| Connection: close
| Content-Type: text/html
|
|_ (Request type: HEAD)
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --script "ssh-*" gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 16:01 GMT
NSE: [ssh-run] Failed to specify credentials and command to run.
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user

9. Perform a Fast Scan

Enable **Fast Mode**:

```
$ nmap -F 192.168.123.1
```

* *Scan fewer ports than the default scan.*


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:
File Actions Edit View Help
NSE: [ssh-brute] Trying username/password pair: root:arsenal
NSE: [ssh-brute] Trying username/password pair: admin:arsenal
NSE: [ssh-brute] Trying username/password pair: administrator:arsenal
NSE: [ssh-brute] Trying username/password pair: webadmin:arsenal
NSE: [ssh-brute] Trying username/password pair: sysadmin:arsenal
NSE: [ssh-brute] Trying username/password pair: netadmin:arsenal
NSE: [ssh-brute] Trying username/password pair: guest:arsenal
NSE: [ssh-brute] Trying username/password pair: user:arsenal
NSE: [ssh-brute] Trying username/password pair: web:arsenal
NSE: [ssh-brute] Trying username/password pair: test:arsenal
NSE: [ssh-brute] Trying username/password pair: root:maggie
NSE: [ssh-brute] Trying username/password pair: admin:maggie
NSE: [ssh-brute] Trying username/password pair: administrator:maggie
NSE: [ssh-brute] Trying username/password pair: webadmin:maggie
NSE: [ssh-brute] Trying username/password pair: sysadmin:maggie
NSE: [ssh-brute] Trying username/password pair: netadmin:maggie
NSE: [ssh-brute] Trying username/password pair: guest:maggie
NSE: [ssh-brute] Trying username/password pair: user:maggie
NSE: [ssh-brute] Trying username/password pair: web:maggie
NSE: [ssh-brute] Trying username/password pair: test:maggie
NSE: [ssh-brute] Trying username/password pair: root:peanut
NSE: [ssh-brute] Trying username/password pair: admin:peanut
NSE: [ssh-brute] Trying username/password pair: administrator:peanut
NSE: [ssh-brute] Trying username/password pair: webadmin:peanut
NSE: [ssh-brute] Trying username/password pair: sysadmin:peanut
NSE: [ssh-brute] Trying username/password pair: netadmin:peanut
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0046s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
| ssh-brute:
| Accounts: No valid accounts found
|_ Statistics: Performed 1606 guesses in 602 seconds, average tps: 2.8
|_ssh-run: Failed to specify credentials and command to run.
| ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
| ssh-hostkey:
| 256 14:b2:17:81:f5:d1:ed:ab:17:7d:6a:47:07:08:bb:d0 (ECDSA)
|_ 256 04:eb:f3:1f:ea:ef:b3:1a:15:b7:49:45:39:22:d4:d2 (ED25519)
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 602.80 seconds
(kali㉿kali)-[~]
$

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**:

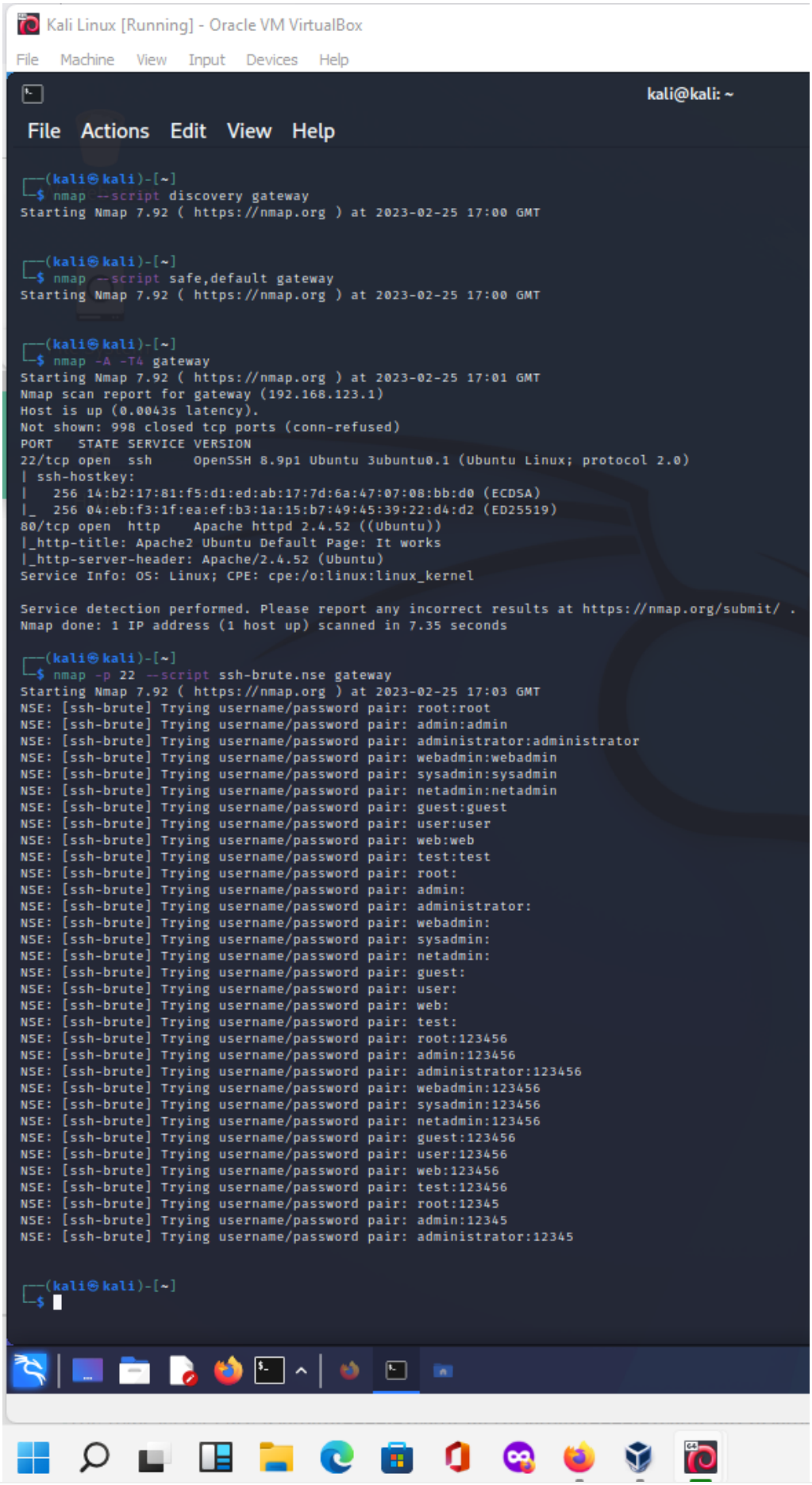
```
$ nmap -sV 192.168.123.1
```

* *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
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap --script discovery gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:00 GMT
┌──(kali㉿kali)-[~]
└─$ nmap --script safe,default gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:00 GMT
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:01 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0043s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 14:b2:17:81:f5:d1:ed:ab:17:7d:6a:47:07:08:bb:d0 (ECDSA)
|_ 256 04:eb:f3:1f:ea:ef:b3:1a:15:b7:49:45:39:22:d4:d2 (ED25519)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (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 7.35 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-brute.nse gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:03 GMT
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: user:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: user:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: root:12345
NSE: [ssh-brute] Trying username/password pair: admin:12345
NSE: [ssh-brute] Trying username/password pair: administrator:12345
┌──(kali㉿kali)-[~]
└─$

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
```

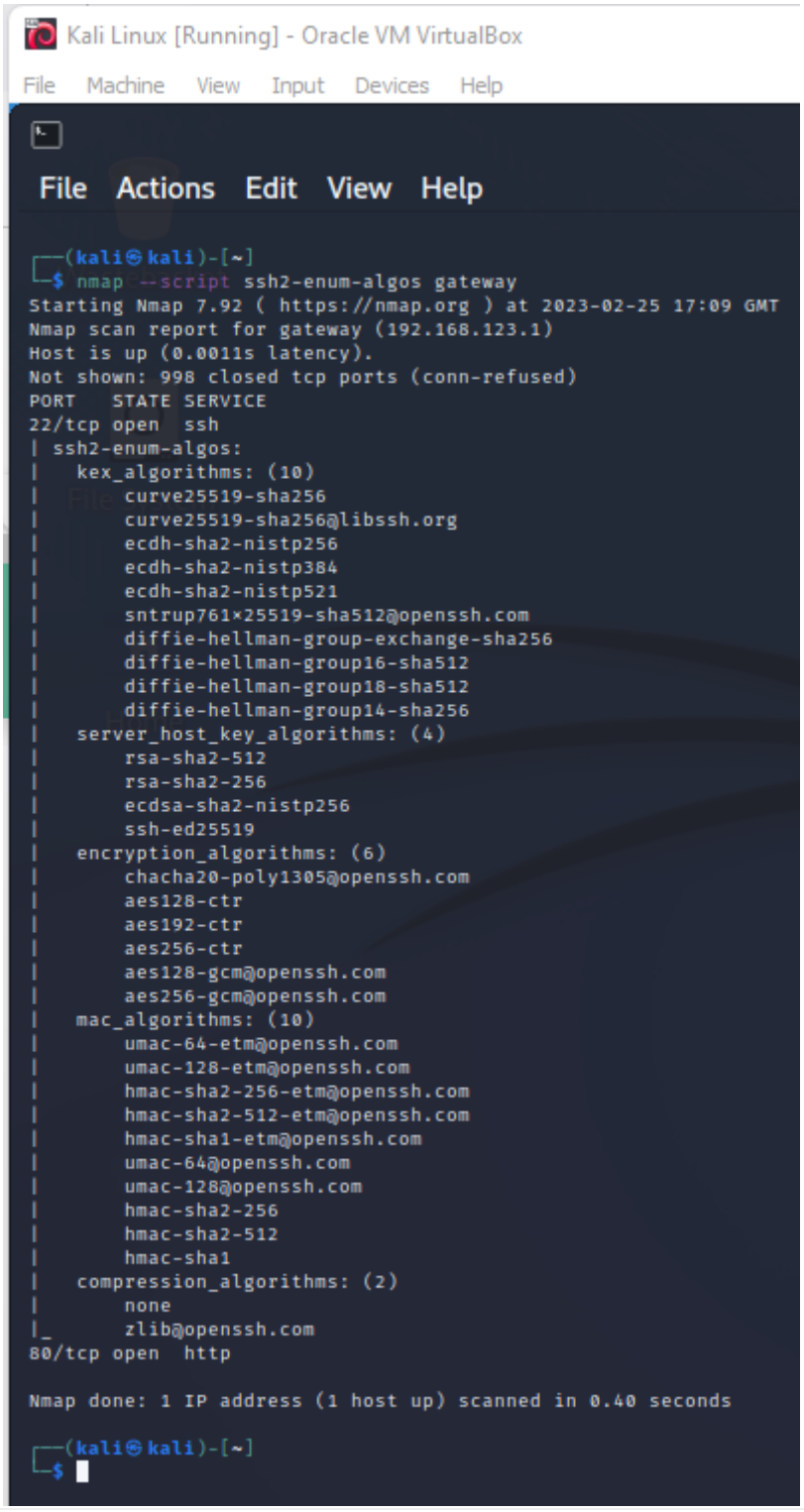
* *Well known as a half-open scanning, as it doesn't open a full TCP connection.*


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script=ssh-run gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:06 GMT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0018s latency).
PORT STATE SERVICE
22/tcp open ssh
|_ssh-run: Failed to specify credentials and command to run.
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s latency).
PORT STATE SERVICE
22/tcp open ssh
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0022s latency).
PORT STATE SERVICE
22/tcp closed ssh
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0030s latency).
PORT STATE SERVICE
22/tcp closed ssh
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0025s latency).
PORT STATE SERVICE
22/tcp open ssh
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
┌──(kali㉿kali)-[~]
└─$

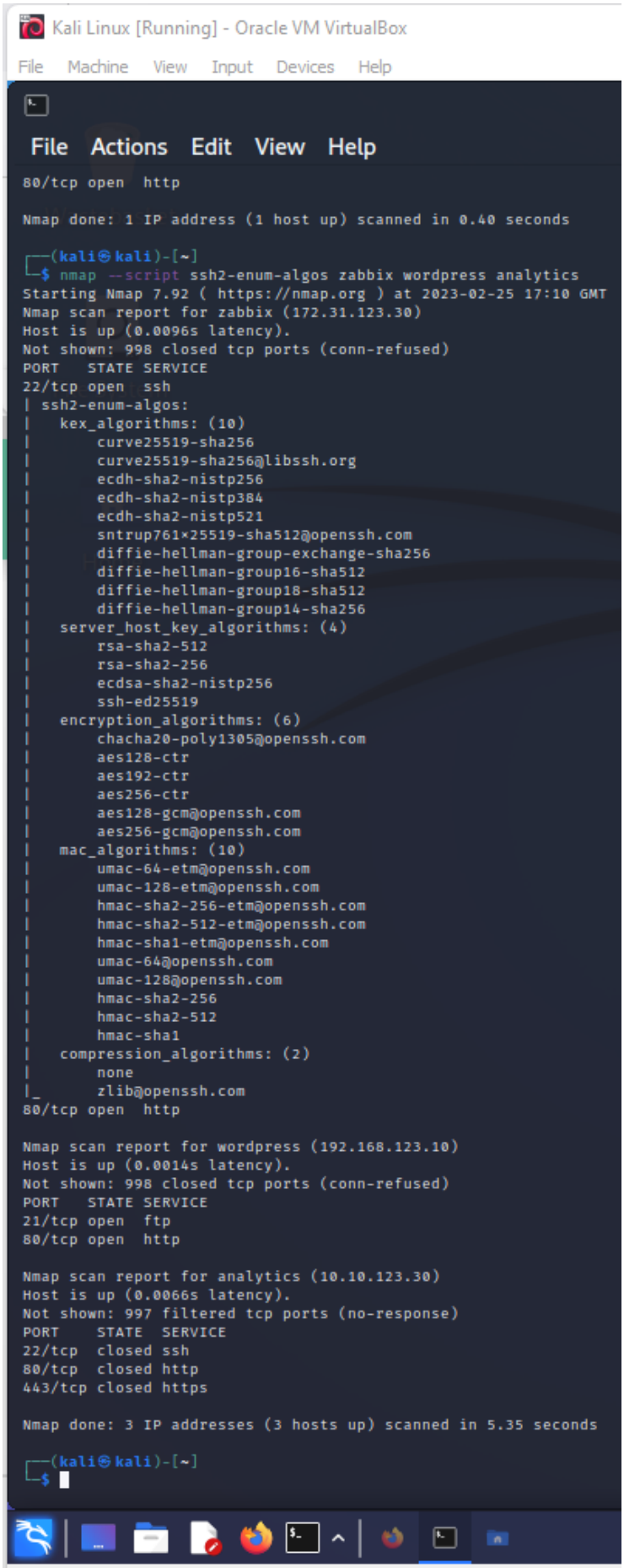
16. Save Output of Nmap Scan to a File

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

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

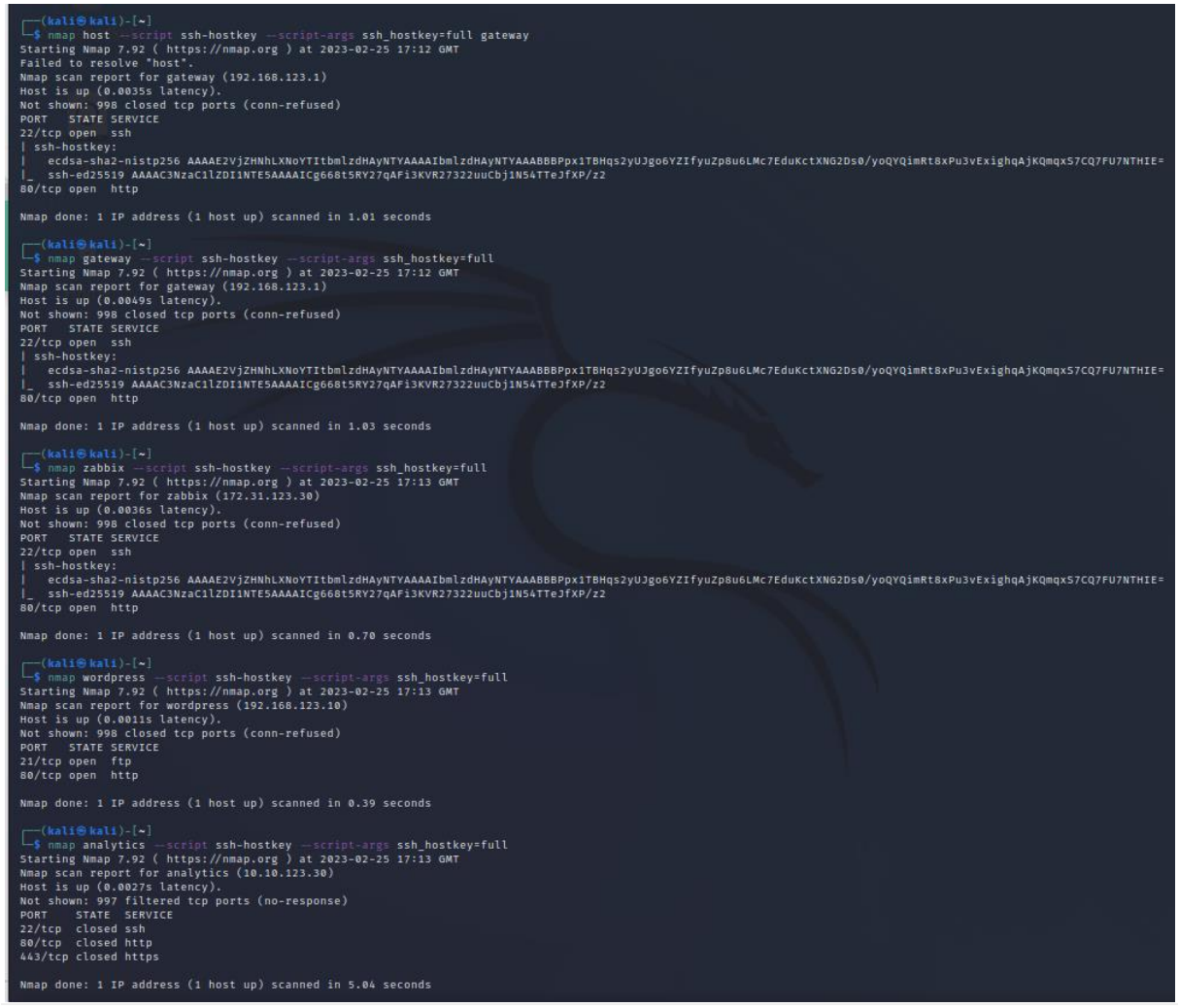



```
$ nmap -oN output.txt 192.168.123.1
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --script ssh2-enum-algos zabbix wordpress analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:10 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0096s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
| ssh2-enum-algos:
| kex_algorithms: (10)
| curve25519-sha256
| curve25519-sha256@libssh.org
| ecdh-sha2-nistp256
| ecdh-sha2-nistp384
| ecdh-sha2-nistp521
| sntrup761x25519-sha512@openssh.com
| diffie-hellman-group-exchange-sha256
| diffie-hellman-group16-sha512
| diffie-hellman-group18-sha512
| diffie-hellman-group14-sha256
| server_host_key_algorithms: (4)
| rsa-sha2-512
| rsa-sha2-256
| ecdsa-sha2-nistp256
| ssh-ed25519
| encryption_algorithms: (6)
| chacha20-poly1305@openssh.com
| aes128-ctr
| aes192-ctr
| aes256-ctr
| aes128-gcm@openssh.com
| aes256-gcm@openssh.com
| mac_algorithms: (10)
| umac-64-etm@openssh.com
| umac-128-etm@openssh.com
| hmac-sha2-256-etm@openssh.com
| hmac-sha2-512-etm@openssh.com
| hmac-sha1-etm@openssh.com
| umac-64@openssh.com
| umac-128@openssh.com
| hmac-sha2-256
| hmac-sha2-512
| hmac-sha1
| compression_algorithms: (2)
| none
|_ zlib@openssh.com
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0014s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0066s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 3 IP addresses (3 hosts up) scanned in 5.35 seconds
┌──(kali㉿kali)-[~]
└─$

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

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

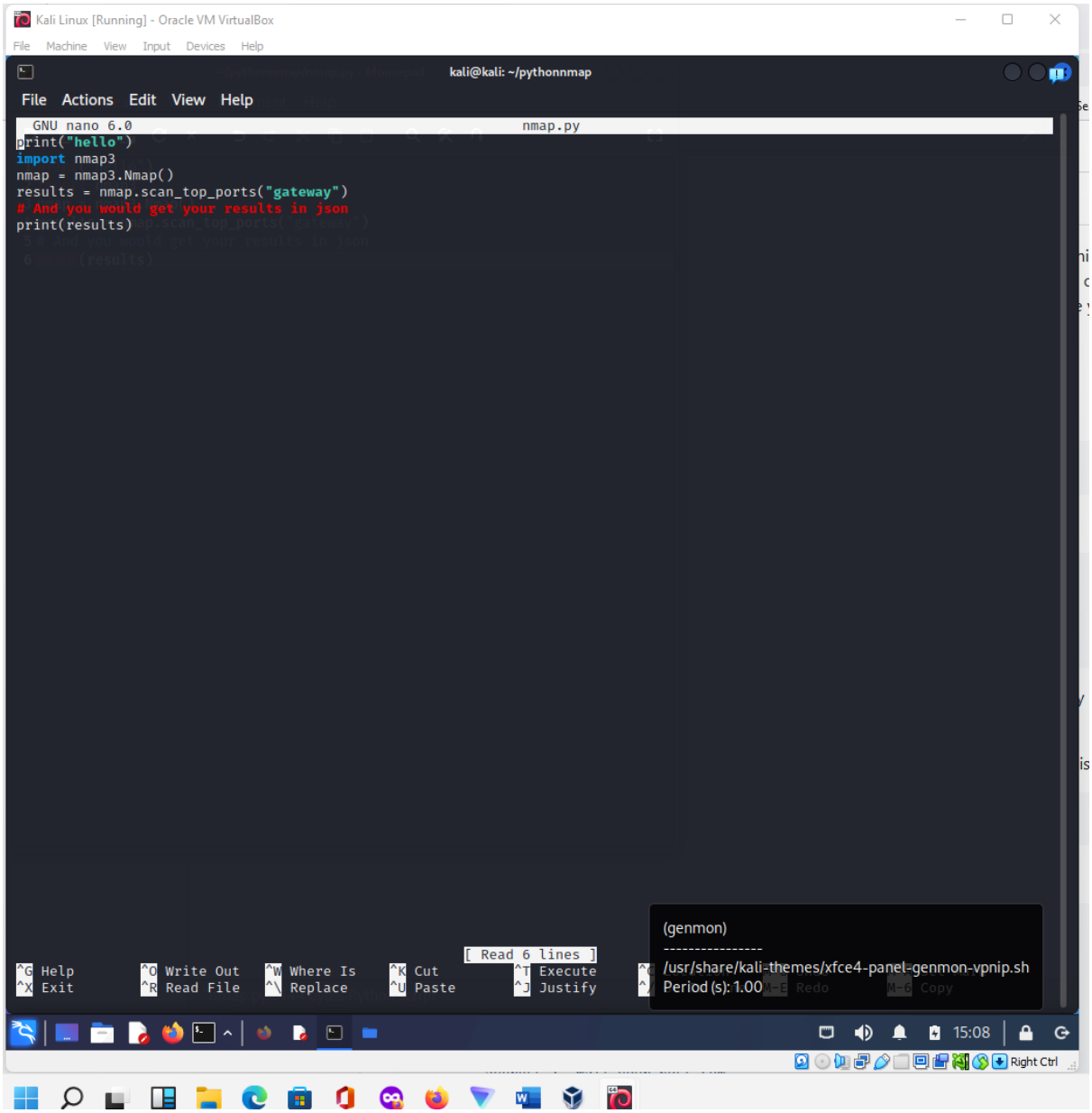


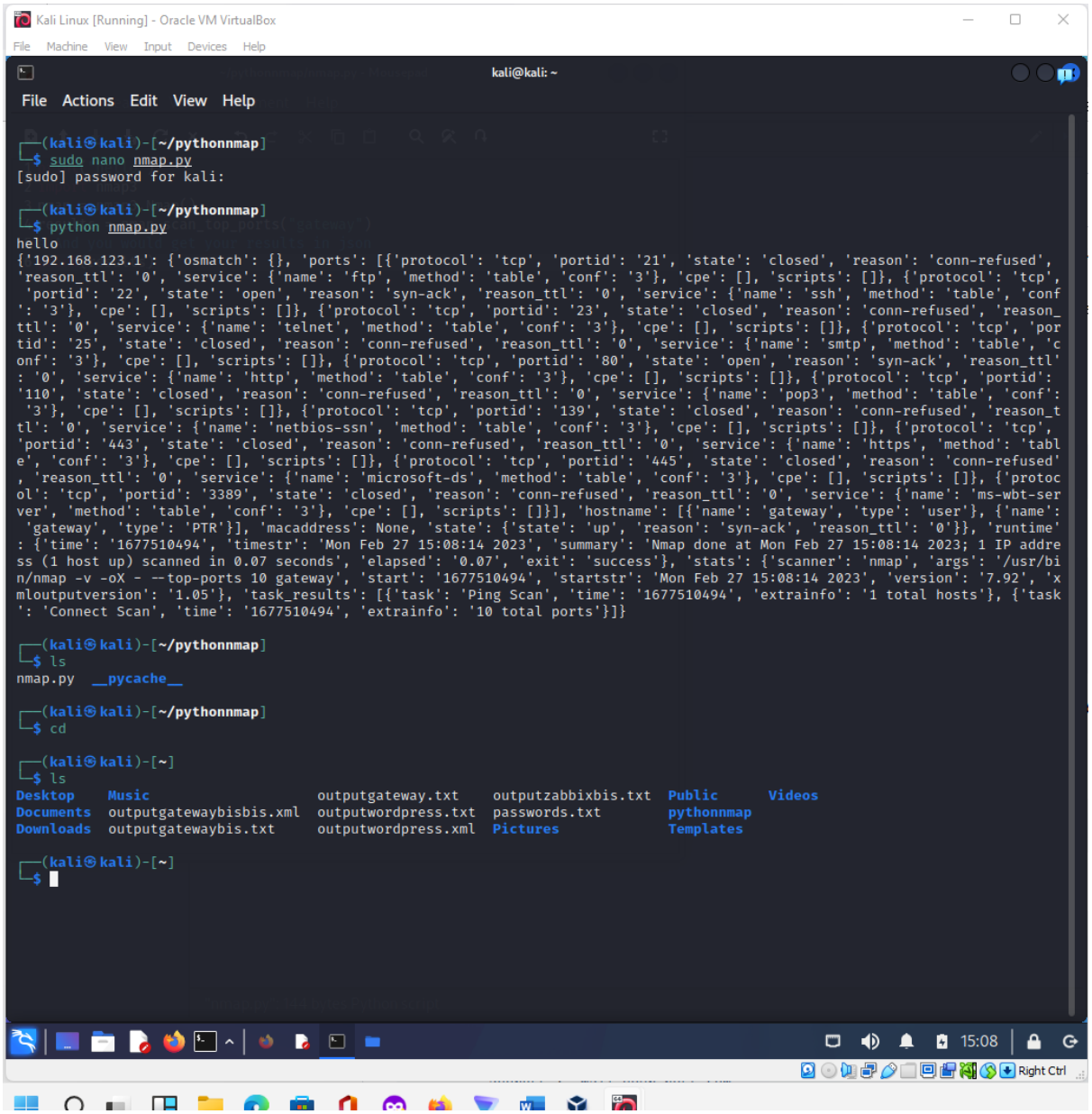
SOURCE: https://www.shellhacks.com/20-nmap-examples/ (Accessed 29th October 2022)

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)


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/pythonnmap
File Actions Edit View Help
GNU nano 6.0 nmap.py
print("hello")
import nmap3
nmap = nmap3.Nmap()
results = nmap.scan_top_ports("gateway")
# And you would get your results in json
print(results)
[Read 6 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
(genmon)
/usr/share/kali-themes/xfce4-panel-genmon-vpnip.sh
Period (s): 1.00
15:08
Right Ctrl



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.
Brief WOW Factor Description (if completed)	Moodle discussion, extra nmap commands and scripts. Investigation with host names and pings (see screenshoots).

Student Name:	Tony
Student ID:	YIT19488399

##END##