

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:	<p>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.</p> <p>LO4: Evaluate risks to privacy and anonymity in commonly used applications.</p>

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:

GNU nano 2.2.6 File: /etc/hostname

```
student
```

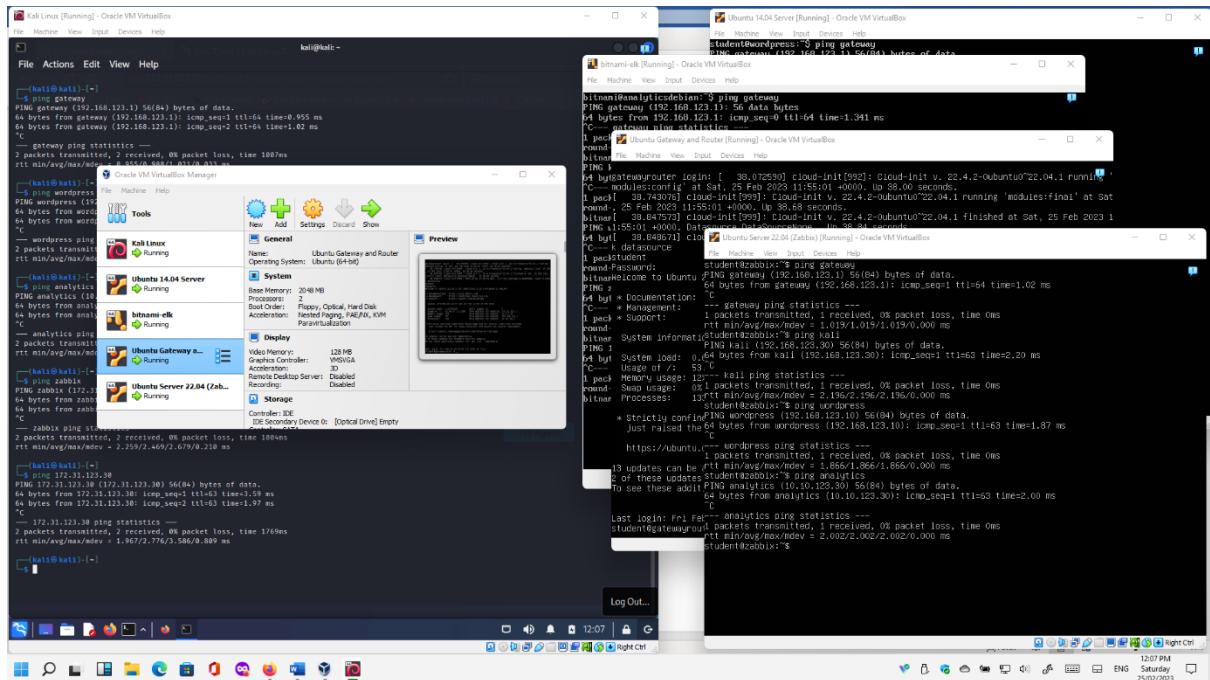
[Read 1 line]

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U Uncut Text ^T To Spell

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)

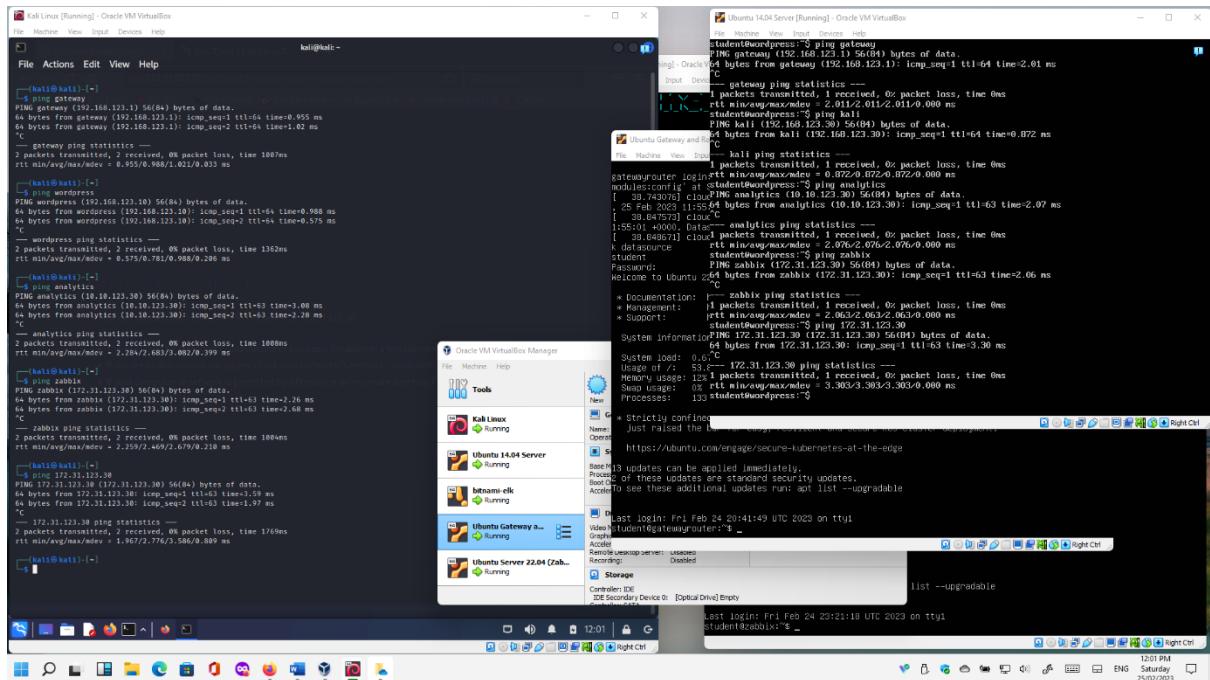
As this is also a WordPress server change the hostname to `wordpress`. Type:

```
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)

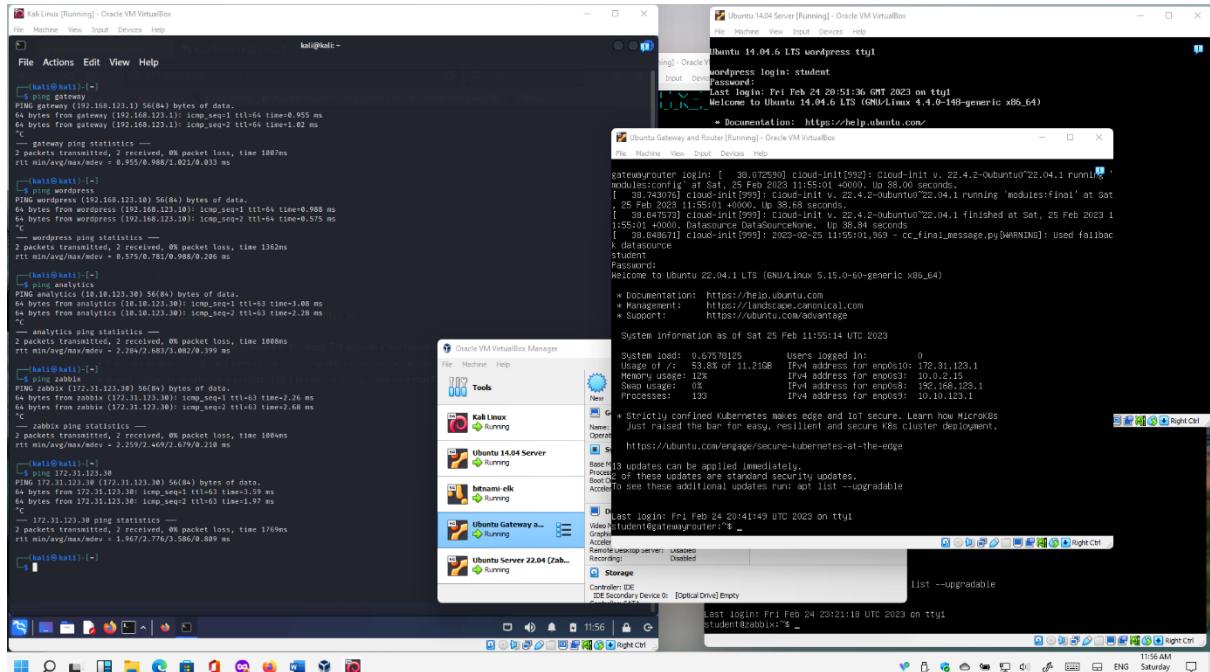
As this is a gateway server, change the hostname to gateway. Type:

```
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

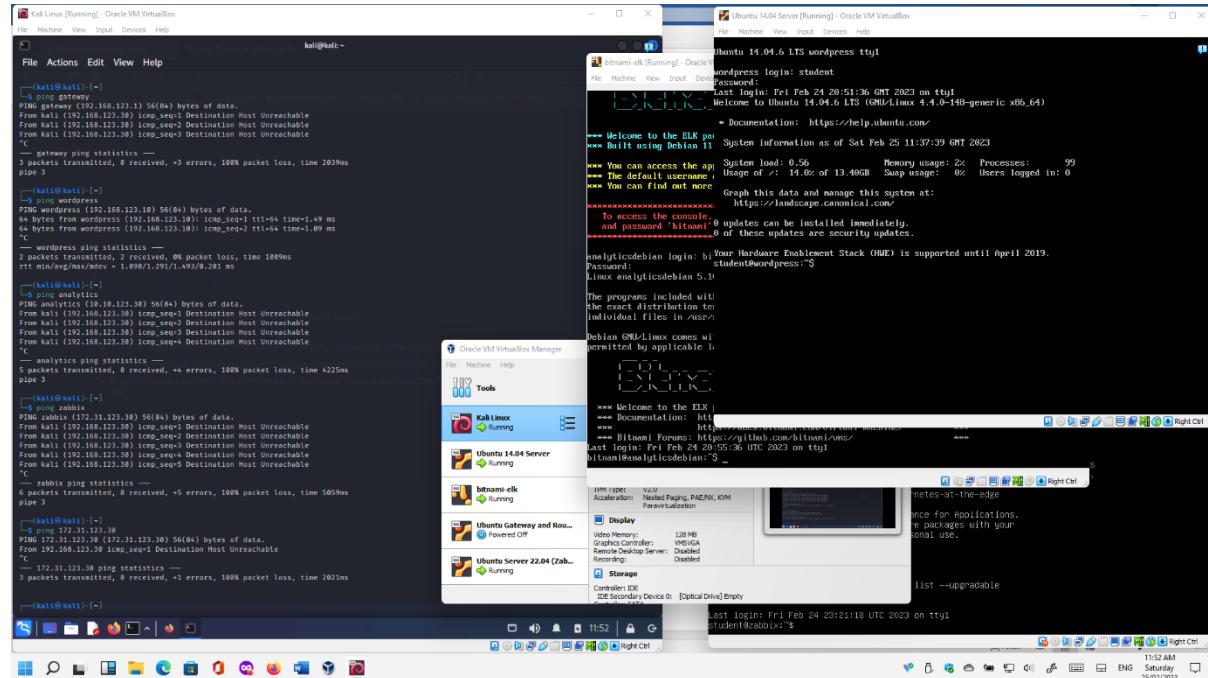
As this is an Elastic Search server (ELK Stack) change the hostname to `analytics`. Type:

```
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!

```
File Actions Edit View Help
GNU nano 6.0                                         /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
192.168.123.1  gateway
192.168.123.30 kali
192.168.123.10 wordpress
10.10.123.30  analytics
172.31.123.30 zabbix

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

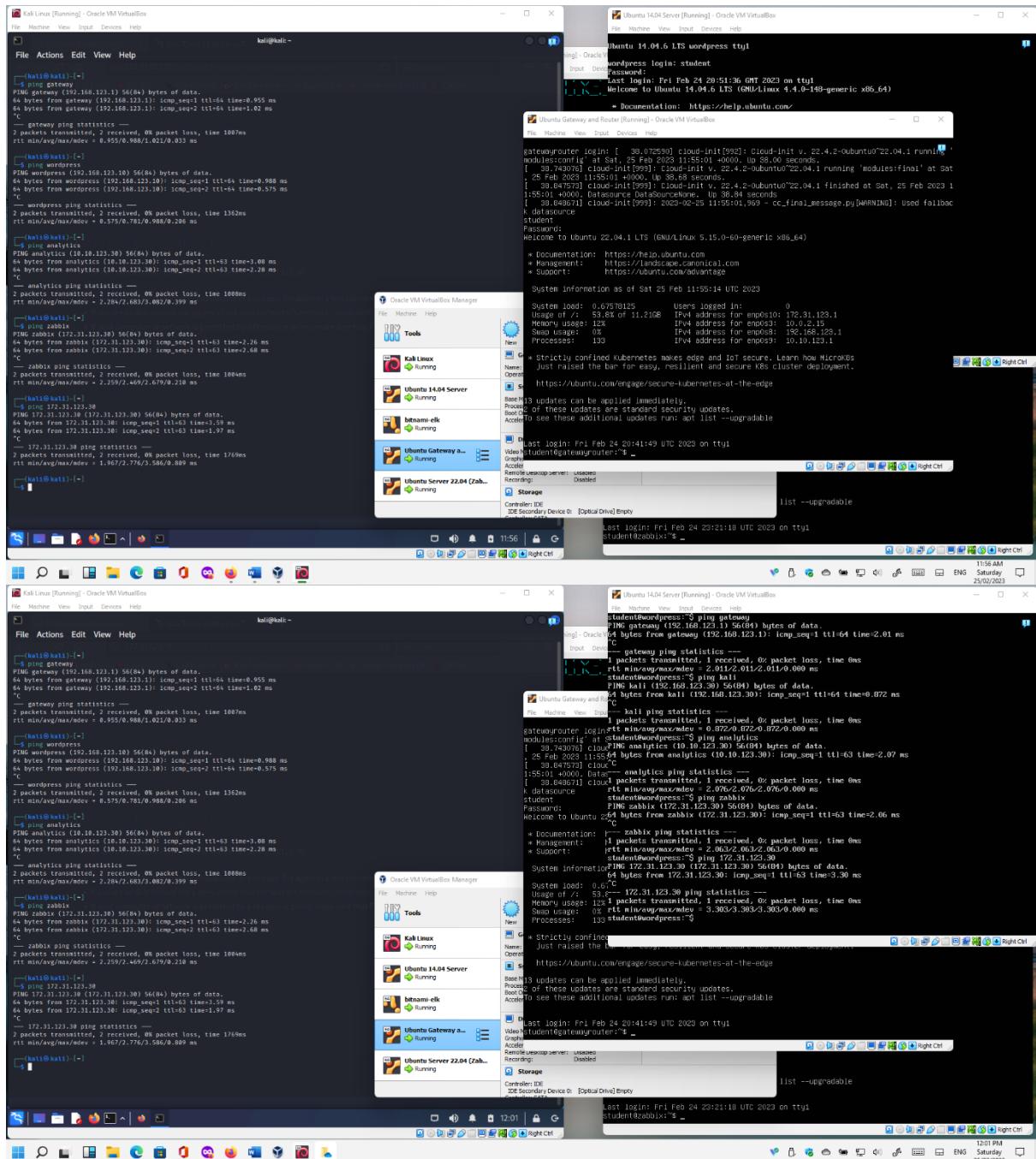
Save the open *hosts* file by typing **Ctrl x**, followed by **y**, then press **Enter**. From your kali terminal, test that you can **ping** the host names.

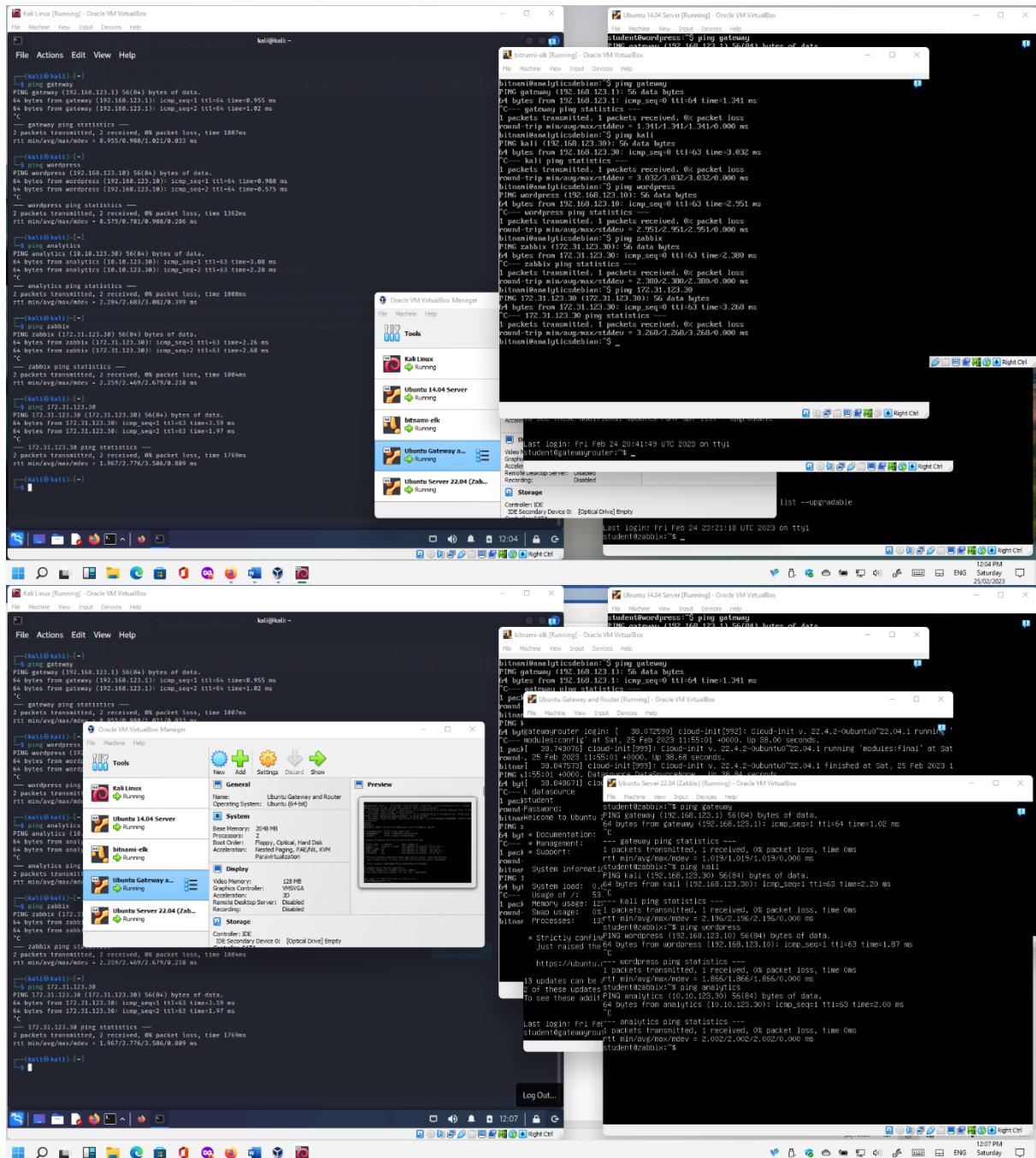
6. Repeat the steps in task 5 for the other virtual machines on your network.

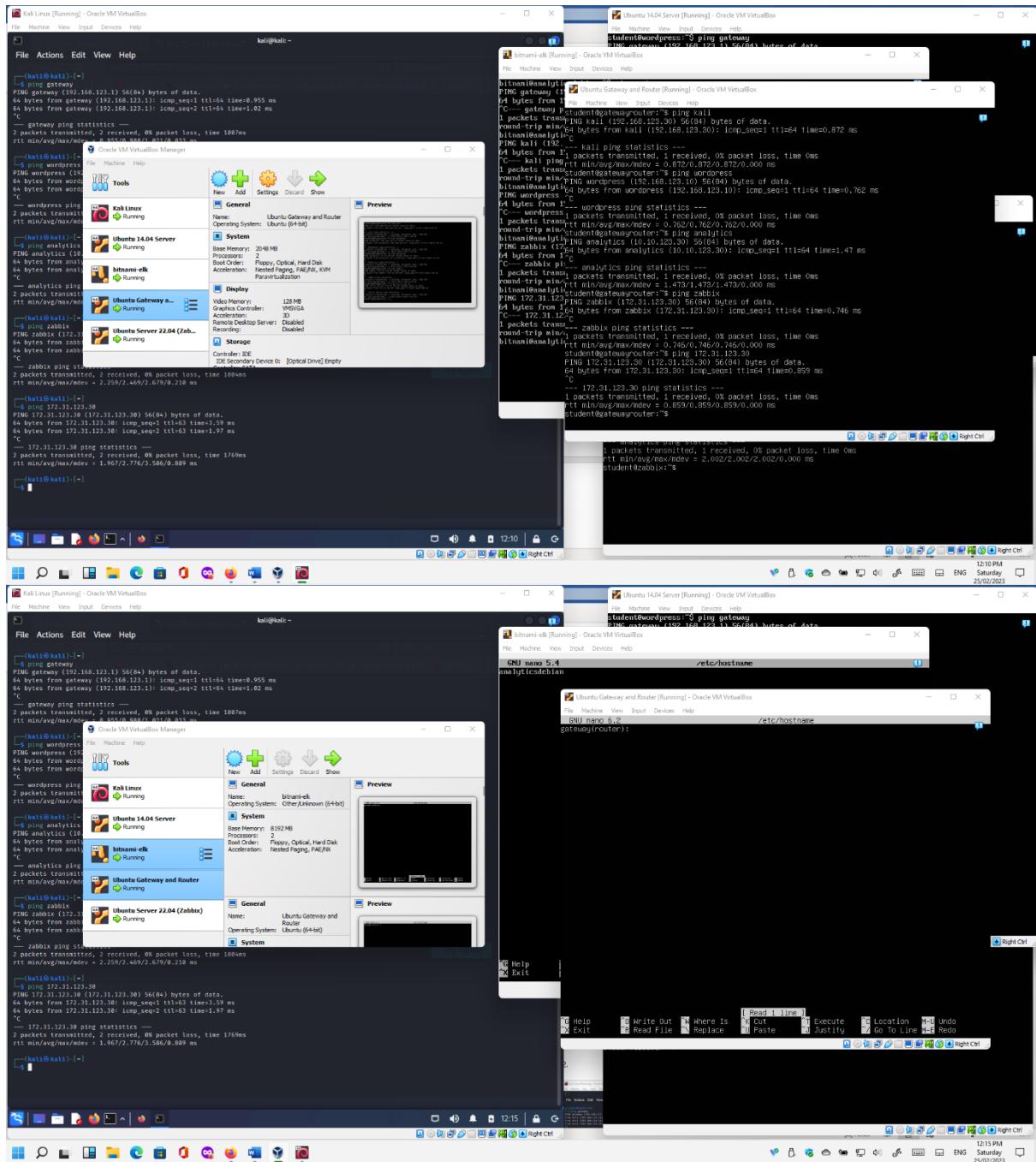
Amend the **hosts** file for **wordpress**, **analytics**, **zabbix** and **gateway**. Once completed, you should be able to ping any of the configured host names on any of the virtual machines and resolve each host name to its respective IP address.

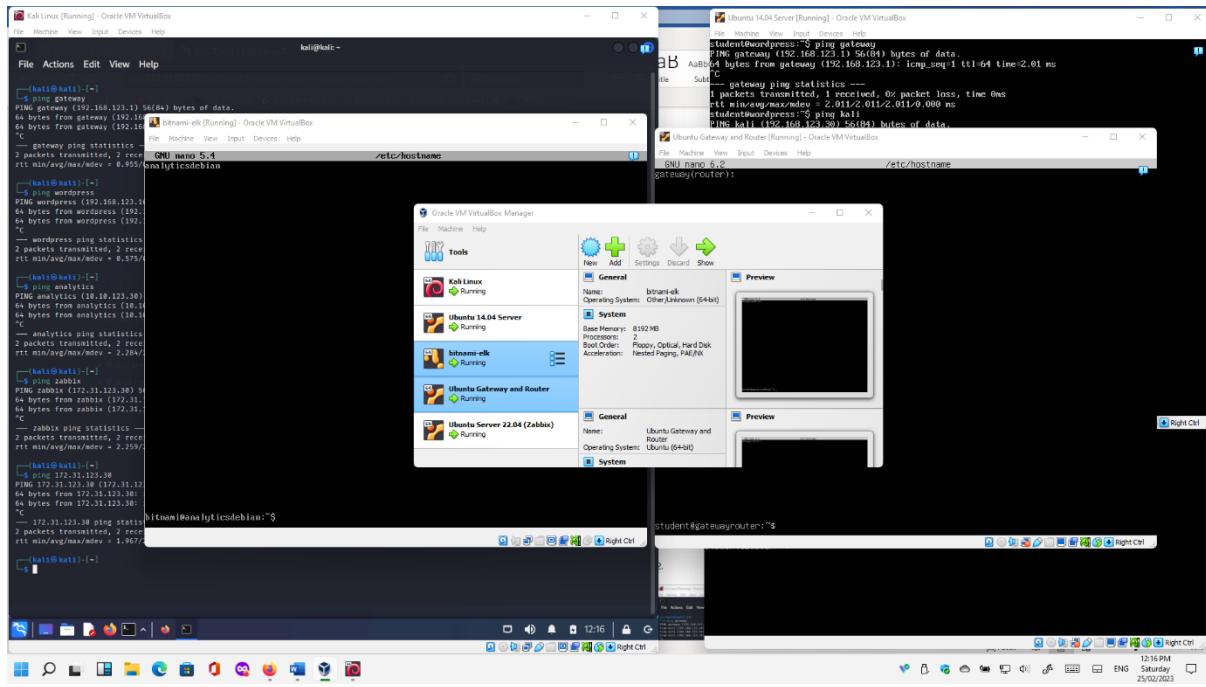
Requirement A: Demonstration Tasks

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.









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.

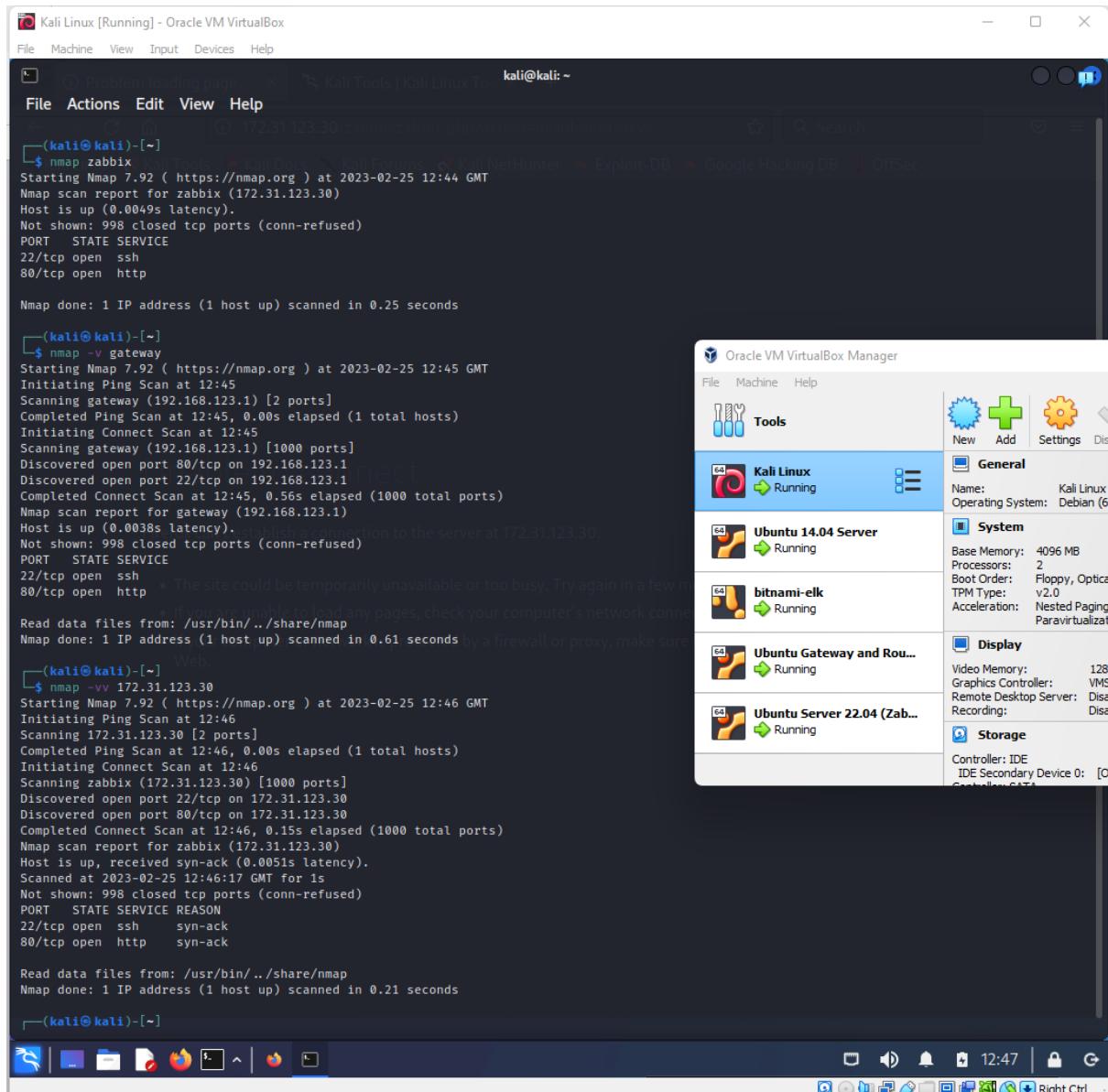
*Businesses can also use the port scanning technique to send packets to specific ports and analyze responses for any potential vulnerability. They can then use tools like IP scanning, network mapper (**Nmap**), and Netcat to ensure their network and systems are secure."*

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
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
-(kali㉿kali)-[~]
$ nmap zabbix analytics
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 12:48 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0050s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for analytics (10.10.123.30)
Host is up (0.0035s 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: 2 IP addresses (2 hosts up) scanned in 4.95 seconds

-(kali㉿kali)-[~]
$ nmap 192.168.123.10,1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 12:50 GMT
Failed to resolve "192.168.123.10,".
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.07 seconds

-(kali㉿kali)-[~]
$ nmap 192.168.123.10,1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 12:50 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0020s latency). Computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.29 seconds

-(kali㉿kali)-[~]
$ 
```

3. Scan a Subnet:

```
$ nmap 192.168.123.0/24
```

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~

File Actions Edit View Help

172.31.123.30/abniv/abniv.php?action=dashboard.view

\$ nmap 192.168.123.10/24

Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:51 GMT

Nmap scan report for gateway (192.168.123.1)

Host is up (0.0016s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

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 kali (192.168.123.30)

Host is up (0.00092s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT STATE SERVICE

53/tcp open domain

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.35 seconds

Firefox can't establish a connection to the server at 172.31.123.30.

\$(kali㉿kali)-[~]

\$ nmap 192.168.123.*

Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:51 GMT

Nmap scan report for gateway (192.168.123.1)

Host is up (0.0017s latency). Try again in a few moments.

Not shown: 998 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap scan report for wordpress (192.168.123.10)

Host is up (0.0021s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT STATE SERVICE

21/tcp open ftp

80/tcp open http

Nmap scan report for kali (192.168.123.30)

Host is up (0.0019s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT STATE SERVICE

53/tcp open domain

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.03 seconds

\$(kali㉿kali)-[~]

\$

Try Again

```
$ nmap 192.168.123.*
```

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

172.31.123.30/zabbix/zabbix.php?action=dashboard.view

kali@kali: ~

```
$ nmap 192.168.123.0-255
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 12:55 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0013s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0023s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http

Nmap scan report for kali (192.168.123.30)
Host is up (0.0018s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.53 seconds
```

Firefox can't establish a connection to the server at 172.31.123.30.

```
$(kali㉿kali)-[~]
$ nmap 10.10.123.0-255
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 12:55 GMT
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan Try again in a few moments.
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 10.10.123.1
Host is up (0.0020s latency).
The target machine or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for analytics (10.10.123.30)
Host is up (0.0046s 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: 256 IP addresses (2 hosts up) scanned in 24.28 seconds
```

Try Again

```
$(kali㉿kali)-[~]
$ 
```

12:55 | Right Ctrl

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

```
$ nmap 192.168.123.0-200
```

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

(kali㉿kali)-[~]

```
$ nmap -sn 192.168.123.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:05 GMT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 57.81% done; ETC: 13:05 (0:00:01 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0036s latency).
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0013s latency).
Nmap scan report for kali (192.168.123.30)
Host is up (0.00051s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.03 seconds
```

```
[(kali㉿kali)-[~]]$ nmap -sn 192.168.123.10/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:05 GMT
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 96.48% done; ETC: 13:05 (0:00:00 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0089s latency).
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0016s latency).
Nmap scan report for kali (192.168.123.30)
Host is up (0.00059s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.32 seconds
```

```
[(kali㉿kali)-[~]]$ echo 192.168.123.{1..254}|xargs -n1 -P0 ping -c1|grep "bytes from"
64 bytes from 192.168.123.1: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.123.10: icmp_seq=1 ttl=64 time=1.23 ms
64 bytes from 192.168.123.30: icmp_seq=1 ttl=64 time=0.038 ms
* If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the
[(kali㉿kali)-[~]]$ nmap -sn 10.10.123.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:06 GMT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 68.07% done; ETC: 13:06 (0:00:01 remaining)
Nmap scan report for 10.10.123.1
Host is up (0.0017s latency).
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0032s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.87 seconds
```

```
[(kali㉿kali)-[~]]$ echo 10.10.123.{0..255}|xargs -n1 -P0 ping -c1|grep "bytes from"
64 bytes from 10.10.123.1: icmp_seq=1 ttl=64 time=1.54 ms
64 bytes from 10.10.123.30: icmp_seq=1 ttl=63 time=2.93 ms
```

```
[(kali㉿kali)-[~]]$ echo 10.10.123.{0..255}|xargs -n1 -P0 ping -c1|grep "bytes from"
64 bytes from 10.10.123.1: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 10.10.123.30: icmp_seq=1 ttl=63 time=3.01 ms
```

```
[(kali㉿kali)-[~]]$
```

13:07 | Right Ctrl

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

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)-[~] • If you are unable to load any pages, check your computer's
$ 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㉿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]# 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: 08:00:27:6A:6D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds

[root@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

[roo[root@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

[roo[root@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

[roo[root@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
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)

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

[roo[root@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

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
```

Scan for All Ports:

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

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices 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

Dashboard Zabbix Integrations and

File Actions Edit View Help

→ C 🏠 https://www.zabbix.com/integ

```
(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
```

```
(kali㉿kali)-[~]
└─$ nmap -O gateway
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
└─# nmap -O gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:26 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:00:27:66:0A:60 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds

(root㉿kali)-[~/home/kali]
└─# nmap -O wordpress
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:27 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.00082s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
MAC Address: 00:00:27:25:44:B2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds

(root㉿kali)-[~/home/kali]
└─# nmap -O kali
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:27 GMT
Nmap scan report for kali (127.0.1.1)
Host is up (0.000097s 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 (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds

(root㉿kali)-[~/home/kali]
└─# nmap -O zabbix
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:27 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0023s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```

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

Dashboard Zabbix Integrations and Monitoring and Integration

kali@kali: ~ kali@kali: ~

```
File Actions Edit View Help https://www.zabbix.com/integrations
(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
```

All Categories Official Templates Agents API Applications Security Services Servers Storage Telephon Web

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/kali

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
```

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

(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
```

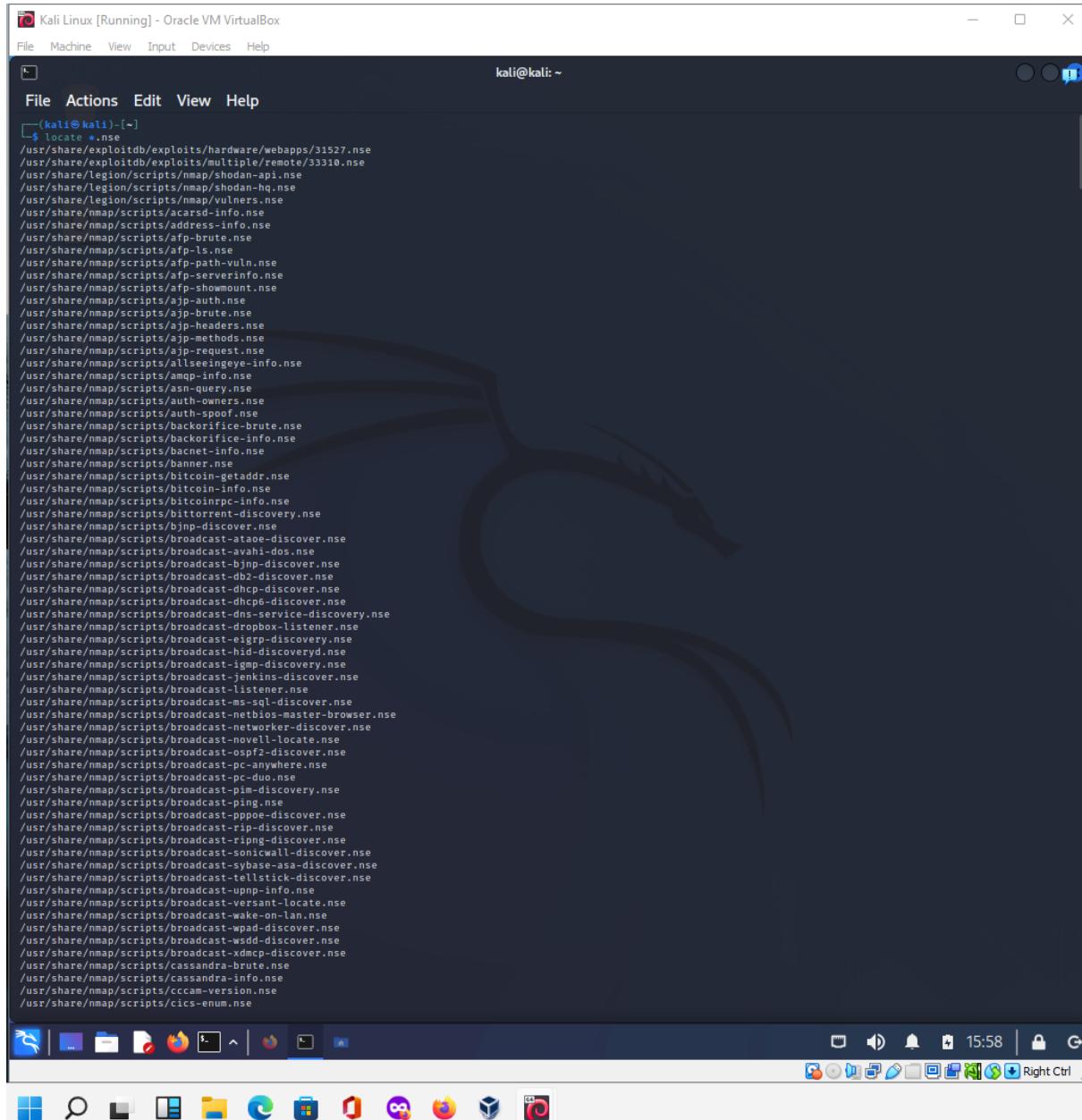
(kali㉿kali)-[~]

```
$ █
```



Scan for Particular UDP Ports:

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



The screenshot shows a terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The command `locate *.nse` has been run, displaying a long list of Nmap Scripting Engine (NSE) files located in various directories under /usr/share. The list includes scripts for webapps, shodan, vulners, acarsd, address, ftp, http, https, amqp, asn, auth, headers, methods, request, allseengey, info, amqp, info, asn, query, auth, owners, auth-spoof, backorifice, brutes, bacnet, banner, bitcoin, bitcoinrpc, bttorrent, bittorrent, discovery, bittorrent, discover, broadcast, ataoc, avahi, dos, db2, dhcpc, dhcp, dhcp6, dns, dropbox, eigrp, hid, ighp, jenkins, listener, ms, msq, netbios, networker, novell, ospf2, pc, anywhere, pc, duo, pim, ping, ppoe, rip, rping, sonicwall, sybase, asa, discover, tellstick, upnp, info, versant, locate, wake-on-lan, wps, wsdd, discover, xdmc, cassandra, brute, cassandra, info, cccam, version, cics, enum, and others.

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: ~

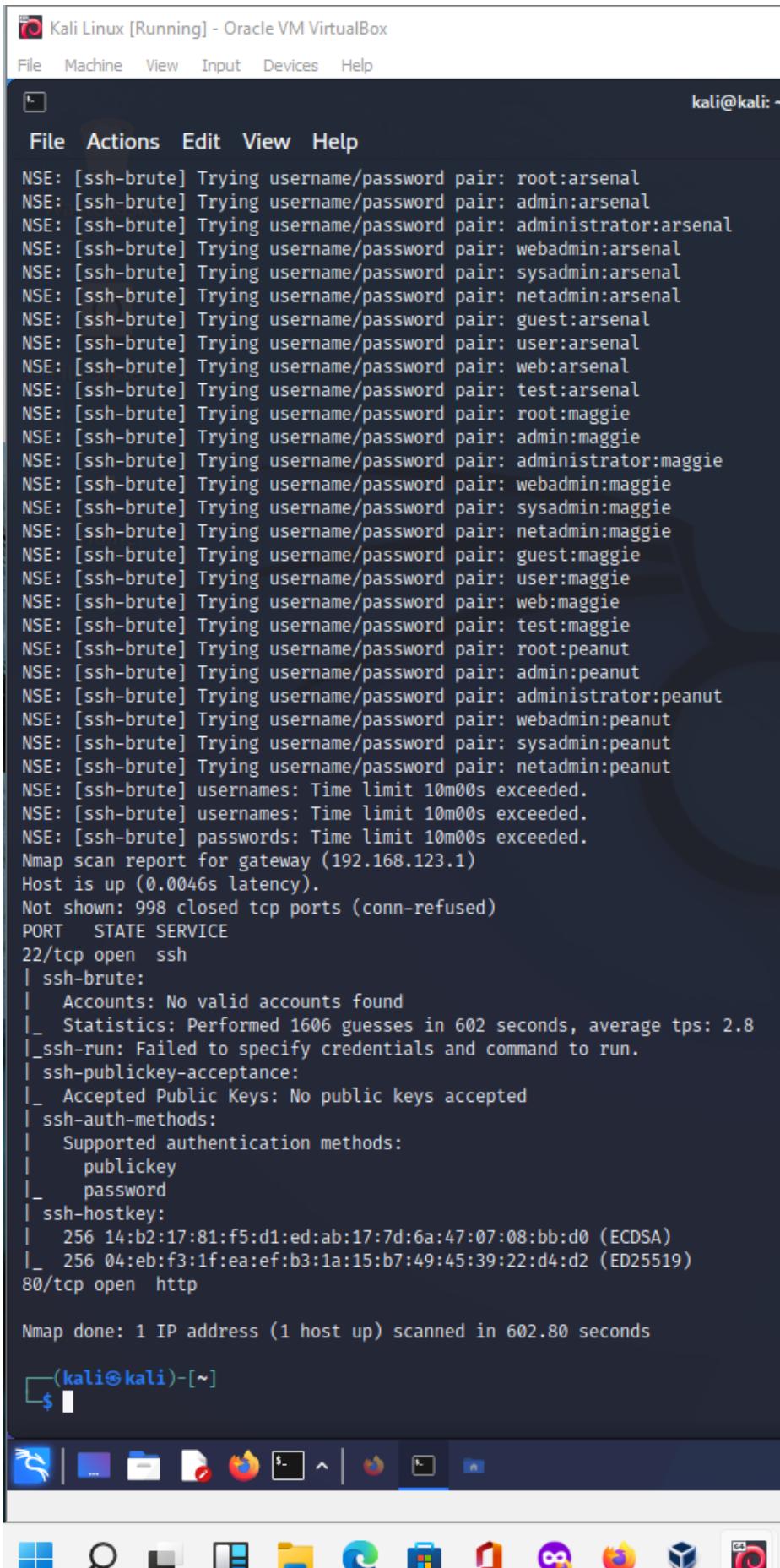
File Actions Edit View Help

```
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
```



The screenshot shows a terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The command entered is \$ nmap --reason 192.168.123.1. The output of the command is displayed below:

```
(kali㉿kali)-[~]
└─$ nmap --script "not vuln" gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 16:22 GMT
Pre-scan script results:
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
|_ http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_ hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0037s latency).
Not shown: 996 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
| banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
| ssh2-enum-algos:
|   kex_algorithms: (10)
|   server_host_key_algorithms: (4)
|   encryption_algorithms: (6)
|   mac_algorithms: (10)
|_ compression_algorithms: (2)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     password
| ssh-run: Failed to specify credentials and command to run.
| 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)
| ssh-brute:
|_ Accounts: No valid accounts found
| Statistics: Performed 22 guesses in 1807 seconds, average tps: 0.3
80/tcp    open  http
| http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=gateway
|_ Found the following error pages:

  Error Code: 404
  http://gateway:80/manual
| http-slowloris: false
| http-mobileversion-checker: No mobile version detected.
| http-config-backup: ERROR: Script execution failed (use -d to debug)
| http-vhosts:
|_ 128 names had status 200
| http-server-header: Apache/2.4.52 (Ubuntu)
| http-title: Apache2 Ubuntu Default Page: It works
|_ citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-sitemap-generator:
|   Directory structure:
|   /
|   Other: 1
|   /icons/
|   png: 1
| Longest directory structure:
|   Depth: 1
|   Dir: /icons/
| Total files found (by extension):
|   Other: 1; png: 1
| http-xssed:
  UNFIXED XSS vuln.

  http://technologygateway.nasa.gov/index.cfm?fuseaction=%22%3E%3Ciframe%20src=%22http://xssed.com%22%<br>%E
  http://gateway.mdgms.com/login.html?LANG=%22%27%3E%3Cscript%3Ealert(%22XSS%22)%3C/script%3E
  http:// www.workgateways.com/login.php?User=%22%20/%3E%3Cscript%3Ealert%28%22XSS%20by%20MadAgent%22%2<br>%3C/script%3E%3Cbr%20%22
```

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
```



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~

File Actions Edit View Help
lwp-trivial
libcurl-agent/1.0
PHP/
python-urllib/2.5
GT :: WWW
Snoopy
MFC_Tear_Sample
HTTP::Lite
PHPCrawl
URI::Fetch
Zend_Http_Client
http client
PECL :: HTTP
Wget/1.13.4 (linux-gnu)
WWW-Mechanize/1.34
http-brute:
Path "/" does not require authentication
http-feed: Couldn't find any feeds.
http-headers:
Date: Sat, 25 Feb 2023 16:53:37 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)
http-fetch: Please enter the complete path of the directory to save data in.
http-date: Sat, 25 Feb 2023 16:53:41 GMT; +1h00m09s from local time.
http-comments-displayer:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=gateway

Path: http://gateway:80/
Line number: 3
Comment:
<!--
     Modified from the Debian original for Ubuntu
     Last updated: 2022-03-22
     See: https://launchpad.net/bugs/1966004
-->

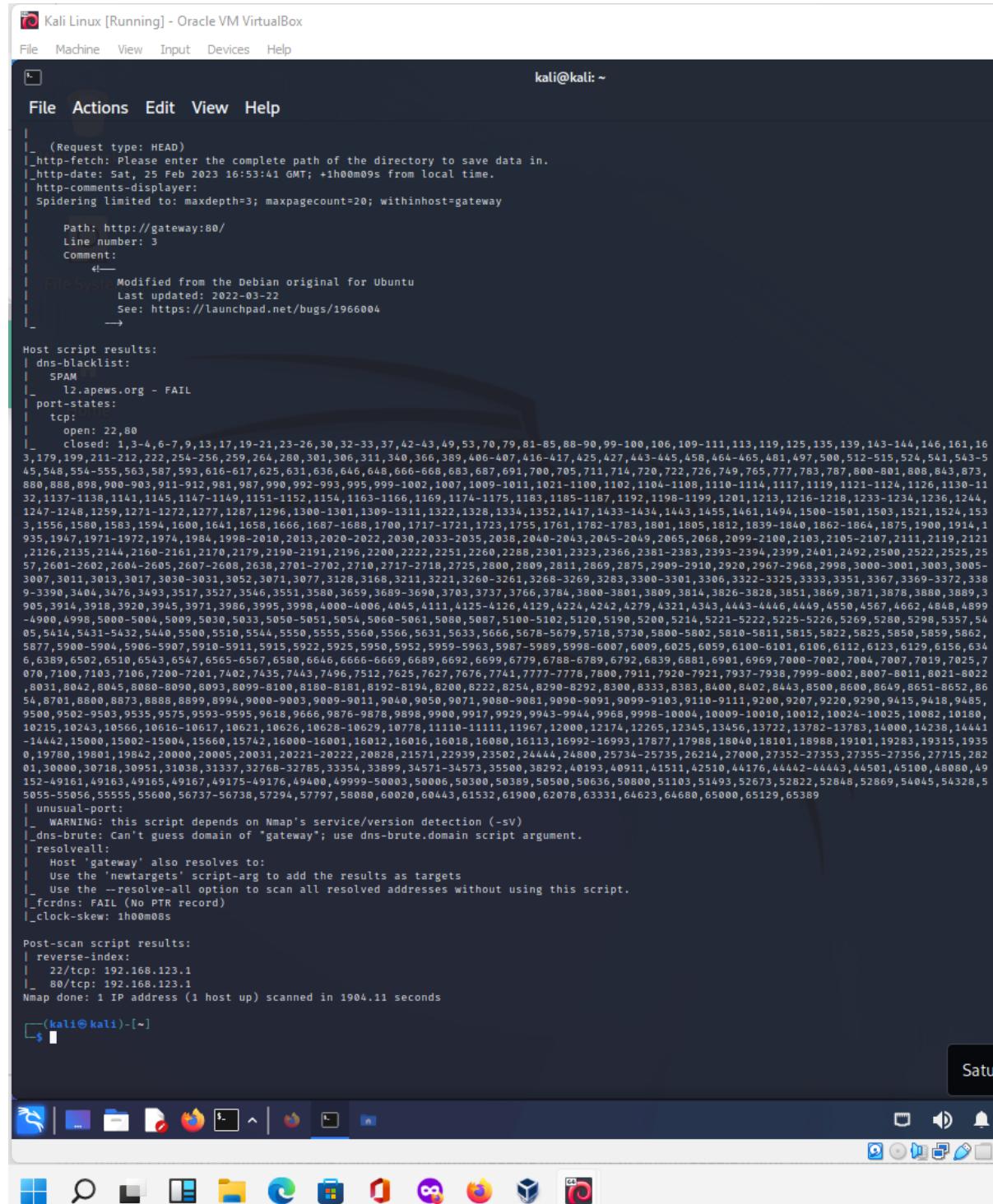
Host script results:
dns-blacklist:
SPAM
l2.apews.org - FAIL
port-states:
tcp:
open: 22,80
closed: 1,3-4,6-7,9,13,17,19-21,23-26,30,32-33,37,42-43,49,53,70,79,81-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,16
3,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-5
45,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,
880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-11
32,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,
1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,153
3,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1
935,1947,1971-1972,1974,1984,1986-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121
,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,25
57,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-
3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,338
9-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3
905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899
-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5357,54
05,5414,5431-5432,5440,5450,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,
5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,634
6,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7
07,7100,7103,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022
,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,86
54,8701,8800,8873,8888,8899,8894,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,
```

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.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~

|_ (Request type: HEAD)
|_.http-fetch: Please enter the complete path of the directory to save data in.
|_.http-date: Sat, 25 Feb 2023 16:53:41 GMT; +1h00m09s from local time.
|_.http-comments-displayer:
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=gateway

| Path: http://gateway:80/
| Line number: 3
| Comment:
|   ←
| File System Modified from the Debian original for Ubuntu
|   Last updated: 2022-03-22
|   See: https://launchpad.net/bugs/1966004
|   →

Host script results:
| dns-blacklist:
|   SPAM
|_ l2.apews.org - FAIL
port-states:
tcp:
| open: 22,80
| closed: 1,3-4,6-7,9,13,17,19-21,23-26,30,32-33,37,42-43,49,53,70,79,81-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,16
3,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-5
45,548,554,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,
880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-11
32,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,
1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,153
3,1556,1580,1583,1593,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1
935,1947,1971-1972,1974,1984,1988-2010,2013,2020-2022,2030-2035,2038,2040-2043,2045-2049,2068,2099-2100,2103,2105-2107,2111,2119,2121
,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,25
57,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-
3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,338
9-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3
905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899
-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,54
05,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,
5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6122,6129,6156,634
6,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7
070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022
,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,86
54,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,
9500,9502-9503,9539,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,
10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441
-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,1935
0,19780,19801,19842,20000,20005,20031,20221-20222,20282,20571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,282
01,30000,30718,30951,31038,31307,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49
152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,5
5055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389
|_ unusual-port:
|_ WARNING: this script depends on Nmap's service/version detection (-sv)
|_ dns-brute: Can't guess domain of "gateway"; use dns-brute.domain script argument.
|_ resolveall:
| Host 'gateway' also resolves to:
|   Use the 'newtargets' script-arg to add the results as targets
|   Use the --resolve-all option to scan all resolved addresses without using this script.
|_ fcrdns: FAIL (No PTR record)
|_ clock-skew: 1h00m08s

Post-scan script results:
| reverse-index:
|   22/tcp: 192.168.123.1
|   80/tcp: 192.168.123.1
Nmap done: 1 IP address (1 host up) scanned in 1904.11 seconds

[~] $
```

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

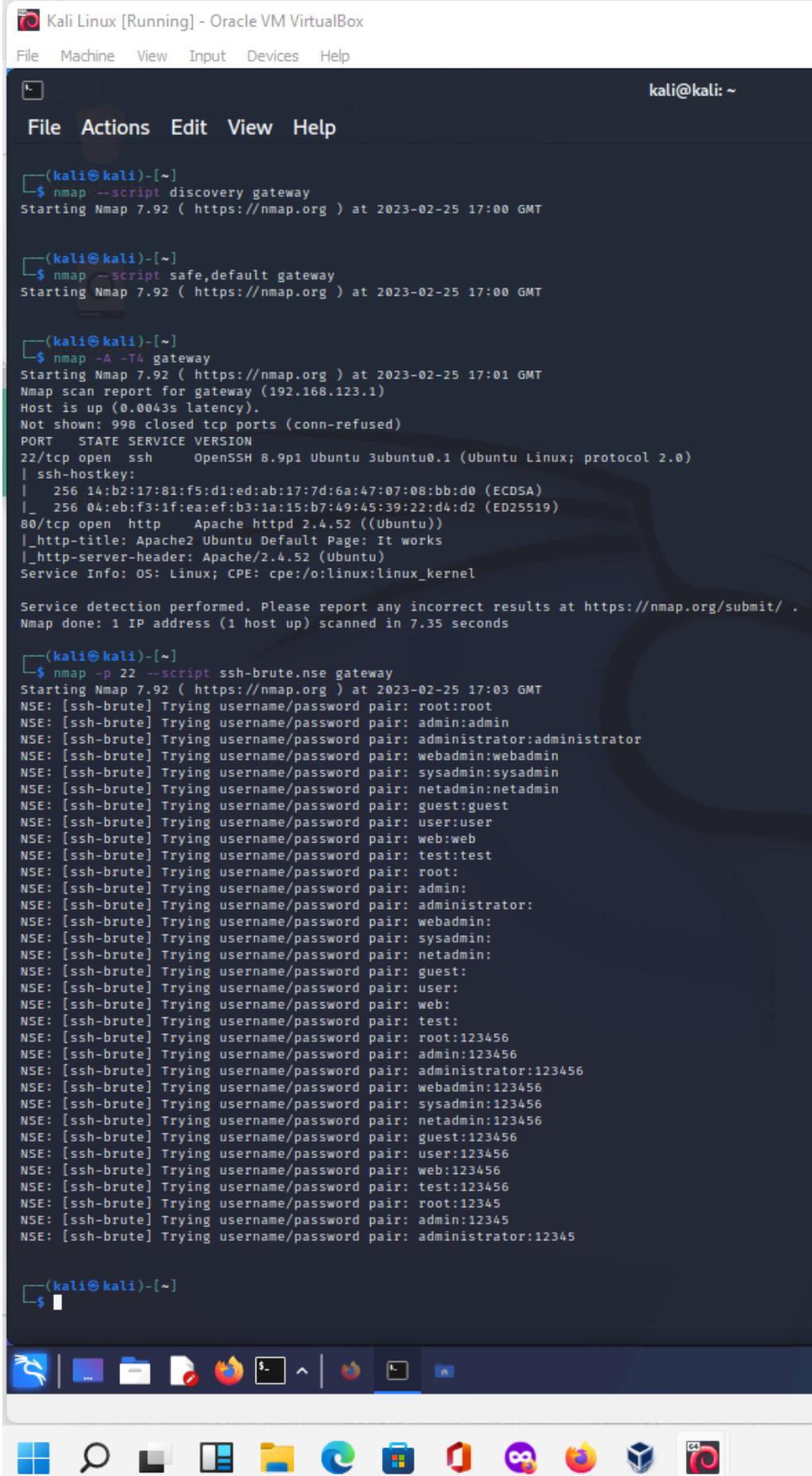
(kali㉿kali)-[~]
$ nmap --script safe,default gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:00 GMT

(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.
|_File System
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
NSE: [ssh-auth-methods] Failed to specify credentials and command to run.
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
NSE: [ssh-auth-methods] Failed to specify credentials and command to run.
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
NSE: [ssh-auth-methods] Failed to specify credentials and command to run.
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
NSE: [ssh-auth-methods] Failed to specify credentials and command to run.
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

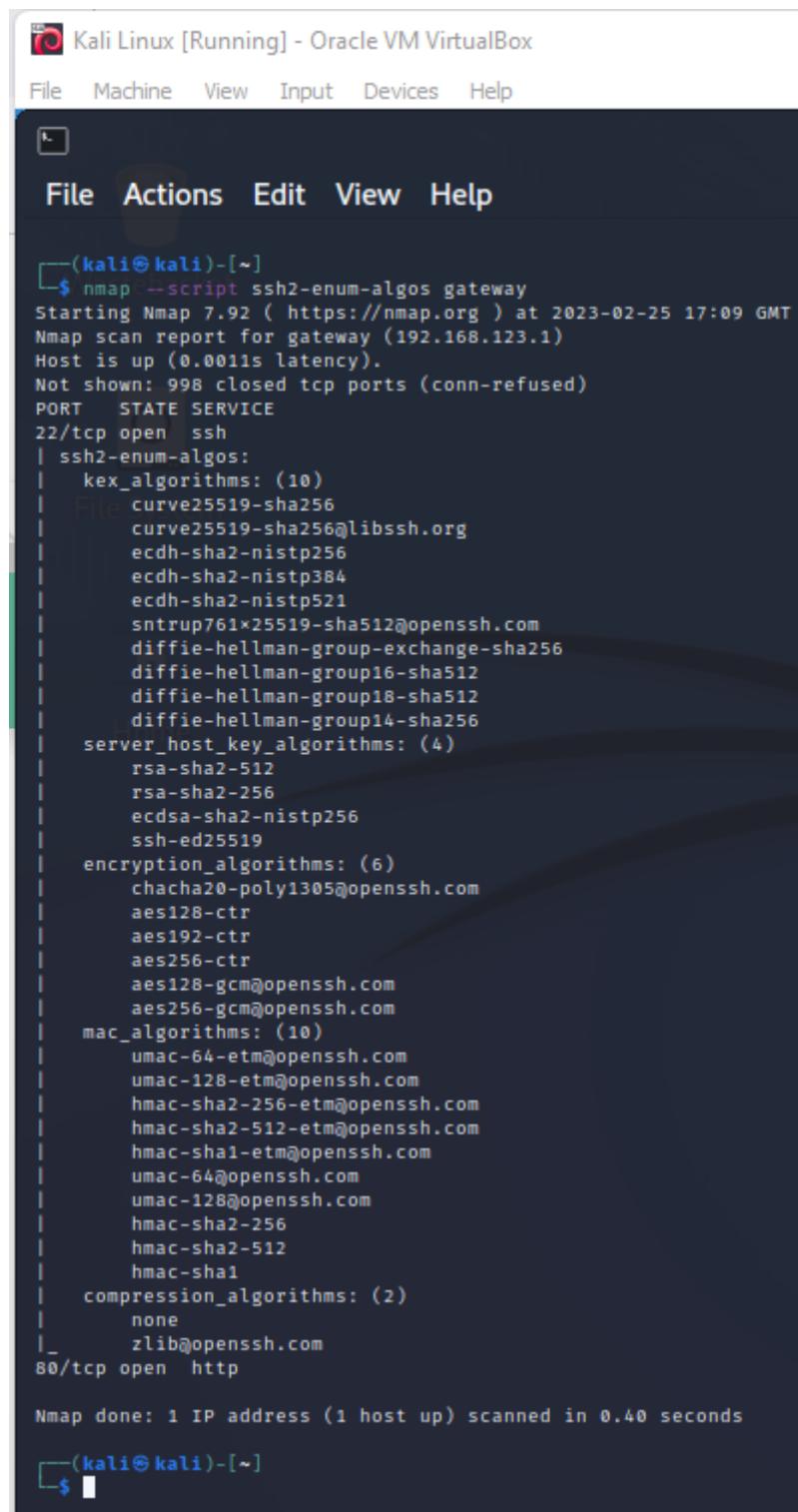
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

(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
```



The screenshot shows a terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The window contains the command-line output of an Nmap scan. The output shows a detailed breakdown of SSH2 enum-algorithms, including various key exchange, encryption, and MAC algorithms. It also lists the open port 80/tcp and its service as http. The scan was completed in 0.40 seconds.

```
(kali㉿kali)-[~]
└─$ nmap --script ssh2-enum-algos gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:09 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s 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 done: 1 IP address (1 host up) scanned in 0.40 seconds
└─$
```

```
$ 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

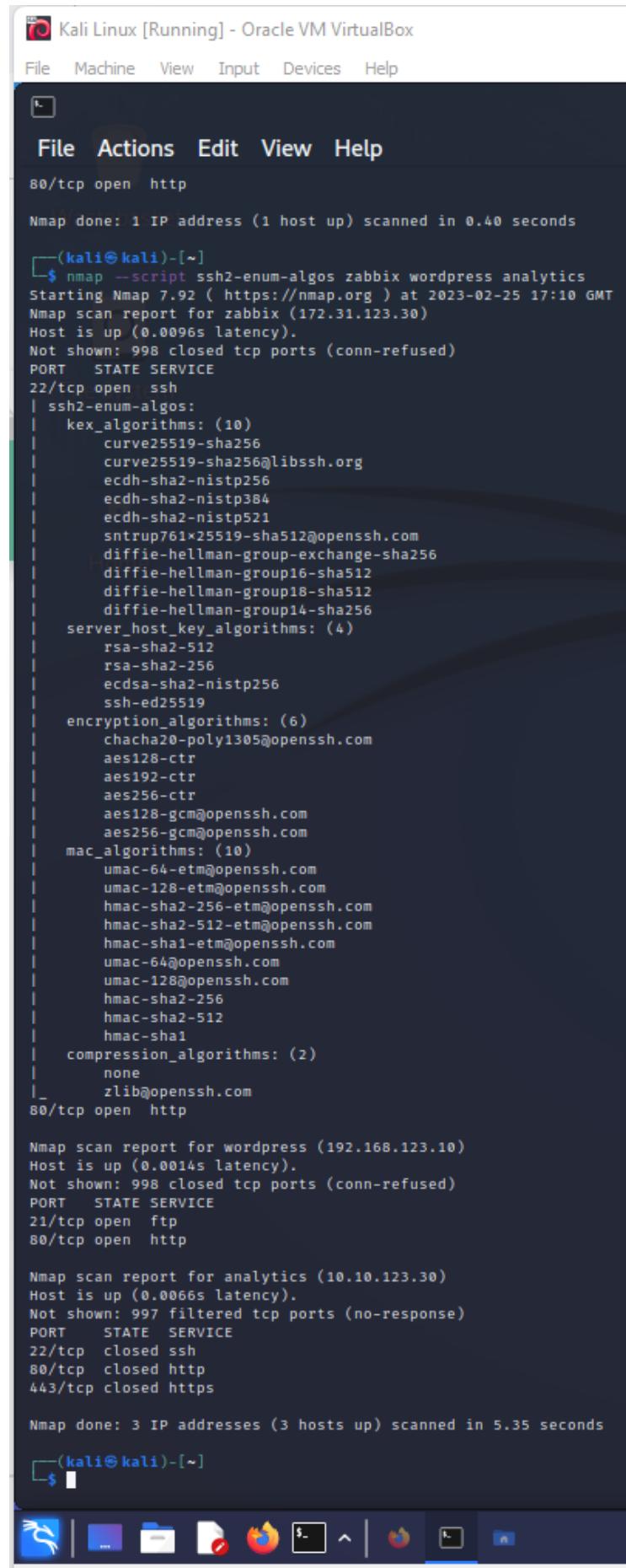
└─(kali㉿kali)-[~]
    $ nmap --script ssh2-enum-algos zabbix wordpress analytics
    Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:10 GMT
    Nmap scan report for zabbix (172.31.123.30)
    Host is up (0.0096s latency).
    Not shown: 998 closed tcp ports (conn-refused)
    PORT      STATE 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
```

```
[kali㉿kali:~] $ nmap host --script ssh-hostkey --script-args ssh_hostkey=full gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:12 GMT
Failed to resolve "host".
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0035s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|_ ecDSA-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIBmlzdHAYNTYAAABBBPpx1TBHqs2yUJgo6YZIfyuZp8u6LMc7EdUkctXNG2Ds0/yoQQQimRt8xPu3vExighqAjKQmqx57CQ7FU7NTHIE=
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIcG668t5RY27qAfI3KVR2732uuCbj1N54TTeJfxP/z2
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds

[kali㉿kali:~] $ nmap gateway --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:12 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0049s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|_ ecDSA-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIBmlzdHAYNTYAAABBBPpx1TBHqs2yUJgo6YZIfyuZp8u6LMc7EdUkctXNG2Ds0/yoQQQimRt8xPu3vExighqAjKQmqx57CQ7FU7NTHIE=
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIcG668t5RY27qAfI3KVR2732uuCbj1N54TTeJfxP/z2
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds

[kali㉿kali:~] $ nmap zabbix --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:13 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0036s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|_ ecDSA-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIBmlzdHAYNTYAAABBBPpx1TBHqs2yUJgo6YZIfyuZp8u6LMc7EdUkctXNG2Ds0/yoQQQimRt8xPu3vExighqAjKQmqx57CQ7FU7NTHIE=
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIcG668t5RY27qAfI3KVR2732uuCbj1N54TTeJfxP/z2
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds

[kali㉿kali:~] $ nmap wordpress --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:13 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0011s 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 0.39 seconds

[kali㉿kali:~] $ nmap analytics --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:13 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0027s 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: 1 IP address (1 host up) scanned in 5.04 seconds
```

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)
# And you would get your results in json
(results)
```

^G Help ^O Write Out ^W Where Is ^K Cut [Read 6 lines]
^X Exit ^R Read File ^\ Replace ^U Paste ^T Execute ^J Justify

(genmon)

/usr/share/kali-themes/xfce4-panel-genmon-vpnip.sh
Period(s): 1.00 -E Redo M-C Copy

15:08

This screenshot shows a Kali Linux desktop environment. In the background, there is a terminal window titled 'nmap.py' displaying Python code related to Nmap port scanning. In the foreground, there is a file manager window titled '(genmon)' showing a configuration file for a panel plugin. The desktop interface includes a top bar with standard system icons like network, battery, and volume, and a bottom dock with various application icons.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~

File Actions Edit View Help

```
(kali㉿kali)-[~/pythonnmap]
$ sudo nano nmap.py
[sudo] password for kali:

(kali㉿kali)-[~/pythonnmap]
$ python nmap.py
nmap.py  __pycache__
```

{'192.168.123.1': {'osmatch': {}, 'ports': [{'protocol': 'tcp', 'portid': '21', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'ftp', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '22', 'state': 'open', 'reason': 'syn-ack', 'reason_ttl': '0', 'service': {'name': 'ssh', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '23', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'telnet', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '25', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'smtp', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '80', 'state': 'open', 'reason': 'syn-ack', 'reason_ttl': '0', 'service': {'name': 'http', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '110', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'pop3', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '139', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'netbios-ssn', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '443', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'https', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '445', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'microsoft-ds', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '3389', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'ms-wbt-server', 'method': 'table', 'conf': '3'}}, {'cpe': [], 'scripts': []}], 'hostname': [{"name": "gateway", "type": "user"}], {"name": "gateway", "type": "PTR"}, {"macaddress": None, "state": {"state": "up", "reason": "syn-ack", "reason_ttl": "0"}}, {"runtime": {"time": "1677510494", "timestr": "Mon Feb 27 15:08:14 2023", "summary": "Nmap done at Mon Feb 27 15:08:14 2023; 1 IP address (1 host up) scanned in 0.07 seconds", "elapsed": "0.07", "exit": "success"}, "stats": {"scanner": "nmap", "args": "/usr/bin/nmap -v -oX --top-ports 10 gateway", "startstr": "Mon Feb 27 15:08:14 2023", "version": "7.92", "xmloutputversion": "1.05"}, "task_results": [{"task": "Ping Scan", "time": "1677510494", "extrainfo": "1 total hosts"}, {"task": "Connect Scan", "time": "1677510494", "extrainfo": "10 total ports"}]}]

```
(kali㉿kali)-[~/pythonnmap]
$ ls
nmap.py  __pycache__
```

```
(kali㉿kali)-[~/pythonnmap]
$ cd
```

```
(kali㉿kali)-[~]
$ ls
Desktop    Music          outputgateway.txt  outputzabbixbis.txt  Public      Videos
Documents  outputgateawaybisbis.xml  outputwordpress.txt  passwords.txt   pythonnmap
Downloads  outputgateawaybis.txt    outputwordpress.xml  Pictures       Templates
```

```
(kali㉿kali)-[~]
$
```

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 screenshots).

Student Name:	Tony
Student ID:	YIT19488399

#####END#####