Wrocław 01.10.2022

CYBERSECURITY

LAB 11

1. Introduction

Enumerating target is a process that is used to find and collect information about ports, operating systems, and services available on the target machines. This process is usually done after we have discovered that the target machines are available. In penetration testing practice, this task is conducted at the time of the discovery process. The goal of performing the enumeration process is to collect information about the services available on the target systems.

From the attacker's point of view, the same process is used to find weaknesses in the attacked systems that will allow them to bypass the applied security measures. In modern systems, attacks that allow breaking through security are expensive, both in terms of time and computing resources, so network reconnaissance is an important step in preparing the final attack. The development of network infrastructure and devices communicating through network protocols means that especially in corporate networks there are many elements that can be used as furs to take over data, accounts or control on the network.

Nmap (Network Mapper) is a security scanner used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run.

Please keep in mind some legal restrictions on the use of Nmap. In some countries it is prohibited by law to use tools that can be used to carry out or facilitate hacking attacks. In this case, using Nmap even to find devices on the network you are using (e.g. for testing the API of services on them) will be considered a violation of the law. At the same time, in other countries these issues are not regulated by law in any way, and sometimes using tools such as Nmap leads to litigation.

The choice of scanning parameters is also an important issue. Depending on the options used, the process may be practically undetectable, but it will last for weeks or you will get the results in seconds or minutes, but the traffic generated during the scan will be easy to notice.

Besides being used as a port scanner, Nmap has several other capabilities as follows:

- Host discovery
- Service/version detection
- Operating system detection
- Network traceroute

There are six port states that are recognized by Nmap as follows:

- **Open**: This means that there is an application accepting a TCP connection, UDP datagram, or SCTP association.
- **Closed**: This means that although the port is accessible, there is no application listening on the port.
- **Filtered**: This means that Nmap can't determine whether the port is open or not because there is a packet-filtering device blocking the probe to reach the target.
- **Unfiltered**: This means that the port is accessible, but Nmap cannot determine whether it is open or closed.

- **Open|Filtered**: This means that Nmap is unable to determine whether a port is open or filtered. This happens when a scan to open ports doesn't give a response. It can be achieved by setting the firewall to drop packets.
- **Closed|Filtered**: This means Nmap is unable to determine whether a port is closed or filtered.

In order to correctly interpret the results obtained as a result of the scan, it is necessary to remember the basic differences between connection protocols (e.g. TCP) and nonconnection protocols (e.g. UDP). As a result of the scan Nmap reports different responses depending on which connections the port is open to.

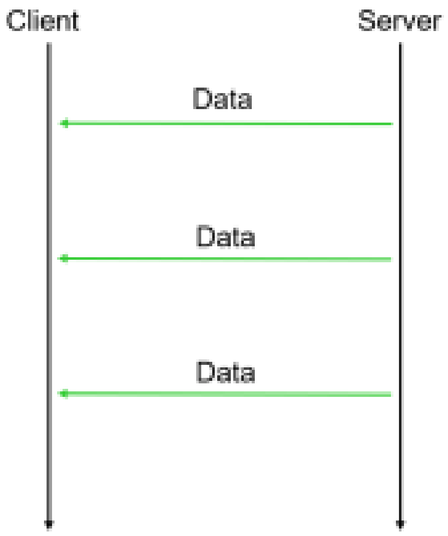


Figure 1 TCP connection

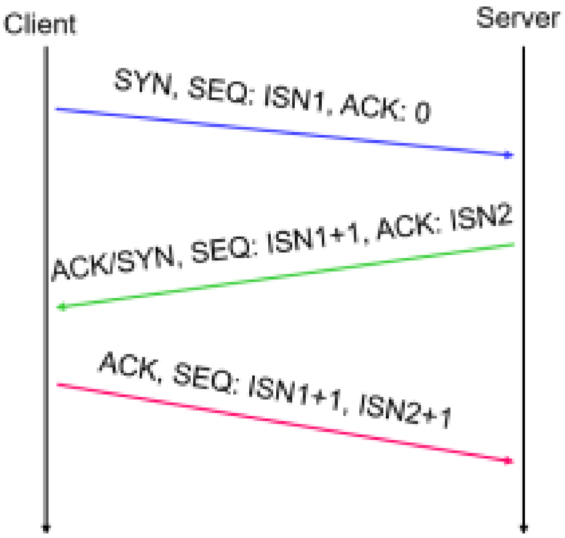


Figure 2 UDP connection

- **SYN:** The beginning of a connection
- **ACK:** Acknowledge receipt of a previous packet or transmission
- **ISN:** Initial sequence number

2. Required virtual machines

- Kali
- Metasploitable 2 or 3

3. Prerequisites

Get familiar with the following elements:

- TCP/IP protocol
- Port Scanning

The following options may be used to help you evade the firewall/IDS:

- **-f** (fragment packets):
- The purpose of this option is to make it harder to detect the packets. By specifying this option once, Nmap will split the packet into 8 bytes or less after the IP header. • **--mtu:**
- With this option, you can specify your own packet size fragmentation. The Maximum Transmission Unit (MTU) must be a multiple of eight or Nmap will give an error and exit.
- **-D** (decoy):

- By using this option, Nmap will send some of the probes from the spoofed IP addresses specified by the user. The idea is to mask the true IP address of the user in the logfiles. The user IP address is still in the logs. You can use RND to generate a random IP address or RND:number to generate the<number> IP address. The hosts you use for decoys should be up, or you will flood the target.

- Also remember that by using many decoys you can cause network congestion, so you may want to avoid that especially if you are scanning your client network. • **--source-port <portnumber> or -g** (spoof source port): This option will be useful if the firewall is set up to allow all incoming traffic that comes from a specific port. • **--data-length**:

- This option is used to change the default data length sent by Nmap in order to avoid being detected as Nmap scans.

- **--max-parallelism**: This option is usually set to one in order to instruct Nmap to send no more than one probe at a time to the target host.

- **--scan-delay** <time>: This option can be used to evade IDS/IPS that uses a threshold to detect port scanning activity.

4. Problems and questions

I. Are the results obtained by nmap reliable?

> The accuracy of the results obtained by using Nmap can vary. It depends on a number of factors such as the network conditions, target interference and the options that you select during the scan.

II. Does the information obtained about the target host depend on the scanning options?

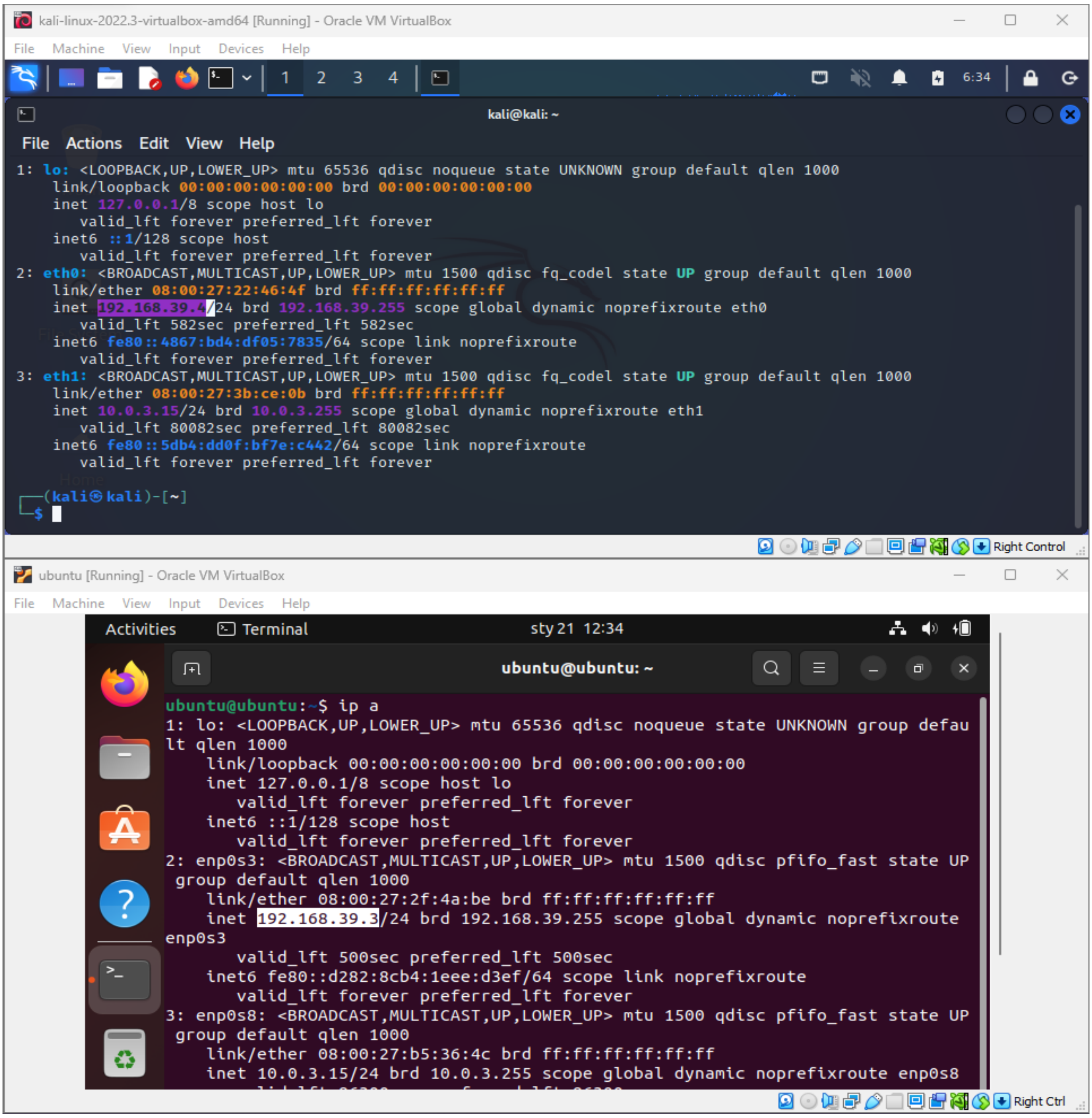
> Yes, the information that you obtain about the target host can be affected by the scanning options that you select. Different options can provide different levels of detail and accuracy.

III. Is it permitted to use nmap to scan hosts without permission?

> It is not always legal to use Nmap to scan hosts without permission, as it is considered unauthorized access to a computer system. It is always recommended to obtain proper authorization before conducting any security testing or network reconnaissance, to avoid any legal issues.

5. Tasks

I. Run all VM you have installed in VirtualBOX,

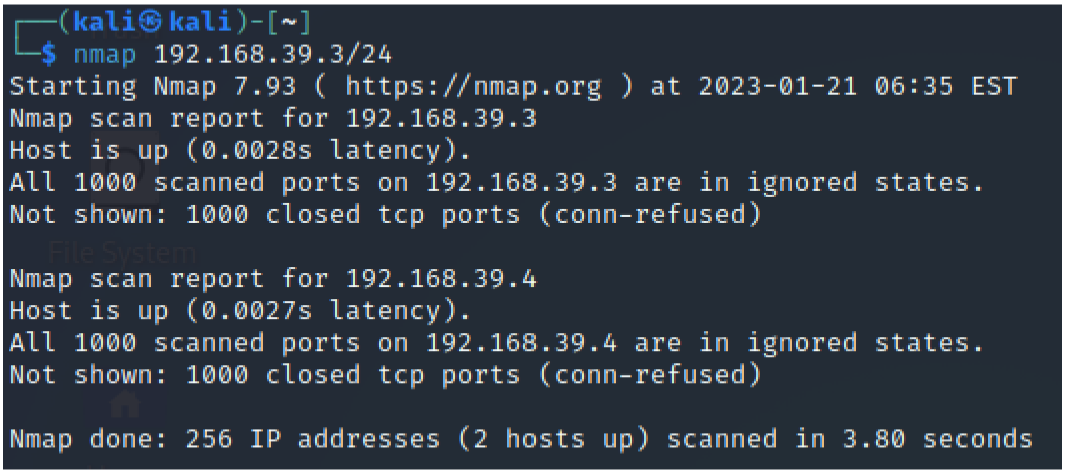

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
6:34
kali@kali: ~
File Actions Edit View Help
Right Control
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
sty 21 12:34
ubuntu@ubuntu: ~
Right Ctrl

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.39.4/24 brd 192.168.39.255 scope global dynamic noprefixroute eth0
       valid_lft 582sec preferred_lft 582sec
    inet6 fe80::4867:bd4:df05:7835/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3b:ce:0b brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
       valid_lft 80082sec preferred_lft 80082sec
    inet6 fe80::5db4:dd0f:bf7e:c442/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
 group default qlen 1000
    link/ether 08:00:27:2f:4a:be brd ff:ff:ff:ff:ff:ff
    inet 192.168.39.3/24 brd 192.168.39.255 scope global dynamic noprefixroute
enp0s3
       valid_lft 500sec preferred_lft 500sec
    inet6 fe80::d282:8cb4:1eee:d3ef/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
 group default qlen 1000
    link/ether 08:00:27:b5:36:4c brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute enp0s8
```

Execute the following command:

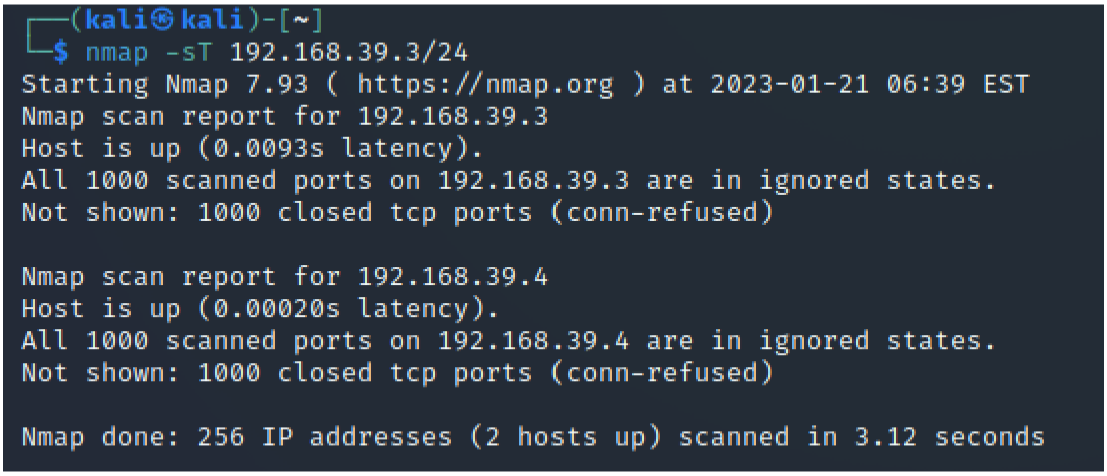
***nmap** 192.168.x.x/24* (substitute the example network address with your subnet IP range defined in your Virtual Network)



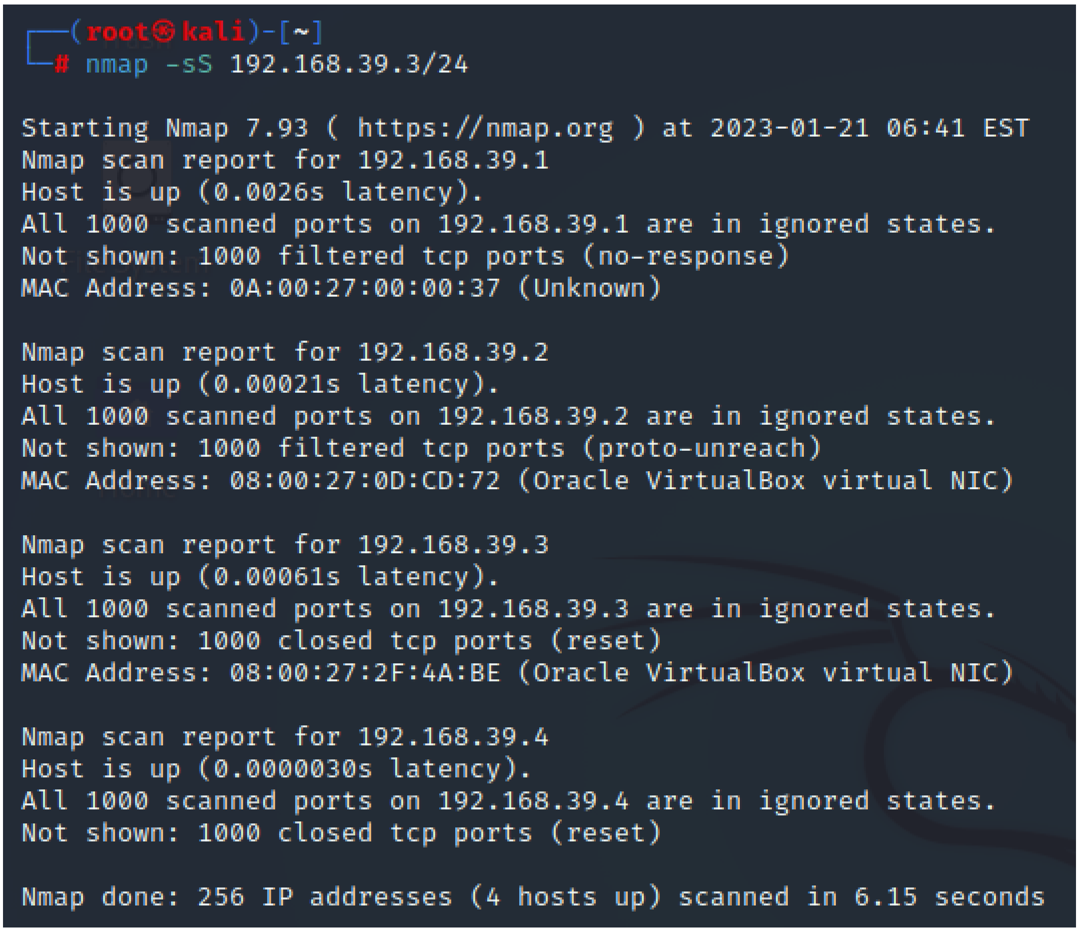
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.39.3/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:35 EST
Nmap scan report for 192.168.39.3
Host is up (0.0028s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.39.4
Host is up (0.0027s latency).
All 1000 scanned ports on 192.168.39.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.80 seconds
```

II. Execute different types of TCP scans and compare results:

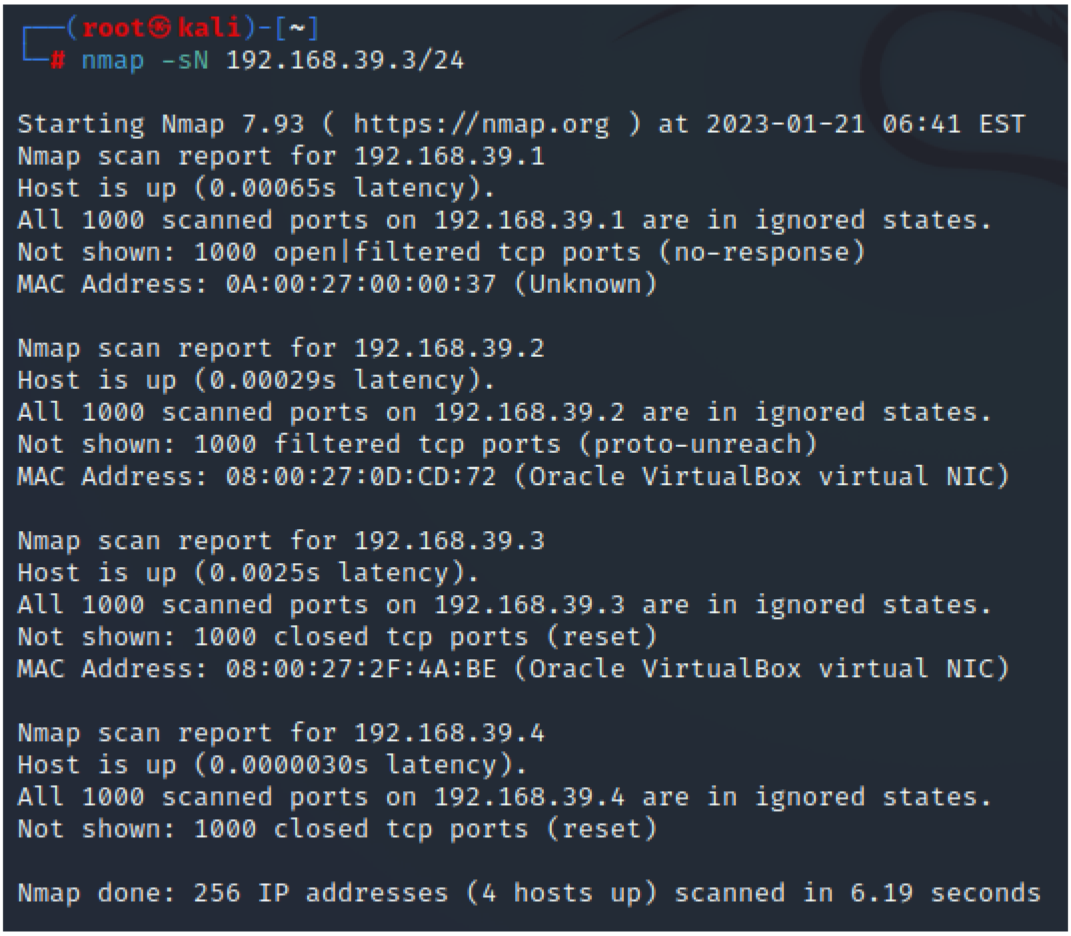
a. options -sT, -sS -sN, -sM, -sA, -sW, -sI)



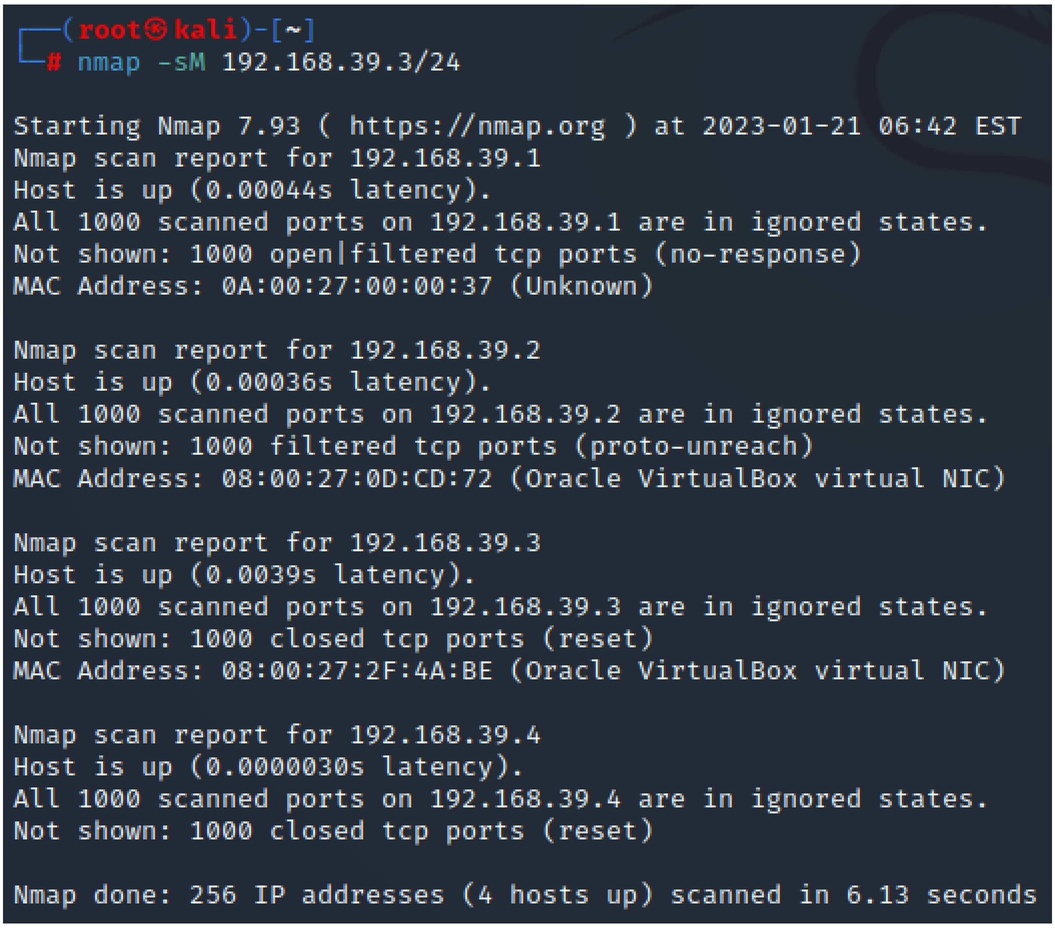
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.39.3/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:39 EST
Nmap scan report for 192.168.39.3
Host is up (0.0093s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.39.4
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.39.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.12 seconds
```



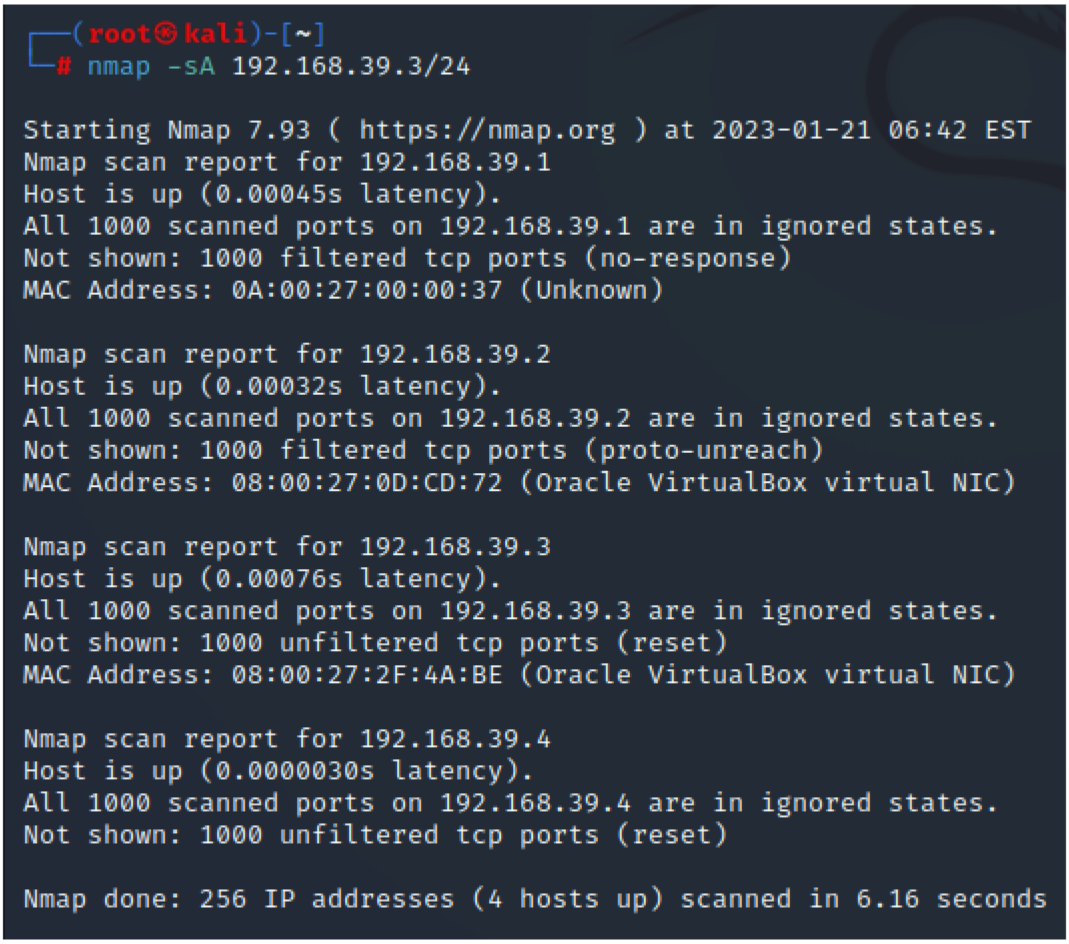
```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.39.3/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:41 EST
Nmap scan report for 192.168.39.1
Host is up (0.0026s latency).
All 1000 scanned ports on 192.168.39.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:37 (Unknown)

Nmap scan report for 192.168.39.2
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.39.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:0D:CD:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.3
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.4
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.39.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.15 seconds
```



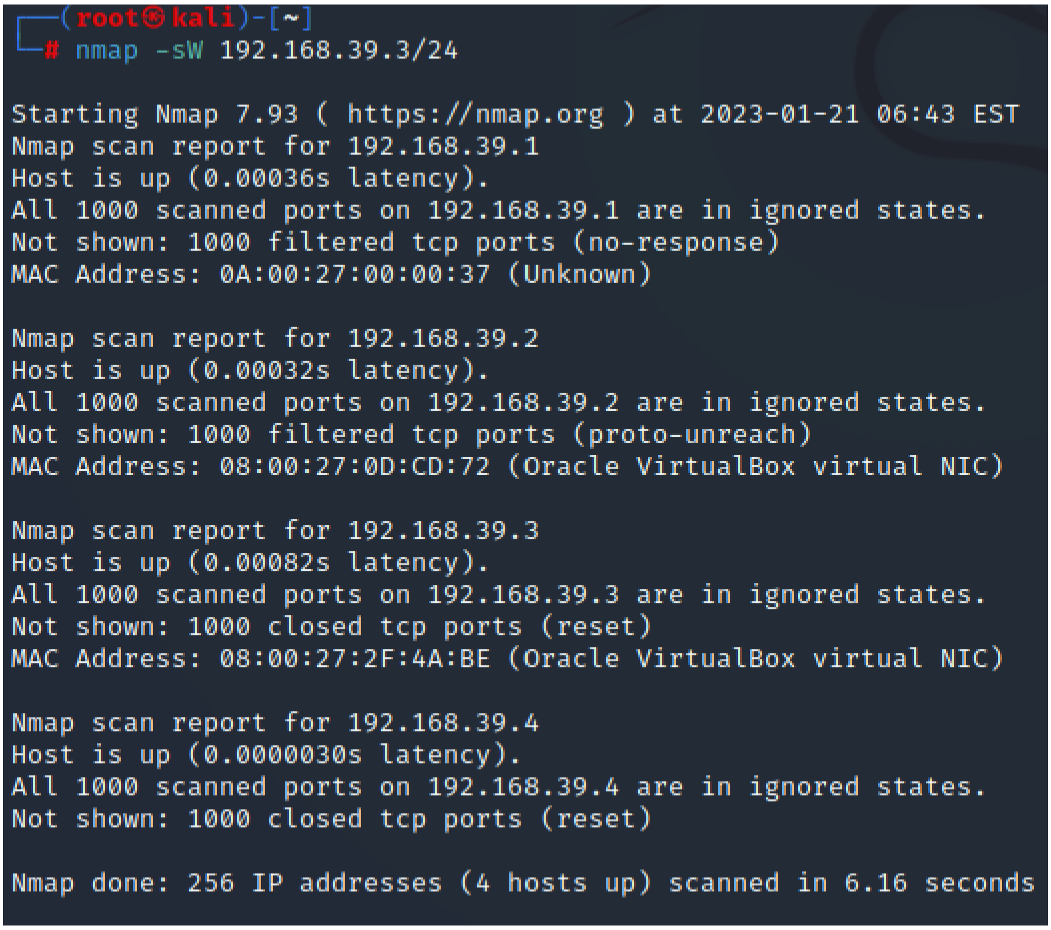
```
┌──(root㉿kali)-[~]
└─# nmap -sN 192.168.39.3/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:41 EST
Nmap scan report for 192.168.39.1
Host is up (0.00065s latency).
All 1000 scanned ports on 192.168.39.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:37 (Unknown)

Nmap scan report for 192.168.39.2
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.39.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:0D:CD:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.3
Host is up (0.0025s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.4
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.39.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.19 seconds
```



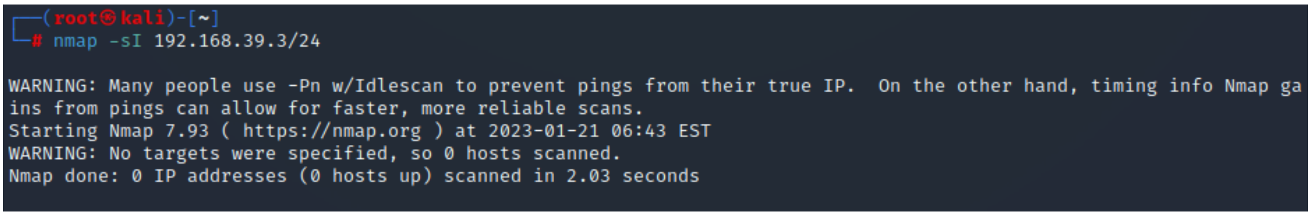
```
┌──(root㉿kali)-[~]
└─# nmap -sM 192.168.39.3/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:42 EST
Nmap scan report for 192.168.39.1
Host is up (0.00044s latency).
All 1000 scanned ports on 192.168.39.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:37 (Unknown)

Nmap scan report for 192.168.39.2
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.39.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:0D:CD:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.3
Host is up (0.0039s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.4
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.39.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.13 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.39.3/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:42 EST
Nmap scan report for 192.168.39.1
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.39.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:37 (Unknown)

Nmap scan report for 192.168.39.2
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.39.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:0D:CD:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.3
Host is up (0.00076s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.4
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.39.4 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.16 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sW 192.168.39.3/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:43 EST
Nmap scan report for 192.168.39.1
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.39.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:37 (Unknown)

Nmap scan report for 192.168.39.2
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.39.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:0D:CD:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.3
Host is up (0.00082s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.4
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.39.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.16 seconds
```



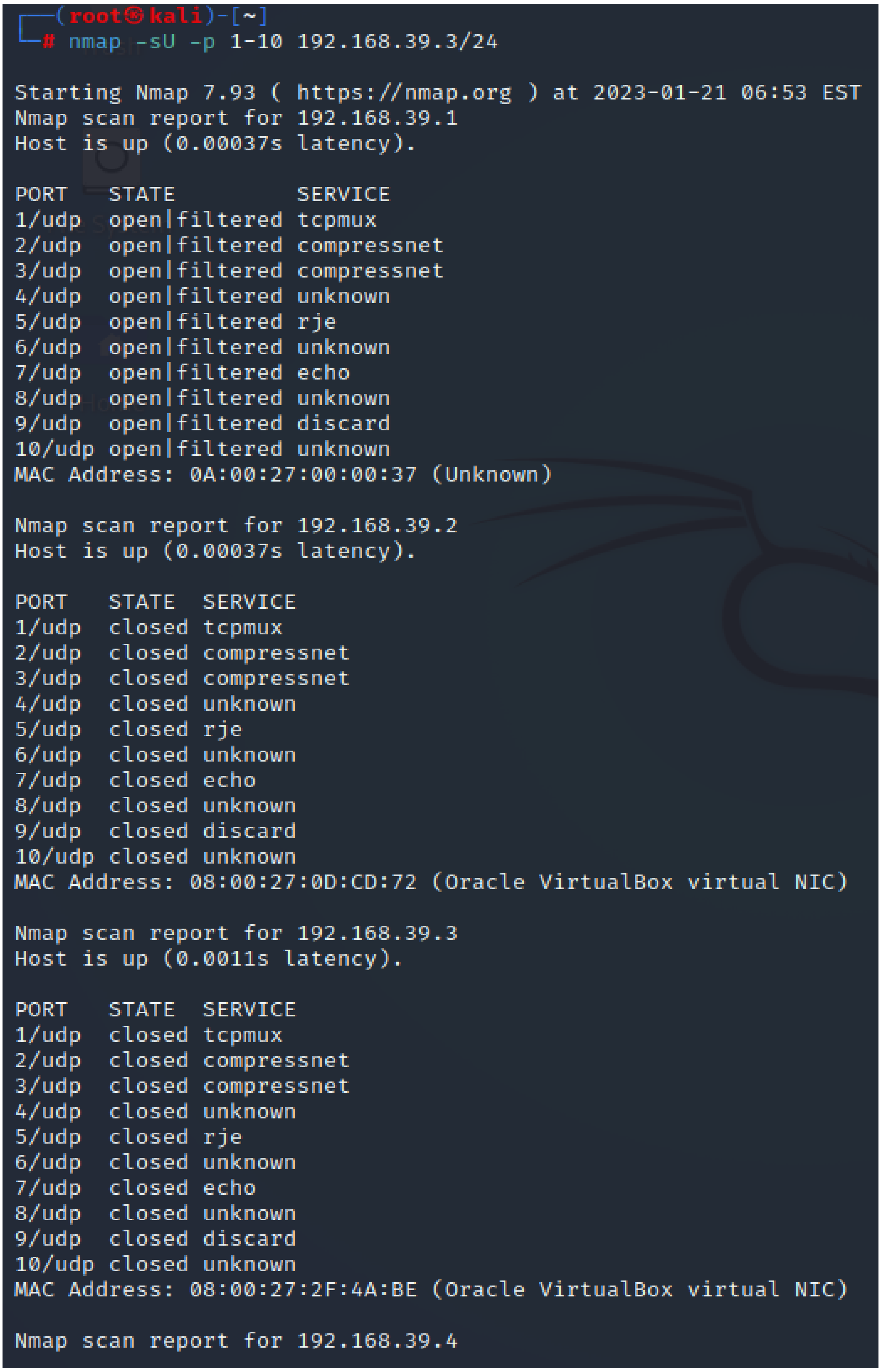
```
┌──(root㉿kali)-[~]
└─# nmap -sI 192.168.39.3/24

WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, timing info Nmap ga
ins from pings can allow for faster, more reliable scans.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:43 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.03 seconds
```

b. describe the differences between scanning with aforementioned options

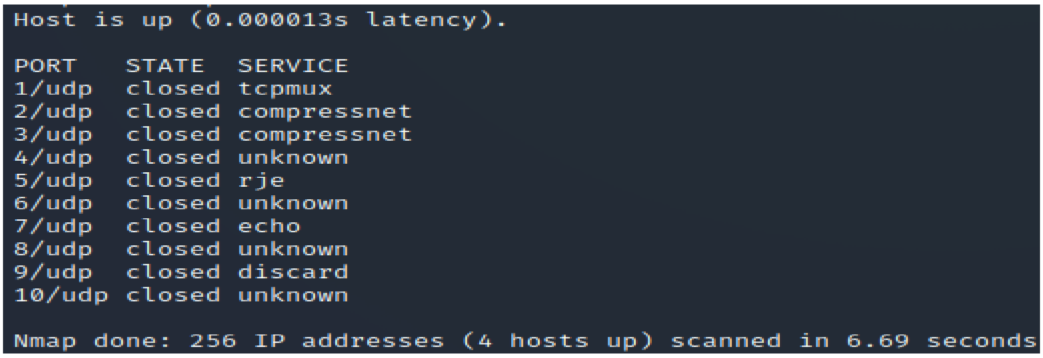
> Options -sT, -sS, -sN, -sM, -sA, -sW, and -sI uses a unique method to gather information about open ports on the target host. For example, one option may use the full TCP connection process to determine if a port is open, while another option may use a "zombie" host to scan the target host. Each option has its own advantages and disadvantages.

III. Execute UDP scan

> Since there was no port open i went with first 100 ports,



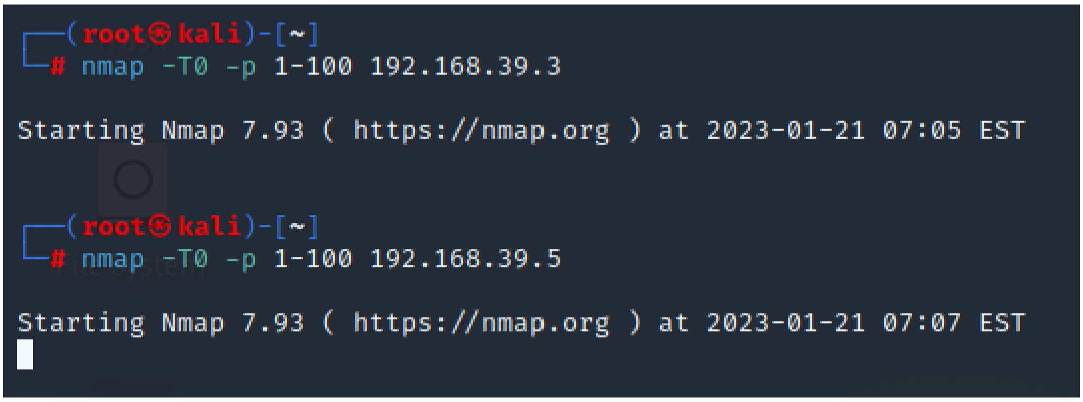
```
┌──(root㉿kali)-[~]
└─# nmap -sU -p 1-10 192.168.39.3/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:53 EST
Nmap scan report for 192.168.39.1
Host is up (0.00037s latency).

PORT   STATE         SERVICE
1/udp  open|filtered tcpmux
2/udp  open|filtered compressnet
3/udp  open|filtered compressnet
4/udp  open|filtered unknown
5/udp  open|filtered rje
6/udp  open|filtered unknown
7/udp  open|filtered echo
8/udp  open|filtered unknown
9/udp  open|filtered discard
10/udp open|filtered unknown
MAC Address: 0A:00:27:00:00:37 (Unknown)

Nmap scan report for 192.168.39.2
Host is up (0.00037s latency).

PORT   STATE  SERVICE
1/udp  closed tcpmux
2/udp  closed compressnet
3/udp  closed compressnet
4/udp  closed unknown
5/udp  closed rje
6/udp  closed unknown
7/udp  closed echo
8/udp  closed unknown
9/udp  closed discard
10/udp closed unknown
MAC Address: 08:00:27:0D:CD:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.3
Host is up (0.0011s latency).

PORT   STATE  SERVICE
1/udp  closed tcpmux
2/udp  closed compressnet
3/udp  closed compressnet
4/udp  closed unknown
5/udp  closed rje
6/udp  closed unknown
7/udp  closed echo
8/udp  closed unknown
9/udp  closed discard
10/udp closed unknown
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.39.4
```



```
Host is up (0.000013s latency).

PORT   STATE  SERVICE
1/udp  closed tcpmux
2/udp  closed compressnet
3/udp  closed compressnet
4/udp  closed unknown
5/udp  closed rje
6/udp  closed unknown
7/udp  closed echo
8/udp  closed unknown
9/udp  closed discard
10/udp closed unknown

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.69 seconds
```

IV. Try different nmap timing options (-T) from a set of values 0,1,2,3,4,5. What is the difference in results and performance?

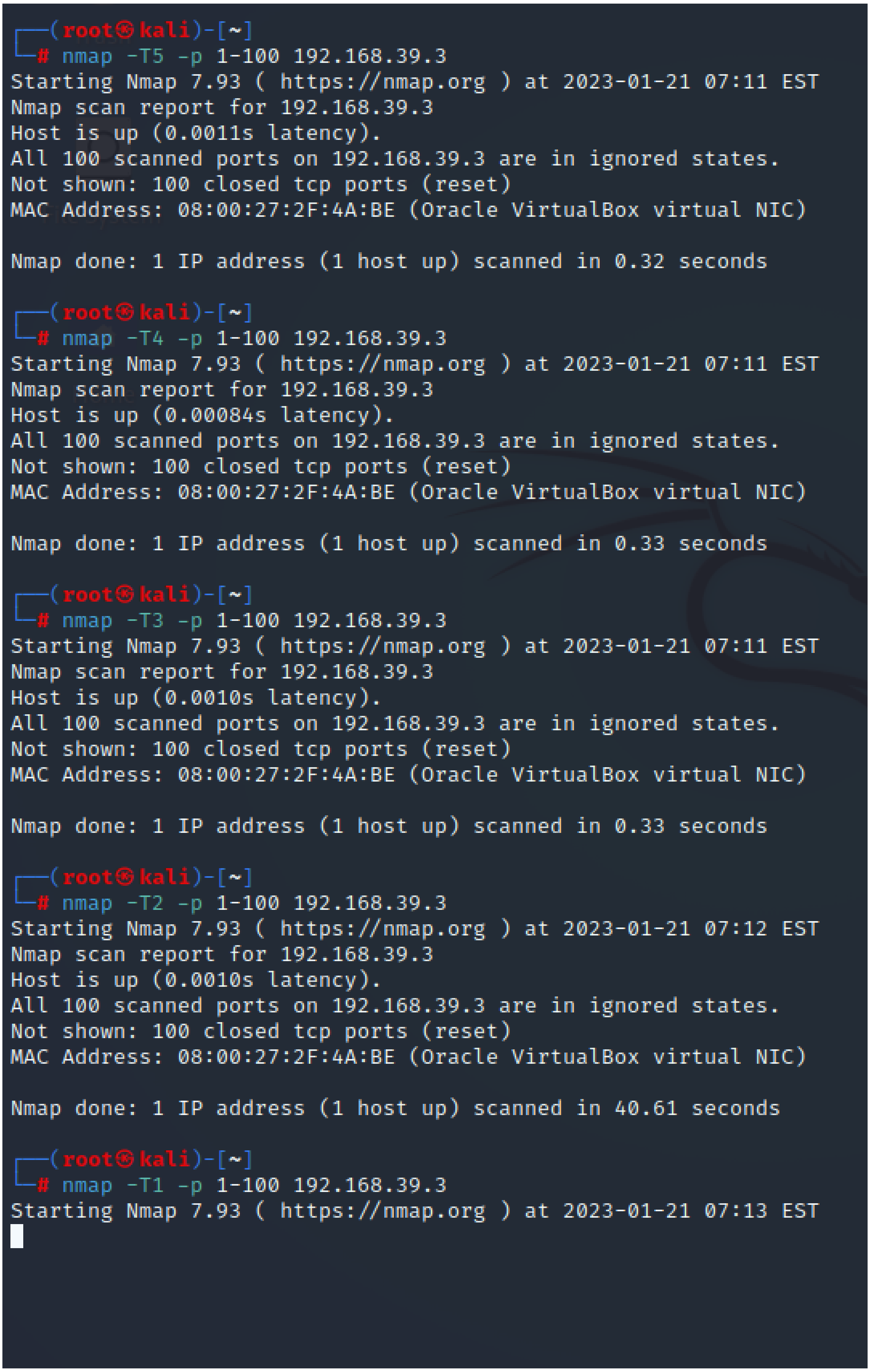
>



```
┌──(root㉿kali)-[~]
└─# nmap -T0 -p 1-100 192.168.39.3

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:05 EST


┌──(root㉿kali)-[~]
└─# nmap -T0 -p 1-100 192.168.39.5

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:07 EST
█
```

For -T0 it just keeps loading for ubuntu or metasploitable!

Well judging by this experiment & some quick search the more number we use the faster i sends packets and we can see the time difference to check the first 100 packets :

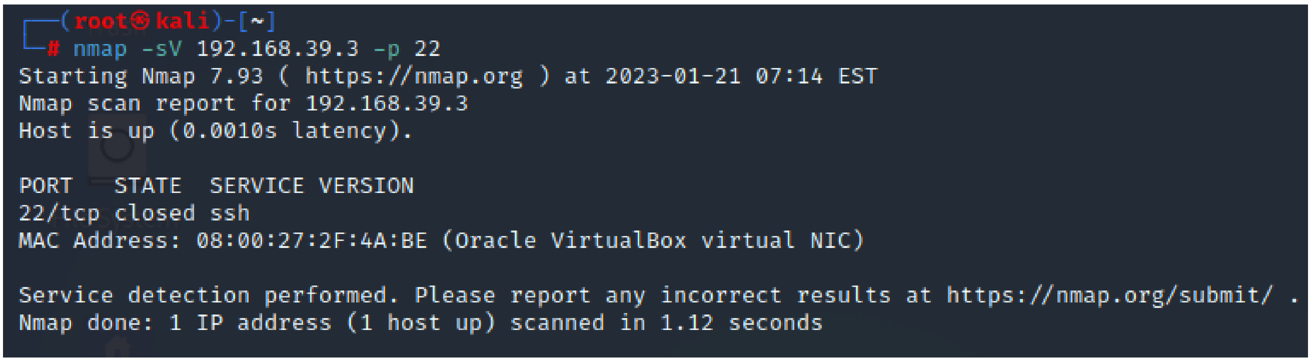


```
┌──(root㉿kali)-[~]
└─# nmap -T5 -p 1-100 192.168.39.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:11 EST
Nmap scan report for 192.168.39.3
Host is up (0.0011s latency).
All 100 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

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

┌──(root㉿kali)-[~]
└─# nmap -T4 -p 1-100 192.168.39.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:11 EST
Nmap scan report for 192.168.39.3
Host is up (0.00084s latency).
All 100 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

┌──(root㉿kali)-[~]
└─# nmap -T3 -p 1-100 192.168.39.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:11 EST
Nmap scan report for 192.168.39.3
Host is up (0.0010s latency).
All 100 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

┌──(root㉿kali)-[~]
└─# nmap -T2 -p 1-100 192.168.39.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:12 EST
Nmap scan report for 192.168.39.3
Host is up (0.0010s latency).
All 100 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 40.61 seconds

┌──(root㉿kali)-[~]
└─# nmap -T1 -p 1-100 192.168.39.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:13 EST
```

V. For selected system and selected service use service version detection (-sV) eg.

nmap -sV 192.168.x.x -p 22

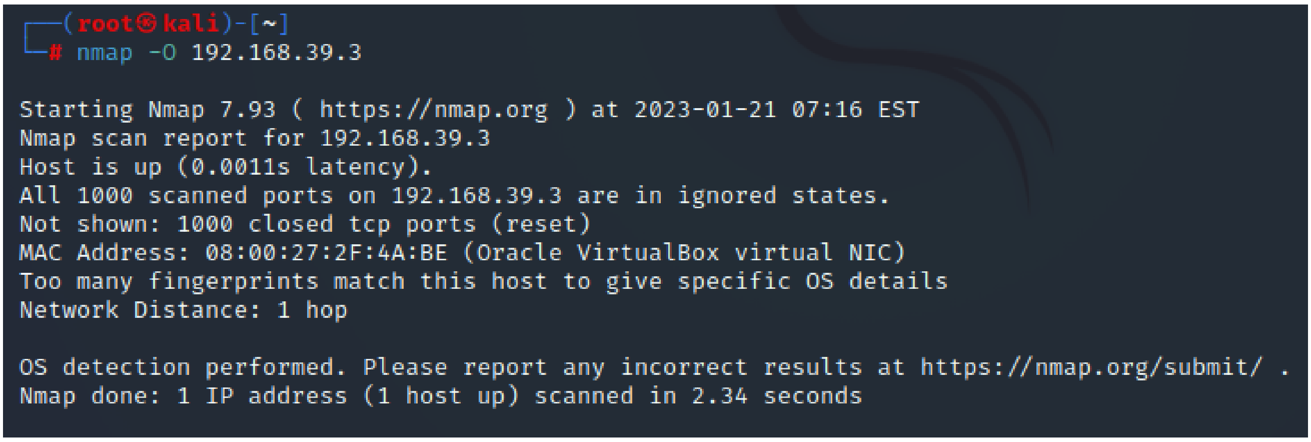
>



```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.39.3 -p 22
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:14 EST
Nmap scan report for 192.168.39.3
Host is up (0.0010s latency).

PORT   STATE  SERVICE VERSION
22/tcp closed ssh
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

VI. Try to discover the operating system version installed on VMs (option –O)

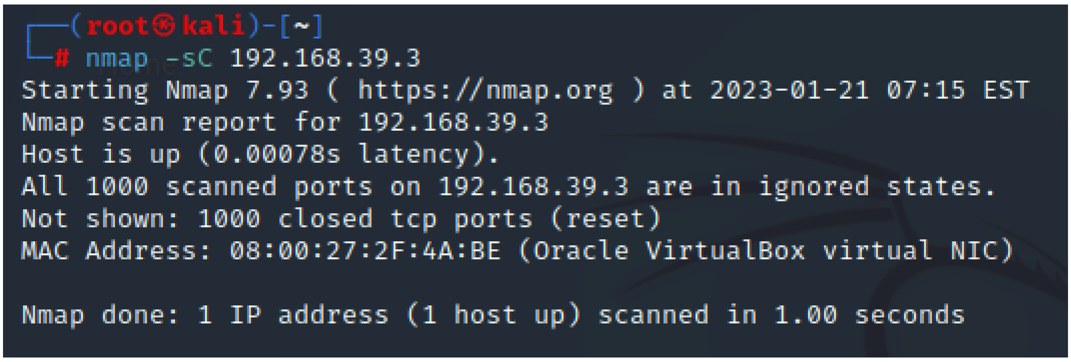
>



```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.39.3

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:16 EST
Nmap scan report for 192.168.39.3
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 2.34 seconds
```

VII. Check the directory /usr/share/nmap/scripts and find a few various nmap scripts and describe their application

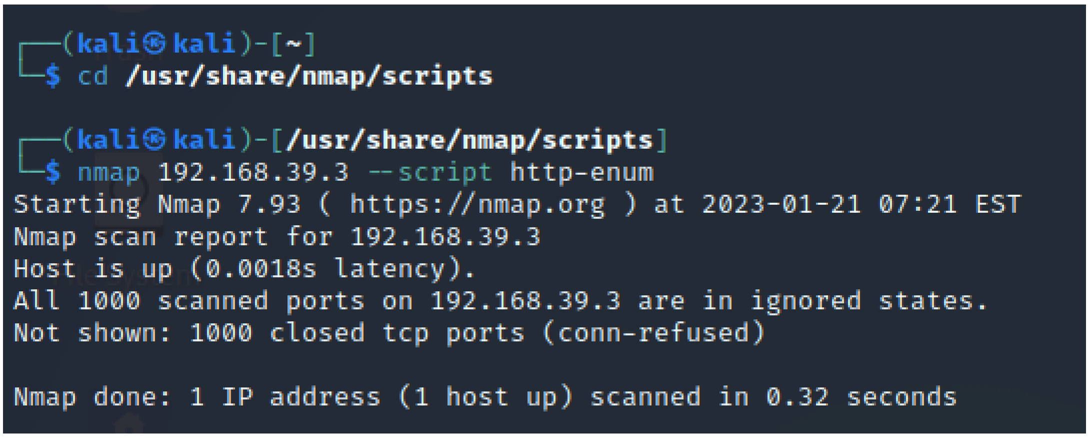
a. Execute nmap -sC 192.168.56.103 (change the IP address)



```
┌──(root㉿kali)-[~]
└─# nmap -sC 192.168.39.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:15 EST
Nmap scan report for 192.168.39.3
Host is up (0.00078s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2F:4A:BE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

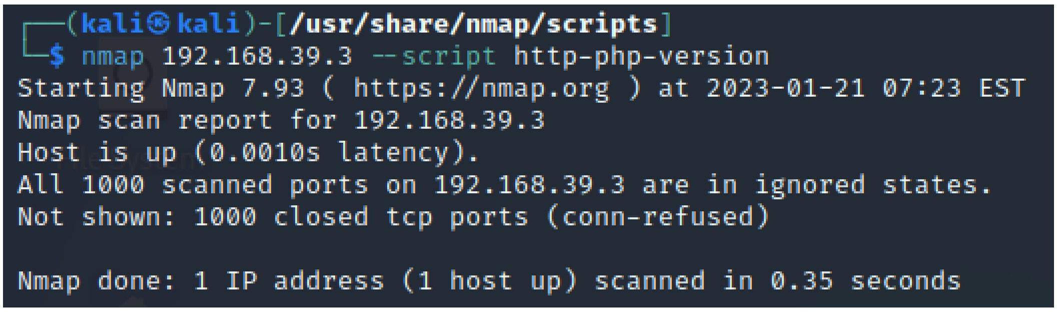
>

b. Execute nmap --script http-enum,http-headers,http-methods,http-phpversion



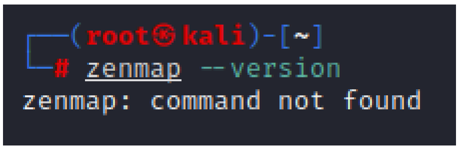
```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/nmap/scripts

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap 192.168.39.3 --script http-enum
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:21 EST
Nmap scan report for 192.168.39.3
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

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

>



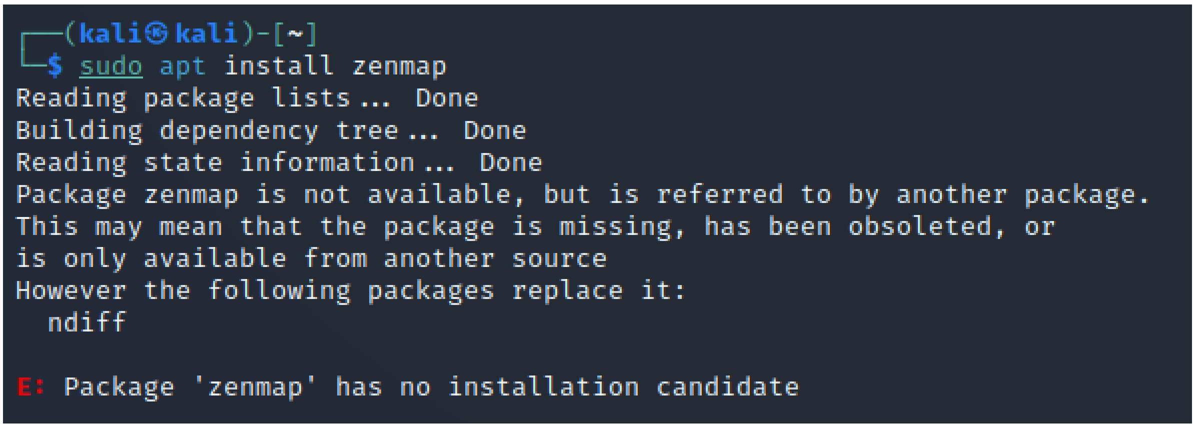
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap 192.168.39.3 --script http-php-version
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 07:23 EST
Nmap scan report for 192.168.39.3
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.39.3 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

VIII. Use Zenmap to discover the Virtual Network structure and VMs operating systems and active services



```
┌──(root㉿kali)-[~]
└─# zenmap --version
zenmap: command not found
```

>



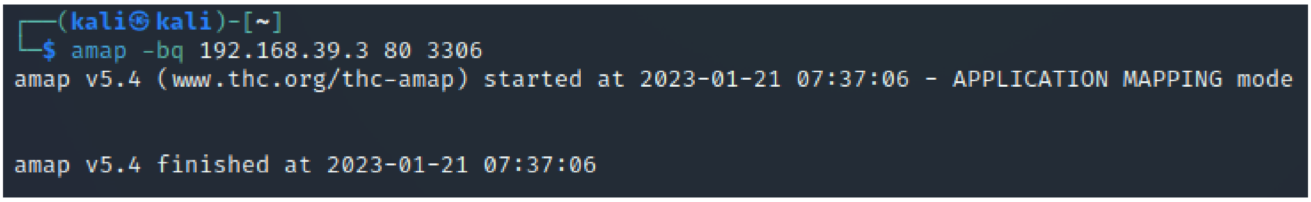
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zenmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package zenmap is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source
However the following packages replace it:
  ndiff

E: Package 'zenmap' has no installation candidate
```

It should be auto installed yet there was error installing

I tried few methods.

IX. Use amap tool against selected VM and compare the results with those obtained during nmap scan

amap -bq 192.168.x.x 80 3306



```
┌──(kali㉿kali)-[~]
└─$ amap -bq 192.168.39.3 80 3306
amap v5.4 (www.thc.org/thc-amap) started at 2023-01-21 07:37:06 - APPLICATION MAPPING mode


amap v5.4 finished at 2023-01-21 07:37:06
```