Assignment 2 – Part I (Multiple choice, OSI Model Fundamentals)

Q-1. According to the OSI model, at which of the following layers internet Protocol(IP) addresses are assigned?

A. Session
B. Data link
C. Presentation
D. Network

Q-2. Which of the following is the correct sequence of layers in the OSI Model (From lowest layers to highest)?

A. Physical, Network, Data link, Session, Transport, Presentation, Application
B. Physical, Data link, Network, Transport, Session, Presentation, Application
C. Transport, Session, Data link, Application, Presentation, Network, Physical
D. Physical, Data link, Network, Transport, Presentation, Session, Application

Q-3. According to the OSI Which layer Performs parity checking and Error Detection?

A. Session
B. Data Link
C. Presentation
D. Physical

Q-4. Which of the Following Layers of OSI Model Does Ethernet Operate?

A. Physical
B. Data Link
C. Network
D. Transport
E. Both Physical and Data link layer
F. Both Physical and Network Layers

Q-5. According to the OSI Model which layer is responsible for Routing?

A. Session
B. Data link
C. Presentation
D. Network

Q-6. According to the OSI model which layer handles the LAN switching?

A. Session
B. Data link
C. Presentation
D. Network

Q-7. At which Layer of OSI Model Does a Network Bridges and Switches operate?

A. Network
B. Physical
C. Session
D. Data Link

Q-8. According to the OSI model, which Layer is responsible for Sending Acknowledgements of Successful data transfer?

A. Session
B. Transport
C. Data Link
D. Presentation

Q-9. According to the OSI model, which Layer organizes data bits into small data units called frames?

A. Network
B. Data link
C. Transport
D. Physical

Q-10. When Compared to OSI model, the functionality of which of the two sub layers is incorporated in the application layer of TCP/IP model?

A. Session and Presentation
B. Transport and Session
C. Session and Physical
D. Presentation and Data link

Q-11. Which Layer is Broken Down into MAC and LLC Sub layers?

A. Network
B. Data Link
C. Session
D. Physical

Q-12. According to the OSI model ,which layer provides services such as file transfer, data base access and email, Remote login to hosts?

A. Application
B. Presentation
C. Session
D. Data link

Q-13. At which Layer of OSI Model Does HUB operate?

A. Network
B. Physical
C. Session
D. Data Link

Q-14. Which Layer of OSI model Corresponds to TCP

A. Network
B. Transport
C. Session
D. Data Link

Q-15. Which OSI layer is responsible for data encryption and decryption?

A. Physical Layer
B. Data Link Layer
C. Presentation Layer
D. Transport Layer

Q-16. In the OSI model, which layer is responsible for routing and logical addressing?

A. Network Layer
B. Session Layer
C. Data Link Layer
D. Transport Layer

Q-17. Which OSI layer is responsible for establishing, maintaining, and terminating connections?

A. Physical Layer
B. Data Link Layer
C. Transport Layer
D. Session Layer

Q-18. What is the primary function of the Transport Layer in the OSI model?

A. Data encryption
B. Error detection and correction
C. End-to-end communication
D. Physical medium control

Q-19. Which OSI layer is responsible for error detection and correction at the bit level?

A. Data Link Layer
B. Network Layer
C. Transport Layer
D. Session Layer

Q-20. Which layer is responsible for segmenting data into smaller packets and reassembling them at the destination in the OSI model?

A. Physical Layer
B. Data Link Layer
C. Transport Layer
D. Presentation Layer

Q-21. What is the primary function of the Data Link Layer?

A. Logical addressing
B. End-to-end communication
C. Flow control and error checking
D. Routing

Q-22. Which OSI layer is responsible for translating data between different character encodings and data formats?

A. Presentation Layer
B. Network Layer
C. Transport Layer
D. Application Layer

Q-23. Which OSI layer is responsible for checking whether data has been received correctly and requesting retransmission if necessary?

A. Transport Layer
B. Network Layer
C. Data Link Layer
D. Presentation Layer

Q-24. Which OSI layer deals with the physical transmission of data over the network medium?

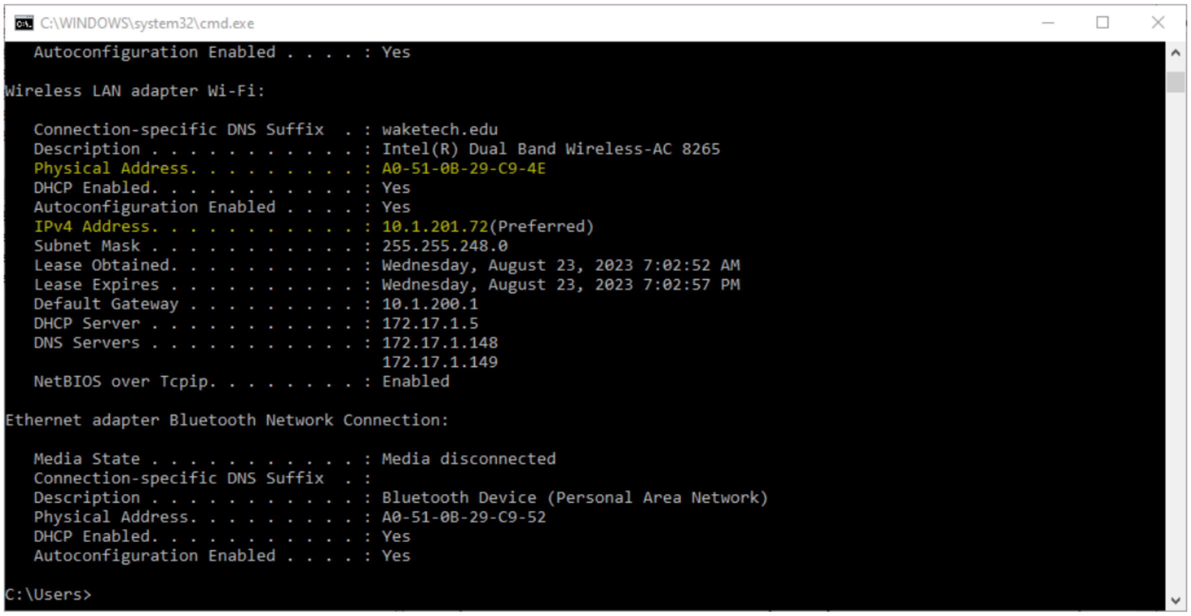
A. Data Link Layer
B. Network Layer
C. Transport Layer
D. Physical Layer

Q-25. What is the primary role of the Session Layer in the OSI model?

A. Error checking
B. Session management and synchronization
C. Data encryption
D. Logical addressing

Assignment 2 – Part II (Free Response)

Suppose you are given the following display:



```
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : waketech.edu
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : A0-51-0B-29-C9-4E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.1.201.72(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 23, 2023 7:02:52 AM
   Lease Expires . . . . . . . . . . : Wednesday, August 23, 2023 7:02:57 PM
   Default Gateway . . . . . . . . . : 10.1.200.1
   DHCP Server . . . . . . . . . . . : 172.17.1.5
   DNS Servers . . . . . . . . . . . : 172.17.1.148
                                       172.17.1.149
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : A0-51-0B-29-C9-52
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users>
```

What is the MAC (Physical) address of our network interface?___________________________

What is the IPv4 address of our network interface?_____________________________________

What is the IPv4 address of the Default Gateway?______________________________________

As a hint, when you Run an "ipconfig /all" to get the IPv4 address and the MAC address this is the screen that generally appears. On Kali Linux, "sudo ifconfig" produces a similar display.

Assignment 2 – Part 3 (Create a Shell Script for Port Scanning with Nmap)

Example – Creating your first shell script, in any open root terminal

```
┌──(root💀kali)-[/home/kali/Downloads/scripts]

└─# mkdir scripts

┌──(root💀kali)-[/home/kali/Downloads/scripts]

└─# cd scripts

┌──(root💀kali)-[/home/kali/Downloads/scripts]

└─# touch script.sh

┌──(root💀kali)-[/home/kali/Downloads/scripts]

└─# echo 'echo hello-world' >> script.sh

┌──(root💀kali)-[/home/kali/Downloads/scripts]

└─# chmod -R 777 .

┌──(root💀kali)-[/home/kali/Downloads/scripts]

└─# ./script.sh
```

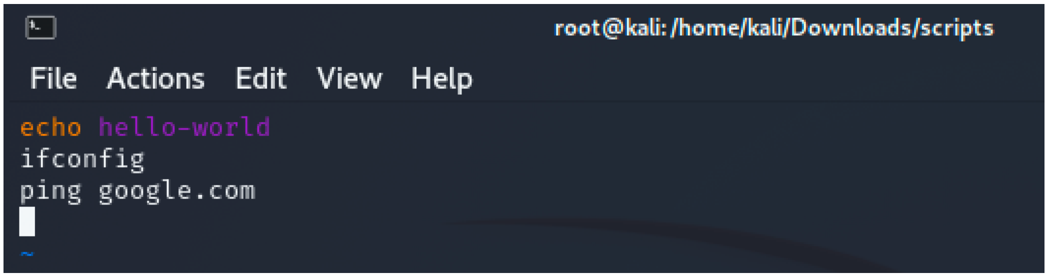
Adding commands to your shell script is a sinch; afterwards, simply vim into your script and add the commands that interest you.

For example,

To add ifconfig and ping you may perform the following operations:

```
┌──(root💀kali)-[/home/kali/Downloads/scripts]

└─#  vim script.sh
```


root@kali: /home/kali/Downloads/scripts
File Actions Edit View Help

```
echo hello-world
ifconfig
ping google.com

~
```

Afterwards, hit the “Esc” key followed by typing :wq to save and quit out. Afterwards, running

```
┌──(root💀kali)-[/home/kali/Downloads/scripts]
└─# ./script.sh
```

Will produce ifconfig results along with packets taken from google.com.

To complete this assignment, develop a custom script that incorporates 3 of the 15 Nmap commands (see next page for details); explain your choices and how these three processes together achieve a larger goal for detecting vulnerabilities on your system – use your knowledge of OSI layers to justify your responses with respect to what Nmap looks through – for example, what layer would expect to find ports on? Ethernet connections, etc…

Please create .txt file for submission and a sufficient explanation (2-3 paragraphs) of the tools and IP address ranges you chose to scan, for example, 127.0.0.1 or 10.0.2.15/24 among many other possibilities. Hint: in the commands below <target> is a generic place holder for IP addresses you wish to look through (e.g, 10.0.2.15/24, 127.0.0.1, etc…), you may choose to customize these as you wish, and I would highly recommend setting these up to be run whenever you are casually inspecting your network traffic to find immediate vulnerabilities on your system on startup.

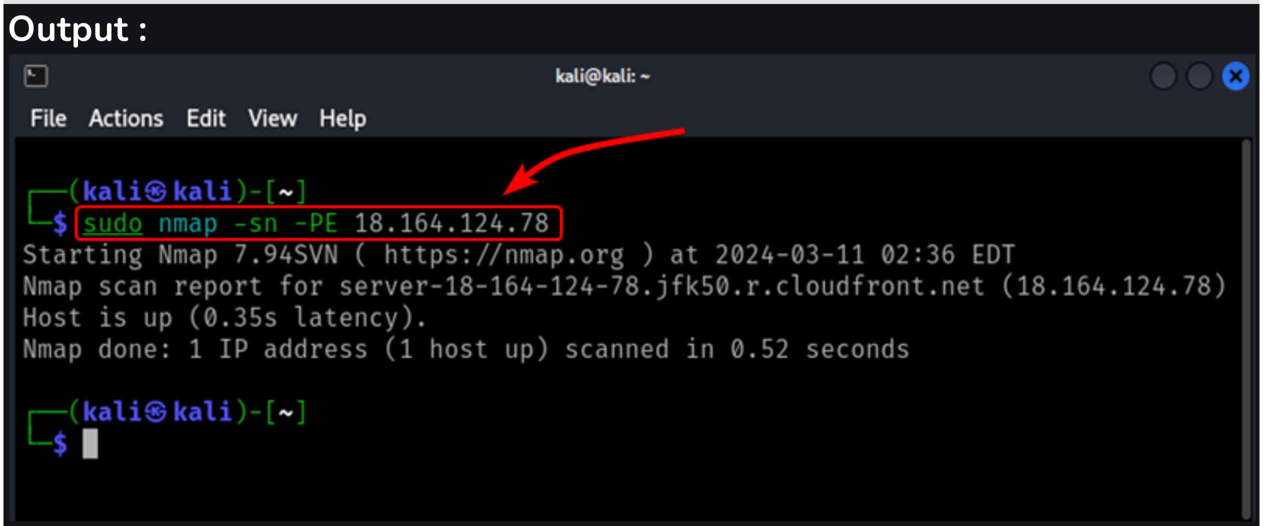
1. Active Reconnaissance with Nmap Command

The Following command is used to perform a ping scan on the specified target to determine which hosts are online or active. So when you run this command, Nmap will send ICMP Echo (ping) requests to all IP addresses in the specified target range. The hosts that respond to these ping requests are considered alive or active, and their IP addresses will be displayed in the output.

Command :

```
sudo nmap -sn -PE <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 18.164.124.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 02:36 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.78)
Host is up (0.35s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

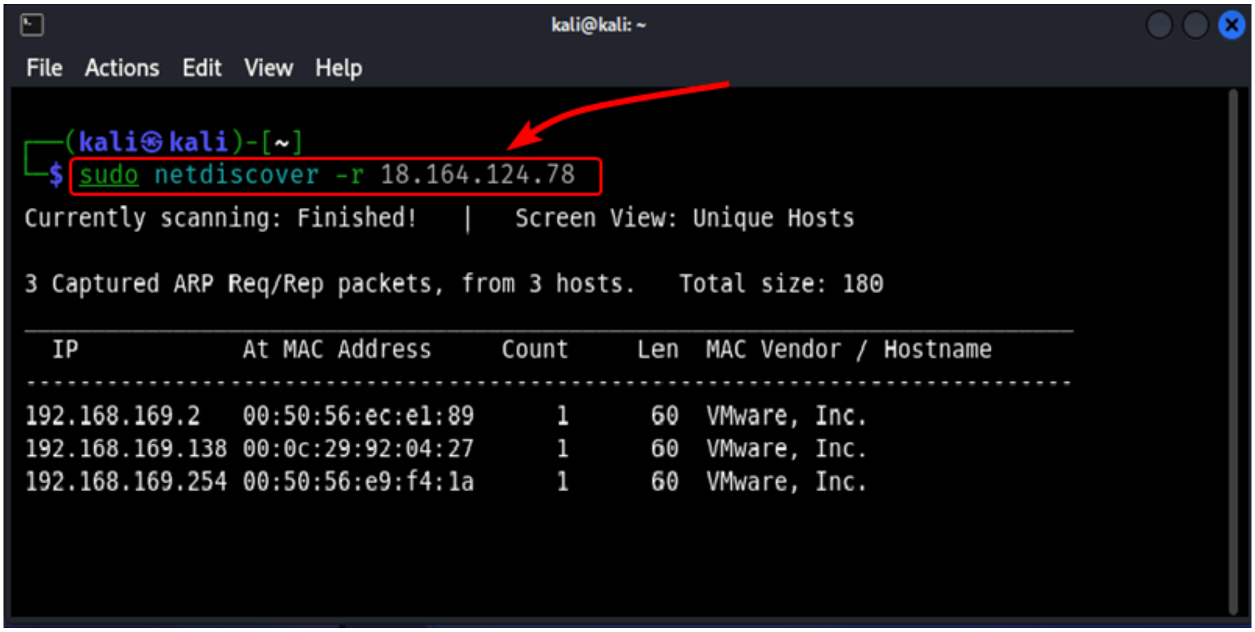
2. Find Alive Hosts with Netdiscover

The following command is used to scan for active devices or hosts on the local network using ARP requests. When you run this command, netdiscover will continuously send ARP requests to all IP addresses within the specified target range. Any active device on the network that receives the ARP request will respond with its MAC address and IP address.

Command :

```
sudo netdiscover -r <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -r 18.164.124.78
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.169.2   00:50:56:ec:e1:89      1      60  VMware, Inc.
192.168.169.138 00:0c:29:92:04:27      1      60  VMware, Inc.
192.168.169.254 00:50:56:e9:f4:1a      1      60  VMware, Inc.
```

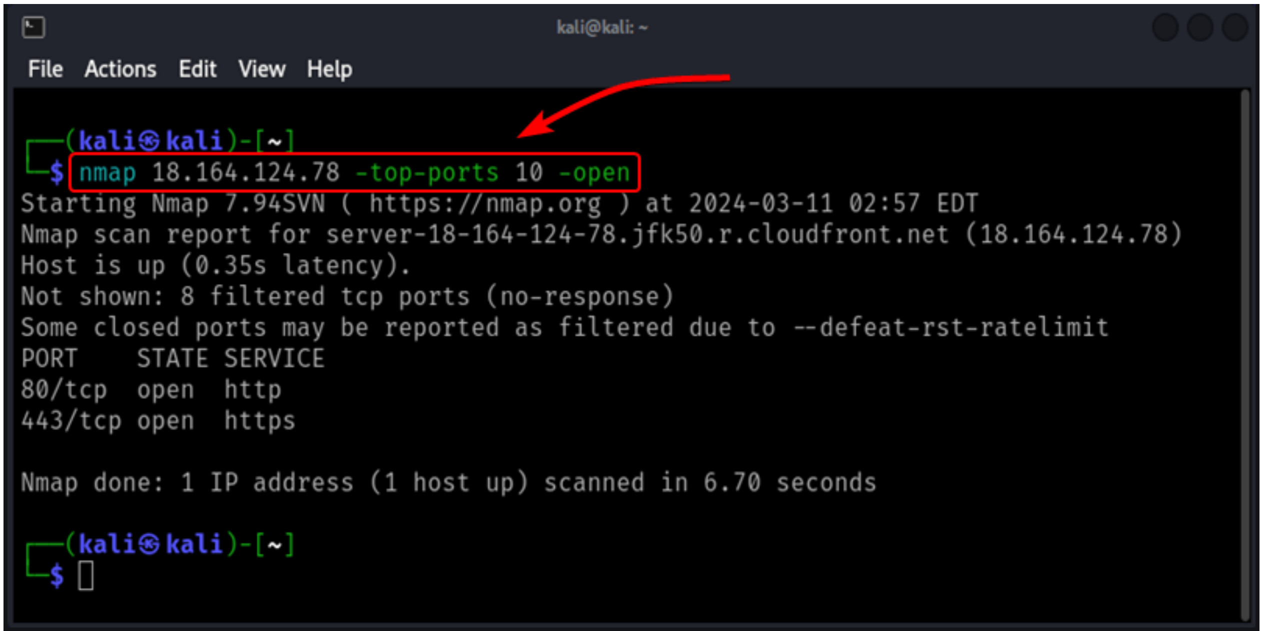
3. Find Top 10 Open Ports with Nmap (Fast Scan)

The Following nmap command is used to perform a quick scan on the specified target to identify the top 10 most commonly used open ports. When you run this command, Nmap will scan the specified target(s) and check the 10 most commonly used ports (such as 21, 22, 23, 25, 80, 110, 143, 443, 3306, and 3389) to see if they are open or listening for incoming connections. The output will display a list of the open ports found on the target(s), along with some basic information about the associated services or applications running on those ports.

Command :

```
nmap <target> –top-ports 10 –open
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap 18.164.124.78 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 02:57 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.78)
Host is up (0.35s latency).
Not shown: 8 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

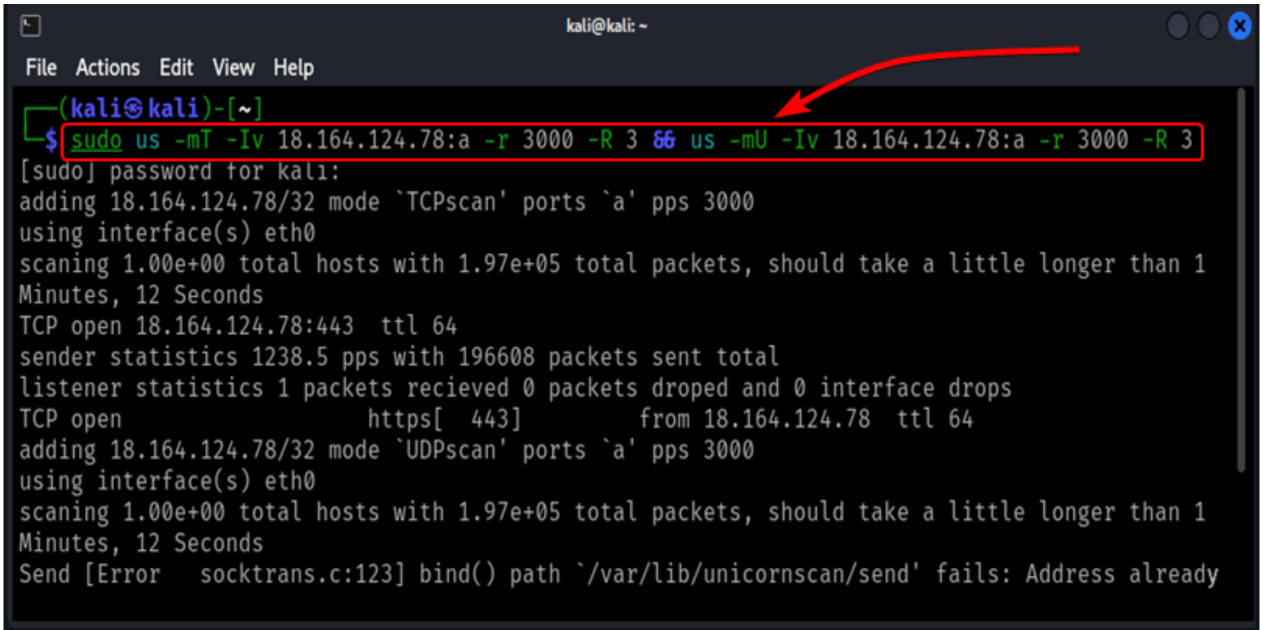
4. Scanning with Unicornscan

The Following command is a combination of two separate commands using the "unicornscan". At, first It will Scan the specified target IP range for open TCP ports at a rate of 3000 packets per second, with verbose output, retrying up to 3 times for each port. After the TCP scan finishes, it will scan the same target IP range for open UDP ports, also at 3000 packets per second, with verbose output and up to 3 retries.

Command :

```
sudo us -mT -Iv <target>:a -r 3000 -R 3 && us -mU -Iv <target>:a -r 3000 -R 3
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ sudo us -mT -Iv 18.164.124.78:a -r 3000 -R 3 && us -mU -Iv 18.164.124.78:a -r 3000 -R 3
[sudo] password for kali:
adding 18.164.124.78/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1
Minutes, 12 Seconds
TCP open 18.164.124.78:443  ttl 64
sender statistics 1238.5 pps with 196608 packets sent total
listener statistics 1 packets recieved 0 packets droped and 0 interface drops
TCP open                 https[  443]         from 18.164.124.78  ttl 64
adding 18.164.124.78/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1
Minutes, 12 Seconds
Send [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/send' fails: Address already
```

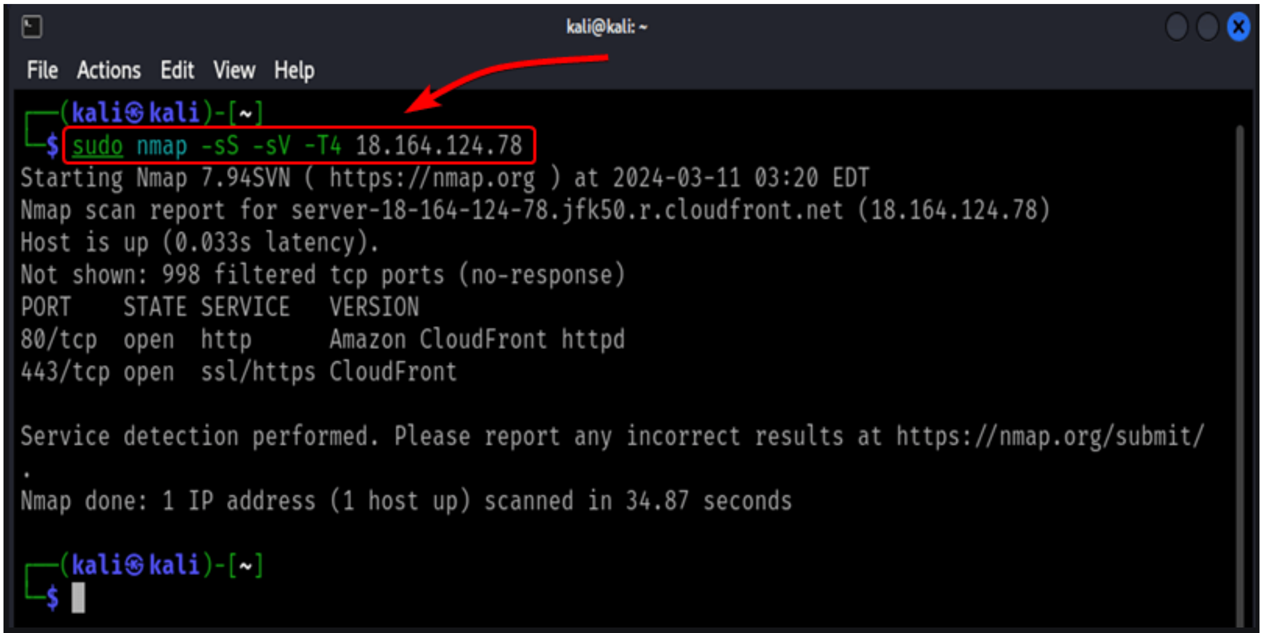
5. TCP Syn Scan with Nmap

The Following nmap command is used to perform a stealthy TCP scan and service/version detection on the specified target, with increased speed. When you run this command, Nmap will perform a SYN scan on the specified target(s) to find open TCP ports. For each open port, it will then try to determine the service or application running on that port, along with its version information.

Command :

```
sudo nmap -sS -sV -T4 <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 18.164.124.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 03:20 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.78)
Host is up (0.033s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Amazon CloudFront httpd
443/tcp open  ssl/https CloudFront

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 34.87 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

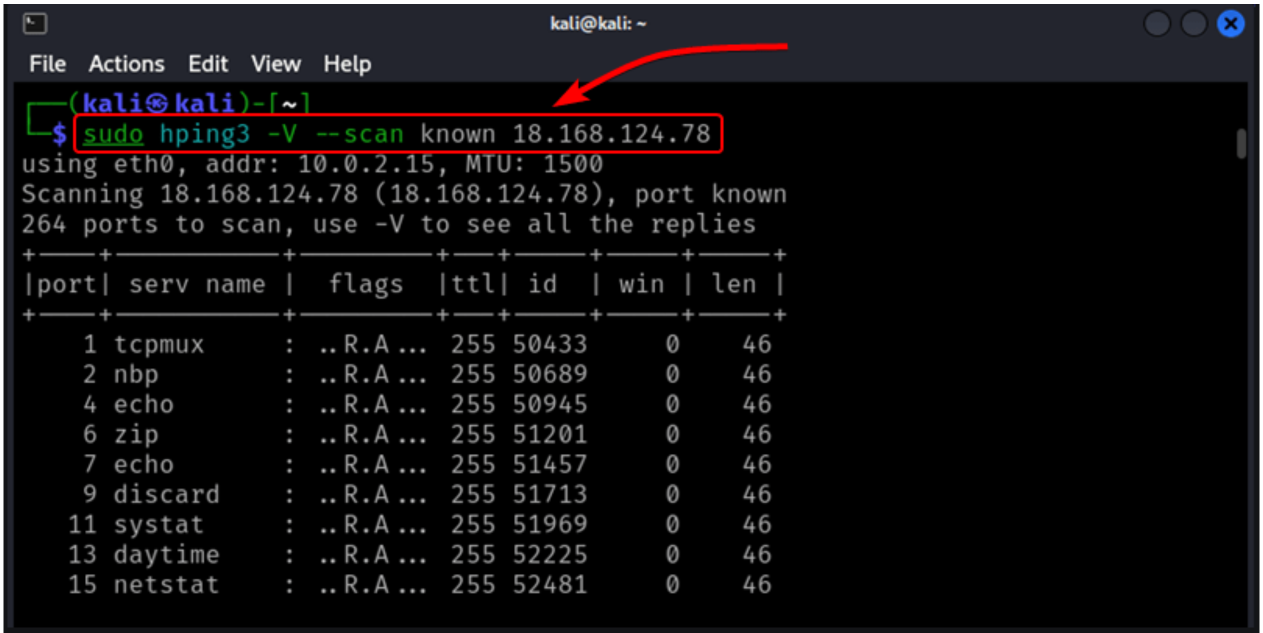
6. Scanning with HPING3

The following hping3 command will --scan known <target> is used to perform a basic TCP scan on the specified target using the hping3 utility in Kali Linux. When you run this command, hping3 will send TCP connection requests to all well-known ports (ports 1-1024) on the specified target. The output will display the open ports found on the target system.

Command :

```
hping3 –scan known <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -V --scan known 18.168.124.78
using eth0, addr: 10.0.2.15, MTU: 1500
Scanning 18.168.124.78 (18.168.124.78), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
    1 tcpmux     : ..R.A... 255 50433     0    46
    2 nbp        : ..R.A... 255 50689     0    46
    4 echo       : ..R.A... 255 50945     0    46
    6 zip        : ..R.A... 255 51201     0    46
    7 echo       : ..R.A... 255 51457     0    46
    9 discard    : ..R.A... 255 51713     0    46
   11 systat     : ..R.A... 255 51969     0    46
   13 daytime    : ..R.A... 255 52225     0    46
   15 netstat    : ..R.A... 255 52481     0    46
```

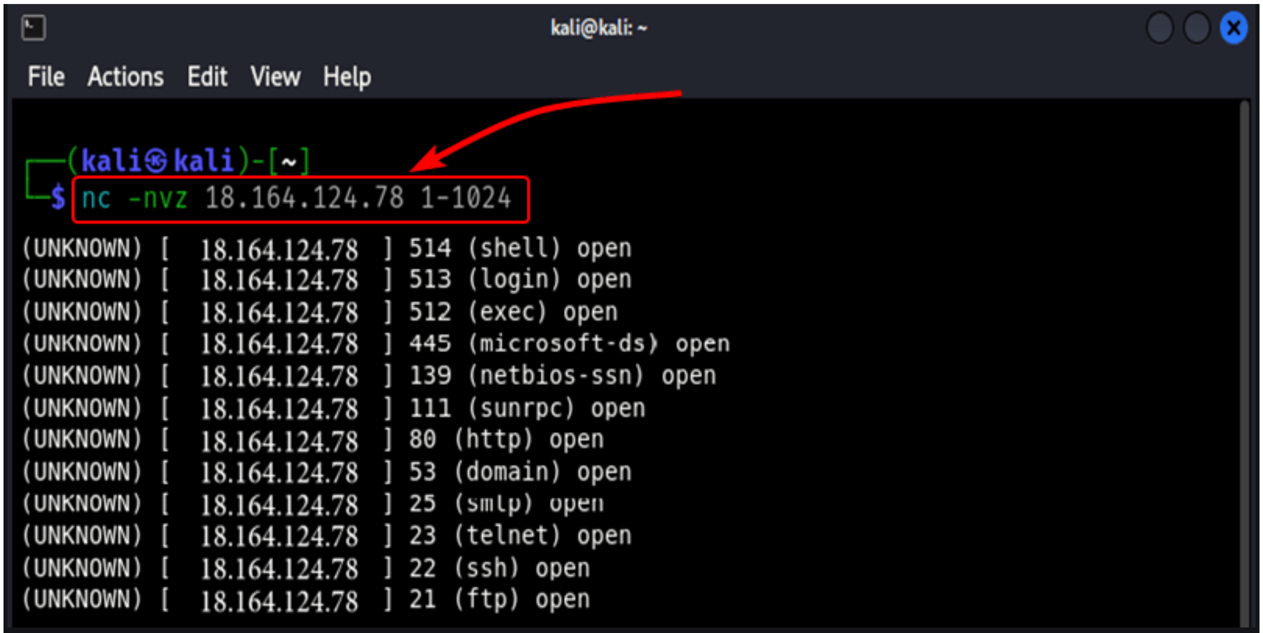
7. Port Scanning with Netcat

The following nc command is used to perform a TCP port scan on the specified target using the nc (netcat) tool in Kali Linux. When you run this command, nc will attempt to connect to each TCP port in the range 1-1024 on the specified target. If a port is open and accepting connections, nc will report it as "open". If the port is closed or filtered, it will report it as "closed".

Command :

```
nc -nvz <target> 1-1024
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 18.164.124.78 1-1024
(UNKNOWN) [ 18.164.124.78 ] 514 (shell) open
(UNKNOWN) [ 18.164.124.78 ] 513 (login) open
(UNKNOWN) [ 18.164.124.78 ] 512 (exec) open
(UNKNOWN) [ 18.164.124.78 ] 445 (microsoft-ds) open
(UNKNOWN) [ 18.164.124.78 ] 139 (netbios-ssn) open
(UNKNOWN) [ 18.164.124.78 ] 111 (sunrpc) open
(UNKNOWN) [ 18.164.124.78 ] 80 (http) open
(UNKNOWN) [ 18.164.124.78 ] 53 (domain) open
(UNKNOWN) [ 18.164.124.78 ] 25 (smtp) open
(UNKNOWN) [ 18.164.124.78 ] 23 (telnet) open
(UNKNOWN) [ 18.164.124.78 ] 22 (ssh) open
(UNKNOWN) [ 18.164.124.78 ] 21 (ftp) open
```

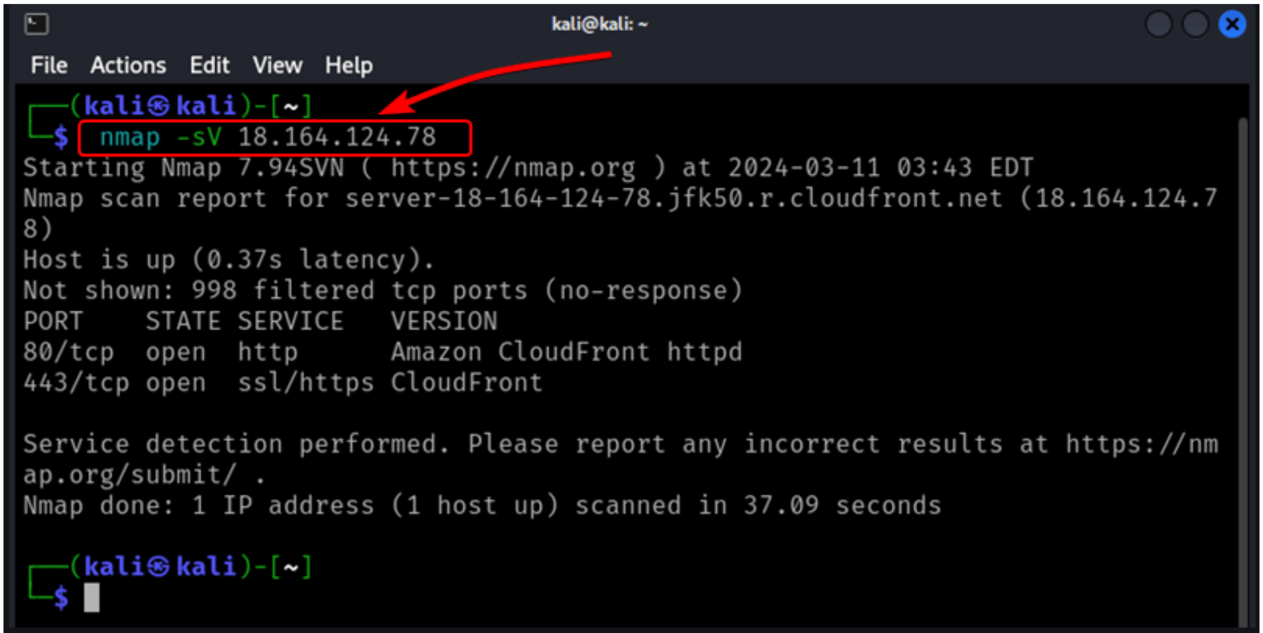
8. Version Scanning with Nmap

The following nmap command is used to perform service and version detection scanning on the specified target using the Nmap tool in Kali Linux. When you run this command, Nmap will first perform a TCP connect scan on the specified target(s) to find open ports. For each open port, it will then try to determine the service or application running on that port and its associated version information.

Command :

```
nmap -sV <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 18.164.124.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 03:43 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.7
8)
Host is up (0.37s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Amazon CloudFront httpd
443/tcp open  ssl/https CloudFront

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.09 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

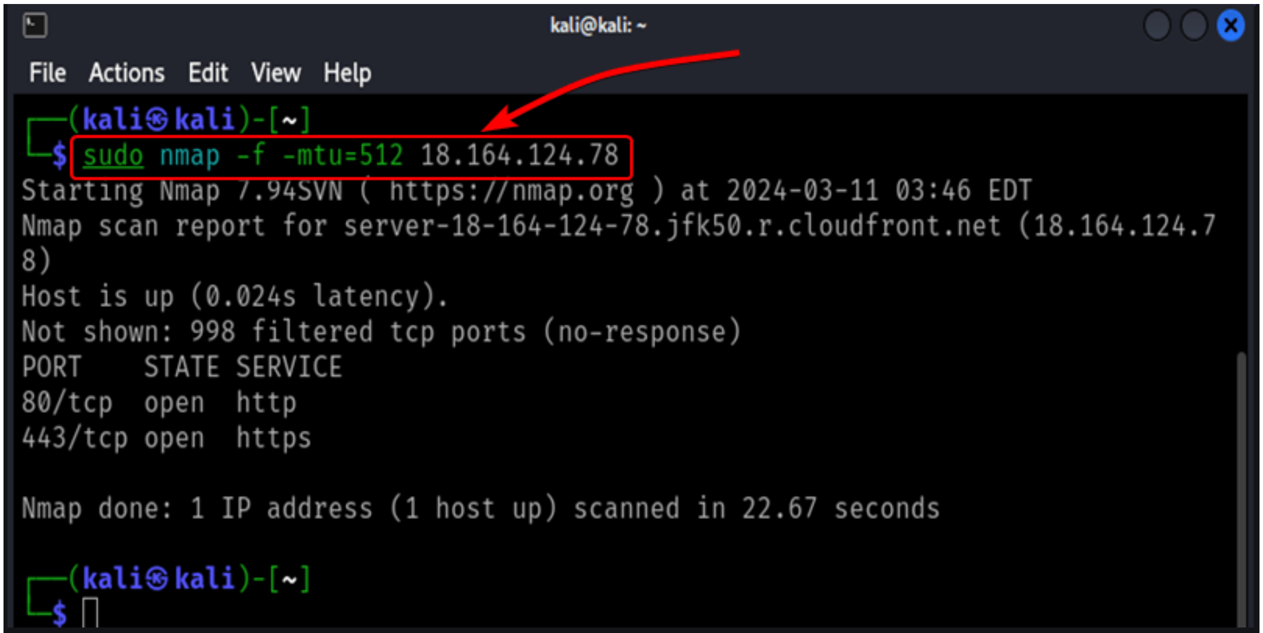
9. Firewall Bypass

The following nmap command is used to perform a fragmented packet scan on the specified target using Nmap in Kali Linux. When you run this command, Nmap will split its scanning packets into smaller fragments of 512 bytes or less and send them to the target system. This can sometimes allow the scan to bypass certain firewall rules or intrusion detection systems that may be configured to block or detect larger, unfragmented packets.

Command :

```
sudo nmap -f –mtu=512 <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -f -mtu=512 18.164.124.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 03:46 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.7
8)
Host is up (0.024s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 22.67 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

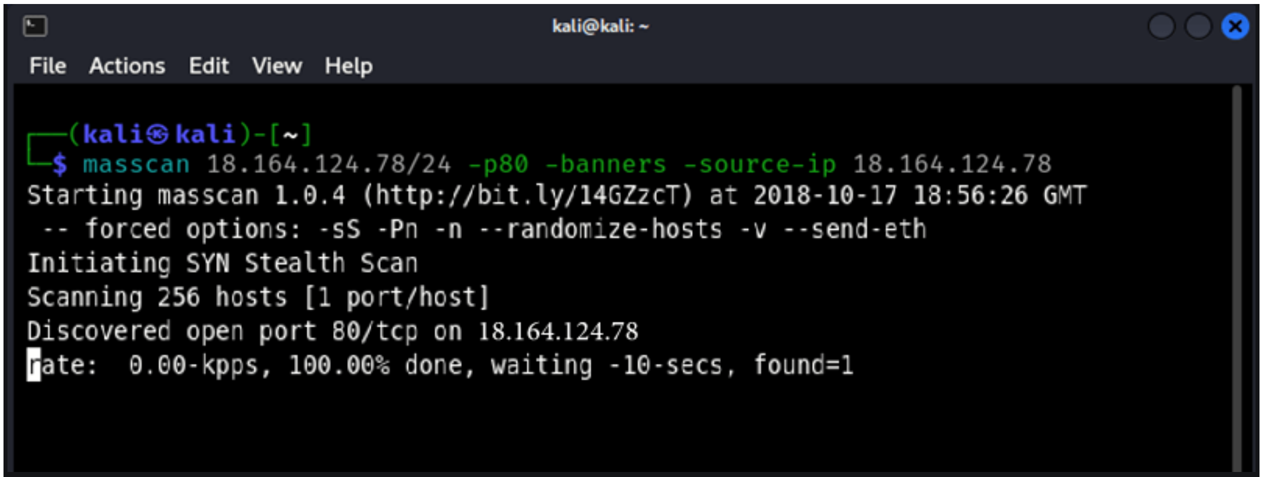
10. Scanning with Masscan

The following command is used to perform a fast TCP port scan on the specified network or IP range, targeting port 80 (HTTP), and capturing banner information while spoofing the source IP address. When you run this command, masscan will rapidly scan the specified network range, sending TCP connection requests to port 80 on each IP address. If port 80 is open on a target system, masscan will capture and display any banner information returned by the service running on that port.

Command :

```
masscan <network> -p80 –banners –source-ip <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ masscan 18.164.124.78/24 -p80 -banners -source-ip 18.164.124.78
Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2018-10-17 18:56:26 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 18.164.124.78
rate:  0.00-kpps, 100.00% done, waiting -10-secs, found=1
```

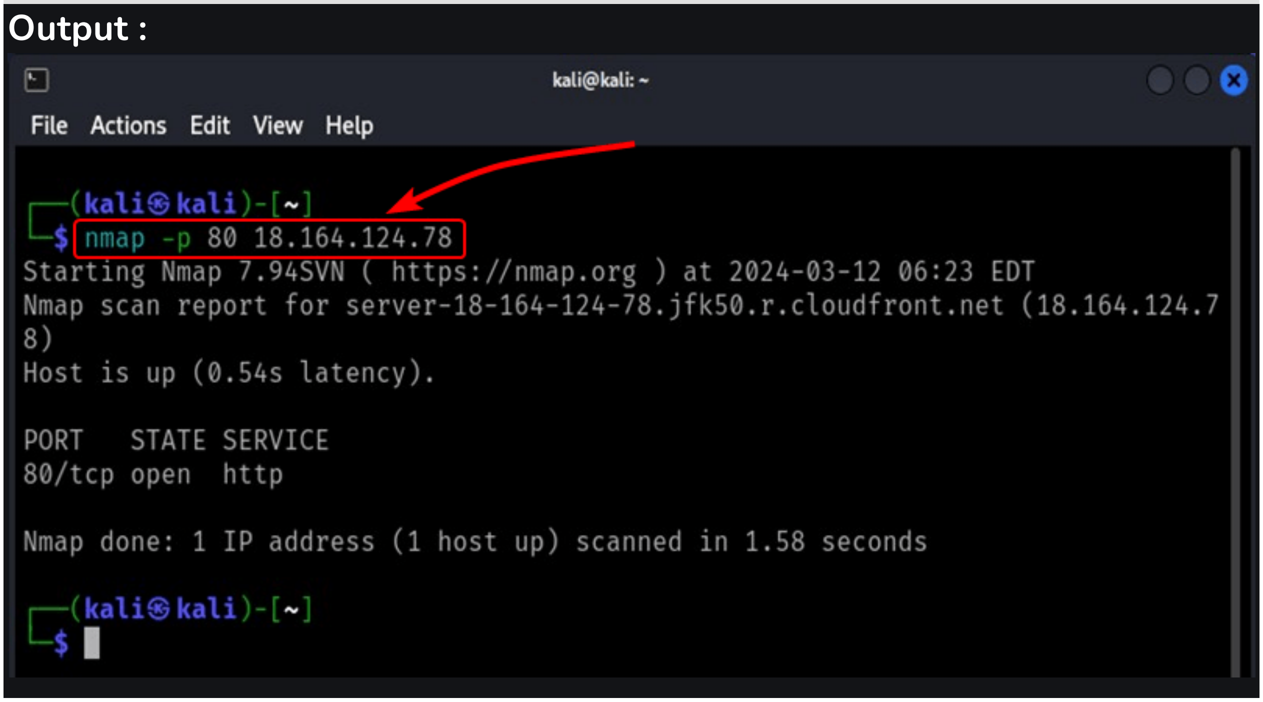
11. Specific Port Scanning

The following command is used to perform a TCP port scan on the specified target system, specifically targeting port 80 using the Nmap tool in Kali Linux. When you run this command, Nmap will send TCP connection requests to port 80 on the specified target(s). If port 80 is open and accepting connections, it will be reported as "open" in the scan results. If port 80 is closed or filtered, it will be reported as "closed" or "filtered" respectively.

Command :

```
nmap -p 80 <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 18.164.124.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:23 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.7
8)
Host is up (0.54s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

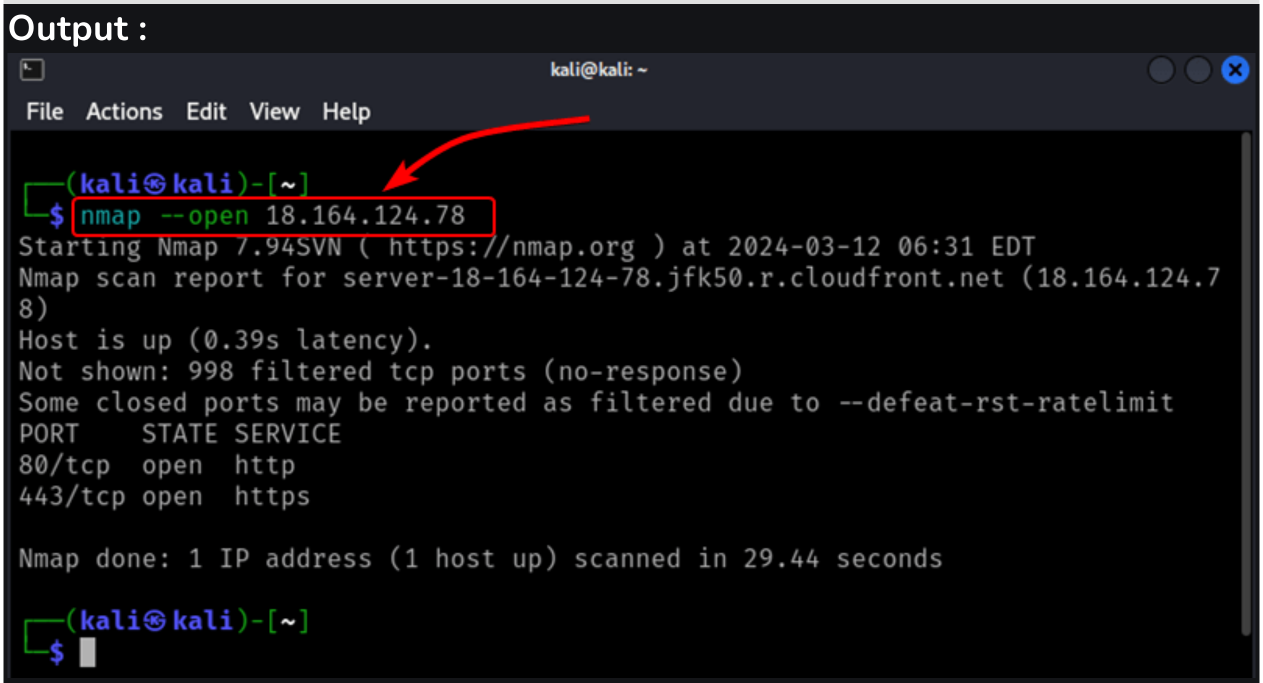
12. Open Ports Scanning

The following command is used to perform a TCP connect scan on the target IP address and only show the ports that are open or listening for incoming connections. When you run this command, Nmap will scan all 65,535 TCP ports on the target IP address using a TCP connect scan, which is the most reliable way to determine if a port is open or closed.

Command :

```
nmap --open <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap --open 18.164.124.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:31 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.7
8)
Host is up (0.39s latency).
Not shown: 998 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 29.44 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

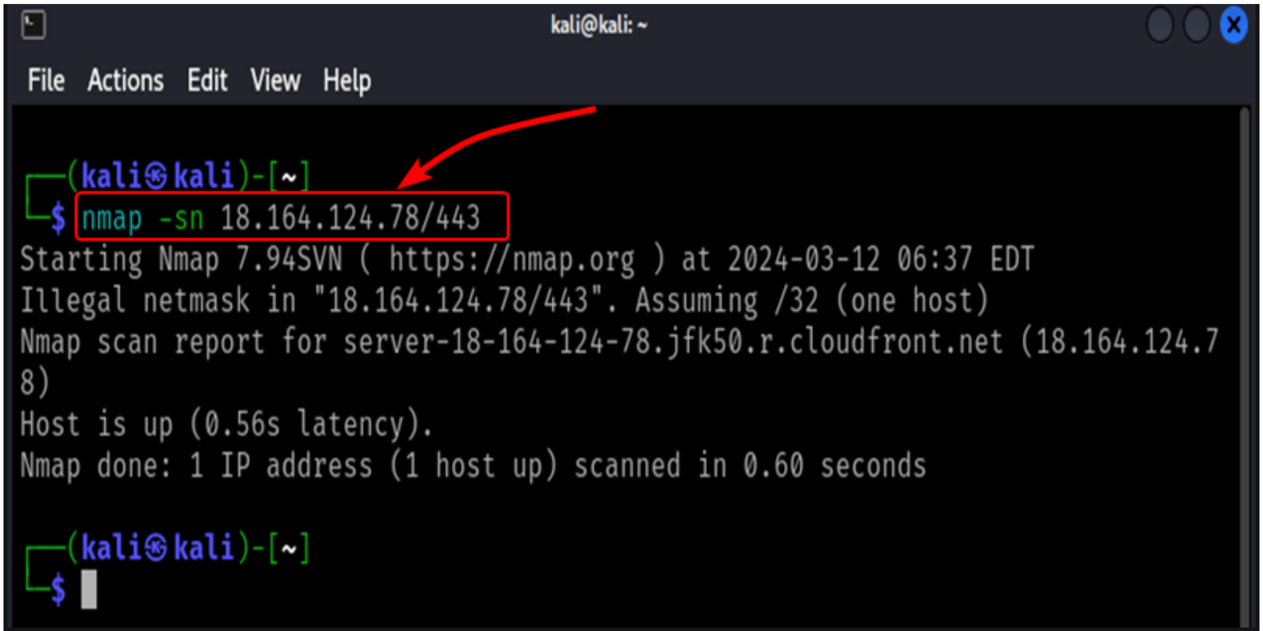
13. Active Remote Hosts Scanning

The following command is used to perform a ping scan on the specified network range using the Nmap tool in Kali Linux. When you run this command, Nmap will send ICMP (ping) requests to all IP addresses within the network range. It will then report back a list of IP addresses that responded to the ping requests, indicating that those hosts or devices are online and active on the network.

Command :

```
nmap -sn <target/port>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 18.164.124.78/443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:37 EDT
Illegal netmask in "18.164.124.78/443". Assuming /32 (one host)
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.7
8)
Host is up (0.56s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

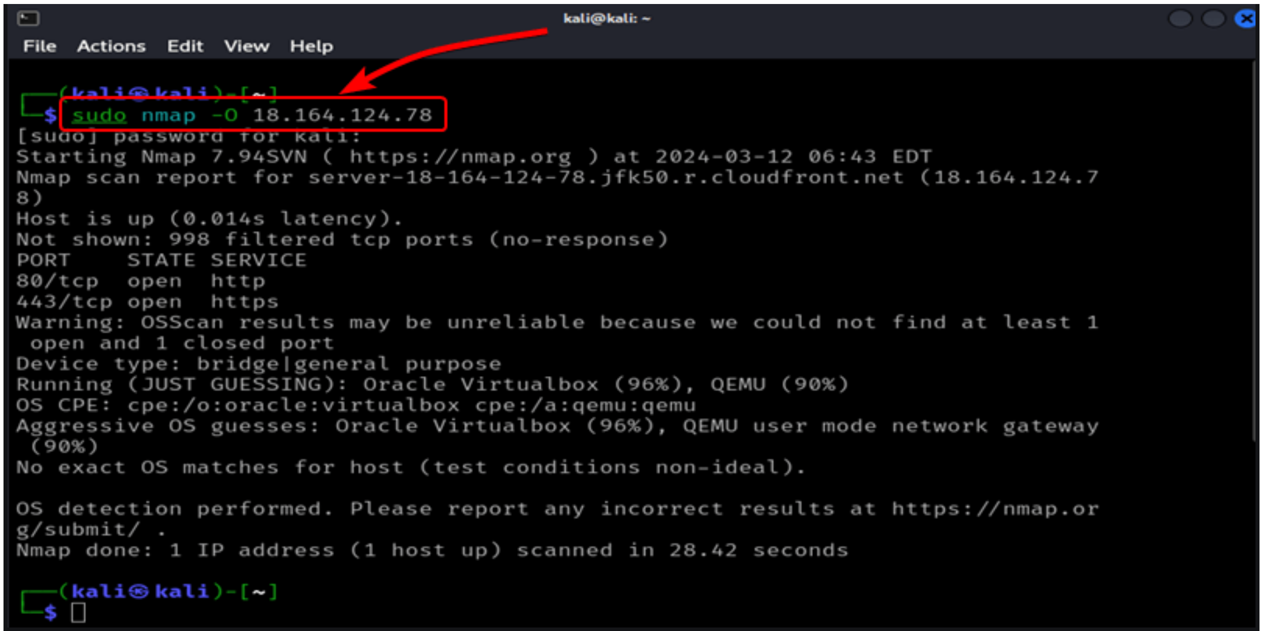
14. OS fingerprinting

The following command is used to perform remote operating system detection on the target system with the IP address using the Nmap tool in Kali Linux. When you run this command, Nmap will send a series of specially crafted packets to the target IP address and analyze the responses it receives. Based on these responses, Nmap will attempt to fingerprint the target system and determine the operating system (OS) it is running.

Command :

```
nmap -O <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 18.164.124.78
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:43 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.7
8)
Host is up (0.014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1
 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway
 (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.42 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

15. Performing a detailed scan

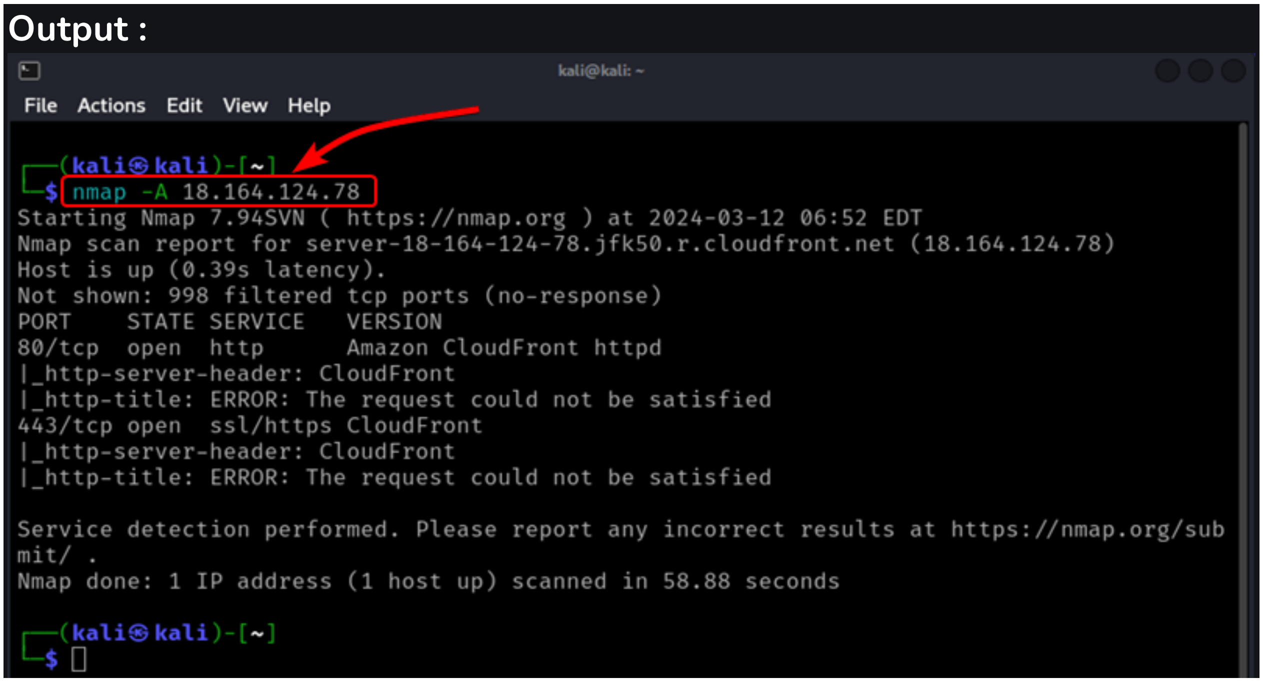
The following command is used to perform an aggressive scan on the target system with the IP address using the Nmap tool in Kali Linux. When you run this command, Nmap will perform a comprehensive scan on the target IP address, combining various scanning techniques to gather as much information as possible about the target system. Specifically, the -A option enables the following :

- **1. OS Detection:** Nmap will attempt to detect the operating system running on the target system.
- **2. Version Detection:** Nmap will probe open ports to determine the service/version information of the applications running on those ports.
- **3. Script Scanning:** Nmap will run a collection of default scripts designed to gather additional information about the target system, such as detecting vulnerabilities or collecting system data.
- **4. Traceroute:** Nmap will perform a traceroute to determine the network path to the target system.

Command :

```
nmap -A <target>
```

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 18.164.124.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:52 EDT
Nmap scan report for server-18-164-124-78.jfk50.r.cloudfront.net (18.164.124.78)
Host is up (0.39s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: ERROR: The request could not be satisfied
443/tcp open  ssl/https CloudFront
|_http-server-header: CloudFront
|_http-title: ERROR: The request could not be satisfied

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.88 seconds

┌──(kali㉿kali)-[~]
└─$ 
```