Network Scanning using Nmap

Project Description

In this project, we will utilize **Nmap (Network Mapper)**, a powerful tool used for network discovery and security auditing. Nmap allows us to discover hosts and services on a computer network, effectively creating a comprehensive “map” of the network.

We’ve structured this project into **11 tasks** to analyze the network and explore various options provided by Nmap. For each task, we’ll delve into the Nmap code and examine its output. Finally, in the **11th task**, we’ll consolidate all the information into a single-line code snippet and save it in a file format.

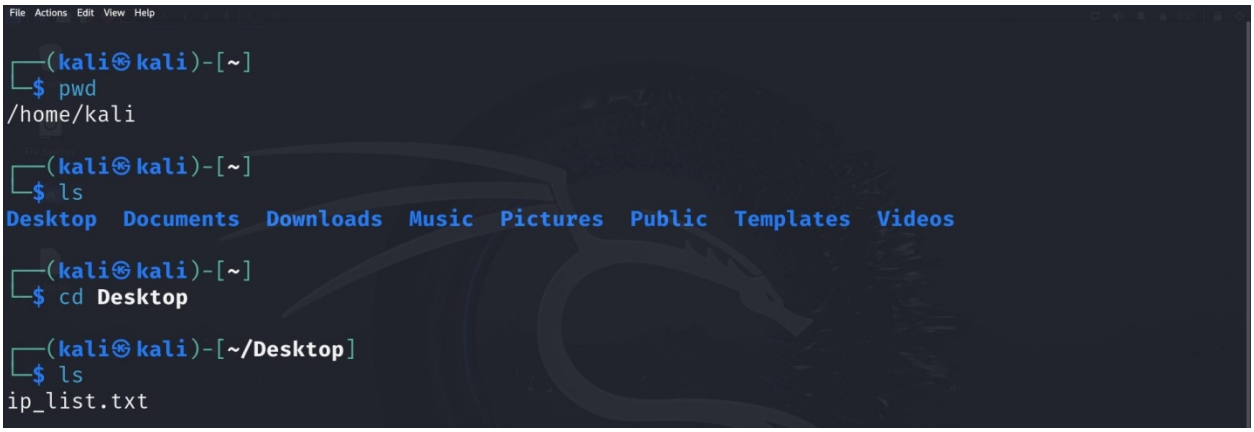
Task 1: Scan the list of IP’s in the ip_list.txt file.

For this task, we are going to scan the list of IP address files ip_list present in the Desktop directory.

To complete this task we have to follow these two steps:-

1. Navigate to the desktop directory
2. Scan ip_list.txt file

1). We started by checking our current directory for which we used **pwd** command. Then we listed the items present in our current directory by using the **ls** command, the Desktop directory is inside our current directory. So we used **cd Desktop** command to enter in Desktop directory and use **ls** command to list item present in Desktop directory. Finally we got our ip_list.txt file.



Output:-

- **pwd**: This command prints the current working directory. The output here is */home/kali*, indicating that the user is in their home directory.

- **ls**: This command lists the contents of the current directory. It shows typical home directories such as *Desktop, Documents, Downloads, Music, Pictures, Public, Templates, Videos*.

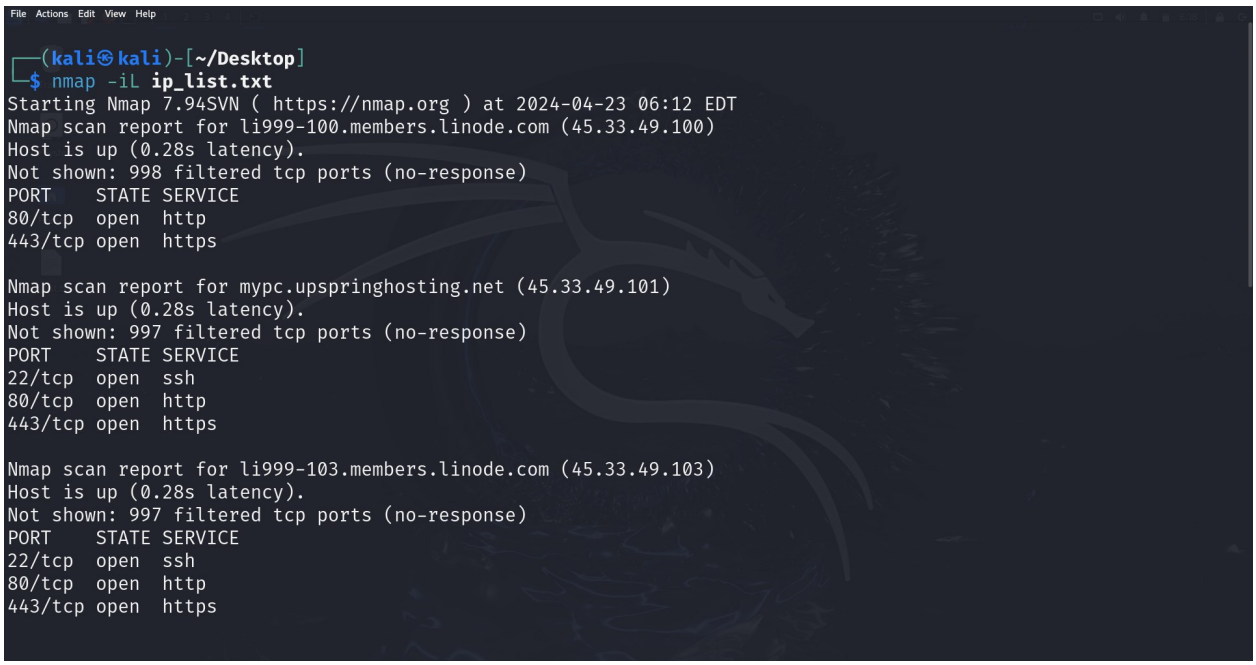
- **cd Desktop**: This command changes the current directory to the Desktop directory.

- **ls**: This command is entered again after changing to the Desktop directory, shows ip_list.txt file.

2). Next step is to scan list of IP addresses present in ip_list.txt file, for which we use command **nmap –iL ip_list.txt** file.

- **nmap**: This is the network mapper command-line tool.

- **-iL**: This option tells nmap to get the list of target hosts from a file. In this case, the file is ip_list.txt.



Output: -

The output shows the results of scanning multiple IP addresses listed in the ip_list.txt file. For each IP address, it provides the following details:

- **IP Address**: The IP address that was scanned.
- **Open TCP Ports**: The open TCP ports(22, 80,443) on the scanned IP address.
- **State**: The state of the port (open).
- **Service**: The service running on each open port (http, https, or ssh).
- **Not shown**: Lines indicating that other scanned ports are filtered or closed.
- Finally end it tells that Nmap had scanned 7 IP address of 7 host in 201.20 seconds.

This information can be useful for understanding the network services running on a host and can be a starting point for further investigation or auditing.

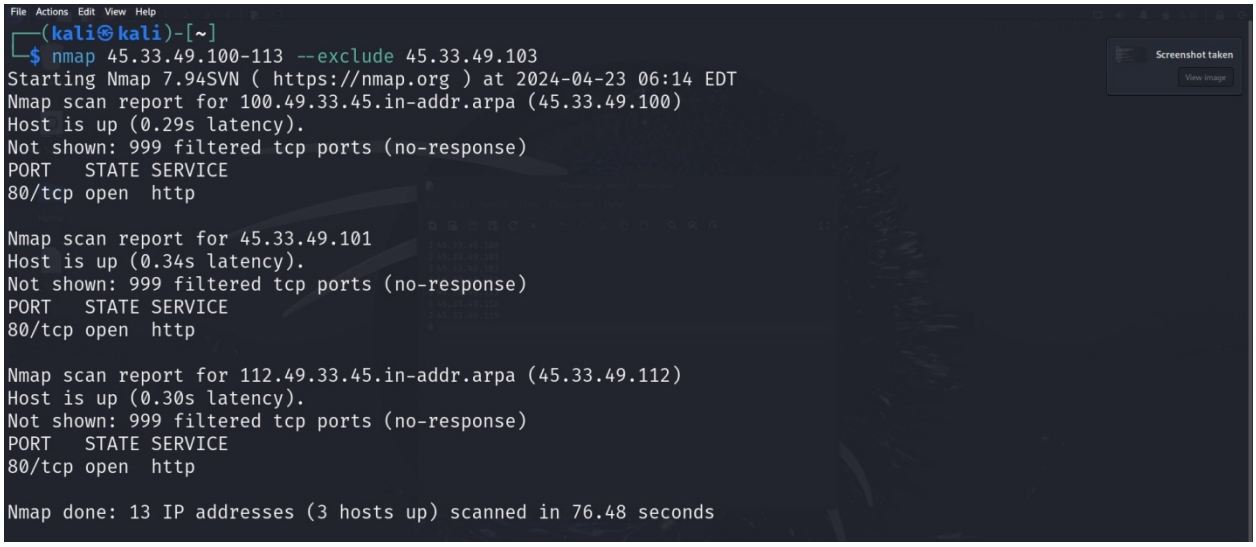
Task 2: Scan IP range and exclude one IP

In this task we are checking number of hosts present between IP addresses 45.33.49.100 to 45.33.49.113 excluding one host with IP address 45.33.49.103. To complete this task we use command:-

nmap 45.33.49.100-113 --exclude 45.33.49.103

Let's break it down:

- **nmap**: This is the network mapper command-line tool.
- **45.33.49.100-113**: This is the range of IP addresses to be scanned. It will scan from 45.33.49.100 to 45.33.49.113.
- **--exclude 45.33.49.103**: This option tells nmap to exclude the IP address 45.33.49.103 from the scan.



Output:-

The output shows the results of scanning the specified range of IP addresses 45.33.49.100-113, excluding the specified IP 45.33.49.103. For each scanned IP address, it provides the following details:

- **Host Status**: Whether the host is up (active) or down (inactive).
- **Latency**: The delay in the network communication.
- **Filtered Ports**: The ports that are protected by a firewall or filter.
- **Open Ports**: The open ports on the scanned IP address along with their associated services (in this case, HTTP on port 80).

Three hosts are up according to the results, and it took 76.48 seconds to scan 13 IP addresses in total.

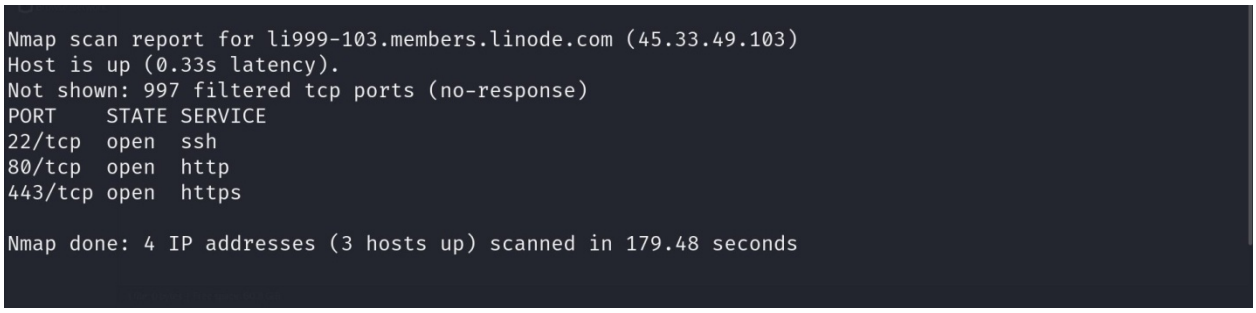
Task 3: Scan subnet

In this task we will be scanning subnet with IP address 45.33.49.100/30. *Subnet is network inside network.* To complete this task we use command

nmap 45.33.49.100/30

Let's break down the nmap command you've asked about:

- **45.33.49.100/30**: This is a CIDR notation which represents an IP address range. The IP address 45.33.49.100 is the network address, and /30 is the subnet mask.



Output:

The output shows the results of scanning the specified range of IP addresses. For each scanned IP address, it provides the following details:

- **IP Address**: The IP address that was scanned.
- **Open TCP Ports**: The open TCP ports on the scanned IP address.
- **State**: The state of the port (open).
- **Service**: The service running on each open port (http, https, or ssh).
- **Filtered Ports**: The ports that are protected by a firewall or filter.

For the first IP address 45.33.49.100, the scan reveals that it has 998 filtered TCP ports with no response, indicating they are protected or closed, and two open TCP ports:

- Port 80 with HTTP service
- Port 443 with HTTPS service

For the second IP address 45.33.49.101, there are 997 filtered TCP ports with no response and three open TCP ports:

- Port 22 with SSH service
- Port 80 with HTTP service
- Port 443 with HTTPS service

For the third IP address 45.33.49.103, there are 997 filtered TCP ports with no response and three open TCP ports:

- Port 22 with SSH service
- Port 80 with HTTP service
- Port 443 with HTTPS service

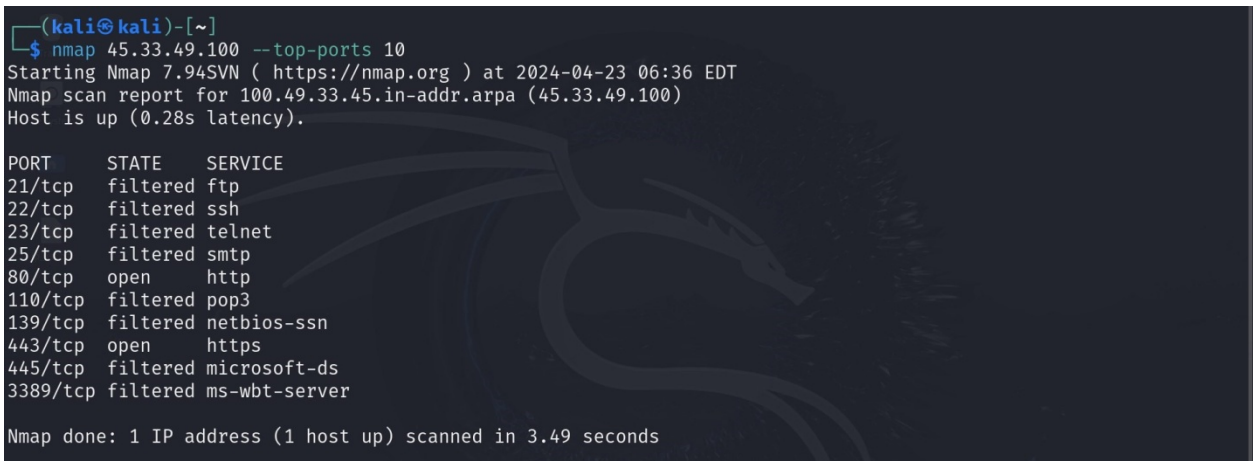
There are 4 IP addresses and 3 hosts are up according to the results, and it took 179.48 seconds to scan.

Task 4: top 10 ports

In this task we will scan top 10 most common ports. The command used is to complete this task is **nmap 45.33.49.100 --top-ports 10**

Here's what each part of the command does:

- **nmap**: This is the command itself, which starts the network mapper.
- **--top-ports 10**: This option tells nmap to scan only the top 10 most common ports.
- **45.33.49.100**: This is the IP address that is being scanned.



Output:-

The output of the command shows the status of the top 10 most common ports for the IP address 45.33.49.100.

- The output indicates that ports 80/tcp and 443/tcp are open, which typically means that HTTP and HTTPS services are running on the server.
- The other ports like FTP, SSH, Telnet, SMTP, POP3, NetBIOS-SSN, Microsoft-DS, and MS-WBT-Server are filtered, which means they are protected by a firewall or packet filter.

Task 5: http port

In this task we will scan ports associated with HTTP service. To complete this task we will use this command **nmap 45.33.49.100 -p http**

Here's what each part of the command does:

- **nmap**: This is the command itself, which starts the network mapper.
- **45.33.49.100**: This is the IP address that is being scanned.
- **-p http**: This option tells nmap to scan only ports associated with the HTTP service.

Output:

The output of the command shows the status of the HTTP ports for the IP address 45.33.49.100. The output indicates that port 80/tcp is open, which typically means that HTTP service is running on the server. Port 8008/tcp is filtered, which means it's not accessible for HTTP service.

One host is up according to the results, and it took 3.60 seconds to scan one IP addresses in total.

Task 6: Scanning at different speed

In this task we will perform one T3 (Normal) and one T5 (aggressive) timing templates scan.

Nmap provides several predefined timing templates that we can use to adjust the timing of the scan to suit our needs. This allows us to adjust the scan per our requirements, whether we're looking to quickly gather information about a target or perform a more through and detailed scan.

Here are the six timing templates in Nmap:

- **T0 (Paranoid)**: This template is the slowest and most conservative. This template is extremely useful for avoiding detection, but it might take a long time to complete the scan.
- **T1 (Sneaky)**: This scan is a little bit faster than the T0 scan.
- **T2 (Polite)**: The T2 faster than T0 and T1 scan and is the last scanning template to utilize the serial scanning method.
- **T3 (Normal)**: This is the default scan for Nmap.
- **T4 (Aggressive)**: The T4 template runs its scanning in parallel increasing speed. The scan_delay for this template is set to 0 seconds to 10 milliseconds.

- **T5 (Insane)**: This is the fastest template and it can potentially lead to inaccurate results due to its speed.

To complete this task we use command **nmap 45.33.49.119 -T5**

Here's what each part of the command does:

- **nmap**: This is the command itself, which starts the network mapper.
- **45.33.49.119**: This is the IP address that is being scanned.
- **-T5**: This option sets the timing template to insane. Nmap will spend less time waiting for replies, which is useful for scanning many hosts, but it might miss some information.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 45.33.49.119 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 06:51 EDT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.26s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 21.04 seconds
```

Output:-

The output of the command shows the status of the ports for the IP address 45.33.49.119. The output indicates that ports 22/tcp, 25/tcp, 80/tcp, and 443/tcp are open, which typically means that SSH, SMTP, HTTP, and HTTPS services are running on the server respectively.

996 other TCP ports were filtered and did not respond during the scan, which was completed in 21.04 seconds.

Now we will perform normal timing scan by using command

nmap 45.33.49.119 –T3

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 45.33.49.119 -T3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 07:01 EDT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.30s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 22.49 seconds
```

Output:-

The output of the command shows the status of the ports for the IP address 45.33.49.119. The output indicates that ports 22/tcp, 25/tcp, 80/tcp, and 443/tcp are open, which typically means that SSH, SMTP, HTTP, and HTTPS services are running on the server respectively.

996 other TCP ports were filtered and did not respond during the scan, which was completed in 22.49 seconds.

Task 7: http header response

The **HTTP-headers** script executes a HEAD request targeting the root folder (“/”) of a web server. This script presents the HTTP headers that the server returns. These headers can offer valuable insights about the server, such as:

- Server type
- Whether the connection is open or closed
- The technologies utilized by the server
- Other server configurations

This information can be crucial for understanding the server’s setup and operation.

```
┌──(kali㉿kali)-[~]
└─$ nmap nmap.org --script http-headers
```

This command tells Nmap to scan the target **nmap.org** using the http-headers script.

```
┌──(kali㉿kali)-[~]
└─$ nmap nmap.org --script http-headers
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 07:05 EDT
Nmap scan report for nmap.org (45.33.49.119)
Host is up (0.30s latency).
Other addresses for nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
| http-headers:
|   Date: Tue, 23 Apr 2024 11:06:24 GMT
|   Server: Apache/2.4.6 (CentOS)
|   Location: https://nmap.org/
|   Content-Length: 298
|   Connection: close
|   Content-Type: text/html; charset=iso-8859-1
|
|_  (Request type: GET)
443/tcp open  https
| http-headers:
|   Date: Tue, 23 Apr 2024 11:06:24 GMT
|   Server: Apache/2.4.6 (CentOS)
|   Strict-Transport-Security: max-age=31536000; preload
|   Vary: Host
|   Accept-Ranges: bytes
|   Connection: close
|   Transfer-Encoding: chunked
|   Content-Type: text/html; charset=utf-8
|
|_  (Request type: GET)

Nmap done: 1 IP address (1 host up) scanned in 34.30 seconds
```

Output:

- The scan report provides information about the target IP address **(45.33.49.119)** and reverse DNS record (ack.nmap.org).
- The report shows that ports 22 (SSH), 25 (SMTP), 80 (HTTP), and 443 (HTTPS) are open on the target.
- The http-headers script returns the HTTP headers for the server running on **port 80**. These headers provide information about the server and its configuration, including:
    - **Date:** the response was sent on Tue, 23 April 2024 at 11:06:24 GMT

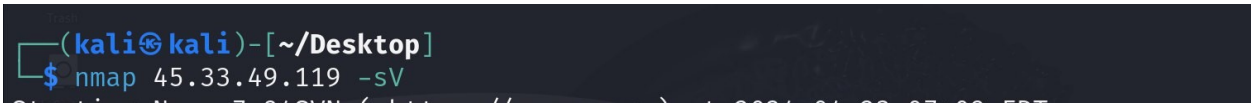
    - **Server:** The type and version of the server software is Apache/2.4.6 on CentOS.
    - **Content-Length:** The size of the response body in bytes is 298
    - **Connection:** Indicates that the server will close the connection after completing the response.
    - **Content-Type:** The media type of the resource is text/html

- The http-headers script returns the HTTP headers for the server running on **port 443**. These headers provide information about the server and its configuration, including:
    - **Date**: The date and time at which the HTTP response was generated by the server Tue, 23 Apr 2024 11:06:24 GMT.
    - **Server:** The type and version of the server software is Apache/2.4.6 on CentOS.
    - **Strict-Transport-Security:** This HTTP header tells browsers to always use HTTPS, even for future requests, for the next 31536000 seconds (about one year). The preload directive means that the site is included in the HSTS preload list, which is built into browsers and ensures that they always connect to the site over HTTPS.
    - **Vary:** This header indicates that the response may vary depending on the value of the 'Host' header in the request. This is often used for caching purposes.
    - **Accept-Ranges:** This header indicates that the server accepts range requests, which allow a client to request a specific part of a resource. The value 'bytes' means that ranges are specified in terms of bytes.
    - **Connection:** This header indicates that the server will close the connection after completing the response.
    - **Content-Type:** The media type of the resource is text/html.

- Nmap done is the summary of the scan. It shows that one IP address was scanned, one host was up, and the scan took 34.30 seconds.

Task 8: Scan IP service version

In this task we will find the version of service



This command tells Nmap to scan the target IP address 45.33.49.119 using the **-sV** option, which enables version detection. This can help identify the versions of services running on open ports.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 45.33.49.119 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 07:09 EDT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.26s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
80/tcp  open  http     Apache httpd 2.4.6
443/tcp open  ssl/http Apache httpd 2.4.6
Service Info: Hosts:  ack.nmap.org, issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.31 seconds
```

Output:

- Scan report provides information about the target IP address 45.33.49.119 and hostname that is ack.nmap.org.
- For each open port, the service version is displayed. For example, for port 22, the service is SSH and the version is OpenSSH 7.4 (protocol 2.0). For port 25, the service is SMTP and the version is Postfix smtpd. For ports 80 and 443, the service is Apache httpd 2.4.6.
- **Service Info:** hosts: provides additional information about the host, including the hostnames (acme.map.org, ISSUES.map.org).
- Nmap done is summary of the scan. It shows that one IP address was scanned, one host was up, and the scan took 38.31 seconds.

Task 9: Scan OS

In this task we will find operating system of the network by using IP addresses.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 45.33.49.119 -O
[sudo] password for kali:
```

This command tells Nmap to scan the target IP address 45.33.49.119 with root privileges.

This task required root privilege so that why we used sudo in command to find operating system

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 45.33.49.119 -O
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 07:10 EDT
Nmap scan report for 119.49.33.45.in-addr.arpa (45.33.49.119)
Host is up (0.12s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  open   smtp
70/tcp  closed gopher
80/tcp  open   http
113/tcp closed ident
443/tcp open   https
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (92%), QEMU (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (92%), QEMU user mode network gateway (88%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.33 seconds
```

Output:

- The report shows that ports 22 (SSH), 25 (SMTP), 80 (HTTP), and 443 (HTTPS) are open on the target. Ports 70 (GOPHER) and 113 (IDENT) are closed.
- The device type is identified as a bridge or general purpose device. The running OS could be Oracle Virtualbox or QEMU OS. The OS details suggest a high likelihood of Oracle Virtualbox (92%) and QEMU model network gateway (88%).
- This is a summary of the scan. It shows that one IP address was scanned, one host was up, and the scan took 56.33 seconds.

Task 10: Scan OS, service version and traceroute

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 45.33.49.119 -A
```

This command tell Nmap to perform a scan, which enables OS detection, version detection, script scanning and traceroute.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 45.33.49.119 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 07:15 EDT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.048s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  open   ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d (RSA)
|   256 88:2b:29:00:d0:c7:81:ac:dd:f4:90:42:d2:aa:f0:5b (ECDSA)
|_  256 64:d6:39:35:04:76:1c:ba:17:f3:fd:4f:1f:b3:71:61 (ED25519)
25/tcp  open   smtp     Postfix smtpd
|_smtp-commands: ack.nmap.org, PIPELINING, SIZE 102400000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
 DSN
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=insecure.com
| Subject Alternative Name: DNS:insecure.com, DNS:insecure.org, DNS:issues.nmap.org, DNS:issues.npcap.org, DNS:
nmap.com, DNS:nmap.net, DNS:nmap.org, DNS:npcap.com, DNS:npcap.org, DNS:seclists.com, DNS:seclists.net, DNS:sec
lists.org, DNS:sectools.com, DNS:sectools.net, DNS:sectools.org, DNS:secwiki.com, DNS:secwiki.net, DNS:secwiki.
org, DNS:svn.nmap.org, DNS:www.nmap.org
| Not valid before: 2024-04-12T09:07:43
|_Not valid after:  2024-07-11T09:07:42
70/tcp  closed gopher
80/tcp  open   http     Apache httpd 2.4.6
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.6 (CentOS)
113/tcp closed ident
443/tcp open   ssl/http Apache httpd 2.4.6
| ssl-cert: Subject: commonName=insecure.com
| Subject Alternative Name: DNS:insecure.com, DNS:insecure.org, DNS:issues.nmap.org, DNS:issues.npcap.org, DNS:
nmap.com, DNS:nmap.net, DNS:nmap.org, DNS:npcap.com, DNS:npcap.org, DNS:seclists.com, DNS:seclists.net, DNS:sec
lists.org, DNS:sectools.com, DNS:sectools.net, DNS:sectools.org, DNS:secwiki.com, DNS:secwiki.net, DNS:secwiki.
org, DNS:svn.nmap.org, DNS:www.nmap.org
| Not valid before: 2024-04-12T09:07:43
|_Not valid after:  2024-07-11T09:07:42
|_ssl-date: TLS randomness does not represent time
|_http-title: Did not follow redirect to https://nmap.org/
|_http-server-header: Apache/2.4.6 (CentOS)
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (92%), QEMU (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (92%), QEMU user mode network gateway (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Hosts:  ack.nmap.org, issues.nmap.org

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.11 ms 10.0.2.2 (10.0.2.2)
2   0.10 ms ack.nmap.org (45.33.49.119)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.63 seconds
```

Output:

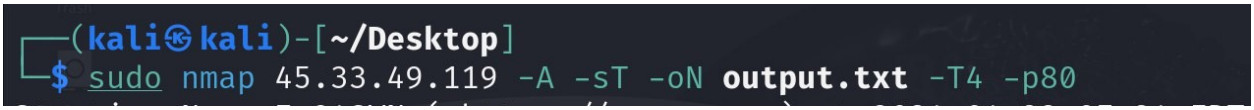
- Scan report provides information about the target IP address 45.33.49.119 and hostname that is ack.nmap.org.
- The report shows that ports 22 (SSH), 25 (SMTP), 80 (HTTP), and 443 (HTTPS) are open on the target. Ports 70 (GOPHER) and 113 (IDENT) are closed.
- The device type is identified as a bridge or general purpose device. The running OS could be Oracle Virtualbox or QEMU OS. The OS details suggest a high likelihood of Oracle Virtualbox (92%) and QEMU model network gateway (88%).
- The output is from a **traceroute** operation using port 80/tcp.

- We have 2 HOP which means our packet has to go through 2 machines or router to reach its final destination.
- RTT (Round Trip Time) for first hop is 0.011ms and the second hop has an RTT of 0.010 ms.
- The first hop IP address is 10.0.2.2 and the second hop domain name is “ack.nmap.org” with the IP address 45.33.49.119.

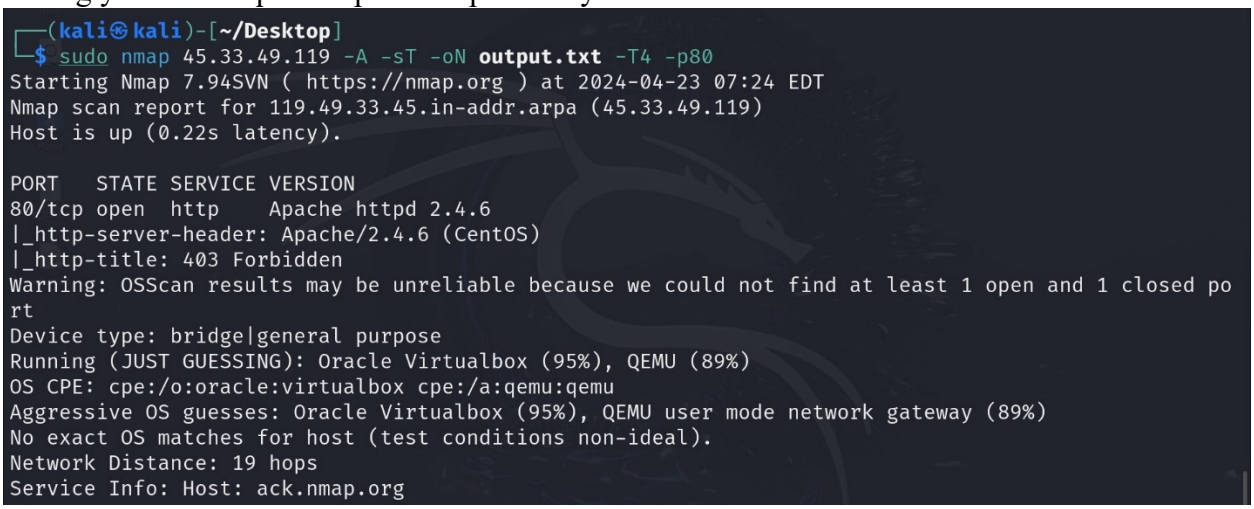
- This is a summary of the scan. It shows that one IP address was scanned, one host was up, and the scan took 106.3 seconds.

Task 11 : Scanning all above task and save in output

In this task, we will perform all the above tasks in a single code and save the scanning report in output.txt file.



Saving your scan report help can help to analysis it in future.



```
TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   1.38 ms   10.0.2.2 (10.0.2.2)
2   242.83 ms dlinkrouter (192.168.0.1)
3   242.85 ms csp1.zte.com.cn (192.168.10.1)
4   243.84 ms 10.106.0.1 (10.106.0.1)
5   247.47 ms 125.20.126.81
6   256.44 ms 116.119.72.0
7   293.89 ms 182.79.149.244
8   297.96 ms 101.73.127.202.in-addr.arpa (202.127.73.101)
9   ...
10  482.38 ms 234.140.84.202.in-addr.arpa (202.84.140.234)
11  476.66 ms 234.140.84.202.in-addr.arpa (202.84.140.234)
12  252.84 ms 198.143.84.202.in-addr.arpa (202.84.143.198)
13  252.83 ms 198.143.84.202.in-addr.arpa (202.84.143.198)
14  254.45 ms 57.251.84.202.in-addr.arpa (202.84.251.57)
15  270.05 ms 196.116.223.206.in-addr.arpa (206.223.116.196)
16  ... 18
19  443.17 ms 119.49.33.45.in-addr.arpa (45.33.49.119)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 30.35 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
ip_list.txt  output.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat output.txt
# Nmap 7.94SVN scan initiated Tue Apr 23 07:24:23 2024 as: nmap -A -sT -oN output.txt -T4 -p80 45.33.49.1
19
Nmap scan report for 119.49.33.45.in-addr.arpa (45.33.49.119)
Host is up (0.22s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.6
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-title: 403 Forbidden
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 (95%), QEMU (89%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops
Service Info: Host: ack.nmap.org

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   1.38 ms   10.0.2.2 (10.0.2.2)
2   242.83 ms dlinkrouter (192.168.0.1)
3   242.85 ms csp1.zte.com.cn (192.168.10.1)
4   243.84 ms 10.106.0.1 (10.106.0.1)
5   247.47 ms 125.20.126.81
6   256.44 ms 116.119.72.0
7   293.89 ms 182.79.149.244
8   297.96 ms 101.73.127.202.in-addr.arpa (202.127.73.101)
9   ...
10  482.38 ms 234.140.84.202.in-addr.arpa (202.84.140.234)
11  476.66 ms 234.140.84.202.in-addr.arpa (202.84.140.234)
12  252.84 ms 198.143.84.202.in-addr.arpa (202.84.143.198)
13  252.83 ms 198.143.84.202.in-addr.arpa (202.84.143.198)
14  254.45 ms 57.251.84.202.in-addr.arpa (202.84.251.57)
15  270.05 ms 196.116.223.206.in-addr.arpa (206.223.116.196)
16  ... 18
19  443.17 ms 119.49.33.45.in-addr.arpa (45.33.49.119)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Apr 23 07:24:54 2024 -- 1 IP address (1 host up) scanned in 30.35 seconds
```

Output:

- The tasks we performed earlier given the same output, so it will be easier to understand now. That's why I'm skipping the explanation.

- We have saved the scan report in a file named **'output.txt'** on the desktop directory. To check the output file, we use the 'ls' command.

- Now, let's open the 'output.txt' file by using the command 'cat output.txt'."

Conclusion

The project provides an in-depth exploration of Nmap. It combines various scanning techniques, port analysis, service detection, OS identification, and other methods. In the final step, I saved the output to a file. This project significantly enhanced my understanding of the network landscape.