

Module 3 :- Scanning

In cybersecurity, scanning refers to the process of systematically inspecting systems, networks, and applications to identify potential vulnerabilities, weaknesses, or misconfigurations that could be exploited by attackers. It involves using various techniques and tools to probe and examine the target environment, helping organizations proactively identify and address security risks before they can be exploited.

Here's a more detailed explanation:

What it involves:

- **Systematic Examination:**

Scanning involves a methodical approach, using specific tools and methods to gather information about the target.

- **Vulnerability Detection:**

The primary goal is to identify vulnerabilities, which are weaknesses in software, hardware, or configurations that attackers can exploit.

- **Network Mapping:**

Scanning can help map out a network, identifying active hosts, open ports, and services.

- **Code Scanning:**

This involves examining code to find bugs, errors, and security flaws.

- **Penetration Testing:**

This type of scanning simulates an attack to test the security of systems and networks.

Why it's important:

- **Proactive Security:**

Scanning helps organizations identify vulnerabilities before attackers can exploit them.

- **Risk Reduction:**

By identifying and addressing weaknesses, organizations can significantly reduce their risk profile.

- **Compliance:**

Many security standards and regulations require regular vulnerability scanning.

- **Maintaining System Integrity:**

Scanning helps ensure that systems and applications are secure and functioning as intended.

Types of Scanning:

- **Vulnerability Scanning:** This involves using automated tools to detect security weaknesses in software, systems, and networks.
- **Network Scanning:** This involves identifying active hosts, open ports, and services within a network.
- **Code Scanning:** This examines code to identify bugs, errors, and security flaws.
- **Penetration Testing:** This simulates an attack to test the security of systems and networks.
- **Network Scanning :** network scanning refers to set a procedures used for identifying hosts , ports and services in a network

Network scanning is one of the components of information gathering which can be used by an attacker to create a profile of the target organization

Network scanning is a process that identifies active devices and services on a network, often used for network administration, security assessments, and vulnerability analysis. It involves sending probes (packets) to a network to gather information about hosts, open ports, services, and potentially, even the operating system of those hosts.

Here's a more detailed breakdown:

Purpose of Network Scanning:

- **Network Administration:**

Understanding the devices and services on the network is crucial for efficient management.

- **Security Assessments:**

Scanning helps identify potential vulnerabilities and weaknesses in the network's security posture.

- **Vulnerability Analysis:**

Detecting open ports and misconfigurations can reveal areas that could be exploited by attackers.

How it Works:

- **Host Discovery:**

Network scanning tools send out probes to identify which IP addresses are active on the network and which are not.

- **Port Scanning:**

Once active hosts are identified, the scanner probes specific ports (like TCP and UDP) to determine which services are running.

- **Service and OS Detection:**

Some scanners can even attempt to identify the services running on those ports and potentially even the operating system of the host.

Types of Scanning:

- **Ping Sweep:** A basic form of scanning where the tool sends ping requests to a range of IP addresses to see which are active.
- **TCP Scanning:** Uses TCP connections to probe ports.
- **UDP Scanning:** Uses UDP packets to probe ports.
- **Stealth Scanning:** Techniques to avoid detection by firewalls and intrusion detection systems.

Tools:

- **Nmap:** A widely used open-source tool for network scanning, port scanning, and OS detection.
- **Masscan:** A high-speed network scanner for quickly scanning large networks.
- **Other Commercial Tools:** Various commercial network scanners offer advanced features and capabilities.

Benefits of Network Scanning:

- **Improved Security:**

Identifying and addressing vulnerabilities can strengthen network security.

- **Better Network Management:**

Understanding the network's topology and services helps in efficient management.

- **Proactive Threat Detection:**

Scanning can help detect suspicious activity or potential attacks before they impact the network.

- **Objective :**

- To discover live host , IP , addresses and open or live ports.
- To discover services running on hosts.
- To discover vulnerability in live host
- To discover operating system and service architecture .

- **types of scanning :**

- ports scanning
- network scanning
- vulnerability scanning
- host scanning

Nmap

Nmap is a powerful, open-source tool used for network discovery and security auditing. It's essentially a command-line utility that sends packets to target hosts and analyzes the responses to gather information about the network. This includes identifying live hosts, open ports, services running on those ports, operating systems, and even potential vulnerabilities.

Here's a more detailed breakdown:

Functionality:

- **Host Discovery:** Nmap can determine which hosts on a network are active and responding.
- **Port Scanning:** It can scan for open ports on those hosts, revealing which services are potentially running.
- **Service and Version Detection:** Nmap can identify the services running on open ports and even their specific versions.
- **OS Detection:** It can often guess the operating system of a host based on its responses.
- **Vulnerability Detection:** Nmap can also be used to scan for known vulnerabilities in software and services.

How it Works:

- Nmap sends packets (like ICMP, TCP SYN, etc.) to the target hosts.
- It analyzes the responses to determine the state of the ports (open, closed, filtered).
- By examining the packet headers and responses, Nmap can infer information about the hosts, services, and operating systems.

Uses:

- **Network Auditing:**

Network administrators use Nmap to map their networks, identify potential security issues, and ensure that services are running as expected.

- **Penetration Testing:**

Security professionals use Nmap to assess the security of systems by identifying vulnerabilities and potential attack vectors.

- **Vulnerability Assessment:**

Nmap can be used to scan for known vulnerabilities in software and services, helping to identify systems that may be at risk.

- **Network Monitoring:**

Nmap can be used to monitor the status of hosts and services, ensuring that they are running as expected.

Important Considerations:

- **Ethical Usage:**

Nmap should be used responsibly and ethically, only on systems you have permission to scan.

- **Potential Risks:**

Improper use of Nmap can lead to legal issues, network disruptions, or even compromise of systems.

- **Legal Ramifications:**

Using Nmap to scan systems without permission can have legal consequences, so it's crucial to be aware of the local laws and regulations.

- **Host discovery :** this technique is used for check active host in target networks .

Example of host discovery scanning

- ARP ping scan
- UDP ping scan

- ICMP ping scan
- TCP ping scan
- IP protocol ping scan

- Command :

nmap -sn -PR <target>

-sn = it is used for no port scan

-PR = for ARP ping

scan # nmap -pU <target>

>

-pU = for UDP ping scan to identify host is UP or DOWN

nmap -PE <target>

-PE = for echo normal

ping scan

nmap -PP <target>

-PP = for perform the ICMP timestamps ping scan

nmap -PM <target>

-pm = for ICMP mask ping scan

nmap -PS <target>

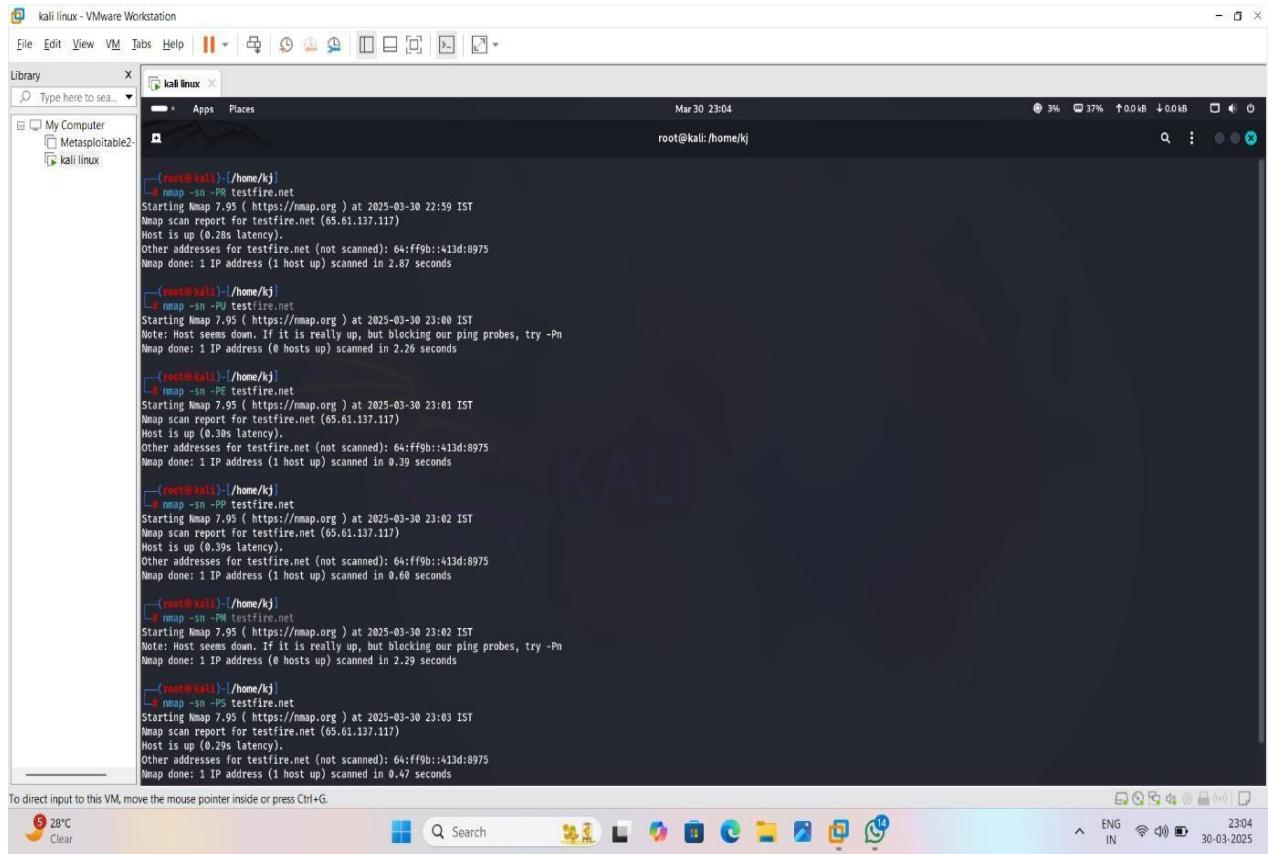
-PS = for TCP SYN ping scan

nmap -PA <target>

-PA = for TCP ACK ping scan

nmap -PO <target>

-PO = for IP protocol ping scan / this technique sends different probe packets of different IP protocols to the target .



The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. The desktop has a standard Windows-style taskbar at the bottom with icons for Start, Search, Task View, File Explorer, Edge, and others. The main window displays a terminal session as root (@kali) in /home/kali. The terminal shows five consecutive nmap scans of the target host 65.61.137.117. Each scan uses a different combination of arguments: -sn -PR, -sn -PU, -sn -PE, -sn -PM, and -sn -PS. All scans report the same results: the host is up with 0.285 latency, and other addresses for the host (not scanned) are 64:ff9b:413d:8975. The total time for each scan is approximately 2.87 seconds.

```
(root㉿kali)-[~/home/kali]
└─# nmap -sn -PR testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 22:59 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.285 latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds

(root㉿kali)-[~/home/kali]
└─# nmap -sn -PU testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:00 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.26 seconds

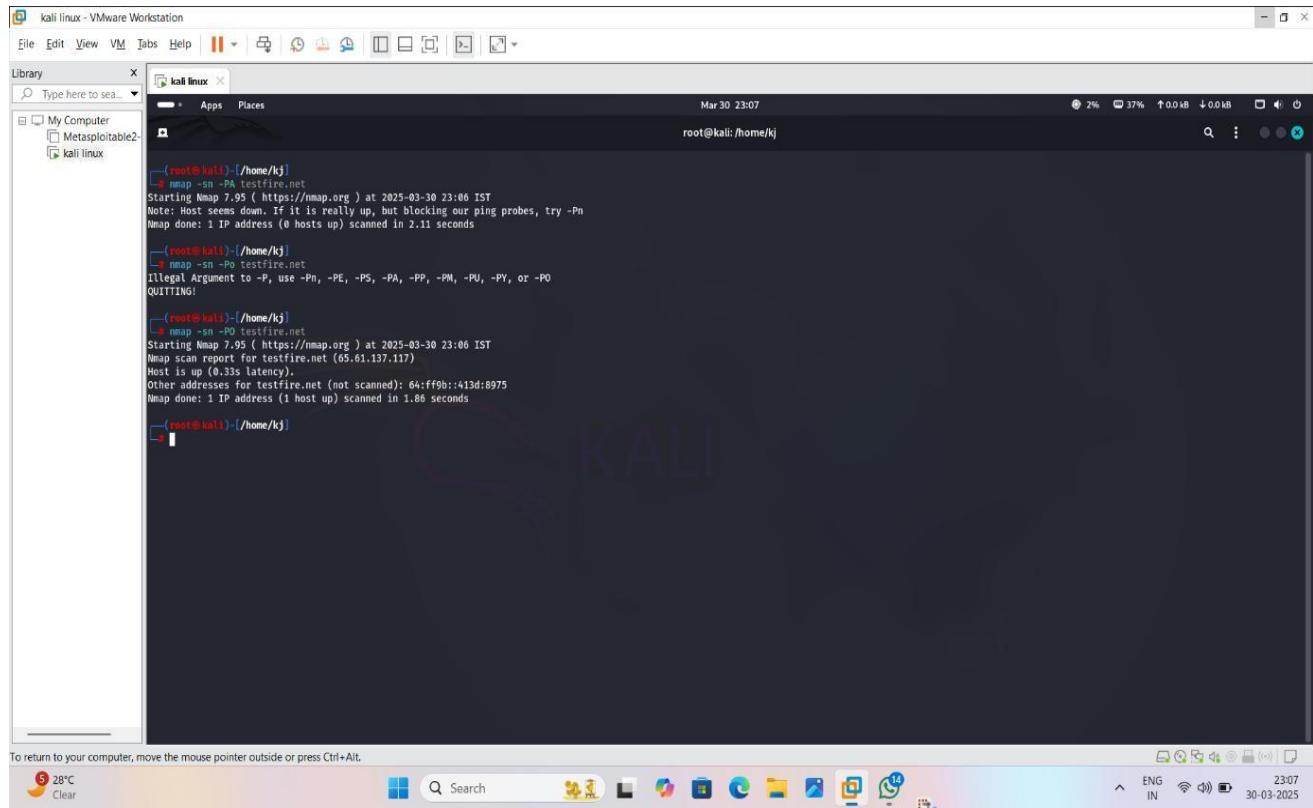
(root㉿kali)-[~/home/kali]
└─# nmap -sn -PE testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:01 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.305 latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

(root㉿kali)-[~/home/kali]
└─# nmap -sn -PP testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:02 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.39s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds

(root㉿kali)-[~/home/kali]
└─# nmap -sn -PM testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:02 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.29 seconds

(root㉿kali)-[~/home/kali]
└─# nmap -sn -PS testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:03 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.29s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

Here are some phtotos that show you host is up or down in the target network .



The screenshot shows a terminal window titled 'kali linux' running on a Kali Linux VM. The terminal displays three separate Nmap command executions:

```
(root㉿kali)-[~/home/kj]
└─# nmap -sn -PA testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:06 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.11 seconds

(root㉿kali)-[~/home/kj]
└─# nmap -sn -PO testfire.net
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, or -PO
QUITTING!

[root@kali]-[~/home/kj]
└─# nmap -sn -PO testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:06 IST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.33s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
```

- **Ports and service discovery :** - this is for identifying open ports and services running on the target IP .

➤ TCP scanning method

TCP scanning is a network security practice where tools send specific TCP packets to a target system's ports to determine which are open, closed, or filtered. This helps security professionals identify potential vulnerabilities and understand a system's exposed services.

Here's a more detailed explanation:

- **Purpose:**

TCP scanning aims to identify open ports on a target system, which might indicate running services or applications that could be exploited.

- **How it works:**

Scanners send SYN (synchronize) packets to a range of ports on the target.

- **Open ports:** If a port is open, the target will respond with a SYN-ACK (synchronize-acknowledge) packet.

- **Closed ports:** If a port is closed, the target will respond with an RST (reset) packet.
- **Filtered ports:** If the port is filtered by a firewall, the target might not respond, or the scan may receive no response.
- **TCP Three-Way Handshake:**
A standard TCP connection involves a three-way handshake (SYN, SYN-ACK, ACK). TCP scanning techniques like SYN scanning don't fully complete the handshake, making them less detectable.
- **Popular Scanning Methods:**
 - **SYN Scan (Stealth Scan):** Sends SYN packets without completing the handshake, making it stealthy and faster.
 - **Connect Scan:** Establishes a full TCP connection with the target, providing more information but also being more detectable.
 - **Other Scans:** NULL, FIN, and Xmas scans utilize TCP header flags in different ways to identify port states.
- **Tools:**
Nmap is a widely used tool for TCP scanning, and there are many others available.
- **Importance:**
TCP scanning is a crucial part of network security assessments, helping to identify vulnerabilities and assess a system's security posture.

commands :-

```
# nmap -v -sT <target>
```

-v = this is used for printing live result
-sT = this is used for full scan

```

kali linux - VMware Workstation
File Edit View VM Tabs Help
Library Type here to search... Mar 30 23:15
My Computer Apps Places root@kali:/home/kj
Metasploitable2.kali linux
└── (root@kali) /home/kj
    $ nmap -sT testfire.net
    Starting Nmap 7.99 ( https://nmap.org ) at 2025-03-30 23:13 IST
    Initiating Ping Scan at 23:13
    Scanning testfire.net (65.61.137.117) [4 ports]
    Completed Ping Scan at 23:13, 0.32s elapsed (1 total hosts)
    Initiating Parallel DNS resolution of 1 host at 23:13
    Completed Parallel DNS resolution of 1 host at 23:13, 0.78s elapsed
    Initiating Connect Scan at 23:13
    Scanning testfire.net (65.61.137.117) [1000 ports]
    Discovered open port 443/tcp on 65.61.137.117
    Discovered open port 8080/tcp on 65.61.137.117
    Discovered open port 80/tcp on 65.61.137.117
    Discovered open port 2000/tcp on 65.61.137.117
    Completed Connect Scan at 23:13, 20.62s elapsed (1000 total ports)
    Nmap scan report for testfire.net (65.61.137.117)
    Host is up (0.09s latency).
    Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
    Not shown: 993 filtered tcp ports (no-response)
    PORT      STATE SERVICE
    80/tcp    open  http
    113/tcp   closed ident
    443/tcp   open  https
    2000/tcp  open  Cisco-Scp
    5000/tcp  open  sip
    8080/tcp  open  http-proxy
    8443/tcp  closed https-alt
    Read data files from: /usr/share/nmap
    Nmap done: 1 IP address (1 host up) scanned in 21.96 seconds
    Raw packets sent: 4 (152B) | Rcvd: 1 (28B)

    └── (root@kali) /home/kj

```

nmap -sS < target >

-sS = for half scan **or** hidden scan **or** stealth scan **or** 2 way handshake

```

kali linux - VMware Workstation
File Edit View VM Tabs Help
Library Type here to search... Mar 30 23:31
My Computer Apps Places root@kali:/home/kj
Metasploitable2.kali linux
└── (root@kali) /home/kj
    $ nmap -sS testfire.net
    Host is up (0.31s latency).
    Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
    All 1000 scanned ports on testfire.net (65.61.137.117) are in ignored states.
    Not shown: 1000 filtered tcp ports (no-response)
    Read data files from: /usr/share/nmap
    Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds
    Raw packets sent: 2010 (80.68KB) | Rcvd: 13 (572B)

    └── (root@kali) /home/kj
    $ nmap -v -sS testfire.net
    Starting Nmap 7.99 ( https://nmap.org ) at 2025-03-30 23:31 IST
    Initiating Ping Scan at 23:31
    Scanning testfire.net (65.61.137.117) [4 ports]
    Completed Ping Scan at 23:31, 0.57s elapsed (1 total hosts)
    Initiating Parallel DNS resolution of 1 host at 23:31
    Completed Parallel DNS resolution of 1 host at 23:31, 1.16s elapsed
    Initiating SYN Stealth Scan at 23:31
    Scanning testfire.net (65.61.137.117) [1000 ports]
    Discovered open port 443/tcp on 65.61.137.117
    Discovered open port 8080/tcp on 65.61.137.117
    Discovered open port 80/tcp on 65.61.137.117
    Discovered open port 5000/tcp on 65.61.137.117
    Discovered open port 2000/tcp on 65.61.137.117
    Completed SYN Stealth Scan at 23:31, 24.55s elapsed (1000 total ports)
    Nmap scan report for testfire.net (65.61.137.117)
    Host is up (0.30s latency).
    Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
    Not shown: 993 filtered tcp ports (no-response)
    PORT      STATE SERVICE
    80/tcp    open  http
    113/tcp   closed ident
    443/tcp   open  https
    2000/tcp  open  Cisco-Scp
    5000/tcp  open  sip
    8080/tcp  open  http-proxy
    8443/tcp  closed https-alt
    Read data files from: /usr/share/nmap
    Nmap done: 1 IP address (1 host up) scanned in 26.63 seconds
    Raw packets sent: 2009 (88.372KB) | Rcvd: 20 (812B)

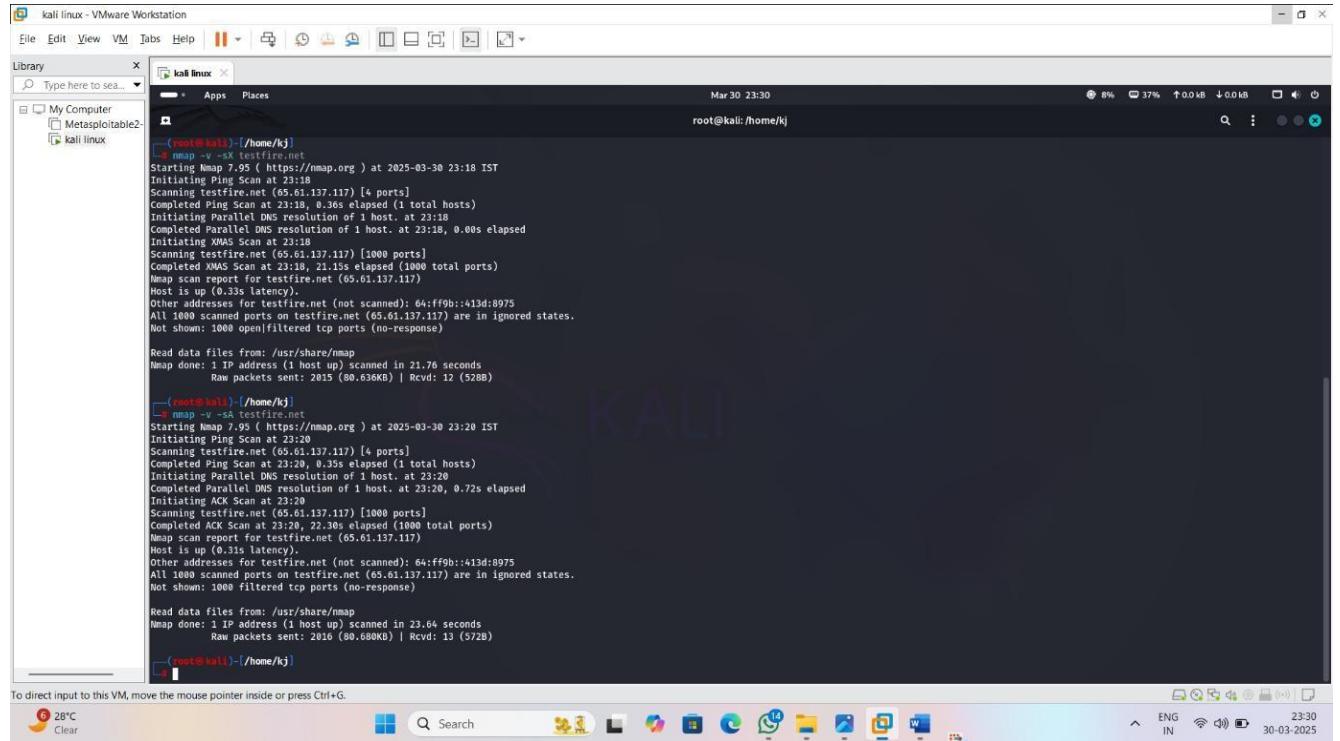
    └── (root@kali) /home/kj

```

nmap -sX < target >

-sX = xmas scan
nmap -sA < target >

-sA = for ACK scan to check target has firewall or not .



```
(root@kali) [~/home/kj]
└─# nmap -v -sX testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:18 IST
Initiating Ping Scan at 23:18
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 23:18, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:18
Completed Parallel DNS resolution of 1 host. at 23:18, 0.00s elapsed
Initiating XMAS Scan at 23:18
Scanning testfire.net (65.61.137.117) [1000 ports]
Completed XMAS Scan at 23:18, 21.15s elapsed (1000 total ports)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.33s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
All 1000 scanned ports on testfire.net (65.61.137.117) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.76 seconds
  Raw packets sent: 2015 (80.636KB) | Rcvd: 12 (528B)

(root@kali) [~/home/kj]
└─# nmap -v -sA testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:20 IST
Initiating Ping Scan at 23:20
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 23:20, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:20
Completed Parallel DNS resolution of 1 host. at 23:20, 0.72s elapsed
Initiating ACK Scan at 23:20
Scanning testfire.net (65.61.137.117) [1000 ports]
Completed ACK Scan at 23:20, 22.30s elapsed (1000 total ports)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.31s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
All 1000 scanned ports on testfire.net (65.61.137.117) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds
  Raw packets sent: 2016 (80.680KB) | Rcvd: 13 (572B)

(root@kali) [~/home/kj]
```

> UDP scanning method

UDP scanning involves sending UDP packets to various ports on a target host to determine which ports are open and potentially running services. This is a method for identifying open ports and services, similar to TCP scanning, but utilizing the UDP protocol. Unlike TCP scans which establish a connection, UDP scans rely on responses (or lack thereof) to infer port status.

Here's a more detailed explanation:

1. The Basics:

- **UDP (User Datagram Protocol):**

UDP is a connectionless transport protocol, meaning it doesn't require a pre-established connection before sending data.

- **Scanning Process:**

UDP scanning involves sending UDP packets to the target ports.

- **Response Interpretation:**

A response to a UDP packet indicates that the port is open and a service may be listening.

- **No Response:**

A lack of response can be interpreted as the port being closed or filtered, meaning the service is not active or the firewall is blocking UDP traffic.

2. How it Works:

- **Sending Packets:** The scanner sends UDP packets to each port on the target.
- **Empty or Payload Packets:** For many ports, a simple, empty UDP packet may be sent. For some known ports, like DNS (port 53) or SNMP (port 161), the scanner may send protocol-specific payloads to elicit a response.
- **Waiting for Responses:** The scanner waits for a response from the target.
- **ICMP (Internet Control Message Protocol):** If the port is closed or filtered, the target may send an ICMP "Destination Unreachable" message. This indicates that the port is not open.
- **No Response:** If no ICMP message or other response is received, the port is often assumed to be open.

3. Challenges and Considerations:

- **Open|Filtered Ambiguity:**

Distinguishing between a truly open port and a filtered port can be challenging.

- **Slower than TCP:**

UDP scanning can be slower than TCP scanning due to the nature of UDP and the need for ICMP responses.

- **UDP Services:**

While fewer UDP services are commonly scanned compared to TCP, there are still exploitable UDP services, and UDP scanning can be valuable for identifying them.

- **UDP is Connectionless:**

UDP's connectionless nature means that it's less reliable than TCP, and packet loss is possible.

- **Security Implications:**

Attackers can use UDP scans to identify open ports and potential vulnerabilities, making it important for network administrators to understand and mitigate this threat.

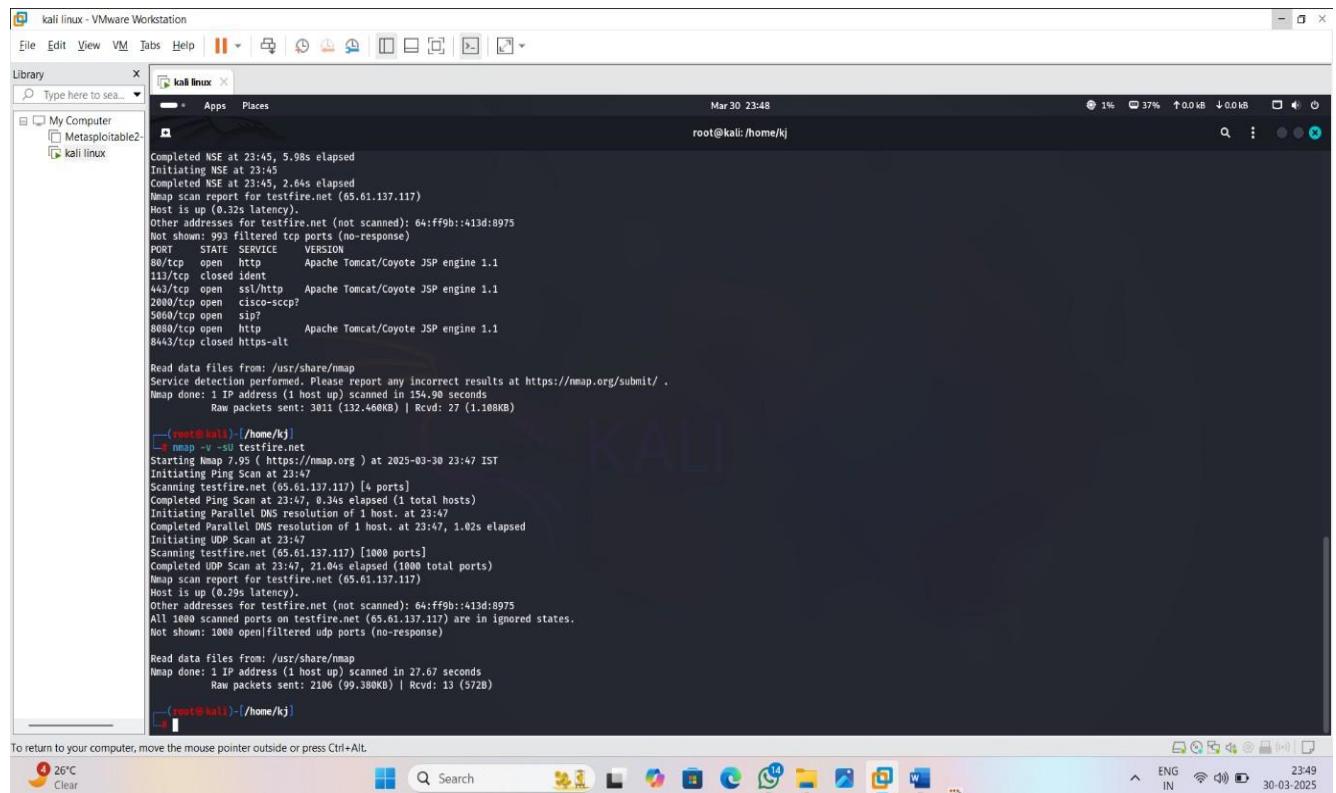
4. Nmap:

- Nmap (Network Mapper) is a widely used tool for port scanning, including UDP scans.
- The nmap -sU command is used to perform a UDP scan.
- Nmap can send specific payloads for certain ports to try and trigger a response from the service running on that port.

In essence, UDP scanning is a technique used to identify open UDP ports by sending UDP packets and observing responses, relying on ICMP messages to indicate closed ports, and interpreting the absence of responses as potentially open ports. It's a valuable tool for security professionals and attackers alike.

nmap -sU < target >

-sU = UDP scan



```
Completed NSE at 23:45, 5.98s elapsed
Initiating NSE at 23:45
Completed NSE at 23:45, 2.64s elapsed
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.32s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache Tomcat/Coyote JSP engine 1.1
113/tcp   closed ident
443/tcp   open  ssl/http Apache Tomcat/Coyote JSP engine 1.1
2000/tcp  open  cisco-sscp?
5060/tcp  open  sip?
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
8443/tcp  closed https-alt

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 154.90 seconds
Raw packets sent: 3011 (32.460KB) | Rcvd: 27 (1.108KB)

[root@kali]: /home/kj]
└─# nmap -sU testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 23:47 IST
Initiating Ping Scan at 23:47
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 23:47, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:47
Completed Parallel DNS resolution of 1 host. at 23:47, 1.02s elapsed
Initiating UDP Scan at 23:47
Scanning testfire.net (65.61.137.117) [1000 ports]
Completed UDP Scan at 23:47, 21.04s elapsed (1000 total ports)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.29 latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
All 1000 scanned ports on testfire.net (65.61.137.117) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.67 seconds
Raw packets sent: 2106 (99.380KB) | Rcvd: 13 (572B)

[root@kali]: /home/kj]
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

26°C Clear ENG IN 23:49 30-03-2025

nmap -v -sV <target>

-sV = check version

The screenshot shows a terminal window titled "kali linux - VMware Workstation". The terminal is running a command to scan the target IP address 65.61.137.117. The output of the nmap command is displayed, showing various ports and services identified on the target host.

```
Starting Nmap 7.05 ( https://nmap.org ) at 2025-03-30 23:42 IST
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 23:42
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 23:42, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:42
Completed Parallel DNS resolution of 1 host. at 23:42, 0.01s elapsed
Initiating SYN Stealth Scan at 23:42
Scanning testfire.net (65.61.137.117) [1000 ports]
Discovered open port 2000/tcp on 65.61.137.117
Discovered open port 80/tcp on 65.61.137.117
Discovered open port 8080/tcp on 65.61.137.117
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 5000/tcp on 65.61.137.117
Completed SYN Stealth Scan at 23:43, 49.22s elapsed (1000 total ports)
Initiating Service scan at 23:43
Scanning 5 services on testfire.net (65.61.137.117)
Completed Service scan at 23:45, 96.12s elapsed (5 services on 1 host)
NSE: Script scanning 65.61.137.117.
Initiating NSE at 23:45
Completed NSE at 23:45, 5.98s elapsed
Initiating NSE at 23:45
Completed NSE at 23:45, 2.64s elapsed
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.32s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 993 filtered tcp ports (no-response)
      STATE      SERVICE      VERSION
http/tcp      open   Apache Tomcat/Coyote JSP engine 1.1
https/tcp     closed  ident
443/tcp      open   ssl/http   Apache Tomcat/Coyote JSP engine 1.1
2000/tcp     open   cisco-sscp?
5000/tcp     open   sip?
8080/tcp     open   http      Apache Tomcat/Coyote JSP engine 1.1
8443/tcp    closed  https-alt

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 154.90 seconds
  Raw packets sent: 3011 (132.460KB) | Rcvd: 27 (1.108KB)
```

nmap -A -T4 -v < target >

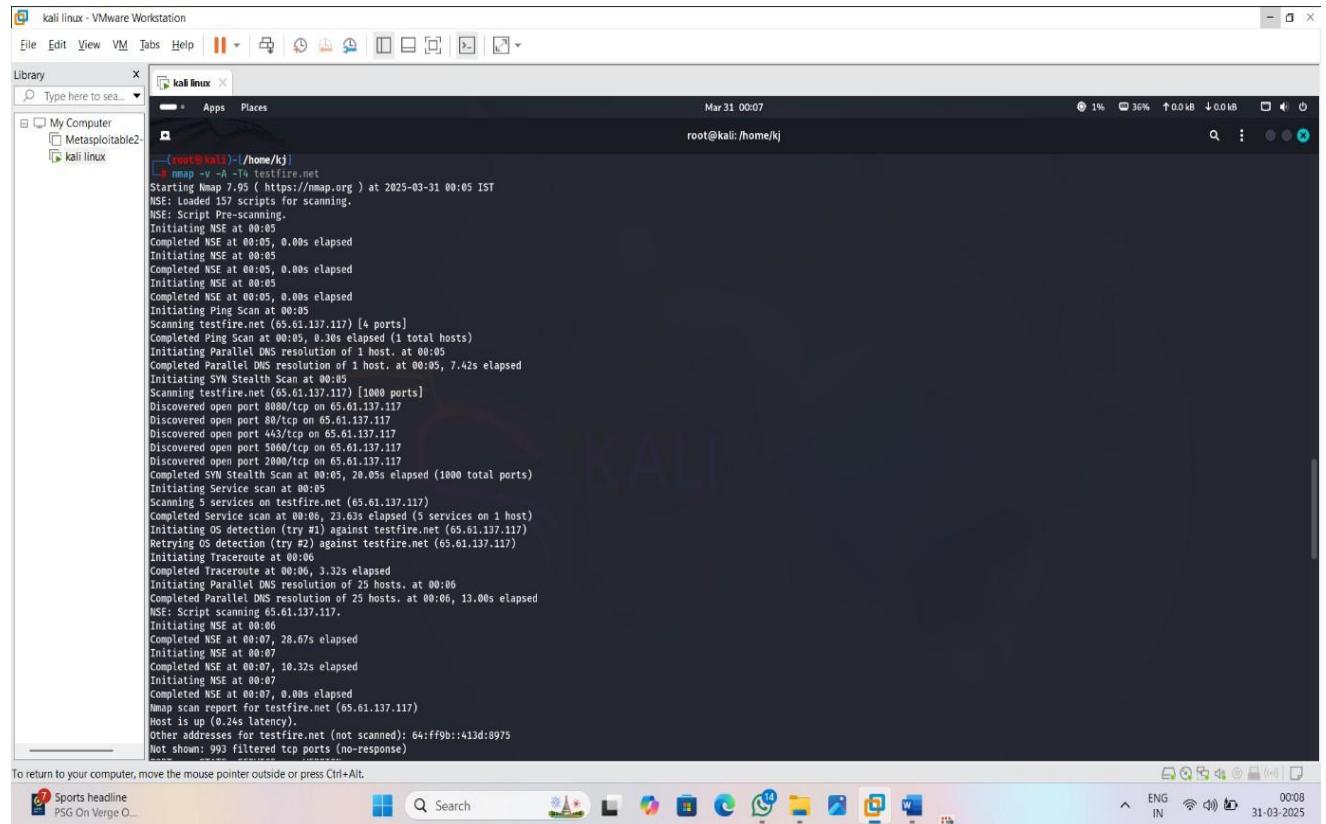
-A = for all types of scan (advance)

You should not use **-A** against target networks

without permission .

-T4 = is used for aggressive

Name : Kunal Jawale



The screenshot shows a terminal window titled "kali linux - VMware Workstation" running on a Kali Linux desktop. The terminal displays the output of an Nmap scan against the target "testfire.net" (IP 65.61.137.117). The scan results show several open ports, including 8080/tcp, 80/tcp, 443/tcp, 5060/tcp, and 2000/tcp. The output also includes OS detection information and a summary of the scan.

```
[root@kali ~]# nmap -v -A -T4 testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:05 IST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
Initiating Ping Scan at 00:05
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 00:05, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:05
Completed Parallel DNS resolution of 1 host. at 00:05, 7.42s elapsed
Initiating SYN Stealth Scan at 00:05
Scanning testfire.net (65.61.137.117) [1000 ports]
Discovered open port 8080/tcp on 65.61.137.117
Discovered open port 80/tcp on 65.61.137.117
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 5060/tcp on 65.61.137.117
Discovered open port 2000/tcp on 65.61.137.117
Completed SYN Stealth Scan at 00:05, 28.05s elapsed (1000 total ports)
Scanning 5 services on testfire.net (65.61.137.117)
Completed Service scan at 00:06, 23.63s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against testfire.net (65.61.137.117)
Retrying OS detection (try #2) against testfire.net (65.61.137.117)
Initiating Traceroute at 00:06
Completed Traceroute at 00:06, 3.32s elapsed
Initiating Parallel DNS resolution of 25 hosts. at 00:06
Completed Parallel DNS resolution of 25 hosts. at 00:06, 13.00s elapsed
NSE: Script scanning 65.61.137.117.
Initiating NSE at 00:06
Completed NSE at 00:07, 28.67s elapsed
Initiating NSE at 00:07
Completed NSE at 00:07, 10.32s elapsed
Initiating NSE at 00:07
Completed NSE at 00:07, 0.00s elapsed
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.24s latency).
Other addresses for testfire.net (not scanned): 64:ff9b::413d:8975
Not shown: 993 filtered tcp ports (no-response)
```

Name : Kunal Jawale

The image shows two Kali Linux virtual machines running in VMware Workstation. The top window displays an Nmap scan of a target with port 80/tcp open and Apache Tomcat/Coyote JSP engine 1.1. It also lists various SSL certificates and their fingerprints. The bottom window shows an Nmap traceroute from port 8443/tcp to the IP 195.89.101.185, listing 27 routers along the path. Both windows have standard Linux desktop toolbars at the top and bottom.

* OS discovery :-

OS (Operating System) discovery, also known as OS fingerprinting or banner grabbing, is a technique used to identify the operating system (OS) running on a target machine. This process involves analyzing network traffic and responses to probes sent to the target, allowing attackers or penetration testers to gather intelligence about the target system.

Why is OS discovery important?

- **Vulnerability Exploitation:**

Knowing the OS allows attackers to tailor their attacks to exploit known vulnerabilities specific to that operating system.

- **Network Reconnaissance:**

OS discovery is crucial for network reconnaissance, helping to understand the overall landscape of a network and identify potential targets.

- **Penetration Testing:**

Penetration testers use OS discovery to understand the environment they are testing and prepare appropriate exploits.

- **Security Audits:**

OS information is valuable for verifying system configurations and ensuring compliance with security standards.

How is OS discovery performed?

- **TCP/IP Stack Fingerprinting:**

Nmap and other tools use TCP/IP stack fingerprinting to send probes (packets) to the target and analyze the responses.

- **Response Analysis:**

The tool examines the responses, looking for patterns and characteristics unique to different operating systems.

- **Database Comparison:**

The collected information is compared against a database of known OS fingerprints.

- **Information Extraction:**

If a match is found, the tool provides details about the operating system.

Benefits of OS Discovery:

- **Enhanced Threat Modeling:**

Knowing the OS allows for more realistic threat models and better preparation for potential attacks.

- **Targeted Exploitation:**

OS information enables the use of specific exploits and tools designed for a particular OS.

- **Improved Security Practices:**

Understanding the OS helps system administrators implement appropriate security measures and configurations.

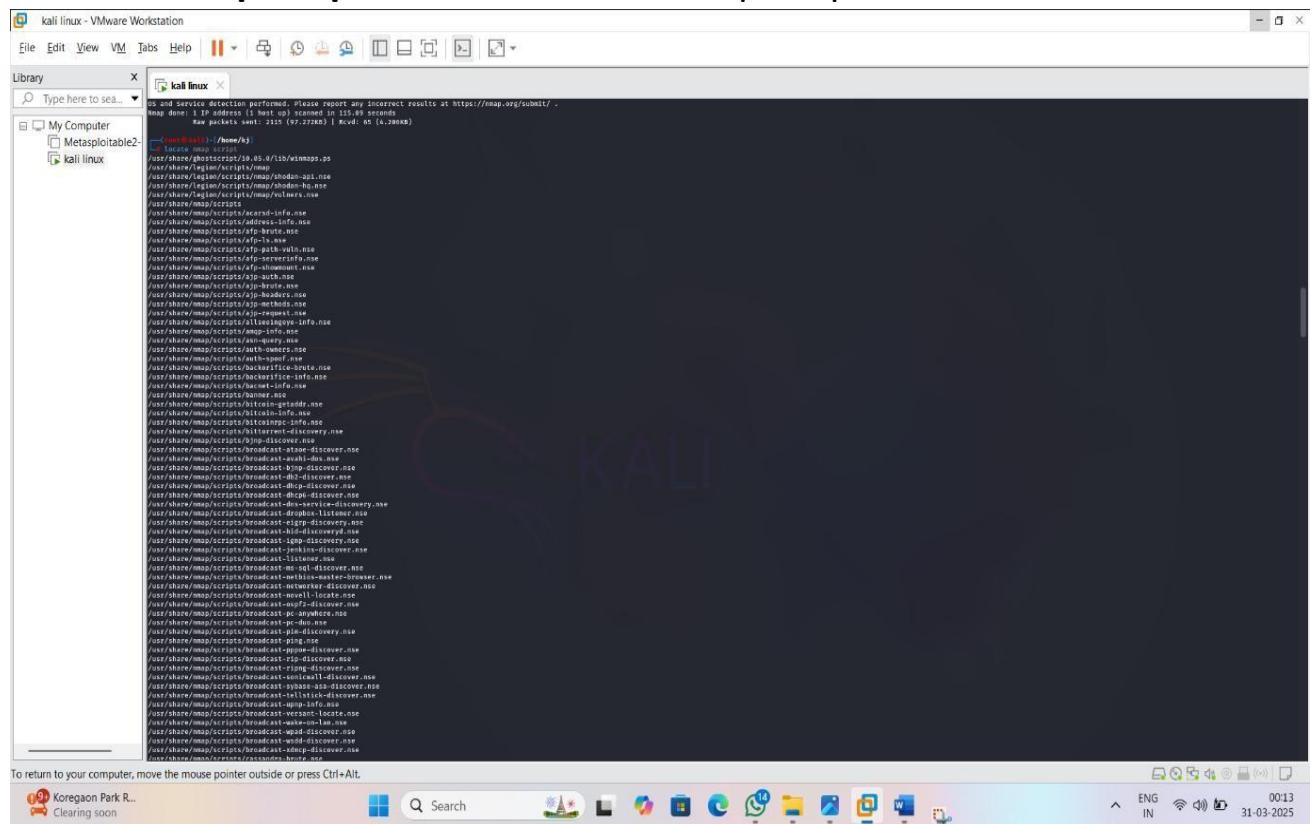
- **Faster Troubleshooting:**

OS information can aid in troubleshooting network and system issues.

OS discovery is also called banner grabbing and OS fingerprinting . it is used to determine the OS running on a remote target system .

Run nmap scripts :

locate nmap script :- this shows all nmap scripts



```
# nmap -v --script (copy the script which you want) <target> :- for run  
the script
```

```

kali linux - VMware Workstation
File Edit View VM Tabs Help || Library Applications Places Mar 31 00:17
root@kali:/home/kj
nmap -v --script /usr/share/nmap/scripts/ftp-brute.nse testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:15 IST
NSE: Loaded 2 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:15
Completed NSE at 00:15, 0.00s elapsed
Initiating Ping Scan at 00:15
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 00:15, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:15
Completed Parallel DNS resolution of 1 host. at 00:15, 1.26s elapsed
Initiating SYN Stealth Scan at 00:15
Completed SYN Stealth Scan at 00:16, 21.33s elapsed (1000 total ports)
Scanning testfire.net (65.61.137.117) [1000 ports]
Discovered open port 80/tcp on 65.61.137.117
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 80/tcp on 65.61.137.117
Discovered open port 2000/tcp on 65.61.137.117
Discovered open port 5060/tcp on 65.61.137.117
Completed SYN Stealth Scan at 00:16, 21.33s elapsed (1000 total ports)
Host is up (0.16s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8080/tcp  open  http-proxy
8443/tcp  closed https-alt

NSE: Script Post-scanning.
Initiating NSE at 00:16
Completed NSE at 00:16, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.85 seconds
Raw packets sent: 2007 (88.284KB) | Rcvd: 18 (748B)

```

- Here are some additional command for nmap # nmap -f <target>

-f = for fragmentation , -F = for fast scan

Normally -f is used to tiny fragment packets to bypass firewall and IDS

```

kali linux - VMware Workstation
File Edit View VM Tabs Help || Library Applications Places Mar 31 00:29
root@kali:/home/kj
NSE: Script Post-scanning.
Initiating NSE at 00:16
Completed NSE at 00:16, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.85 seconds
Raw packets sent: 2007 (88.284KB) | Rcvd: 18 (748B)

(root@kali):/home/kj
└─# nmap -v -f testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:18 IST
Initiating Ping Scan at 00:18
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 00:18, 0.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:18
Completed Parallel DNS resolution of 1 host. at 00:18, 0.00s elapsed
Initiating SYN Stealth Scan at 00:18
Completed SYN Stealth Scan at 00:18, 5.91s elapsed (100 total ports)
Host is up (0.16s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 93 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8080/tcp  open  http-proxy
8443/tcp  closed https-alt

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.37 seconds
Raw packets sent: 199 (8.732KB) | Rcvd: 10 (408B)

(root@kali):/home/kj
└─# nmap -v -g 80 testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:20 IST

```

Name : Kunal Jawale

```
# nmap -v -g 80 <target>
```

This command is used for spoofing or using fake identity .

```
# nmap -v -sO <target>
```

this is used for scan IP protocol

kali linux - VMware Workstation

File Edit View VM Tabs Help || Library

Type here to search

My Computer Metasploitable2 kali linux

Not shown: 993 filtered tcp ports (no-response)

PORT	STATE	SERVICE
80/tcp	open	http
113/tcp	closed	ident
443/tcp	open	https
2800/tcp	open	cisco-sscp
5060/tcp	open	sip
8080/tcp	open	http-proxy
8443/tcp	closed	https-alt

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 20.13 seconds
Raw packets sent: 2007 (86.284KB) | Rcvd: 18 (732B)

```
(root@kali:~/home/kali)
# nmap -v -o testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:21 IST
Initiating Ping Scan at 00:21
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 00:21, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:21
Completed Parallel DNS resolution of 1 host. at 00:21, 0.38s elapsed
Initiating IPProto Scan at 00:21
Scanning testfire.net (65.61.137.117) [256 ports]
Discovered open port 1/1p on 65.61.137.117
Completed IPProto Scan at 00:21, 22.40s elapsed (256 total ports)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.28s latency).
Other addresses for testfire.net (not scanned): 64:ff9b::413d:8975
Not shown: 255 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1 open icmp

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds
Raw packets sent: 518 (10.680KB) | Rcvd: 5 (140B)

(root@kali:~/home/kali)
# nmap -v -P testfire.net
Warning: The -P option is deprecated. Please use -PE
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:21 IST
Initiating Ping Scan at 00:21
Scanning testfire.net (65.61.137.117) [1 port]
Completed Ping Scan at 00:21, 0.32s elapsed (1 total hosts)
```

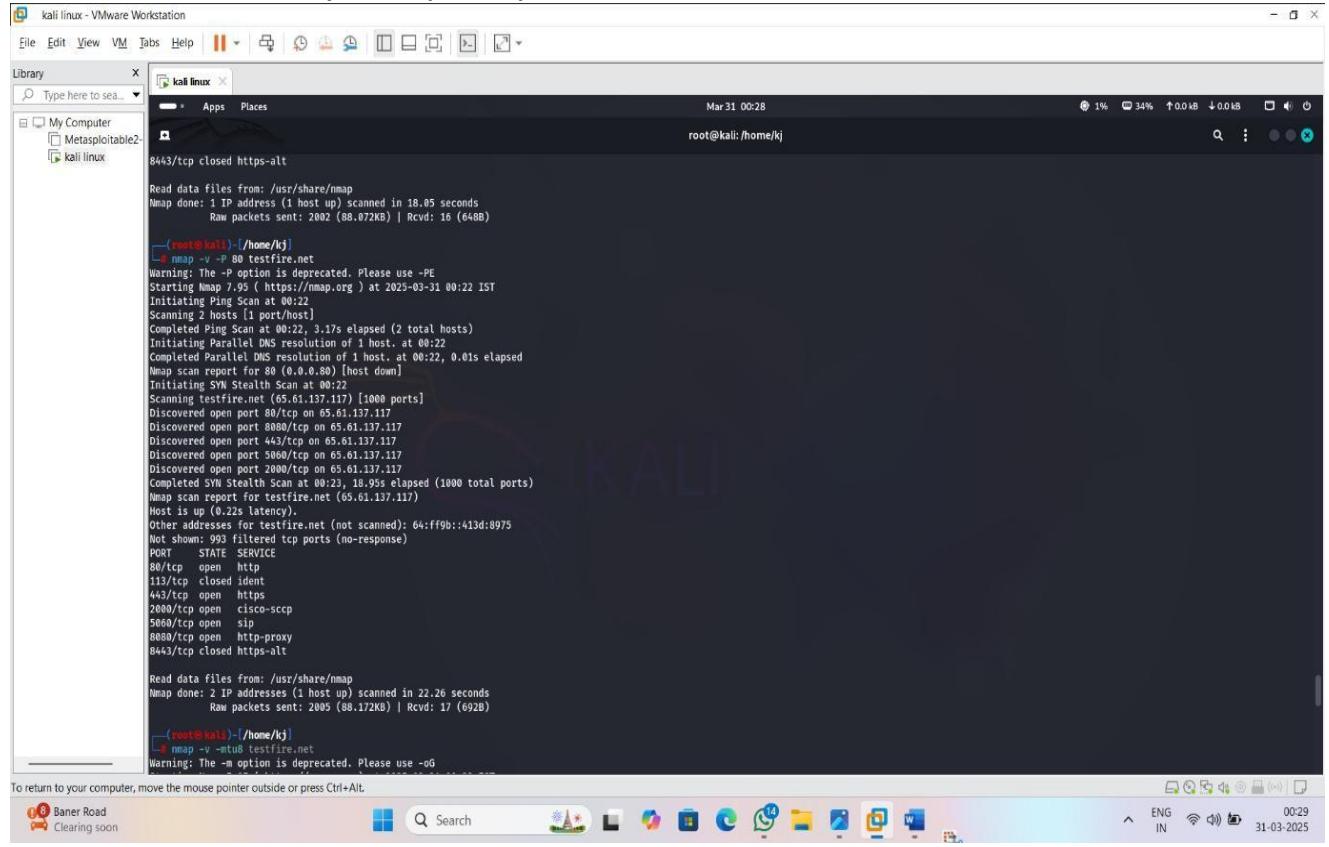
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Baner Road Clearing room

Search

ENG IN 00:29 31-03-2025

nmap -v -p < target >
 for only scan specific ports .



```

kali linux - VMware Workstation
File Edit View VM Tabs Help || Library Applications Places Mar 31 00:28
root@kali:/home/kj
kali linux
Type here to search
My Computer Metasploitable2 kali linux
8443/tcp closed https-alt
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.05 seconds
  Raw packets sent: 2002 (88.072KB) | Rcvd: 16 (648B)

[root@kali ~]# nmap -v -p 80 testfire.net
Warning: The -P option is deprecated. Please use -PE
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:22 IST
Initiating Ping Scan at 00:22
Scanning 2 hosts [1 port/host]
Completed Ping Scan at 00:22, 3.17s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:22
Completed Parallel DNS resolution of 1 host. at 00:22, 0.01s elapsed
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.24s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
80/tcp    open  ident
443/tcp   open  https
2000/tcp  open  cisco-sscp
5680/tcp  open  sip
8080/tcp  open  http-proxy
8443/tcp  closed https-alt

Read data files from: /usr/share/nmap
Nmap done: 2 IP addresses (1 host up) scanned in 22.26 seconds
  Raw packets sent: 2005 (88.172KB) | Rcvd: 17 (692B)

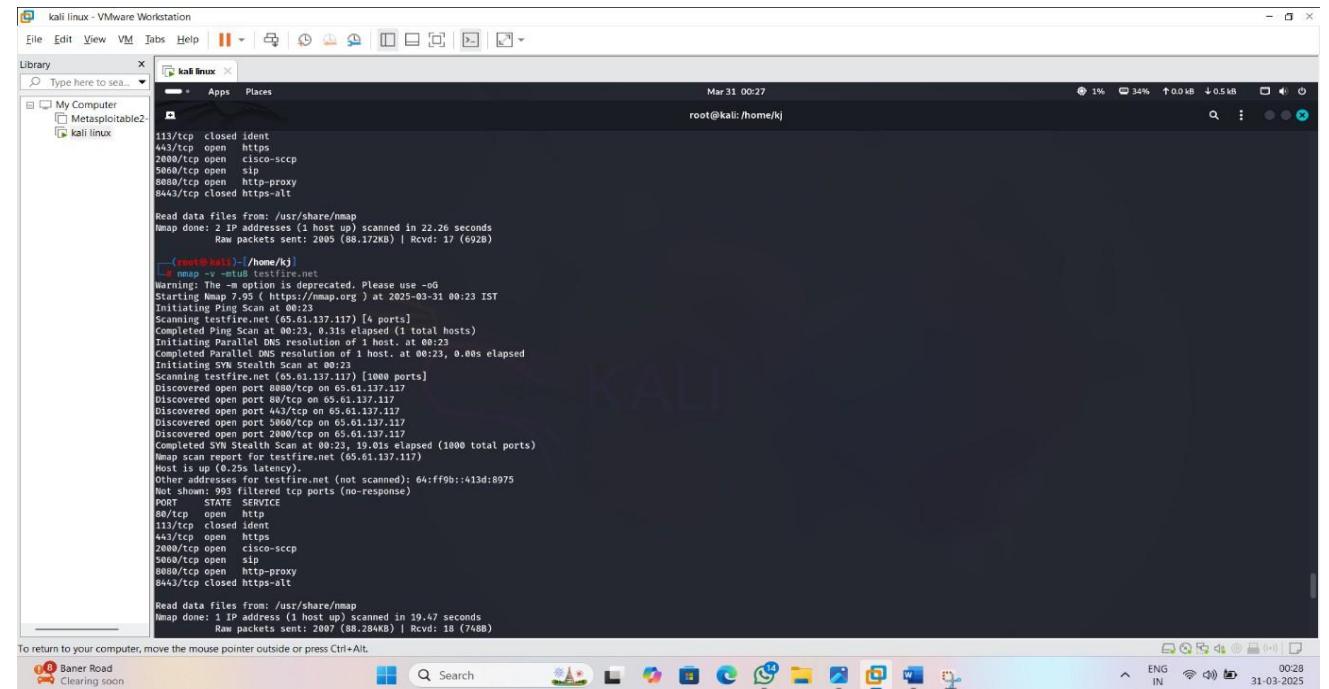
[root@kali ~]# nmap -v -mtu8 testfire.net
Warning: The -m option is deprecated. Please use -oG

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

nmap -v -mtu8 < target >

using mtu smaller packets are transmitted instead of sending one complete packet at a time . this techniques evades the filtering and detection mechanism



```

kali linux - VMware Workstation
File Edit View VM Tabs Help || Library Applications Places Mar 31 00:27
root@kali:/home/kj
kali linux
Type here to search
My Computer Metasploitable2 kali linux
113/tcp closed ident
443/tcp open  https
2000/tcp open  cisco-sscp
5680/tcp open  sip
8080/tcp open  http-proxy
8443/tcp closed https-alt
Read data files from: /usr/share/nmap
Nmap done: 2 IP addresses (1 host up) scanned in 22.28 seconds
  Raw packets sent: 2009 (88.172KB) | Rcvd: 17 (692B)

[root@kali ~]# nmap -v -mtu8 testfire.net
Warning: The -m option is deprecated. Please use -oG
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:23 IST
Initiating Ping Scan at 00:23
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 00:23, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:23
Completed Parallel DNS resolution of 1 host. at 00:23, 0.00s elapsed
Initiating SYN Stealth Scan at 00:23
Scanning testfire.net (65.61.137.117) [1000 ports]
Discovered open port 8880/tcp on 65.61.137.117
Discovered open port 88/tcp on 65.61.137.117
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 5680/tcp on 65.61.137.117
Discovered open port 2000/tcp on 65.61.137.117
Completed SYN Stealth Scan at 00:23, 19.01s elapsed (1000 total ports)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.24s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sscp
5680/tcp  open  sip
8080/tcp  open  http-proxy
8443/tcp  closed https-alt

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 19.47 seconds
  Raw packets sent: 2007 (88.284KB) | Rcvd: 18 (748B)

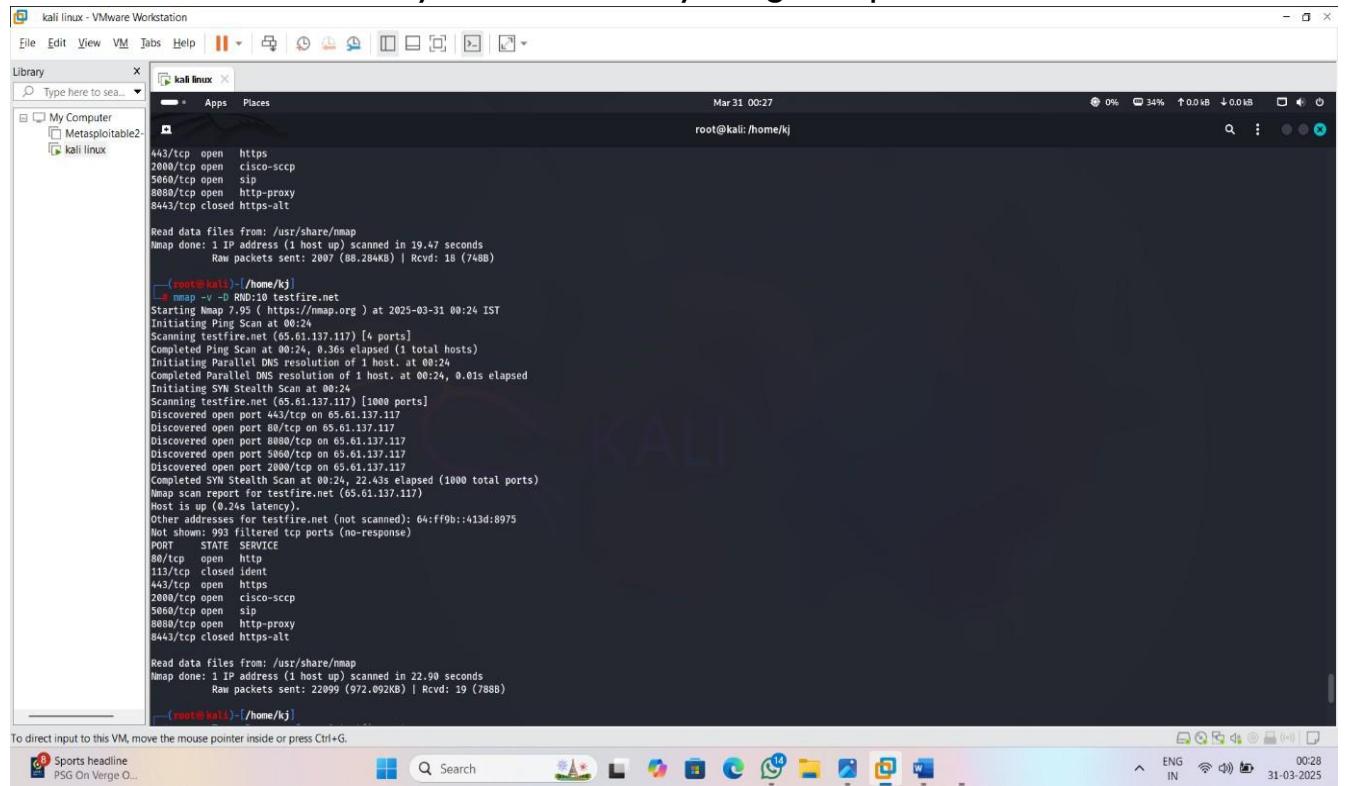

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Name : Kunal Jawale

nmap -v -D RND:10 <target>

This technique is used for hide IP using multiple IP
-D = to hide your IP or identity using multiple IP



```
root@kali:~/home/kj
# nmap -v -D RND:10 testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:24 IST
Initiating Ping Scan at 00:24
Scanning testfire.net (65.61.137.117) [4 ports]
Completed Ping Scan at 00:24, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:24
Completed Parallel DNS resolution of 1 host. at 00:24, 0.01s elapsed
Initiating SYN Stealth Scan at 00:24
Scanning testfire.net (65.61.137.117) [1000 ports]
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 88/tcp on 65.61.137.117
Discovered open port 8880/tcp on 65.61.137.117
Discovered open port 5060/tcp on 65.61.137.117
Discovered open port 2000/tcp on 65.61.137.117
Completed SYN Stealth Scan at 00:24, 22.43s elapsed (1000 total ports)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.24s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8880/tcp  open  http-proxy
9443/tcp  closed https-alt

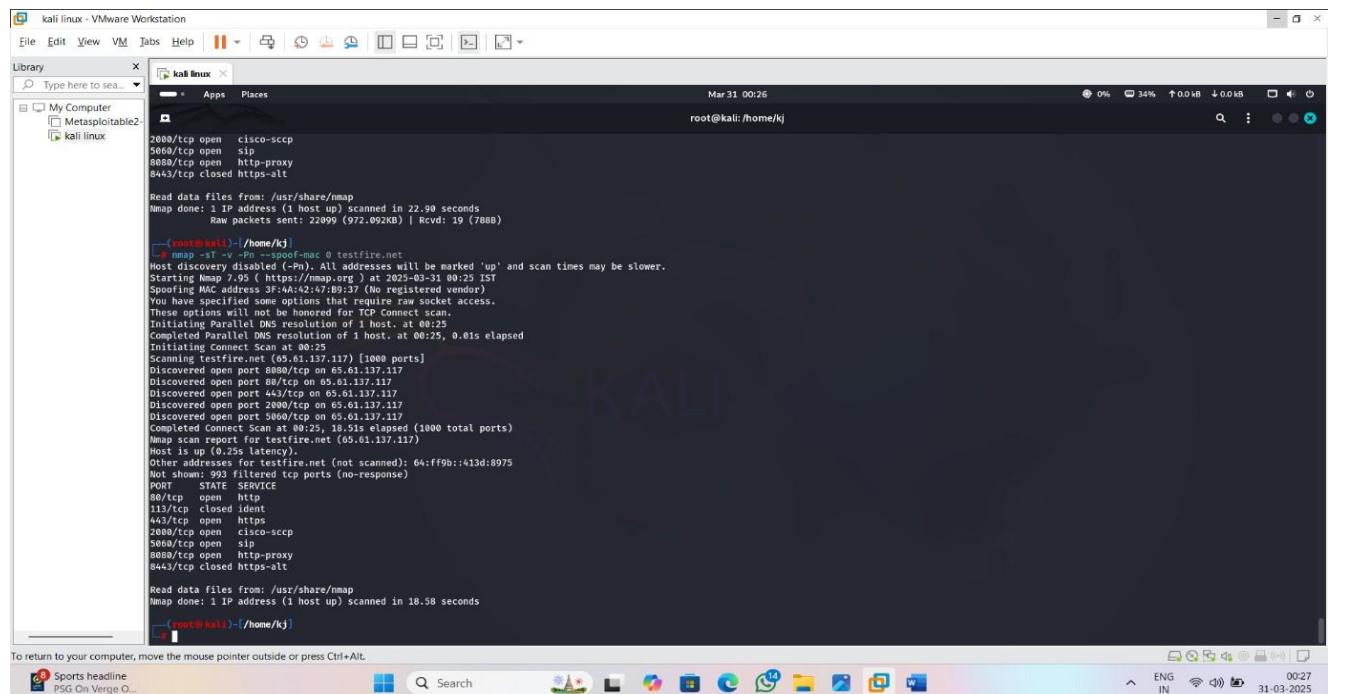
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 22.00 seconds
Raw packets sent: 22099 (972.092KB) | Rcvd: 19 (788B)

(root@kali):~/home/kj
```

nmap -sT -v -pn -- spoof-mac 0 < target>

To hide or spoofing mac -address

0 = for random ac address



```
root@kali:~/home/kj
# nmap -sT -v -pn -- spoof-mac 0 testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 00:25 IST
Nmap discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Scanning testfire.net (65.61.137.117) [1000 ports]
You have specified some options that require raw socket access.
These options will now be honored for TCP Connect scan.
Initiating Parallel DNS resolution of 1 host. at 00:25
Completed Parallel DNS resolution of 1 host. at 00:25, 0.01s elapsed
Initiating Connect Scan at 00:25
Scanning testfire.net (65.61.137.117) [1000 ports]
Discovered open port 8800/tcp on 65.61.137.117
Discovered open port 88/tcp on 65.61.137.117
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 2000/tcp on 65.61.137.117
Discovered open port 5060/tcp on 65.61.137.117
Completed Connect Scan at 00:25, 18.51s elapsed (1000 total ports)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.25s latency).
Other addresses for testfire.net (not scanned): 64:ff9b:413d:8975
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8880/tcp  open  http-proxy
9443/tcp  closed https-alt

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.58 seconds

(root@kali):~/home/kj
```

- Here are some port scanning technique using msfconsole :

Commands :::

msfconsole :- to run metasploitable
>search portscan :- for searching related portscan
>use 5 :- you choose whatever you want
>set RHOST <IP> :- to set IP
> set ports :- to set port range
> show :- to show
> run:- for scanning

Name : Kunal Jawale

The screenshot shows a Kali Linux VM running in VMware Workstation. The terminal window displays the Metasploit framework version 6.4.50-dev. It includes a welcome message, exploit counts (2496 exploits, 1283 auxiliary, 431 post, 1610 payloads, 49 encoders, 13 nops, 9 evasion), and links to documentation and search functions. Below this, a list of matching modules is shown, followed by a table of auxiliary/scanner modules. The table includes columns for Name, Disclosure Date, Rank, Check, and Description. The last module listed is auxiliary/scanner/http/wordpress_pingback_access. The user then interacts with the msf6 prompt to set the RHOST to 192.168.1.1 and run the module.

```
(root㉿kali)-[~/kali]
└─# msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

[metasploit v6.4.50-dev
+ --=[ 2496 exploits - 1283 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
search portscan
msf6 > search portscan

Matching Modules
=====
# Name          Disclosure Date  Rank   Check  Description
- -----
0 auxiliary/scanner/ftpbounce      .          normal  No    FTP Bounce Port Scanner
1 auxiliary/scanner/natpmp/natpmp_portscanner .          normal  No    NAT-PMP External Port Scanner
2 auxiliary/scanner/sap/sap_router_portscanner .          normal  No    SAPRouter Port Scanner
3 auxiliary/scanner/portscan/xmas     .          normal  No    TCP "Xmas" Port Scanner
4 auxiliary/scanner/portscan/ack     .          normal  No    TCP ACK Firewall Scanner
5 auxiliary/scanner/portscan/tcp     .          normal  No    TCP Port Scanner
6 auxiliary/scanner/portscan/syn     .          normal  No    TCP SYN Port Scanner
7 auxiliary/scanner/http/wordpress_pingback_access .          normal  No    Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use ? or use auxiliary/scanner/http/wordpress_pingback_access

msf6 > use 5
msf6 auxiliary(scanner/portscan/tcp) > set RHOST 192.168.1.1
RHOST => 192.168.1.1
msf6 auxiliary(scanner/portscan/tcp) > run
[*] 192.168.1.1:19200 - TCP OPEN
```

* **hping3 :-** hping3 is a network tool that's able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies .

📌 What is hping3?

hping3 is an advanced network packet crafting tool that allows you to generate and manipulate packets for various network protocols, including TCP, UDP, ICMP, and RAW-IP. It is primarily used for network security testing, firewall testing, advanced network diagnostics, and even penetration testing. Think of it as a more powerful version of the traditional ping command, but with much more control over the packets being sent.

🌐 Main Features of hping3:

1. TCP/IP Packet Manipulation:

You can craft and send custom TCP, UDP, ICMP, and RAW-IP packets.

2. Port Scanning:

hping3 can perform basic to advanced port scanning.

3. Firewall Testing:

Test firewall rules by crafting specific packets and analyzing the responses.

4. Network Trace Routing:

Similar to traceroute, you can track the path packets take across the network.

5. Advanced Packet Crafting:

You have control over packet headers, flags (SYN, ACK, FIN), TTL, window size, and more.

6. Flooding and DoS Simulation:

Simulate high packet loads to test the resilience of servers.

7. Data Transfer Testing:

Send raw data over different protocols to test throughput and reliability.

8. OS Fingerprinting:

Infer the operating system of a remote host by analyzing packet responses.

📌 Basic Syntax of hping3:

hping3 [options] [host]

Common Options:

Option	Description
-c <count>	Number of packets to send
-i <interval>	Interval between packets (e.g., -i u1000 for 1ms)
-S	Send a SYN packet (used in SYN scans)
-A	Send an ACK packet
-F	Send a FIN packet
-P	Send a PUSH packet
-R	Send an RST packet
-U	Send a UDP packet
-p <port>	Specify the target port
-t <ttl>	Set the TTL (Time To Live) value
-V	Verbose output
--flood	Send packets as fast as possible
--rand-source	Randomize the source IP address

❖ Examples of hping3 Usage:

▢ ICMP Ping (like traditional ping):

```
hping3 -1 192.168.1.1
```

- -1 indicates ICMP mode (like a normal ping).
- This sends ICMP Echo Requests to 192.168.1.1.

▢ SYN Scan on Port 80:

```
hping3 -S -p 80 192.168.1.1
```

- -S sends a SYN packet.
- -p 80 targets port 80.
- Useful for testing if a web server is open.

▢ ACK Scan to Test Firewall Rules:

```
hping3 -A -p 22 192.168.1.1
```

- -A sends an ACK packet.
- -p 22 targets the SSH port (22).
- If there's no response, it could indicate a stateful firewall is blocking it.

4 Flood a Target with UDP Packets:

```
hping3 --flood -2 -p 80 192.168.1.1
```

- --flood sends packets as fast as possible.
- -2 selects UDP mode.
- Be cautious—this can overwhelm the target system.

5 Traceroute using TCP instead of ICMP:

```
hping3 -S -p 80 --traceroute 192.168.1.1
```

- --traceroute traces the path.
- TCP packets are used instead of ICMP.

6 Sending Custom Data in TCP Packet:

```
hping3 -S -p 80 --data 40 192.168.1.1
```

- --data 40 adds 40 bytes of payload to the packet.



Advanced Usage Scenarios:

1. Firewall Evasion:

hping3 allows you to change packet headers to bypass basic firewall rules.

2. MTU Path Discovery:

You can test the Maximum Transmission Unit of a path by setting the packet size and observing the responses.

3. Operating System Fingerprinting:

By analyzing TCP/IP responses, you can deduce the OS of the target.

4. Idle Scanning:

Use a third-party host as a "zombie" to determine open ports without revealing your own IP.



⚠ Legal and Ethical Considerations:

- hping3 is a **powerful tool** often used in network testing and security auditing.
- **Unauthorized usage** on networks you do not own or have permission to test is **illegal** and violates cybersecurity laws.

- Always have **explicit permission** before testing any network.

Commands :

man hping3 :- this command is show you how hping3 works and their commands .

```

kali linux - VMware Workstation
File Edit View VM Tabs Help || Library Apps Places Mar 31 00:43
root@kali:/home/kali
System Manager's Manual
HPING3(8) HPING3(8)

NAME
    hping3 - send (almost) arbitrary TCP/IP packets to network hosts

SYNOPSIS
    hping3 [ -hvngVnZ012WrfvykQhFSRPAuXyjBwUTG ] [ -c count ] [ -i wait ] [ --fast ] [ -T interface ] [ -9 signature ] [ -a host ] [ -t ttl ] [ -m in id ] [ -w ip protocol ] [ -g fragoff ] [ -m mtu ] [ -o tos ] [ -c icmp type ] [ -K icmp code ] [ -s source port ] [ -p[t][+] dest port ] [ -w tcp window ] [ -o tcp offset ] [ -m tcp sequence number ] [ -L tcp ack ] [ -d data size ] [ -E filename ] [ -e signature ] [ -i icmp-inver version ] [ -ic平-ic平en length ] [ -sicmp-ic平en length ] [ --icmp-ic平id id ] [ --icmp-ic平roto protocol ] [ --icmp-cksum checksum ] [ --icmp-ts ] [ -ic平-addr ] [ --tcpexitcode ] [ --tcp-mss ] [ --tcp-timestamp ] [ --tr-stop ] [ --tr-keep-ttl ] [ --tr-no-rtt ] [ --rand-dest ] [ --rand-source ] [ --beep ] hostname

DESCRIPTION
    hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping3 you are able to perform at least the following stuff:
    - Test firewall rules
    - Advanced port scanning
    - Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
    - Path MTU discovery
    - Transferring files between even really fascist firewall rules.
    - Traceroute-like under different protocols.
    - Firewalk-like usage.
    - Remote OS fingerprinting.
    - TCP/IP stack auditing.
    - A lot of others.

    It's also a good didactic tool to learn TCP/IP. hping3 is developed and maintained by antirez@invece.org and is licensed under GPL version 2. Development is open so you can send me patches, suggestion and affronts without inhibitions.

HPING SITE
    primary site at http://www.hping.org. You can found both the stable release and the instruction to download the latest source code at http://www.hping.org/download.html

BASE OPTIONS
    -h --help
        Show an help screen on standard output, so you can pipe to less.

    -v --version
        Show version information and API used to access to data link layer, linux sock packet or libpcap.

    -c --count count
        Stop after sending (and receiving) count response packets. After last packet was send hping3 wait COUNTREACHED_TIMEOUT seconds target host replies. You are able to tune COUNTREACHED_TIMEOUT editing
        Manual page hping3(8) line 1 (press h for help or q to quit)

```

- Here are some **hping3 command which is used for down any target and you should not use against target network without permission**

hping3 -I <IP> -a <IP> -p <port no> --fast

-I = ICMP

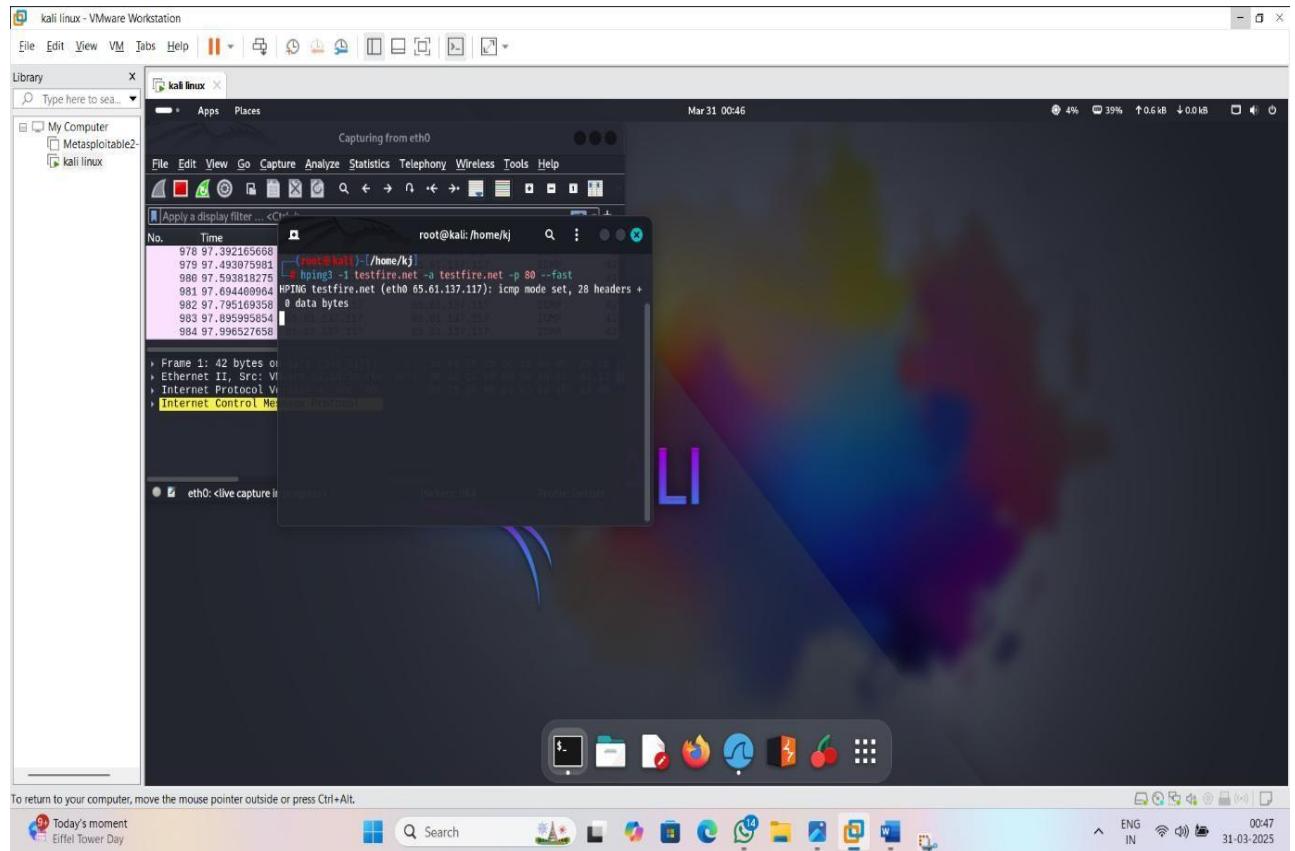
-a = for spoofing

-p = for open port

-- faster = to fast scan

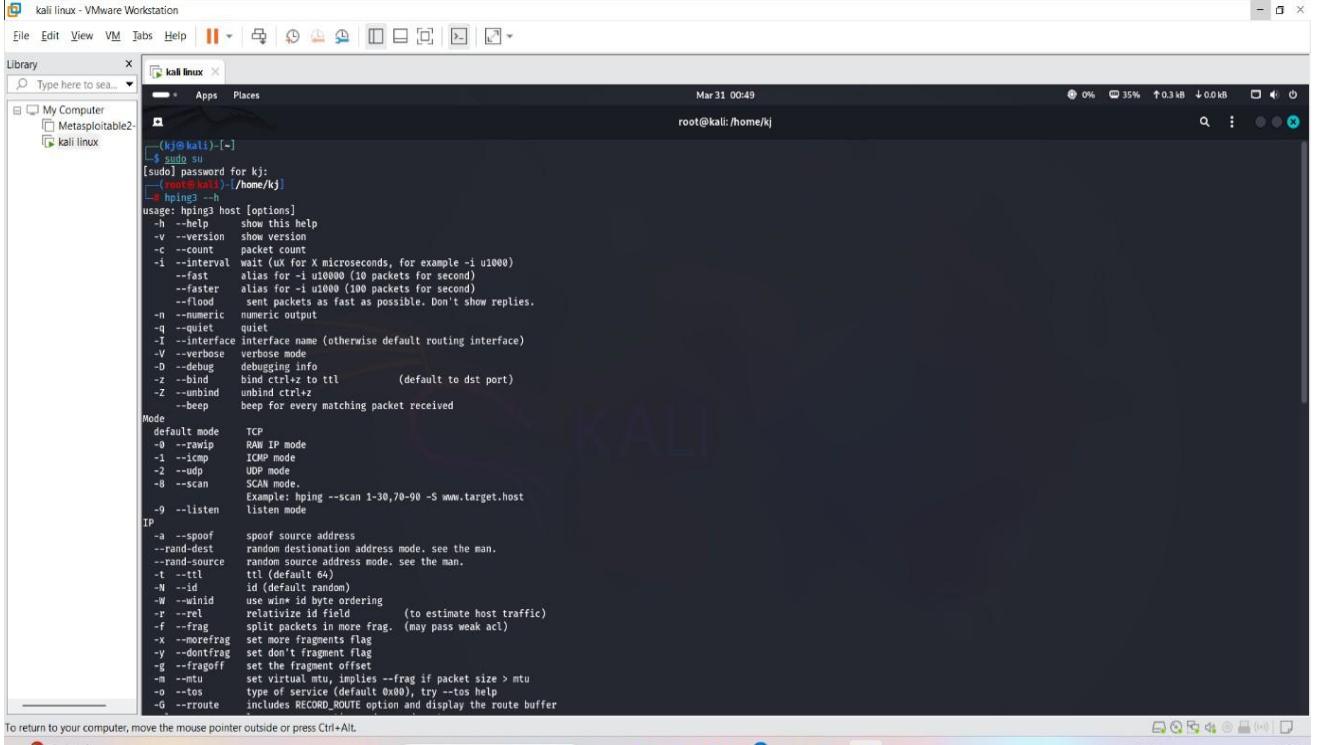
-- flood = 10 time faster

-c = countset



```
# hpng3 -1 <IP> --rand-source -p <port no> --faster
--rand-source = for random search
```

```
# hpng3 –help = for commands
```



The screenshot shows a terminal window titled "kali linux - VMware Workstation" running on Kali Linux. The user is viewing the man page for the hping3 command. The terminal window includes a menu bar with File, Edit, View, VM, Tabs, Help, and various icons. The status bar at the bottom right shows battery level (0%), signal strength (35%), and system information (root@kali: /home/kj). The terminal itself has a dark background with white text. It displays the command [sudo] password for kj: followed by the full hping3 man page. The man page covers various options for host, Mode (TCP, RAW IP, ICMP, UDP, SCAN), and IP spoofing parameters like --spoof, --rand-dest, and --ttl.

```
[sudo] password for kj:  
[kj@kali:~] hping3 --h  
usage: hping3 host [options]  
-h --help show this help  
-v --version show version  
-c --count packet count  
-i --interval wait (uX for X microseconds, for example -i u1000)  
--fast alias for -i u10000 (10 packets for second)  
--faster alias for -i u1000 (100 packets for second)  
--flood sent packets as fast as possible. Don't show replies.  
-n --numeric numeric output  
-q --quiet quiet  
-I --interface interface name (otherwise default routing interface)  
-V --verbose verbose mode  
-D --debug debugging info  
-z --bind bind ctrlz to ttl (default to dst port)  
-Z --unbind unbind ctrlz  
--beep beep for every matching packet received  
Mode  
default mode TCP  
-0 --rawip RAW IP mode  
-1 --icmp ICMP mode  
-2 --udp UDP mode  
-8 --scan SCAN mode.  
Example: hping --scan 1-30,70-90 -S www.target.host  
-9 --listen listen mode  
IP  
-a --spoof spoof source address  
--rand-dest random destination address mode. see the man.  
--rand-source random source address mode. see the man.  
-t --ttl ttl (default 64)  
-N --id id (default random)  
-W --winid use win* id byte ordering  
-r --rel relativize id field (to estimate host traffic)  
-f --frag split packets in more frag. (may pass weak acl)  
-x --morefrag set more fragments flag  
-y --dontrfrag set don't fragment flag  
-g --fragoff set the fragment offset  
-m --mtu set maximum transmission unit --frag if packet size > mtu  
-o --tos type of service (default 0x00), try --tos help  
-d --rroute includes RECORD_ROUTE option and display the route buffer
```

Name : Kunal Jawale