Name : Kunal Jawale

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 use an attacker to create 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

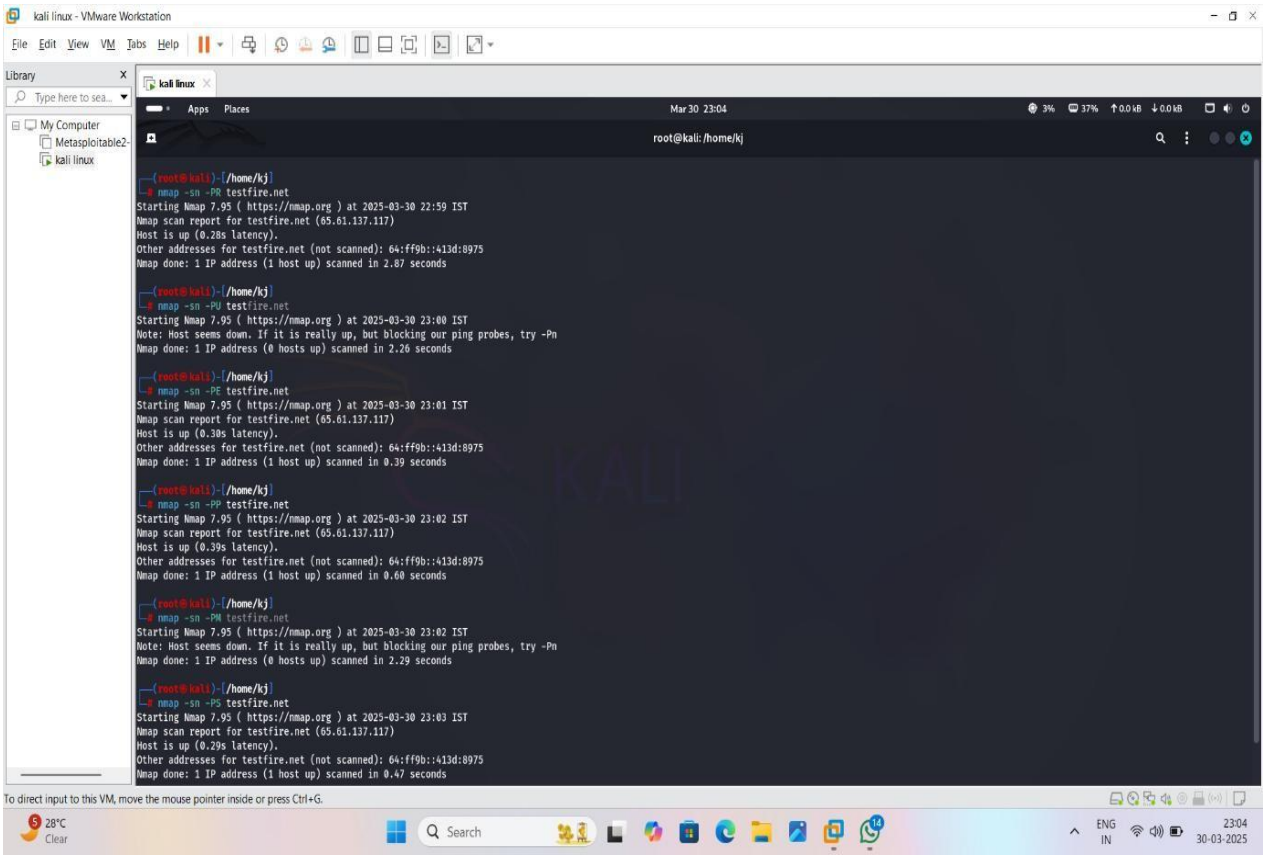
 # nmap -PA < target>

-PA = for TCP ACK ping scan

 # nmap -PO < target >

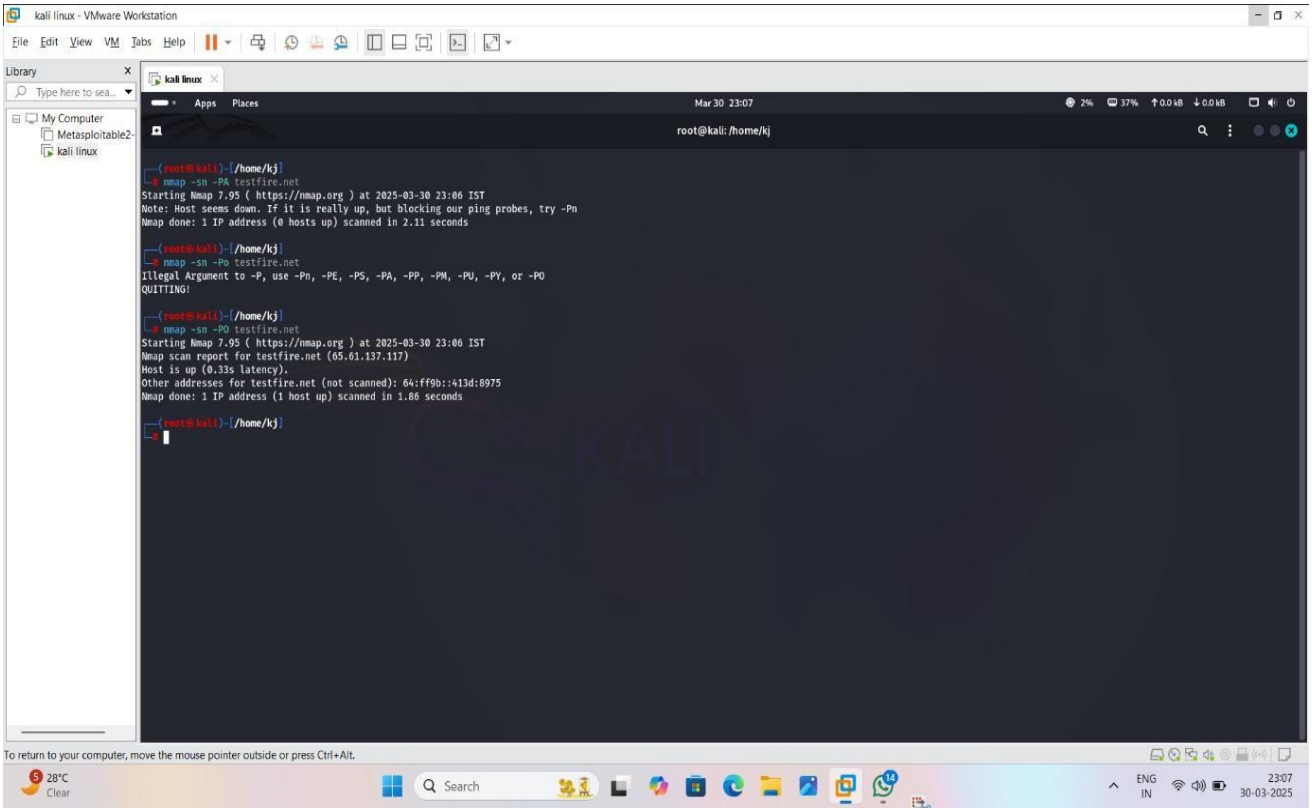
-PO = for IP protocol ping scan / this technique sends different probe packets of different IP protocols to the target .

Name : Kunal Jawale



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

Name : Kunal Jawale



- **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.

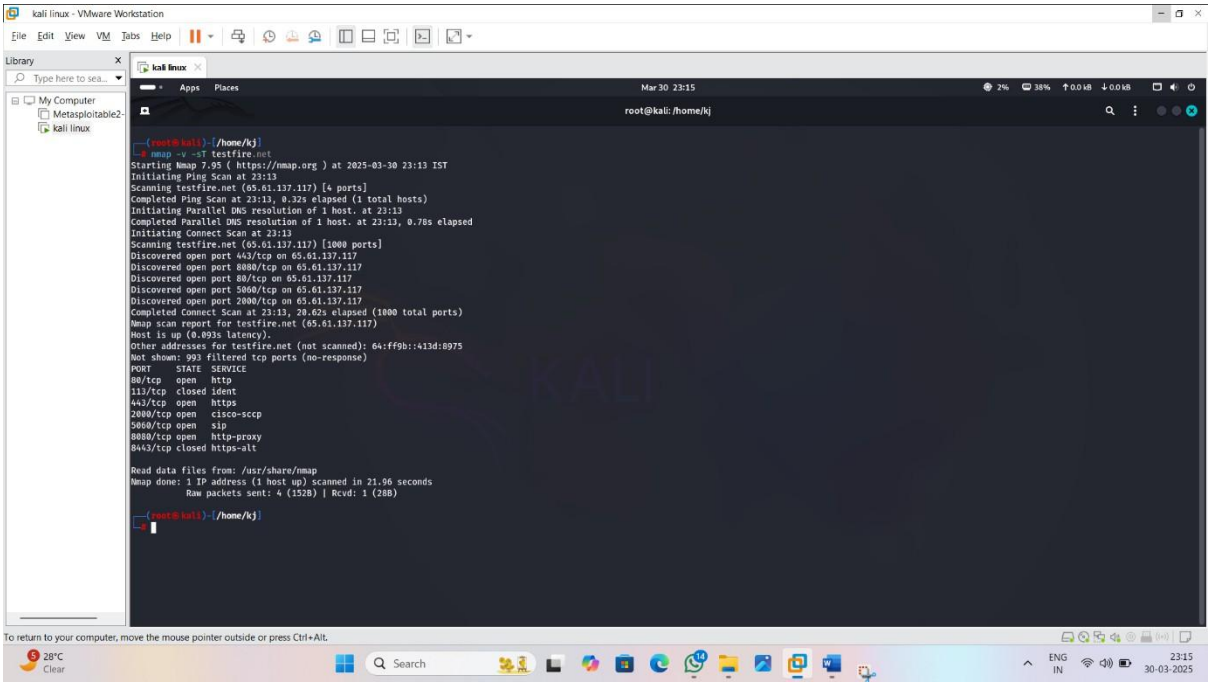
commands :-

 # nmap -v -sT < target >

-v = this is used for printing live result

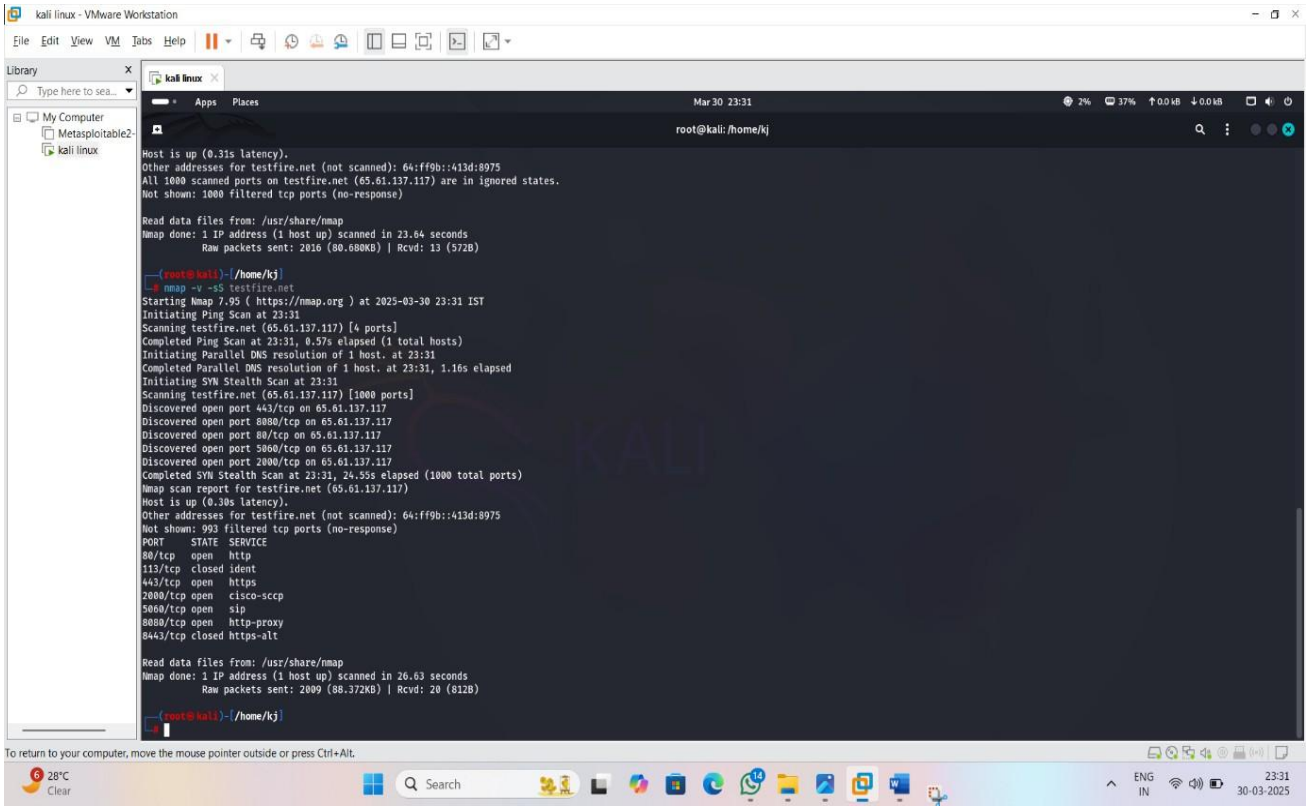
-sT = this is used fot full scan

Name : Kunal Jawale



 # nmap -sS < target >

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



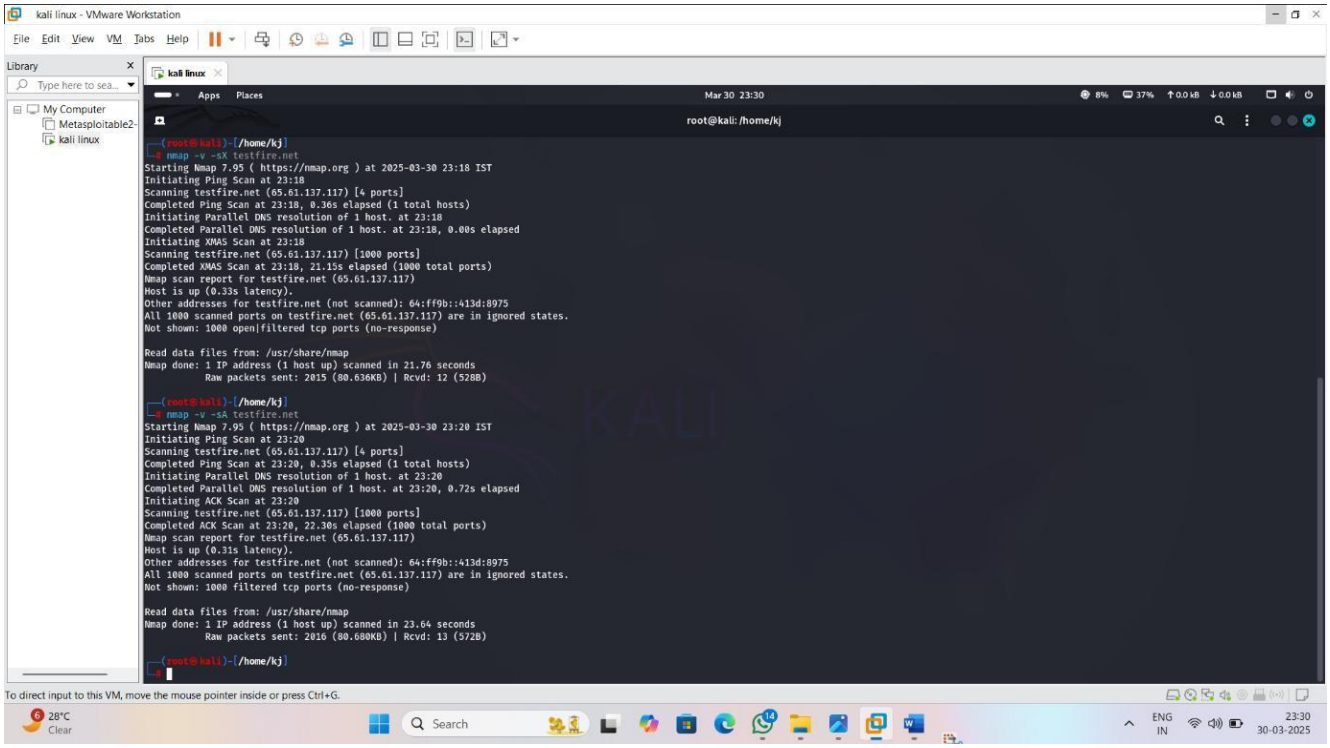
 # nmap -sX < target >

Name : Kunal Jawale

-sX = xmas scan

 # nmap -sA < target >

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



> 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:

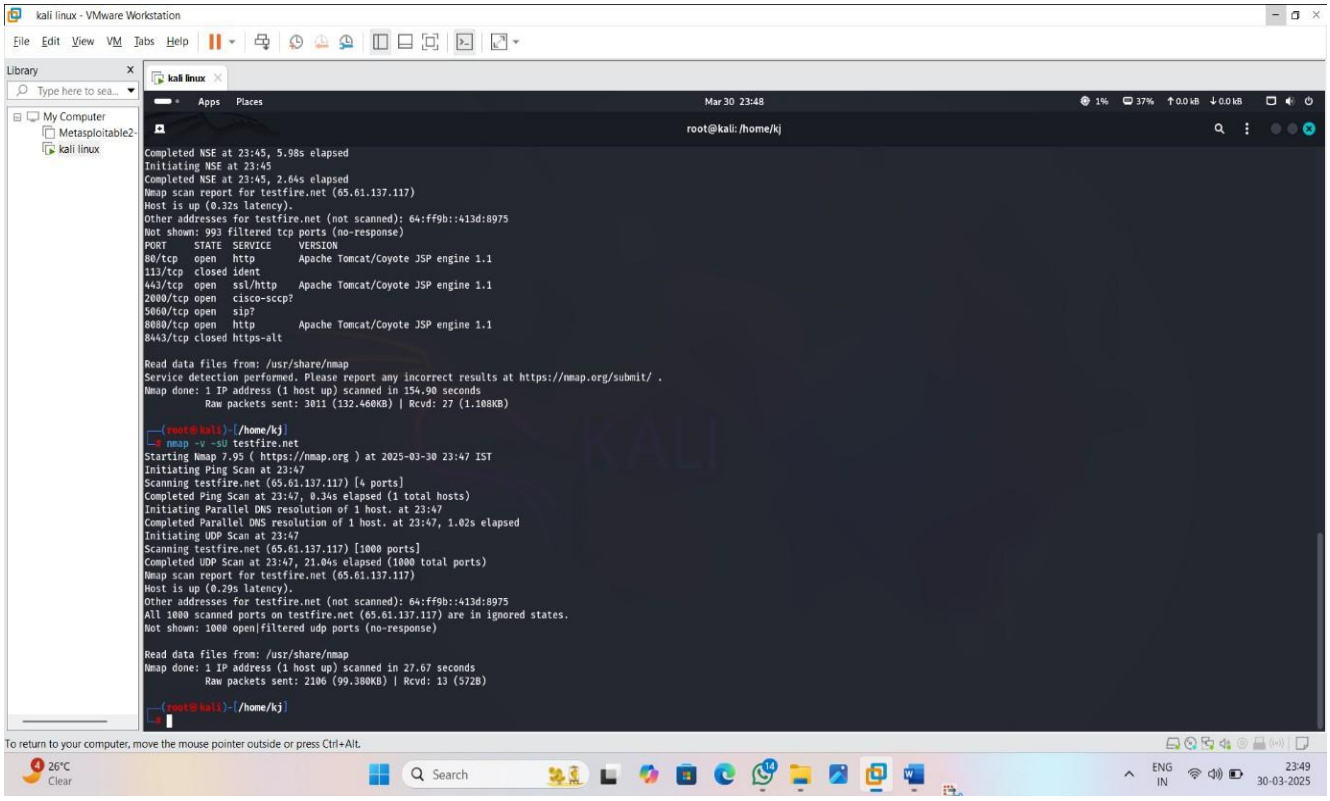
Name : Kunal Jawale

- 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 >

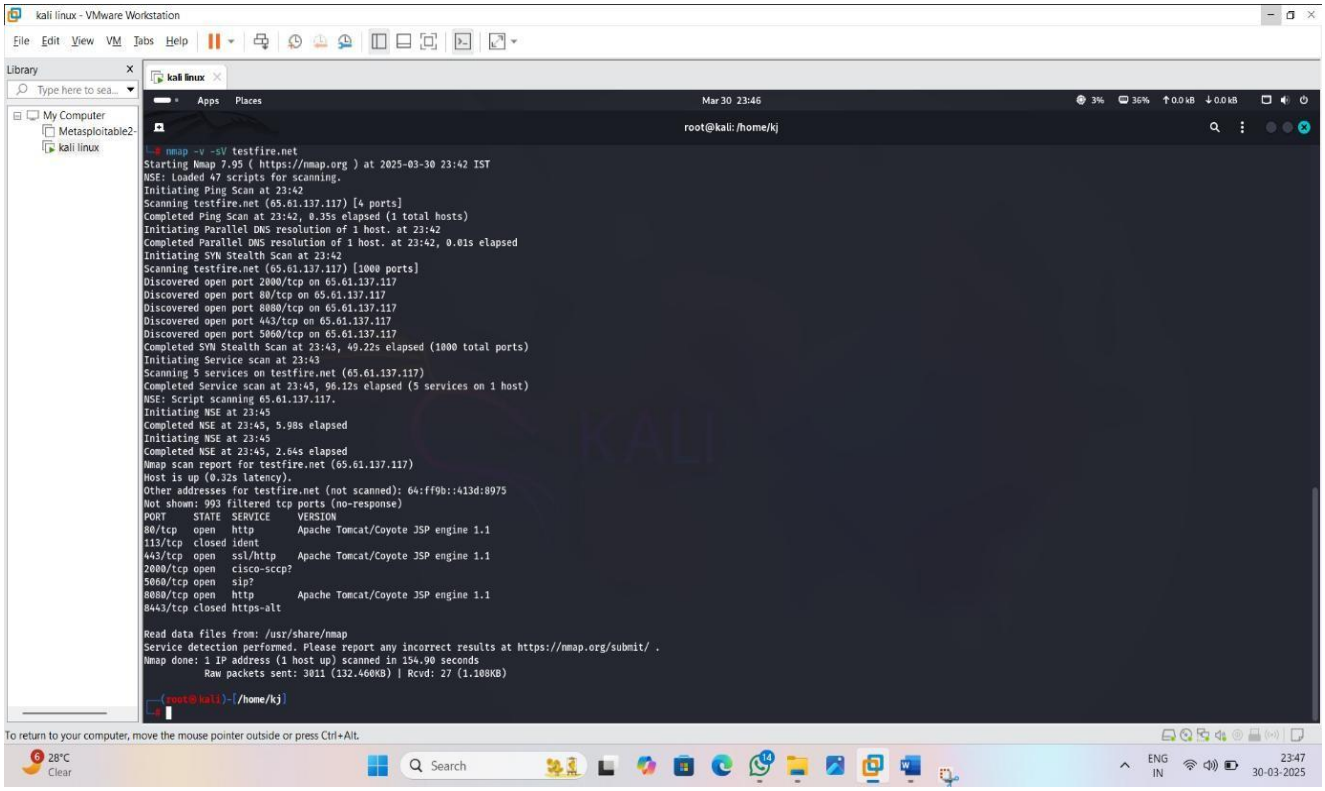
-sU = UDP scan



 # nmap -v -sV <target>

-sV = check version

Name : Kunal Jawale



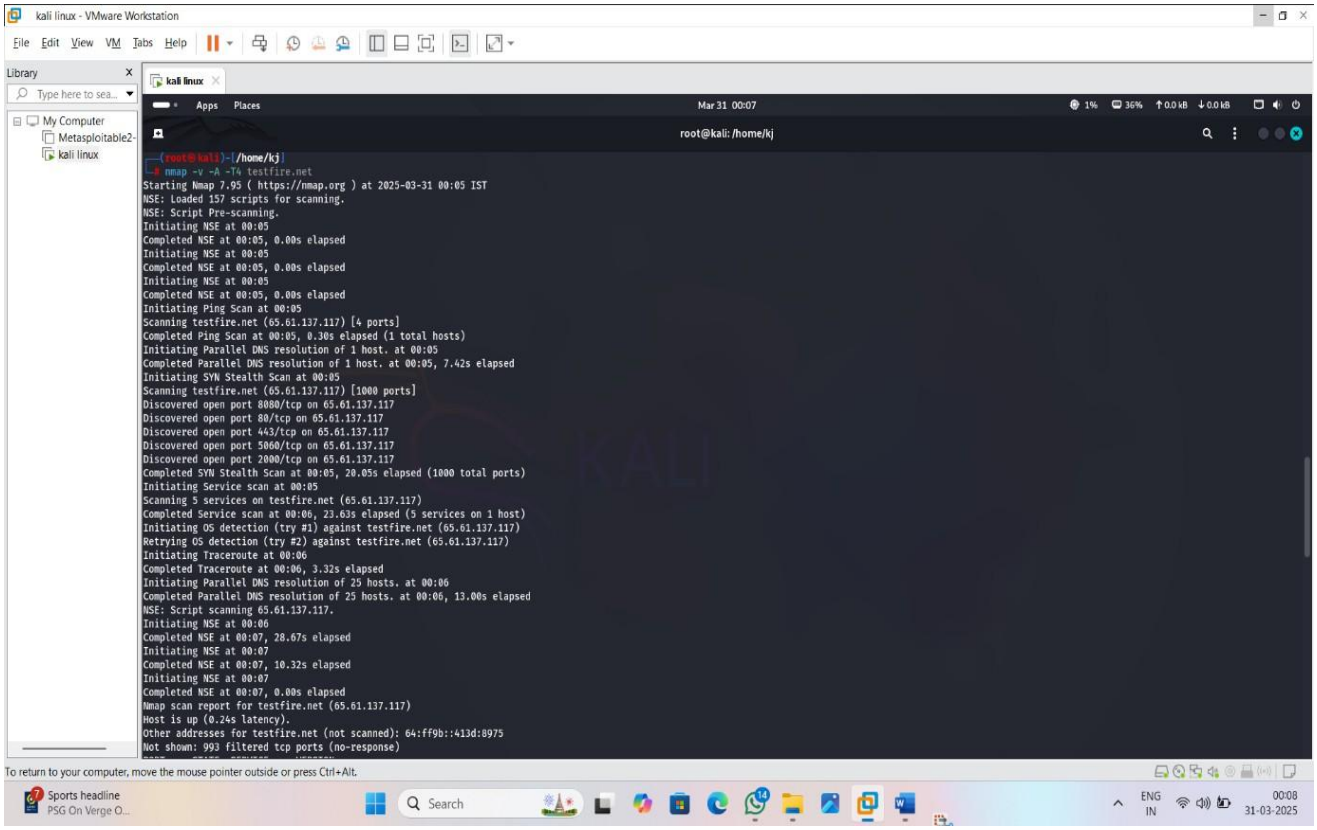
 # nmap -A -T4 -v < target >

-A = for all types of scan (advance)

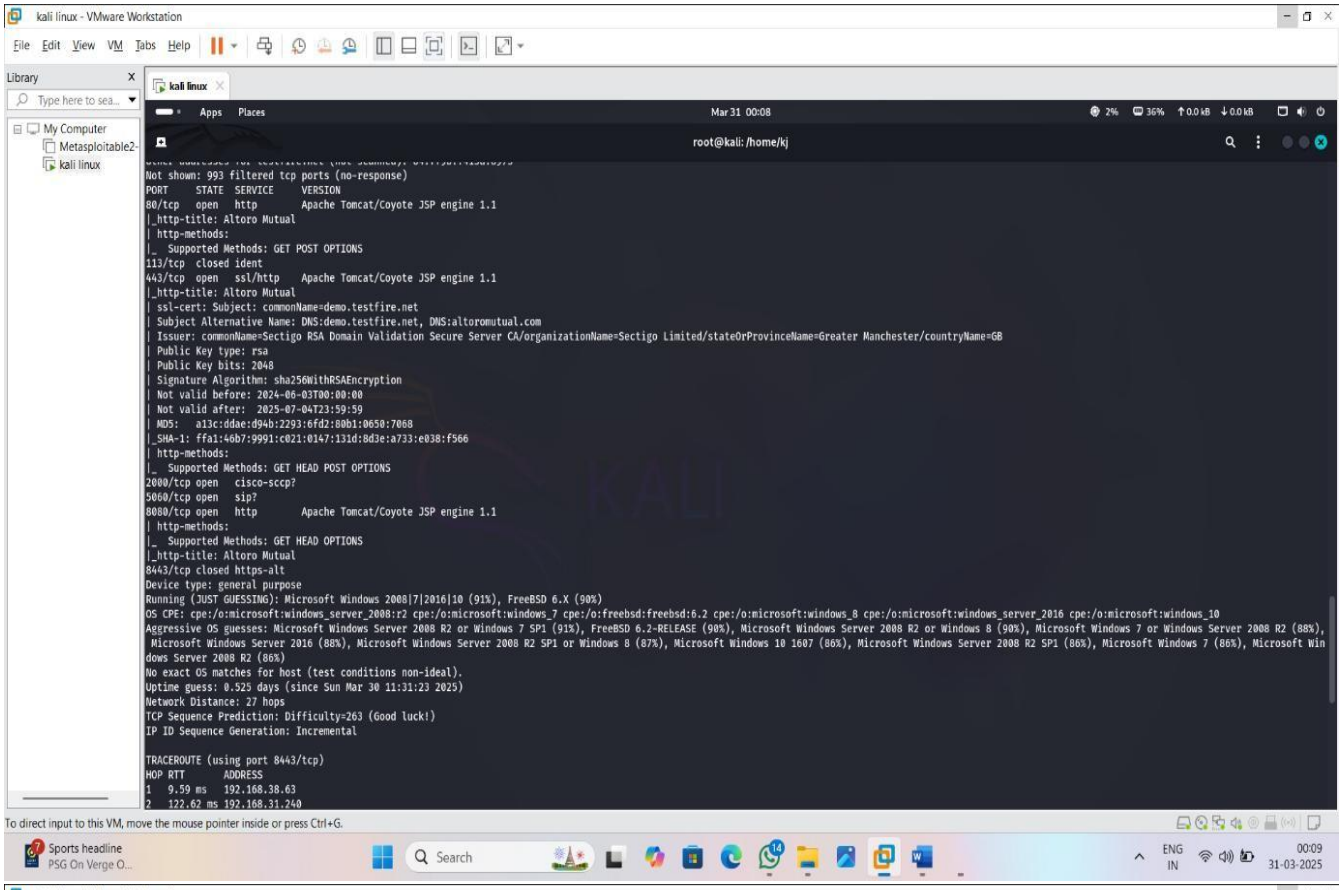
You should not use -A against target networks without permission .

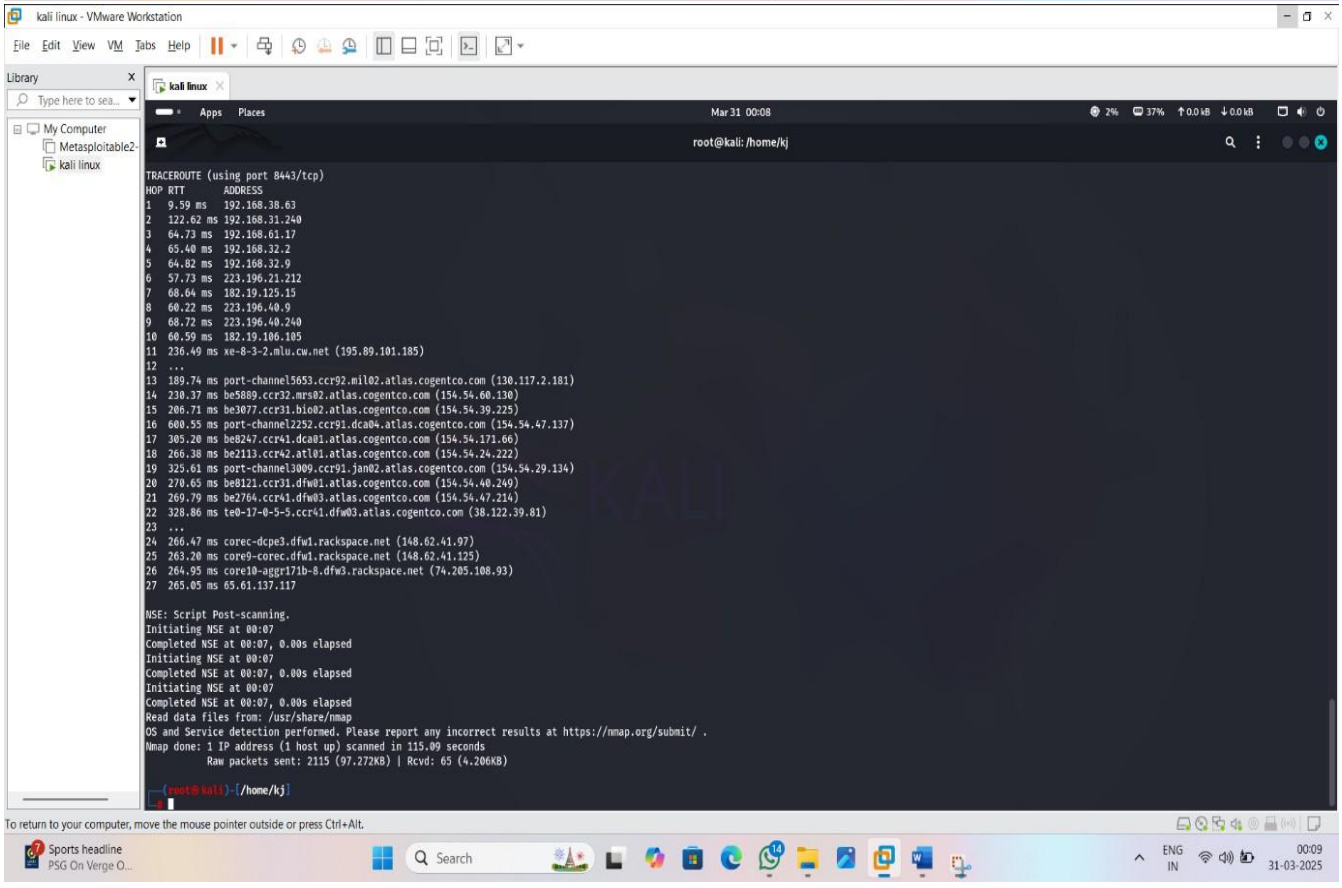
-T4 = is used for aggressive

Name : Kunal Jawale



Name : Kunal Jawale





* 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.

Name : Kunal Jawale

- **Targeted Exploitation:**

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

- **Improved Security Practices:**

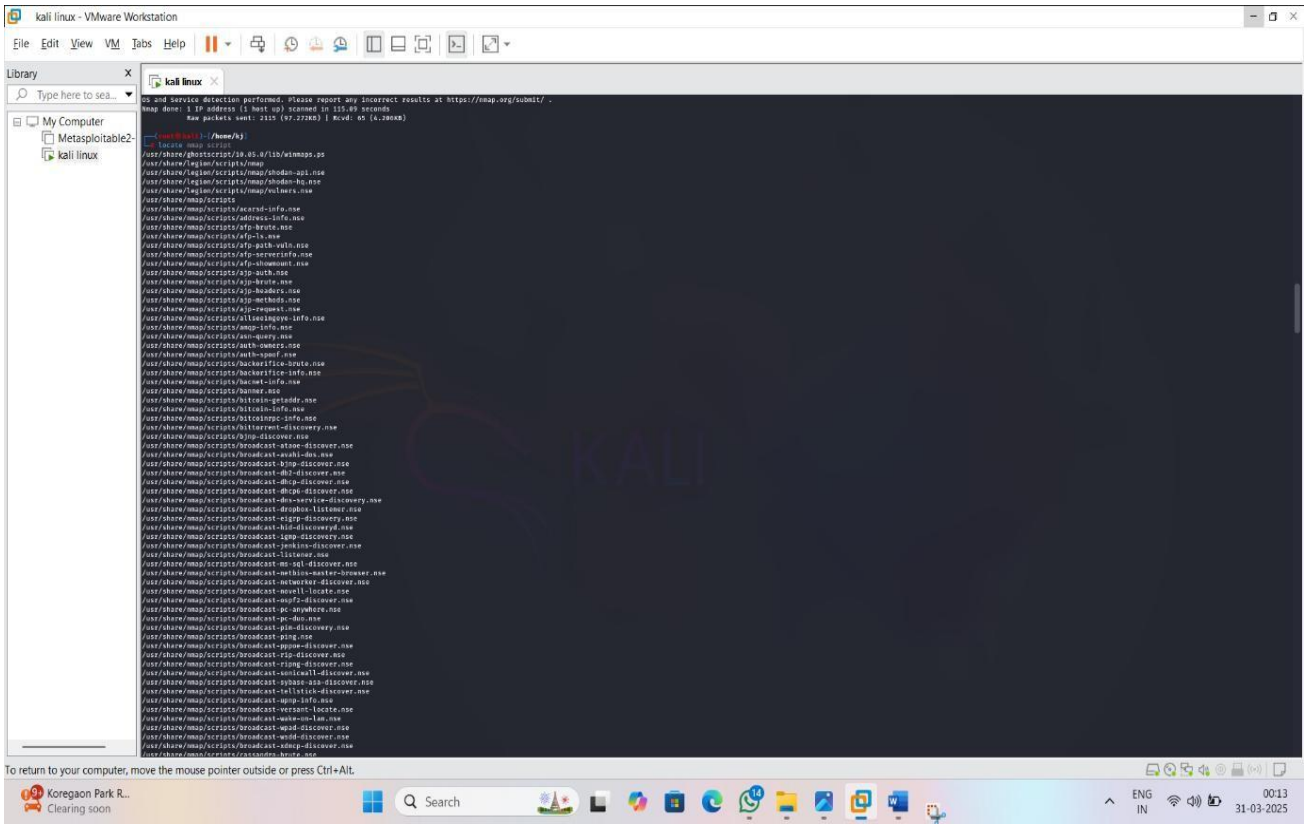
  Understanding the OS helps system administrators implement appropriate security measures and configurations.

- **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 .

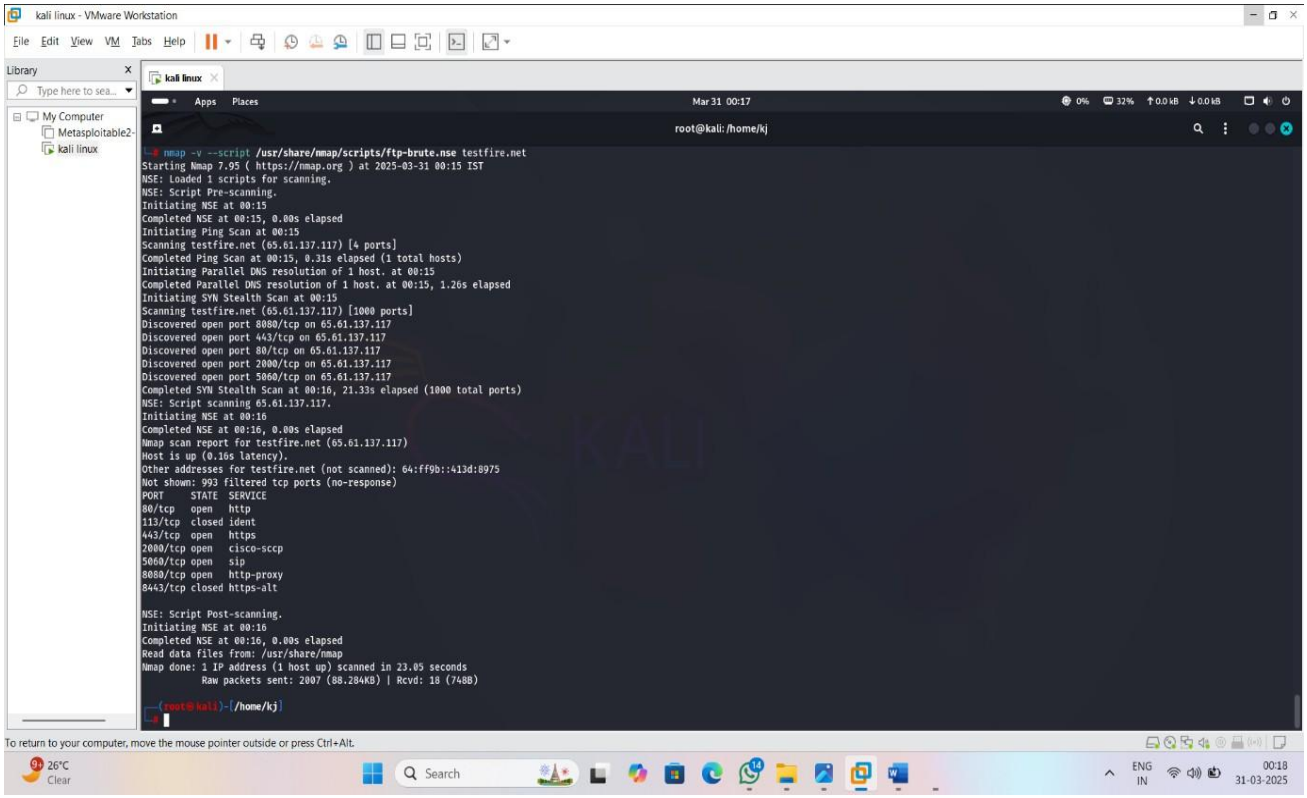
Run nmap scripts :

 # locate nmap script :- this shows all nmap scripts



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

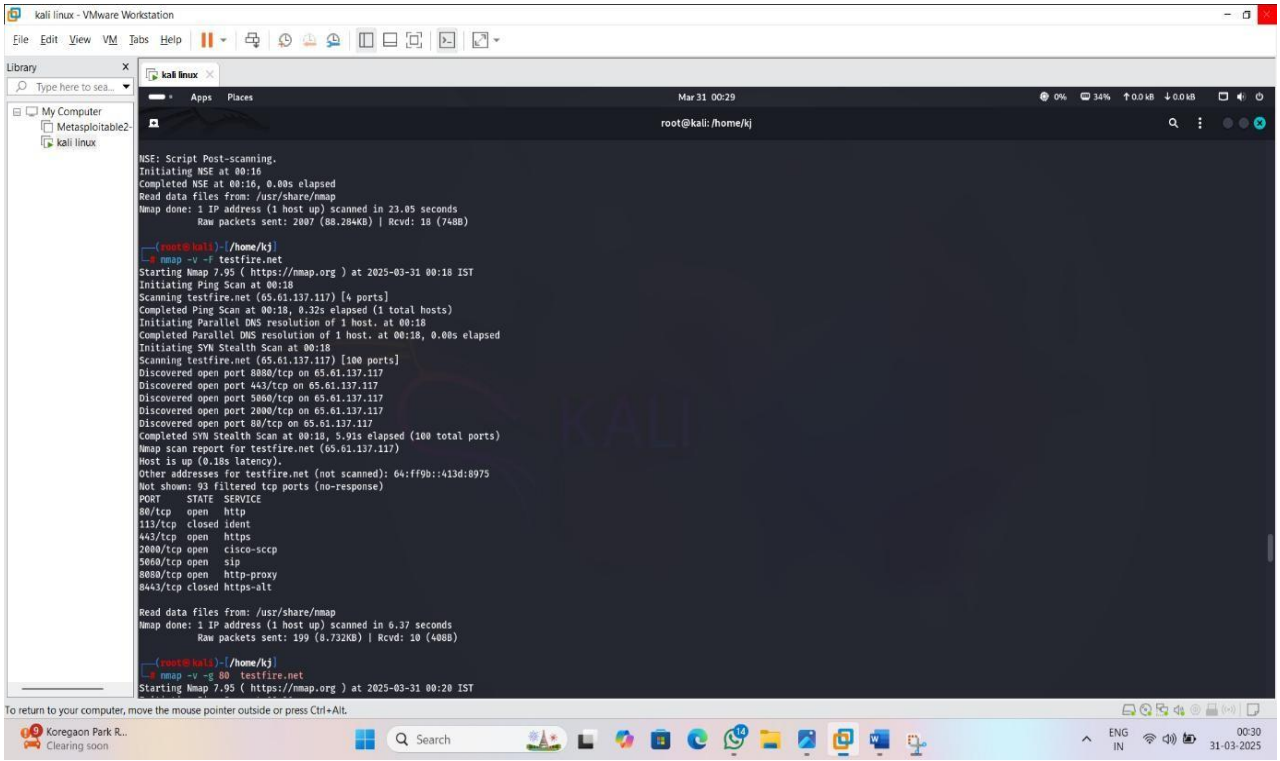
Name : Kunal Jawale



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

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

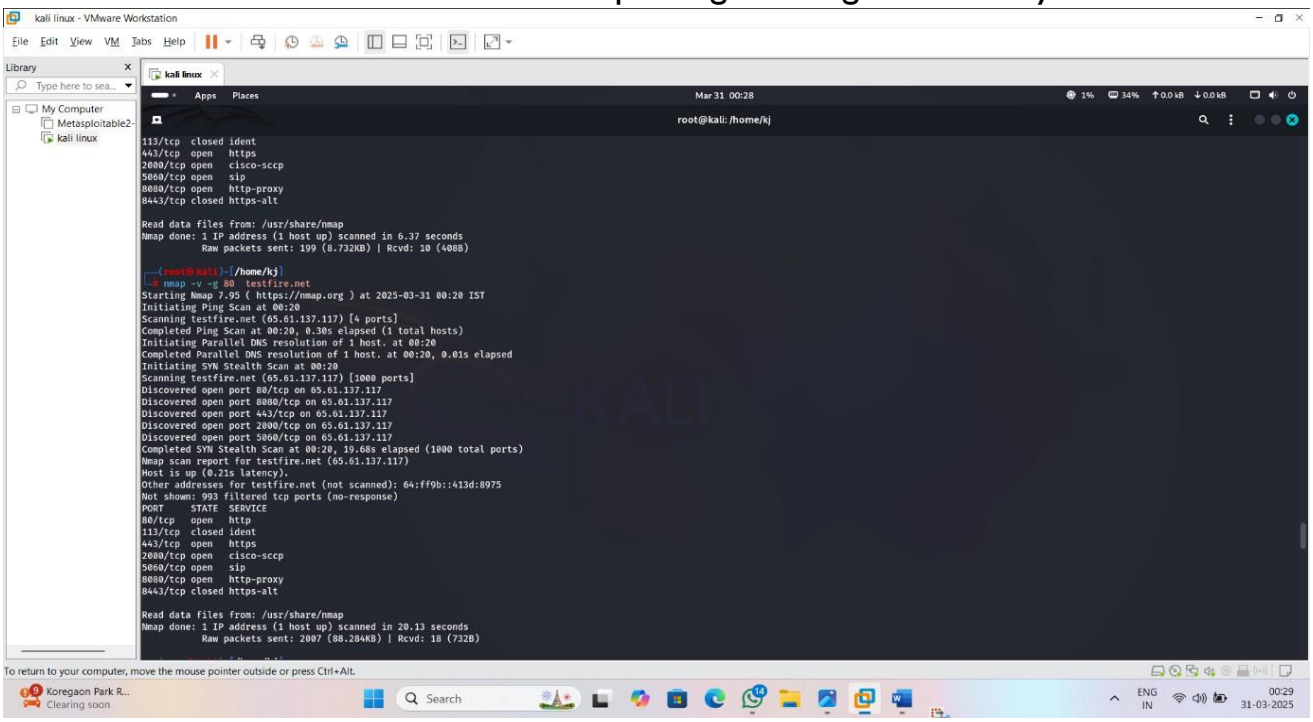
  Normally -f is used to tiny fragment packets to bypass firewall and IDS



Name : Kunal Jawale

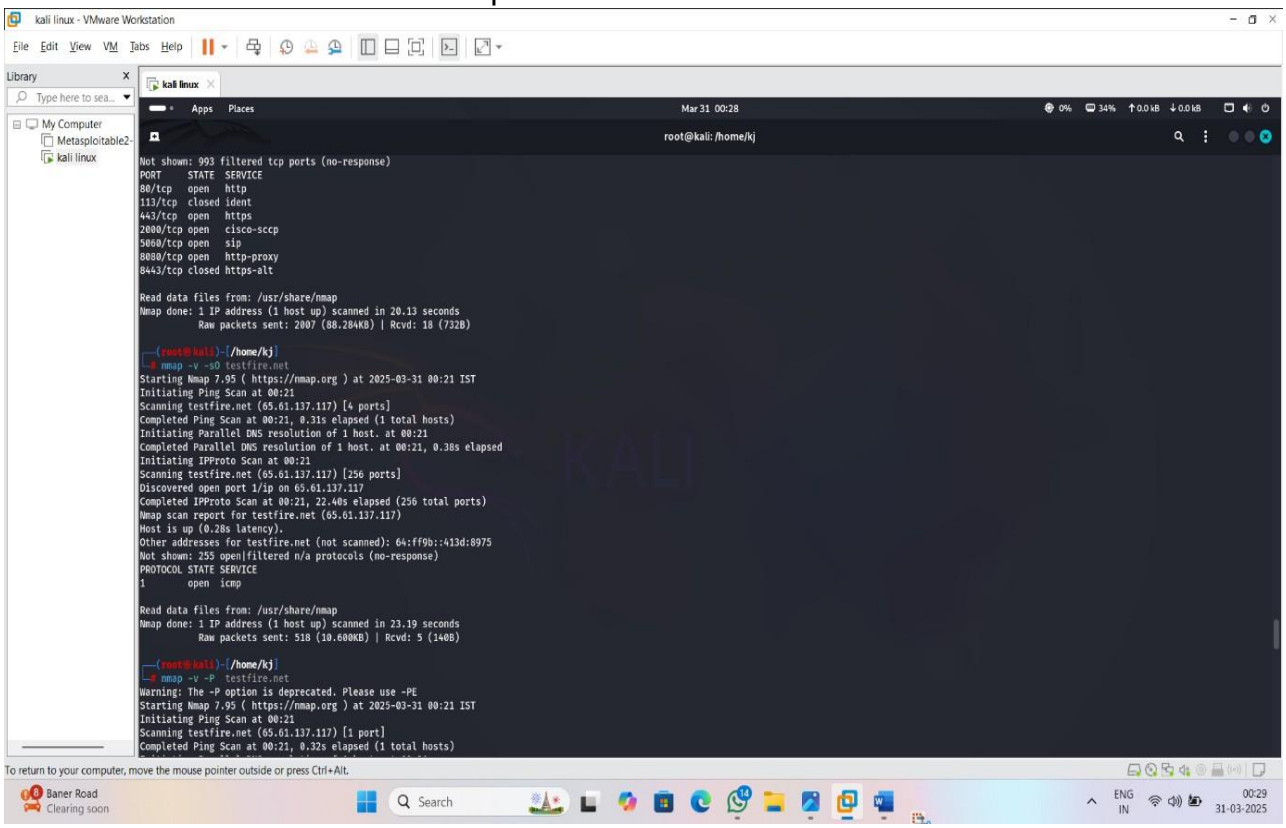
nmap -v -g 80 < target >

This command is used for spoofing or using fake identity .



nmap -v - sO < target >

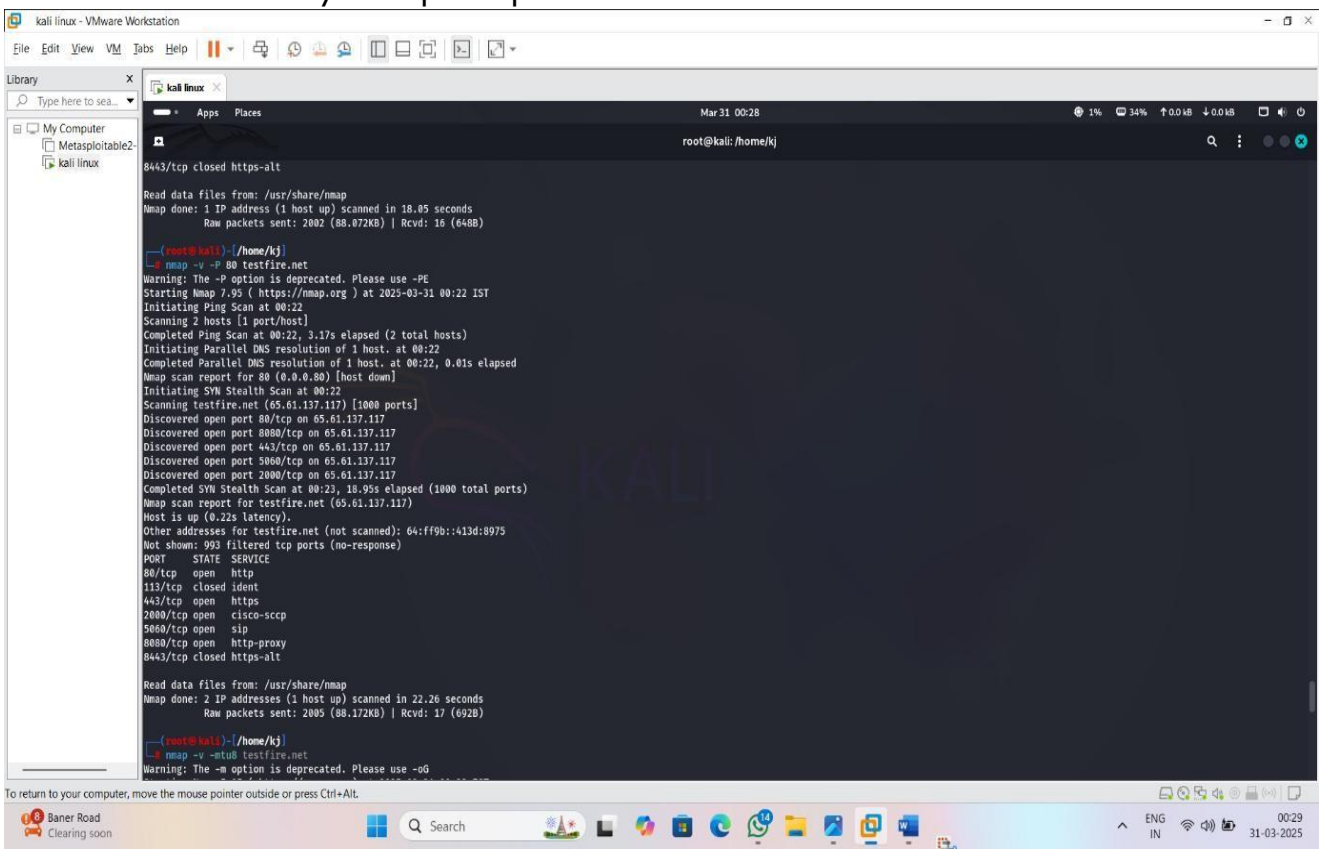
this is used for scan IP protocol



Name : Kunal Jawale

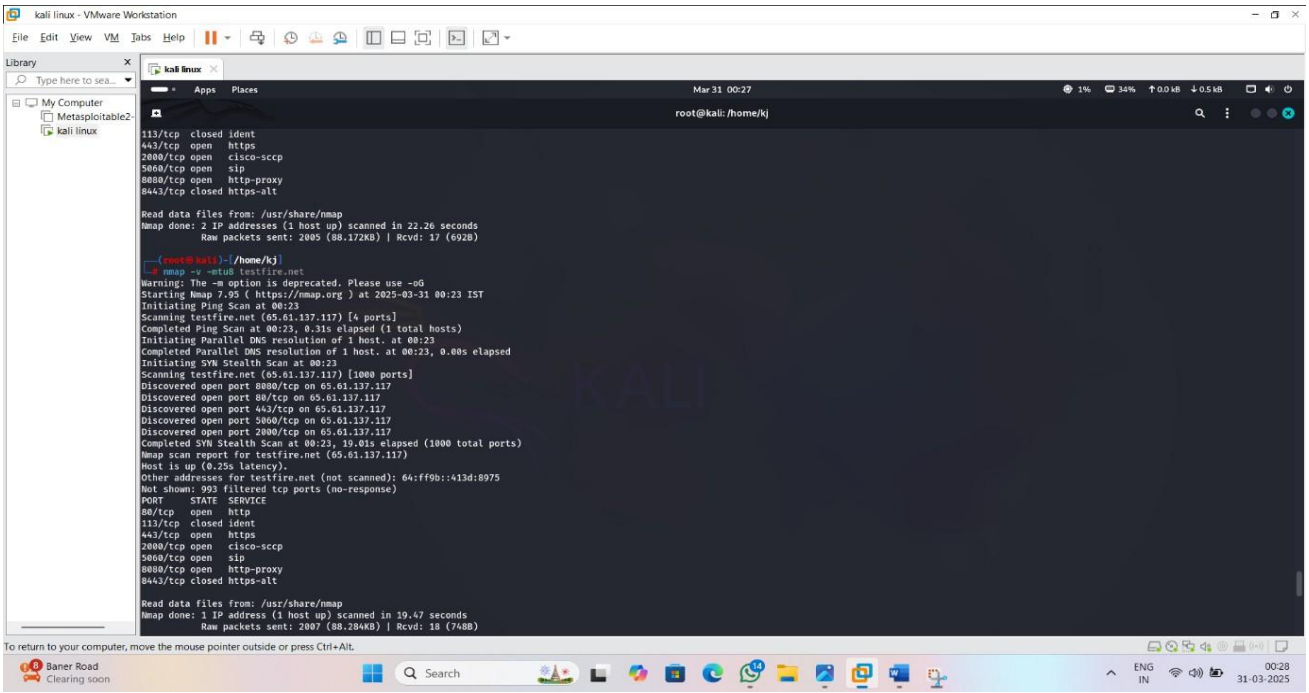
 # nmap -v -p < target >

for only scan specific ports .



 # 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

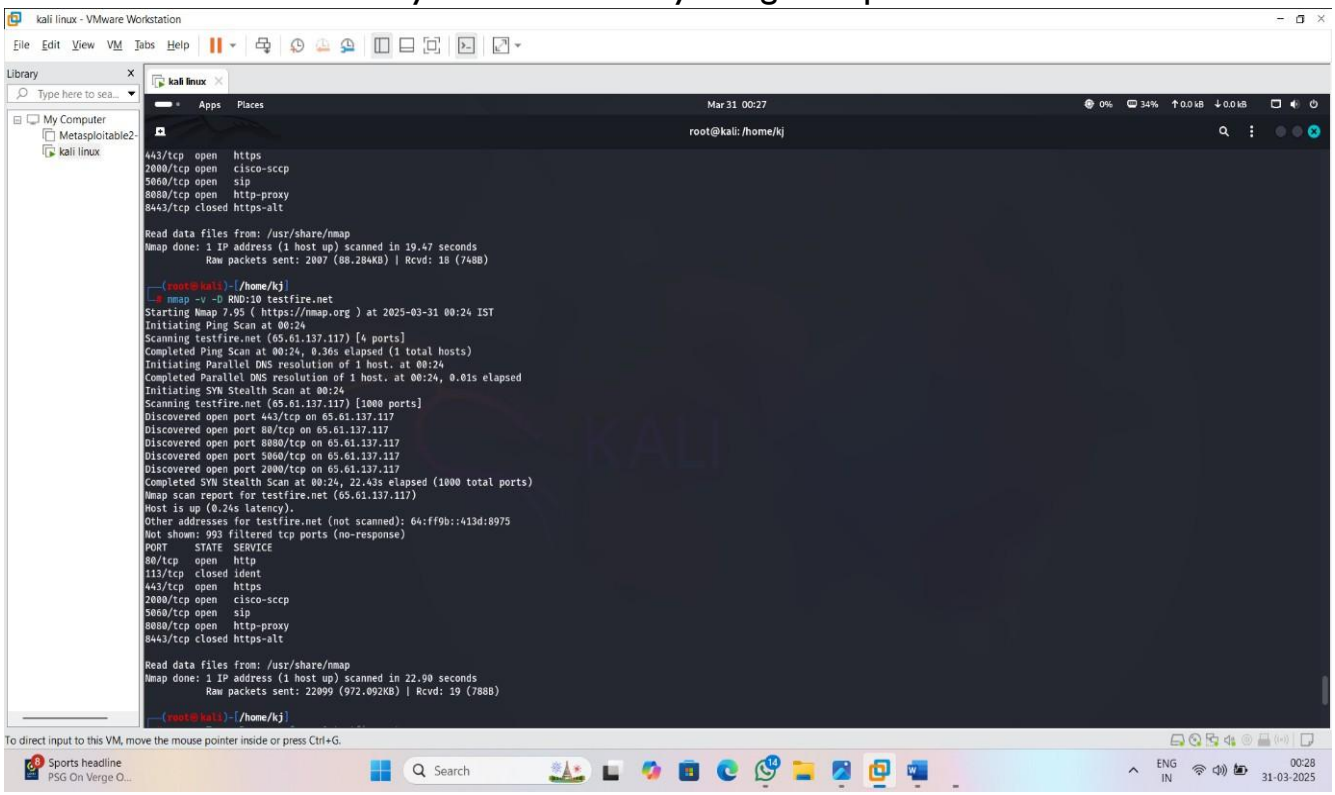


Name : Kunal Jawale

nmap -v -D RND:10 <target>

This technique is used for hide IP using multiple IP

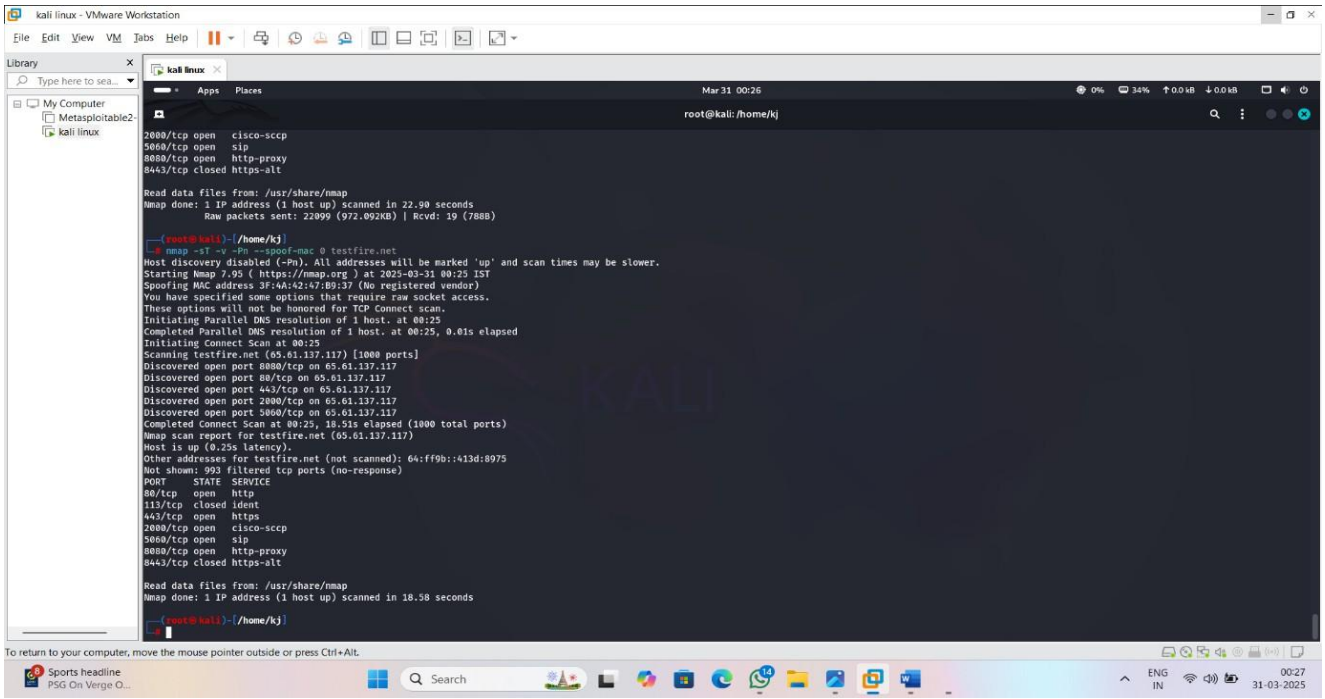
-D = to hide your IP or identity using multiple IP



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

To hide or spoofing mac -address

0 = for random ac address



Name : Kunal Jawale

- **Here are some port scanning technique using msfconsole :**

Commands :::

msfconsole :- to run metasploitable

>search portscan :- for searching releted portscan

>use 5 :- you choose whatever you want

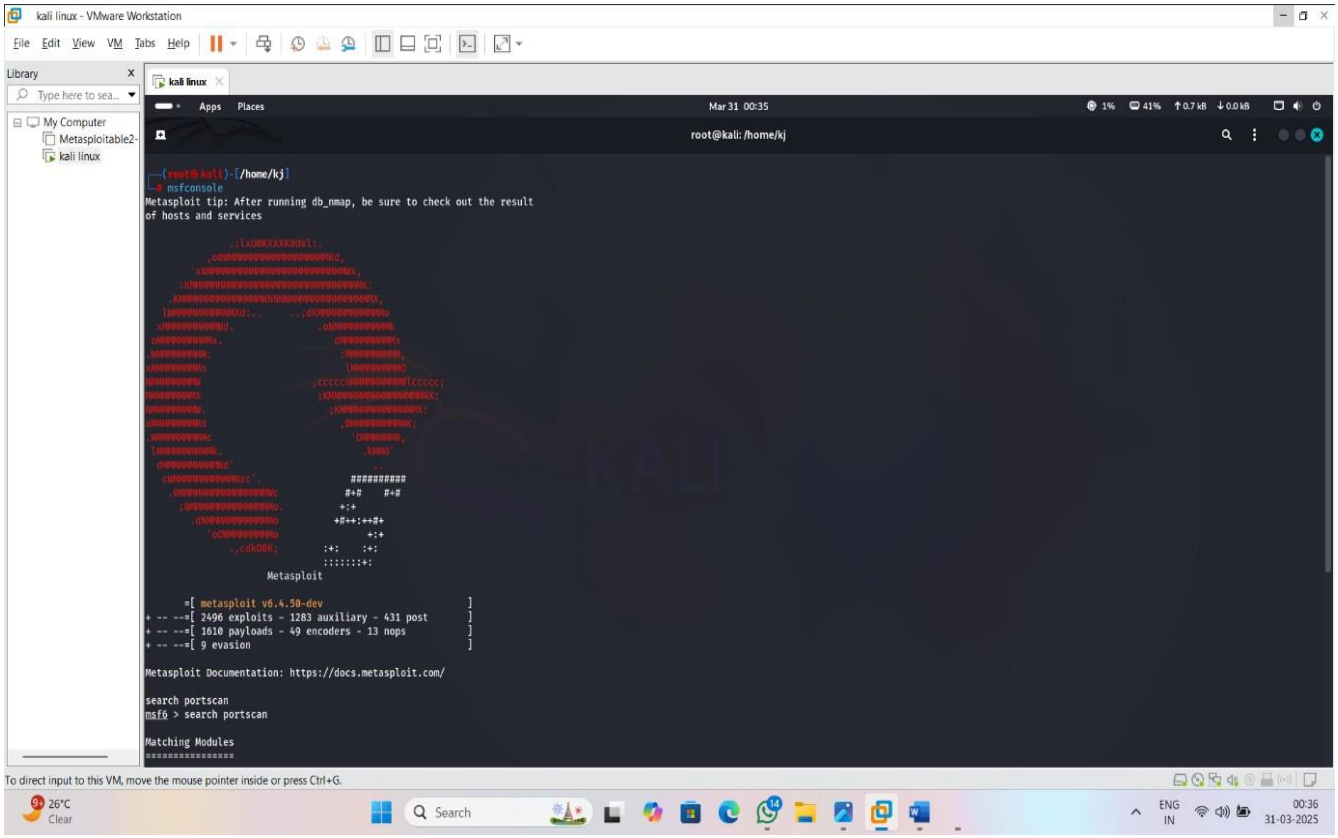
>set RHOST <IP> :- to set IP

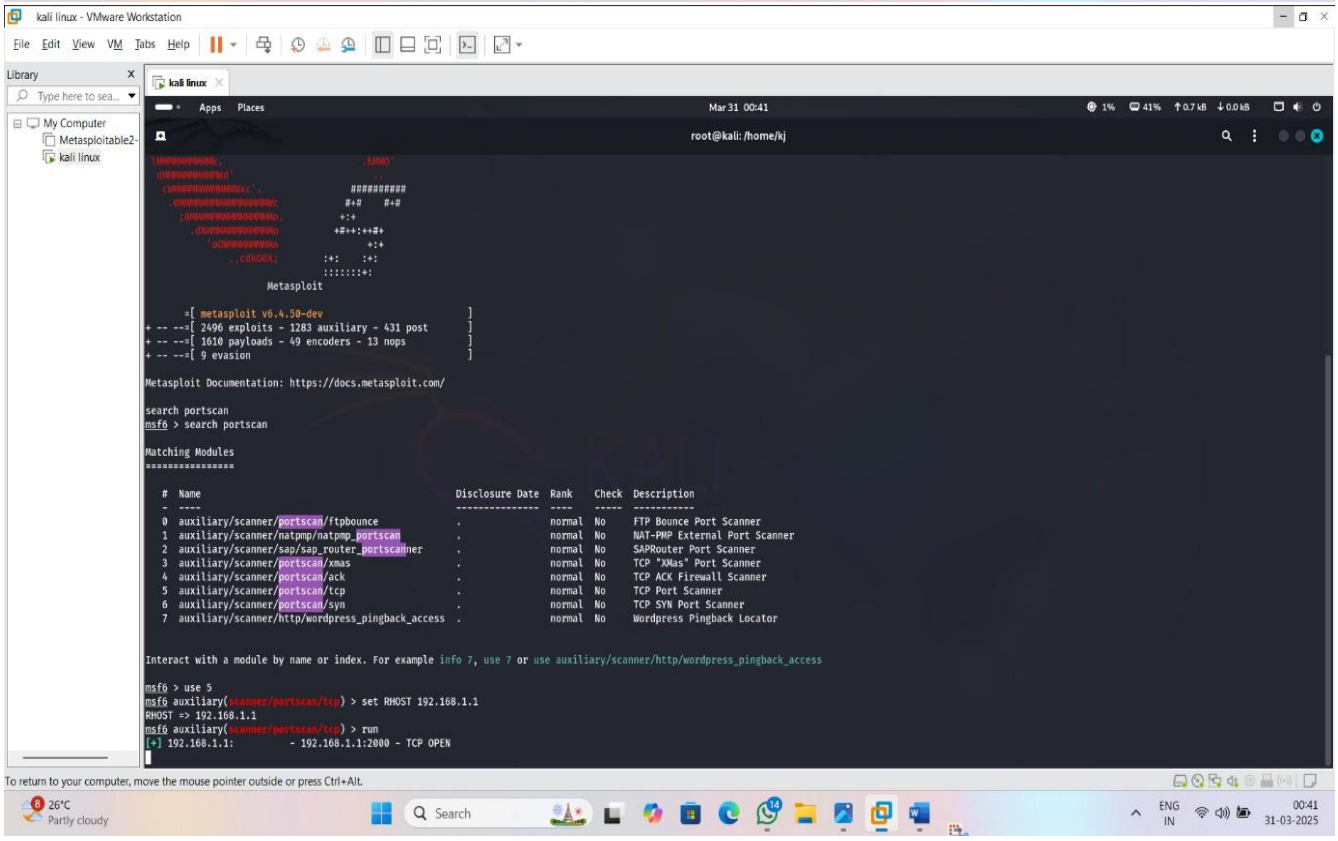
> set ports :- to set port range

> show :- to show

> run:- for scanning

Name : Kunal Jawale





Name : Kunal Jawale

*** 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:

1️⃣ 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`.

2️⃣ 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.

3️⃣ 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.

4️⃣ 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.

5️⃣ 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.

6️⃣ 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.

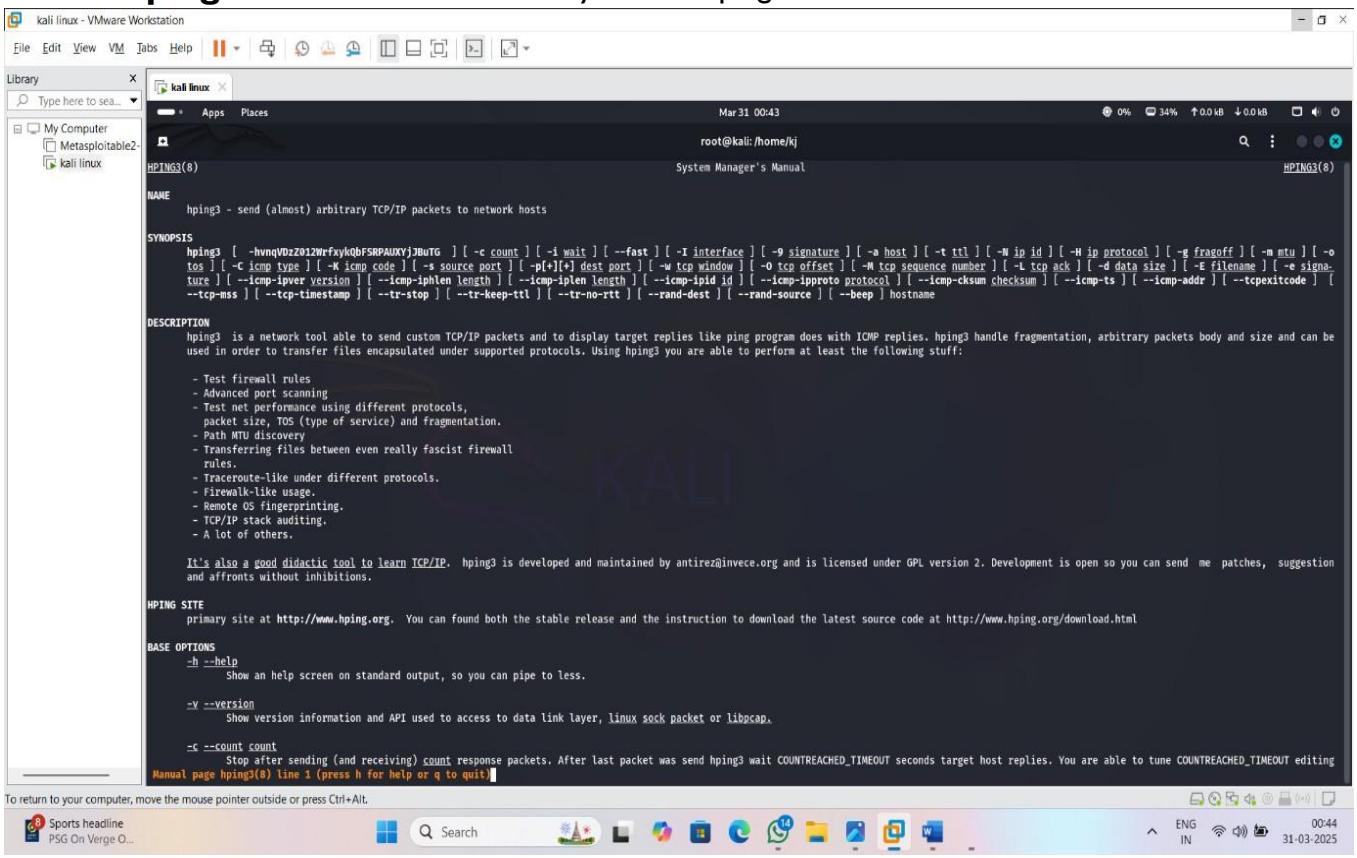
⚠️ Legal and Ethical Considerations:

- `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 .



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

  # hping3 -1 <IP> -a <IP> -p <port no > - - fast

  -1 = ICMP

  -a = for spoofing

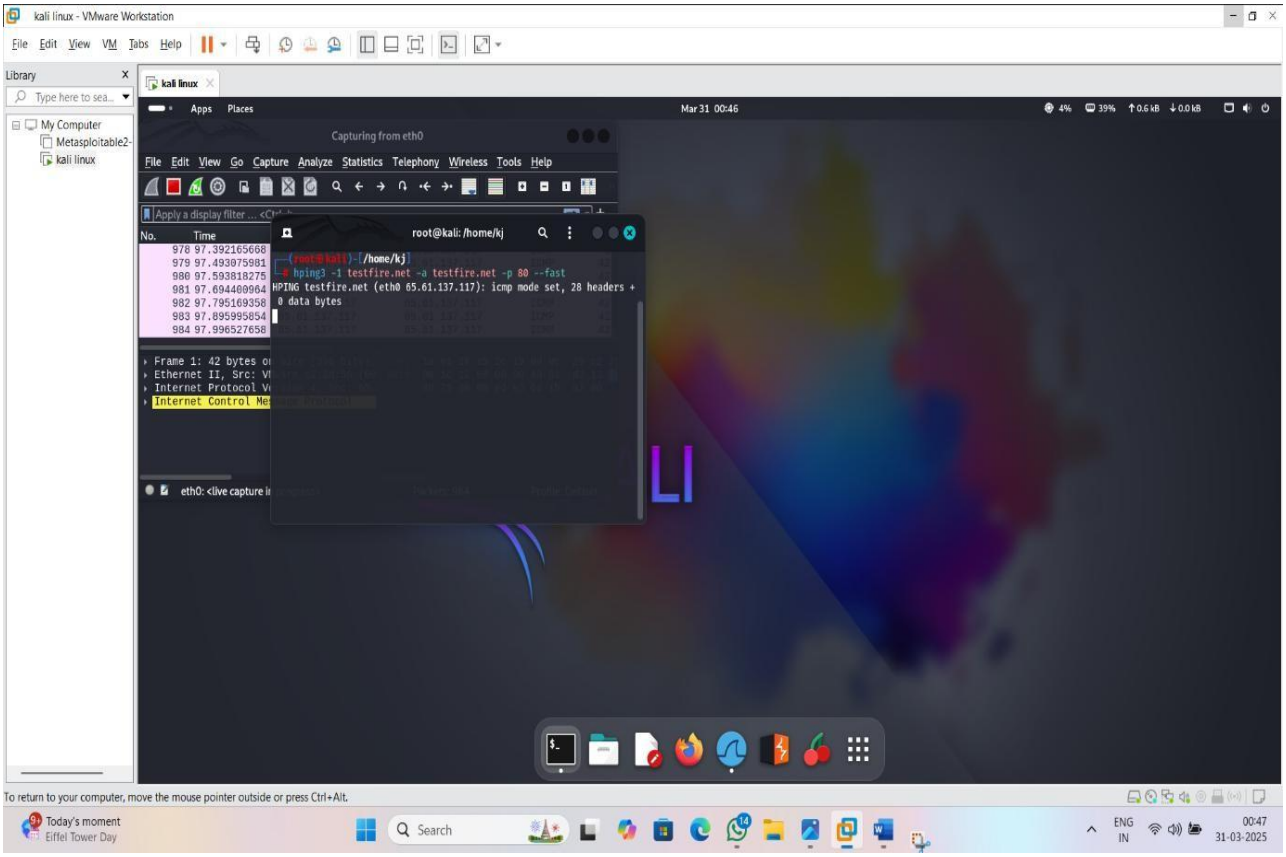
  -p = for open port

  -- faster = to fast scan

  -- flood = 10 time faster

  -c = countset

Name : Kunal Jawale

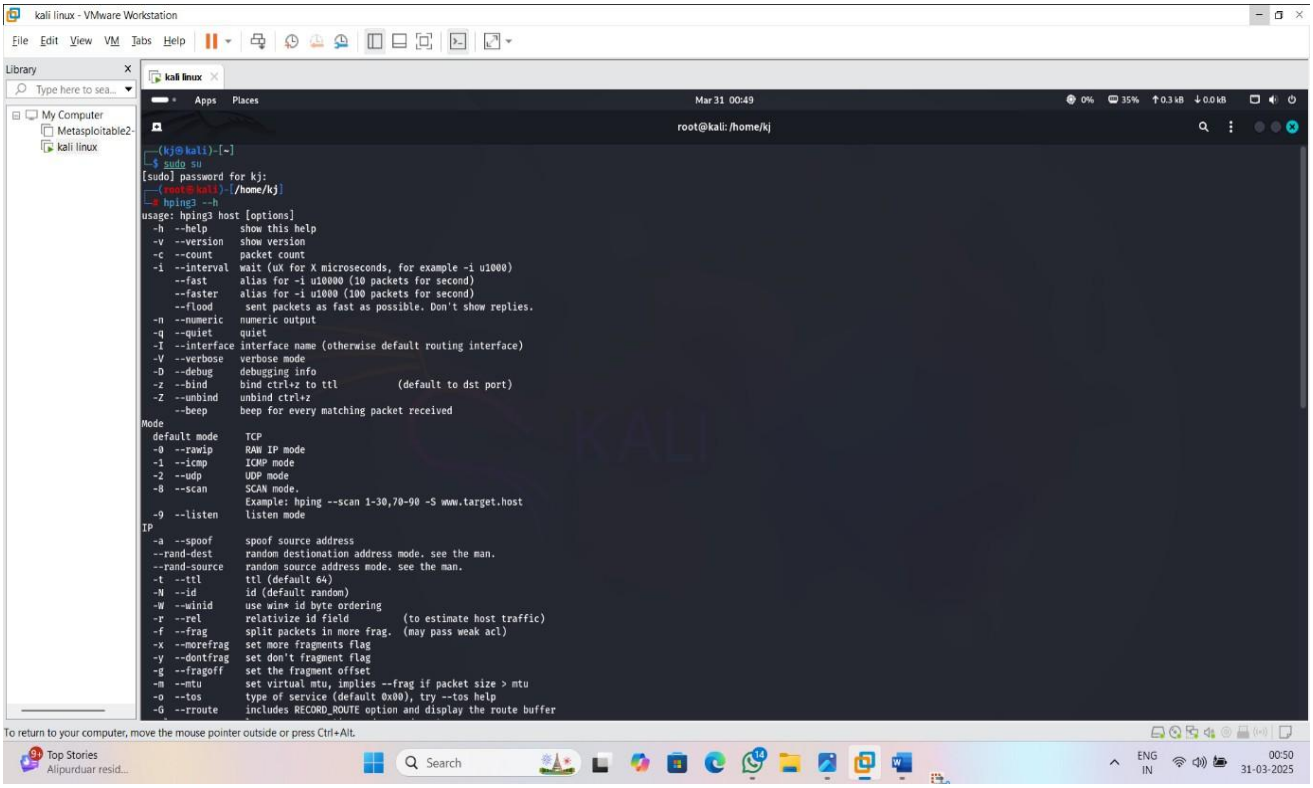


 # hping3 -1 <IP> --rand-source -p <port no> -- faster

--rand-source = for random search

hping3 –help = for commands

Name : Kunal Jawale



Name : Kunal Jawale