Internship assignment

Name AMIT MAURYA

DATE 23/06/2025

Day 1 Assignment: Network Scanning and Packet Capture

What is an IP Address?

An **IP Address** is a unique identifier for devices on a network.

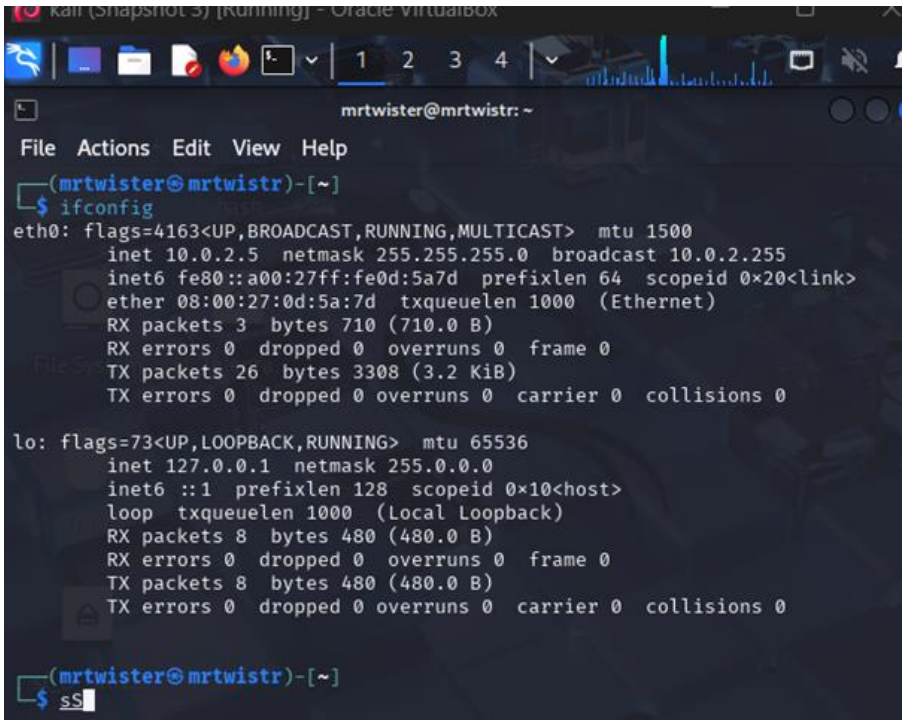
- **IPv4 example:** 192.168.1.1
- **IPv6 example:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334

How to Find Your IP Address:

- On Windows: ipconfig
- On Linux/Mac: ifconfig or ip a

On mobile: Available in Wi-Fi settings

Output of command **ifconfig**



What Are Ports?
In networking, a port is a logical communication endpoint on a device. It is like a door or a channel through which data enters or leaves a system.

- Every device on a network has an IP address (like a house address).

- Ports are like doors in that house.
- Ports allow multiple services to run on the same device without interfering with each other.

Example:

- Your web browser uses port 80 for HTTP (websites) and port 443 for HTTPS (secure websites).
- **Your email client may use port 25 for sending emails.**

What Are Services?

A service is a specific program or function running on a device that listens for incoming network traffic on a specific port.

Example:

- Port 80 → Web Service (HTTP)
- Port 443 → Secure Web Service (HTTPS)
- Port 21 → File Transfer Protocol (FTP) Service
- Port 53 → DNS Service

🔗 Relationship Between Ports and Services:

- Port = Door
- Service = The shop or facility behind the door

So, when you send a request to port 80, you're asking the web server to give you a webpage. When you send a request to port 21, you're asking the FTP service to allow file transfers.

What Does an Open Port Mean?

An open port means the door is open and actively listening for incoming connections.

- If a port is open → the related service is running → the system is ready to communicate.
- Open ports can be safe or dangerous depending on how well they are secured.

Example of Open Port:

- If port 80 is open, the web server is available, and anyone can try to connect to it.
- If port 445 is open, the SMB service is running, and it could be vulnerable to attacks like EternalBlue.

Types of Port States:

Port State	Meaning
Open	Service is running and accepting connections.
Closed	No service is listening, but the port is reachable.
Filtered	The port is hidden or protected by a firewall, so Nmap can't determine if it's open or closed.

Quick Real-Life Analogy:

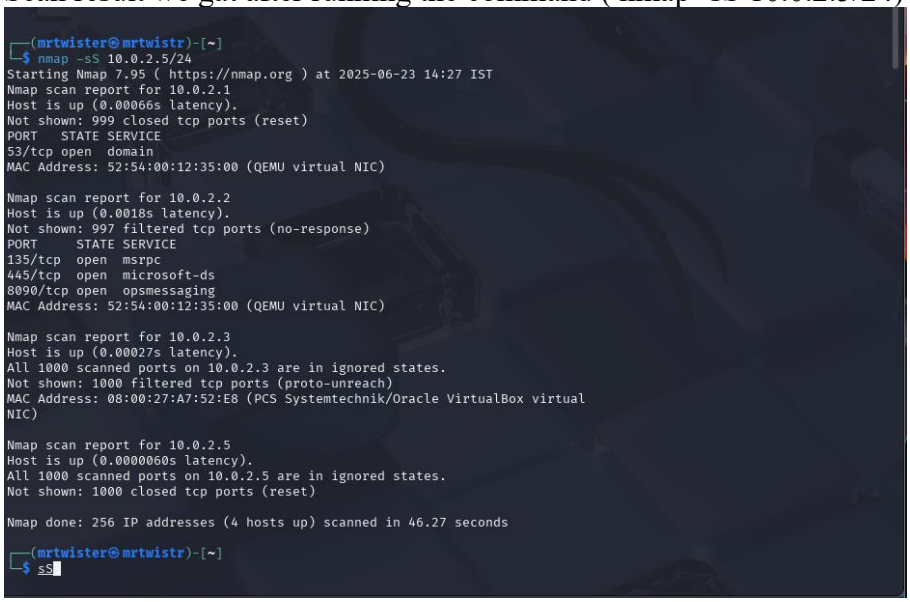
- IP Address = House Address
- Port = Door Number
- Service = Type of Shop Behind the Door (Web Shop, File Store, DNS Help Desk)
- Open Port = The shop is open for business
- Closed Port = The shop is closed
- Filtered Port = The shop is hidden behind a security gate (firewall)

1. Introduction to Nmap

Nmap (Network Mapper) is a free, open-source tool used for **network discovery and security auditing**. It is widely used to:

- Detect live hosts on a network.
- Identify open ports and services.
- Perform OS detection and version scanning.
- Assist in vulnerability assessment.

Scan result we gat after running the command (nmap -sS 10.0.2.5/24)



AFTER GOING THROUGH THIS SCAN WE DISCOVERED SOME OPEN PORTS

Explanation of the Open Ports and How to Exploit Them

1. Port 53 – DNS (Domain Name System)

- **What it does:**
  Port 53 is used for DNS, which translates website names (like google.com) into IP addresses.
- **Possible Risk:**
  If the DNS server is misconfigured, an attacker can try to extract all internal records (called a **zone transfer**).
  Attackers can also perform **DNS cache poisoning** to make the target system visit fake or malicious websites.
- **How to Exploit:**
  An attacker can request the DNS server to share all its internal records (zone transfer). If allowed, the attacker can see all the device names and IPs in the network.

Cache poisoning can trick the DNS server into storing fake entries that lead users to fake websites controlled by attackers.

---

2. Port 135 – Microsoft RPC (Remote Procedure Call)

- **What it does:**
  Port 135 is used by Windows systems for remote communication between applications. It helps Windows manage tasks and services remotely.
- **Possible Risk:**
  This port has been historically vulnerable. For example, it was exploited by the **Blaster worm** to take control of systems remotely.
  Attackers can exploit this to run malicious code on the victim's computer without permission.
- **How to Exploit:**
  An attacker would search for old vulnerabilities in Windows systems related to port 135.
  If the system is not updated, the attacker can send specially crafted requests that force the system to open a backdoor for remote access.

---

3. Port 445 – SMB (Server Message Block)

- **What it does:**
  Port 445 is used for file sharing, printer sharing, and network browsing in Windows systems.
- **Possible Risk:**
  This port was famously exploited by **ransomware like WannaCry** using the **EternalBlue** vulnerability.
  Attackers can use this port to remotely control a system, install malicious programs, or steal files.
- **How to Exploit:**
  If the system is not patched, an attacker can send harmful requests that give them full control over the system.
  Even if the system is patched, if SMB is open without proper protection, attackers can attempt to steal login credentials using other attacks like SMB relay.

---

4. Port 8090 – opsmessaging

- **What it does:**
  Port 8090 is often used by web-based applications or messaging services. Sometimes it is used by administrative dashboards or APIs.
- **Possible Risk:**
  If this service is misconfigured, it might reveal sensitive information or allow

unauthorized access.
Attackers may try to access a login page, guess passwords, or search for hidden files.

- **How to Exploit:**
  The attacker would open the service in a web browser and check if there are any weak security settings or exposed data.
  If a login page is found, the attacker might try common or default usernames and passwords.
  They may also try to find hidden files or directories that could give them more information or access.

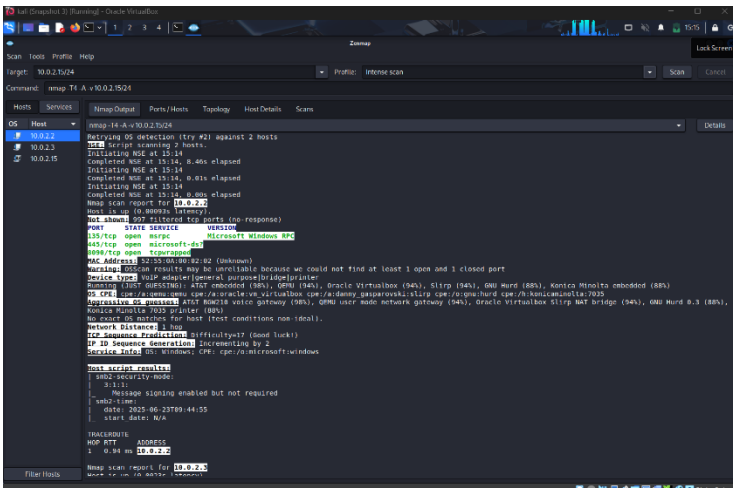
Alternative to nmap to perform a scan in Kali on the subnet

Introduction to Zenmap

Zenmap is the **graphical user interface (GUI) version of Nmap.**

- It makes Nmap easier to use by allowing users to input scan commands and view results visually.
- It displays network topology maps and detailed scan reports.

SCAN RESULT OF ZEN MAP



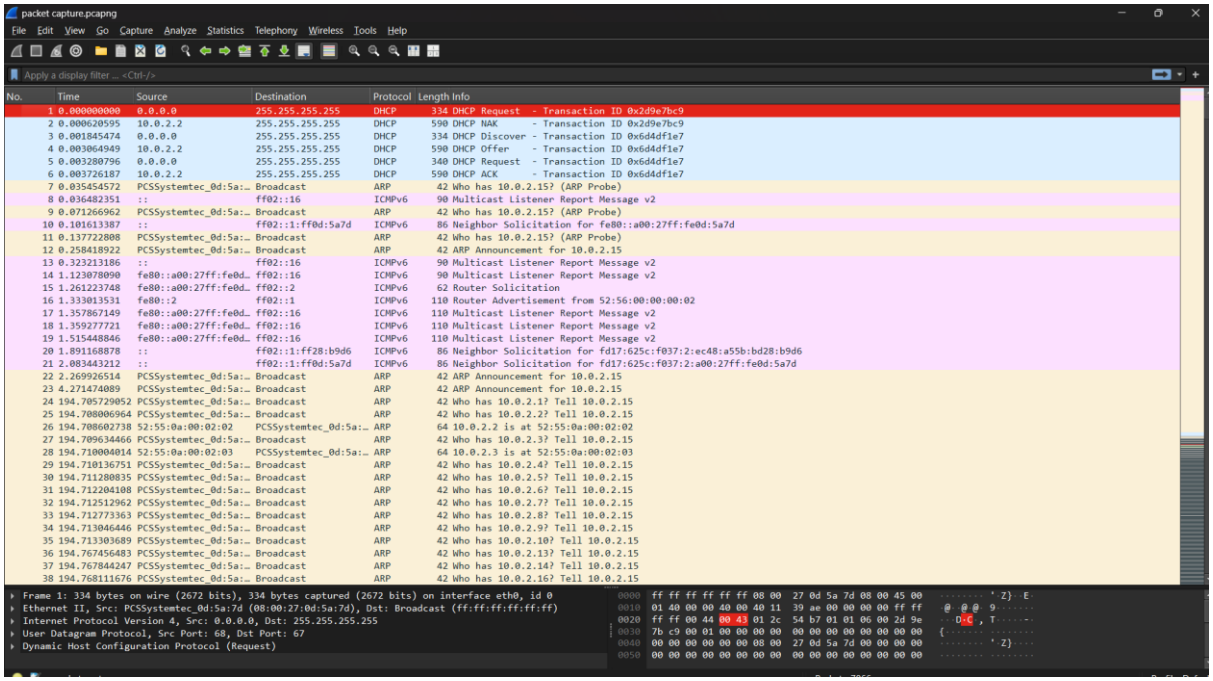
WIRESHARK

How to Capture Packets in Wireshark

Step-by-Step:

1. Open Wireshark and select the active network interface (like eth0 or wlan0).
2. Click Start Capturing Packets.
3. During your Nmap scan, Wireshark will capture TCP SYN packets, SYN-ACK responses, DNS queries, etc.
4. You can apply filters like:
   - tcp to view only TCP traffic.
   - ip.addr == 10.0.2.2 to filter traffic to/from a specific IP.
5. After scanning, stop the capture and analyze the packets for connection attempts and responses.

Output of Wireshark scan result (packet captured)



Answer of the Interview question

1. What is an open port?

An open port is a network port that is configured to accept connections. It means the service listening on that port is accessible, which can allow communication but can also be a security risk if improperly secured.

---

2. How does Nmap perform a TCP SYN scan?

Nmap performs a TCP SYN scan (also called half-open scanning) by sending a SYN packet to the target port:

- If it receives a SYN-ACK, the port is open.
- If it receives an RST, the port is closed.
- If there is no response, the port may be filtered.
  The connection is never fully established, making it a fast and stealthy method.

---

3. What risks are associated with open ports?

- Open ports can expose vulnerable services.
- Attackers may exploit these ports for unauthorized access.
- Services running on open ports may be susceptible to denial of service (DoS) attacks.
- They can leak sensitive information if not properly configured.

---

4. Explain the difference between TCP and UDP scanning.

- TCP Scanning: Establishes (or attempts to establish) a connection using the three-way handshake. TCP scans are more reliable because you know whether the port is open, closed, or filtered.
- UDP Scanning: Sends a UDP packet to the target port. If no response, the port may be open or filtered. If "port unreachable" is received, it's closed. UDP scans are slower and less reliable but can uncover services that TCP scans miss.

---

5. How can open ports be secured?
- Close unused ports.
- Use firewalls to restrict access.
- Enable intrusion detection systems.
- Regularly update and patch services.
- Implement network segmentation to isolate critical services.

---

6. What is a firewall's role regarding ports?
A firewall controls incoming and outgoing network traffic based on security rules. It can:
- Block or allow traffic on specific ports.
- Prevent unauthorized access to open ports.
- Protect internal systems by filtering traffic.

---

7. What is a port scan and why do attackers perform it?
A port scan systematically checks a range of ports to identify which are open, closed, or filtered.
Attackers use port scans to:
- Discover vulnerable services.
- Map the network.
- Plan potential exploits or attacks.

---

8. How does Wireshark complement port scanning?
- Wireshark captures and analyzes live network traffic.
- It can verify Nmap scan results by showing packet-level details.
- Helps in understanding handshake processes, responses, and anomalies.
- Useful in detecting suspicious scanning activities.