**Assignment 04**

**Port Discovery Techniques**

**CS4061**

**Ethical Hacking Concepts and Practices**

**Submitted by:** Ahmed Yar

**Roll number:** 20i-0850

**Date:** 24-03-2024

**Table of Contents**

[ **Introduction** 3](#_Toc143364655)

[ **Steps** 3](#_Toc143364656)

[ **Summary** 3](#_Toc143364657)

[ **References** 11](#_Toc143364658)

# **Introduction**

For network scanning, there are multiple techniques available like host discovery and port scanning techniques. Being a student of ethical hacking concepts and practices, you have to have hands-on experience on these techniques. In this assignment you have to use Nmap, Hping, Scapy, or any tool to achieve the following tasks of port discovery. Include screenshot of each scanning result with clearly highlighting command you have used and results you have received. Also include description of each screenshot like what command you have entered with explain each flag. You can consult with course book, generative AI, or with anyone. If you use generative AI tools like ChatGPT or Gemini, must include screenshots in your report. All screenshots must be of Full Screen including task bar and title bar.

# **Steps**

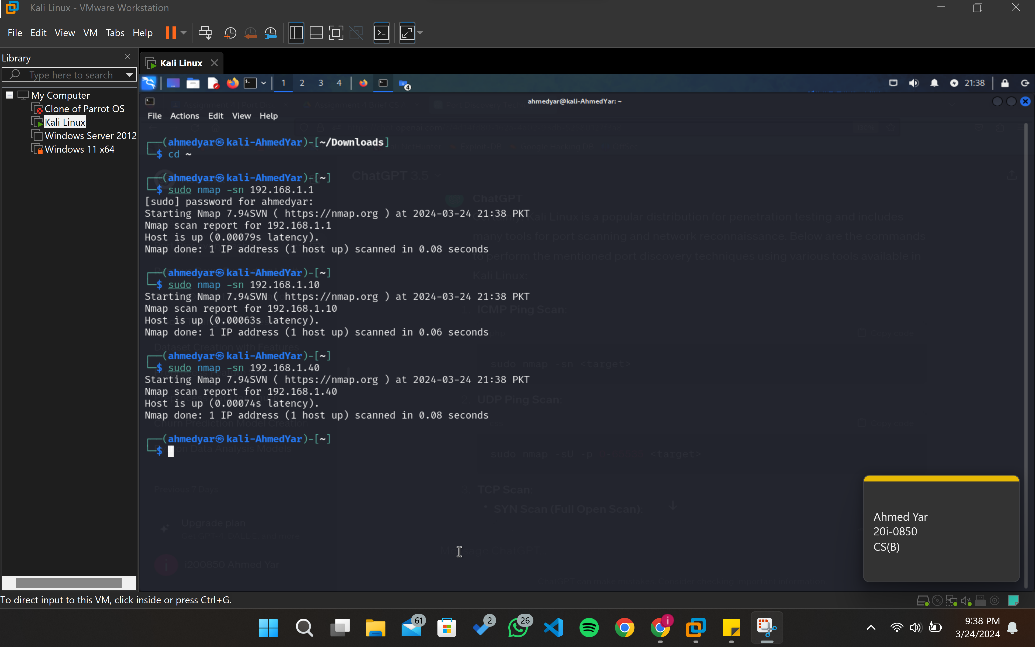
# **ICMP Ping Scan**

**Command:** sudo nmap -sn <target>

**Explanation:** This command uses Nmap, a popular network scanning tool, with the -sn option to perform an ICMP ping scan. It sends ICMP echo requests (ping) to the specified target(s) to check if they are reachable and online.

**How it works:** Nmap sends ICMP echo requests to the target(s) and waits for responses. Devices that respond are considered active on the network, while non-responsive ones are likely offline or firewalled.

**The kali linux terminal command and result is added below**:



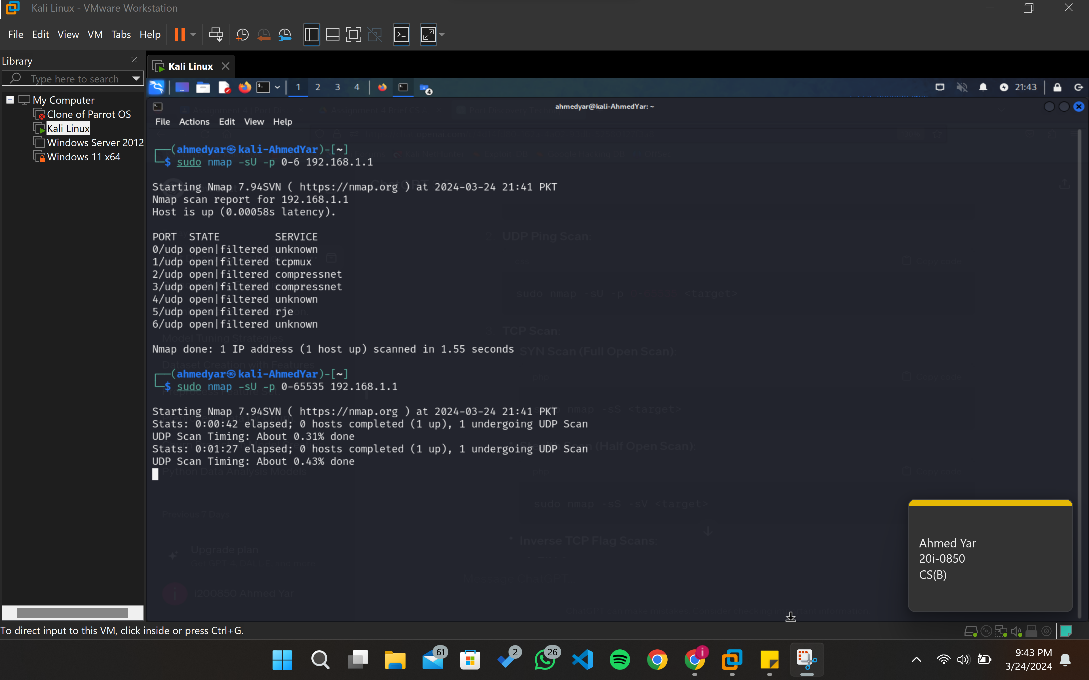
# **UDP Ping Scan**

**Command**: sudo nmap -sU -p 0-65535 <target>

**Explanation**: This command uses Nmap with the -sU option to perform a UDP ping scan. It sends UDP packets to various ports (0-65535) of the target(s) to check for responses.

**How it works**: Nmap sends UDP packets to the target(s) and analyzes responses. Devices that respond to UDP packets are considered active on the network.

**The kali linux terminal command and result is added below**:



# **TCP Scan**

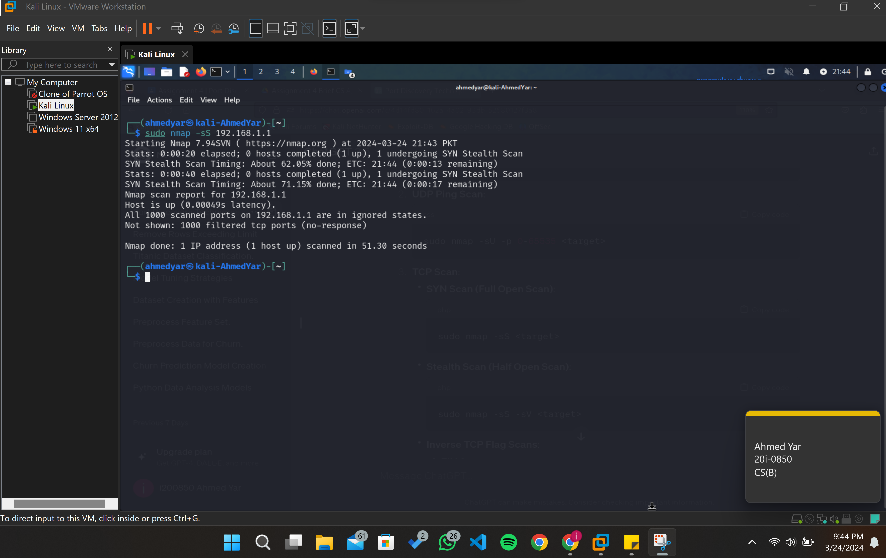
# SYN Scan (Full Open Scan)

**Command**: sudo nmap -sS <target>

**Explanation**: This command uses Nmap with the -sS option to perform a SYN scan (also known as a full open scan). It sends SYN packets to the specified target(s) to check for open ports.

**How it works**: Nmap sends SYN packets to the target(s). If a SYN-ACK (synchronization acknowledgment) is received, it means the port is open.

**The kali linux terminal command and result is added below**:



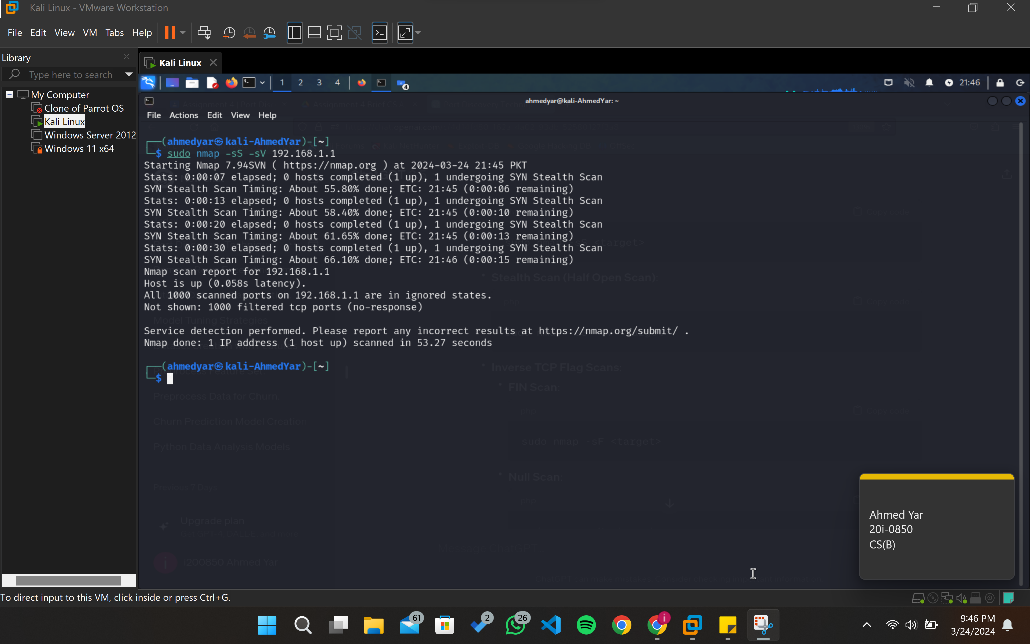
# **Stealth Scan (Half Open Scan)**

**Command**: sudo nmap -sS -sV <target>

**Explanation**: This command combines SYN scan (-sS) with service version detection (-sV) to perform a stealth scan (half open scan). It sends SYN packets to the target(s) without completing the TCP handshake.

**How it works**: Nmap sends SYN packets to the target(s) but doesn't complete the TCP handshake. It analyzes responses to determine open ports and attempts to identify the services running on those ports.

**The kali linux terminal command and result is added below**:



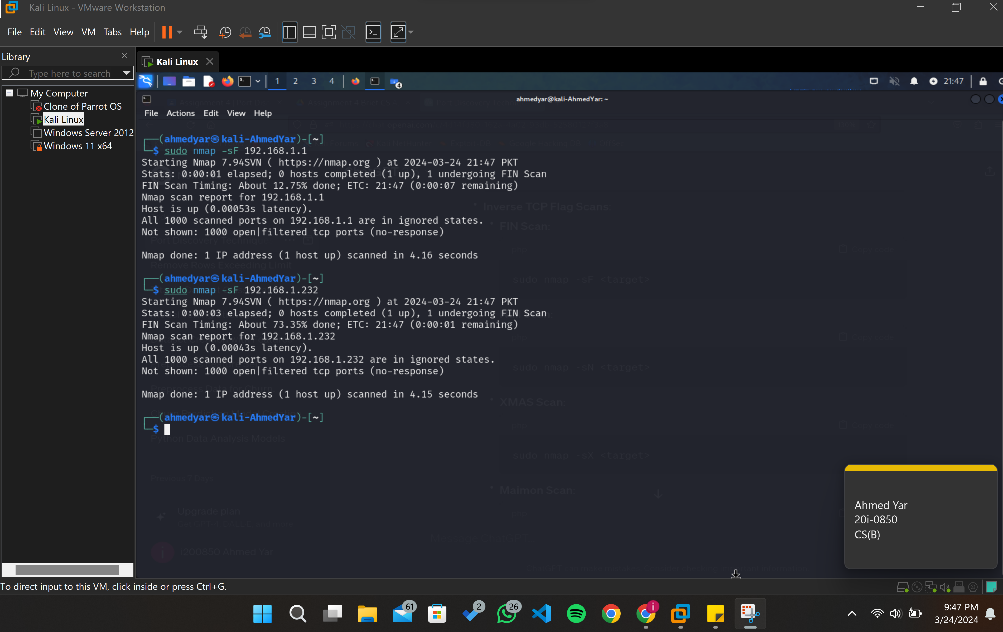
# **Inverse TCP Flag Scan**

# **FIN Scan**

**Command**: sudo nmap -sF <target>

**Explanation**: Sends packets with only the FIN flag set.

**The kali linux terminal command and result is added below**:

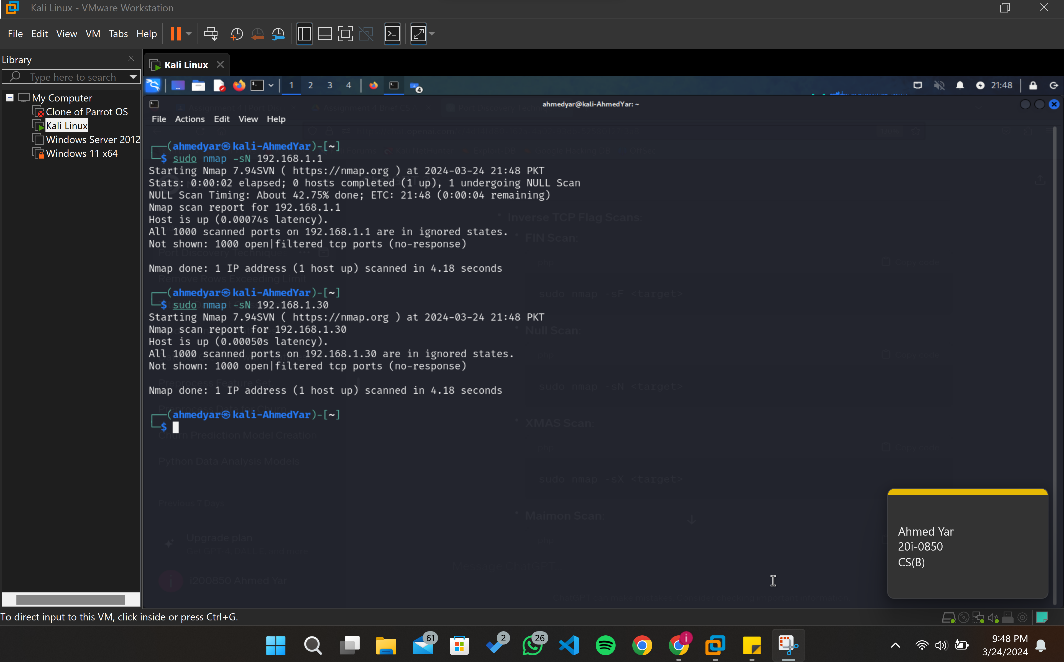


# **Null Scan**

**Command**: sudo nmap -sN <target>

**Explanation**: Sends packets with no TCP flags set.

**The kali linux terminal command and result is added below**:

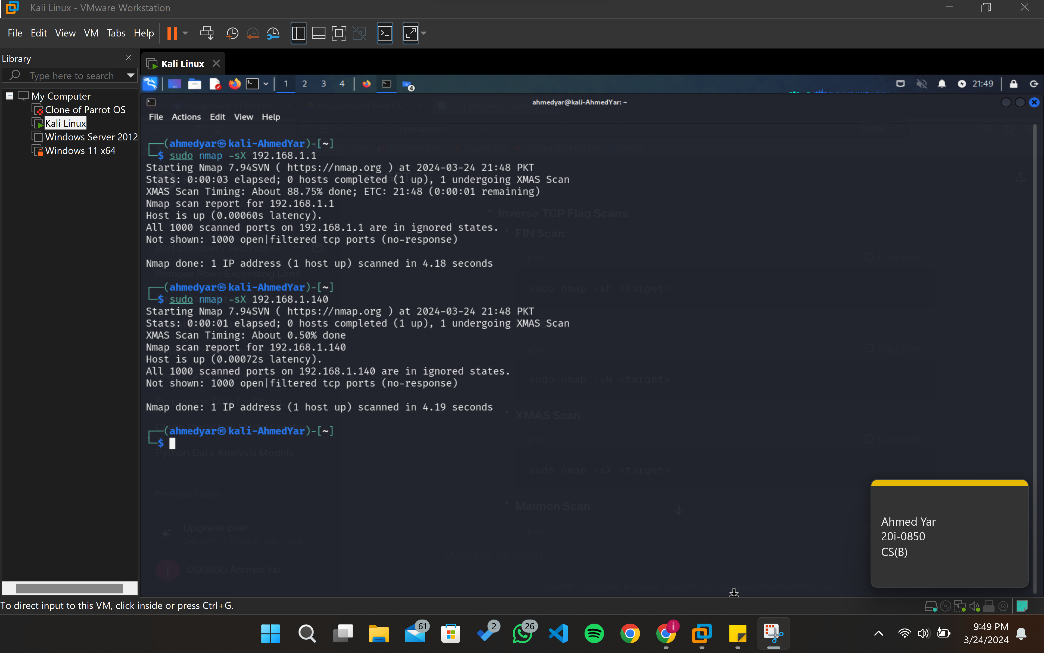


# **XMAS Scan**

**Command**: sudo nmap -sX <target>

**Explanation**: Sends packets with the FIN, PSH, and URG flags set.

**The kali linux terminal command and result is added below**:

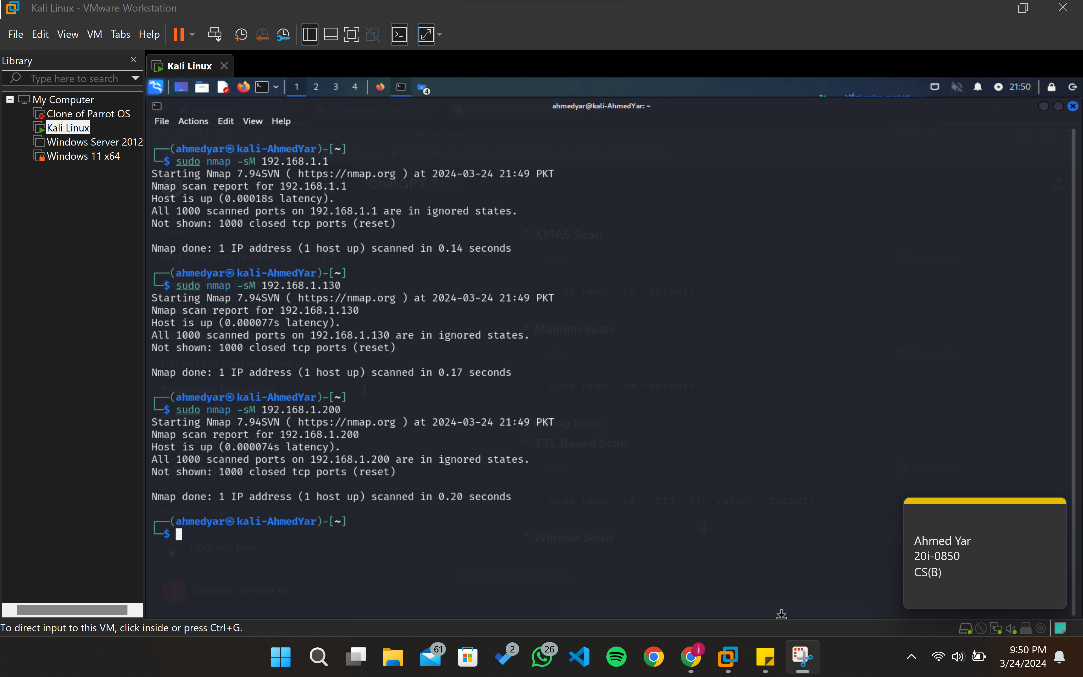


# **Maimon Scan**

**Command**: sudo nmap -sM <target>

**Explanation**: A variation similar to the XMAS scan.

**The kali linux terminal command and result is added below**:



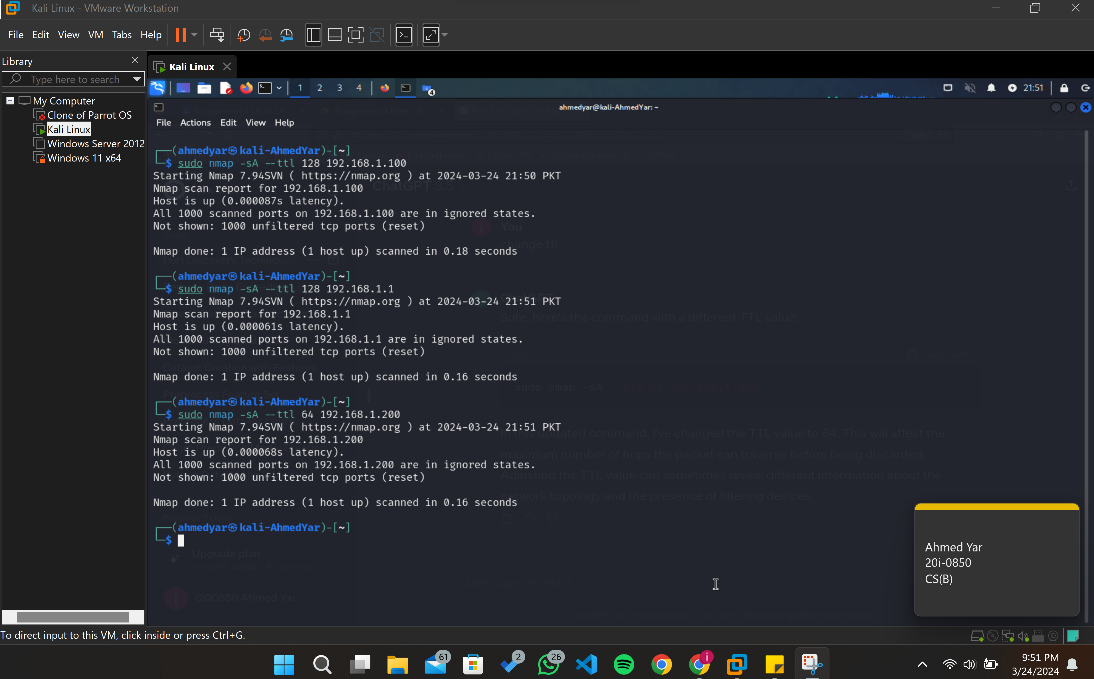
# **ACK Flag Scan**

# **TTL Based Scan**

**Command**: sudo nmap -sA --ttl <TTL\_value> <target>

**Explanation**: Sends packets with the ACK flag set and allows specifying a TTL value.

**The kali linux terminal command and result is added below**:

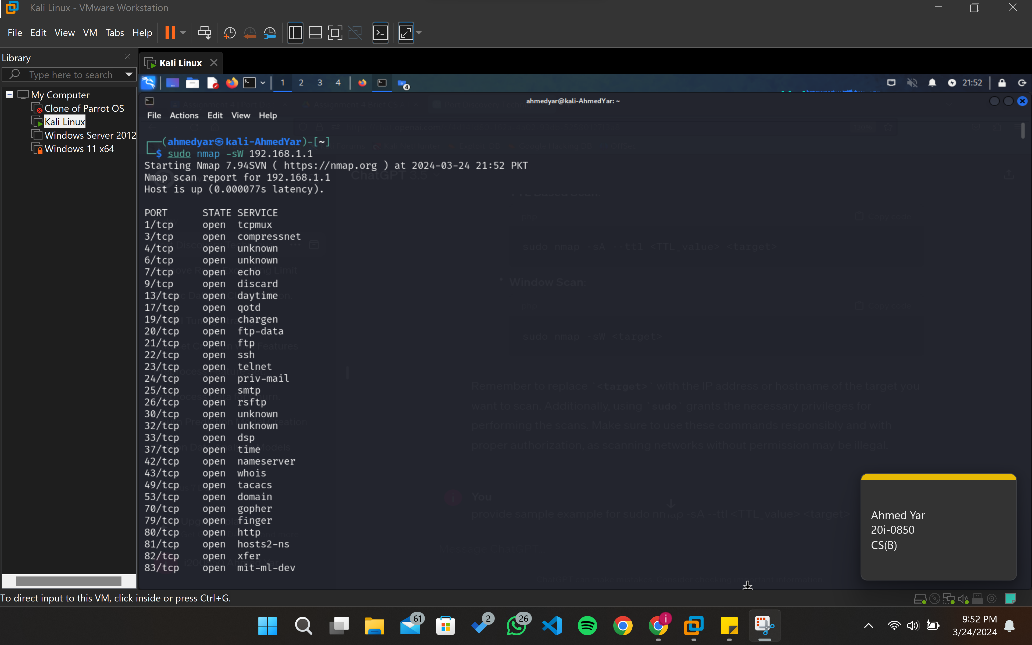


# **Window Scan**

**Command**: sudo nmap -sW <target>

**Explanation**: Relies on the TCP window size field in the TCP header to identify open ports.

**The kali linux terminal command and result is added below**:



# **Summary**

The provided Kali Linux commands offer a comprehensive suite of port discovery techniques for network reconnaissance and vulnerability assessment. With ICMP Ping Scan, Nmap sends ICMP echo requests to determine active hosts on the network, while UDP Ping Scan probes various ports using UDP packets to identify responsive hosts. For TCP Scans, options like SYN Scan (Full Open Scan) and Stealth Scan (Half Open Scan) enable the identification of open ports by sending SYN packets, with the latter maintaining stealthiness by not completing the TCP handshake. Additionally, Inverse TCP Flag Scans, including FIN, NULL, XMAS, and Maimon scans, provide alternative methods for port probing. Moreover, ACK Flag Scan examines responses to packets with the ACK flag set, revealing open ports and potential firewall or filtering devices. These commands offer security professionals invaluable insights into network topology, device availability, and potential vulnerabilities, empowering them to enhance network security effectively and responsibly. It's imperative to utilize these tools ethically and with proper authorization to adhere to legal and ethical standards.

# **References**

* + https://nmap.org/book/host-discovery-techniques.html
  + https://medium.com/@Aircon/nmap-live-host-discovery-tryhackme-thm-47c5c69f1bd7
  + https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-network
  + https://chat.openai.com/c/5d9f8a43-e8df-48de-916d-7e5d42c211b2