**Assignment 03**

**Host Discovery Techniques**

**CS4061**

**Ethical Hacking Concepts and Practices**

**Submitted by:** Faizan Pervaz

**Roll number:** 20I-0565

**Date:** 16-03-2024

**Table of Contents**

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

[ **Steps** 3](#_Toc143364656)

[ **Summary** 14](#_Toc143364657)

[ **References** 14](#_Toc143364658)

# **Introduction**

# In the realm of ethical hacking, understanding various network scanning techniques is crucial. In this report, we delve into different host discovery techniques using the popular network scanning tool, Nmap. Each technique serves to identify active hosts within a network through different protocols and packet types.

# **Steps**

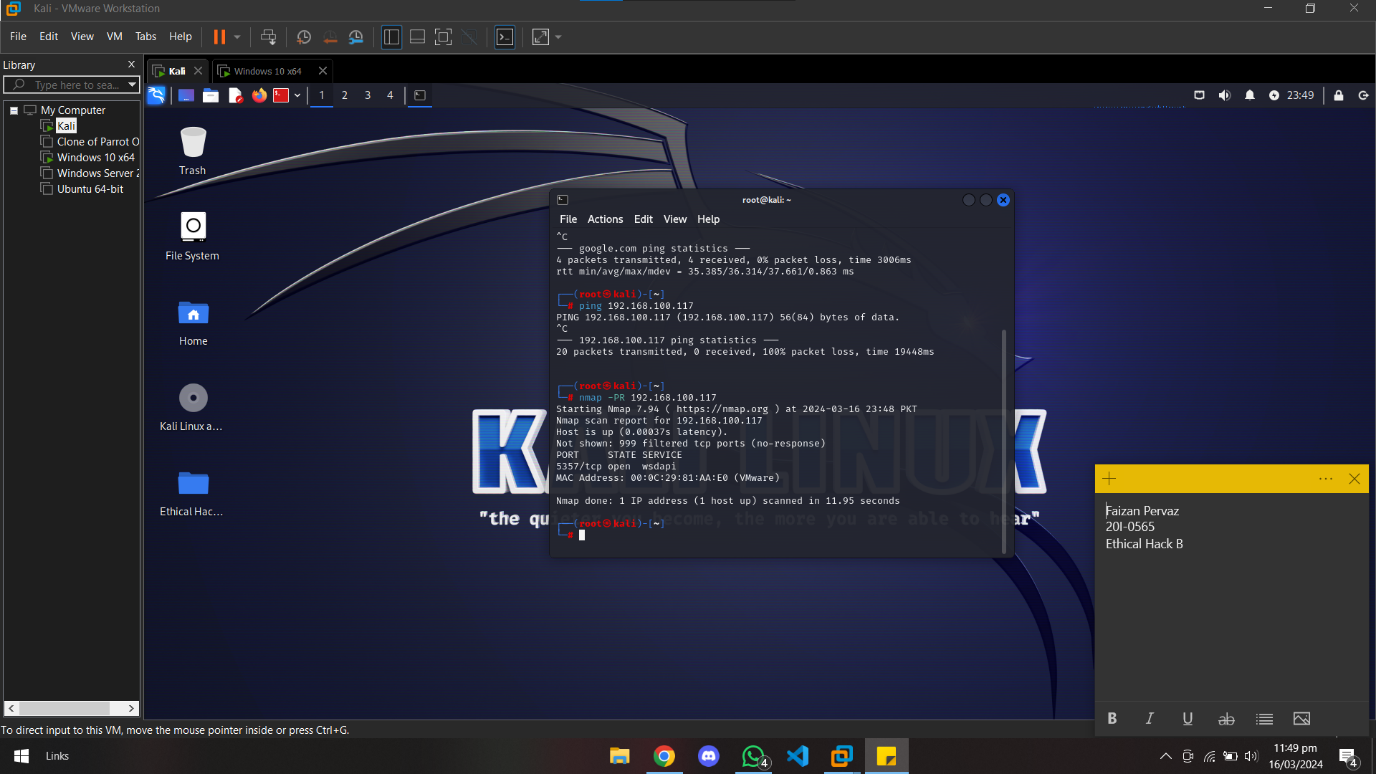
**1. ARP Ping Scan**

**Command**:

* **nmap -PR 192.168.100.117**

**Description**:

* ARP Ping Scan leverages Address Resolution Protocol (ARP) to discover hosts on a local network. It sends ARP requests to the specified IP addresses and examines the responses to determine active hosts.



**2. ICMP Ping Scan**

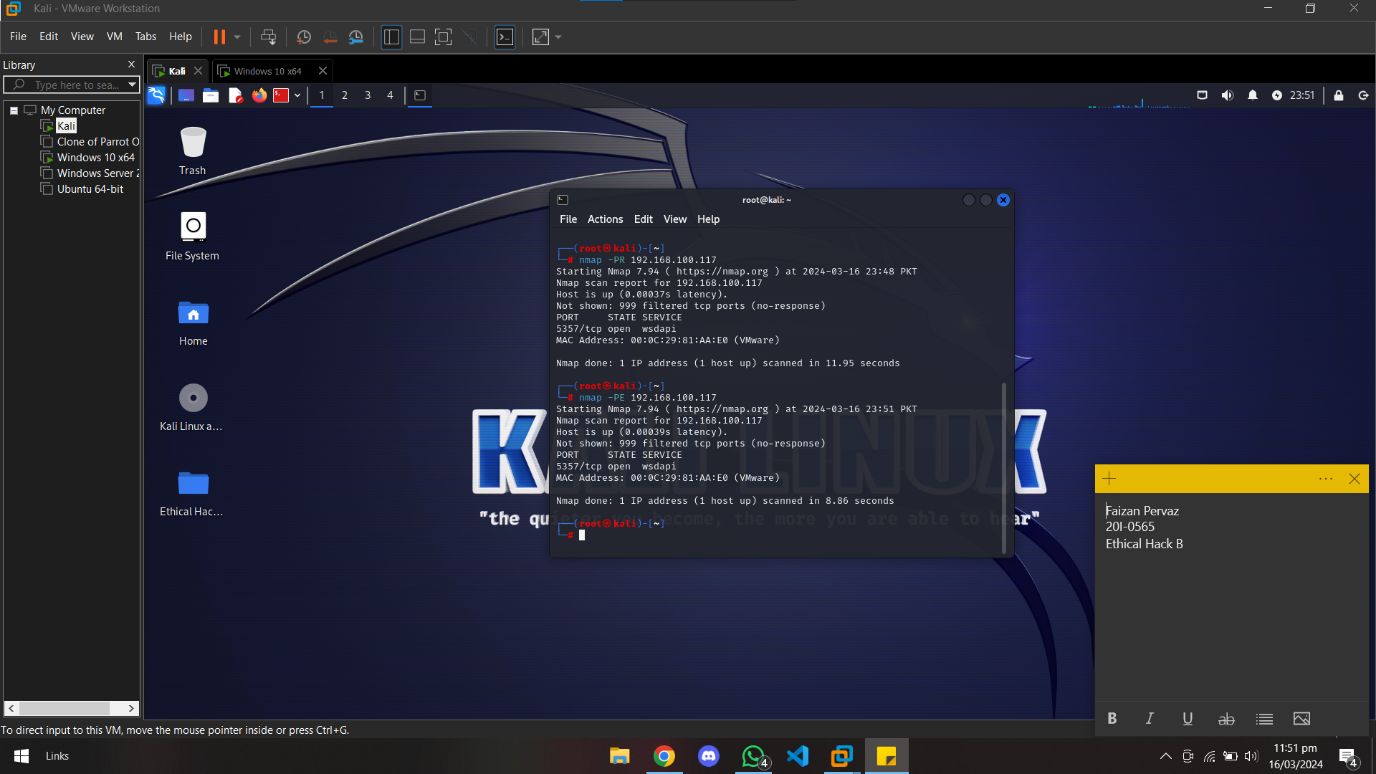
**ICMP Echo Ping**

**Command**:

* + **nmap -PE 192.168.100.117**

**Description**:

* + ICMP Echo Ping sends ICMP Echo Request packets to the target hosts and waits for ICMP Echo Reply packets, indicating an active host.



**ICMP Echo Ping Sweep**

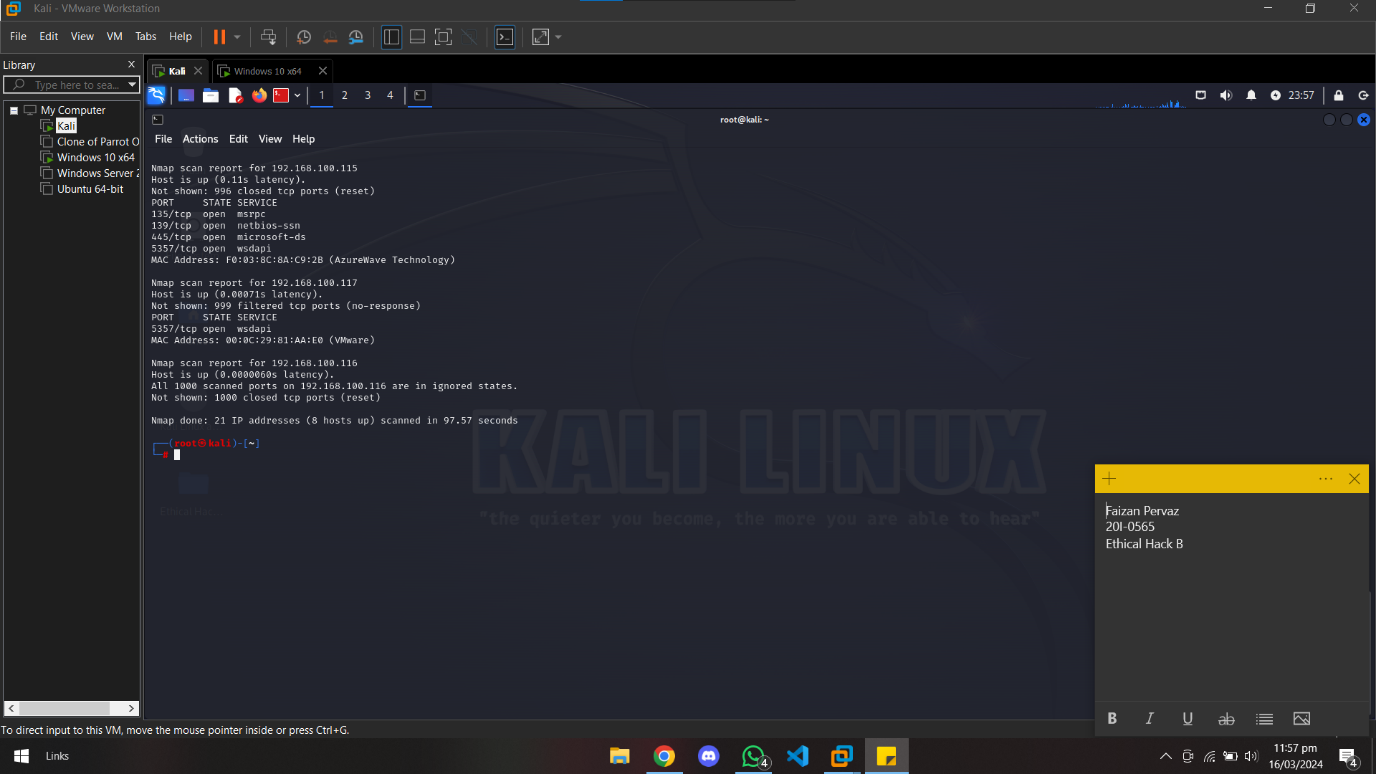
**Command**:

* + Range of IPs: **nmap -PE 192.168.100.100-120**

**Description**:

* + ICMP Echo Ping Sweep performs a sweep across a range of IP addresses, sending ICMP Echo Request packets to each IP and collecting responses.





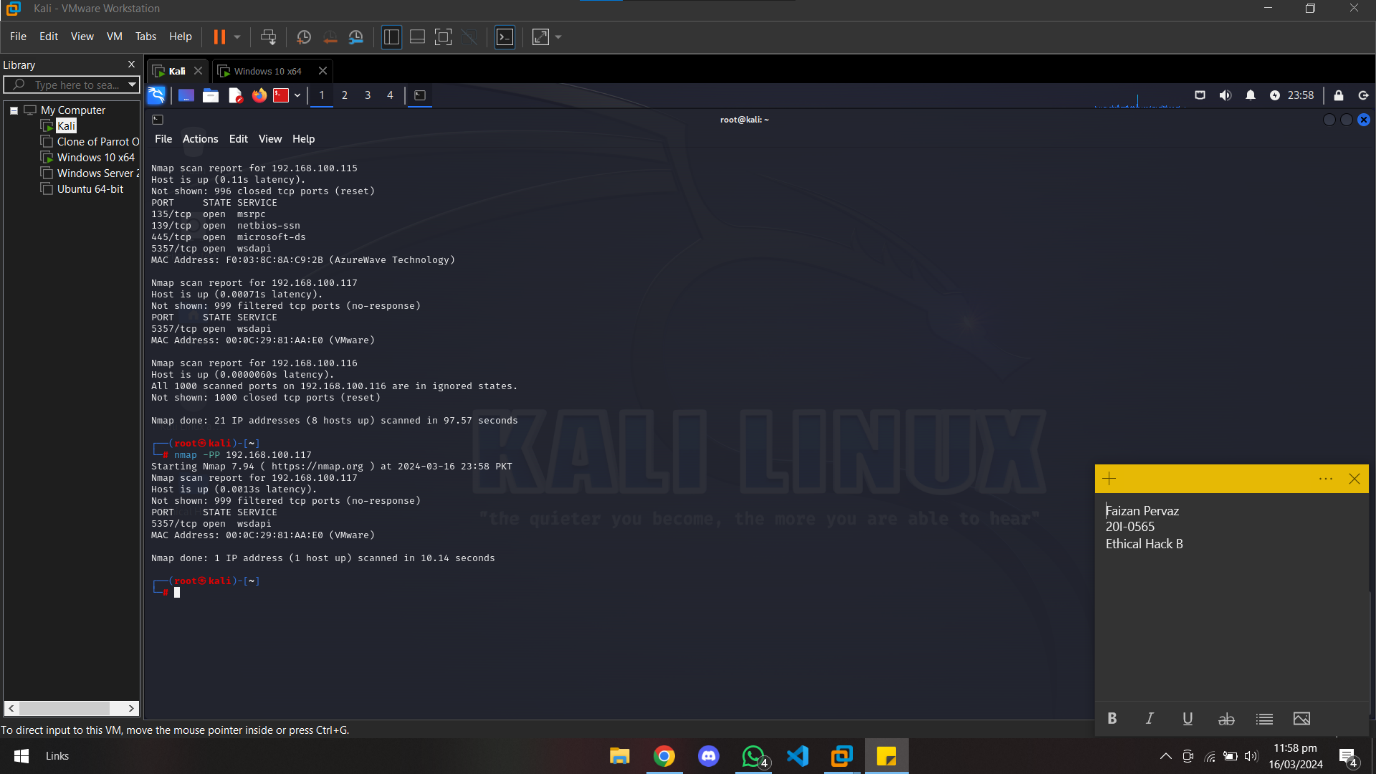
**ICMP Timestamp Ping**

**Command**:

* + **nmap -PP 192.168.100.117**

**Description**:

* + ICMP Timestamp Ping sends ICMP Timestamp Request packets to the target hosts, requesting their current timestamp.



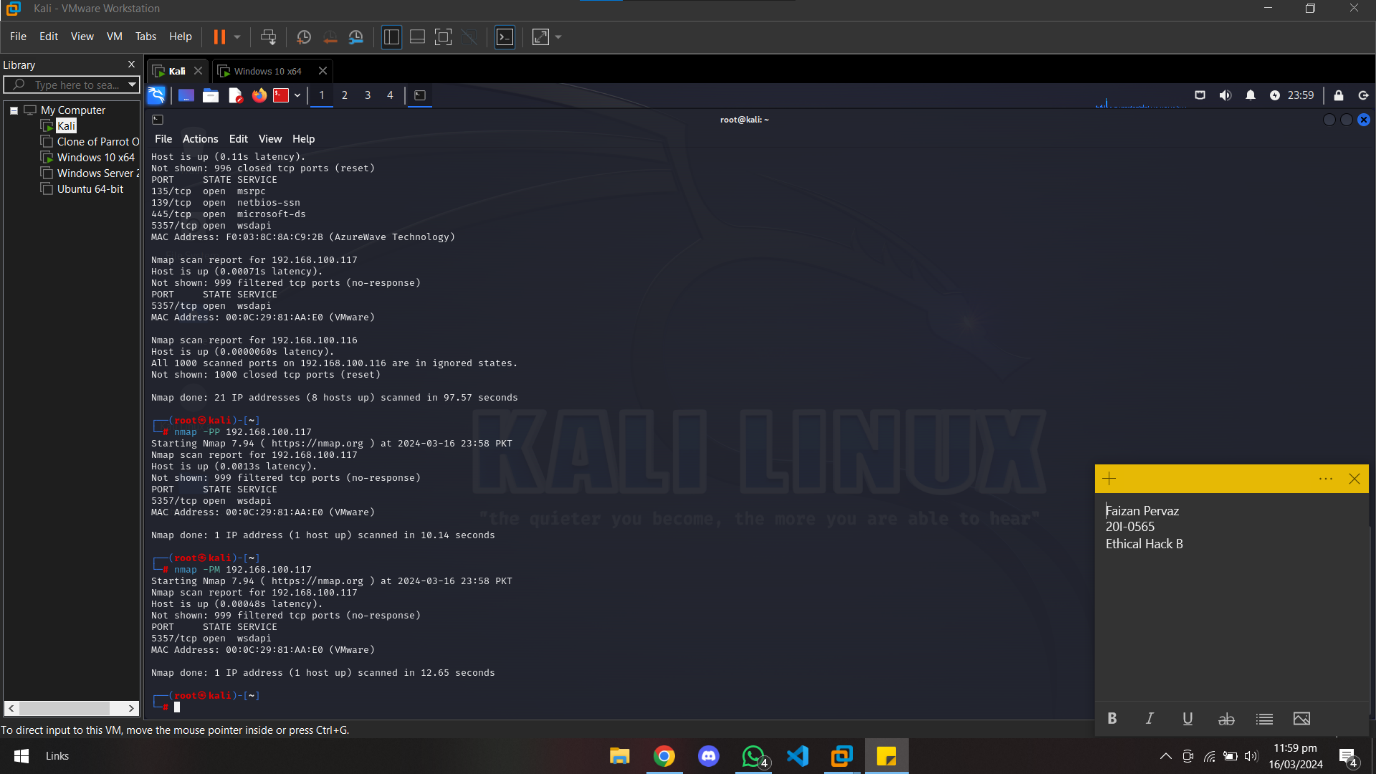
**ICMP Address Mask Ping**

**Command**:

* + **nmap -PM 192.168.100.117**

**Description**:

* + ICMP Address Mask Ping sends ICMP Address Mask Request packets to the target hosts, probing for their subnet mask information.



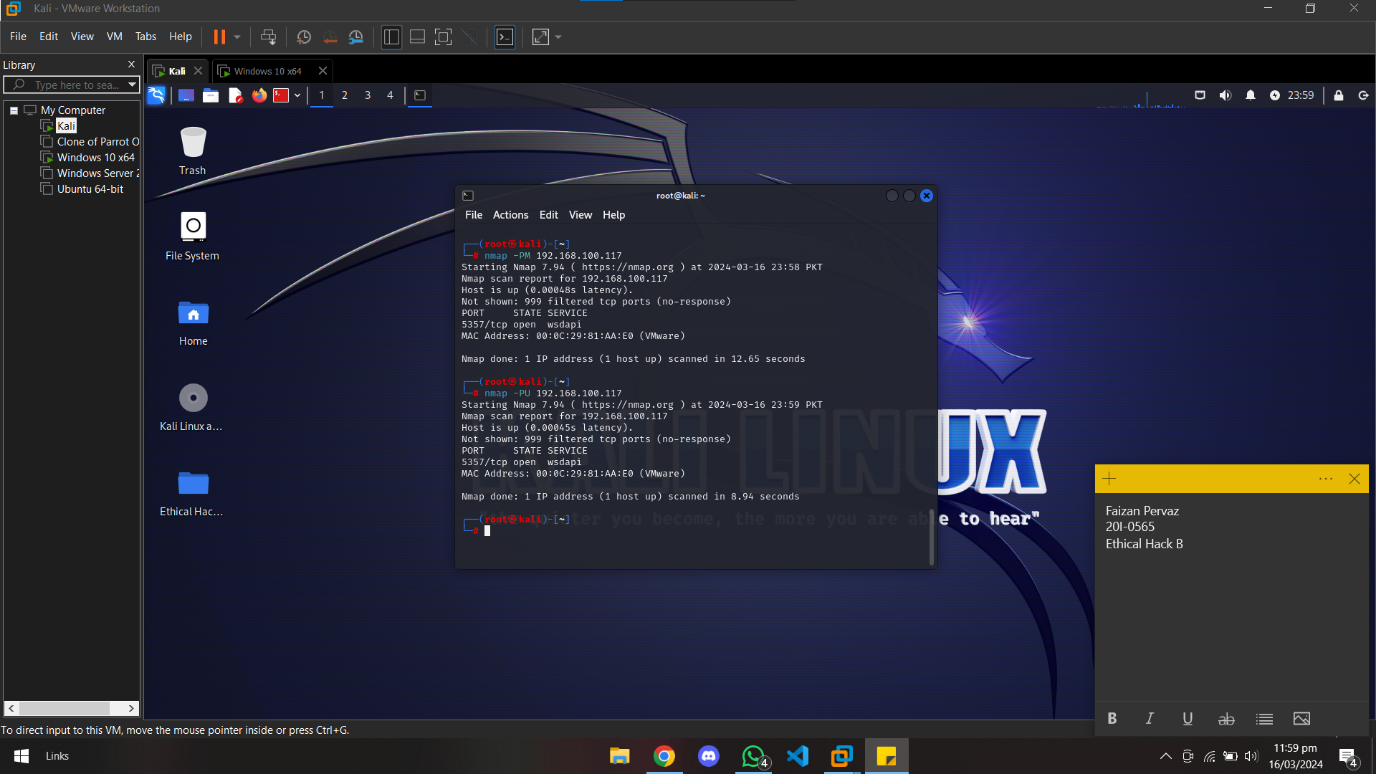
**3. UDP Ping Scan**

**Command**:

* **nmap -PU 192.168.100.117**

**Description**:

* UDP Ping Scan sends UDP packets to the specified ports on target hosts, aiming to elicit responses indicating active hosts.



**4. TCP Ping Scan**

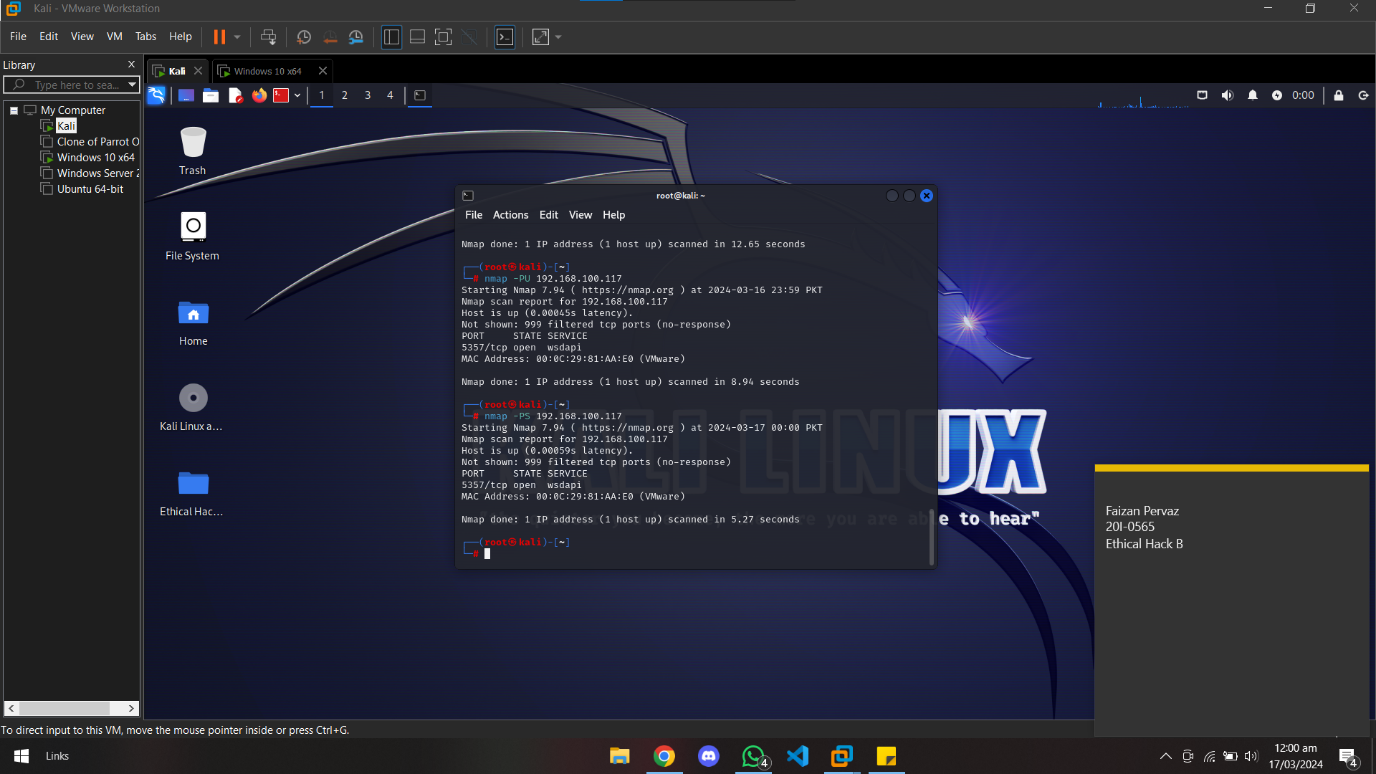
**TCP SYN Scan**

**Command**:

* + **nmap -PS 192.168.100.117**

**Description**:

* + TCP SYN Scan sends SYN packets to target hosts and analyzes responses to identify active hosts.



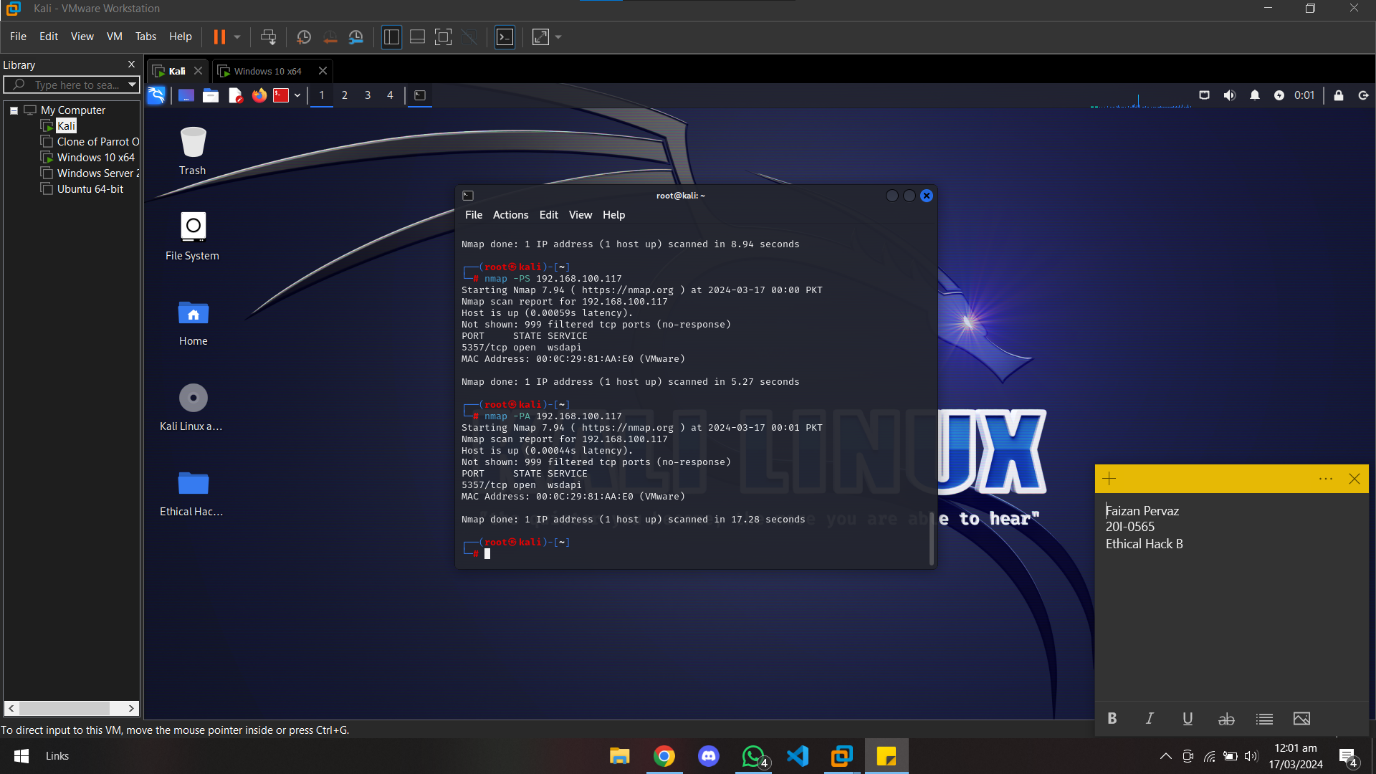
**TCP Ack Scan**

**Command**:

* + **nmap -PA 192.168.100.117**

**Description**:

* + TCP Ack Scan sends ACK packets to target hosts, expecting RST responses from closed ports and no response from open ports.



**TCP Null Scan**

**Command**:

* + **nmap -sN 192.168.100.117**

**Description**:

* + TCP Null Scan sends TCP packets with no flags set to target hosts, aiming to elicit different responses from open and closed ports.



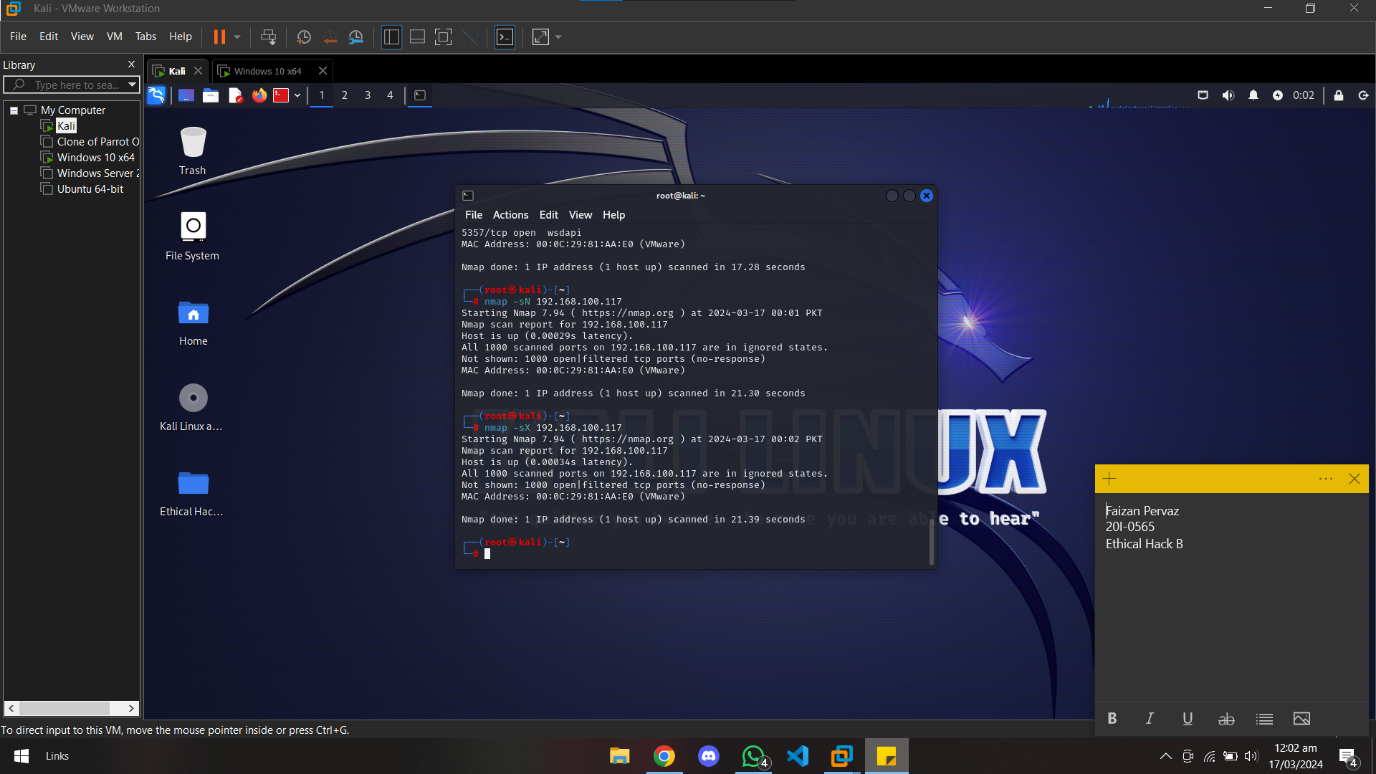
**TCP XMAS Scan**

**Command**:

* + **nmap -sX 192.168.100.117**

**Description**:

* + TCP XMAS Scan sends TCP packets with various flags (FIN, URG, PSH) set to target hosts, exploiting differences in responses from open and closed ports.



**TCP FIN Scan**

**Command**:

* + **nmap -sF 192.168.100.117**

**Description**:

* + TCP FIN Scan sends TCP packets with only the FIN flag set to target hosts, examining responses to determine port state.



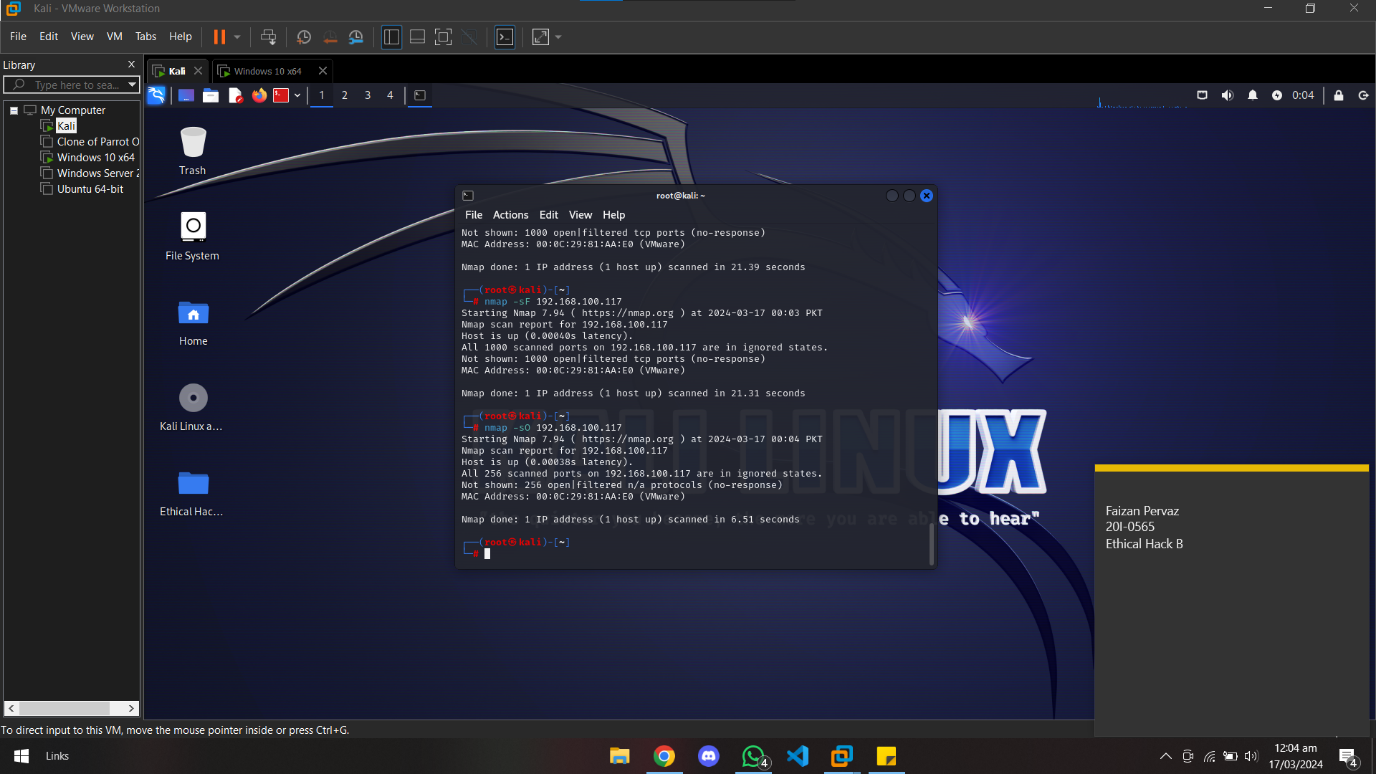
**5. IP Protocol Ping Scan**

**Command**:

* **nmap -sO 192.168.100.117**

**Description**:

* IP Protocol Ping Scan probes hosts for supported IP protocols, allowing detection of active hosts based on their responses to protocol queries.



# **Summary**

Through the utilization of various host discovery techniques, ethical hackers can gain insights into network topology, identify potential vulnerabilities, and enhance overall network security. Understanding the intricacies of each scanning technique enables practitioners to effectively assess network assets and fortify defenses against malicious actors.

# **References**

1. <https://www.hackingarticles.in/network-scanning-using-nmap-beginner-guide/>
2. <https://nmap.org/docs.html>
3. <https://nmap.org/book/>
4. <https://www.tutorialsfreak.com/ethical-hacking-tutorial/what-is-network-scanning-and-its-types>
5. <https://www.cybrary.it/blog/top-nmap-tricks-for-a-vulnerability-assessment>