**Assignment 04**

**Port Discovery Techniques**

**CS4061**

**Ethical Hacking Concepts and Practices**

**Submitted by:** Muhammad Ahmed

**Roll number:** 20I-1855

**Date:** 24-03-2024

**Table of Contents**

[ **Introduction** 4](#_Toc162199414)

[ **Steps** 4](#_Toc162199415)

[Understanding Port Scanning Techniques 4](#_Toc162199416)

[1. ICMP Ping Scan 4](#_Toc162199417)

[2. UDP Ping Scan 4](#_Toc162199418)

[3. SYN Scan (Full Open Scan) 5](#_Toc162199419)

[4. Stealth Scan (Half Open Scan) 5](#_Toc162199420)

[5. FIN Scan 5](#_Toc162199421)

[6. Null Scan 5](#_Toc162199422)

[7. XMAS Scan 6](#_Toc162199423)

[8. Maimon Scan 6](#_Toc162199424)

[9. ACK Flag Scan 6](#_Toc162199425)

[10. TTL Based Scan 6](#_Toc162199426)

[11. Window Scan 7](#_Toc162199427)

[Running the Program: 7](#_Toc162199428)

[Analyzing Scan Results: 7](#_Toc162199429)

[Comparative Analysis: 7](#_Toc162199430)

[Experimentation and Exploration: 7](#_Toc162199431)

[ **Summary** 8](#_Toc162199432)

[ **References** 8](#_Toc162199433)

# **Introduction**

Port scanning is a fundamental technique used in cybersecurity to identify open ports and services on target systems. Understanding how port scanning works and the various techniques available is essential for assessing the security posture of networks and identifying potential vulnerabilities. In this assignment, we explore different port discovery techniques implemented in a Python program. We will learn about the implementation details of each technique, their strengths and limitations, and how to interpret the obtained from port scans.

# **Steps**

## Understanding Port Scanning Techniques

* Following is the scanning techniques that were implemented after a thorough understanding:

### 1. ICMP Ping Scan

* ICMP Ping Scan is a basic technique used to determine if a target IP address is reachable.
* The program sends ICMP echo request packets to the target IP address and waits for responses.
* If a response is received, the target is considered up. If no response is received, the target may be down or blocking ICMP traffic.

### 2. UDP Ping Scan

* UDP Ping Scan is another method to determine if a target IP address is reachable, especially when ICMP traffic is blocked.
* The program sends UDP packets to a specific port (e.g., port 1) and waits for responses.
* If a response is received, the target is considered up. If no response is received, the target may be down or blocking UDP traffic.

### 3. SYN Scan (Full Open Scan)

* SYN Scan, also known as Full Open Scan, is a stealthy port scanning technique to identify open ports on a target system.
* The program sends TCP SYN packets to the target ports and waits for SYN-ACK responses.
* If a SYN-ACK response is received, the port is considered open. If no response is received, the port may be closed or filtered.

### 4. Stealth Scan (Half Open Scan)

* Stealth Scan, also known as Half Open Scan, is similar to SYN Scan but does not complete the TCP handshake, making it less detectable.
* The program sends TCP SYN packets to the target ports but does not respond to SYN-ACK packets.
* Open ports are identified based on SYN-ACK responses, similar to SYN Scan.

### 5. FIN Scan

* FIN Scan is a port scanning technique that sends TCP FIN packets to determine if ports are open.
* The program sends TCP FIN packets to the target ports and waits for RST-ACK responses.
* If a RST-ACK response is received, the port is considered closed. If no response is received, the port may be open or filtered.

### 6. Null Scan

* Null Scan is a port scanning technique that sends TCP packets with no flags set to identify open ports.
* The program sends TCP packets with no flags set to the target ports and waits for RST-ACK responses.
* Similar to FIN Scan, if a RST-ACK response is received, the port is considered closed. No response may indicate an open or filtered port.

### 7. XMAS Scan

* XMAS Scan sends TCP packets with the FIN, URG, and PSH flags set to identify open ports.
* The program sends XMAS packets to the target ports and waits for responses.
* XMAS Scan may not work correctly on Windows systems due to how they handle such packets.

### 8. Maimon Scan

* Maimon Scan sends TCP packets with the SYN and ACK flags set to identify open ports.
* The program sends Maimon packets to the target ports and waits for responses.
* Similar to SYN Scan, open ports are identified based on SYN-ACK responses.

### 9. ACK Flag Scan

* ACK Flag Scan sends TCP packets with only the ACK flag set to identify open ports.
* The program sends ACK packets to the target ports and waits for responses.
* Open ports are identified based on the absence of RST responses.

### 10. TTL Based Scan

* TTL Based Scan involves sending ICMP packets with varying TTL values to determine network topology and identify live hosts.
* The program sends ICMP packets with different TTL values and observes responses.
* If a response is received, the TTL value indicates the number of hops to the target.

### 11. Window Scan

* Window Scan identifies open ports by analyzing TCP window sizes in response packets.
* The program sends TCP packets to the target ports and examines window sizes in responses.
* Ports with non-default window sizes are considered open.

## Running the Program:

* Execute the Python program on your local machine or a virtual environment.
* Follow the prompts to input the target IP address and select the port discovery technique you want to use.

## Analyzing Scan Results:

* Analyze the obtained from each port scanning technique.
* Understand how to interpret open and closed ports, as well as any limitations or special considerations for each technique.

## Comparative Analysis:

* Compare the effectiveness, stealthiness, and limitations of different port scanning techniques.
* Identify which techniques may be more suitable for specific scenarios or environments.

## Experimentation and Exploration:

* Experiment with different target IP addresses and port ranges to observe how the scan vary.
* Explore the behavior of port scanning techniques on different operating systems and network configurations.

# **Summary**

In conclusion, this assignment provides valuable hands-on experience with various port scanning techniques commonly used in cybersecurity assessments. By understanding how each technique works and analyzing their results, you gain insights into network reconnaissance and vulnerability assessment processes. Port scanning is a foundational skill in cybersecurity, and mastering these techniques will enhance your ability to identify and mitigate potential security risks in networked environments.

# **References**

Add at least 3 references to your assignment.





