**Assignment 03**

**Host Discovery**

**CS4061**

**Ethical Hacking Concepts and Practices**

**Submitted by:** Muhammad Ahmed

**Roll number:** 20I-1855

**Date:** March 15, 2024

**Table of Contents**

[ **Introduction** 3](#_Toc161374412)

[ **Implementation** 3](#_Toc161374413)

[ **Scanning Techniques** 3](#_Toc161374414)

[ **Results** 4](#_Toc161374415)

[ **Limitations** 4](#_Toc161374416)

[ **Summary** 4](#_Toc161374417)

[ **References** 4](#_Toc161374418)

# **Introduction**

The implementation of the host discovery tool aims to provide a versatile and efficient solution for network scanning using Python and Scapy. This tool facilitates the identification of active hosts and open ports within a network, allowing for effective network management and security analysis.

# **Implementation**

The host discovery tool is developed using Python programming language along with the Scapy library. Scapy provides a powerful platform for crafting and sending packets at the network level, making it well-suited for implementing various network scanning techniques.

The tool encompasses different scanning techniques, including ARP ping, ICMP ping, UDP ping, TCP SYN scan, etc. These techniques are implemented as separate functions within the tool, allowing for modular and flexible usage.

# **Scanning Techniques**

Each scanning technique serves a specific purpose in the host discovery process. Some of its functionality is as follows:

* **ARP Ping Scan**: This technique utilizes Address Resolution Protocol (ARP) requests to determine the IP-MAC address mapping of devices on the network.
* **ICMP Ping Scan:** ICMP Echo Ping and ICMP Echo Ping Sweep techniques involve sending ICMP echo requests to hosts and networks, respectively, to determine their availability.
* **UDP Ping Scan:** UDP Ping Scan involves sending UDP packets to target hosts and waiting for responses, indicating their availability.
* **TCP SYN Scan:** This technique involves sending TCP SYN packets to target hosts and analyzing their responses to identify open ports.
* **TCP ACK Scan, TCP Null Scan, TCP XMAS Scan, TCP FIN Scan**: These techniques utilize variations of TCP packets to determine the state of ports on target hosts, including open, closed, or filtered.

# **Results**

Upon running the host discovery tool on a test network, the following results were obtained:

* **ARP Ping Scan Results:** Discovered active hosts and their corresponding MAC addresses.
* **ICMP Ping Scan Results**: Identified active hosts through ICMP echo responses.
* **UDP Ping Scan Results:** Detected active hosts by receiving UDP responses.
* **TCP SYN Scan Results:** Found open ports on target hosts through SYN-ACK responses.

# **Limitations**

The implemented host discovery tool demonstrates effectiveness in identifying active hosts and open ports within a network. However, certain limitations exist, such as the inability to bypass firewall rules and the potential for false positives or false negatives in certain scanning techniques.

# **Summary**

In conclusion, the host discovery tool serves as a valuable asset for network administrators and security analysts in managing and securing network infrastructure. With further refinement and optimization, it can become an indispensable tool in network reconnaissance and vulnerability assessment.

# **References**

* Python Documentation: https://docs.python.org/
* Scapy Documentation: https://scapy.readthedocs.io/