Cairo University, Faculty of Computers and Artificial Intelligence

FACULTY OF COMPUTERS AND AI, CAIRO UNIVERSITY

IT331 – Data Communication

Assignment #1

Course Instructors:

Dr. Iman EL-Sayed

Prepared By:

Belal Mohamed Youness (20220087) belalyouness494@gmail.com

Documentation

Overview

This tool is a network scanner designed to meet the objectives outlined in the assignment. It leverages the Scapy library to provide various functionalities, including network discovery, packet analysis, packet creation, and performance measurement. The tool also logs results to ensure proper analysis and reporting.

How Each Feature Works

1. Network Discovery

- The `scan` function takes a subnet (e.g., `192.168.1.0/24`) as input.
- An ARP request is broadcasted using `Ether(dst="ff:ff:ff:ff:ff:ff")`.
- Responses are collected using `srp`, mapping IP addresses to MAC addresses.
- Outputs a list of active devices.

2. Packet Analysis

- The `packet_analysis` function accepts:
  - Target IP(s). o Protocol filter (e.g., TCP, UDP, ICMP).
  - Maximum number of packets to capture.
- Captures packets using `sniff` with a filter like `ip and tcp`.
- Extracts packet details (IP addresses, ports, size, etc.) using Scapy layers (e.g., `IP`, `TCP`).
- Saves packets to a PCAP file using `wrpcap`.

3. Custom Packet Creation and Transmission

- The `create_and_send_packet` function constructs packets based on user-defined protocols:
  - ICMP ping packets with `ICMP()`.
  - TCP SYN packets with `TCP(flags="S", dport=80)`.
  - UDP packets targeting DNS with `UDP(dport=53)`.
- Sends packets with `send`.

4. Traffic Monitoring and Logging

- Logs packet details during analysis using the captured packet list.
- Stores packet logs in PCAP format for further analysis.

5. Network Performance Measurement

- The `measure_network_performance` function calculates:
    - **Latency**: Time taken to send an ICMP request and receive a response. o **Throughput**: Number of packets divided by elapsed time.
    - **Jitter**: Variability in latency.
- Logs metrics to a text file for record-keeping.

6. Command-Line Interface

- The `main` function provides an interactive menu:
    - Option 1: Scan subnet for active devices.
    - Option 2: Analyze traffic for a specific IP/protocol. o Option 3: Create and send a custom packet. o Option 4: Measure network performance. o Option 5: Exit.

How It Works

1. Run the script using Python.
2. Follow the prompts in the command-line interface to select tasks.
3. Provide necessary inputs (e.g., subnet, target IP, protocol) as prompted.
4. View results directly in the terminal or output files (traffic_capture.pcap, performance_log.txt).