COMP 7003
Assignment 2
User Guide

Towa Quimbayo
A01086002
Feb 3rd, 2025

Purpose

The purpose of this document is to provide a comprehensive guide for setting up and running the Assignment 2 program that captures and parses packets. To further elaborate, the program uses Python with Scapy package to capture real-time network traffic and manually parse the packet headers for ARP and IPv4 (including UDP, TCP, and ICMP). The guide will explain the installation requirements, the steps needed to configure the environment, and commands to correctly run the application. The document also dives deeper in describing the command line arguments and includes instructions for testing the program with sample `pcap` files provided in the `/pcap` folder.

Installing

Prerequisites

- **Python Installation**: Ensure you have Python installed on your system.
- **Virtual Environment Setup**: Create and activate a virtual environment.
  ```
  python3 -m venv venv
  source venv/bin/activate
  ```
- **Modules Installation**: Install the required Python modules using pip.
  ```
  pip install scapy psutil
  ```
- **OS Compatibility**: The program works best on Linux environments and for the purpose of this guide, examples and commands are tailored for Ubuntu using WSL.
- **Sample PCAP Files**: 5 sample `pcap` files are provided in the `/pcap` folder which can be used for testing and validation on different parsers.

Running

To run the program, execute the command below in the terminal but ensure to replace the arguments in square brackets “[ ]” with the appropriate values which can be reference further below in the Command Line Arguments section.

```
sudo python3 main.py -i [interface] -c [count] -f [filter]
```

Command Line Arguments

The program supports the following command line arguments:

Variable	Purpose
`-i` or **`--interface`**	The network interface to capture packets on, including `eth0`, `wlan0`, or `any`.

`-c` or **`--count`**	Number of packets to capture.
`-f` or **`--filter`**	An optional BPF filter to apply such as `arp`, `udp`, `tcp`, or `icmp`.

Example Commands

1. ARP protocol filter with 1 packet on eth0 interface.

```
sudo python3 main.py -i eth0 -c 1 -f arp
```

2. UDP (IPv4) protocol filter with 1 packet on eth0 interface.

```
sudo python3 main.py -i eth0 -c 1 -f udp
```

3. TCP (IPv4) protocol filter with 2 packets on any interface.

```
sudo python3 main.py -i any -c 2 -f tcp
```

4. ICMP (IPv4) protocol filter with 2 packets on any interface.

```
sudo python3 main.py -i any -c 2 -f icmp
```

5. DNS (IPv4 / UDP) protocol filter with 2 packets on any interface.

```
sudo python3 main.py -i any -c 2 -f "src port 53"
sudo python3 main.py -i any -c 2 -f "dst port 53"
```