COMP 7003
Assignment 2
User Guide

Andy Tran
A01266629
Oct 2nd, 2024

Purpose

- A program to capture and analyze network packets in real-time based on custom BPF filters, displaying packet details for Ethernet, ARP, IPv4, TCP and UDP protocols in Hex, Decimal, and Binary for flags.

Installing

Obtaining

```
git clone https://github.com/AyyyTran/COMP7003Assign2.git
```

Building

```
Cd COMP7003Assign2
cd source
Cd src
```

Running

sudo python scanner.py --interface <network-interface> --filter <BPF-filter> --count <number-of-packets>

Environment Variables

The following environment variables alter the behaviour of main:

Variable	Purpose

Configuration

The following configuration values can be set in <file>:

Variable	Purpose

Command Line Arguments

The following configuration values can be set in <file>:

Variable	Purpose
--interface	Network interface to sniff packets
--filter	BPF filter to capture specific traffic
--count	Number of packets to capture

Examples

sudo python scanner.py --interface wlo1 --filter tcp --count 10

sudo python scanner.py --interface wlo1 --filter udp --count 5

sudo python scanner.py --interface wlo1 --filter ip --count 5

sudo python scanner.py --interface wlo1 --filter arp --count 50