Packet Sniffer

Vibudh Bhardwaj

Feb 04, 2025

CONTENTS:

CHAPTER

ONE

PACKET SNIFFER DOCUMENTATION

1.1 Overview

pktsniffer.py is a Python-based packet sniffer that reads *.pcap* files and analyzes network traffic by displaying Ethernet, IP, TCP, UDP, and ICMP headers. It includes filtering options to focus on specific packet types, host IP addresses, ports, and networks.

1.2 Requirements

- Python 3.x
- *scapy* library
- *.pcap* file for analysis

To install *scapy*, use:

```
pip install scapy
```

1.3 Usage

```
python pktsniffer.py -r <pcap_file> [options]
```

1.4 Command-Line Arguments

Argument	Description
-r, –read	Path to the *.pcap* file (Required)
-c, –count	Number of packets to analyze (default: all)
-host	Filter packets by a specific host IP address
-port	Filter packets by a specific port number
-ip	Show only IP packets
-tcp	Show only TCP packets
-udp	Show only UDP packets
-icmp	Show only ICMP packets
-net	Filter packets by a specific network address

1.5 Functionality

1.5.1 parse_arguments()

Parses command-line arguments using *argparse* and returns the parsed options.

1.5.2 packet_filter(pkt, args)

Filters packets based on user-specified criteria. - Checks for specific protocol layers (IP, TCP, UDP, ICMP). - Filters packets based on host IP, port number, and network address.

1.5.3 print_packet_summary(index, pkt)

Prints detailed packet information, including: - Ethernet header (MAC addresses, EtherType) - IP header (Source/Destination IP, TTL, Flags, etc.) - TCP header (Ports, Sequence/Acknowledgment numbers, Flags) - UDP header (Ports, Length, Checksum) - ICMP header (Type, Code, Checksum)

1.5.4 main()

- Parses command-line arguments.
- Reads packets from the *.pcap* file.
- Applies filtering criteria.
- Prints packet details for filtered packets.

1.6 Example Usage

Read and analyze all packets in *traffic.pcap*:

```
python pktsniffer.py -r traffic.pcap
```

Filter packets to only show TCP traffic:

```
python pktsniffer.py -r traffic.pcap -tcp
```

Filter packets to only show traffic from/to *192.168.1.1*:

```
python pktsniffer.py -r traffic.pcap -host 192.168.1.1
```

Filter by port *80* (HTTP traffic):

```
python pktsniffer.py -r traffic.pcap -port 80
```

Analyze the first 10 packets:

```
python pktsniffer.py -r traffic.pcap -c 10
```

1.7 Notes

- If an invalid network address is provided, the script will discard the filter.
- If multiple filters are specified, packets must match **all** criteria to be displayed.

1.8 License

This script is intended for educational and debugging purposes only. Unauthorized packet sniffing may violate network policies and laws. Use responsibly.