pktsniffer

Geoffrey Tse

Sep 26, 2025

CONTENTS:

Add your content using `reStructuredText` syntax. See the reStructuredText documentation for details.

CHAPTER

ONE

WELCOME TO PKTSNIFFER'S DOCUMENTATION!

1.1 Modules

pktsniffer.**build_filters**(*tokens: List[str]*) → List[Tuple[str, str]]

Convert a list of filter tokens (strings) into a structured list of (filter_type, value) tuples.

Supported filter formats:

- "host <ip>" → match packets from/to a specific host IP
- "ip <ip>" → match packets containing a specific IP
- "port <num>" → match packets using a given port number
- "net <cidr>" → match packets in a given network (e.g. 192.168.0.0/24)
- "tcp" → match only TCP packets
- "udp" → match only UDP packets
- "icmp" → match only ICMP packets

Filters are parsed left-to-right. Tokens without value are assumed boolean filters (tcp/udp/icmp).

pktsniffer.**flags_str**(*flags_field*) → str

Convert a packet flags field into a string.

Parameters
flags_field – The flags value from a packet (e.g., TCP flags)

Returns
String representation of the flags if possible, otherwise an empty string "" if conversion fails.

pktsniffer.**ip_in_network**(*ip_str: str*, *network_str: str*) → bool

Check if a given IP address belongs to a given network.

Parameters

- **ip_str** (*str*) – The IP address to test (e.g. "192.168.1.5").
- **network_str** (*str*) – The network in CIDR form (e.g. "192.168.1.0/24"). If no "/mask" is given and it's IPv4, assume "/24".

Returns
True → if the IP is inside the network False → if the IP is not in the network or input is invalid

pktsniffer.**is_ip_literal**(*s: str*) → bool

Check if the given string is a valid IP address (IPv4 or IPv6).

Returns
True → if the string is a valid IP address False → if the string is not a valid IP address

pktsniffer.**main**()

pktsniffer.**match_filters**(*pkt*, *filters: List[Tuple[str, str]]*) → bool

Check if a packet matches all given filters. (All filters must pass → AND logic)

Parameters

- **pkt** – A Scapy packet object
- **filters** – A list of (filter_type, value) tuples

Returns
True → if the packet matches every filter False → if the packet fails any filter

pktsniffer.**parse_args**() → Namespace

Parse command-line arguments for the pktsniffer program.

Returns

An object containing all parsed arguments
(e.g., args.read, args.count, args.filters).

Return type
argparse.Namespace

pktsniffer.**print_packet_summary**(*idx: int*, *pkt*) → None

Print details for a single Scapy packet object.

PYTHON MODULE INDEX