Packet-Sniffer

Author: Vivo234

Description: This is a packet sniffer that can be used to capture and analyze network traffic.

Usage:

Install Python.
Save the code snippet in a file called `sniffer.py.`
Run the following command in the terminal: is a simple packet sniffer

```
python sniffer.py
```

The packet sniffer will start capturing packets. The packets will be printed to the console.
You can stop the packet sniffer by pressing Ctrl+C.
Options:

The sniffer can be configured to capture packets on a specific interface. To do this, specify the interface name when you run the sniffer. For example:

```
python sniffer.py eth0
```

The sniffer can be configured to capture a specific type of packet. To do this, use the -t option and specify the type of packet. For example:

```
python sniffer.py -t tcp
```

Output:

The sniffer will print the following information for each packet:

- The source and destination addresses
- The protocol
- The length of the packet
- The payload of the packet
- Limitations:

The sniffer can only capture packets that are sent or received on the local machine.
The sniffer cannot capture encrypted packets.

Disclaimer:

This sniffer is for educational purposes only. Do not use this sniffer to spy on other people or to violate their privacy.