PacketFilterX: Real-Time Packet Sniffer and Analyzer

A tool by - Akash Prasanna S

Introduction

PacketFilterX is an innovative, real-time packet sniffer and network analyzer designed to monitor, detect, and analyze network traffic for anomalies. Built using Python and the powerful Scapy library, this tool empowers cybersecurity professionals, network administrators, and enthusiasts to secure their networks by identifying potential threats such as port scanning, ARP spoofing, and abnormal packet behavior.

Why PacketFilterX?

PacketFilterX is more than just a packet sniffer—it is a proactive defense mechanism. It empowers users to safeguard their networks with minimal effort and maximum efficiency, making it a must-have tool in any cybersecurity arsenal.

The tool’s lightweight design and user-friendly interface make it accessible to beginners while retaining the advanced functionality required by professionals. With a focus on flexibility, users can define custom scanning durations and network interfaces, ensuring tailored monitoring to meet their unique needs. Moreover, the detailed logging system enhances accountability and simplifies post-event analysis, helping users stay ahead of evolving cybersecurity threats.

Unlike traditional packet sniffers, PacketFilterX focuses on anomaly detection by identifying suspicious activities such as port scanning, ARP spoofing, and unusual traffic patterns. These features help detect early signs of attacks like reconnaissance or man-in-the-middle (MITM) attempts. What sets PacketFilterX apart is its real-time feedback system, which categorizes packets as “good” or “bad,” enabling immediate action.

Features of PacketFilterX

- **Real-Time Packet Sniffing:**
  Monitors network traffic in real time, capturing detailed information about source, destination, and protocol.

- **Anomaly Detection:**
  Identifies suspicious activities such as port scanning, ARP spoofing, and abnormal packet behavior, flagging them for immediate attention.

- **Categorized Packet Status:**
  Differentiates between “Good” and “Bad” packets, allowing users to easily identify threats.

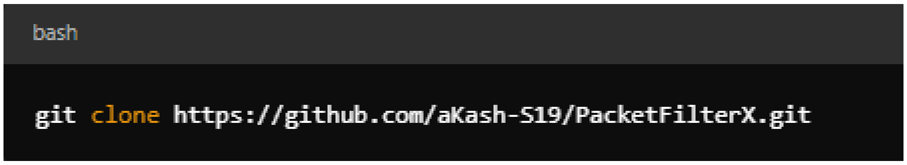
- **Comprehensive Logging System:**
  Records network activity and anomalies in a detailed log file for analysis and reporting.

- **Customizable Scans:**
  Allows users to specify the network interface and scan duration for targeted traffic monitoring.

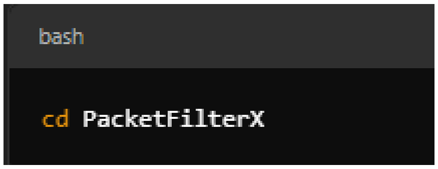
- **Lightweight and Flexible:**
  Designed to be fast and efficient, suitable for both beginners and professionals, with minimal setup requirements.

Installation Guide

I. Clone the Github repository to your computer.

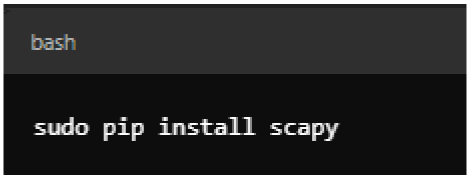


```bash
git clone https://github.com/aKash-S19/PacketFilterX.git
```



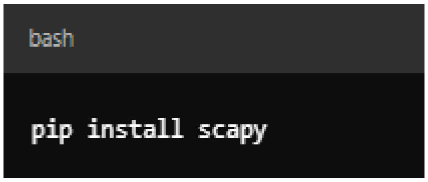
```bash
cd PacketFilterX
```

II. Install dependencies.



```bash
sudo pip install scapy
```

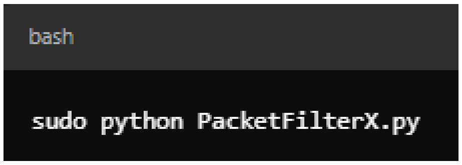
i)Linux



```bash
pip install scapy
```

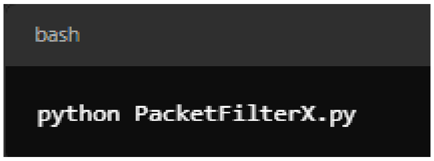
ii)Windows

III. Run PacketFilterX



```bash
sudo python PacketFilterX.py
```

i)Linux



```bash
python PacketFilterX.py
```

ii)Windows

IV. Start Scanning

- Select your network interface (e.g., `eth0`, `wlan0`).
- Specify the scanning duration.
- Analyze live results and logs generated during the process.

Conclusion

PacketFilterX is a modern, intuitive tool that brings simplicity and power to network security. With real-time monitoring, intelligent anomaly detection, and comprehensive logging, it empowers users to safeguard their networks effortlessly. Designed for professionals and enthusiasts alike, PacketFilterX is your go-to solution for staying ahead of threats in a fast-evolving digital landscape.

Acknowledgment

PacketFilterX is proudly developed by **Akash Prasanna S**, with the vision of simplifying network security for everyone. This project reflects a dedication to fostering secure online environments and advancing cybersecurity practices. Contributions and feedback are welcome on the GitHub repository: aKash-S19.