Vahid Ramezani

9722762359

I have chosen C as my project's programming language. C, without a doubt, is a powerful language hence it supports powerful libraries. It supports libpcap and there is no need for a libpcap wrapper. I have talked about the libraries used to code packet analyzing programs in the next section.

Packet sniffing

Packet sniffers are programs that intercept the network traffic flowing in and out of a system through network interfaces.

Therefore, if you are browsing the internet then traffic is flowing and a packet sniffer would be able to catch it in the form of packets and display them for whatever reasons required.

Sniffing includes utilizing sniffer tools that empower constant checking and investigation of packets flowing streaming over PC systems. It very well may be an equipment gadget, a separate software program, or a blend of both. It is likewise called as packet sniffing, snoop, packet analyzer, arrange analyzer, or convention analyzer.

Essentially, it looks at traffic on the system and takes preview duplicates of the bundle information. System sniffing is utilized for ethical just as deceptive purposes. System executives utilize these as system checking and analyzer tools to analyze and avoid organize related issues, for example, traffic bottlenecks. Digital lawbreakers utilize these as hacking devices to sniff, capture, and take private data, for example, client characters, passwords, login certifications, card subtleties, messages, texts, information, and furthermore for ridiculing information.

Packet sniffers are used for various needs like analyzing protocols, monitoring network, and assessing the security of a network.

Wireshark for example is the most popular packet sniffer out there and is available for all platforms. It is GUI based and very easy to use.

Packet sniffers can be coded by either using **SOCKETS** API provided by the kernel, or by using some packet capture library like **LIBPCAP**.

It is similar to as wiretapping to a telephone network. It is mostly used by *crackers and hackers* to collect information illegally about network. It is also used by *ISPs, advertisers and governments*.

ISPs use packet sniffing to track all your activities such as:

- who is receiver of your email
- what is content of that email
- what you download
- sites you visit
- what you looked on that website
- downloads from a site
- Streaming events like video, audio, etc.

Advertising agencies or internet advertising agencies are paid according to:

- Number of ads shown by them.
- Number of clicks on their ads also called PPC (pay per click).

To achieve this target, these agencies use packet sniffing to *inject advertisements* into the flowing packets. Most of the time these ads *contain malware*.

References

1- www.kaspersky.com

2- www.geeksforgeeks.org

3- www.hypr.com

4- www.binarytides.com

My git repo:
https://github.com/ConnorLynch2000/CN-project