COMPUTER NETWORKS
PROJECT – PHASE 0

Author : Soroosh Faal
Student ID: 9722762393

PACKET SNIFFING

What is Packet Sniffing?

Packet sniffing is a method of tapping each packet as it flows across the network; i.e., it is a technique in which a user sniffs data belonging to other users of the network. Packet sniffers can operate as an administrative tool or for malicious purposes. It depends on the user's intent. Network administrators use them for monitoring and validating network traffic. Packet sniffers are basically applications. They are programs used to read packets that travel across the network layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) layer. (Basically, the packets are retrieved from the network layer and the data is interpreted.) Packet sniffers are utilities that can be efficiently used for network administration. At the same time, it can also be used for nefarious activities. However, a user can employ a number of techniques to detect sniffers on the network and protect the data from sniffers. The technique behind packet sniffing on shared bus broadcast LANs is explained.

Is Packet Sniffing good or bad?

The Good use of it

Packet sniffing for business is an important part of maintaining a safe, efficient and reliable company network. Network administrators use packet sniffing as a diagnostic tool to perform tests on the network, monitor activity and troubleshoot any network problems. They will use commercial/professional packet-sniffing software and hardware devices to monitor the traffic on their network. They'll also use packet sniffing to help them detect if hackers have broken into their networks.

The bad use of it

Hackers, on the other hand, use packet-sniffing software (which is available free online!) to break into company networks and steal data. With it, they are virtually able to eavesdrop on any unencrypted information that's being exchanged between computers and traveling on a network. Let's be clear. Packet sniffers aren't reading our data for fun, they steal passwords, account numbers, Social Security Numbers and more. They're out to do steal money or ruin an organization's or individual's reputation. They also can learn intimate details about the networks they've invaded, and start to plan a bigger attack for the future.

PACKET ANALYZING

What is Packet Analyzing?

Packet analysis is a primary traceback technique in network forensics, which, providing that the packet details captured are sufficiently detailed, can play back even the entire network traffic for a particular point in time. This can be used to find traces of nefarious online behavior, data breaches, unauthorized website access, malware infection, and intrusion attempts, and to reconstruct image files, documents, email attachments, etc. sent over the network.

AVAILABLE LIBRARIES

Here are some C/C++ libraries for packet analyzing and generally network programming:

- Boost.Asio
- Asio is also available as a stand-alone library.
- ACE A bit more mature and has a couple of books to support it.
- C++ Network Library
- POCO
- Qt
- Raknet
- ZeroMQ (C++)
- nanomsg (C Library)
- nng (C Library)
- Berkeley Sockets
- libevent
- Apache APR
- yield
- Winsock2(Windows only)
- wvstreams
- zeroc
- libcurl
- libuv (Cross-platform C library)
- SFML's Network Module
- C++ Rest SDK (Casablanca)
- RCF
- Restbed (HTTP Asynchronous Framework)
- SedNL
- SDL_net
- OpenSplice|DDS
- facil.io (C, with optional HTTP and Websockets, Linux / BSD / macOS)
- GLib Networking
- grpc from Google
- GameNetworkingSockets from Valve
- CYSockets To do easy things in the easiest way

The selected language for this project will be C.

Network programming enables processes to communicate with each other over a computer network, but it is a complex task that requires programming with multiple libraries and protocols. With its support for third-party libraries and structured documentation, C is an ideal language to write network programs.

Besides, there is going to be extra marks for C.

Repository for project:

https://github.com/JuliusAndreas/NetworkingProject

Sources used:

- https://www.packtpub.com/product/hands-on-network-programming-with-c/9781789349863#:~:text=Network%20programming%20enables%20processes%20to,language%20to%20write%20network%20programs.
- https://medium.com/cyber-explorer/choosing-library-for-writing-a-network-packet-sniffer-a866ac915084
- https://www.sciencedirect.com/science/article/pii/S1742287619302002#:~:text=Packet%20analysis%20is%20a%20primary,a%20particular%20point%20in%20time.
- https://ieeexplore.ieee.org/document/1166620/authors#authors
- https://whatismyipaddress.com/packet-sniffing#:~:text=The%20good%20of%20it.,and%20troubleshoot%20any%20network%20problems.
- https://stackoverflow.com/questions/118945/best-c-c-network-library