Farzad Mehrabi
9913027109

Network programming basics

Preface:

Computer Networks has always been a diverse and dynamic area, and since the emergence of the Internet, its intricacies have been dramatically increased.

Although C , C++ and other low-level programming languages are still wildly used, and are considered as the backbone of many operating systems and infrastructures, they can be hard to work with, and tend to overcomplicate simple tasks. Therefore, I have chosen **python** which adheres a clear and simple syntax while providing an extensive number of libraries.

As this research is just a pre-phase for the Network programming project, it's assumed that an explicit description of inquired concepts will suffice.

Packet sniffing:

Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass through a computer network, regardless of how the packet is addressed. In this way, every packet, or a defined subset of packets, may be gathered for further analysis.

Packet analysis:

Packet analysis is a primary traceback technique in network forensics, which, providing that the captured packets are sufficiently detailed, can even play back 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.

Commonly used libraries:

PCAP:

PCAP (short for Packet Capture) is the name of the API commonly used to record packet metrics. PCAP files are especially helpful because they can record multilayer traffic data, capturing packets originating from the data link layer all the way to the application layer. PCAP has unique formats based on its operating system, the purpose and function of PCAP analysis remain the same across platforms.

Libpcap:

The Libpcap library allows developers to write code to receive link-layer packets (Layer 2 in the OSI model) on different flavors of UNIX operating systems without having to worry about the idiosyncrasy of different operating systems' network cards and drivers. Essentially, the Libpcap library grabs packets directly from the network cards, which allowed developers to write programs to decode, display, or log the packets.

Github https://github.com/Farzad-Mehrabi/Network_programming.git

Bibliography

Contributor, Dnsstaff: Staff. *pcap analysis*. 24 February 2021. 27 March 2021.

group, Paessler monitoring. *paessler packet-sniffing*. 2019. 27 March 2021.

Jay Beale, Jeffrey Posluns, James C. Foster, Brian Caswell. "Snort: The Inner Workings." *Snort Intrusion Detection 2.0*. Elsevier Inc, 2003. 93-139.

Sikos, Leslie F. "Packet analysis for network forensics: A comprehensive survey." *Forensic Science International: Digital Investigation* (2020): 13.