Abstract

Network security is a rapidly growing and is the major area of concern for every network. Firewalls are used as a security check point in network environment even then different types of security issues keep on emerging. In order to protect the network from illegal access, the concept of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) is been developed. An IDS is a system where the events occurring in a network is monitored and analyzed for identifying the sign of possible incidents. These incidents may either be violations or the threats that are about to happen violating the computer security policies or standard security policies. Java programming language is made use for developing the Intrusion Detection System. JPCap package is used along with winpcap for developing the traffic monitoring system. The network packets are captured online i.e., as they come across the interface of the network. The IDS is aimed to provide the preliminary level of detection techniques so as to secure the systems present in the networks.
Architecture for Real Time Monitoring and Modeling of Network Behavior for Enhanced Security

Index Terms

Computer Science

Security
Keywords

Firewalls  Intrusion Detection System (IDS)  Intrusion Prevention System (IPS)

Winpcap

Jpcap