Rule Based Intrusion Detection Frame Work

This part of the software sniffs the ip packets coming over the network and determines whether incoming connection is a intrusion or not. The dectection of the intrusion is done by comparing a set of parameters from the input connections with the predefined rule data base. Thus the name Rule based intrusion detection frame work. There are several files in this modules like hidesmain.c, packet\_processor.c, read\_processor.c ,std\_convert.c ,

In hides\_main.c ip the packets are sniffed from the network. This sniffing is a passive action such that the actual network traffic flows without any intervention. We are using a header file known as pcap.h for the packet capture purpose. each the packet is captured a programmer defined function named got\_packet is called. All the packet processing actions are defined in packet\_processor.c. each packet is analyzed such that the software will follow up different tcp connection going on the through the network. Here different parameters of each tcp connections are extracted like source ip address, destination ip ,souce port, destination port, duration , number bytes transferred.

All these parameters are convert to a standard format which defined in the file std\_convert.c . and these parameters in the standard format is written on to a file. Now these parameters are combined with the pre defined rule data base to check for an intrusion according to the signature given in the rule data base. These comprised in compare\_rules.c file. It includes many string manipulations. If a typical attack is determined then it is reported by means of a log file.