Data Normalization Plugins

The plugins are responsible for converting raw-data in any form to the uniform event format to be stored in the SQLite backend. Currently the plugin framework consists of two separate tools:

1. p2db- to convert packet raw data to events.
2. normalizer.py - to convert ascii raw data to events.

Available plugins

Note that more plugins will be added in due course of time and the plugin architecture will be improved. Also, more attributes may be added.

Plugin	Raw Data Input	Event Output	Event Attributes	Example event databases (SQLite)
p2db	pcap files	PACKET_TCP	sipaddr, dipaddr, sport, dport, totalpacketlen, protocol, tos, ipid, ipoffset, ipcksum, ipttl, tcpseq, tcpack, tcpflags	Example PACKET_TCP events
		PACKET_UDP	sipaddr, dipaddr, sport, dport, totalpacketlen, protocol, tos, ipid, ipoffset, ipcksum, ipttl, udplen, udpcksum	Example PACKET_UDP events
		PACKET_ICMP	sipaddr, dipaddr, sport, dport, totalpacketlen, protocol, tos, ipid, ipoffset, ipcksum, ipttl, icmptype, icmpcode, icmpcksum	
		PACKET_DNS	sipaddr, dipaddr, sport, dport, totalpacketlen, protocol, tos, ipid, ipoffset, ipcksum, ipttl, udplen, udpcksum, dnsid , dnsaa, dnsopcode, dnsqrflag, dnsnumques, dnsnumans, dnsnumadd, dnsnumauth, dnsquestype, dnsquesname, dnsquesclass, dnsansarec, dnsansns, dnsanscname, dnsauth , dnsaddarec, dnsaddns, dnsaddcname	Example PACKET_DNS events
		PACKET_IP	sipaddr, dipaddr, sport, dport, totalpacketlen, protocol, tos, ipid, ipoffset, ipcksum, ipttl	
syslog	Syslog files	SYSLOG	hostname,daemon, pid, charstring	
apache	Apache combined log	APACHE	sipaddr, identd, remoteuser, httpreq, httpstatus,contentlength, referrer, useragent	

bind	Syslog files	BINDDNSQUERY	hostname,daemon, pid, clientip, clientport, query, rrname, rrtype, options, nsname	
mysql	Mysql server logs	MYSQL	loglevel, charstring	
argus	Argus flow records output from *ra* tool.	ARGUS_FLOW	Click on the plugin name for details.	