Snort简介

Snort有三种工作模式：嗅探器、数据包记录器、网络入侵检测系统。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。数据包记录器模式把数据包记录到硬盘上。网络入侵检测模式是最复杂的，而且是可配置的。我们可以让snort分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的动作。

Snort能够对网络上的数据包进行抓包分析，但区别于其它嗅探器的是，它能根据所定义的规则进行响应及处理。Snort 通过对获取的数据包，进行各规则的分析后，根据规则链，可采取Activation（报警并启动另外一个动态规则链）、Dynamic（由其它的规则包调用）、Alert（报警），Pass（忽略），Log（不报警但记录网络流量）五种响应的机制。

Snort有数据包嗅探，数据包分析，数据包检测，响应处理等多种功能，每个模块实现不同的功能，各模块都是用插件的方式和Snort相结合，功能扩展方便。例如，预处理插件的功能就是在规则匹配误用检测之前运行，完成TIP碎片重组，http解码，telnet解码等功能，处理插件完成检查协议各字段，关闭连接，攻击响应等功能，输出插件将得理后的各种情况以日志或警告的方式输出。