Applying packet generator for secure network environment

ABSTRACT

Problem statement: Viruses and hacker attacks typically generate a recognizable pattern or "signature" of packets. Most of Network Traffic Analyzer can identify these packets and alert the administrator to their presence on the network via email or page. Approach: Most traffics analyzers let you set alarms to be triggered when a particular pattern is seen. Results: Some network traffic analyzers can be programmed to send an email or page when these conditions are met. Of course; this assumes that the virus and its signature have been seen before and incorporated the analyzer's list of packet filters. ((The packet filters once started the filtering process and also by using packet decode together they can determine the traffic type whether it has normal or abnormal activities. Conclusion/Recommendations: In this study we used Packet Generator to generate a traffic that supposes to act the intruder or hacker signature to prove up that Network Traffic Analysis has the ability to detect like this kind of traffics. And also we have explained in depth about network traffic analysis and its ability to monitor all the network traffics (incoming and outgoing) and view their headers and payload and all other information such as traffic source and destination)).

Keyword: Attacks signatures; Filter traffics; Network security; Network traffic analysis; Packet generator; Packets decode; Security and forensics; Virus