Assignment No. 4 B

snort intrusion detection package

Problem Statement :

Use the snort intrusion detection package to analyze traffic and create a signature to identify problem traffic.

Theory:

Snort

Snort is an open source network intrusion detection system created Sourcefire founder and former CTO Martin Roesch. Cisco now develops and maintains Snort. Snort is referred to as a packet sniffer that monitors network traffic, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. Long a leader among enterprise intrusion prevention and detection tools, users can compile Snort on most Linux operating systems (OSes) or Unix. A version is also available for Windows.

Snort is based on library packet capture (libpcap). Libpcap is a tool that is widely used in Transmission Control Protocol/Internet Protocol address traffic sniffers, content searching and analyzers for packet logging, real-time traffic analysis, protocol analysis and content matching. Users can configure Snort as a sniffer, packet logger -- like TCPdump or Wireshark -- or network intrusion prevention method.

Intrusion prevention system mode

As an open source network intrusion prevention system, Snort will monitor network traffic and compare it against a user-defined Snort rule set -- the file would be labeled snort.conf. This is Snort's most important function.Snort applies rules to monitored traffic and issues alerts when it detects certain kinds of questionable activity on the network. It can identify cybersecurity attack methods, including OS fingerprinting, denial of service, buffer overflow, common gateway interface attacks, stealth port scans and Server Message Block probes. When Snort detects suspicious behavior, it acts as a firewall and sends a real-time alert to Syslog, to a separate alerts file or through a pop-up window.

Packet logger and sniffer mode

If a subscriber configures Snort to operate as a sniffer, it will scan network packets and identify them. Snort can also log those packets to a disk file. To use Snort as a packet sniffer, users set the host's network interface to promiscuous mode to monitor all network traffic on the local network interface. It then writes the monitored traffic to its console. By writing desired network traffic to a disk file, Snort logs packets.

Conclusion – SNORT is a network based intrusion detection system. Snort is real-time traffic monitor, Packet logging tool. It is also used for analysis of protocol.