Session 07 – Snort Wei Cui

Snort is an open-source network intrusion prevention system (IPS) by Cisco. It can perform real-time traffic analysis and packet logging on IP networks. These services have lots of applications including application-aware triggered quality of service (AATQoS), to de-prioritize bulk traffic when latency-sensitive applications are in use. Snort can conduct protocol analysis, content searching and matching, and detect various attacks and probes. Snort can be utilized as a packet logger (useful for network traffic debugging), or as a full-blown IPS for network.

Snort can be configured in three main modes[1]: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified. [2]

Reference:

[1]. www.snort.org

[2]. snort – Wikipedia https://en.wikipedia.org/wiki/Snort\_(software), last accessed: 9/8/2017