Name – Jay S. Chatpalliwar

PRN -21510018

Assignment no 12

Snort : **Snort** is a [free](https://en.wikipedia.org/wiki/Free_software) [open source](https://en.wikipedia.org/wiki/Open_source_software) network intrusion detection system (IDS) and intrusion prevention system (IPS)

Snort's open-source network-based [intrusion detection/prevention system](https://en.wikipedia.org/wiki/Intrusion_prevention_system) (IDS/IPS) has the ability to perform real-time traffic analysis and [packet logging](https://en.wikipedia.org/wiki/Packet_analyzer) on [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) networks. Snort performs protocol analysis, content searching and matching.

The program can also be used to detect probes or [attacks](https://en.wikipedia.org/wiki/Attack_(computing)), including, but not limited to, [operating system fingerprinting](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting) attempts, [semantic URL attacks](https://en.wikipedia.org/wiki/Semantic_URL_attack), [buffer overflows](https://en.wikipedia.org/wiki/Buffer_overflow), [server message block](https://en.wikipedia.org/wiki/Server_message_block) probes, and stealth [port scans](https://en.wikipedia.org/wiki/Port_scanner).[[11]](https://en.wikipedia.org/wiki/Snort_%28software%29#cite_note-11)

Snort can be configured in three main modes: 1. sniffer, 2. packet logger, and 3. network intrusion detection.[[12]](https://en.wikipedia.org/wiki/Snort_%28software%29#cite_note-12)

**Sniffer Mode**

[[edit](https://en.wikipedia.org/w/index.php?title=Snort_(software)&action=edit&section=2)]

The program will read network packets and display them on the console.

**Packet Logger Mode**

[[edit](https://en.wikipedia.org/w/index.php?title=Snort_(software)&action=edit&section=3)]

In packet logger mode, the program will log packets to the disk.

**Network Intrusion Detection System Mode**

[[edit](https://en.wikipedia.org/w/index.php?title=Snort_(software)&action=edit&section=4)]

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.[[13]](https://en.wikipedia.org/wiki/Snort_%28software%29#cite_note-13)











