### 1. Describe how Snort uses rules to detect malicious activity.

Snort capture network traffic and breaks it down into packets. Each packet is compared to the rule set and if a packet matches a rule, Snort triggers the specified action (e.g logging, alerting, dropping, blocking the packet). Each rule define a set of conditions that Snort uses to inspect packets. These conditions include various attributes such as protocol, source and destination IP addresses, ports, and payload data.

### 2. Mention at least 6 limitations of signature-based intrusion detection systems like Snort with a small description for each one.

* **Known signatures**: Signature-based systems can only detect attacks that matches predefined rulea. They cannot detect new, unknown threats or variations of known attacks.
* **High false positives**: Non-malware packets can trigger alerts if they match a rule’s pattern.
* **High false negatives**: Slightly modified payload can bypass detection. Snort fails to detect.
* **Encrypted Traffic**: Snort cannot inspect the content of encrypted traffic (e.g HTTPS) Malicious activities within these cannot be detected.
* **Low performance**: Searching in a large database of rules can lead to high CPU and memory usage, causing system’s low performance.
* **Static rules**: Rules are static, so they cannot understand the behaviour of previus attacks and adapt dynamically. There is a need of continuous manually updating the rules database.

### 3. Pros and cons of using Snort in a real-world scenario.

#### Pros:

* Snort is free and open source.
* Anyone can write custom rules and as a result snort can adapt in the need of any use-case (Customizability).
* Widely used and a result it has a big community suport, documentation online etc.
* Compatibility with any OS.
* Multiple functionalities in a single tool. (logger, sniffer, IDS etc).

#### Cons:

All these maintioned above about signature-based IDS are Cons of using snort in a real-world scenario.

* To minimize high false negatives and positives, continuous updating and ‘tuning’ of rules is required.
* Writting custom rules, analyze logs and keep up to date need manual expertise.

In conclusion, Snort is a powerful tool with some serius limitations. So as to ensure the maximum protection, real-world scenarios must combine snort with other security measures.