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

Snort detects malicious activity by checking every incoming packet for user assigned rules. Each rule consists of a header and an options portion. The header checks specific src/dst ips and ports that match the common malicious packets. This detection is further improved by using the options which keep track and filter based on network flow states sand the packet payloads (malicious packets signatures).

(maybe add about snort modes)

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

* Malicious actors can often produce variants of known threats which can go undetected.
* Needs to be constantly manually maintained by administrators to keep up to date with current threats.
* In certain cases, is limited to only header monitoring when dealing with encrypted packets.
* Cannot detect new threats only known ones.
* A badly maintained signature database can raise the false-positive rate (due to overlaps).
* Performance issues with increasing size.

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

Pros:

* Efficient for real time analysis of a large stream of packets.
* Quickly identifies known threats, providing a reliable buffer for unsophisticated/copycat attacks.
* Low false-positive rate, signature matching is reliable.

Cons:

* Can be often bypassed by producing malicious packet variants.
* Needs constant manual updating of the database.
* Overlapping snort rules can cause issues when database size increases.