Theoretical Questions

1. Snort uses a rule-based approach to detect malicious activity by analyzing network traffic against predefined rules. Each rule has 2 parts. Firstly, the header, which specifies the action (alert, log, etc.), protocol, source/destination IPs, and ports. Secondly, the options which contain detailed matching criteria, such as payload patterns or protocol behaviors.

More specifically it works as following. Firstly, snort decodes packets to understand their structure. Secondly, It checks the packet against the rule header, then evaluates options like content or metadata. Finally, If a match is found, Snort performs the specified action (e.g., alert, log, drop).

2.

* Can’t spot new attacks: These systems only catch threats they already know about. If hackers create a brand-new attack, it slips through unnoticed.
* Misses cleverly disguised attacks: If attackers tweak a known threat—like encrypting it or slightly altering its behavior—the system might not recognize it, letting the attack go undetected.
* Struggles with heavy traffic: The more rules it has to check, the slower it gets. In busy networks, it can become a bottleneck, struggling to keep up with all the traffic.
* Needs Constant Updates: Someone has to keep feeding it new rules to catch the latest threats. If the rules aren’t updated regularly, the system becomes outdated and less effective.
* Lacks Big-Picture Awareness: It looks at each packet individually, without connecting the dots to see if it’s part of a larger, ongoing attack or a more sophisticated strategy.
* Too Many False Alarms: It often flags harmless activities as threats, leading to "alert fatigue." This makes it harder for security teams to focus on real problems.

3. Snort is a budget-friendly choice since it’s open-source and free, making it accessible even for smaller organizations. Moreover, It’s highly flexible, letting you create custom rules to fit your network’s specific needs. Furthermore, with a strong community and regular updates, you can stay ahead of emerging threats. Snort is also versatile, working as both an intrusion detection (IDS) and prevention system (IPS). Finally, it’s lightweight enough to run on modest hardware, which is great for smaller networks without heavy infrastructure.

On the downside, Snort relies on known signatures, so it can’t detect brand-new or unknown threats. Secondly, It tends to flag a lot of false positives, which can overwhelm your team and make it hard to focus on real issues. In addition, keeping Snort effective takes effort—it needs frequent updates and skilled hands to maintain. Also, in busy networks, it can slow down as it processes a large number of rules. Lastly, Snort looks at packets in isolation, so it might miss more complex, multi-step attacks that require context to identify.