Theoretical Questions

1. How Snort Uses Rules to Detect Malicious Activity

Snort uses a set of predefined or custom rules to analyze network traffic and detect malicious activity. It captures packets in real-time, processes them through decoders and preprocessors, and checks if they match any rule. If a match is found, Snort generates an alert or logs the event. Rules specify the protocol, source/destination IP, ports, and packet content to look for malicious patterns.

2. Limitations of Signature-Based IDS like Snort

- Can’t catch new or unknown attacks without matching signatures.
- Can’t inspect the contents of encrypted packets.
- Legitimate traffic may trigger rules, creating unnecessary alerts.
- Struggles with high traffic or large rule sets, causing delays or missed packets.
- Doesn’t analyze multi-step attacks or user behavior.

3. Pros and Cons of Using Snort in Real-World Scenarios

Pros

- Free and Open-Source
- Customizable
- Real-Time Alerts

Cons

- Limited Against New Threats
- Resource-Heavy
- False Positives
- Encrypted Traffic Issues