1. What is port scanning?

Port scanning is the process of systematically scanning a computer or network for open ports. (Endpoints that applications use for communication)

1. What is Intrusion Detection?

Intrusion detection is a security mechanism designed to detect unauthorized access or suspicious activities within a computer network or system.

1. Why is port scanning a threat to an organisation?

Because it may highlight possible weaknesses in their network's architecture. Attackers may be able to obtain information about the services and programmes that are operating on a system, opening the door to potential exploitation or unauthorised access.

1. Did Snort detect the tunnelling of telnet through port 80?

It detects the commands but doesn’t detect once the connection is established.

1. How should an organisation deal with port scanning in its security policy?

- Prohibition: Make it very clear that accessing the organization's network or systems without authorisation is not permitted at all.

- Monitoring: Use intrusion detection systems (IDS) or intrusion prevention systems (IPS) to continuously monitor network traffic for indications of port scanning activity.

- Access Controls: Implement access controls to restrict authorised personnel's ability to scan ports for legitimate security testing purposes and to limit access to network resources.

1. What might be some of the limitations of an Intrusion Detection System such as Snort?

- False Positives: An excessive number of false positives can result from IDS raising alarms for harmless activity.

- Encrypted Traffic: IDS's capacity to identify threats within encrypted communications may be limited by its inability to inspect encrypted traffic.

- Zero-Day Attacks: Because intrusion detection systems (IDS) rely on signature-based detection, they are powerless against zero-day attacks and other unknown threats unless they are paired with behaviour-based detection methods.