**Cybersecurity 401**

**Module 3 - Security Operations**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **Read 14 - Intrusion Detection and Prevention Systems (IDS/IPS)**



**| Rodrigo Brasil 11/2023 |**

Questions

1. **List 2 differences between firewalls and an IDS?**
   1. Their purpose, firewalls act as a barrier between the internet and a LAN by looking at the traffic and controlling what comes inside the network. An IDS only looks at the traffic and responds if there is a threat in the network.
2. **Under what circumstances would you choose a network-based IDS over a host-based IDS?**
   1. A NIDS is used for monitoring network traffic and detecting suspicious patterns or anomalies while a HIDS is used to monitor a individual host
3. **Name 3 major drawbacks of a NIDS?**
   1. False Positives Are Frequent
   2. IP Packets Can Be Faked
   3. Does Not Process Encrypted Packets