### **Part 3: IDS, IPS, DiD, and Firewalls**

Now, we will work on another lab. Before you start, complete the following review questions.

#### **IDS vs. IPS Systems**

1. Name and define two ways an IDS connects to a network.  
   Answer 1: Network TAP (Test Access Port)  
   Answer 2: SPAN (Switched Port Analyzer)
2. Describe how an IPS connects to a network.  
   Answer: Inline with the flow of data, typically between the firewall and network switch.
3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?  
   Answer: Signature-based
4. Which type of IDS is beneficial for detecting all suspicious traffic that deviates from the well-known baseline and is excellent at detecting when an attacker probes or sweeps a network?  
   Answer: Anomaly-based

#### **Defense in Depth**

1. For each of the following scenarios, provide the layer of Defense in Depth that applies:
   1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.  
      Answer: Perimiter / Physical
   2. A zero-day goes undetected by antivirus software.  
      Answer: Application
   3. A criminal successfully gains access to HR’s database.  
      Answer: Data
   4. A criminal hacker exploits a vulnerability within an operating system.  
      Answer: Endpoint
   5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.  
      Answer: Network
   6. Data is classified at the wrong classification level.  
      Answer: Policy-Management
   7. A state-sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.  
      Answer: Perimiter
2. Name one method of protecting data-at-rest from being readable on a hard drive.  
   Answer: Hard Drive Encryption
3. Name one method to protect data-in-transit.  
   Answer: TLS (Transport Layer Security)
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop?  
   Answer: Geo-tracking
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
   Answer: Secure-boot or a password in the BIOS / UEFI

#### 

#### **Firewall Architectures and Methodologies**

1. Which type of firewall verifies the three-way TCP handshake? TCP handshake checks are designed to ensure that session packets are from legitimate sources.

Answer: Packet-Filtering Firewall (Stateful)

1. Which type of firewall considers the connection as a whole? This means, that instead of looking at only individual packets, these firewalls look at whole streams of packets at one time.

Answer: Packet-Filtering Firewall (Stateful)

1. Which type of firewall intercepts all traffic prior to being forwarded to its final destination. In a sense, do these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it?

Answer: Application (Proxy) Firewall

1. Which type of firewall examines data within a packet as it progresses through a network interface by examining the source and destination IP address, port number, and packet type- all without opening the packet to inspect its contents?

Answer: Packet-Filtering Firewall (Stateless)

1. Which type of firewall filters are based solely on the source and destination MAC address?

Answer: MAC-layer Firewall