Certified Network Defender Practice Test Questions and Answers

1. Which tool is most effective for detecting network intrusions in real-time?

A) Packet sniffer only

B) Intrusion Detection System (IDS) with behavioral analysis

C) Basic firewall logs

D) Manual network monitoring

2. What is the primary difference between a signature-based and anomaly-based detection system?

A) Cost and implementation complexity

B) Signature-based detects known threats, anomaly-based detects unusual behavior patterns

C) Hardware requirements

D) Network speed compatibility

3. Which technique is most effective for preventing DDoS attacks?

A) Installing antivirus software only

B) Rate limiting, traffic filtering, and distributed mitigation services

C) Changing network passwords frequently

D) Using only wireless connections

4. What should be the first step when responding to a confirmed network security incident?

A) Immediately shut down all systems

B) Contain the threat while preserving evidence and maintaining business operations

C) Delete all suspicious files

D) Change all user passwords

Answers: 1-B 2-B 3-B 4-B