GCIA Practice Test Questions and Answers

1. What does GCIA certification primarily focus on?

A) Network penetration testing

B) Intrusion detection and incident analysis

C) Digital forensics investigation

D) Vulnerability assessment

2. Which protocol is commonly used for network intrusion detection systems (NIDS) to capture packets?

A) SNMP

B) PCAP

C) ICMP

D) DHCP

3. In network security analysis, what does the term "false positive" refer to?

A) An attack that goes undetected

B) An alert generated for legitimate network activity

C) A successful intrusion attempt

D) A misconfigured security device

4. Which TCP flag combination is typically associated with a port scan?

A) SYN and ACK

B) SYN only

C) FIN, URG, and PSH

D) RST and ACK

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