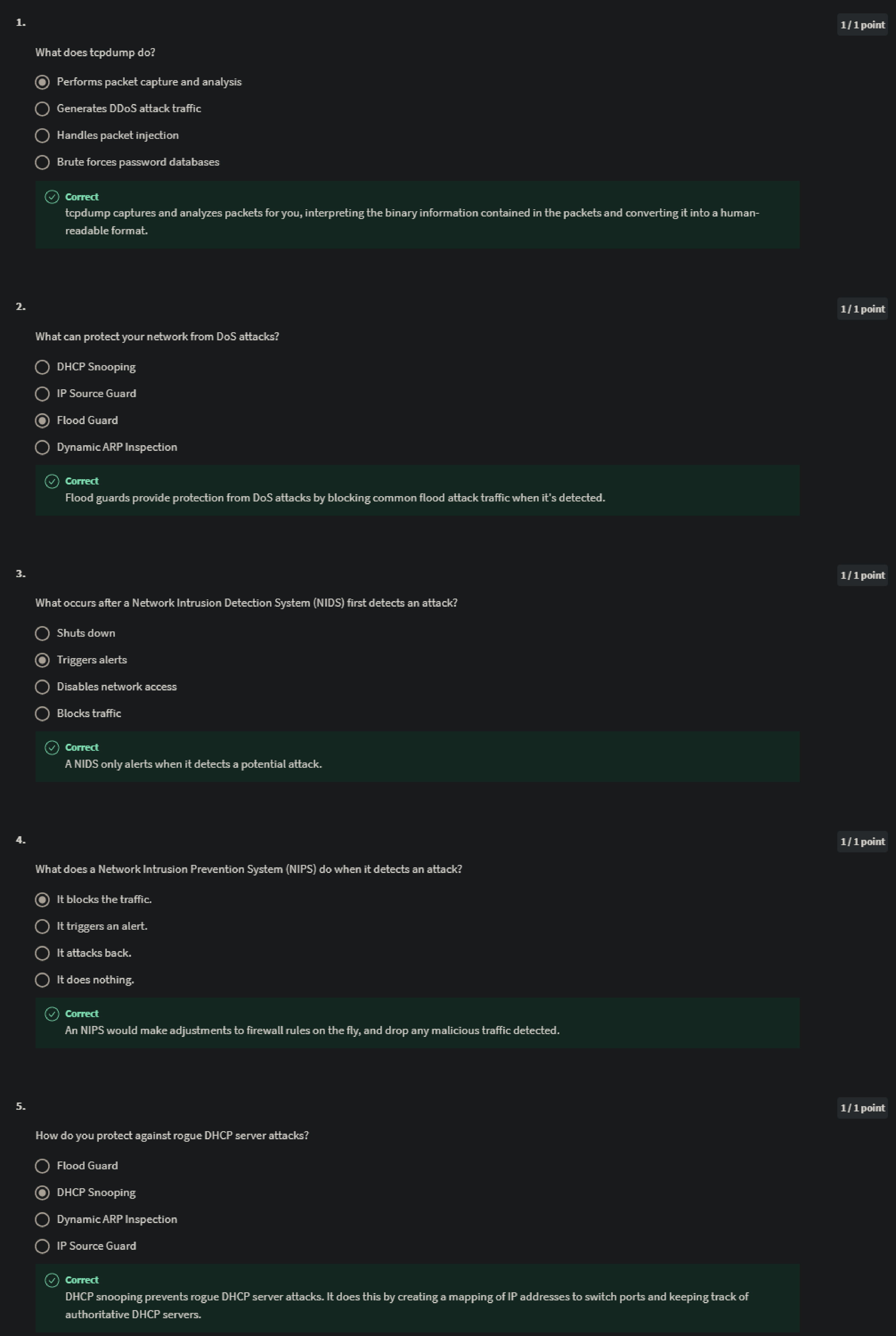

1.

1 / 1 point

What does tcpdump do?

● Performs packet capture and analysis

○ Generates DDoS attack traffic

○ Handles packet injection

○ Brute forces password databases

✓ **Correct**

tcpdump captures and analyzes packets for you, interpreting the binary information contained in the packets and converting it into a human-readable format.

2.

1 / 1 point

What can protect your network from DoS attacks?

○ DHCP Snooping

○ IP Source Guard

● Flood Guard

○ Dynamic ARP Inspection

✓ **Correct**

Flood guards provide protection from DoS attacks by blocking common flood attack traffic when it's detected.

3.

1 / 1 point

What occurs after a Network Intrusion Detection System (NIDS) first detects an attack?

○ Shuts down

● Triggers alerts

○ Disables network access

○ Blocks traffic

✓ **Correct**

A NIDS only alerts when it detects a potential attack.

4.

1 / 1 point

What does a Network Intrusion Prevention System (NIPS) do when it detects an attack?

● It blocks the traffic.

○ It triggers an alert.

○ It attacks back.

○ It does nothing.

✓ **Correct**

An NIPS would make adjustments to firewall rules on the fly, and drop any malicious traffic detected.

5.

1 / 1 point

How do you protect against rogue DHCP server attacks?

○ Flood Guard

● DHCP Snooping

○ Dynamic ARP Inspection

○ IP Source Guard

✓ **Correct**

DHCP snooping prevents rogue DHCP server attacks. It does this by creating a mapping of IP addresses to switch ports and keeping track of authoritative DHCP servers.

6. 1 / 1 point

What underlying symmetric encryption cipher does WEP use?

○ DES

● RC4

○ RSA

○ AES

✓ **Correct**
WEP uses the RC4 stream cipher.

7. 1 / 1 point

What traffic would an implicit deny firewall rule block?

● Everything that is not explicitly permitted or allowed

○ Nothing unless blocked

○ Outbound traffic only

○ Inbound traffic only

✓ **Correct**
Implicit deny means that everything is blocked, unless it's explicitly allowed.

8. 1 / 1 point

What allows you to take all packets from a specified port, port range, or an entire VLAN and mirror the packets to a specified switch port?

○ Network hub

● Port Mirroring

○ Promiscuous Mode

○ DHCP Snooping

✓ **Correct**
Port mirroring allows you to capture traffic on a switch port transparently, by sending a copy of traffic on the port to another port of your choosing.

9. 1 / 1 point

What kind of attack does IP Source Guard (IPSG) protect against?

○ Rogue DHCP Server attacks

● IP Spoofing attacks

○ DoS attacks

○ ARP Man-in-the-middle attacks

✓ **Correct**
IP Source Guard protects against IP spoofing. It does this by dynamically generating ACLs for each switch port, only permitting traffic for the mapped IP address for that port.

10. 1 / 1 point

What can be configured to allow secure remote connections to web applications without requiring a VPN?

○ NIDS

● Reverse proxy

○ RC4

○ Web browser

✓ **Correct**
A reverse proxy can be used to allow remote access into a network.