

AP Cybersecurity

Name: _____ Score: _____

1. An adversary secretly sitting between two parties, reading their traffic, performs a(n)..
 - ☐ DoS attack
 - ☐ phishing
 - ☐ brute force
 - ☐ on-path (man-in-the-middle) attack
2. Which is the strongest current wireless encryption?
 - ☐ HTTP
 - ☐ WPA
 - ☐ WPA3
 - ☐ WEP
3. A DMZ (screened subnet) typically holds..
 - ☐ nothing at all
 - ☐ public-facing servers
 - ☐ employee laptops
 - ☐ the most secret internal data
4. In a firewall ACL, which rule is applied to a packet?
 - ☐ All rules at once
 - ☐ A random rule
 - ☐ The first matching rule
 - ☐ The last rule
5. Which system detects an attack and raises an alert but does NOT block it?
 - ☐ VPN
 - ☐ UPS
 - ☐ NIPS
 - ☐ NIDS
6. When many machines flood a target at once, it is a distributed denial of service (DDoS).
 - ☐ True ☐ False

7. WEP is a safe choice for a modern secure wireless network.
- ☐ True ☐ False
8. VLANs can logically separate devices that share the same physical switch.
- ☐ True ☐ False
9. If an ALLOW rule appears below a DENY rule for the same traffic, the traffic is allowed.
- ☐ True ☐ False
10. Signature-based detection reliably catches brand-new attacks with no known signature.
- ☐ True ☐ False

AP Cybersecurity

1. **on-path (man-in-the-middle) attack**

This is an **on-path** / man-in-the-middle attack.

2. **WPA3**

WPA3 is today's strongest.

3. **public-facing servers**

A **DMZ** holds public-facing servers.

4. **The first matching rule**

The **first matching** rule wins.

5. **NIDS**

A **NIDS** alerts only; a **NIPS** can block.

6. **True**

Many attackers at once = **DDoS**.

7. **False**

WEP is broken; use **WPA3**.

8. **True**

VLANS separate devices logically.

9. **False**

False. Firewall rules are checked top-down and the first match wins, so the DENY above fires first and the traffic is blocked.

10. **False**

False. Signature-based detection is fast with few false positives, but it misses attacks with no known signature; anomaly-based detection is needed for those.