

3. Securing Networks

Starter Quiz · 课前小测

AP Cybersecurity

Name: _____ Score: _____

1. An adversary secretly sitting between two parties, reading their traffic, performs a(n)...

- ☐ DoS attack
- ☐ on-path (man-in-the-middle) attack
- ☐ brute force
- ☐ phishing

2. Which is the strongest current wireless encryption?

- ☐ WEP
- ☐ WPA
- ☐ WPA3
- ☐ HTTP

3. A DMZ (screened subnet) typically holds...

- ☐ the most secret internal data
- ☐ public-facing servers
- ☐ nothing at all
- ☐ employee laptops

4. In a firewall ACL, which rule is applied to a packet?

- ☐ The last rule
- ☐ The first matching rule
- ☐ A random rule
- ☐ All rules at once

5. Which system detects an attack and raises an alert but does NOT block it?

- ☐ NIPS
- ☐ NIDS
- ☐ VPN
- ☐ UPS

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. Placing a DENY rule above an ALLOW rule for the same traffic blocks that traffic.

- ☐ True
- ☐ False

10. Signature-based detection is fast and has few false positives.

- ☐ 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. **True**

First match wins — the **DENY** fires first.

10. **True**

But it misses attacks with no known signature.