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

   ☐ denial-of-service (DoS) attack

   ☐ phishing email attack

   ☐ brute-force password attack

   ☐ on-path (man-in-the-middle) attack

2. Which is the strongest current wireless encryption?

   ☐ HTTP

   ☐ WPA

   ☐ WPA3

   ☐ WEP

3. How did the Target attackers first get into the network?

   ☐ By breaking into a store

   ☐ Through a customer's phone

   ☐ By guessing the CEO's password

   ☐ Through a heating and air-conditioning contractor's login

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. What first made Stoll suspicious?

   ☐ A ransom note

   ☐ A broken window

   ☐ A 75-cent accounting error

   ☐ A slow website

6. When many machines flood a target at once, it is a distributed denial of service (DDoS).

   ☐ True ☐ False

exercises.lol exercises.com.cn

☐ True ☐ False

8. In a flat network, one infected device can reach every other device.

   ☐ 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 can miss brand-new attacks.

    ☐ True ☐ False

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. **Through a heating and air-conditioning contractor's login**

   A third-party account.

4. **The first matching rule**

   The **first matching** rule wins.

5. **A 75-cent accounting error**

   A small anomaly.

6. **True**

   Many attackers at once = **DDoS**.

7. **False**

   WEP is broken; use **WPA3**.

8. **True**

   Nothing contains it.

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. **True**

    No signature exists yet.