1. How did Mirai take over devices?

   ☐ By trying factory-default usernames and passwords

   ☐ By stealing them from shops

   ☐ By breaking their cases

   ☐ By sending postal letters

2. A cryptographic hash output is...

   ☐ always longer than the input

   ☐ variable length

   ☐ the original password

   ☐ a fixed length regardless of input

3. Microsoft's patch came out on 14 March 2017 and WannaCry spread on 12 May 2017. About how many days apart is that? (March has 31 days, April 30.)

   _____

4. Evidence in a log that an adversary has compromised a device is an...

   ☐ ACL (access control list)

   ☐ ISP (Internet service provider)

   ☐ SSID (service set identifier)

   ☐ IoC (indicator of compromise)

5. Which is an embedded computer?

   ☐ A desktop PC

   ☐ The controller in a smart thermostat

   ☐ A gaming laptop

   ☐ A web server

6. Trying one common password against many accounts is...

   ☐ salting

   ☐ credential stuffing

   ☐ a rainbow table

   ☐ password spraying



exercises.lol exercises.com.cn

   ☐ True ☐ False

8. Offline password attacks set off lockout alarms on your login server.

   ☐ True ☐ False

9. Which are device vulnerabilities?

   ☐ Default passwords

   ☐ A long, unique password

   ☐ Unpatched software

   ☐ Unnecessary open services

   *Tick every correct option.*

10. Salt makes two identical passwords produce the same stored hash.

    ☐ True ☐ False

1. **By trying factory-default usernames and passwords**

   About 60 default logins.

2. **a fixed length regardless of input**

   A hash is **fixed-length** and one-way.

3. **59**

   17 + 30 + 12 = 59 days.

4. **IoC (indicator of compromise)**

   An **IoC** is an indicator of compromise.

5. **The controller in a smart thermostat**

   Built in to do one job.

6. **password spraying**

   **Password spraying** = one password, many users.

7. **True**

   New malware appears every day.

8. **False**

   False. Offline cracking happens on the adversary's own machine against a stolen hash file, so your systems see no failed logins to detect.

9. **Default passwords; Unpatched software; Unnecessary open services**

   A strong password is a protection.

10. **False**

    False. A unique salt per user changes each hash, so identical passwords produce different stored hashes and precomputed tables do not work.



exercises.lol exercises.com.cn