

4. Securing Devices

Starter Quiz · 课前小测

AP Cybersecurity

Name: _____ Score: _____

1. Which malware spreads WITHOUT any user action?
 - ☐ Virus
 - ☐ Worm
 - ☐ Trojan
 - ☐ Spyware
2. A cryptographic hash output is...
 - ☐ variable length
 - ☐ a fixed length regardless of input
 - ☐ always longer than the input
 - ☐ the original password
3. Why does keeping software updated make a device safer?
 - ☐ It makes the screen brighter
 - ☐ Patches close known vulnerabilities
 - ☐ It deletes all files
 - ☐ It adds a camera
4. Evidence in a log that an adversary has compromised a device is an...
 - ☐ IoC (indicator of compromise)
 - ☐ ISP
 - ☐ SSID
 - ☐ ACL
5. Malware that encrypts your files and demands payment is...
 - ☐ spyware
 - ☐ ransomware
 - ☐ a rootkit
 - ☐ a worm
6. An internet-connected thermostat is an example of an IoT device.
 - ☐ True
 - ☐ False

7. Salt makes two identical passwords produce different stored hashes.
 - ☐ True
 - ☐ False

8. Anti-malware software uses a database of signatures to spot malicious files.

☐ True ☐ False

9. Offline password attacks generally cannot be detected on your systems.

☐ True ☐ False

10. Software with no recent security update installed is called _____ software.

AP Cybersecurity

1. **Worm**

A **worm** self-spreads; a **virus** needs a user.

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

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

3. **Patches close known vulnerabilities**

A **patch** closes a known hole.

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

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

5. **ransomware**

Ransomware encrypts for money.

6. **True**

Everyday embedded devices are **IoT**.

7. **True**

Unique **salt** per user changes each hash.

8. **True**

It quarantines files matching a **signature**.

9. **True**

The cracking happens on the adversary's own machine.

10. **unpatched**

Unpatched software has open, known holes.