

AP Cybersecurity

Name: _____ Score: _____

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

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

☐ True ☐ False

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

☐ True ☐ False

9. An internet-connected thermostat is an example of an IoT device.

☐ True ☐ False

10. Using two or more authentication factors is called _____.

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. **False**

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

7. **True**

It quarantines files matching a **signature**.

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. **True**

Everyday embedded devices are **IoT**.

10. **MFA**

MFA combines factors for stronger security.