Week 18

AP Cybersecurity

Homework bundle for this week

本周作业合集

exercises.lol

Contents 目录

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.

    _____

4. Securing Devices

Answers · 答案

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.

AP CYBERSECURITY • EXERCISE SHEET

4.1 Device Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

KEY WORDS malware 恶意软件 • virus 病毒 • worm 蠕虫 • iot 物联网 • ransomware 勒索软件

Objective

Build the skills to answer exam questions on device types and **malware** 恶意软件.

You must be able to:

- identify types of device, including **IoT** 物联网 devices
- name malware by its behaviour (virus, worm, ransomware, RAT, rootkit)
- rate device risk high, moderate, or low

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Naming malware

A virus needs a user to run a file. A worm spreads by itself. Ransomware encrypts files for money. A remote access trojan (RAT) gives remote control. A rootkit hides deep in the OS.

■ Rating device risk

High = an unpatched critical device (e.g. a hospital server). Low = a low-value device with an unused open port. The value and criticality of the device set the level.

2 Practice

2.1 State the key difference between a virus and a worm. [2]

2.2 Name the malware that encrypts a victim's files and demands payment. [1]

2.3 An organisation has not applied a critical security update to its email server.

(a) State the risk level. [1]

(b) Justify your answer. [1]

3 Exam-style questions

3.1 Which malware spreads across a network WITHOUT any user action? [1]

- **A** virus
- **B** worm
- **C** trojan
- **D** spyware

3.2 An internet-connected thermostat is an example of a(n) [1]

- **A** server
- **B** IoT device
- **C** mainframe
- **D** firewall

3.3 Malware on a device gives an adversary full remote control of it.

(a) Name the type of malware. [1]

(b) State one action the adversary could then take. [1]

Solutions

2.1 a virus needs a user to open/run a file; a worm spreads by itself with no human action.

2.2 ransomware.

2.3 (a) high. (b) an unpatched critical service can be exploited with serious impact.

3.1 B. a worm self-spreads; a virus needs a user.

3.2 B. everyday embedded connected devices are IoT devices.

3.3 (a) a remote access trojan (RAT). (b) e.g. steal files, watch the user, or use it as a foothold.

AP CYBERSECURITY • EXERCISE SHEET

4.2 Authentication

Name: _____ Class: _____ Date: _____ **Total: 12 marks**

KEY WORDS hash 散列值 • hashing 散列 • cryptographic hash function 密码散列函数 • salt 盐值 • password spraying 密码喷洒

Objective

Build the skills to answer exam questions on **hashing** 散列, **salt** 盐值, password attacks, and authentication factors.

You must be able to:

- state the properties of a cryptographic hash (one-way, fixed length, repeatable)
- explain how salt protects stored passwords
- classify authentication factors (know / have / are / where) and password attacks

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Hashing and salt

A service stores the hash of a password, never the plaintext. Salt (random bits) is added before hashing so two identical passwords produce different stored hashes.

■ Password attacks

Password spraying = one common password against many accounts. Credential stuffing = stolen or default credentials. A rainbow table = a precomputed table of passwords and their hashes.

2 Practice

2.1 State two properties of a cryptographic hash function. [2]

2.2 Explain how **salt** protects stored passwords. [2]

2.3 Classify each authentication factor as know / have / are / where.

(a) A fingerprint [1]

(b) A code sent to your phone [1]

(c) A PIN [1]

3 Exam-style questions

3.1 A cryptographic hash output is [1]

- **A** variable length
- **B** a fixed length regardless of input
- **C** the original password
- **D** always longer than the input

3.2 Trying one common password against many accounts is [1]

- **A** credential stuffing
- **B** password spraying
- **C** salting
- **D** a rainbow table

3.3 A company enables multifactor authentication (MFA).

(a) State what MFA requires. [1]

(b) Explain why it is stronger than a password alone. [2]

Solutions

2.1 any two of: one-way/cannot reverse; fixed-length output; repeatable/same input same output.

2.2 salt adds unique random bits before hashing, so two identical passwords have different stored hashes.

2.3 (a) are / biometric. (b) have. (c) know.

3.1 B. a hash is fixed length and one-way.

3.2 B. one password, many users = password spraying.

3.3 (a) two or more different authentication factors. (b) an adversary must defeat two factors, so a stolen password alone cannot log in.

4. A network technician is unable to access a server using port 443 from a machine with an IP address of 192.168.45.37.

   Consider the following access control list (ACL) for the server's firewall.

Rule Number	Allow/Deny	Direction	Protocol	Port	Source
1	Allow	Inbound	TCP	22	ALL
2	Allow	Inbound	TCP	80	ALL
3	Deny	Inbound	TCP	443	192.168.0.0 - 192.168.255.255
4	Allow	Inbound	ICMP	ALL	ALL
5	Allow	Inbound	TCP	3306	ALL
6	Deny	Inbound	TCP	3389	ALL
7	Allow	Inbound	TCP	443	ALL
8	Allow	Inbound	TCP	587	ALL
9	Deny	Inbound	TCP	8140	192.168.45.0 - 192.168.45.255
10	Deny	Inbound	ALL	ALL	ALL

   Which of the following changes to the firewall would allow the network technician to access the server?

   (A) Swap firewall rule 1 with firewall rule 10

   (B) Swap firewall rule 3 with firewall rule 4

   (C) Swap firewall rule 3 with firewall rule 7

   (D) Swap firewall rule 4 with firewall rule 7

5. A system administrator runs two hashing functions on four files. Consider the following outputs for the two hashing functions.

Function 1 outputs

```
file1.txt - 8d8e115e5ebc50c8e03930beac6802a94ef4f36ab
file2.txt - 79a7d08081d12ecf123d63845e38c14c09956ee79
file3.txt - 02db6aefd093c317f8cf78a2fbe52a31b58a6bc5e
file4.txt - bcd3cf9d8527f711031d0d908d84cbb0df97ce90b
```

Function 2 outputs

```
file1.txt - 804537a7adfa4e1bce4d72d0b212a80af2dae3a5e
file2.txt - ba429665c8b95d05a963ee89fded2c7f18892d13e
file3.txt - 804537a7adfa4e1bce4d72d0b212a80af2dae3a5e
file4.txt - 7fa2901ebbb731eb283487afc033e45dae210a89e
```

Which of the following statements is supported by the file hashes?

(A) The files **`file1.txt`** and **`file3.txt`** are exact copies of each other.

(B) Function 1 is more secure than Function 2.

(C) Function 1 and Function 2 are the same hashing function.

(D) The files **`file1.txt`** and **`file3.txt`** have a collision in one hashing function.

6. The security manager at a hospital is planning to upgrade the hospital's physical security system to ensure that only authorized personnel can access areas containing sensitive medical equipment and patient records. Because these areas require a high level of security, the manager wants an authentication method that is unique to each individual and extremely difficult for an adversary to duplicate or spoof. Which of the following authentication methods is best suited for these areas?

   (A) Authentication token

   (B) Password

   (C) Retina scan

   (D) Access card

7. Which of the following best describes how offline password attacks work?

   (A) Adversaries attempt user:password combinations in an active authentication portal.

   (B) Adversaries intercept communication as it travels across a network and read the password in transit.

   (C) Adversaries exploit weak access controls to directly retrieve plaintext passwords stored in a database.

   (D) Adversaries use automated tools to hash many potential passwords and compare them to a captured hash.

12. The system administrator at a high school receives an alert that there may have been multiple unauthorized login attempts to the school's online grading system. To investigate, the administrator decides to review the authentication logs. Which of the following best describes how authentication logs can be used to determine whether unauthorized login attempts have occurred?
    (A) The logs record which password was used in each login attempt, which allows the administrator to verify account ownership.
    (B) The logs record all login activity, which allows the administrator to reconstruct when and how login attempts occurred.
    (C) The logs record the location of each user attempting to log in, which allows the administrator to identify login attempts from other geographic regions.
    (D) The logs record the type of device attempting to log in, which allows the administrator to block unauthorized devices.

13. The network administrator for a manufacturing facility has implemented a signature-based network detection system. Which of the following is a potential impact of using this network detection method instead of anomaly-based detection?
    (A) More false negative alerts
    (B) Higher operating costs
    (C) Slower detection time
    (D) More alert fatigue

14. Consider the following lines from a log file.

```
2025-09-25 08:01:14 ARP Reply: 192.168.1.13 is-at 00:01:5e:00:fc:16
2025-09-25 09:14:15 ARP Reply: 192.168.1.13 is-at 00:3b:cc:5e:ee:01
```

    Which of the following attack types is indicated in the log file?
    (A) ARP poisoning attack
    (B) DNS poisoning attack
    (C) Evil-twin attack
    (D) MAC flooding attack

15. Which of the following best describes the length of a cryptographic hash function output?
    (A) The length of the output is longer than the input due to the hashing process.
    (B) The length of the output is fixed regardless of the length of the input.
    (C) The length of the output varies based on the length of the input.
    (D) The length of the output is shorter than the length of the input.

18. Which of the following types of attacks occurred when the adversary submitted a string that included `' OR '1'='1';--`?
    (A) SQL injection attack
    (B) Buffer overflow attack
    (C) Cross site scripting attack
    (D) Directory traversal attack

19. Which of the following security controls would most likely prevent an attack like this in the future?
    (A) Encryption
    (B) Stateful firewall
    (C) Input sanitization
    (D) Access control list

20. Which of the following best explains how the adversary attempted to manipulate the bank's customer database through the online loan application form?
    (A) When user input is fed into a server's file system, HTTP requests can access sensitive data.
    (B) When user input contains executable scripts, those scripts can run in the user's browser and access sensitive data.
    (C) When user input exceeds the size of the designated memory, it can allow the adversary to access, modify, and delete files.
    (D) When user input from a web form is fed directly into a database query, an adversary can inject control characters that can allow an adversary to view or modify the contents of a database.

21. An organization only allows their users to log into a system if they are physically in one of the following time zones (a time zone is a region where everyone uses the same clock time).
    - Eastern time zone
    - Central time zone
    - Mountain time zone
    - Pacific time zone

    Which of the following authentication factors is being used to verify the identity of the users?
    (A) Biometric factor
    (B) Knowledge factor
    (C) Location factor
    (D) Possession factor

AP CYBERSECURITY • EXERCISE SHEET

4.3 Protecting Devices

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

KEY WORDS acceptable use policy 可接受使用政策 • host-based firewall 主机防火墙 • anti-malware software 反恶意
• patch 补丁 • malware 恶意软件

Objective

Build the skills to answer exam questions on protecting a device with policies, anti-malware, patching, and a **host-based firewall** 主机防火墙.

You must be able to:

- give managerial controls: acceptable use, password, software installation policies
- explain how anti-malware and patching protect a device
- describe what a host-based firewall does

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Patching

When a vendor releases a patch, they reveal the hole it fixes - so adversaries target anyone who has not updated. Prompt patching closes known holes before they are exploited.

■ Host-based firewall

A host-based firewall controls traffic in and out of one single device, blocking ports and services it does not need - adding a layer even on a compromised network.

2 Practice

2.1 Explain why keeping software updated makes a device safer. [2]

2.2 State what a **host-based firewall** protects. [1]

2.3 How does anti-malware software detect malicious files? [2]

3 Exam-style questions

3.1 A firewall that controls traffic for just one device is a [1]

- **A** network firewall
- **B** host-based firewall
- **C** stateless proxy
- **D** VPN

3.2 The policy listing what users may and may not do on company devices is the [1]

- **A** password policy
- **B** acceptable use policy
- **C** wireless policy
- **D** router policy

3.3 A host-based firewall on a laptop blocks outbound FTP.

(a) Explain how this could stop data theft. [2]

Solutions

2.1 a patch closes a known vulnerability before an adversary can exploit it.

2.2 traffic in and out of one single device.

2.3 it keeps a database of malware signatures and quarantines files that match a signature.

3.1 B. a host-based firewall guards a single device.

3.2 B. the acceptable use policy sets device usage rules.

3.3 (a) if malware infects the laptop and tries to exfiltrate files over FTP, the host firewall blocks the outbound connection even though the network allowed FTP.

AP CYBERSECURITY • EXERCISE SHEET

4.4 Detecting Attacks on Devices

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS indicator of compromise (ioc) 入侵指标 • credential stuffing 撞库 • password spraying 密码喷洒 • hash 散列值 • malware 恶意软件

Objective

Build the skills to answer exam questions on **indicators of compromise (IoCs)** 入侵指标 and reading authentication logs.

You must be able to:

- define an IoC and name host-, file-, and behaviour-based IoCs
- read auth logs to tell guessing, spraying, and stuffing apart
- explain why offline password attacks cannot be detected

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Reading auth logs

One user with many wrong passwords = a guessing attack. Many users failing from one IP = password spraying. A burst of default credentials = credential stuffing.

■ Offline attacks

Offline password attacks cannot be detected because the adversary already stole the hash database and is cracking it on their own computer, far from your logs.

2 Practice

2.1 Define an **indicator of compromise (IoC)**. [2]

2.2 A log shows 50 failed logins for user 'admin' from one IP in 30 seconds. What does this indicate? [2]

2.3 Explain why offline password attacks cannot be detected. [2]

3 Exam-style questions

3.1 Many different users failing to log in from ONE IP address suggests [1]

- **A** credential stuffing
- **B** password spraying
- **C** salting
- **D** patching

3.2 A file whose hash matches known malware is an example of a [1]

- **A** host-based IoC
- **B** file-based IoC
- **C** behaviour-based IoC
- **D** network segment

3.3 An analyst reviews authentication logs after an alert.

(a) State one pattern that would indicate credential stuffing. [1]

(b) State one pattern that would indicate a single-account guessing attack. [1]

Solutions

2.1 evidence in logs or files that an adversary has compromised a device or network.

2.2 an online password-guessing attack on one account; many wrong passwords fast for one user is the signature.

2.3 the cracking happens on the adversary's own computer, away from the victim's systems and logs.

3.1 B. one IP, many users = password spraying.

3.2 B. matching a known-malware hash is a file-based IoC.

3.3 (a) a burst of default username:password pairs tried in quick succession. (b) many wrong passwords for one user account.

12. The system administrator at a high school receives an alert that there may have been multiple unauthorized login attempts to the school's online grading system. To investigate, the administrator decides to review the authentication logs. Which of the following best describes how authentication logs can be used to determine whether unauthorized login attempts have occurred?

    (A) The logs record which password was used in each login attempt, which allows the administrator to verify account ownership.

    (B) The logs record all login activity, which allows the administrator to reconstruct when and how login attempts occurred.

    (C) The logs record the location of each user attempting to log in, which allows the administrator to identify login attempts from other geographic regions.

    (D) The logs record the type of device attempting to log in, which allows the administrator to block unauthorized devices.