HOLIDAY HOMEWORK 假期作业

AP Cybersecurity

Exercise sheets, topic by topic.

每个单元：练习卷。

For class or self-study • no answer keys included.

Contents 目录

1 People, passwords, and public networks – Part 1

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
Social engineering	社会工程学			
intimidation	恐吓			
urgency	紧迫感			
online password attack	在线密码攻击			
evil twin	双胞胎恶意热点			
encrypted	加密的			
VPN	虚拟专用网络			

Recall

- You already lock your phone with a **password** or fingerprint.
- You know a scam email when the grammar is bad or the offer is too good.
- You have joined free Wi-Fi in a café or airport before.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Social engineering

Social engineering 社会工程学 tricks a person into breaking security, instead of hacking the computer. Attackers use **intimidation** 恐吓 (a threat) and **urgency** 紧

迫感 (a deadline) to make you act before thinking.

Worked example. An email says "Verify in 1 hour or lose access." The 1-hour deadline is urgency - it rushes you into clicking.

■ 2 Password attacks

In an **online password attack** 在线密码攻击, an attacker tries many guessed passwords at a login. The log shows many failed logins fast. Weak, patterned passwords (like `Summer24!`) are easy to guess.

Worked example. A log shows 40 failed logins for one user in a minute - a clear guessing attack.

■ 3 Staying safe on Wi-Fi

An **evil twin** 双胞胎恶意热点 is a fake Wi-Fi that copies the real network's name. Prefer **encrypted** 加密的 sites (HTTPS) and use a **VPN** 虚拟专用网络 so your traffic is protected.

Worked example. On a fake café Wi-Fi, your bank login still stays safe because the bank uses HTTPS.

Watch out: A negative sign of a strong password is length, not a symbol at the end. `P@ssw0rd!` looks strong but follows a common pattern an attacker expects.

Practice

2.1 Define social engineering in one sentence. [2]

2.2 An email says "Reply within 10 minutes or your account closes." Name the tactic and explain how it works. [2]

2.3 State two signs of an online password attack in a log. [2]

2.4 Explain why an HTTPS website stays safe even on an evil-twin network. [2]

2.5 State two ways to make a password stronger. [2]

1 AI in attack and defence – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
deepfake	深度伪造			
phishing	钓鱼			
shared secret	共享秘密			
MFA	多因素身份验证			

Recall

- You have seen AI chatbots write fluent text and answer questions.
- You know a photo or video can be edited to look real.
- You understand that some emails try to trick you (phishing).

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 AI helps attackers

AI lets attackers make a **deepfake** 深度伪造 (a fake voice or face) to impersonate someone, and write flawless **phishing** 钓鱼 emails in any language. Bad grammar used to expose scams; AI removes that clue.

Worked example. A caller sounds exactly like your manager but is an AI deepfake asking you to transfer money.

■ 2 Defending against AI attacks

Agree a **shared secret** 共享秘密 word with close contacts to check identity, and enable **MFA** 多因素身份验证 so a cloned voice alone cannot log in. Never trust AI output without checking a real source.

Worked example. You ask the ”manager” a secret question only the real one would know - the deepfake fails.

3 AI helps defenders

A network makes millions of events a day - too many to read. AI sorts likely-malicious events from harmless ones and **alerts** staff in seconds. A human must still review AI advice, because AI only guesses probabilities.

Worked example. AI flags 12 suspicious events out of 20 million and alerts the team instantly.

Watch out: AI is dual-use: the same tool (a language model, code analysis) can help both an attacker and a defender. Read the question to see which side it means.

Practice

2.1 Explain how AI makes phishing emails harder to spot. [2]

2.2 Name one defence against a deepfake voice call and explain how it helps. [2]

2.3 Why should you never type sensitive data into a chatbot? [2]

2.4 Explain why AI is useful for reading network logs. [2]

2.5 State one task that should be left to a human, not the AI, and why. [2]

2 The CIA triad and managing risk – Part 1

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
CIA triad	中央情报三要素			
confidentiality	保密性			
integrity	完整性			
availability	可用性			
risk	风险			
threat	威胁			
vulnerability	漏洞			
asset	资产			
defense in depth	纵深防御			

Recall

- You keep some things private, trust that a document is unchanged, and expect a service to work when needed.
- You lock your door (a physical control) and follow rules like ”do not share your PIN.”
- You know some risks are worth avoiding and some you just accept.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 The CIA triad

Security has three goals - the **CIA triad** 中央情报三要素: **confidentiality** 保密性 (only the right people read it), **integrity** 完整性 (it is unaltered), and **availability** 可用性 (it works when needed).

Worked example. Encryption protects confidentiality; a file hash checks integrity; a backup protects availability.

■ 2 Risk and responses

A **risk** 风险 appears when a **threat** 威胁 exploits a **vulnerability** 漏洞 to harm an **asset** 资产. You can avoid, transfer, mitigate, or accept it.

Worked example. Buying insurance against a cyber loss is transferring the risk to the insurer.

■ 3 Types of control

Controls are grouped by **type** (physical, technical, managerial) and by **function** (preventative, detective, corrective). Layering many is **defense in depth** 纵深防御.

Worked example. A camera is physical by type and detective by function.

Watch out: Do not mix up the two groupings. Type = where it works; function = what it does. A camera can be classified both ways.

Practice

2.1 State the three goals of the CIA triad. [3]

2.2 Which CIA goal does encryption mainly protect? [1]

2.3 Define a risk in terms of a threat, a vulnerability, and an asset. [2]

2.4 Name the four ways to respond to a risk. [2]

2.5 Classify a door lock and a CCTV camera by function. [2]

2 Protecting and watching physical spaces – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
Piggybacking	尾随蒙骗			
tailgating	尾随潜入			
Shoulder surfing	肩窥			
card readers	读卡器			
access control vestibule	门禁前室			
UPS	不间断电源			
motion sensors	运动传感器			

Recall

- You have swiped a card or entered a code to open a door.
- You have seen CCTV cameras at shop entrances.
- You know a stranger following you through a locked door is suspicious.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Physical attacks

Piggybacking 尾随蒙骗 tricks someone into holding a door; **tailgating** 尾随潜入 slips in behind them unseen. **Shoulder surfing** 肩窥 watches you type a password.

Worked example. Someone carrying boxes gets a helpful worker to hold the door - piggybacking.

■ 2 Protecting the space

Use locks, fences, **card readers** 读卡器, and an **access control vestibule** 门禁前室 (a two-door airlock) that lets one person pass at a time. A **UPS** 不间断电源 keeps devices on during a power cut.

Worked example. An access control vestibule stops anyone slipping in behind an employee.

■ 3 Detecting attacks

Cameras, guards, and **motion sensors** 运动传感器 detect attacks. Place cameras at entrances and sensors in quiet areas - a busy hallway causes false alarms.

Worked example. A door log shows a door held open 20 seconds - a sign someone piggybacked through.

Watch out: A motion sensor in a busy area triggers so often that staff ignore it. Placement matters as much as having the control.

Practice

2.1 State the difference between piggybacking and tailgating. [2]

2.2 Explain how an access control vestibule stops piggybacking. [2]

2.3 Name two controls that DETECT physical attacks. [2]

2.4 Explain why a motion sensor should not go in a busy hallway. [2]

2.5 State what a UPS does. [1]

3 Network attacks and firewalls – Part 1

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
ARP poisoning	地址解析投毒			
on-path attack	中间人攻击			
denial of service (DoS)	拒绝服务			
firewall	防火墙			
access control list (ACL)	访问控制列表			
Network segmentation	网络分段			
subnets	子网			
screened subnet	屏蔽子网			

Recall

- You know a network connects devices so they share data.
- You have heard of a firewall blocking unwanted traffic.
- You understand that a flood of traffic can crash a website.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Network attacks

In **ARP poisoning** 地址解析投毒 the attacker sends fake messages so traffic flows to them - an **on-path attack** 中间人攻击. A **denial of service (DoS)** 拒绝服务

floods a target so real users cannot connect.

Worked example. A log shows one IP with two different MAC addresses - the sign of ARP poisoning.

■ 2 Firewalls and ACLs

A **firewall** 防火墙 allows or denies traffic using an ordered **access control list (ACL)** 访问控制列表. Rules are checked top-down and the **first match wins**.

Worked example. A DENY rule above an ALLOW rule for the same traffic blocks it, even though the ALLOW is lower down.

■ 3 Segmentation

Network segmentation 网络分段 splits a network into isolated **subnets** 子网 so a breach is contained. A **screened subnet** 屏蔽子网 (DMZ) holds public servers away from private systems.

Worked example. If a web server in the DMZ is hacked, the attacker is trapped there by the second firewall.

Watch out: Firewall rule order is everything. Swapping two rules can turn ”allowed” into ”denied” for the same packet.

Practice

2.1 A log shows one IP with two MAC addresses. Name the likely attack. [1]

2.2 Explain what happens in an on-path (man-in-the-middle) attack. [2]

2.3 In a firewall ACL, which rule is applied to a matching packet? [1]

2.4 Explain the main security benefit of network segmentation. [2]

2.5 State what a screened subnet (DMZ) holds and where it sits. [2]

3 Wireless security and detecting attacks – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
WPA3	无线加密协议			
MAC filtering	地址过滤			
NIDS	网络入侵检测系统			
NIPS	网络入侵防御系统			
SIEM	安全信息与事件管理			
Signature-based	基于特征			
Anomaly-based	基于异常			
baseline	基线			

Recall

- You choose a Wi-Fi network by its name and enter a password.
- You know some networks are open and some are locked.
- You understand that alarms should only go off when something is really wrong.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Wireless security

Use **WPA3** 无线加密协议 encryption - old **WEP** and the original **WPA** are broken. Disable beacon frames, control the signal so it does not leak outside, and use **MAC filtering** 地址过滤.

Worked example. A café controls its signal strength so the Wi-Fi stops at the walls, not the car park.

■ 2 Detection systems

A **NIDS** 网络入侵检测系统 detects and alerts; a **NIPS** 网络入侵防御系统 can also block; a **SIEM** 安全信息与事件管理 correlates data from many sources.

Worked example. A NIDS raises an alert but waits for a human; a NIPS closes the port itself.

■ 3 Detection methods

Signature-based 基于特征 detection matches known attacks - fast, few false alarms, but misses new ones. **Anomaly-based** 基于异常 compares to a normal **baseline** 基线 - catches new attacks but costs more.

Worked example. A brand-new worm slips past signature detection but trips the anomaly detector.

Watch out: The one-letter difference matters: an IDS only alerts, an IPS can block. Read which the question means.

Practice

2.1 State the strongest current wireless encryption protocol. [1]

2.2 Explain why controlling a Wi-Fi signal's strength improves security. [2]

2.3 State the difference between a NIDS and a NIPS. [2]

2.4 Which detection method is more likely to catch a brand-new attack? [1]

2.5 Give one advantage and one disadvantage of signature-based detection. [2]

4 Devices, malware, and authentication – Part 1

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
virus	病毒			
worm	蠕虫			
ransomware	勒索软件			
hash	散列值			
Salt	盐值			
biometric	生物特征			
MFA	多因素身份验证			

Recall

- You use several devices: a phone, a laptop, maybe a smart speaker.
- You have heard of viruses and know updates are important.
- You log in with passwords and sometimes a texted code.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Malware types

A **virus** 病毒 needs a user to run a file; a **worm** 蠕虫 spreads by itself; **ransomware** 勒索软件 encrypts files for money; a **rootkit** hides in the OS.

Worked example. Ransomware locks a hospital's files and demands payment for the key.

■ 2 Hashing and salt

Passwords are stored as a one-way **hash** 散列值, never as plaintext. **Salt** 盐值 (random bits) makes two identical passwords hash differently.

Worked example. Two users both pick `sunshine`; with unique salt, their stored hashes look completely different.

■ 3 Authentication factors

Factors are: something you **know** (a password), **have** (a phone), **are** (a **biometric** 生物特征 like a fingerprint), or **where** you are. Two or more is **MFA** 多因素身份验证.

Worked example. A password plus a texted code is MFA - far stronger than a password alone.

Watch out: A worm and a virus are not the same. A worm spreads on its own; a virus needs a person to run it.

Practice

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

2.2 Name the malware that encrypts files and demands payment. [1]

2.3 Explain how salt protects stored passwords. [2]

2.4 Classify a fingerprint, a texted code, and a PIN by factor type. [3]

2.5 Explain why MFA is stronger than a password alone. [2]

4 Protecting and monitoring devices – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
Anti-malware software	反恶意软件			
patching	打补丁			
host-based firewall	主机防火墙			
password spraying	密码喷洒			
credential stuffing	撞库			

Recall

- You get reminders to update your phone or laptop.
- You may have antivirus software installed.
- You know a log records what happened, like a diary.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Protecting devices

Anti-malware software 反恶意软件 quarantines files matching known signatures. Prompt **patching** 打补丁 closes known holes. A **host-based firewall** 主机防火墙 guards one device by blocking unneeded ports.

Worked example. A host firewall blocks outbound FTP, stopping malware from sending files out.

■ 2 Reading authentication logs

Many wrong passwords for one user = guessing. Many users failing from **one IP** = **password spraying** 密码喷洒. Default credentials in bursts = **credential stuffing** 撞库.

Worked example. 50 failed logins for 'admin' from one IP in 30 seconds is an online guessing attack.

■ 3 What cannot be detected

Offline password attacks cannot be detected, because the attacker cracks the stolen hash on their own computer, away from your logs.

Worked example. Once a hash database is stolen, cracking it happens off-site and leaves no trace on you.

Watch out: Offline password attacks leave no trace on your systems - the only defence is strong, salted hashing in the first place.

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 Many users failing to log in from one IP address suggests which attack? [1]

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

2.5 How does anti-malware software detect a malicious file? [2]

5 Application attacks and access control – Part 1

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
SQL injection	数据库注入			
directory traversal	目录遍历			
Data validation	数据验证			
RBAC	基于角色的访问控制			
RuBAC	基于规则的访问控制			
DAC	自主访问控制			
MAC	强制访问控制			
least privilege	最小权限			

Recall

- You have typed into search boxes and login forms on websites.
- You know some files are private and some are shared.
- You understand that only certain people should edit certain things.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Application attacks

Unchecked user input is the danger. **SQL injection** 数据库注入 puts commands into a form to read a database; **directory traversal** 目录遍历 uses `../` to reach other files. **Data validation** 数据验证 is the defence.

Worked example. Typing `' OR '1'='1` into a login makes the query always true - SQL injection.

■ 2 Access control models

RBAC 基于角色的访问控制 follows your role; **RuBAC** 基于规则的访问控制 follows a condition (like time); **DAC** 自主访问控制 lets the owner decide; **MAC** 强制访问控制 uses central levels.

Worked example. "Only during business hours" is a condition, so it is RuBAC.

■ 3 Linux permissions

Each file gives **read (4), write (2), execute (1)** to the owner, group, and others. `chmod 640` = owner read+write (6), group read (4), others none (0). Follow **least privilege** 最小权限.

Worked example. Owner rwx, group r-x, others none = 7,5,0 = chmod 750.

Watch out: Do not gloss over the direction of `../` - it climbs UP folders. Three of them reach the root of the file system.

Practice

2.1 A login field receives ' OR '1'='1. Name the attack. [1]

2.2 Explain how a directory traversal attack works. [2]

2.3 "Access allowed only during business hours" - name the access-control model. [1]

2.4 Write the chmod number for owner read+write, group read, others none. [2]

2.5 State what the principle of least privilege means. [2]

5 Cryptography and detecting data attacks – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
plaintext	明文			
key	密钥			
ciphertext	密文			
Symmetric encryption	对称加密			
AES	高级加密标准			
key pair	密钥对			
public key	公钥			
private key	私钥			
honeypot	蜜罐			
hash	散列值			

Recall

- You know a secret code turns a message into something unreadable.
- You have seen the padlock icon (HTTPS) in a browser.
- You understand that checking a file's fingerprint can show if it changed.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

1 Symmetric encryption

Encryption combines **plaintext** 明文 with a **key** 密钥 to make **ciphertext** 密文. **Symmetric encryption** 对称加密 (like **AES** 高级加密标准) uses the same key both ways; the challenge is sharing that key safely.

Worked example. A 4-bit key has $2^4 = 16$ possible values - a real key is far longer.

2 Asymmetric encryption

A **key pair** 密钥对 has a **public key** 公钥 (shared) and a **private key** 私钥 (secret). To send Bob a secret, encrypt with Bob's public key; only his private key decrypts it.

Worked example. This solves symmetric's problem - no secret key had to be shared first.

3 Detecting data attacks

A **honeypot** 蜜罐 is a fake valuable file - any access is an alarm. A **hash** 散列值 check re-hashes a file to see if it changed. Logs reveal attacks: `OR 1=1` = SQL injection, `<script>` = XSS, `../` = traversal.

Worked example. A fake `passwords.xlsx` triggers an alert the moment anyone opens it.

Watch out: To send a secret, use the recipient's PUBLIC key, not your own. Mixing up whose key to use is the most common mistake.

Practice

2.1 Explain what 'symmetric' means in symmetric encryption. [2]

2.2 How many possible keys does a 4-bit key have? [1]

2.3 Which key do you use to encrypt a message you are sending to someone? [1]

2.4 Explain how a honeypot detects an attacker. [2]

2.5 Match each log clue to its attack: `OR 1=1`, `<script>`, `../`. [3]