Identifying and preventing vulnerabilities

1.4.2 · Computer systems (Paper 1) · revision notes

The common ways of finding and preventing weaknesses: penetration testing, anti-malware software, firewalls, user access levels, passwords, encryption and physical security. Questions ask how each method works and which method best prevents a given threat, often in a scenario or an 8-mark discussion.

Key facts

- Penetration testing: authorised, simulated attacks to find weaknesses
- Firewall: monitors traffic in and out; blocks what does not meet its rules
- Strong password: long, mixed characters, not guessable; lock accounts after failed attempts
- Physical security: locks, key cards, biometrics, CCTV
- Anti-malware: scans, compares with known malware, quarantines or deletes; keep it updated
- User access levels: each user gets only the permissions they need
- Encryption: stolen or intercepted data is unreadable without the key

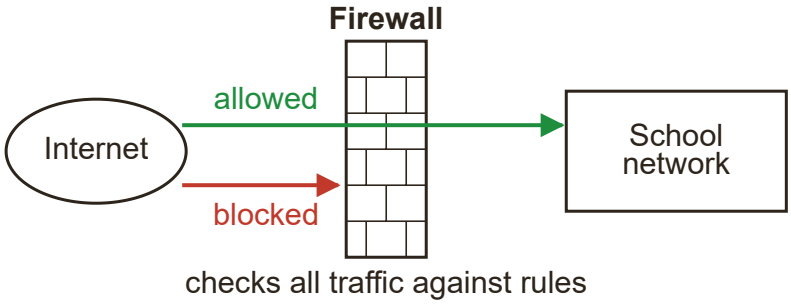
Notes

Finding weaknesses

- **Penetration testing**: authorised experts carry out **simulated attacks** on a system to find vulnerabilities, so they can be fixed **before criminals find them**.
- Testers may be given no inside information, to act like an outside attacker, or given a normal user's access, to act like a dishonest employee.

Protecting software and data

- **Anti-malware software**: scans files, emails and downloads, compares them with a database of known malware, and quarantines or deletes threats. It must be **updated regularly** to recognise new malware.
- **Firewall**: hardware or software that **monitors incoming and outgoing traffic** and blocks any that does not meet a set of rules, preventing unauthorised access.



A firewall checks traffic in and out and blocks anything that breaks its rules

- **Encryption**: data is scrambled, so intercepted or stolen data cannot be understood without the key.

Controlling access

- **User access levels**: each user is given only the permissions they need (e.g. read-only, or no access to some folders). This limits the damage an insider or a hacked account can do.
- **Passwords**: strong passwords are long, use a mix of upper and lower case letters, numbers and symbols, and are not words or personal details. Locking an account after a few wrong attempts stops brute-force attacks. Two-factor authentication adds a second check, such as a code sent to a phone.
- **Physical security**: locks, key cards, biometric scanners, CCTV and security staff stop people reaching servers and devices.

Matching methods to threats

- Malware → anti-malware software and a firewall. Phishing and blagging → staff training. Brute force → strong passwords and account lockout.
- DoS → a firewall to filter traffic. Interception → encryption. SQL injection → input validation (and penetration testing to find the weakness). Stolen devices → physical security and encryption.
- No single method stops every threat, so organisations use several **layers of protection**.

How to answer each type of question

Describe how a method protects a system

2 to 3 marks | Grade 5

1. Say what the method does: monitors, scans, restricts or scrambles.
2. Say how it decides: rules, known malware, permissions or a key.
3. Say what it prevents.

Example. Describe how a firewall helps to protect a school network. [3]

Model answer. A firewall monitors the data coming into and going out of the network (1). It checks the data against a set of rules, e.g. which addresses or ports are allowed (1), and blocks any data that does not meet the rules, preventing unauthorised access (1).

Explain the purpose of penetration testing

2 marks | Grade 6

1. Say what it is: authorised, simulated attacks.
2. Say why: to find weaknesses so they can be fixed before criminals exploit them.

Example. Explain why a bank pays a company to carry out penetration testing. [2]

Model answer. The testers carry out authorised, simulated attacks to find weaknesses in the bank's systems (1), so the weaknesses can be fixed before criminals find and exploit them (1).

Choose a prevention method for each threat

2 marks per threat | Grade 7

1. Name a method that really stops this threat (not a firewall for everything).
2. Explain how it stops this particular threat.

Example. For each threat, identify a suitable prevention method and explain how it helps.
(a) A laptop containing customer data is left on a train. [2]
(b) Staff receive emails asking them to confirm their passwords on a website. [2]

Model answer.

(a) Encrypt the laptop's storage (1), so whoever finds it cannot read the customer data without the key (1).

(b) Train staff to recognise phishing emails (1), so they do not click the link or enter their passwords, and report the email instead (1).

8-mark: discuss how to protect an organisation 8 marks (marked in levels) **Grade 8**

1. Choose several methods that fit the organisation's data, size and budget.
2. For each, explain which threat it stops and how.
3. Prioritise: say which methods matter most here and why.
4. End with a supported conclusion.

Example. A doctors' surgery has 12 staff. Its network stores patient records, and patients book appointments on the surgery's website. Discuss how the surgery should protect its network and patient data. [8]

Model answer.

Patient records are sensitive, so the surgery must keep them secure under the Data Protection Act 2018. User access levels should let doctors see full medical records while reception staff see only contact details and appointments, which limits the damage if one account is misused. Every member of staff should use a strong password, and accounts should lock after several wrong attempts to stop brute-force attacks.

A firewall should block unauthorised traffic from the Internet, and anti-malware software, kept up to date, should scan emails and downloads. The records should be encrypted and the website should use HTTPS, so intercepted or stolen data cannot be read. The booking form should validate its input to prevent SQL injection.

The server should be in a locked room, because physical access would get round many of these methods. Staff should be trained to spot phishing, since a firewall cannot stop someone giving away their password. Penetration testing would show whether these measures actually work.

Conclusion: no single method is enough; access levels, encryption and staff training matter most because the data is so sensitive.

Top band (6–8 marks): chooses several methods, explains how each protects this surgery's patient data, and prioritises them in a supported conclusion.

Don’t lose marks

- Saying a firewall removes viruses. A firewall filters traffic; anti-malware software finds and removes malware.
- Saying encryption stops hackers getting in. It stops them understanding the data they get.
- Describing penetration testing as a real attack by criminals. It is authorised by the organisation.
- Recommending the same method (usually a firewall) for every threat.

More tips

Memory tricks

- Match the method to the threat: people problems need people solutions (training); technical attacks need technical solutions.
- A firewall is a bouncer checking a guest list (its rules); anti-malware is a sniffer dog searching for known threats.
- Penetration testing is hiring a friendly burglar to find the unlocked windows before a real one does.

Exam technique

- In 'identify and explain' tables, the explanation mark depends on choosing a suitable method, so choose carefully.
- Apply methods to the scenario: a small business may not afford penetration testing; a hospital must protect very sensitive records.
- In 8-mark answers, prioritise: say which methods matter most for this organisation and why.

What each grade needs

What you need to be able to do, from the first marks up to the top grade.

Grade 3

Name methods to protect a network

Penetration testing, anti-malware, firewalls, user access levels, passwords, encryption and physical security.

Grade 4

Describe features of a strong password

Long, a mix of upper and lower case letters, numbers and symbols, and not a word or a personal detail.

Grade 5

Describe how a firewall works

It monitors incoming and outgoing traffic and blocks data that does not meet its rules.

Grade 5

Describe how anti-malware software works

It scans files, compares them with a database of known malware, and quarantines or deletes threats.

Grade 6

Explain the purpose of penetration testing

Authorised, simulated attacks find weaknesses so they can be fixed before criminals exploit them.

Grade 7

Match prevention methods to specific threats

E.g. training for phishing, input validation for SQL injection, encryption for interception.

Grade 8

Evaluate the security for an organisation

Recommend and prioritise a combination of methods suited to the organisation's data, budget and staff.

Free notes, Full packs, practice papers and mock exams at chhetriacademy.com. Written for this site; not taken from past papers. Stuck? 1-to-1 tutoring with a free 30-minute trial lesson.