Network security and identifying vulnerabilities

4.2.1a · Networks · revision notes

Why network security matters, and the two ways of finding weaknesses before criminals do that are on the specification: penetration testing and ethical hacking. Expect definitions, 'Explain why…' questions set in contexts such as hospitals, banks and schools, and occasionally a 6-mark 'Discuss'.

Key facts

- Vulnerability: a weakness that an attacker could exploit
- Ethical hacking: hacking with the owner's permission to find and report weaknesses so they can be fixed
- Impacts of a breach: data theft, financial loss, fines, damage to reputation, downtime
- Grade 7+ only Black-box test: testers know nothing (like an outsider); white-box test: testers have full details (like an insider)
- Penetration testing: an authorised, simulated attack to find vulnerabilities before criminals do
- Malicious hacking: without permission, to steal, damage or make money (illegal)
- Penetration test stages: scope and permission → gather information → attack → report → fix → retest

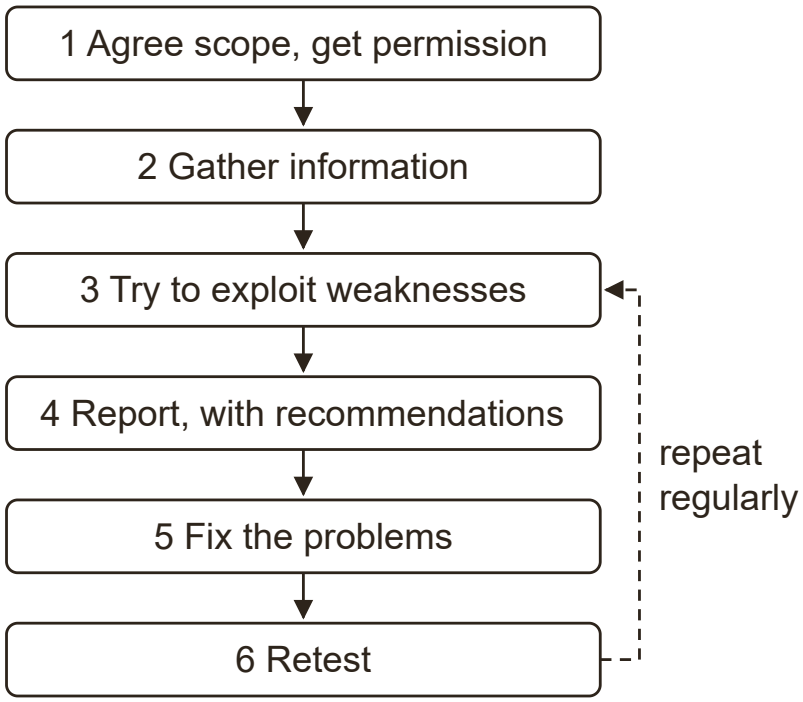
Notes

Why network security matters

- Networks hold valuable data, such as personal details, bank details, medical records and business secrets, so criminals try to break in.
- Network security aims to stop data being accessed without authorisation, changed or deleted, and to keep systems **available** to the people who need them.
- A breach can lead to: theft or loss of data; financial loss (stolen money, ransom demands, repair costs); fines and legal action, because organisations have a legal duty to protect personal data; damage to reputation and loss of customers' trust; and systems being unavailable, so work stops.
- A **vulnerability** is a weakness that an attacker could exploit, e.g. software that has not been updated, a weak password, an old account that is still active or an unlocked server room. Organisations try to find vulnerabilities before criminals do.

Penetration testing

- **Penetration testing** is an authorised, simulated attack on a network or system to find vulnerabilities that a real attacker could exploit.
- Typical stages: agree what will be tested and get written permission; gather information about the network; try to exploit weaknesses as a real attacker would; report what was found, with recommendations; fix the problems; retest.



The stages of a penetration test. Tests are repeated, e.g. after changes to the network.

- Testers may be given no information about the network, to act like an outside attacker (black-box testing), or full details, to act like an insider (white-box testing). Grade 7+ only
- A test only shows the weaknesses that existed, and were found, at the time, so it must be repeated regularly, e.g. after changes to the network. Grade 8+ only

Ethical hacking

- **Ethical hacking** is hacking into a system **with the owner's permission** to find weaknesses and report them so that they can be fixed. Penetration testing is one form of ethical hacking.
- Ethical hackers may work for the organisation, be hired from a security company, or be rewarded for reporting flaws through a 'bug bounty' scheme.
- Malicious hackers break in without permission to steal data, cause damage or make money. Hacking without permission is illegal.

How to answer each type of question

Define penetration testing or ethical hacking

1 to 2 marks | Grade 5

1. Include both key ideas: it is authorised (done with permission), and its purpose is to find weaknesses so that they can be fixed.
2. Use the word 'vulnerabilities' or 'weaknesses'.

Example. (a) Define the term 'penetration testing'. (1)
(b) Explain the difference between ethical hacking and malicious hacking. (2)

Model answer.

(a) An authorised, simulated attack on a network to find vulnerabilities before criminals can exploit them (1)

(b) An ethical hacker has the owner's permission to try to break in (1) and reports the weaknesses they find so that they can be fixed, whereas a malicious hacker has no permission and aims to steal data, cause damage or make money (1).

Explain why network security is important for an organisation

2 to 4 marks | Grade 6

1. Identify what could go wrong: theft of data, fines, damage to reputation, downtime.
2. Explain the consequence for this organisation or its customers.
3. Use the context: name the kind of data or service that the organisation holds.

Example. A building society stores its customers' personal and financial details on its network.
Explain **two** reasons why network security is important for the building society. (4)

Model answer. Customers' financial details could be stolen and used for fraud (1), so the building society could lose money and its customers' trust (1). It has a legal duty to protect personal data (1), so a breach could lead to a large fine or legal action (1).

Explain why an organisation would use penetration testing

2 to 3 marks | Grade 6

1. Say what the testers do: simulate the attacks a real criminal might try.
2. Say why: to find the vulnerabilities first.
3. Say what happens next: the weaknesses are fixed, reducing the risk of a breach.

Example. A school pays a security company to carry out a penetration test on its network.
Explain why the school does this. (3)

Model answer. The testers simulate the attacks that a real criminal might try (1), so the school finds the vulnerabilities in its network before criminals do (1). The school can then fix these weaknesses, e.g. by installing missing updates, which reduces the risk of pupils' data being stolen (1).

Describe the stages of a penetration test 3 to 4 marks **Grade 7**

1. Put the stages in order: plan and get permission, gather information, attack, report.
2. Give a short detail for each stage.
3. If there is a spare mark, add what happens afterwards: the problems are fixed and the test is repeated.

Example. Describe the stages of a penetration test. (4)

Model answer. The organisation and the testers agree what will be tested and when, and the organisation gives written permission (1). The testers gather information about the network, e.g. by scanning it to find the devices that could be attacked (1). They try to exploit weaknesses in the same way as a real attacker would (1). They report the vulnerabilities they found to the organisation, with recommendations for fixing them (1).

Don't lose marks

- Defining penetration testing as 'hacking into a network' without saying that it is authorised and done to find weaknesses.
- Saying ethical hacking is legal 'because it is for a good reason'. It is legal because the owner has given permission.
- Giving vague impacts such as 'bad things happen'. Name the impact: fines, financial loss, damage to reputation, downtime.
- Thinking that one penetration test makes a network secure for good. New vulnerabilities appear all the time.
- Answering a question about identifying vulnerabilities with a method of protection, such as a firewall or passwords.

More tips

Memory tricks

- Ethical hacking = permission + purpose (to find and fix weaknesses). You usually need both for the mark.
- Impacts of a breach, DRAFT: Data stolen, Reputation damaged, Availability lost (downtime), Fines, Theft of money.
- A penetration test in four words: plan, probe, attack, report.
- Identify weaknesses: penetration testing and ethical hacking. Protect against them: access control, physical security and firewalls.

Exam technique

- Learn precise definitions: 'authorised', 'simulated attack' and 'find vulnerabilities' are the key phrases.
- In 'Explain why security matters' questions, use the context: a hospital's patient records, a shop's card details, a school's pupil data.
- If a question asks how to identify vulnerabilities, answer with penetration testing or ethical hacking, not firewalls or passwords.
- In a 6-mark answer, weigh the benefits (finds real weaknesses) against the drawbacks (cost, only a snapshot in time, testers may see sensitive data).

What each grade needs

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

Grade 3

Give reasons why network security is important

To stop data being stolen, changed or deleted, and to keep systems working.

Grade 4

Give impacts of a security breach

Data theft, financial loss, fines, damage to reputation and systems being unavailable.

Grade 5

Define penetration testing and ethical hacking

Both are authorised attempts to find weaknesses in a system so that they can be fixed.

Grade 6

Explain why organisations use penetration testing

To find vulnerabilities before criminals exploit them, so that they can be fixed.

Grade 6

Distinguish ethical hacking from malicious hacking

Ethical hackers have permission and report what they find; malicious hackers have no permission and aim to cause harm.

Grade 7

Describe the stages of a penetration test

Agree the scope and get permission, gather information, attempt attacks, report, then fix and retest.

Grade 8

Evaluate the limits of penetration testing

A test is a snapshot of one moment, so new vulnerabilities appear afterwards and testing must be repeated.

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.