1. Describe how a firewall protects a local area network (LAN).

(2)

2. A company stores statistics about its business on a server.

Explain **one** type of access to the statistics file a student on work experience at the company should be given.

(2)

3. A company needs to secure its network from attacks by its employees.

Explain the best choice of penetration testing the company should use.

(2)

4. What is a network vulnerability? (1)

5. Give 2 examples of network vulnerabilities. (2)

6. What is ethical hacking? (1)

7. Discuss methods a movie streaming company could use to secure its network.

Your answer should consider:

- physical security
- access control
- firewalls.

(6)

ANSWERS

1. A **firewall** is a security device that acts as a protective barrier between your LAN and the outside world, such as the internet.
   It monitors and controls the flow of data traffic, ensuring that only authorized data passes through while blocking unauthorized or potentially harmful traffic.
   Firewalls are like digital bouncers that use predefined rules to determine whether a packet should be permitted or denied. These rules specify what types of traffic are acceptable.

2. The student should be given read-only access. This means they can view the data but cannot edit it or delete it. This protects the data. For some files no-access might be more appropriate. This would stop the student from viewing any sensitive or private data.

3. Penetration testing tests for vulnerabilities and security weaknesses within a network.
   The company has a choice between internal (white box) penetration testing and external (black box) penetration testing. External means that the tester acts as an external hacker with no specific knowledge of the network. They look for any security vulnerabilities that could be identified by an external hacker. Internal pen testing acts from within the network. Either as employees with internal knowledge of the network or from the point of view of a hacker who has gained access. Internal pen testing might test access (can people get unauthorised access to data), weak passwords and whether employees fall for phishing scams.

4. A **network vulnerability** refers to a weakness in a network's security that could potentially be exploited by attackers to gain unauthorized access, disrupt services, or compromise data.

5. Here are some examples of network vulnerabilities: **unpatched apps/software** – always update when prompted!; **weak passwords; poorly set up firewalls; out of data anti-malware software**

6. **Ethical hacking** involves using hacking techniques to uncover, understand, and fix security vulnerabilities in a network or computer system. Unlike malicious hackers, ethical hackers aim to improve network security without causing harm.

7. Physical security measures include access controls (pin codes, biometrics, security cameras, fences – on server rooms holding the movies). Other access controls to restrict access to the movies include strong passwords and two-factor authentication as well as access rights set up by the network administrator to limit the number of people who can access parts of the network. This protects data. Firewalls protect the network from unauthorised access from outside the network. The network administrator should set up firewall rules to stop unauthorised accesss.