OCR Computer Science GCSE

1.4 – Network security

Advanced Notes

1.4.1 Threats to computer systems and networks

Forms of attack

Malicious code (malware)

Malicious code (malware) is an umbrella term used to refer to a variety of forms of hostile or intrusive software. Forms of malware include:

- **Computer virus:** A type of malware that attaches itself to a legitimate program or file and spreads when the infected file is opened. It can corrupt or delete data, slow down systems, or even make them unusable.
- **Trojan:** A malicious program that disguises itself as legitimate software. Once installed, it can create backdoors, allowing hackers to control the system, steal data, or install more malware without the user's knowledge.
- **Spyware:** A type of malware that secretly gathers information about a user's activity, such as keystrokes, login details, or browsing habits, and sends this information to the attacker.

Social engineering

Social engineering is the art of manipulating people so they give up confidential information. It is often said that people are the "weak point" of secure systems, as they have access to computer systems and information that outsiders don't - however, they are susceptible to being socially engineered.

One form of social engineering is phishing: a technique of fraudulently obtaining private information, often using email or SMS. Typically, the victim will receive a communication designed to look like it has come from a reputable source, such as their bank, which then contains a link to trick them into giving away their personal information, such as login details.

Brute-force attacks

A brute-force attack is a method where an attacker tries many different combinations of usernames and passwords until the correct one is found. This is usually automated using software that quickly tests thousands of possible combinations. The purpose of this attack is to break into user accounts or systems by guessing login credentials.

Denial of service attacks

A denial of service (DOS) attack is used to overwhelm a website or online service with excessive traffic, making it slow or completely inaccessible to real users. This is usually done by sending a massive number of requests to the server in a short space of time.

Data interception and theft

Data interception and theft occurs when cybercriminals capture data being transmitted over a network without permission. This is often done on unsecured networks using special software that listens for unencrypted data, such as login details or credit card numbers. The purpose of this attack is to steal sensitive information, which can then be used for identity theft, fraud, or unauthorised access to systems.

SQL injection

SQL is a form of database - databases are used to store data in a structured way. SQL injection is an attack where an attacker enters specially crafted SQL code into a website's input fields, such as a login box or search form. If the website does not properly check the input, the malicious code is run by the database. The purpose of this attack is to gain unauthorised access to or control over the database, allowing the attacker to view, change or delete private data.

1.4.2 Identifying and preventing vulnerabilities

There are several methods which can be used to limit the threats posed by the methods of attack covered in section 1.4.1.

Penetration testing

Penetration testing is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. This can be carried out to test the effectiveness of security measures, and find any vulnerabilities / weaknesses that a hacker could exploit, before real attacks happen. Measures can then be taken to increase the security of any weaknesses exposed.

Anti-malware software

Scans for malware, by comparing files to a database of known malware. When malware is found on a user's system then the anti-malware software should alert them and request they take an action, such as quarantining or deleting the malware. If malware is identified as being downloaded, then the download will be stopped.

Firewalls

Scans incoming and outgoing traffic, comparing it to a criteria. This data will be blocked or allowed based on a set of security rules. For example, it might block traffic from suspicious IP addresses or stop certain types of data from entering a network.

User access levels

User access levels are used to control what data and features different users can access within a system. For example, in a school, an administrator may have full access, while a student or teacher is given limited access. This method helps prevent misuse of data or accidental changes by ensuring users only have access to what they need. It limits attacks by reducing the risk of insider threats or damage if a low-level account is compromised.

Passwords

Passwords are used to protect user accounts and systems by ensuring that only authorised users can log in. A strong password should be long, complex and hard to guess. Passwords help prevent unauthorised access, including brute-force attacks, by making it difficult for attackers to guess the correct login details.

Encryption

Encryption is a method of converting data into a coded format so that only authorised users with the correct decryption key can understand it. This prevents information from being obtained by hackers in a readable format, reducing the risk of data leaks.

Physical security

Physical security involves using barriers and controls to protect computer systems and data from physical threats. This includes locks on doors, keycard entry, alarms, security guards and CCTV. It helps prevent theft, tampering or unauthorised access to hardware.

Prevention method	Types of attacks limited or prevented
Penetration testing	SQL injection, brute-force attacks, data interception
Anti-malware software	Malware attacks (e.g. viruses, trojans, spyware, ransomware)
Firewalls	Denial of service attacks, malware from the internet
User access levels	Insider threats, misuse of data, damage from compromised low-level accounts
Passwords	Brute-force attacks, unauthorised access to accounts or systems
Encryption	Data interception and theft during transmission or if devices are stolen
Physical security	Theft of devices, unauthorised physical access, tampering with hardware or systems