1.4 Network Security

There are various ways in which a computer system or network can be attacked including: Malware, social engineering, brute force attacks, denial of service attacks, data interception and SQL injection

There are several different types of malware:

- Virus - Is hidden inside, or attached to, another file or program. Deletes or corrupts data and files.
- Worm - Is self-replicating. Slows the computer and creates back doors.
- Trojan - Looks like legitimate software
- Ransomware - Denies a user access to their system until a ransom is paid.
- Spyware - Is often bundled with free software. Logs activity and keystrokes and sends these back to a criminal.
- Pharming - Redirects a user to a spoof website without their knowledge by modifying DNS entries.

Ways of preventing malware

- Install anti-virus and anti-spyware software.
- Ensure that the operating system is up to date.
- Implement user access levels to prevent standard users from being able to install software.
- Only download programs from trusted websites.
- Educate users about the risks of opening emails and attachments from unknown sources

Social engineering involves tricking or manipulating people into giving away critical information or access details. Methods include phishing, pretexting and shouldering. Way to prevent these are to educate users so that they are aware of the tactics of criminals and can guard against them. And ensure that network and security policies are followed.

Brute force attacks involve the use of automated software to crack passwords in order to gain access to a system. Way to prevent these are to; Use long passwords that include special characters. Use complex passphrases rather than single words. Use a password manager. Limit the number of login attempts allowed and use two-factor authentication.

Denial of service attacks occur when a server is flooded with bogus requests in order to bring it down. Way to prevent is to install a firewall to reject packets that originate from the same source or that have identical contents. Configure a firewall to restrict the number of packets that can be accepted within a particular time frame.

SQL injection uses SQL commands entered into input fields on online forms to gain access to databases. To prevent use input validation to set password and username rules that don't permit characters which can be used in SQL injection attacks. Use input sanitisation to remove special characters and SQL command words from an input before processing it.

Network communications can be intercepted on their way to their destinations. Data interception and theft can occur through packet sniffing or the use of fake Wi-Fi hotspots. To prevent use strong encryption, especially on Wi-Fi networks; do not use unencrypted free public Wi-Fi networks. Use MAC address authentication on networks so that only known devices can connect. Ensure that websites are using HTTPS connections so that if data is intercepted it cannot be read.

Penetration testing is used to identify weaknesses and vulnerabilities in computer systems so that they can be addressed.