CAIE Computer Science IGCSE
5.3 Cyber security

Flashcards

How are brute-force attacks normally conducted?

How are brute-force attacks normally conducted?

Using automated software that quickly tests thousands of possible combinations of usernames and passwords.

What is the purpose of brute-force attacks?

What is the purpose of brute-force attacks?

To break into user accounts or systems by guessing login credentials.

Which type of networks are particularly vulnerable to data interception and theft?

Which type of networks are particularly vulnerable to data interception and theft?

Unsecured networks.

How are distributed denial of service attacks normally conducted?

How are distributed denial of service attacks normally conducted?

By sending a massive number of requests, from multiple different devices with different IP addresses, to a server in a short space of time.

What is hacking?

What is hacking?

The act of gaining unauthorised access to computer systems or networks.

What is malware?

What is malware?

Malicious software, an umbrella term used to refer to a variety of forms of hostile or intrusive software.

Name six forms of malware.

Name six forms of malware.

Viruses, worms, Trojan horses, spyware, adware, and ransomware.

What is a computer virus?

What is a computer virus?

A type of malware that attaches itself to a legitimate program or file and spreads across a network when the infected file is opened.

What is a worm?

What is a worm?

A type of malware that can spread and replicate without any user action. Unlike viruses, worms do not need to attach themselves to files or programs.

What is a Trojan horse?

What is a Trojan horse?

A malicious program that disguises itself as legitimate software to avoid detection.

What is spyware?

What is spyware?

A type of malware that secretly gathers information about a user's activity, such as keystrokes, and sends this information to the attacker.

What is adware?

What is adware?

Software that automatically displays or downloads unwanted advertising material when a user is online.

What is ransomware?

What is ransomware?

A type of malware that encrypts the user’s files or locks them out of their system, demanding payment for the attacker to release the system.

What is pharming?

What is pharming?

A technique that redirects users from a legitimate website to a fake one without their knowledge.

How is pharming normally conducted?

How is pharming normally conducted?

By exploiting vulnerabilities in a computer’s DNS settings or by compromising a website’s server.

What is phishing?

What is phishing?

Sending victims a communication that looks genuine, containing a link to fraudulently obtain their personal information.

What is social engineering?

What is social engineering?

An umbrella term used for a range of techniques that are used to manipulate people into giving away confidential information.

What are access levels?

What are access levels?

Restrictions on what each user can view or change in a system, based on their role.

What is the primary function of anti-malware software?

What is the primary function of anti-malware software?

To scan for malware by comparing files to a database of known malware and alert users to quarantine or delete threats.

Name two forms of anti-malware software.

Name two forms of anti-malware software.

Anti-virus and anti-spyware software.

What is authentication?

What is authentication?

The process of verifying a user's identity before granting system access.

Give three common methods of authentication.

Give three common methods of authentication.

Usernames and passwords, biometric data, and two-step verification.

Why is automating software updates important?

Why is automating software updates important?

It keeps software up-to-date with security patches, reducing vulnerabilities without needing manual action.

How can checking the spelling and tone of messages help users?

How can checking the spelling and tone of messages help users?

It helps identify phishing attempts, which often have spelling mistakes or unusual (typically demanding) language.

Why should users check the URL attached to a link before clicking?

Why should users check the URL attached to a link before clicking?

To ensure it leads to a legitimate site and avoid phishing attacks using fake URLs.

What is the role of a firewall?

What is the role of a firewall?

To scan incoming and outgoing network traffic and block or allow data based on security rules.

How do privacy settings help users?

How do privacy settings help users?

By controlling what personal information is shared and who can access it, protecting data from misuse.

What does a proxy server do?

What does a proxy server do?

Acts as an intermediary between a user and the internet, hiding the user’s IP address and filtering harmful content.

What is SSL and why is it important?

What is SSL and why is it important?

Secure Socket Layer is a protocol that encrypts data between a browser and web server to protect sensitive information from interception.

How can you tell if a website is using SSL?

How can you tell if a website is using SSL?

The URL starts with “https” and a padlock icon appears in the browser.