Cybersecurity | Revision Mat

Shoulder Surfing

- This type of attack uses direct observation to get information from a user.

- It is relatively simple to perform as it can involve standing next to someone and watching them as they fill out a form, or enter a PIN number.

SQL Injection

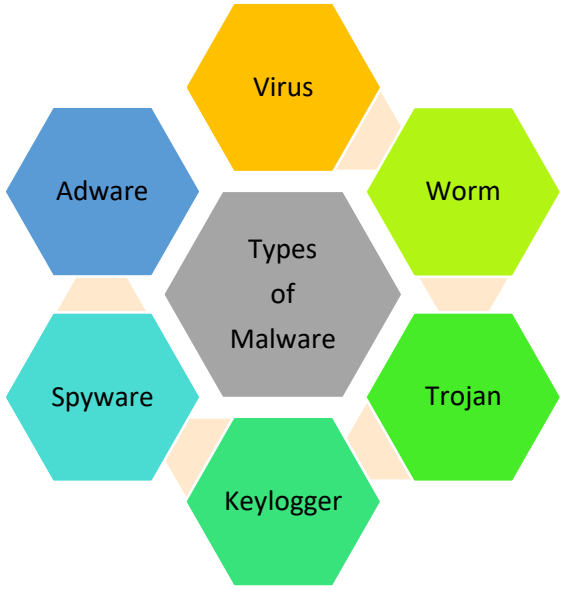
- This is a technique where malicious users can inject SQL commands into existing SQL statements.

- Injected SQL commands can alter SQL statements and compromise the security of information held in database systems.

DoS Attack

- This is a technique where malicious users can inject SQL commands into existing SQL statements.

- Injected SQL commands can alter SQL statements and compromise the security of information held in database systems.



Password-based

- The following types of password attacks can be carried out by an individual / computer program:

- Dictionary Attack
- Brute Force Attack
- Guess

IP Address Spoofing

- IP address spoofing involves an attacker changing the IP address of a website so that a visitor who types in the URL of a website is taken to a fraudulent website.

- The attacker can then use this website to steal sensitive data.

Social Engineering

- Social engineering involves tricking a user into giving out sensitive information such as a password by posing as a system administrator.

- This type of attack is normally carried out through phishing emails.

Methods of Protection Against Malware

- Virus Protection Software
- Firewall
- Operating System Updates
- Latest Version of Web Browsers
- Identify Phishing Emails

Methods of Identifying Vulnerabilities in Computer Systems

- Footprinting
- Ethical Hacking
- Penetration Testing
- Secure By Design

Cybersecurity refers to the range of measures that can be undertaken to protect computer systems, networks and data from unauthorised access or cyberattack. Cyberattacks are primarily carried out through the use of malware. Malware is the term used to describe malicious software. This type of software is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Cybersecurity | Glossary

Access levels
- User access levels are a method used on a network to determine what read and write permissions a user can have.

Encryption
- Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users.

Archiving
- Archiving is the process of storing data which is no longer in current or frequent use. It is held for security, legal or historical reasons.

Cybersecurity
- Cybersecurity refers to the range of measures that can be undertaken to protect computer systems, networks and data from unauthorised access or cyberattack.

Cyberattacks
- Cyberattacks are attacks carried out on a network by the use of malware.

Malware
- Malware is a term used to describe software which is designed to disrupt and potentially damage a computer system.

Virus
- A virus is a program that can replicate itself and spread from one system to another by attaching itself to host files.

Worm
- Worms are self-replicating programs that identify vulnerabilities in operating systems and enable a hacker to gain remote control of an infected computer system.

Trojan
- A Trojan is a program that appears to perform a useful function for a user, but also provides a 'backdoor' that enables data to be stolen.

Keyloggers
- This type of malware records the key presses from a user on a computer system. These records are then studied by a third party so that they can easily identify and exploit personal and sensitive data such as passwords.

Adware
- These programs inject adverts into pages and programs on a user's computer system with the aim that the creator would be able to get advertising revenue from the adware program.

Spyware
- Spyware is software which can be used to collect a user's data without their knowledge.

Virus protection software
- This is a piece of software that is loaded into memory when a computer system is running. It monitors activity the computer system for the signs of a virus infection.

Shoulder surfing
- Shoulder surfing involves using direct observation to get information.

SQL injection
- This is a technique where malicious users can inject SQL commands into existing SQL statements.

DoS attack
- A denial of service (DoS) attack doesn't attempt to break system security it attempts to make your website and servers unavailable to users.

Dictionary attack
- This type of password attack uses a simple file containing words found in a dictionary. This attack uses exactly the kind of words that many people use as their password.

Brute force attack
- This type of password attack is similar to a dictionary attack but is able to detect non-dictionary words by working through all possible alphanumeric. combinations from aaa1 to zzz10

IP address spoofing
- IP address spoofing involves an attacker changing the IP address of a website so that a visitor who types in the URL of a website is taken to a fraudulent website.

Social engineering
- Social engineering involves tricking a user into giving out sensitive information such as a password by posing as a system administrator.

Footprinting
- Footprinting involves gathering all available information about a computer system. A penetration tester should then be able to use this information to discover how much detail a potential attacker could find out about that computer system.

Cardiff University Prifysgol Caerdydd School of Computer Science and Informatics Ysgol Cyfrifiadureg a Gwybodeg
Undeb Ewropeaidd European Union Llywodraeth Cymru Welsh Government Cronfa Gymdeithasol Ewrop European Social Fund
Prifysgol Abertawe Swansea University
Cardiff University Prifysgol Caerdydd
Prifysgol Bangor University
Cardiff Metropolitan University Prifysgol Metropolitan Caerdydd
technocamps Inspiring | Creative | Fun Ysbrydoledig | Creadigol | Hwyl
i.t.wales
Prifysgol Aberystwyth University
Prifysgol Glyndŵr Wrecsam Wrexham Glyndŵr University
University of South Wales Prifysgol De Cymru
institute of CODING