SECURITY TOOLS

Computer security also known as cyber security is the protection of information systems from theft or damage to the hardware, the software and to the information on them, as well as from disruption of the services they provide.

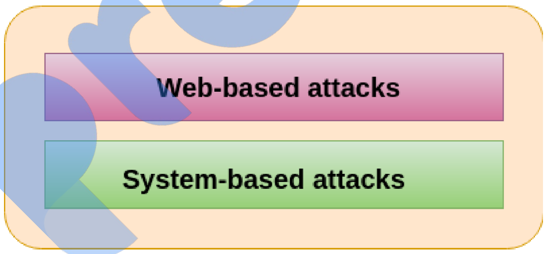
Internet security is a branch of computer security specifically related to not only Internet, often involving browser security and the World Wide Web. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information, which leads to a high risk of intrusion or fraud, such as phishing, online viruses, Trojans, worms and more. Many methods are used to protect the transfer of data, including encryption and from-the-ground-up engineering.

Security is based on the following issues:

- **Privacy:** The ability to keep things private/confidential.
- **Trust:** we trust data from an individual or a host.
- **Authenticity:** Are security credentials in order.
- **Integrity:** Has the system been compromised /altered already.

Types of attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. Attacks can be classified into the following categories:



Classification of Cyber attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows:

- **Injection attacks**
  - It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
  - Example- SQL Injection, code Injection; log Injection, XML Injection etc.
- **DNS Spoofing**
  - DNS spoofing is a type of computer security hacking whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or any other computer.

    - The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

- **Session Hijacking**
    - It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.
- **Phishing**
    - Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.
- **Brute force**
    - It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.
- **Denial of Service**
    - It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-
    - Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
    - Protocol attacks- It consumes actual server resources, and is measured in a packet.
    - Application layer attacks- Its goal is to crash the web server and is measured in request per second.
- **Dictionary attacks**
    - This type of attack stored the list of a commonly used password and validated them to get original password.
- **URL Interpretation**
    - It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.
- **File Inclusion attacks**
    - It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.
- **Man in the middle attacks**
    - It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

- A computer virus is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.
- A virus can be spread by opening an email attachment, clicking on an executable file, visiting an infected website or viewing an infected website advertisement. It can also be spread through infected removable storage devices, such USB drives.
- Once a virus has infected the host it has the capacity to corrupt or to delete data on your computer and it can utilize an email program to spread the virus to other computer systems. In the worst case scenario, it can even delete everything on your hard disk. The purpose of it is to disrupt the operation of the computer or the program.
- Ripper, Stuxnet, Petya, Wanna cry, Code red, Melissa, Sasser, Zeus, Mydoom, Crypto Locker, Flashback are some example of Viruses.

2. Computer Worm

- A computer worm is a malicious, self-replicating software program (malware) which affects the functions of software and hardware programs.
- Before widespread use of networks, computer worms were spread through infected storage media, such as floppy diskettes, which, when mounted on a system, would infect other storage devices connected to the victim system.
- USB drives are still a common vector for computer worms.

Differences between worms and viruses:

Computer worms "are self-replicating programs that spread with no human intervention after they are started." In contrast, "viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems."

3. Trojan horse

- Trojan horse or Trojan is any malware which misleads users of its true intent. Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.
- Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network.

- Ransomware attacks are often carried out using a Trojan. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create backdoors to give malicious users access to the system.
- Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

4. Malware

- Short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software.

5. Ransomware

- Ransomware is a type of malware program that infects and takes control of a system. It infects a computer with the intention of extorting money from its owner.

6. Spyware

- Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information. Spyware is classified as a type of malware designed to gain access to or damage your computer, often without your knowledge.
- Just like viruses, spyware can be installed when you open an e-mail attachment containing the malicious software or through cookies. It can also be installed when you install another program that has a spyware installer attached to it.

7. Adware

- Adware, or advertising-supported software, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process.
- The software may generate two types of revenue: one is for the display of the advertisement and another on a "pay-per-click" basis, if the user clicks on the advertisement.
- The software may implement advertisements in a variety of ways, including a static box display, a banner display, full screen, a video, pop-up ad or in some other form.

8. Key logger

- A key logger is a type of malware that stores all keystrokes of a computer. It can record all sorts of personal information, such as usernames, passwords, credit card numbers, and personal documents such as emails and reports.

9. Phishing

- Phishing is the fraudulent attempt to obtain access credentials such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
- Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

10. Spoofing

- A Spoofing attack is a situation in which one person or program successfully represents oneself as another by falsifying data and thereby gaining an illegitimate advantage.

11. Pharming

- Pharming is a cyber-attack intended to redirect a website's traffic to another, fake site.
- Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.
- DNS servers are computers responsible for resolving Internet names into their real IP addresses.
- Users of online banking and e-commerce websites are more prone to this attack.

Important Terms

1. **Anti-virus** software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, and adware.

2. **Firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules

3. **Authorization** is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy.

4. **Authentication** is the act of confirming the truth of an attribute of a single piece of data or entity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, Authentication often involves verifying the validity of at least one form of identification.

5. A person who uses his or her expertise to gain access to other people’s computers to get information illegally or do damage is a **Hacker**.

6. **Zombie** is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction.

7. **Breach** is the moment a hacker successfully exploits vulnerability in a computer or device, and gains access to its files and network.

8. **Bot/Botnet** is a type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected computers is known as a "botnet" and is controlled by the hacker or "bot-herder".

9. **Spam** is unwanted emails. In other words, we can call them as unsolicited promotional mail.

10. **Encryption** is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Good Computing Tips and Practices

- Minimize your storage of sensitive information.
- Protect your passwords and use those passwords that can be easily guessed by others.
- Protect your information while using the email and internet.
- Also, make sure that your computer has security patches and updates. Also, it should be protected with any kind of anti-virus.
- Furthermore, secure your mobile devices and laptops, computers all the time.
- Do not download or install any third party software or unknown programs.