19CSE311

Computer Security

S Abhishek

AM.EN.U4CSE19147

Malicious Code:

- Malicious code is a type of malicious computer programming that is used to generate or exploit system flaws.
- Malicious code allows an attacker to undesirable change, corrupt, harm, or persistent access to computer systems.
- Back doors, security breaches, data, and information theft, and other possible harms to files and computer systems may all be the consequence of malicious code.
- Malicious code is a hazard to application security that cannot be effectively addressed by traditional antivirus software alone.
- Malicious code is self-executing and can take the form of plug-ins, scripting languages, or other computer languages.
- Malicious code can infiltrate network storage and proliferate after it has gained access to your environment.

- Malicious software can provide a person with remote access to a machine which we can refer to as an application backdoor.
- Backdoors can be developed maliciously to obtain access to sensitive corporate or consumer information.
- They can, however, be developed by a programmer who needs rapid access to an application for debugging.
- They can also be formed accidentally as a result of programming faults.
- Visiting infected websites or clicking on a malicious email link or file are common ways for malicious codes to enter your system.
- The greatest defense is antivirus software with automatic updates, malware eradication capabilities, Web-browsing security, and the capacity to identify all forms of infestations.
- The computer virus is the most prevalent type of malicious code, infecting a computer by attaching itself to another program or software and then propagating when that program is executed.

Worm:

- Computer worms can transmit themselves from one machine to another automatically.
- They can replicate themselves.

- To spread, computer worms frequently rely on the behaviors of, and weaknesses in, networking protocols.
- When a computer worm loads and starts running on a freshly infected system, its primary goal is to stay active on the infected system for as long as feasible while spreading to as many additional vulnerable systems as possible.
- Exploiting software flaws makes worms easily enter into the system.
- They can easily transmit through email attachments or spam emails or even auto instant and redirect messages when a file is opened.
- The worm infiltrates the device without the user's knowledge once it has been installed.
- Worms are capable of deleting and editing files. They can potentially install more malicious software on a computer or other device.
- Sometimes the worm's primary objective is to replicate itself over and over again, wasting computer resources such as bandwidth or hard disc space.
- Worms may also steal sensitive files and pave a way for an attacker to get access to the machine by deploying a gateway.
- The worm, for instance, may transmit ransomware, viruses, or other malware, all of which inflict damage to afflicted computers.

Intruders:

- An incursion is any unauthorized and unlawful method of executing suspicious behavior on a data network.
- Individuals or part of an organized group frequently engage in cyber operations such as identity theft, financial credential theft, industrial espionage, data ransomware, phishing, and denial of service attacks in order to exploit system weaknesses for unlawful purposes.
- Intruders can be classified as cyberactivists or hacktivists who fight for political or social reasons and steal all of the user's primary data and credentials.
- Intruders,
    - Investigate the company website for information on the business structure, staff, important systems, and particular web servers and operating systems utilized.
    - Obtain information about the target network by utilizing DNS lookup tools and other tools like NMAP.
    - Send a query email to the customer service contact, then examine the response for information on the email, client, server, and operating system used, as well as the details of the person responding.

  - Perform Privilege Escalation, Information misuse & System Exploitation, Managing Access and cover tracks.

- Intruders are classified as,
- **Masquerador :**
  - An attacker who poses as someone who is not a valid user and uses illicit ways to gain access to a legitimate user's account from the outside.
- **Misfeador :**
  - A genuine, authorised user who performs unlawful acts that provide the attackers with access to sensitive and confidential information and renders their system exposed to the attackers. This user is an insider.
- **Clandestine User :**
  - These users might come from both inside and outside.
  - These attackers gain system control over access in order to circumvent auditing, collection, and access constraints.

Thankyou!!