UNIT-7

Malicious Logic

⊛Malicious Logic:

It is a software program designed to damage or do other unwanted actions on a computer system. It is a set of instructions that cause a site's security policy to be violated. These are the most sophisticated types of threats to computer systems that exploit vulnerabilities.

Malicious software can be divided into two categories:

i) Independents: These are self-contained programs that can be scheduled and ran by the operating system. E.g. Worms, Zombie. etc.

ii) Needs host program: These are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program. E.g. Viruses, Trojan Horse, logic Bombs, Backdoors. etc.

⊛Types of Malicious logic:

1) Virus: A computer virus is a program that inserts itself into one or more files and then performs some actions. It can damage hardware, software or files.

Phases of virus:

i) Dormant phase: The virus is idle at this phase, waiting for trigger event.

ii) Propagation phase: The virus places an identical copy of itself into another programs.

iii) Trigging phase: The virus is actived to perform the function for which it was intended.

iv) Execution phase: The desired function is performed such as message on the screen, damaging the programs and data files etc.

Types of viruses:

i) Parasitic virus: It attaches itself to executable files and replicates when the infected program is executed.

ii) Memory-resident virus: It stays in the main memory and infects every program that executes.

iii) Boot sector virus: Infects a boot record and spreads when the system is booted from the disk containing virus.

iv) Stealth virus: A virus explicitly designed to hide itself from antivirus software.

v) Polymorphic virus: A virus that mutates with every infection, making detection very difficult.

2) Worms:

A computer worm is a self-replicating program that copies itself from one computer to another. It uses a computer network to send copies of itself to other nodes and do so without any user intervention. It searches for servers with security holes and copies itself here.

Email worm and internet worms are the two most common worm.

i) Email worm:

→ Email worm goes into a user's contact/address book and chooses every users in that contact list.

→ It then copies itself and puts itself into an attachment; then the user will open the attachment and the process will start over again.

ii) Internet worm:

→ Internet worm scans the computer for open internet ports that the worm can download itself into the computer.

→ Once inside the computer the worm scans the ~~computer~~ internet to infect more computers.

3> Trojan Horse:

A trojan horse is a program with an known look and a unwanted effect. It performs a desired task but also performs unexpected functions. It requires human action to run, it does not self-replicate.

Types:

i) Remote Access Trojan: A Trojan horse designed to provide the attacker with complete control of victim's system.

ii) Data Sending Trojan: A Trojan horse that is designed to provide the attacker with sensitive data such as passwords.

iii) Destructive Trojan: A type of trojan horse designed to destroy and delete files.

iv) Proxy Trojan: A type of trojan horse designed to use the victim's computer as a proxy server.

v) Security Software Disable Trojan: A type of trojan horse designed to stop or kill security programs such as antivirus program without the user knowing.

4> Zombies:

Zombies are the program which secretly takes over another networked computer and force it to run under a common command and control infrastructure. Zombies has been used extensively to send email spam; between 50% to 80% of all spam worldwide is now sent by zombie computer.

5> Denial of Service (DOS) Attack:

A Denial of Service (DoS) attack is an attack where an attacker attempts to disrupt the services provided by a host, by not allowing it's intended users to access the host from the Internet. If the attack succeeds, the targeted computer will become unresponsive and nobody will be able to connect with it. The goal of DoS attack is not to gain unathorized access to machines or data, but to prevent legitimate users of a service from using it.

Typical aims of DoS attack:

→ Consuming bandwidth with large traffic volumes.

→ Overload or crash the network handling software.

→ Send specific types of packets to consume limited available resources.

⊗. Difference between Virus, Worms and Trojan Horse: [Imp]

Virus	Worm	Trojan Horse
i) A computer virus is a program that inserts itself into one or more files and then performs some actions.	i) A computer worm is a self-replicating program that copies itself from one computer to another.	i) A trojan horse is a program with an known look and unwanted effect.
ii) Virus replicates itself.	ii) Worms also replicate itself.	ii) Trojan horse does not replicate itself.
iii) It cannot be controlled remotely.	iii) It can be controlled remotely.	iii) It can also be controlled remotely.
iv) Spreading rate of viruses are moderate.	iv) Spreading rate of worms are faster than virus and Trojan horse.	iv) Spreading rate of Trojan horse is slow in comparision of both virus and worms.
v) It is used to modify the information.	v) It is used to halt the CPU and memory.	v) It is used to steal the user's information.

⊛. Intrusion:

Intrusion is any set of actions that attempts to compromise the confidentiality, integrity or availability of a computer resource.

⊛. Intruders:

An intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.

Three classes of intruders are as follows:

i) Masquerader → An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

ii) Misfeasor → A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized for such access but misuse his or her privileges.

iii) Clandestine user → An individual who seizes supervisory control of the system and uses his control to evade auditing and access controls or to suppress audit collection.

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

⊛. Intrusion Detection System (IDS): [Imp]

→ Intrusion detection is the process of identifying and responding to malicious activity targeted at resource.

→ IDS is a system designed to test/analyze network system traffic/events against a given set of parameters and alert/capture data when these threshold are met.

→ IDS uses collected information and pre-defined knowledge-based system to reason about the possibility of an intrusion.

→ IDS also provides services to cop with intrusion such as giving alarms, activating programs to try to deal with intrusion etc.

⊛. Approaches to Intrusion Detection:

1) **Statistical Anomaly Detection:** Statistical anomaly detection involves the collection of data relating to the behaviour of legitimate users over a period of time. Then statistical tests are applied to observed behaviour to determine with a high level of confidence whether the behaviour is not legitimate user behaviour. Statistical anomaly detection falls in two broad categories:

i) **Threshold detection:** Threshold detection involves counting the numbers of occurrences of specified event type over an interval of time.

ii) **Profile-based anomaly detection:** Profile-based anomaly detection focuses on characterizing the past behaviour of individual users or related groups of users and then detecting significant deviations.

2) **Rule-Based Detection:**

Rule-based detection involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of an intruder.

i) **Rule-based anamoly detection:** With rule-based anamoly detection, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns.

ii) **Rule-based penetration identification:** Rule-based penetration identification uses rules for identifying known penetrations or penetrations that would exploit known weaknesses.