Unit-VII
Malicious Logic

Malicious Logic

It is a software program designed to damage or do other unwanted actions on a computer system.

Malicious software can be divided into two categories:

- ***Independents:*** are self-contained program that can be scheduled and ran by the operating system. E.g. worms, zombie programs etc.
- ***Needs host program:*** are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program. E.g. viruses, logic bombs 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:

1. ***Dormant phase–*** the virus is idle, waiting for trigger event.
2. ***Propagation phase –*** the virus places an identical copy of itself into another programs.
3. ***Trigging phase –*** the virus is activated to perform the function for which it was intended.
4. ***Execution phase –*** the desired function is performed such as massage on the screen, damaging the programs and data files.

Types of viruses:

- ***Parasitic Virus:*** It attaches itself to executable files and replicates when the infected program is executed.
- ***Memory-resident Virus:*** Lodges in the main memory and infects every program that executes.
- ***Boot Sector Virus:*** Infects a boot record and spreads when the system is booted from the disk containing virus.
- ***Stealth Virus:*** A virus explicitly designed to hide itself from antivirus software.
- ***Polymorphic Virus:*** A virus that mutates with every infection, making detection very difficult.
- ***Metamorphic Virus:*** Mutates with every infection, rewriting itself completely at each iteration changing behavior or appearance, increasing the difficulty of detection.

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.

- ***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.

- ***Internet worm:***

- An internet worm is designed to be conspicuous to the user.
- The worm scans the computer for open internet ports that the worm can download itself into the computer.
- Once inside the computer the worms scans the internet to infect more computers.

Other types of worms:

- ***Instant Messaging Worm:*** Instant Messaging Worms spread by sending links to the contact list of instant messaging applications (messenger, WhatsApp, Skype etc.).
- ***File sharing Network Worm:*** File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

3. Trojan Horse

A Trojan horse is a program with an overt (known) look and a covert (unwanted) effect. It performs a desired task but also performs unexpected functions. It requires human action to run, do not self-replicate.

- A Trojan may give a hacker remote access to a targeted computer system.

Types:

- ***Remote Access Trojan:*** A Trojan horse designed to provide the attacker with complete control of victim's system.
- ***Data Sending Trojan:*** A Trojan horse that is designed to provide the attacker with sensitive data such as passwords.
- ***Destructive Trojan:*** A type of Trojan horse designed to destroy and delete files.
- ***Proxy Trojan:*** A type of Trojan horse designed to use the victim's computer as a proxy server.
- ***File Transfer Protocol (FTP) Trojan:*** A type of Trojan horse designed to open port 21 (the port for FTP transfer) and lets the attacker connect to your computer using FTP.
- ***Security Software Disable Trojan:*** A type of Trojan horse designed to stop or kill security programs such as antivirus program without the user knowing.
- ***Denial of Service (DOS) Trojan:*** A type of attack on a network that is designed to bring the network to its knees by flooding it without useless traffic.

4. Zombies

- The program which secretly takes over another networked computer and force it to run under a common command and control infrastructure.
- Infected computers - mostly Windows machines – are now the major delivery method of spam.
- Zombies have been used extensively to send e-mail spam; between 50 % to 80 % of all spam worldwide is now sent by zombie computer.
- Zombies are frequently used in denial-of-service attacks (DDoS), which refers to the saturation of websites with a multitude of computers accessing at the same time. As so many users are making requests at the same time to the server hosting the Web page, the server crashes, denying access to genuine users.

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 its 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 unauthorized 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.

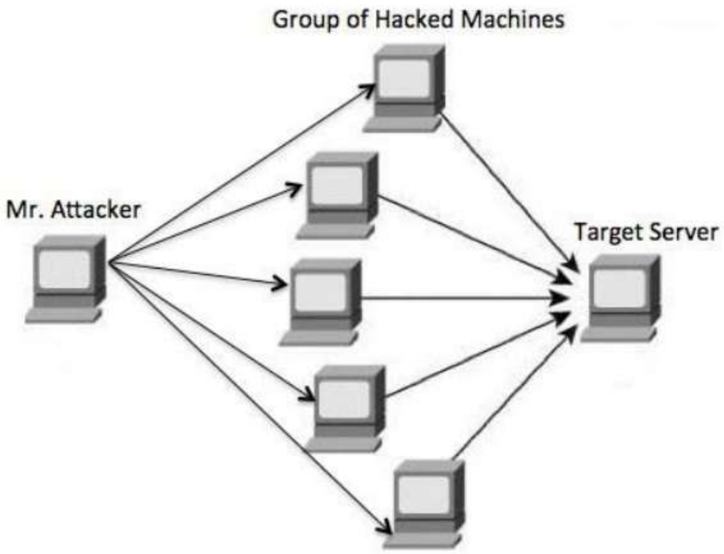
The two most common forms of DoS attacks are:

- ***Service Overloading:*** This may happen to servers for instance, if anyone write a small loop that sends continuous request for a particular file. The server tries to respond in good faith. It may also happen due to accidental infinite loops.
- ***Message Flooding:*** This occurs when someone send a very large file to a message box every few minutes. This message box rapidly grows in size and begins to occupy all the space on the disk and increases the number of receiving processes on the recipient's machine, trying it up even more and often causing a disk crash.

Distributed Denial of Service (DDoS) Attack

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service or a website unavailable by overloading it with huge floods of traffic generated from multiple sources.

Attackers build a network of hacked machines which are known as **botnets**, by spreading malicious piece of code through emails, websites, and social media. Once these computers are infected, they can be controlled remotely, without their owners' knowledge.



A DDoS flood can be generated in multiple ways. For example −

- Botnets can be used for sending more number of connection requests than a server can handle at a time.
- Attackers can have computers send a victim resource huge amounts of random data to use up the target's bandwidth.

Due to the distributed nature of these machines, they can be used to generate distributed high traffic which may be difficult to handle. It finally results in a complete blockage of a service.

Difference between Virus, Worms and Trojan Horse

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

Following are the examples of intrusions:

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Dialing into an unsecured modem and gaining internal network access

etc.

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:

1. **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.
2. **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.
3. **Clandestine user:** An individual who seizes supervisory control of the system and uses this 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)

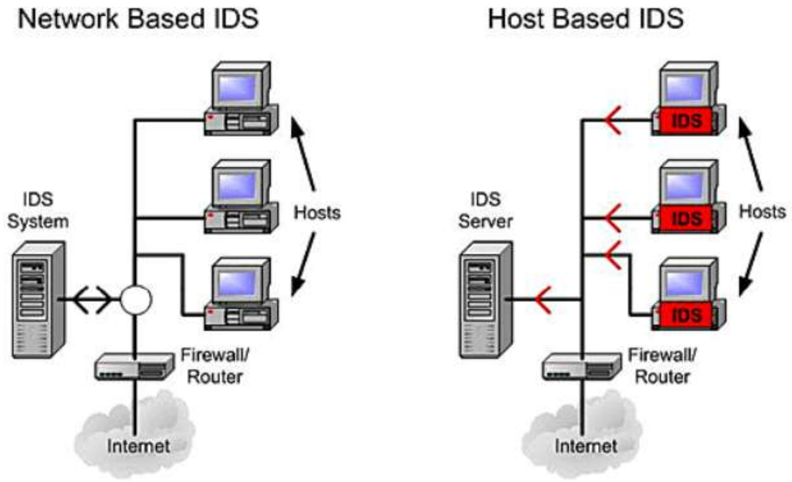
Intrusion detection is the process of identifying and responding to malicious activity targeted at resource.

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

IDS uses collected information and pre-defined knowledge-based system to reason about the possibility of an intrusion. It also provides services to cop with intrusion such as giving alarms, activating programs to try to deal with intrusion, etc.

Classification of Intrusion Detection System

- ***Host Intrusion Detection System (HIDS):*** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.
- ***Network Intrusion Detection System (NIDS):*** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.



Approaches to Intrusion Detection

Following approaches are used for intrusion detection:

- Statistical anomaly detection
- Rule-based detection

- ***Statistical Anomaly Detection:***

Statistical anomaly detection involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether the behavior is not legitimate user behavior.

Statistical anomaly detection falls into two broad categories:

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

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

- ***Rule-Based Detection:***

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

1. ***Rule-based anomaly detection:*** With rule-based anomaly detection, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privilege, time slot, terminals, and so on. Current behavior is the then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.
2. ***Rule-based penetration identification:*** Rule-based penetration identification uses rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage. Typically, the rules used in these systems are specific to the machine and operating system. Also, such rules are generated by "experts" rather than by means of an automated analysis of audit records.

Please let me know if I missed anything or anything is incorrect.

poudeljayanta99@gmail.com