# Chapter 6

# Malicious Software and Intrusion

## Table of Contents

Malicious Software ........................................................2
Virus and its phases ........................................................3
Virus Classification........................................................5
Worm, Worm Propagation Model, State of Worm Technology ........................................................7
Intrusion and Intruders........................................................9
Intrusion Detection System..............................................11
Analysis Approaches: Anomaly Based, Signature Based ........................................................14
Honeypot..............................................................18

# Malicious Software

Malicious software, also commonly referred to as **malware**, is any software program intentionally designed to harm a computer system or network.

These programs can be created by cybercriminals with various malicious goals, such as stealing data, disrupting operations, or holding your information hostage.

## Types of Malware:

- **Viruses:** These malicious programs replicate themselves and spread to other computers, often by attaching to files or emails. Once a virus infects a system, it can damage files, steal data, or slow down performance.
- **Worms:** Similar to viruses, worms can also spread quickly across networks. However, worms differ by replicating themselves independently, whereas viruses need to be attached to a program or file to spread. Worms can consume system resources and clog up networks.

- **Trojan horses (Trojans):** They pretend to be harmless software, like a game or a helpful program, but they actually do bad stuff when you use them.
- **Logical Bomb:** A logical bomb is a destructive program that performs an activity when a certain action has occurred. These are hidden in programming code. Executes only when a specific condition is met.
- **Spyware:** These programs are designed to spy on user activity without their knowledge. Spyware can steal sensitive information like passwords, browsing history, and financial data.

## Virus and its phases

A computer virus is a type of malicious software (malware) that spreads by inserting copies of itself into other programs or files.

**The phases of a computer virus:**

1. **Dormant Phase**: In this phase, the virus is idle and does not perform any malicious activity.

It's like the virus is just sitting quietly and not causing any harm.

2. **Propagation Phase**: This is when the virus starts spreading to other files or programs on your computer or across a network. It might do this by attaching copies of itself to other files, like how a real virus spreads from person to person.
3. **Triggering Phase**: At a certain point, often triggered by a specific event or condition (like a date, time, or user action), the virus becomes active. This phase is like the virus waking up and starting to do its bad stuff.
4. **Execution Phase**: Once triggered, the virus executes its malicious payload. This could mean deleting files, stealing information, or causing other harmful effects on your computer or device.
5. **Concealment Phase**: To avoid detection and removal, some viruses try to hide their presence on your system. They might change their code or use techniques to evade antivirus programs.

# Virus Classification

1. **Macro Viruses**:
   - These viruses are written in the same macro language used for software applications like Microsoft Word or Excel. They can spread through documents and perform actions such as deleting files or formatting hard drives.
2. **Logic Bomb**:
   - This type of malicious code is triggered by a specific condition or event, such as a particular date or the deletion of a certain file. Once triggered, it executes a harmful function, such as deleting files or corrupting data.
3. **Boot Sector Viruses**:
   - These viruses infect the boot sector of a hard drive, which is a crucial part of the drive that starts the computer. When the computer boots up, the virus gets loaded into memory and can spread to other disks and drives.

4. **Multipartite Viruses**:

    - These viruses can infect a computer in multiple ways, such as through boot sectors and executable files. They can spread and cause damage in several ways, making them harder to remove.

5. **Polymorphic Virus**:

    - This type of virus can change its code or appearance each time it infects a new system or file, making it difficult for antivirus software to detect it using signature-based methods.

6. **File Infectors**:

    - These viruses attach themselves to executable files (files that perform certain tasks or operations when run). When the infected file is run, the virus activates and can spread to other files and systems.

# Worm, Worm Propagation Model, State of Worm Technology

A computer worm is a type of malicious software (malware) that spreads independently across computer networks and systems.

Unlike viruses, worms do not need to attach themselves to existing files or programs to propagate.

Instead, they exploit vulnerabilities in network protocols or software to replicate themselves and spread to other computers.

## Worm Propagation Model

The worm propagation model describes how computer worms spread through networks and systems.

Here's a simplified explanation of the typical stages involved in the propagation of a worm:

1. **Discovery**: The worm starts by searching for vulnerable computers or systems on the network.

It may scan IP addresses or exploit known vulnerabilities in software or operating systems.

2. **Infection**: Once a vulnerable system is identified, the worm gains access and installs itself on that system. It can do this by exploiting security weaknesses such as unpatched software or weak passwords.
3. **Replication**: After infecting a system, the worm begins to replicate itself. It might create copies of its code or segments and attempt to spread to other computers or devices on the same network or connected networks.
4. **Propagation**: The worm continues to propagate by spreading to additional systems using various methods. This could include sending copies of itself through email, exploiting shared network resources, or leveraging other communication channels like instant messaging.
5. **Payload Activation**: Some worms have a payload—a malicious action they are designed to carry out. This could be deleting files, stealing data, launching denial-of-service attacks, or installing backdoors for future access.

6. **Covering Tracks**: To evade detection and removal, worms may attempt to cover their tracks by deleting or modifying logs, disabling security software, or using encryption to conceal their communication.

# Intrusion and Intruders

## Intrusion:

- An intrusion refers to the **unauthorized access** to a computer system or network. This can be a deliberate attempt to gain access for malicious purposes, or it could be an accidental breach by someone who shouldn't be there.
- Intrusions can happen in various ways, such as:
    - **Exploiting vulnerabilities:** Taking advantage of weaknesses in software, hardware, or network security to gain access.
    - **Social engineering:** Tricking or manipulating users into granting access or revealing sensitive information.
    - **Password cracking:** Using brute force or other methods to guess a valid password.

## Intruders:

- An intruder is the **individual or entity** who carries out the intrusion. These can be:
    - **Hackers:** Individuals with technical knowledge who may exploit systems for personal gain (financial or reputation), ideological reasons, or simply for the challenge.
    - **Cybercriminals:** Individuals or groups motivated by financial gain who may steal data, disrupt operations, or hold systems hostage for ransom.
    - **Malicious insiders:** Authorized users who misuse their access privileges for malicious purposes.
    - **Careless or uninformed users:** People who unintentionally compromise security through actions like clicking on phishing links or downloading malware.

# Intrusion Detection System

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations.

## Working of Intrusion Detection System(IDS)

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

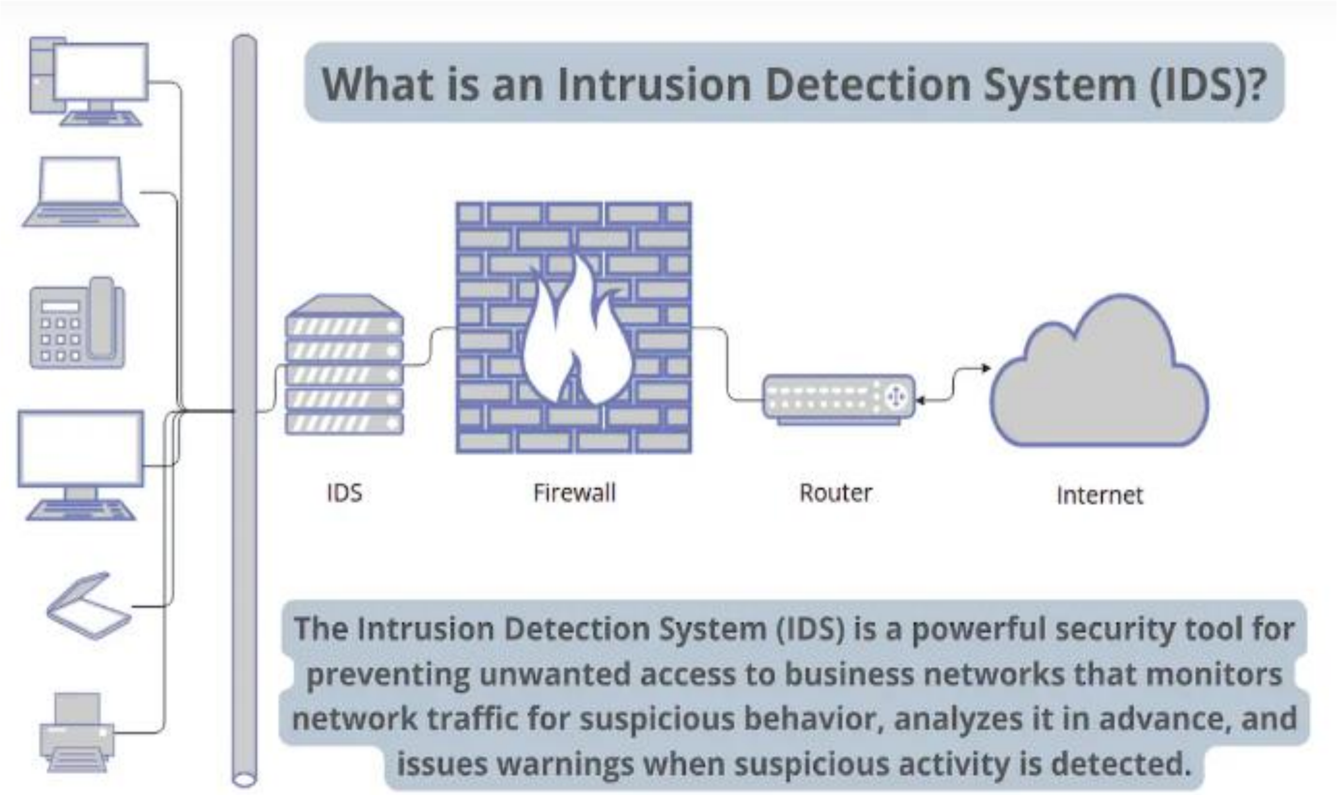
What is an Intrusion Detection System (IDS)?
IDS
Firewall
Router
Internet
The Intrusion Detection System (IDS) is a powerful security tool for preventing unwanted access to business networks that monitors network traffic for suspicious behavior, analyzes it in advance, and issues warnings when suspicious activity is detected.

Figure: functionality of an intrusion detection system

## Types of IDS:

1. **Network-Based IDS (NIDS)**:
   - Monitors network traffic in real-time to detect suspicious patterns or signatures indicative of attacks.
   - Positioned at strategic points within the network to analyze incoming and outgoing traffic.

  - Useful for detecting network-based attacks such as port scanning, denial-of-service (DoS) attacks, and network intrusion attempts.

2. **Host-Based IDS (HIDS)**:
   - Runs on individual hosts or servers to monitor activities occurring within the host's operating system and applications.
   - Focuses on detecting unauthorized access attempts, file modifications, privilege escalations, and other suspicious activities specific to the host.
   - Provides detailed visibility into the security status of individual systems.

3. **Detection Methods**:
   - **Signature-Based Detection**: Compares observed activities against a database of known attack patterns or signatures.
   - **Anomaly-Based Detection**: Establishes a baseline of normal behavior and alerts on deviations that may

indicate potential attacks or misuse.

- **Behavior-Based Detection**: Analyzes patterns of behavior to detect suspicious activities that do not match known attack signatures.

# Analysis Approaches: Anomaly Based, Signature Based

Anomaly-based and signature-based detection are the two fundamental approaches used in intrusion detection systems (IDS) to identify and alert about potential security threats.

### 1. Signature-Based Detection

Imagine a security guard who has a list of known criminals and checks IDs against that list. Signature-based detection works similarly:

- **Concept:** It relies on pre-defined patterns or "signatures" of known malicious activities, including specific network packets, file types, system calls, or code sequences associated with malware or attacks.
- **Detection Method:** The IDS continuously monitors network traffic or system logs and compares them against the signature database. If a match is found, it raises an alert, indicating a potential threat.
- **Advantages:**
    - **Fast and Efficient:** Matching signatures is a relatively quick process, allowing for real-time detection of known threats.
    - **High Accuracy:** For established attacks with well-defined signatures, this approach offers high accuracy in identifying threats.
    - **Low False Positives:** Since it relies on established patterns, there are fewer chances of flagging legitimate activity as suspicious.

- **Disadvantages:**
  - **Limited to Known Threats:** It can only detect threats with existing signatures in the database. New or zero-day attacks may go unnoticed.
  - **Signature Maintenance:** Security teams need to continually update the signature database to stay ahead of evolving threats.
  - **Potential for Evasion:** Cybercriminals can modify their attack methods to bypass known signatures.

### 2. Anomaly-Based Detection

Think of a security guard who monitors for unusual behavior, like someone lingering near a restricted area. Anomaly-based detection takes this approach:

- **Concept:** It establishes a baseline of normal activity for your network or system and identifies deviations from that baseline as potential threats.
- **Detection Method:** The IDS continuously analyzes network traffic, system logs, or resource usage patterns.

It then uses statistical algorithms or machine learning techniques to identify activities that significantly deviate from the established norm.

- **Advantages:**
  - **Detects Unknown Threats:** This approach can identify new or zero-day attacks that don't have known signatures.
  - **Adapts to Changing Environment:** As your network usage patterns evolve, the baseline automatically adjusts, improving detection accuracy over time.
- **Disadvantages:**
  - **Higher False Positives:** Deviations from the norm might not always indicate an attack, leading to wasted time investigating false alarms.
  - **Configuration and Tuning:** Setting up the baseline and fine-tuning anomaly detection algorithms can be complex and require expertise.
  - **Slower Detection:** Analyzing complex patterns for anomalies can take longer than signature matching.

# Honeypot

Honeypot is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers.

It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

Honeypots are mostly used by large companies and organizations involved in cybersecurity.

It helps cybersecurity researchers to learn about the different type of attacks used by attackers.

The **cost of a honeypot** is generally **high** because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources still preventing attacks at the backend and access to any production system.

A **honeynet** is a combination of two or more honeypots on a network.

## Types of Honeypot:

Honeypots are classified based on their deployment and the involvement of the intruder.

Based on their deployment, honeypots are divided into :

1. **Research honeypots-** These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.
2. **Production honeypots-** Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.