Introduction to Malware Analysis

Aprenderemos:

- What malware means and its role in the cyber-attacks
- Malware analysis and its significance in digital forensics
- Different types of malware analysis
- Setting up the lab environment
- Various sources to obtain malware samples

What is Malware?

Malware is a code that performs malicious actions. It generally gets into your PC without wour consent and performs covert actions like:

- Disrupting computer operations
- Stealing sensitive information
- Unauthorized access to victim's system
- Spying on the victim
- Sending spam emails
- Engaging in DDOS attacks
- Ransomware

Types of malware

- **Virus / worm:** Capable of spreading itself and copying to other computers (Virus needs human intervention, worm does not)
- **Trojan:** Malware that disguises itself as another program to trick users to install it in their system
- **Backdoor / RAT:** Trojan that enables the attacker to access infected computer
- **Adware:** Malware that presents unwanted ads to the user
- **Botnet:** Group of computers infected with the same malware waiting to recieve instructions from the command and control server
- **Information stealer:** Malware designed to steal sensitive data (Keyloggers, spyware, sniffers)
- **Ransomware:** Malware that holds the system on ransom by locking users out of the computer by encrypting files
- **Rootkit:** Malware that provides the attacker with priviledged access to the infected system
- **Downloader or dropper:** Malware designed to download additional malware components

What is Malware Analysis?

The study of Malware's behavior. The objective is to understand the working of malware and how to detect and eliminate it.

Why Malware Analysis?

To extract information from the malware sample, wich can help in responding to a malware incident. The goal is to: Determine the capability of a Malware, detect it and contain it.

Types of Malware Analysis

- **Static analysis:** Analysis of a binary without executing it
- **Dynamic analysis:** Executing suspected malware in a isolated environment and monitor it's behavior
- **Code analysis:** Advanced technique focused on analyzing the code to understand the inner workings of the binary
- **Memory analysis:** Analysis of the computer's RAM for forensic artifacts