Malware Analysis

Malware analysis is the process of analyzing a malware sample/binary and extracting as much information as possible from it. The information we extract helps us understand the scope of the functionality of the Malware, how the system was infected with the malware and how to defend against similar attacks in the future

Objectives of Malware Analysis

- ✓ To understand the type of malware and the entire scope of what it can do (functionality). Is it a Keylogger, RAT or Ransomware?
- ✓ How the system was infected with the malware. Is it a targeted attack or a phishing attack?
- ✓ How it communicates with the attacker.
- ✓ To exfiltrate useful indicators like registry entries/keys and filenames for the purpose of generating signatures that can be used to detect future detection.

Types of Malware Analysis

Static analysis – This is the process of analysing malware without executing or running it. The objective is to extract as much metadata from the malware as possible. Example; strings, PE headers.

Dynamic analysis – This is the process of executing malware and analyzing it's functionality and behaviour. The objective is to understand exactly how and what the malware does during the execution. This is done in a debugger.

Code Analysis – This is the process of analyzing/reverse engineering assembly code. This can be both statically and dynamically done (Static and dynamic code analysis)

Behavioural analysis – This is the process of analyzing and monitoring the malware after execution. It involves monitoring the processes, registry entries and network monitoring to determine the workings of the malware.

THANKS