SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit V- **CYBER ANALYSIS**
Topic :Malware analysis

- Malware Analysis is the practice of determining and analyzing suspicious files on endpoints and within networks using dynamic analysis, static analysis, or full reverse engineering.

- Malware analysis is the process of examining malicious software, commonly known as malware, to understand its functionality, behavior, and impact on a system.

- The primary goal of malware analysis is to gain insight into the malware's inner workings, identify its purpose, and develop strategies to detect, mitigate, and remove it.

There are generally three main approaches to malware analysis:

1. Static Analysis

This analysis involves **examining the malware without executing it**.

It **focuses on inspecting the file's structure, code, and other characteristics to identify potential malicious behaviors.**

Static analysis techniques include examining **file headers, extracting embedded strings, analyzing metadata, and disassembling or decompiling** the code to understand its logic.

2.Dynamic Analysis

Dynamic analysis involves **executing the malware in a controlled environment**, such as a virtual machine or sandbox, to observe its behavior.

During execution, the **analyst monitors system activities, network traffic, file system changes, and API calls made by the malware.**

This approach helps identify the malware's actions, such as file modifications, network communication, registry changes, and processes created or terminated.

3. Hybrid Analysis

Hybrid analysis combines both static and dynamic analysis techniques to **gain a comprehensive understanding of the malware**.

It provides a more detailed view of the malware's behavior by analyzing the static properties and characteristics before executing it in a controlled environment.

Tools commonly used in malware analysis include:

- Disassemblers and decompilers: Tools like IDA Pro, Ghidra, or Radare2 help analyze the assembly code of malware samples.

- Sandboxes and virtual machines: Tools like Cuckoo Sandbox, FireEye Malware Analysis, or VMware allow for safe execution of malware samples in controlled environments.

- Network analysis tools: Wireshark, tcpdump, or NetworkMiner help capture and analyze network traffic generated by malware.

- Debuggers: Tools like OllyDbg, WinDbg, or GDB help analyze the behavior of malware during runtime by stepping through the code and inspecting memory.

Any Query????

Thank you……