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 :19SB701 PATTERN RECOGNITION TECHNIQUES IN CYBER CRIME

IV YEAR / VII SEMESTER

Unit IV- **MALWARE ANALYSIS AND NETWORK TRAFFIC ANALYSIS**

Topic :Malware Analysis Defining

Malware Analysis refers to the process of examining and understanding malicious software (malware) to determine its behavior, purpose, and impact on systems.

The goal is to gain insights into how the malware operates, how it spreads, and how to defend against it.

This analysis is crucial for developing effective countermeasures and improving cyber security.

Key Objectives of Malware Analysis:

1.Identify the Type and Purpose of Malware:

1. Understanding what kind of malware it is (e.g., virus, worm, ransomware, trojan) and what its intended effect is (e.g., data theft, system disruption, unauthorized access).

2.Determine the Malware's Behavior:

1. Analyzing how the malware interacts with the system, what changes it makes, and what external connections it establishes.

3. Develop Countermeasures and Remediation Strategies:

Creating and deploying security solutions to prevent infection and mitigate the impact of the malware.

4.Extract Indicators of Compromise (IOCs): Identifying patterns, signatures, or artifacts associated with the malware to improve detection and response.

5.Understand the Attack Vectors: Learning how the malware was introduced to the system, whether through phishing, exploit kits, or other methods.

Types of Malware Analysis:

1.Static Analysis:

1. **Definition:** Examining the malware without executing it. This involves analyzing the code, binaries, and metadata.
2. **Techniques:** Disassembly, decompilation, and examining file properties.
3. **Pros:** Safe to perform since it doesn't require execution of the malware.
4. **Cons:** May not reveal all behaviors, especially if the malware uses obfuscation or anti-analysis techniques.

Dynamic Analysis:

- **Definition:** Observing the malware in a controlled environment (sandbox) to see how it behaves during execution.
- **Techniques:** Monitoring system calls, file modifications, network activity, and process behavior.
- **Pros:** Provides insights into the real-time behavior and impact of the malware.
- **Cons:** Requires a safe environment and can be time-consuming

Hybrid Analysis:

- **Definition:** Combining static and dynamic analysis to gain a comprehensive understanding of the malware.
- **Techniques:** Using both code examination and behavioral monitoring.
- **Pros:** Provides a fuller picture of the malware's capabilities and behavior.
- **Cons:** More complex and resource-intensive than individual methods

Common Malware Types:

1.Virus:

1. **Definition:** A type of malware that attaches itself to a legitimate file or program and spreads to other files or systems.
2. **Impact:** Can corrupt or delete files, and spread to other systems.

Worm:

Definition: A self-replicating malware that spreads across networks without user interaction.

Impact: Can cause network congestion, system overload, or unauthorized data access.

Ransomware:

Definition: Malware that encrypts the victim's data and demands a ransom for decryption.

Impact: Results in data loss and operational disruption until the ransom is paid.

Trojan Horse (Trojan):

Definition: Malware disguised as legitimate software, which performs malicious actions once installed.

Impact: Can lead to unauthorized access, data theft, or system compromise.

Spyware:

Definition: Malware designed to collect and transmit user information without their consent.

Impact: Leads to privacy violations and data theft.

Adware:

Definition: Malware that displays unwanted advertisements, often bundled with legitimate software.

Impact: Can degrade system performance and user experience.

Any Query????

Thank you……