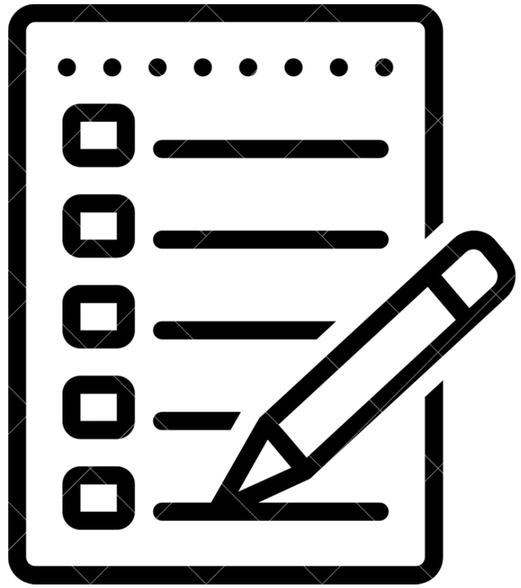
Malware Analysis: Introduction

Presented by Gaurav singh

Agenda

- What is malware?
- Types of malware
- How malware spreads
- Malware analysis techniques
- Tools for malware analysis
- Challenges of malware analysis
- Conclusion



What is malware?

- Malicious software designed to harm a computer system or network
- Can take many forms, including viruses, worms, Trojans, and ransomware
- Purposes: steal data, damage systems, disrupt operations, gain unauthorized access
- Constantly evolving, authors use vague techniques to make it difficult to analyze

Can be classified into two main categories:

- Host-based malware: targets the operating system or applications running on a host machine
- Network-based malware: targets the network infrastructure

Types of malware

- Viruses: replicate themselves and spread from one computer to another
- Worms: can spread themselves over a network without human intervention
- Trojans: disguise themselves as legitimate programs
- Ransomware: encrypts a victim's files and demands a ransom payment to decrypt them
- Spyware: collects information about a victim without their knowledge
- Adware: displays unwanted ads
- Botnets: networks of infected computers that can be controlled by a remote attacker

- Rootkits: give an attacker full control of a system
- Keyloggers: record a victim's keystrokes
- Backdoors: allow an attacker to gain unauthorized access to a system
- Phishing emails: trick victims into clicking on malicious links or opening infected attachments
- Drive-by downloads: infect a system when a victim visits a malicious website
- Exploits: take advantage of vulnerabilities in software to gain unauthorized access

How malware spreads

- Email attachments
- File sharing networks
- Social engineering
- Drive-by downloads
- Exploits
- Physical media
- Infected websites
- Malicious advertisements
- Untrusted software
- Malware-infected removable devices
- Peer-to-peer file sharing
- Spam emails
- Phishing attacks

Malware analysis techniques

- Static analysis: Analyzing the malware's code without executing it
- This can be done by decompiling the code into assembly language or by using a disassembler
- Dynamic analysis: Executing the malware in a controlled environment and observing its behavior
- This can be done in a virtual machine or in a sandbox
- Hybrid analysis: Combining static and dynamic analysis
- This can be done by first performing static analysis to identify suspicious code patterns, and then executing the malware in a controlled environment to confirm the findings

Tools for malware analysis

- **Disassemblers**: Decompile malware code into assembly language
- **Debuggers**: Step through malware code line by line
- **Virtual machines**: Create a safe environment to execute malware
- **Honeypots**: Trap malware-infected machines
- **sandboxes**: Execute malware in a controlled environment
- **Malware analysis frameworks**: Provide a set of tools and utilities for malware analysis
- **Threat intelligence platforms**: Provide information about malware threats

Challenges of malware analysis

- Malware is constantly evolving
- Malware authors use vague techniques to make it difficult to analyze their code
- Malware can be hidden in legitimate files and applications
- Malware analysis is a time-consuming and labor-intensive process
- There is no single silver bullet for malware analysis

Conclusion

- Malware analysis is a critical skill for anyone who wants to protect themselves from cyber threats
- By understanding how malware works, you can better defend yourself against it

THANKYOU