UNIT 6

1. **Malware Definition:**
    - **Malware is any software intentionally designed to harm, exploit, or perform unauthorized actions on a system or network.**
    - **Types include viruses, worms, trojans, ransomware, spyware, adware, etc.**

2. **Common Techniques for Malware Spread:**
    - **Phishing: Fake emails/websites designed to trick users into providing sensitive information or executing malicious payloads.**
    - **Exploiting Vulnerabilities: Attackers exploit flaws in software or hardware (e.g., unpatched systems) to gain unauthorized access.**
    - **Drive-by Downloads: Malware is downloaded onto a device when a user visits a compromised website.**
    - **Social Engineering: Manipulating individuals to execute malicious actions, like opening a file or clicking a link that spreads malware.**
    - **USB Drives: Infected USBs are used to transfer malware when plugged into a system.**
    - **Malvertising: Malware spread through malicious advertisements that exploit ad networks or browser vulnerabilities.**

3. **Malware Forensics Fundamentals:**
    - **Malware forensics focuses on understanding how malware works, how it spreads, and how to detect and mitigate its effects.**
    - **It includes analyzing logs, system traces, network traffic, and file properties to track the origin and behavior of malware.**

4. **Types of Malware Analysis:**
    - **Static Analysis: Involves analyzing the code or binary of malware without executing it. It's about disassembling and decompiling the malware to inspect its structure, dependencies, and functionality.**
    - **Dynamic Analysis: Involves executing the malware in a controlled environment (like a sandbox) to observe its behavior, interactions with the system, and changes made (e.g., files, processes, registry entries, network connections).**

5. **Static Malware Analysis:**
    - **Examines the malware code and its structure without running it.**
    - **Look for suspicious functions, hidden payloads, obfuscation techniques (e.g., encryption or packing), and indicators of malicious intent.**
    - **Tools: IDA Pro, Ghidra, OllyDbg, PEview, and VirusTotal.**

6. **Suspicious Word/PDF Document Analysis:**
    - **Word Documents: Malicious macros can be embedded in Word documents to execute code when the document is opened.**
        - **Look for macros that try to exploit vulnerabilities (e.g., CVE exploits) or call external scripts.**
    - **PDF Files: These files can contain embedded JavaScript or other exploit code that runs when opened.**
        - **Check for unusual embedded objects or scripts that might trigger malicious activities.**

7. **Dynamic Malware Analysis:**
    - **Focuses on observing how malware interacts with the system and network during execution.**
    - **Track system changes like file creation, process initiation, registry edits, network requests, and connections to remote servers.**
    - **Tools: Cuckoo Sandbox, Process Monitor, Wireshark, Sysinternals Suite, Regshot.**

8. **Real-Time System Behavior Analysis:**
    - **In real-time analysis, the goal is to monitor malware's impact on the system, including:**
        - **File system changes: New files created or existing ones modified/deleted.**
        - **Process behavior: New processes launched or altered by the malware.**
        - **Registry alterations: Changes to the system registry, often to maintain persistence or hide traces.**
        - **Persistence: Malware tries to survive reboots by creating autorun keys or modifying startup files.**

9. **Real-Time Network Behavior Analysis:**
    - **Focus on tracking any communication between the infected system and external servers (e.g., command-and-control servers).**
        - **Monitor for unusual DNS queries, HTTP requests, or connections on non-standard ports.**
        - **Look for signs of data exfiltration or lateral movement within a network.**
    - **Tools: Wireshark, TCPDump, NetworkMiner.**

10. **Fileless Malware Attacks:**
    - **Fileless malware operates directly in memory and does not require files to infect a system, making detection harder.**
    - **These attacks typically leverage legitimate system tools like PowerShell, Windows Management Instrumentation (WMI), or macros to execute malicious code in memory.**
    - **Common Indicators: Unusual command-line activity, scripts running without file creation, and system processes being used in unexpected ways.**
    - **Detection: Monitor for abnormal behavior in system utilities, unexpected scripts, or process injection.**

Important MCQ

1. What is the primary purpose of malware?

a) To improve system performance
b) To cause harm or exploit a system
c) To optimize network speed
d) To monitor network traffic

Answer: b) To cause harm or exploit a system

2. Which of the following is a common way malware spreads through emails?

a) Phishing
b) Data exfiltration
c) Port scanning
d) Denial of service

Answer: a) Phishing

3. What technique do attackers commonly use to exploit software vulnerabilities?

a) Social engineering
b) Buffer overflow
c) Man-in-the-middle attacks
d) Encryption

Answer: b) Buffer overflow

4. What is the primary goal of malware forensics?

a) To improve system performance
b) To analyze system logs for errors
c) To understand how malware works and how it spreads
d) To recover deleted files

Answer: c) To understand how malware works and how it spreads

5. Which of the following is an example of static malware analysis?

a) Running malware in a sandbox
b) Analyzing system logs for behavior
c) Disassembling malware to inspect its code
d) Monitoring network traffic

Answer: c) Disassembling malware to inspect its code

6. Which tool is commonly used for static analysis of malware?

a) Wireshark
b) Cuckoo Sandbox
c) Ghidra
d) Process Monitor

Answer: c) Ghidra

7. What type of malware analysis involves running malware in a controlled environment?

a) Static analysis
b) Dynamic analysis
c) Behavioral analysis
d) Memory analysis

Answer: b) Dynamic analysis

8. What is the main goal of dynamic malware analysis?

a) To reverse engineer the malware code
b) To observe the behavior of malware during execution
c) To identify encryption methods used in malware
d) To determine the origin of malware

Answer: b) To observe the behavior of malware during execution

9. Which behavior does fileless malware typically exhibit?

a) It requires a file to execute
b) It executes directly in memory without creating files
c) It uses traditional file-based exploits
d) It installs itself as a system file

Answer: b) It executes directly in memory without creating files

10. In static malware analysis, what is typically examined?

a) System behavior
b) Code structure and functions
c) Network traffic
d) User actions

Answer: b) Code structure and functions

11. Which of the following can be considered a social engineering technique?

a) Exploiting software vulnerabilities
b) Malvertising
c) Phishing
d) Drive-by downloads

Answer: c) Phishing

12. Which tool is used to monitor real-time system behavior during dynamic analysis?

a) Wireshark
b) Regshot
c) Process Monitor
d) Ghidra

Answer: c) Process Monitor

13. What is the role of Cuckoo Sandbox in malware analysis?

a) To capture and analyze network traffic
b) To disassemble malware code
c) To simulate malware execution in a safe environment
d) To recover deleted files from malware

Answer: c) To simulate malware execution in a safe environment

14. Which behavior would you typically monitor in dynamic malware analysis?

a) File system changes
b) User login attempts
c) Hardware performance metrics
d) Network speed

Answer: a) File system changes

15. What kind of malware often hides in system memory without creating files on disk?

a) Rootkit
b) Ransomware
c) Fileless malware
d) Worms

Answer: c) Fileless malware

16. How does malware typically maintain persistence on a system?

a) By modifying system logs
b) By using system administration tools
c) By creating auto-start entries in the registry
d) By deleting system files

Answer: c) By creating auto-start entries in the registry

17. What is a key feature of drive-by downloads?

a) They require user interaction to execute
b) They occur when malware is downloaded without user knowledge during website visits
c) They are spread via USB drives
d) They require opening an infected email attachment

Answer: b) They occur when malware is downloaded without user knowledge during website visits

18. What is commonly targeted in malvertising attacks?

a) System vulnerabilities
b) Network servers
c) Advertising networks
d) File-sharing services

Answer: c) Advertising networks

19. Which of the following actions is associated with network malware analysis?

a) Disassembling the malware code
b) Monitoring file creation
c) Capturing and analyzing network traffic
d) Reversing encryption techniques

Answer: c) Capturing and analyzing network traffic

20. In malware forensics, what is the purpose of analyzing system logs?

a) To check for errors in system performance
b) To determine how malware affected system resources
c) To inspect encryption methods used by malware
d) To recover deleted files

Answer: b) To determine how malware affected system resources

21. What is a trojan?

a) A virus that replicates itself
b) A type of ransomware
c) A malware that disguises itself as legitimate software
d) A tool used for network penetration

Answer: c) A malware that disguises itself as legitimate software

22. Which of the following is a characteristic of ransomware?

a) It spreads through infected email attachments
b) It encrypts user files and demands a ransom for decryption
c) It destroys files without any recovery options
d) It silently monitors user activities

Answer: b) It encrypts user files and demands a ransom for decryption

23. Worms are distinguished from other types of malware by:

a) Their ability to self-replicate and spread without user interaction
b) Their encryption methods
c) Their ability to remain undetected in system memory
d) Their reliance on human action for execution

Answer: a) Their ability to self-replicate and spread without user interaction

24. What is sandboxing used for in malware analysis?

a) To monitor CPU usage
b) To safely execute malware and observe its behavior
c) To recover encrypted files
d) To analyze network traffic

Answer: b) To safely execute malware and observe its behavior

25. Which behavior is typical of spyware?

a) Stealing sensitive data without the user's knowledge
b) Encrypting files and demanding payment
c) Exploiting system vulnerabilities
d) Displaying fake antivirus warnings

Answer: a) Stealing sensitive data without the user's knowledge

26. SQL injection is an example of:

a) A fileless malware attack
b) A vulnerability exploitation technique
c) A network malware analysis technique
d) A method of social engineering

Answer: b) A vulnerability exploitation technique

27. What does a rootkit do?

a) Encrypts data to hold it hostage
b) Deletes files from the system
c) Hides its presence to avoid detection by antivirus software
d) Destroys system files to cause crashes

Answer: c) Hides its presence to avoid detection by antivirus software

28. Which of the following best describes the behavior of adware?

a) It encrypts the user's data
b) It collects and sends data to a remote server
c) It displays unwanted advertisements to the user
d) It monitors user keystrokes

Answer: c) It displays unwanted advertisements to the user

29. What kind of analysis focuses on the execution behavior of malware in real-time?

a) Static analysis
b) Dynamic analysis
c) Memory analysis
d) File integrity monitoring

Answer: b) Dynamic analysis

30. Which of the following is a fileless malware attack tool?

a) PowerShell
b) Ransomware
c) Trojan horse
d) Virus

Answer: a) PowerShell

31. What is the main advantage of dynamic malware analysis over static analysis?

a) It is faster
b) It does not require running the malware
c) It can reveal real-time system and network behavior
d) It is easier to perform

Answer: c) It can reveal real-time system and network behavior

32. What would Wireshark be used for in malware analysis?

a) To recover deleted files
b) To disassemble malware code
c) To monitor and analyze network traffic
d) To execute malware in a sandbox

Answer: c) To monitor and analyze network traffic

33. How can fileless malware avoid detection by traditional antivirus software?

a) By encrypting its files
b) By hiding in system memory without creating files on disk
c) By using legitimate system tools like PowerShell
d) By sending fake alerts

Answer: b) By hiding in system memory without creating files on disk

34. What is an indicator that malware might be using PowerShell for execution?

a) An increase in system file activity
b) An unknown process running in the background
c) Command-line scripts executing on the system
d) Sudden internet connection drops

Answer: c) Command-line scripts executing on the system

35. In the context of malware, what does persistence refer to?

a) The ability of malware to avoid detection
b) The ability of malware to maintain its presence after a system reboot
c) The process of decrypting files
d) The ability of malware to monitor network traffic

Answer: b) The ability of malware to maintain its presence after a system reboot

36. What type of malware typically uses social engineering tactics to spread?

a) Worms
b) Trojans
c) Ransomware
d) Spyware

Answer: b) Trojans

37. What is the primary function of Wireshark in network-based malware analysis?

a) Analyzing and capturing network traffic to identify malicious activity
b) Monitoring system processes
c) Scanning files for malware
d) Reversing malware code

Answer: a) Analyzing and capturing network traffic to identify malicious activity

38. What is a key characteristic of polymorphic malware?

a) It stays hidden by disguising itself and changing its code with each infection
b) It never replicates
c) It encrypts files
d) It only infects mobile devices

Answer: a) It stays hidden by disguising itself and changing its code with each infection

39. Which of the following is a keylogger used for?

a) To encrypt data
b) To monitor and record keystrokes on a system
c) To collect email passwords
d) To cause a denial-of-service attack

Answer: b) To monitor and record keystrokes on a system

40. Botnets are often used for:

a) Encrypting data
b) Distributed denial-of-service (DDoS) attacks
c) Stealing user credentials
d) Data exfiltration

Answer: b) Distributed denial-of-service (DDoS) attacks

41. Which of the following is an example of a network-based malware detection technique?

a) Monitoring system logs for unusual activities
b) Capturing suspicious DNS requests
c) Scanning memory for active malware processes
d) Analyzing file integrity

Answer: b) Capturing suspicious DNS requests

42. What is a common sign that malware is using fileless tactics?

a) Files are being created in the system
b) Antivirus software is unable to detect the malware in the system file system
c) The system is running slow due to a high CPU usage
d) The system is displaying a ransom note

Answer: b) Antivirus software is unable to detect the malware in the system file system

43. What is the role of Command-and-Control (C&C) servers in malware attacks?

a) To monitor system logs
b) To direct infected systems to perform specific malicious tasks
c) To encrypt user data
d) To distribute security patches

Answer: b) To direct infected systems to perform specific malicious tasks

44. Advanced Persistent Threats (APT) typically aim to:

a) Cause immediate system crashes
b) Collect sensitive data over a prolonged period without detection
c) Encrypt files and demand a ransom
d) Self-replicate rapidly across networks

Answer: b) Collect sensitive data over a prolonged period without detection

45. In dynamic malware analysis, what is used to monitor system processes and behavior in real time?

a) Process Monitor
b) Regshot
c) Sysinternals Suite
d) VirusTotal

Answer: a) Process Monitor

46. Which technique does polymorphic malware use to avoid detection?

a) Using the same signature across all instances
b) Modifying its code every time it executes
c) Encrypting its payload
d) Hiding its presence using system processes

Answer: b) Modifying its code every time it executes

47. What is the function of a zombie computer in a botnet?

a) To act as a C&C server
b) To capture sensitive data from other devices
c) To perform malicious tasks as part of a larger network
d) To display advertisements to the user

Answer: c) To perform malicious tasks as part of a larger network

48. Data exfiltration in malware refers to:

a) The act of installing malicious software
b) The process of stealing and sending data to an external server
c) The encryption of user files for ransom
d) The act of monitoring network traffic

Answer: b) The process of stealing and sending data to an external server

49. Which tool is used to reverse-engineer malware and identify its code structure?

a) Wireshark
b) IDA Pro
c) Cuckoo Sandbox
d) Sysinternals Suite

Answer: b) IDA Pro

50. RATs (Remote Access Trojans) are primarily used for:

a) Denial-of-service attacks
b) Remote control of an infected system
c) Encrypting files
d) Collecting user credentials

Answer: b) Remote control of an infected system