1. Introduction to Malware

- **Topics Covered:**
  - What is Malware?
  - Types of Malware
  - Malware Propagation
  - Malware Impact
  - Malware History

Sample MCQs for Introduction to Malware:

1. **What is malware?**
   - A) Software that helps improve computer performance
   - B) Software designed to damage or exploit a computer system
   - C) A tool used for network administration
   - D) A virus scanning tool

Answer: B

2. **Which of the following is a type of malware that replicates itself to spread to other systems?**
   - A) Trojan Horse
   - B) Virus
   - C) Worm
   - D) Spyware

Answer: C

3. **Which of the following is NOT considered malware?**
   - A) Trojan Horse
   - B) Worm
   - C) Firewall
   - D) Adware

Answer: C

4. **Which type of malware is specifically designed to steal sensitive information such as passwords or credit card details?**
   - A) Rootkit
   - B) Adware
   - C) Spyware

- D) Ransomware

Answer: C

5. **The first recorded instance of malware was a:**
   - A) Computer virus in the 1980s
   - B) Trojan in the 1990s
   - C) Worm in the 1970s
   - D) Keylogger in the 2000s

Answer: A

Sample MCQs for Types of Malware:

1. **Which of the following malware types is often delivered via email attachments and is capable of attaching itself to executable files?**
   - A) Virus
   - B) Worm
   - C) Trojan
   - D) Spyware

Answer: A

2. **What does a worm primarily do?**
   - A) Encrypts files and demands payment
   - B) Infects files but needs a host program to run
   - C) Spreads across networks without requiring a host
   - D) Steals personal information without detection

Answer: C

3. **Which malware type masquerades as legitimate software to trick users into installing it?**
   - A) Trojan Horse
   - B) Worm
   - C) Ransomware
   - D) Rootkit

Answer: A

4. **Ransomware typically demands:**
   - A) Unauthorized access to network devices
   - B) A monetary ransom for restoring access to files

- C) Personal data theft
- D) Information about system vulnerabilities

Answer: B

5. **What is the main function of adware?**
    - A) Stealing confidential information
    - B) Showing unwanted advertisements
    - C) Taking control of the system's root access
    - D) Encrypting files to extort payment

Answer: B

3. Malware Analysis

- **Topics Covered:**
    - Malware Behavior Analysis
    - Malware Characteristics
    - Techniques for Analysis
    - Automated vs. Manual Analysis

Sample MCQs for Malware Analysis:

1. **What is the primary goal of malware analysis?**
    - A) To reverse-engineer the malware to understand its behavior
    - B) To find and delete all files on a system
    - C) To create more efficient malware
    - D) To identify the operating system version

Answer: A

2. **Which method of analysis is done without executing the malware?**
    - A) Dynamic Analysis
    - B) Static Analysis
    - C) Behavioral Analysis
    - D) Reverse Engineering

Answer: B

3. **Which type of malware analysis involves observing the behavior of malware during execution?**
    - A) Static Analysis

   - B) Dynamic Analysis
   - C) Manual Analysis
   - D) Heuristic Analysis

Answer: B

4. **Automated analysis of malware can speed up the detection process but often lacks:**
   - A) Accuracy
   - B) Flexibility and adaptability
   - C) High processing power
   - D) Reputation systems

Answer: B

5. **Which of the following is NOT a common tool used in malware analysis?**
   - A) Disassembler
   - B) Debugger
   - C) Memory Dump
   - D) Antivirus

Answer: D

---

4. Static Analysis

- **Topics Covered:**
  - Determining File Type
  - Fingerprinting Malware
  - Multiple Antivirus Scanning
  - Extracting Strings
  - Analyzing Headers

ample MCQs for Static Analysis:

1. **In static analysis, one of the first steps is determining the file type. Which of the following tools can help identify a file type?**
   - A) VirusTotal
   - B) File signature analysis tools
   - C) Dynamic analysis tools
   - D) Memory analysis tools

Answer: B

2. **What is the primary purpose of fingerprinting malware?**
   - A) To identify the malware's origin
   - B) To create a signature for detecting malware
   - C) To reverse-engineer the malware code
   - D) To generate random values in malware code

Answer: B

3. **Which of the following is the most common way to extract strings from a malware sample?**
   - A) Manual inspection of code
   - B) Using strings command in Linux
   - C) Modifying the system's registry
   - D) Analyzing network traffic

Answer: B

4. **Which of the following would NOT typically be found in a file header during static analysis?**
   - A) File size
   - B) Metadata
   - C) Function calls
   - D) Author name

Answer: C

5. **What is the purpose of scanning a malware sample with multiple antivirus tools in static analysis?**
   - A) To check for compatibility with different operating systems
   - B) To compare detection rates and signatures
   - C) To reverse-engineer the code
   - D) To isolate the malware's impact on the system

Answer: B

ample MCQs for Static Analysis:

1. **In static analysis, one of the first steps is determining the file type. Which of the following tools can help identify a file type?**
   - A) VirusTotal
   - B) File signature analysis tools
   - C) Dynamic analysis tools

- D) Memory analysis tools

Answer: B

2. **What is the primary purpose of fingerprinting malware?**
   - A) To identify the malware's origin
   - B) To create a signature for detecting malware
   - C) To reverse-engineer the malware code
   - D) To generate random values in malware code

Answer: B

3. **Which of the following is the most common way to extract strings from a malware sample?**
   - A) Manual inspection of code
   - B) Using strings command in Linux
   - C) Modifying the system's registry
   - D) Analyzing network traffic

Answer: B

4. **Which of the following would NOT typically be found in a file header during static analysis?**
   - A) File size
   - B) Metadata
   - C) Function calls
   - D) Author name

Answer: C

5. **What is the purpose of scanning a malware sample with multiple antivirus tools in static analysis?**
   - A) To check for compatibility with different operating systems
   - B) To compare detection rates and signatures
   - C) To reverse-engineer the code
   - D) To isolate the malware's impact on the system

Answer: B

Introduction to Malware (Continued)

6. **What is the primary difference between a virus and a worm?**
   - A) A virus requires user interaction to spread, while a worm can spread autonomously
   - B) A worm requires user interaction to spread, while a virus spreads autonomously

- C) A worm can only infect files, while a virus can infect memory
- D) There is no difference; they are the same

Answer: A

7. **Which of the following is an example of social engineering used in malware propagation?**
   - A) Exploiting a buffer overflow vulnerability
   - B) Sending phishing emails to steal user credentials
   - C) Using a rootkit to hide malware
   - D) Distributing ransomware through software updates

Answer: B

8. **What type of malware is primarily designed to provide unauthorized remote access to a compromised system?**
   - A) Trojan Horse
   - B) Keylogger
   - C) Rootkit
   - D) Spyware

Answer: C

9. **Which of the following malware types is known for tracking and recording user activity such as keystrokes?**
   - A) Keylogger
   - B) Ransomware
   - C) Rootkit
   - D) Trojan

Answer: A

10. **What is a common method used by malware to avoid detection by antivirus software?**

- A) By using polymorphic or metamorphic code
- B) By deleting system logs
- C) By encrypting files with complex algorithms
- D) All of the above

Answer: D

Types of Malware (Continued)

6. **Which malware type is most likely to corrupt files and demand a ransom for their decryption?**
   - A) Trojan Horse
   - B) Rootkit
   - C) Ransomware
   - D) Worm

Answer: C

7. **Which of the following best describes a "drive-by download"?**
   - A) A type of Trojan Horse that installs malware when a user visits a compromised website
   - B) A worm that spreads through infected USB drives
   - C) A virus that activates when a user downloads an email attachment
   - D) A malware attack through a phishing link

Answer: A

8. **What makes a rootkit particularly dangerous compared to other types of malware?**
   - A) It encrypts user files and demands ransom
   - B) It hides its presence from the operating system and security software
   - C) It replicates and spreads itself across networks
   - D) It floods the system with spam emails

Answer: B

9. **Which malware type is designed to exploit a system's vulnerabilities without the user's knowledge or consent?**
   - A) Virus
   - B) Worm
   - C) Adware
   - D) Trojan Horse

Answer: B

10. **Which of the following is the primary purpose of a keylogger?**
    - A) To provide unauthorized access to the system's administrator
    - B) To track a user's keystrokes and capture sensitive information like passwords
    - C) To damage files and cause system instability
    - D) To perform denial-of-service attacks

Answer: B

Malware Analysis (Continued)

6. **Which of the following tools is commonly used to perform dynamic malware analysis?**
   - A) Hex editor
   - B) Virtual machine (VM)
   - C) Static disassembler
   - D) String extraction tool

Answer: B

7. **In malware analysis, which of the following techniques is used to identify the potential behavior of the malware in a controlled environment?**
   - A) Sandboxing
   - B) File signature analysis
   - C) Code injection
   - D) Heuristic analysis

Answer: A

8. **When analyzing a piece of malware, which type of analysis will involve monitoring the system's network activity?**
   - A) Dynamic Analysis
   - B) Static Analysis
   - C) Signature-based Analysis
   - D) Memory Analysis

Answer: A

9. **What is the purpose of using a "sandbox" during malware analysis?**
   - A) To modify the malware's code
   - B) To execute the malware in a controlled environment to observe its behavior
   - C) To analyze the malware's encryption algorithm
   - D) To extract the malware's strings

Answer: B

10. **Which of the following can be used to detect unknown malware based on behavior and not just signatures?**
    - A) Signature-based detection

- B) Heuristic analysis
- C) File type determination
- D) String extraction

Answer: B

Static Analysis (Continued)

6. **Which tool would you use to examine the file's content for embedded or hardcoded URLs?**
   - A) File signature tools
   - B) Hex editor
   - C) String extraction tools
   - D) Debugger

Answer: C

7. **What can static analysis reveal about a malware sample?**
   - A) The real-time behavior of the malware during execution
   - B) The source code of the malware
   - C) The number of system processes the malware will spawn
   - D) The structure and content of the malware's binary file

Answer: D

8. **Which file characteristic is often analyzed during static analysis to determine the intended architecture of the malware?**
   - A) File extension
   - B) File headers
   - C) File metadata
   - D) File permissions

Answer: B

9. **Which of the following static analysis techniques is useful in identifying the use of packing in malware?**
   - A) File signature analysis
   - B) Reverse engineering the malware code
   - C) Using a disassembler
   - D) Extracting strings

Answer: C

10. **Which of the following best describes the role of multiple antivirus scanning in static analysis?**
    - A) To find out if the malware contains encryption algorithms
    - B) To identify how the malware spreads
    - C) To detect malware signatures and variants in the file
    - D) To identify how malware interacts with the system

Answer: C

Malware Analysis (Advanced)

11. **Which of the following methods is commonly used in reverse engineering to analyze the assembly code of a malware sample?**

- A) File signature analysis
- B) Static disassembling
- C) Memory dump analysis
- D) Debugging the malware in real-time

Answer: B

12. **Which of the following is a key advantage of manual malware analysis over automated tools?**

- A) Faster execution
- B) More accurate identification of zero-day vulnerabilities
- C) Ability to analyze encrypted or polymorphic code
- D) Automatic removal of malware

Answer: C

13. **Which of the following is most likely to occur during dynamic analysis of malware in a virtualized environment?**

- A) Malware code is analyzed for cryptographic patterns
- B) Malware may evade detection by disabling the VM
- C) The system automatically isolates malware from network communication
- D) Malware will be reverse-engineered into its source code

Answer: B

14. **What is an effective technique to prevent malware from escaping a virtual machine during analysis?**

- A) Allow the malware to run with administrative privileges
- B) Use of VM snapshots and rollback techniques

- C) Running the malware in a high-level sandbox environment
- D) Analyzing it using an online malware database

Answer: B

15. **In dynamic malware analysis, which of the following would be most useful in identifying unusual network activity or C2 (Command-and-Control) communication?**

- A) Static code analysis
- B) System file hash checking
- C) Network traffic monitoring
- D) Extracting embedded strings

Answer: C

Reverse Engineering Malware

16. **Which tool is most commonly used to disassemble or decompile malware to analyze its assembly code?**

- A) OllyDbg
- B) Wireshark
- C) RegEdit
- D) FileZilla

Answer: A

17. **What is a common challenge when reverse-engineering packed malware?**

- A) Packed malware is difficult to detect since it can hide its true content
- B) Packed malware runs without any need for memory
- C) Packed malware performs encryption only once
- D) Packed malware is detected automatically by antivirus tools

Answer: A

18. **What is the primary purpose of a debugger in reverse engineering malware?**

- A) To manually remove malware from the infected system
- B) To analyze the execution of malware line by line
- C) To automate the analysis of network traffic
- D) To extract hidden files and logs

Answer: B

19. **When reverse-engineering malware, which of the following is an indicator that the malware may be packed or obfuscated?**

- A) Large number of file extensions within the code
- B) Multiple iterations of repeated code sequences
- C) Presence of complex or cryptic code that seems difficult to understand
- D) Clear variable names and straightforward function calls

Answer: C

20. **Which of the following tools can be used for unpacking or decompressing packed malware during reverse engineering?**

- A) WinRAR
- B) IDA Pro
- C) x64dbg
- D) PEiD

Answer: D

Static Analysis (Advanced)

11. **In static analysis, what does examining a file's Digital Signature help identify?**

- A) The file’s authorship and authenticity
- B) The file’s encrypted sections
- C) The file’s compression method
- D) The execution environment of the malware

Answer: A

12. **When analyzing a malware file using the strings command in Linux, what type of data are you most likely to find?**

- A) System configuration settings
- B) File compression methods
- C) Human-readable text such as URLs, file paths, and strings that may be useful for identifying the malware's behavior
- D) Binary code that represents the malware's executable code

Answer: C

13. **Which of the following is an advantage of performing static analysis over dynamic analysis?**

- A) It provides insights into the malware’s behavior during execution

- B) It allows for monitoring of system modifications during malware execution
- C) It is faster and avoids the risks associated with running malware
- D) It is more effective at detecting polymorphic malware

Answer: C

14. **In static analysis, what can you infer from an unusually large or suspicious PE (Portable Executable) header?**

- A) The file is most likely packed or obfuscated
- B) The file has been scanned by an antivirus solution
- C) The file is a text document
- D) The file has been modified or corrupted

Answer: A

15. **Which technique can be used during static analysis to identify suspicious sections within an executable file that may contain malicious payloads?**

- A) Behavioral analysis
- B) File integrity monitoring
- C) PE header analysis
- D) Network traffic monitoring

Answer: C

Dynamic Analysis (Advanced)

11. **In dynamic analysis, what is the role of a "network analyzer" like Wireshark?**

- A) To capture and inspect the traffic between the malware and external systems, helping to identify command-and-control servers
- B) To automatically patch vulnerabilities in malware
- C) To generate random network traffic to confuse malware
- D) To prevent the malware from sending data to remote servers

Answer: A

12. **Which of the following best describes "hooking" in dynamic analysis?**

- A) A technique used to monitor and manipulate API calls made by malware
- B) A method to encrypt the malware before execution
- C) A way to compress malware files for easier analysis
- D) A technique used to automatically remove malware from infected systems

Answer: A

13. **Why might a malware analyst use a "sandbox" for dynamic analysis?**

- A) To perform malware analysis without the risk of spreading the infection to production systems
- B) To reverse-engineer packed malware
- C) To detect vulnerabilities in the operating system
- D) To extract embedded passwords from malware

Answer: A

14. **Which of the following actions would most likely be observed during dynamic analysis of a malware sample attempting to evade detection?**

- A) Malware immediately begins to encrypt user files
- B) Malware runs only when it detects specific system configurations or time intervals
- C) Malware initiates a brute force attack on the system password
- D) Malware immediately sends a large volume of emails

Answer: B

15. **When performing dynamic analysis, what type of behavior might indicate that the malware is attempting to hide its actions?**

- A) Opening several network ports
- B) Modifying system files and processes
- C) Attempting to disable antivirus or security software
- D) All of the above

Answer: D

Advanced Static Analysis Techniques

16. **What is "polymorphism" in the context of malware, and how does it affect static analysis?**

- A) The ability of malware to change its behavior based on the operating system
- B) The ability of malware to alter its code to avoid detection by signature-based antivirus programs
- C) The process of encryption used by malware
- D) The use of multiple payloads within a malware sample

Answer: B

17. **In static analysis, what is the significance of examining "import tables" within a PE file?**

- A) To identify external libraries or system functions that the malware may use for malicious actions
- B) To detect the exact memory address where the malware is located
- C) To analyze the malware's compression technique
- D) To determine the size and complexity of the malware file

Answer: A

18. **Which of the following is commonly used to identify and analyze embedded or hidden resources in malware during static analysis?**

- A) Network traffic monitoring
- B) PE file analysis
- C) Debugger-based inspection
- D) Memory dump extraction

Answer: B

Dynamic Analysis:

Dynamic Analysis Steps:

1. **What is the first step in dynamic analysis?**
   - A) Analyzing network traffic
   - B) Running the malware in a controlled environment
   - C) Disassembling the malware
   - D) Analyzing system calls
   - **Answer:** B) Running the malware in a controlled environment
2. **Which of the following tools is commonly used for malware dynamic analysis?**
   - A) Ghidra
   - B) OllyDbg
   - C) Wireshark
   - D) VirusTotal
   - **Answer:** B) OllyDbg
3. **What does "sandboxing" refer to in dynamic analysis?**
   - A) Isolating the malware from the system
   - B) Running the malware in an open environment
   - C) Analyzing the source code of malware
   - D) Protecting the system from malware

- **Answer:** A) Isolating the malware from the system

4. **What is commonly checked during dynamic analysis to understand malware behavior?**
   - A) File creation and deletion
   - B) Network traffic
   - C) Registry changes
   - D) All of the above
   - **Answer:** D) All of the above
5. **What is the purpose of monitoring API calls during dynamic analysis?**
   - A) To track the execution flow
   - B) To understand the malware's interaction with the OS
   - C) To detect encryption keys
   - D) To prevent the malware from running
   - **Answer:** B) To understand the malware's interaction with the OS

DLL Analysis:

1. **What is the primary function of a DLL (Dynamic Link Library)?**
   - A) To store system files
   - B) To provide reusable code for applications
   - C) To load operating system drivers
   - D) To store application data
   - **Answer:** B) To provide reusable code for applications
2. **What tool can be used to inspect DLL dependencies?**
   - A) Process Monitor
   - B) Dependency Walker
   - C) OllyDbg
   - D) Wireshark
   - **Answer:** B) Dependency Walker
3. **Which function is commonly used to load a DLL into a process?**
   - A) CreateFile
   - B) LoadLibrary
   - C) SetFilePointer
   - D) VirtualAlloc

  - **Answer:** B) LoadLibrary

4. **What is the purpose of an import table in a DLL?**
   - A) To list the functions the DLL exports
   - B) To list the functions the DLL imports
   - C) To load the DLL into memory
   - D) To execute the DLL functions
   - **Answer:** B) To list the functions the DLL imports
5. **Which of the following is true about DLL injection?**
   - A) It is used to compile DLLs
   - B) It allows a malicious DLL to be loaded into another process
   - C) It is an anti-malware technique
   - D) It only works on 64-bit systems
   - **Answer:** B) It allows a malicious DLL to be loaded into another process

---

Assembly Language and Disassembly Primer:

Introduction to Assembly Language Basics:

1. **Which of the following is the main purpose of assembly language?**
   - A) High-level programming
   - B) Direct control over hardware
   - C) Database management
   - D) Network programming
   - **Answer:** B) Direct control over hardware
2. **Which instruction in assembly is typically used to stop a program?**
   - A) HALT
   - B) NOP
   - C) MOV
   - D) JUMP
   - **Answer:** A) HALT
3. **Which assembly language operation is used to move data between registers?**
   - A) ADD
   - B) MOV

- C) JMP
- D) CMP
- **Answer:** B) MOV

4. **In x86 assembly, what does the instruction ADD AX, 1 do?**
    - A) It moves 1 into the AX register.
    - B) It adds 1 to the AX register.
    - C) It divides AX by 1.
    - D) It subtracts 1 from AX.
    - **Answer:** B) It adds 1 to the AX register.
5. **Which of the following registers is used for storing return addresses in x86 architecture?**
    - A) EAX
    - B) ESP
    - C) EIP
    - D) EBX
    - **Answer:** C) EIP

Registers and Data Transfer Instructions:

1. **What is the primary role of the EAX register in x86 assembly?**
    - A) It stores the return address
    - B) It is used for arithmetic operations and return values
    - C) It stores system status flags
    - D) It stores pointers to data in memory
    - **Answer:** B) It is used for arithmetic operations and return values
2. **Which of the following instructions moves data from one register to another in x86 assembly?**
    - A) MOV
    - B) PUSH
    - C) POP
    - D) CMP
    - **Answer:** A) MOV
3. **What does the instruction PUSH AX do in x86 assembly?**
    - A) Copies the value of AX into memory

    - B) Adds the value of AX to the stack
    - C) Moves the value of AX to the top of the stack
    - D) Pushes AX into a register
    - **Answer:** B) Adds the value of AX to the stack

4. **Which x86 register is used as the stack pointer?**
    - A) EAX
    - B) ESP
    - C) EBP
    - D) ECX
    - **Answer:** B) ESP
5. **What is the effect of the POP instruction in x86 assembly?**
    - A) It removes a value from memory.
    - B) It moves a value from the top of the stack into a register.
    - C) It adds a value to the stack.
    - D) It performs an arithmetic operation.
    - **Answer:** B) It moves a value from the top of the stack into a register.

Arithmetic Operations:

1. **Which instruction performs addition in x86 assembly?**
    - A) ADD
    - B) SUB
    - C) MUL
    - D) DIV
    - **Answer:** A) ADD
2. **What does the IMUL instruction do in x86 assembly?**
    - A) It adds two numbers.
    - B) It multiplies two numbers.
    - C) It divides two numbers.
    - D) It subtracts two numbers.
    - **Answer:** B) It multiplies two numbers.
3. **What is the result of the SUB instruction in assembly?**
    - A) It performs a bitwise operation.

- B) It adds two operands.
- C) It divides one operand by another.
- D) It subtracts one operand from another.
- **Answer:** D) It subtracts one operand from another.

4. **Which instruction is used to perform division in x86 assembly?**
   - A) DIV
   - B) ADD
   - C) CMP
   - D) MOV
   - **Answer:** A) DIV
5. **What is the purpose of the INC instruction in x86 assembly?**
   - A) It decreases the value of a register.
   - B) It compares two registers.
   - C) It increments the value of a register by 1.
   - D) It performs a division.
   - **Answer:** C) It increments the value of a register by 1.

Dynamic Analysis:

Dynamic Analysis Steps:

6. **Which of the following is NOT typically analyzed during dynamic malware analysis?**
   - A) File system modifications
   - B) Network connections
   - C) Malware code structure
   - D) Process creation and termination
   - **Answer:** C) Malware code structure
7. **What tool is used to monitor file system activity during dynamic analysis?**
   - A) Process Explorer
   - B) Filemon
   - C) IDA Pro
   - D) Sysinternals Suite
   - **Answer:** B) Filemon

8. **Which of the following is a major risk of performing dynamic analysis in a live environment without precautions?**
   - A) Data leakage
   - B) Data loss
   - C) Malware spread
   - D) Slower analysis speed
   - **Answer:** C) Malware spread
9. **What is the goal of dynamic analysis in terms of network activity?**
   - A) To detect whether the malware uses encryption
   - B) To track the malware's connection to command and control servers
   - C) To monitor the malware's interaction with anti-virus software
   - D) To isolate the malware from network resources
   - **Answer:** B) To track the malware's connection to command and control servers
10. **Which of the following is an example of a dynamic analysis tool used for network traffic analysis?**
   - A) OllyDbg
   - B) Wireshark
   - C) ProcMon
   - D) PEStudio
   - **Answer:** B) Wireshark

DLL Analysis:

6. **What is the first step when analyzing a suspicious DLL file?**
   - A) Disassembling the DLL file
   - B) Checking the file's integrity
   - C) Analyzing the function names in the export table
   - D) Running the DLL in a controlled environment
   - **Answer:** C) Analyzing the function names in the export table
7. **Which of the following can be used to reverse engineer the functions within a DLL?**
   - A) Ghidra
   - B) PowerShell
   - C) VLC Media Player
   - D) Task Manager

- **Answer:** A) Ghidra

8. **Which of the following describes the function of GetProcAddress in DLLs?**
   - A) It loads a DLL into memory
   - B) It retrieves the address of a function in a DLL
   - C) It unloads a DLL from memory
   - D) It checks the integrity of the DLL
   - **Answer:** B) It retrieves the address of a function in a DLL
9. **What is DLL hijacking?**
   - A) An attacker replaces a legitimate DLL with a malicious one
   - B) An attacker reverse-engineers a DLL to find vulnerabilities
   - C) An attacker exploits a bug in a DLL
   - D) An attacker loads a DLL into an unrelated process
   - **Answer:** A) An attacker replaces a legitimate DLL with a malicious one
10. **What is a key indicator of a suspicious or malicious DLL?**
    - A) The presence of unusual imports or exports
    - B) The absence of any imports
    - C) The file's large size
    - D) The file being digitally signed
    - **Answer:** A) The presence of unusual imports or exports

---

Assembly Language and Disassembly Primer:

Registers and Data Transfer Instructions:

6. **Which of the following registers in x86 is the data register used for arithmetic operations?**
   - A) EAX
   - B) EBX
   - C) ECX
   - D) EDX
   - **Answer:** A) EAX
7. **In x86 assembly, which instruction copies the contents of the source register into the destination register?**
   - A) MOV

- B) PUSH
- C) POP
- D) INC
- **Answer:** A) MOV

8. **What does the LEA instruction do in assembly?**
   - A) It loads the address of a variable into a register
   - B) It loads the value stored at the address of a variable
   - C) It performs a logical AND operation
   - D) It jumps to a specified memory address
   - **Answer:** A) It loads the address of a variable into a register
9. **Which of the following registers holds the value of the function return address in the x86 architecture?**
   - A) EAX
   - B) EBP
   - C) ESP
   - D) EIP
   - **Answer:** D) EIP
10. **Which assembly instruction is used to compare two values?**
    - A) CMP
    - B) MOV
    - C) ADD
    - D) SUB
    - **Answer:** A) CMP

Arithmetic Operations:

6. **What happens when the DIV instruction is used in x86 assembly?**
   - A) The dividend is divided by the divisor
   - B) Two values are added
   - C) One register is incremented
   - D) A logical operation is performed
   - **Answer:** A) The dividend is divided by the divisor
7. **In x86 assembly, what does the NEG instruction do?**

- A) Negates the value in a register
- B) Adds two values
- C) Moves data between registers
- D) Performs a division
- **Answer:** A) Negates the value in a register

8. **Which of the following is the result of the AND operation in assembly?**
    - A) Bitwise AND between two values
    - B) Subtraction of two values
    - C) Logical OR between two values
    - D) Addition of two values
    - **Answer:** A) Bitwise AND between two values
9. **In assembly, which instruction is used for signed multiplication?**
    - A) IMUL
    - B) MUL
    - C) ADD
    - D) SUB
    - **Answer:** A) IMUL
10. **Which instruction would you use to increment a register by 1 in x86 assembly?**
    - A) INC
    - B) ADD
    - C) SUB
    - D) MOV
    - **Answer:** A) INC

Bitwise Operations:

1. **Which of the following performs a bitwise XOR operation in assembly?**
    - A) XOR
    - B) AND
    - C) OR
    - D) NOT
    - **Answer:** A) XOR
2. **In x86 assembly, which instruction clears the contents of a register (sets it to zero)?**

- A) AND
- B) MOV
- C) XOR
- D) NOT
- **Answer:** C) XOR

3. **What is the purpose of the SHL instruction in assembly?**
    - A) Shift the bits of a value to the left
    - B) Shift the bits of a value to the right
    - C) Perform a logical AND operation
    - D) Perform a division operation
    - **Answer:** A) Shift the bits of a value to the left
4. **Which of the following instructions is used to perform a bitwise OR operation in assembly?**
    - A) OR
    - B) AND
    - C) XOR
    - D) NOT
    - **Answer:** A) OR
5. **What is the result of the RCL (Rotate through carry left) operation in assembly?**
    - A) The bits are rotated left through the carry flag
    - B) The bits are rotated right through the carry flag
    - C) The register is shifted left
    - D) The register is shifted right
    - **Answer:** A) The bits are rotated left through the carry flag

Dynamic Analysis:

Dynamic Analysis Steps:

11. **What is the purpose of using a debugger in dynamic analysis?**

- A) To prevent the malware from executing
- B) To step through the malware's code and observe behavior
- C) To extract encryption keys from the malware
- D) To monitor network traffic
- **Answer:** B) To step through the malware's code and observe behavior

12. **In dynamic analysis, which of the following is an indicator that malware is attempting to hide its behavior?**

- A) Unexpected network traffic
- B) Frequent process crashes
- C) The use of obfuscated code
- D) High CPU usage
- **Answer:** C) The use of obfuscated code

13. **Which of the following dynamic analysis techniques helps in identifying memory manipulation by malware?**

- A) API hooking
- B) Static code analysis
- C) Memory dumping
- D) File system monitoring
- **Answer:** C) Memory dumping

14. **What is one of the challenges when performing dynamic analysis of malware?**

- A) Static analysis is always faster than dynamic
- B) Malware might detect the analysis environment and change behavior
- C) Dynamic analysis does not provide insight into how the malware was created
- D) Dynamic analysis cannot detect network activity
- **Answer:** B) Malware might detect the analysis environment and change behavior

15. **Which of the following tools can be used to trace function calls made by malware during dynamic analysis?**

- A) IDA Pro
- B) OllyDbg
- C) ProcMon
- D) FileMon
- **Answer:** B) OllyDbg

DLL Analysis:

11. **Which of the following best describes DLL injection?**

- A) Loading a DLL into memory for execution
- B) Modifying the contents of an existing DLL
- C) Inserting a malicious DLL into another process's memory space

- D) Creating a new DLL from a system process
- **Answer:** C) Inserting a malicious DLL into another process's memory space

12. **Which tool would you use to detect if a DLL is being injected into a process?**

- A) Dependency Walker
- B) ProcMon
- C) Wireshark
- D) PEStudio
- **Answer:** B) ProcMon

13. **When analyzing a DLL, what is the significance of its Export Table?**

- A) It contains the list of external functions the DLL provides
- B) It contains the list of functions the DLL imports
- C) It defines the entry point for the DLL
- D) It contains the metadata about the DLL
- **Answer:** A) It contains the list of external functions the DLL provides

14. **Which of the following is a sign that a DLL might be used for malicious purposes?**

- A) The DLL has no export functions
- B) The DLL is signed by a reputable certificate authority
- C) The DLL imports system-critical libraries like kernel32.dll
- D) The DLL uses unusual function names
- **Answer:** D) The DLL uses unusual function names

15. **Which of the following Windows commands can be used to list the DLLs loaded into a process?**

- A) tasklist
- B) listdlls
- C) procmon
- D) netstat
- **Answer:** B) listdlls

Assembly Language and Disassembly Primer:

Registers and Data Transfer Instructions:

11. **Which register in x86 architecture is used for the stack pointer?**

- A) EAX
- B) EBP
- C) ESP
- D) ECX
- **Answer:** C) ESP

12. **Which of the following is a correct operation of the MOV instruction in x86 assembly?**

- A) It transfers control to another part of the program
- B) It performs a comparison between two registers
- C) It copies data from one location to another
- D) It shifts the bits in a register
- **Answer:** C) It copies data from one location to another

13. **What is the function of the PUSH instruction in x86 assembly?**

- A) It adds data to the top of the stack
- B) It moves data from one register to another
- C) It subtracts a value from a register
- D) It performs a comparison between two registers
- **Answer:** A) It adds data to the top of the stack

14. **Which instruction would you use to decrement the value of a register by 1?**

- A) DEC
- B) ADD
- C) SUB
- D) MOV
- **Answer:** A) DEC

15. **In x86 assembly, which register is typically used to store the frame pointer?**

- A) EAX
- B) EBP
- C) ESP
- D) EIP
- **Answer:** B) EBP

Arithmetic Operations:

11. **What does the MUL instruction do in x86 assembly?**

- A) Performs multiplication of signed numbers
- B) Performs multiplication of unsigned numbers
- C) Subtracts two values
- D) Divides two values
- **Answer:** B) Performs multiplication of unsigned numbers

12. **Which of the following instructions performs subtraction in x86 assembly?**

- A) ADD
- B) SUB
- C) MOV
- D) CMP
- **Answer:** B) SUB

13. **What is the result of ADD AX, BX if AX = 5 and BX = 3 in x86 assembly?**

- A) AX = 2
- B) AX = 8
- C) AX = 15
- D) AX = 3
- **Answer:** B) AX = 8

14. **Which of the following instructions is used to perform division in x86 assembly?**

- A) DIV
- B) MUL
- C) ADD
- D) CMP
- **Answer:** A) DIV

15. **Which of the following registers is used as the dividend in the DIV instruction in x86 assembly?**

- A) EAX
- B) EBX
- C) ECX
- D) EDX
- **Answer:** A) EAX

Bitwise Operations:

6. **What is the result of XOR AX, AX in x86 assembly?**
   - A) AX will be incremented by 1
   - B) AX will be set to 0
   - C) AX will hold the value 1
   - D) AX will remain unchanged
   - **Answer:** B) AX will be set to 0
7. **Which instruction is used to perform a left shift of bits in x86 assembly?**
   - A) SHL
   - B) SHR
   - C) RCL
   - D) ROR
   - **Answer:** A) SHL
8. **What does the ROR instruction do in assembly?**
   - A) Performs a rotate right through carry
   - B) Performs a shift right
   - C) Performs a bitwise OR
   - D) Performs a rotate left through carry
   - **Answer:** A) Performs a rotate right through carry
9. **What happens when the NOT instruction is used in assembly?**
   - A) It clears the value in the register
   - B) It complements each bit of the operand (bitwise NOT)
   - C) It adds 1 to the value in the register
   - D) It performs a logical AND
   - **Answer:** B) It complements each bit of the operand (bitwise NOT)
10. **In x86 assembly, what does SHR do?**
    - A) Shifts bits of a value to the left
    - B) Shifts bits of a value to the right, filling with zeros
    - C) Rotates bits left through the carry flag
    - D) Performs a subtraction operation
    - **Answer:** B) Shifts bits of a value to the right, filling with zeros

UNIT 3

Disassembly using IDA

Static Code Analysis:

1. **What does static code analysis focus on?**
   - A) Observing the runtime behavior of a program
   - B) Analyzing the source code of a program without executing it
   - C) Identifying memory leaks during execution
   - D) Determining the network activity of a program
   - **Answer:** B) Analyzing the source code of a program without executing it
2. **Which of the following is NOT a feature of IDA Pro?**
   - A) Disassembling binary files into assembly code
   - B) Interactive disassembly with dynamic debugging
   - C) Decompiling to higher-level languages
   - D) Reversing graphical user interface elements
   - **Answer:** D) Reversing graphical user interface elements
3. **Which of the following is typically analyzed during static code analysis in IDA Pro?**
   - A) System resource usage
   - B) Network communication patterns
   - C) Control flow graph and function calls
   - D) Memory dump analysis
   - **Answer:** C) Control flow graph and function calls
4. **In IDA Pro, what is the primary purpose of the "Function Window"?**
   - A) To display the hex dump of the binary
   - B) To view and analyze functions in the disassembled code
   - C) To track runtime memory changes

- D) To analyze the file header information
- **Answer:** B) To view and analyze functions in the disassembled code

5. **Which IDA Pro feature allows users to search for specific instructions or patterns within the binary?**
    - A) Hexadecimal view
    - B) String references
    - C) Graph view
    - D) Search for patterns
    - **Answer:** D) Search for patterns
6. **In IDA Pro, what is a "Segment"?**
    - A) A portion of memory where code is executed
    - B) A function that is executed at runtime
    - C) A section of a binary that contains code, data, or other elements
    - D) A collection of related functions in a program
    - **Answer:** C) A section of a binary that contains code, data, or other elements
7. **What type of information can be recovered using static analysis in IDA Pro?**
    - A) The original source code
    - B) The network protocols used by the program
    - C) The high-level structure of the program
    - D) The compiler used to create the binary
    - **Answer:** C) The high-level structure of the program
8. **Which IDA Pro window would you use to visualize a program's flow of execution?**
    - A) Hexadecimal view
    - B) Graph view
    - C) Function window
    - D) Output window
    - **Answer:** B) Graph view
9. **Which of the following is a limitation of static analysis using IDA Pro?**
    - A) Does not execute the program, so runtime issues may not be identified
    - B) It does not allow the analysis of dynamic memory allocations
    - C) It cannot disassemble binaries larger than 1GB

- D) It only supports analysis of Windows executables
- **Answer:** A) Does not execute the program, so runtime issues may not be identified

10. **In IDA Pro, what is the purpose of the "Decompiled" view?**
    - A) To view the source code of the binary in a high-level language
    - B) To view the hex dump of the binary
    - C) To view the function call graph
    - D) To perform runtime analysis of the program
    - **Answer:** A) To view the source code of the binary in a high-level language

---

***Disassembling Windows API*:**

11. **What is the primary purpose of disassembling Windows API calls in malware analysis?**
    - A) To identify system calls and function interactions
    - B) To find unencrypted strings
    - C) To trace the origin of the binary file
    - D) To calculate the execution time of functions
    - **Answer:** A) To identify system calls and function interactions
12. **Which of the following Windows API functions is used to allocate memory dynamically?**
    - A) VirtualAlloc
    - B) CreateFile
    - C) MessageBox
    - D) GetProcAddress
    - **Answer:** A) VirtualAlloc
13. **In IDA Pro, how can you identify which Windows API functions a program is calling?**
    - A) By examining the strings embedded in the binary
    - B) By inspecting the code's import table
    - C) By analyzing the binary's section headers
    - D) By looking at the program's output
    - **Answer:** B) By inspecting the code's import table
14. **Which of the following functions is used by malware to hide a file in a Windows environment?**
    - A) CreateFile

- B) GetFileAttributes
- C) SetFileAttributes
- D) LoadLibrary
- **Answer:** C) SetFileAttributes

15. **What can you infer from the use of CreateRemoteThread in a disassembled binary?**
    - A) The binary is attempting to inject code into another process
    - B) The binary is performing file system operations
    - C) The binary is opening a new network connection
    - D) The binary is manipulating the GUI
    - **Answer:** A) The binary is attempting to inject code into another process

---

Debugging Malicious Binaries

***General Concepts of Debugging*:**

1. **What is the primary goal of debugging malicious binaries?**
    - A) To reverse engineer the source code
    - B) To understand the malware's behavior and functionality
    - C) To detect the encryption methods used in the binary
    - D) To speed up the malware's execution
    - **Answer:** B) To understand the malware's behavior and functionality
2. **What type of debugger is most commonly used for analyzing Windows binaries?**
    - A) GDB
    - B) OllyDbg
    - C) IDA Pro
    - D) WinDbg
    - **Answer:** D) WinDbg
3. **In dynamic analysis, which of the following is typically used to monitor the behavior of a malicious binary?**
    - A) Debugger
    - B) Hex editor
    - C) Decompiler
    - D) Disassembler

- **Answer:** A) Debugger

4. **Which of the following is an essential part of debugging a binary?**
   - A) Analyzing its import table
   - B) Disassembling the code
   - C) Setting breakpoints
   - D) All of the above
   - **Answer:** D) All of the above
5. **Which of the following tools can be used to debug a Windows binary?**
   - A) OllyDbg
   - B) GDB
   - C) IDA Pro
   - D) All of the above
   - **Answer:** D) All of the above

Debugging Binaries:

6. **What is a breakpoint used for in debugging?**
   - A) To stop the execution of the program at a certain point
   - B) To pause the program's execution for analysis
   - C) To log the execution flow
   - D) To monitor memory allocation
   - **Answer:** A) To stop the execution of the program at a certain point
7. **Which of the following best describes the "stack trace" when debugging?**
   - A) A memory dump of the process
   - B) A list of function calls leading to the current point of execution
   - C) A list of network activities performed by the program
   - D) The set of resources accessed by the program
   - **Answer:** B) A list of function calls leading to the current point of execution
8. **What does the n (next) command do in a debugger?**
   - A) Skips over the current line of code and moves to the next instruction
   - B) Steps into the current function call
   - C) Runs the program without pausing
   - D) Exits the current function

- **Answer:** A) Skips over the current line of code and moves to the next instruction

9. **What happens when you set a "watchpoint" during debugging?**
    - A) It causes the debugger to stop when a specific value is changed in memory
    - B) It stops the program at a function call
    - C) It analyzes the memory layout of a specific function
    - D) It pauses the execution every time a loop is encountered
    - **Answer:** A) It causes the debugger to stop when a specific value is changed in memory

10. **Which of the following techniques is used to identify packed or obfuscated binaries?**
    - A) Analyzing system calls
    - B) Using dynamic analysis to watch unpacking behavior
    - C) Setting breakpoints in functions like LoadLibrary
    - D) All of the above
    - **Answer:** D) All of the above

Disassembly using IDA

***Static Code Analysis (Continued)*:**

16. **Which of the following features in IDA Pro helps in identifying code that may have been obfuscated?**
    - A) Control Flow Graph
    - B) Function Names Analysis
    - C) Strings and Imports View
    - D) Hexadecimal View
    - **Answer:** A) Control Flow Graph

17. **In IDA Pro, what does the "Strings" window display?**
    - A) A list of all strings within the binary, including possible plaintext passwords
    - B) A list of all assembly instructions
    - C) A list of all external function calls
    - D) A list of all unreferenced memory addresses
    - **Answer:** A) A list of all strings within the binary, including possible plaintext passwords

18. **When analyzing a binary in IDA Pro, which of the following might suggest the presence of packed code?**

- A) Large unexplained jumps or loops in the code
- B) References to imported functions
- C) Clear, readable assembly instructions
- D) Use of standard Windows API calls
- **Answer:** A) Large unexplained jumps or loops in the code

19. **Which of the following IDA Pro features allows you to interactively change the disassembled code?**
    - A) Graph view
    - B) Interactive mode
    - C) Edit script
    - D) Hex View
    - **Answer:** B) Interactive mode
20. **Which tool would you use in IDA Pro to analyze the interaction between a binary and the operating system's kernel?**
    - A) File offset view
    - B) Debugger
    - C) Kernel debugging
    - D) API function analysis
    - **Answer:** B) Debugger

***Disassembling Windows API (Continued)*:**

16. **Which of the following Windows API functions allows a program to execute shell commands?**
    - A) CreateProcess
    - B) ShellExecute
    - C) CreateThread
    - D) SetWindowsHookEx
    - **Answer:** B) ShellExecute
17. **How can the GetProcAddress function be useful in disassembling a binary?**
    - A) It dynamically resolves function addresses at runtime, useful for API call identification
    - B) It allocates memory for a function's address
    - C) It dissects the code to identify API imports

- D) It unpacks compressed code
- **Answer:** A) It dynamically resolves function addresses at runtime, useful for API call identification

18. **What is the purpose of the LoadLibrary function in Windows API analysis?**
    - A) It loads a dynamic link library (DLL) into the memory of a running process
    - B) It copies a DLL to a specific directory
    - C) It initializes the system for API call interception
    - D) It creates a new process in the background
    - **Answer:** A) It loads a dynamic link library (DLL) into the memory of a running process
19. **What is an indicator that a malicious binary is making use of SetWindowsHookEx?**
    - A) It tries to hook into system-wide keyboard or mouse events
    - B) It creates a new user interface window
    - C) It performs file system operations
    - D) It accesses the internet
    - **Answer:** A) It tries to hook into system-wide keyboard or mouse events
20. **Which Windows API function is commonly used by malware to download files from the internet?**
    - A) DownloadFile
    - B) GetURL
    - C) InternetOpen
    - D) InternetReadFile
    - **Answer:** C) InternetOpen

Debugging Malicious Binaries

General Concepts of Debugging (Continued):

6. **Which of the following commands would you use in a debugger to stop execution and break on a specific condition?**
    - A) Breakpoint
    - B) Step into
    - C) Watchpoint
    - D) Trace
    - **Answer:** A) Breakpoint

7. **Which debugger command is used to execute a program until a specific instruction is encountered?**
    - A) Run until
    - B) Continue
    - C) Step into
    - D) Run to cursor
    - **Answer:** D) Run to cursor
8. **In debugging, what is the purpose of the "call stack"?**
    - A) To display the sequence of function calls made during program execution
    - B) To list all memory allocations made by the program
    - C) To manage program flow during breaks
    - D) To observe network traffic during runtime
    - **Answer:** A) To display the sequence of function calls made during program execution
9. **Which of the following techniques is commonly used to identify if a program is using anti-debugging tricks?**
    - A) Setting breakpoints in the code
    - B) Searching for instructions that check if the program is being debugged
    - C) Monitoring the program's memory usage
    - D) Using static analysis
    - **Answer:** B) Searching for instructions that check if the program is being debugged
10. **In a debugger, what does the "disassembly" view show you?**
    - A) The bytecode of the program
    - B) The actual assembly code for the current instruction pointer
    - C) The memory dump of the program
    - D) The input/output data of the program
    - **Answer:** B) The actual assembly code for the current instruction pointer

Debugging Binaries (Continued):

11. **What is the primary function of a "watchpoint" in debugging?**
    - A) To pause execution when a specific instruction is executed
    - B) To pause execution when a specific memory location is accessed or modified
    - C) To display a variable's value at a certain point in execution
    - D) To step over functions without entering them

- **Answer:** B) To pause execution when a specific memory location is accessed or modified

12. **Which of the following commands would you use in GDB to step over a function call?**
    - A) next
    - B) step
    - C) continue
    - D) finish
    - **Answer:** A) next
13. **What does the step command do in debugging?**
    - A) It continues execution until the program exits
    - B) It executes the current line of code and steps into any function calls
    - C) It pauses the execution without changing any variables
    - D) It skips over the current line of code
    - **Answer:** B) It executes the current line of code and steps into any function calls
14. **Which of the following indicates a malicious binary might be using anti-debugging techniques?**
    - A) It crashes upon attaching a debugger
    - B) It opens many files in the system
    - C) It communicates over HTTP/HTTPS
    - D) It consumes a high amount of memory
    - **Answer:** A) It crashes upon attaching a debugger
15. **In WinDbg, what command would you use to dump the contents of the current stack?**
    - A) !dumpstack
    - B) !stack
    - C) dps
    - D) !list
    - **Answer:** C) dps

Expanding with More Advanced Topics:

I'll continue to add more questions to expand into **advanced debugging**, **disassembling packed code**, and **detecting anti-debugging techniques**.

16. **Which of the following techniques can be used to avoid detection when debugging malware?**
    - A) Delaying execution by inserting NOPs
    - B) Using code obfuscation techniques
    - C) Employing encryption techniques to hide code sections
    - D) All of the above
    - **Answer:** D) All of the above
17. **What does the ptrace system call allow a debugger to do on Linux?**
    - A) Interact with the kernel to perform system-level debugging
    - B) Attach to and control a running process for debugging
    - C) Monitor network traffic
    - D) Analyze memory usage
    - **Answer:** B) Attach to and control a running process for debugging
18. **In IDA Pro, how does the disassembler identify a function in the code?**
    - A) By detecting jumps that occur after the CALL instruction
    - B) By identifying API imports
    - C) By examining the binary header
    - D) By checking the function's address in the import table
    - **Answer:** A) By detecting jumps that occur after the CALL instruction
19. **Which of the following is a common behavior of malware designed to evade sandboxing during debugging?**
    - A) It checks for the presence of virtual machines or debuggers
    - B) It uses polymorphic techniques to change its behavior
    - C) It terminates itself when it detects the presence of a debugger
    - D) All of the above
    - **Answer:** D) All of the above
20. **What is one reason why debugging in a virtual machine (VM) might be preferred when analyzing malware?**
    - A) It speeds up malware execution
    - B) It isolates the system to prevent damage to the host system
    - C) It prevents malware from using anti-debugging techniques
    - D) It allows malware to run in its native environment

- **Answer:** B) It isolates the system to prevent damage to the host system

Disassembly using IDA

***Static Code Analysis (Continued)*:**

21. **What is the primary advantage of using the IDA Pro decompiler?**
    - A) It translates disassembled code to higher-level language code
    - B) It provides an interactive graphical view of memory
    - C) It allows execution of the program in a safe environment
    - D) It generates network traffic analysis reports
    - **Answer:** A) It translates disassembled code to higher-level language code
22. **Which feature in IDA Pro helps to analyze code from multiple architectures?**
    - A) Cross-architecture debugging
    - B) Processor module support
    - C) Dynamic analysis window
    - D) Interactive disassembly
    - **Answer:** B) Processor module support
23. **What does "renaming functions" in IDA Pro accomplish?**
    - A) Makes the disassembled code easier to understand
    - B) Modifies the actual binary code
    - C) Encrypts the code to avoid detection
    - D) It optimizes the code for better performance
    - **Answer:** A) Makes the disassembled code easier to understand
24. **How does IDA Pro handle the analysis of obfuscated code?**
    - A) Automatically de-obfuscates the code for easy reading
    - B) Uses heuristics to suggest possible code de-obfuscation
    - C) It cannot handle obfuscated code at all
    - D) It provides no solution for obfuscated code
    - **Answer:** B) Uses heuristics to suggest possible code de-obfuscation
25. **What feature in IDA Pro allows you to trace code execution in a binary at a lower level?**
    - A) Graph view
    - B) Interactive debugger
    - C) Hexadecimal disassembly

- D) Symbol resolution
- **Answer:** B) Interactive debugger

Disassembling Windows API (Continued):

21. **Which of the following Windows API functions allows a program to allocate memory for use by other programs or for itself?**
    - A) VirtualAllocEx
    - B) GetProcAddress
    - C) WriteProcessMemory
    - D) GetModuleHandle
    - **Answer:** A) VirtualAllocEx
22. **When malware uses the CreateFile Windows API function, what is it most likely doing?**
    - A) Writing to a file in a protected location
    - B) Reading system files
    - C) Reading or writing data to a file, such as a log or configuration file
    - D) Creating a new thread in the background
    - **Answer:** C) Reading or writing data to a file, such as a log or configuration file
23. **Which function is often used in malicious binaries to execute shell commands on a system?**
    - A) CreateRemoteThread
    - B) ShellExecuteEx
    - C) ExitProcess
    - D) MessageBox
    - **Answer:** B) ShellExecuteEx
24. **In malware analysis, what role does the GetProcAddress function typically play?**
    - A) It loads a DLL into memory
    - B) It retrieves the address of a function from a loaded DLL
    - C) It creates a process in memory
    - D) It allocates memory for program use
    - **Answer:** B) It retrieves the address of a function from a loaded DLL
25. **What does the GetModuleHandle function in Windows API do?**
    - A) Loads a module into memory
    - B) Retrieves a handle for a loaded module or DLL

- C) Modifies the execution permissions of a module
- D) Unloads a module from memory
- **Answer:** B) Retrieves a handle for a loaded module or DLL

Debugging Malicious Binaries

General Concepts of Debugging (Continued):

11. **Which command in GDB is used to display the current instruction pointer?**
    - A) info registers
    - B) show ip
    - C) disassemble
    - D) next
    - **Answer:** A) info registers
12. **In debugging, what does "stepping through" a program mean?**
    - A) Skipping over code to reach the next breakpoint
    - B) Running the program normally
    - C) Moving through the program one instruction at a time
    - D) Changing the execution flow of the program
    - **Answer:** C) Moving through the program one instruction at a time
13. **When debugging a binary, why might you use the continue command in a debugger?**
    - A) To move to the next function in the call stack
    - B) To run the program without stopping at breakpoints
    - C) To pause the program's execution at a specific point
    - D) To examine memory usage at runtime
    - **Answer:** B) To run the program without stopping at breakpoints
14. **Which of the following debugging tools supports dynamic analysis by monitoring system calls made by a program?**
    - A) GDB
    - B) Process Monitor (ProcMon)
    - C) IDA Pro
    - D) Wireshark
    - **Answer:** B) Process Monitor (ProcMon)

15. **What is the function of the "disassembly" view in a debugger?**
    - A) It shows the high-level code structure of the program
    - B) It shows the program’s instructions in assembly language
    - C) It displays the stack trace and variables used
    - D) It provides a graphical representation of program flow
    - **Answer:** B) It shows the program’s instructions in assembly language

***Debugging Binaries (Continued)*:**

16. **What is one way to identify if a binary is using anti-debugging tricks?**
    - A) The binary shows abnormal program behavior only when a debugger is attached
    - B) The binary crashes as soon as the debugger starts
    - C) It causes system errors on execution
    - D) All of the above
    - **Answer:** D) All of the above
17. **What does the step command do in most debuggers?**
    - A) It skips over the current instruction
    - B) It executes one line of code, including stepping into function calls
    - C) It continues execution without pausing
    - D) It shows the system call output in a window
    - **Answer:** B) It executes one line of code, including stepping into function calls
18. **What is the main purpose of using a debugger like WinDbg or OllyDbg when analyzing a binary?**
    - A) To interact with a running program and monitor its behavior
    - B) To statically analyze a program’s source code
    - C) To decrypt the binary and find hardcoded strings
    - D) To optimize the program for better performance
    - **Answer:** A) To interact with a running program and monitor its behavior
19. **Which of the following tools can assist in debugging Windows binaries?**
    - A) OllyDbg
    - B) GDB
    - C) WinDbg
    - D) All of the above

- **Answer:** D) All of the above

20. **Why is it important to check the "call stack" while debugging a program?**
    - A) To track the origin of a function call and understand program flow
    - B) To find the memory usage at the current point
    - C) To view the system-level events triggered by the program
    - D) To determine which variable is causing the error
    - **Answer:** A) To track the origin of a function call and understand program flow

---

Final Set of Questions for Completion:

21. **What is the primary function of the SetThreadContext function in Windows API?**
    - A) To manage thread states during execution
    - B) To stop a running thread
    - C) To modify a thread’s context (e.g., registers, stack pointer)
    - D) To create a new thread in a program
    - **Answer:** C) To modify a thread’s context (e.g., registers, stack pointer)
22. **In a debugger, what is the effect of setting a "conditional breakpoint"?**
    - A) It stops the program whenever a certain condition is met
    - B) It pauses execution only at specific function calls
    - C) It tracks the program’s resource usage
    - D) It displays memory contents at a specific address
    - **Answer:** A) It stops the program whenever a certain condition is met
23. **What is the purpose of analyzing the Import Address Table (IAT) during malware analysis?**
    - A) To identify which functions the program imports from DLLs
    - B) To check the location of the program’s resources
    - C) To analyze the program’s system calls
    - D) To determine the entry point of the binary
    - **Answer:** A) To identify which functions the program imports from DLLs
24. **Which of the following tools would you use to analyze malware that has been obfuscated or packed?**
    - A) GDB
    - B) IDA Pro

- C) OllyDbg
- D) All of the above
- **Answer:** D) All of the above

25. **Which of the following commands in WinDbg can be used to list loaded modules?**
    - A) !listmodules
    - B) lm
    - C) !loadmodules
    - D) modules
    - **Answer:** B) lm