**Question Bank**

1. What are the different types of malware, and how do they function?
2. How does a virus differ from a worm?
3. What is a trojan horse, and how does it spread?
4. Define ransomware and explain its impact on organizations.
5. What is spyware, and how does it collect information?
6. Explain adware and how it affects users.
7. What is the purpose of rootkits in malware attacks?
8. How do keyloggers work to capture sensitive information?
9. What are the main objectives of malware analysis?
10. What are the differences between static and dynamic malware analysis?
11. Why is malware forensics essential in cybersecurity?
12. How does malware behavior change in virtual and physical environments?
13. Differentiate between kernel mode and user mode debugging?
14. How is process injection used by malware to evade detection?
15. Explain the concept of hook injection in malicious activity.
16. How do attackers use process replacement for malware execution?
17. What are common anti-debugging techniques used by malware?
18. Discuss the significance of packers in malware and the process of unpacking them?
19. What is the significance of analyzing data encoding in malware behavior?
20. How does anti-disassembly work in malware?
21. Why is a malware analysis laboratory important for professionals?
22. What is a virtual machine (VM), and why is it used in malware analysis?
23. How do you set up reverse engineering (RE) tools for malware analysis?
24. What are the key features of a good debugging tool setup?
25. Why are forensic tools critical in a malware analysis lab?
26. What is hashing, and how is it used in malware analysis?
27. How do you find strings in malicious files?

28. What is FLOSS, and how does it help decode obfuscated strings?
29. How are PE file headers and sections structured?
30. What is the role of linked libraries and functions in malware?
31. Explain the use of Dependency Walker in malware analysis.
32. What is CFF Explorer, and how is it used?
33. How does Resource Hacker assist in analyzing malware?
34. What are malware signatures, and how are they created?
35. How does ClamAV detect malware using signatures?
36. What are YARA signatures, and how are they applied in malware detection?
37. What is a sandbox, and how is it used to analyze malware?
38. How does Process Monitor help in malware analysis?
39. What is the purpose of Process Explorer in malware detection?
40. How is RegShot used to compare system states?
41. Why is faking a network important when analyzing malware?
42. How does Wireshark monitor malware network activity?
43. What are the key components of the x86 CPU architecture?
44. How does the CPU process instructions in registers and stacks?
45. What are the main features of IDA Pro in reverse engineering?
46. How do you translate C code to assembly?
47. What is the importance of understanding underlying constructs in malware?
48. How do you analyze malicious Windows programs effectively?
49. What is Volatility, and how is it used for live memory analysis?
50. What are the differences between source-level and assembly-level debugging?
51. How does user-mode debugging differ from kernel-mode debugging?
52. What are the features of a good debugger?
53. What is the role of breakpoints in debugging?
54. How do exceptions influence program execution during debugging?

55. What is 011yDbg, and how is it used for debugging?

56. How does WinDBG assist in malware analysis?

57. What is the significance of kernel debugging with WinDBG?

58. What is process injection, and how is it executed?

59. How does process replacement differ from other injection techniques?

60. What is hook injection, and what are its implications?

61. How do anti-debugging techniques challenge analysis efforts?

62. What are common anti-virtual machine techniques used by malware?

63. How does data encoding contribute to malware concealment?

64. How do sandboxes help in practical malware detection?

65. What tools are commonly used for setting up a sandbox environment?

66. What are the advantages of running malware in isolated systems?

67. How does network simulation aid in dynamic malware analysis?

68. What are the risks of analyzing malware on a live system?

69. How can Volatility be used to identify malicious processes?

70. What is the significance of collecting memory dumps in forensics?

71. Define the differences between trojans and rootkits.

72. How do worms spread across networks compared to other malwares?

73. What is a zero-day malware, and why is it a critical threat?

74. What is the role of polymorphic malware in evading detection?

75. How does ransomware encrypt files on a victim's system?

76. What are some best practices for malware signature creation?

77. How are YARA rules maintained and updated in real-world scenarios?

78. What is the role of a forensic investigator in malware attack recovery?

79. How do industry professionals respond to malware attacks?

80. What are the ethical considerations when handling malicious samples?

81. What tools can be used to analyze running processes in Windows?

82. How does `Task Manager` differ from `Process Explorer` in malware analysis?

83. What are threads, and how can malware abuse them?

84. How can you detect malicious network connections using `netstat`?

85. What is the significance of handles in Windows malware analysis?

86. How can `Autoruns` help in identifying persistent malware?

87. What Windows logs are critical for malware forensics?

88. How do you identify malicious services using `sc` or `Services.msc`?

89. What are Windows scheduled tasks, and how can malware abuse them?

90. How can you extract malware artifacts from Prefetch files?

91. What command lists all running processes in Linux?

92. How does `lsof` help in identifying malicious file and network activity?

93. What are Linux threads, and how do they differ from Windows threads?

94. How can you check open ports using `netstat` or `ss`?

95. How do you identify malicious services in Linux (`systemctl`, `service`)?

96. What are cron jobs, and how can malware abuse them?

97. How can `/proc` directory help in Linux malware forensics?

98. What logs in `/var/log` are useful for detecting malware?

99. How can you check for rootkits in Linux?

100. What tools can extract malware artifacts from a compromised Linux system?

101. What are common types of Linux malware?

102. How does ELF binary structure differ from PE files?

103. What tools are used for static analysis of Linux malware?

104. How can `strace` and `ltrace` help in dynamic analysis?

105. What are common anti-analysis techniques in Linux malware?

106. What is the architecture of Android OS?

107. How do Android permissions work, and how can malware abuse them?

108. What are common types of Android malware?

109. How can you reverse-engineer an APK file?

110. What tools are used for dynamic analysis of Android malware?