Ethical Hacking

Sample Questions for Self-Assessment

1. Define Ethical Hacking and explain how it is distinct from other hacking types.
2. Discuss the ethical guidelines that govern the practice of ethical hacking.
3. Describe how cyber law and the legal system influence ethical hacking activities.
4. Highlight the importance of understanding the legal context for individuals practicing ethical hacking.
5. Compare and contrast the motivations and methods of White-hat, Black-hat, and Gray-hat hackers.
6. Identify common ethical dilemmas encountered in ethical hacking.
7. Explain the roles and primary duties of ethical hackers within organizations.
8. Explore the potential of ethical hacking in combating cybercrime.
9. Suggest measures that can be taken by individuals and organizations to defend against unauthorized hacking.
10. Reflect on the evolution of ethical hacking and anticipate future trends in the field.
11. Explain the role of the Digital Millennium Copyright Act (DMCA) in safeguarding intellectual property and outline its main elements.
12. Define ethical disclosure within the scope of vulnerability analysis and discuss its significance.
13. Detail the reverse engineering process and give examples of its application.
14. Describe how reverse engineering aids in detecting security flaws in software and digital frameworks.
15. Consider the ethical implications of using reverse engineering for identifying vulnerabilities.
16. Elucidate client-side vulnerabilities, including examples of potential exploits.
17. Discuss the importance of addressing client-side vulnerabilities and their potential effects on end-users and organizations.
18. Recommend strategies for individuals and organizations to shield against client-side vulnerabilities and lessen the chance of exploitation.
19. Examine how privilege escalation happens and the principal factors leading to such security incidents.
20. Address the repercussions of privilege escalation and how it can be prevented or minimized by organizations.
21. Provide examples of malware and discuss their potential impacts on individuals and organizations.
22. Differentiate between viruses, worms, and Trojan horses, highlighting their mechanisms and usage by cybercriminals.
23. Describe how rootkits and spyware function and their primary objectives.

24. Contrast ransomware with other malware types and offer strategies for ransomware attack prevention.
25. Outline the process of malware analysis, including static, dynamic, and behavioral analysis methods.
26. List common cloud computing vulnerabilities, such as insecure APIs and shared technology issues.
27. Discuss the exploitation of cross-site scripting (XSS) vulnerabilities in cloud applications and prevention techniques for developers.
28. Define virtualization vulnerability and its potential for compromising cloud environments by attackers.
29. Explain the risks associated with unencrypted cloud storage and the security measures that can safeguard against data breaches.
30. Describe mobile device vulnerabilities and how they can be exploited to access sensitive data or disrupt operations.
31. Explain the scanning phase in ethical hacking, including methods and tools for detecting network hosts, ports, and services.
32. Clarify the enumeration phase's goals in ethical hacking and its distinction from scanning.
33. Detail how ethical hackers utilize scanning and enumeration to pinpoint system or network vulnerabilities, noting commonly identified issues.
34. Describe penetration testing and its application by organizations to enhance security measures.
35. Introduce the Metasploit framework and its usage in penetration testing for vulnerability assessment.
36. Outline the essential duties, skills, and knowledge base of an ethical hacker.
37. Differentiate between worms and viruses from other malware types, mentioning prevalent distribution strategies by cybercriminals.
38. Discuss computer fraud and abuse, particularly how worms and viruses facilitate such crimes.
39. Enumerate effective strategies and tools, like firewalls and antivirus programs, for guarding against computer fraud and abuse.
40. Explain the concept of vulnerability disclosure and its impact on software and system security enhancements.
41. Discuss the collaborative efforts between software vendors and security researchers in identifying and responsibly disclosing vulnerabilities, including best practices for such disclosures.
42. Define source code auditing and its role in detecting software vulnerabilities and security flaws.
43. Explore how ethical hackers use source code auditing to uncover and potentially exploit software vulnerabilities, considering the ethical implications of these actions.

44. Define reverse engineering in the context of cybersecurity and software development, with examples of its applications.
45. Describe how disassemblers and decompilers facilitate reverse engineering, and address their limitations and ethical concerns.
46. Clarify the concept of privilege escalation and exemplify its use by attackers to bypass security controls for unauthorized system or data access.
47. Detail how privilege escalation techniques vary among different Windows OS versions and mitigation strategies for system administrators.
48. Distinguish between horizontal and vertical privilege escalation, including their methods and goals in unauthorized system access.
49. Explain detection and prevention methods for horizontal privilege escalation, along with attacker strategies for executing such attacks.
50. Define insecure APIs, their role in security breaches, and organizational measures for securing APIs against unauthorized data access.
51. Outline common data breach causes, including the impact of insecure APIs, with prevention best practices.
52. Identify two significant cloud computing vulnerabilities and their potential threats to cloud-stored user data.
53. Describe the collaborative efforts between cloud providers and organizations to address cloud computing vulnerabilities and user strategies for data protection.
54. List prevalent mobile app vulnerabilities and their exploitation methods for unauthorized data access or device control.
55. Recommend measures for app developers and users to safeguard against mobile app vulnerabilities, emphasizing secure coding and updates.
56. Detail the Ethical Hacking process stages and the main goals of each phase.
57. Define Vulnerability, Exploit, Payload, Black-hat Hacker, and Trojan briefly.
58. Introduce Metasploit's role in ethical hacking and penetration testing.
59. Discuss the use of Metasploit by organizations and cybersecurity professionals for network and system security testing, including ethical and compliance considerations.
60. Explain Intelligent Fuzzing and its application by organizations and cybersecurity experts to enhance software security and reliability.
61. Explain the role and application of scanning and enumeration tools in the context of ethical hacking and penetration testing.
62. Identify common tools used for scanning and enumeration in cybersecurity.
63. Describe the concept of network sniffing and its significance in ethical hacking for detecting and analyzing security vulnerabilities, including key tools and methods.
64. Discuss prevalent security flaws in mobile apps, how attackers exploit these, and collaborative strategies for developers and security experts to bolster app security.

65. Define social engineering within cybersecurity, outline typical techniques, and suggest protective measures for individuals and organizations.
66. Case Study: Security Evaluation of a Cloud-Based Application Handling Sensitive Data a. List typical security flaws found in cloud applications. b. Recommend actions to enhance security and prevent data breaches in cloud applications. c. Outline methods an ethical hacker might employ to assess a cloud application's security. d. Suggest corrective measures upon discovering vulnerabilities in the cloud application. e. Discuss the repercussions for a company if it fails to address security vulnerabilities leading to a data breach.
67. Case Study: Assessing and Addressing a Vulnerability in a Mobile Payment Application. Offer your assessment and recommendations for a discovered vulnerability in a mobile payment app that risks user data exposure.
68. What are the ethical and legal considerations when using open source intelligence (OSINT) techniques for cybersecurity purposes?
69. Discuss the importance of patch management in cybersecurity and how it helps in preventing security breaches.
70. How do ethical hackers conduct footprinting, and what tools are utilized in this phase to gather information about a target system or network?