SYSTEM HACKING INTERVIEW QUESTIONS

1.What is steganography?

Answer: Steganography is the practice of hiding information within other non-secret text or data. The goal is to avoid drawing attention to the hidden information.

2.How is steganography different from encryption?

Answer: Encryption scrambles data so it can only be read by someone with the correct decryption key, making the data unreadable to unauthorized users. Steganography, on the other hand, hides the existence of the data, making it invisible to unauthorized users.

3.Can you name some common techniques used in steganography?

Answer: Common techniques include least significant bit (LSB) insertion, masking and filtering, and transforming the data space. For example, hiding data in the LSBs of pixels in an image file.

4.What are some real-world applications of steganography?

Answer: Applications include digital watermarking, confidential communication, and protection of intellectual property.

5.What is the least significant bit (LSB) technique in steganography?

Answer: LSB steganography involves modifying the least significant bits of pixel values in an image to encode hidden data. Since these bits contribute very little to the overall image quality, changes are usually imperceptible to the human eye.

6.What is steganalysis?

Answer: Steganalysis is the process of detecting hidden information in steganographic media. It involves analyzing files to find any anomalies or patterns that indicate the presence of hidden data.

7.What are the goals of steganalysis?

Answer: The primary goals are to detect, extract, and destroy hidden information without necessarily knowing the exact method used for embedding the data.

8.Describe the difference between targeted and blind steganalysis.

Answer: Targeted steganalysis focuses on detecting hidden information using knowledge of the specific embedding algorithm, while blind steganalysis aims to detect hidden information without prior knowledge of the steganographic method used.

9.What are some common techniques used in steganalysis?

Answer: Techniques include statistical analysis, structural analysis, visual inspection, and machine learning approaches to detect anomalies.

10.How does statistical analysis help in steganalysis?

Answer: Statistical analysis examines the properties of the media file (e.g., pixel values in images) to find inconsistencies or deviations from expected patterns that might indicate hidden information.

11.What does 'covering tracks' mean in the context of hacking?

Answer: Covering tracks refers to the techniques hackers use to hide their presence, activities, and traces on a system or network to avoid detection and maintain access.

12.Why is it important for ethical hackers to understand techniques for covering tracks?

Answer: Understanding these techniques helps ethical hackers to think like malicious attackers, allowing them to identify vulnerabilities and improve the security posture of a system or network.

13.What is a common method used to cover tracks on a compromised system?

Answer: A common method is log manipulation, where hackers alter or delete log entries to remove evidence of their activities.

14.How can hiding files and directories help in covering tracks?

Answer: By using techniques such as setting hidden attributes, renaming files, or using rootkits, hackers can conceal malicious files and directories, making them harder to detect.

15.What is a rootkit and how does it aid in covering tracks?

Answer: A rootkit is a collection of software tools that enable unauthorized access and control of a computer system. It helps cover tracks by hiding its processes, files, and other activities from detection tools and system administrators.

16.Explain the use of proxy servers in covering tracks.

Answer: Proxy servers act as intermediaries between the hacker and the target system, masking the hacker's IP address and making it difficult to trace the source of the attack.

17.What role do VPNs play in hiding a hacker's activities?

Answer: VPNs (Virtual Private Networks) encrypt the hacker's internet traffic and route it through remote servers, hiding their true IP address and making their activities more difficult to trace.

18.How can timestamp manipulation be used to cover tracks?

Answer: Hackers can alter file timestamps to make it appear as though files were created, modified, or accessed at different times, thus confusing forensic investigators and hindering their analysis.

19.What is anti-forensic software and how is it used?

Answer: Anti-forensic software is designed to thwart forensic analysis by encrypting, obfuscating, or securely deleting data, making it challenging for investigators to recover evidence.

20.How can system administrators mitigate the risk of track-covering techniques?

Answer: Administrators can implement measures such as regular log monitoring, using integrity-checking tools, maintaining backups, enforcing strict access controls, and employing advanced threat detection systems to identify and respond to suspicious activities.