Task-2

Interview Questions

1.What is phishing?

Ans: Phishing is a type of cyberattack where malicious actors attempt to trick individuals into revealing sensitive information, such as login credentials, credit card details, or personal data, by disguising themselves as a trustworthy entity.

2.How to identify a phishing email?

Ans: To identify a phishing email during a job interview process, pay close attention to the sender's email address, the email's content, and any attachments or links.

3.What is email spoofing?

Ans: Email spoofing is a deceptive practice where the sender manipulates the email header to make it appear as if the message originated from a trusted source, like a colleague, bank, or known organization.

4.Why are phishing emails dangerous?

Ans: Phishing emails are dangerous because they can lead to significant financial loss, identity theft, and compromise of personal and sensitive information

5.How can you verify the sender’s authenticity?

Ans: These methods include checking the sender's address, looking for inconsistencies, verifying domain details, using reverse lookup tools, and examining email headers for authentication.

6.What tools can analyze email headers?

Ans: Popular options include Google's Message Header Toolbox, MXToolbox, and Mailheader, among others.

7.What actions should be taken on suspected phishing emails?

Ans: If you suspect an email is a phishing attempt, do not open it, do not click any links, and do not download any attachments

8.How do attackers use social engineering in phishing?

Ans: Attackers use social engineering in phishing interview scenarios by impersonating legitimate organizations or individuals to trick victims into revealing sensitive information or performing actions that compromise their security. This often involves creating a sense of urgency or trust to bypass normal security protocols.