Assignment-3

Step-1Case Study Analysis:

- Students should summarize the attack, detailing how social engineering was used to breach security.
- They should identify vulnerabilities such as lack of employee awareness training, inadequate authentication measures, or poor email security protocols.
- Discussing the consequences of the attack on the organization's reputation, financial losses, and customer trust is important.
- Recommendations may include implementing regular security training for employees, adopting multi-factor authentication, and improving email filtering systems.

Step-2 Role-play Exercise:

- After the role-play, students should identify the social engineering tactics used by the attacker, such as authority exploitation, urgency, or familiarity.
- Discussing the victim's susceptibility to these tactics and the importance of skepticism and verification in communication is crucial.
- Strategies to mitigate such attacks may include implementing strict verification protocols for sensitive information requests and fostering a culture of security awareness within the organization.

Step-3 Phishing Email Analysis:

- Red flags could include misspelled domain names, urgent language, requests for sensitive information, and generic greetings.
- Students should explore psychological factors such as curiosity, fear, or urgency that might lead individuals to overlook these red flags.
- Strategies for email authentication, such as checking email headers and verifying sender identities, should be discussed as preventive measures against phishing attacks.

Step -4 Documenting the Exploit Process:

- Document the exploit process, including the commands used, the output received, and any challenges encountered.