ASSIGNMENT 9

Social Engineering awareness and mitigation campaign

Project Title: Social Engineering Awareness and Mitigation Campaign

Project Description:

In this project, students will focus on raising awareness about social engineering threats and implementing measures to mitigate the risks associated with human-based, computer-based, and mobile-based social engineering attacks. The project aims to educate and empower individuals to recognize and defend against social engineering tactics.

Project Components:

Select a Target Audience:

Choose a target audience for the awareness campaign, such as employees within a hypothetical organization or members of a community group.

Social Engineering Awareness Materials:

Develop a range of awareness materials, including posters, flyers, infographics, and videos.

Create engaging content that explains social engineering threats, tactics, and potential consequences.

Phishing Attack Simulation:

Plan and conduct a controlled phishing attack simulation on the selected target audience.

Utilize Kali SET (Social Engineering Toolkit) to execute the simulation.

Document the effectiveness of the simulation and the responses of the participants.

Third-Party Phishing Tools:

Explore and demonstrate the use of third-party phishing tools to showcase the variety of attack vectors.

Discuss the risks associated with such tools and the importance of responsible use.

Detecting and Preventing Phishing Attacks:

Educate the target audience on how to detect phishing attempts and the common red flags to look for.

Provide guidance on best practices for preventing falling victim to phishing attacks.

Identity Theft Awareness:

Raise awareness about the risks of identity theft and impersonation.

Explain how personal information can be exploited by social engineers.

Share strategies for protecting personal information.

Physical Security Awareness:

Discuss the importance of physical security measures to prevent unauthorized access and social engineering attempts.

Conduct physical security awareness drills or workshops.

Insider Threats and Impersonation:

Explain the concept of insider threats and how social engineers may impersonate trusted individuals.

Provide examples and guidance on verifying identities.

Reporting Mechanisms:

Establish clear reporting mechanisms for suspected social engineering attempts or incidents.

Ensure that individuals know how to report such incidents to the appropriate authorities.

Security Awareness Campaign:

Launch the social engineering awareness campaign within the target audience.

Measure the effectiveness of the campaign through surveys or assessments.

Documentation and Reporting:

Maintain records of the campaign materials, simulations, and responses.

Create a report summarizing the campaign's impact and lessons learned.

Presentation:

Have students present the outcomes of the awareness campaign and the importance of social engineering defense to the class or instructor.

Project Benefits:

- Promotes cybersecurity awareness and education about social engineering threats.
- Offers practical experience in conducting phishing simulations and awareness campaigns.
- Empowers individuals to recognize and defend against social engineering attacks.
- Emphasizes the importance of responsible use of social engineering tools.