Document Reference:	SERTU-1	Effective Date:	8 May 2024
Document Name:	Social Engineering Red Team Usecase	Expiry Date:	8 May 2025

Social Engineering Red Team Usecase

Redback Operations

Document Owner:	Purple Team	Last Modified By:	Mallikarjuna Reddy K
Next Review Date:	17 July 2024	Last Modified on:	8 Mayh 2024

KEEP
CALM
the
RED TEAM
IS HERE

Version	Modified By	Approver	Date	Changes made
0.1	Mallikarjuna Reddy K		25 April 2024	First Draft
0.2	Joel Daniel		8 May 2024	Cosmetic Changes
1.0	Mallikarjuna Reddy K	Joel Daniel	8 May 2024	Approved for Publishing

Table of Contents

1. Introduction:

Social engineering attacks exploit human psychology to manipulate individuals into revealing sensitive information or compromising security protocols. Techniques include phishing, pretexting (fabricated scenarios), baiting (enticing offers), and tailgating (unauthorized persons following authorized personnel into secure areas). Attackers often impersonate reputable entities via email, telephone, or in person, posing significant risks to organizations.

2. Objective:

Establish a comprehensive framework that simulates social engineering attacks, providing hands-on training and preparedness. The objective is to:

- Enhance understanding of attack methods.
- Identify weaknesses in the organization's current detection and response capabilities.
- Improve resilience by developing effective prevention, detection, response, and recovery strategies.

3. Scope:

The framework targets all departments and communication channels that might facilitate social engineering attacks. This includes email, telephone, face-to-face interactions, and physical security breaches. Simulations will encompass attacks on various employee levels and assess organizational responses.

4. Preconditions:

- **Access to Communication Tools:** Employees have access to email, phone, and other communication tools vulnerable to exploitation.
- **Existing Security Measures:** Security protocols exist but are potentially bypassable through human error or psychological manipulation.
- **Current Security Training:** Employees undergo periodic training, but it might not cover all social engineering techniques.

5. Actors:

- **Employees:** Primary targets of social engineering attacks, ranging from entry-level to high-ranking personnel.
- **IT Security Team:** Responsible for detection, response, and post-incident analysis.
- **HR Department:** Oversees employee awareness training and reporting protocols.
- **Simulated Attackers (Pen Testers):** Execute social engineering simulations.

6. Trigger Event:

The event is triggered by a simulated attempt to obtain sensitive information or unauthorized access via deceptive means. This could involve spear-phishing emails, phone calls (vishing), or a physical intrusion attempt.

7. Simulated Attack Steps:

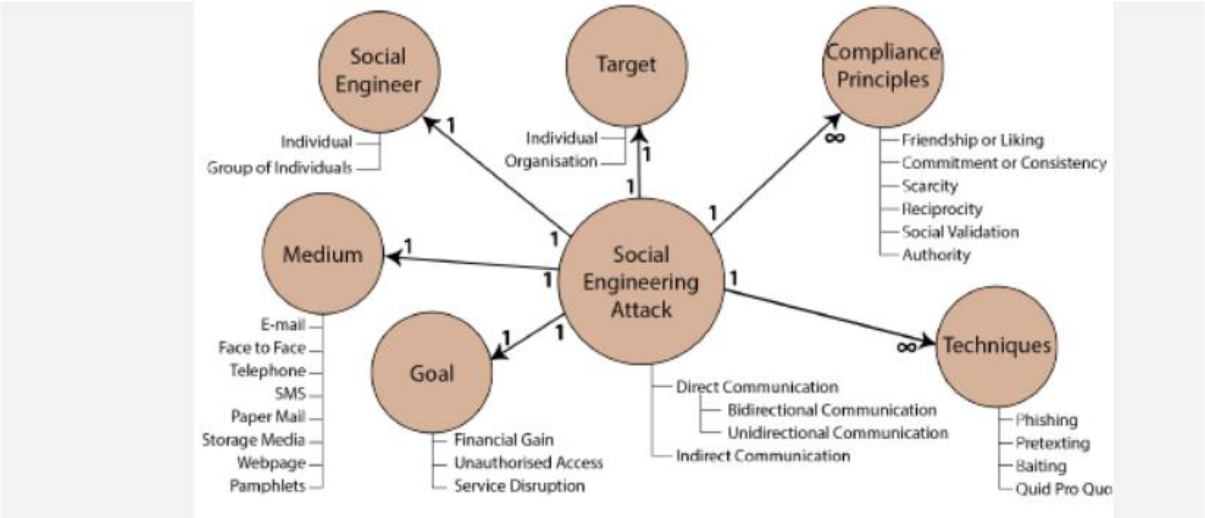
Scenario Setup:

a. Identify Attack Type: Select the most relevant attack types based on the organization's risk profile. Examples include phishing (email deception), vishing (phone deception), and baiting (physical media with malware).

b. Select Target Group: Determine the group size and employee roles targeted. This could range from entry-level to executives, varying by the attack type.

c. Craft Attack Material:

- **Phishing Emails:** Design realistic emails with convincing content, mimicking legitimate internal or external sources.
- **Pretext Calls:** Prepare phone scripts to impersonate known departments or trusted organizations.
- **Baiting Media:** Create enticing files or USB drives with a harmless payload to observe employee actions.

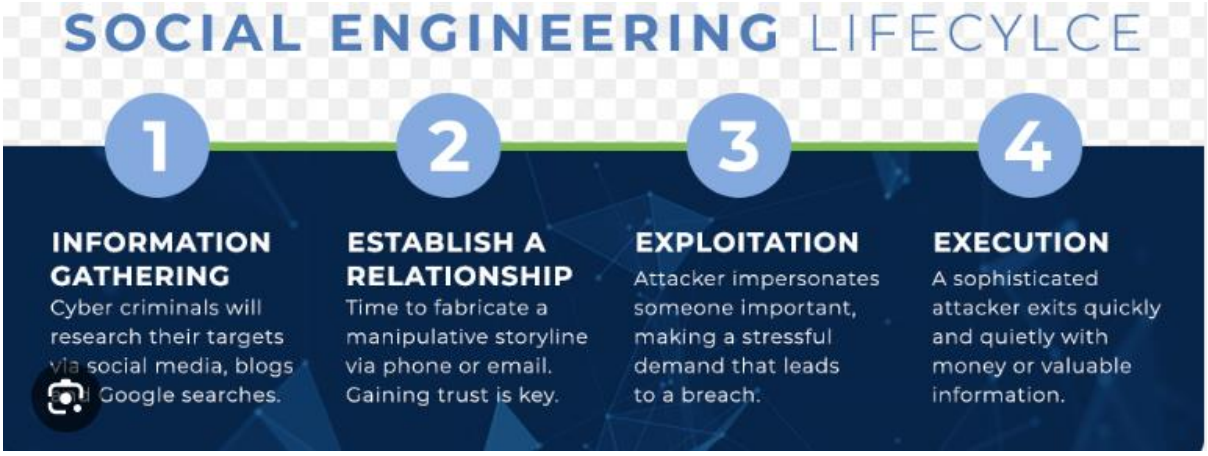


d. Define Metrics:

- Establish measurable goals like click-through rates, login attempts, or bait interaction.
- Consider pre- and post-simulation surveys to gauge awareness.

e. Execution of Simulated Attack:

- **Phishing Email Distribution:** Send targeted phishing emails to the selected group. Monitor who opens the emails, clicks on links, or enters credentials.
- **Pretext Phone Calls:** Conduct phone calls posing as IT support, HR, or external partners to extract sensitive information. Record responses and willingness to share data.
- **Bait Deployment:** Leave USB drives or enticing documents in common areas. Observe who connects them to computers or opens the documents.
- **Tailgating Attempt:** Attempt to follow authorized employees into secure areas, gauging responses from employees and security staff.



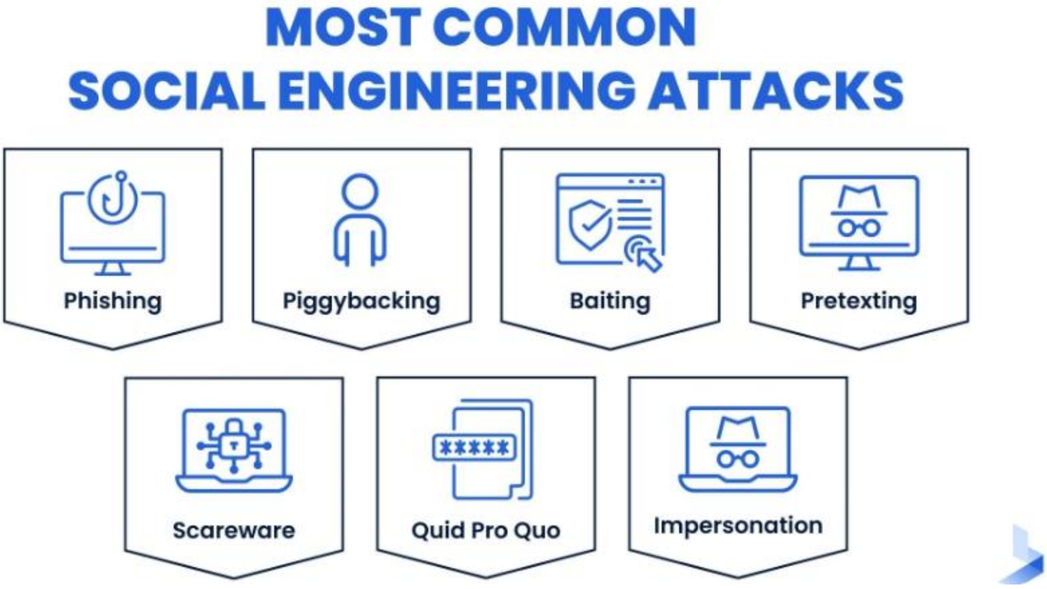
SOCIAL ENGINEERING LIFECYLCE

1 INFORMATION GATHERING
Cyber criminals will research their targets via social media, blogs and Google searches.

2 ESTABLISH A RELATIONSHIP
Time to fabricate a manipulative storyline via phone or email. Gaining trust is key.

3 EXPLOITATION
Attacker impersonates someone important, making a stressful demand that leads to a breach.

4 EXECUTION
A sophisticated attacker exits quickly and quietly with money or valuable information.



MOST COMMON SOCIAL ENGINEERING ATTACKS

Phishing

Piggybacking

Baiting

Pretexting

Scareware

Quid Pro Quo

Impersonation

8. Tools and Techniques:

- **Phishing Tools:** Automated software to design, send, and track phishing email campaigns.
- **Caller ID Spoofing Software:** Modify caller IDs to impersonate known entities.
- **Bait Creation Tools:** Software to mimic legitimate applications on USB drives for data collection.
- **Tailgating Equipment:** RFID card duplicators and access card scanners.

9. Post-Attack Analysis and Feedback:

- **Detection & Reporting Metrics:** Track how many employees identified the simulated attack and how many reported it. Review the efficacy of existing detection systems like email filtering and visitor management.
- **Response Analysis:** Assess the response team's ability to contain and investigate the simulated attack. Identify gaps in communication and coordination among response teams.
- **Training Improvement:** Incorporate simulation findings into future training sessions. Conduct role-playing exercises to reinforce correct behaviors.
- **Policy Updates:** Modify existing verification protocols and response procedures to reinforce security.

10. Conclusion:

Simulating social engineering attacks enables organizations to recognize potential gaps in their security posture. Effective detection, incident response, and employee training help to bolster the organization's resilience. Regular simulations and continuous training improve awareness and ensure that each team member can defend against cyber threats.