Social Engineering

Josh Wilcox (jw14g24)

May 2, 2025

Table of Contents

1. Overview
2. Anatomy of an SE attack
3. Social Engineering Techniques
   - Information Gathering
   - Shoulder Surfing
   - Interaction with Target

Overview

Definition

- Social engineering involves techniques to manipulate people into performing an action or divulging specific information
- Involves very little technical know-how and is more based on the ability to manipulate

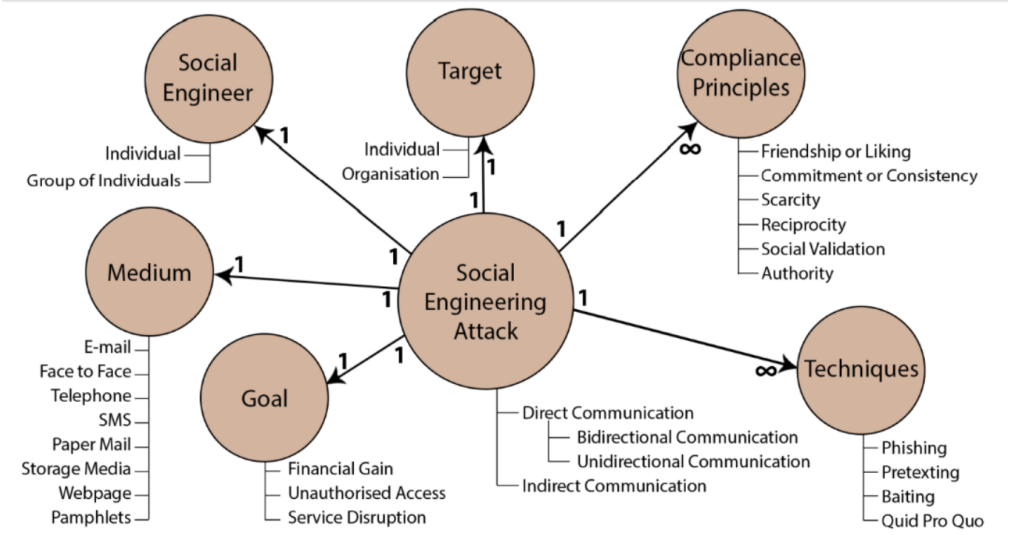
Why does it work

- It is well accepted that most security breaches are due to human error
- People are too kind and usually give the benefit of the doubt - even when being eliminated
- Much easier to simply ask for a password than try to crack it

Anatomy of an SE attack

The steps of a Social Engineering Attack

- Attack Formulation
  - Identify Goals and Targets
- Information Gathering
  - Identify information sources and gather
- Preparation
  - Identify weaknesses in the victim
- Develop Relationship
  - Establish communication and build relationship
- Exploit Relationship
  - Prime the target to finally convince them
  - Get the information you require
- Debrief
  - Potentially maintain the relationship for future attacks



Social Engineering Techniques

The Primary Techniques for Social Engineering

- Information Gathering
  - Research target online
  - Observe patterns and behaviors
  - Collect public documents
- Interaction with the target
  - Pretexting (false scenarios)
  - Phone calls or emails
  - Impersonating authority figures
- Tailgating
  - Following authorized personnel
  - Exploiting courtesy
  - Faking credentials
- Baiting
  - Infected USB drives
  - Malicious downloads
  - False promises

Subsections of Social Engineering Techniques

- Information Gathering
- Shoulder Surfing
- Interaction with Target

Information Gathering

Gathering from the Web

- Company Websites
  - Background of company
  - Executives and Employees of a company
  - Email Addresses
  - Open Job Position
- Social Networks
  - Lots of information can be found on LinkedIn, for example.

Dumpster Diving

- More traditional way of getting information
- Office trash not being shredded or removed correctly
- Can get very very sensitive information

Shoulder Surfing

Overview

- Looking over the targets shoulder
- Can fetch usernames, passwords, and confidential data
- Can be done anywhere

Interaction with Target

Phishing

- Sending emails that appear to be reputable but are not
- Done with URL and Email manipulation
- Commonly done with these vectors:
  - Charity
  - Tech Support
  - Financial
  - Government

Vishing and Smishing

- Caller ID spoofing
- AI voice deepfaking etc.

Physical Impersonation

- Person actually comes up to you posing as someone not suspicious to gain entry into a sensitive system