Social Engineering

Social engineering techniques focus on the human side of information security.

Introduction

Social engineering is the practice of manipulating people through a variety of strategies to accomplish desired actions.

Key Principles

Authority
Relies on the fact that most people will obey someone who appears to be in charge or knowledgeable, regardless of whether or not they actually are.

Example: Claiming to be a manager, a government official, or some other person who would have authority

Intimidation
Relies on scaring or bullying an individual into taking a desired action.

Consensus-based (Social Proof)
Uses the fact that people tend to want to do what others are doing to persuade them to take an action.

Example: Pointing out that everyone else in a department had already clicked on a link, or might provide fake testimonials about a product making it look safe.

Scarcity
Make something look more desirable because it may be the last one available.

Familiarity-based
Rely on you liking the individual or even the organization the individual is claiming to represent.

Trust
Relies on a connection with the individual they are targeting.

Urgency
Relies on creating a feeling that the action must be taken quickly due to some reason or reasons.

Usually more than 1 principle are combined to make an attack effective

Prepending (outside of the exam, you're more likely to run into pretexting than prepending as a technical term)

Adding an expression or phrase, such as adding "SAFE" to a set of email headers to attempt to fool a user into thinking it has passed an antispam tool

Adding information as part of another attack to manipulate the outcome

Suggesting topics via a social engineering conversation to lead a target toward related information the social engineer is looking for

Pretexting is the process of using a made-up scenario to justify why you are approaching an individual.

Techniques

Phishing

Phishing is a broad term used to describe the fraudulent acquisition of information

Phishing is most often done via email

Smishing is when it's done through SMS (text) messages

Vishing is when it's done through a telephone

Defense

One of the most common defenses against phishing of all types is awareness

Filtering that helps prevent phishing using reputation tools, keyword and text pattern matching.

Credential Harvesting

Credential harvesting is the process of gathering credentials like usernames and passwords.

It's often done through phishing but can also be done through system compromises

Once credentials are harvested, attackers will typically leverage them for further attacks

Defense

User awareness

Multifactor authentication (MFA)

Strong monitoring and response processes

Website Attacks

Pharming

Pharming attacks redirect traffic away from legitimate websites to malicious versions.

Pharming typically requires a successful technical attack that can change DNS entries on a local PC or on a trusted local DNS server, allowing the traffic to be redirected.

Typo Squatters

Typo squatters use misspelled and slightly off but similar to the legitimate site URLs to conduct typosquatting attacks.

Typo squatters rely on the fact that people will mistype URLs and end up on their sites, thus driving ad traffic or even sometimes using the typo-based website to drive sales of similar but not legitimate products.

Watering Hole

Using websites that targets frequent to attack them by compromising them or deploying malware through other means

Spam

Spam often employs social engineering techniques to attempt to get recipients to open the message or to click on links inside of it.

Spam over Instant Messaging (SPIM). While the term appear on the exam outline, SPIM never really became a widely used term in the security industry.

In-Person Techniques

Not Really social engineering but they are in the outline of the exam

Dumpster Diving
Retrieving potentially sensitive information from a dumpster.

Defense:
secure dumpsters
use secure disposal services for documents

Shoulder Surfing
The process of looking over a person's shoulder to capture information like passwords or other data.

Defense:
Awareness

Tailgating
Simply following someone who has authorized access to an area so that as they open secured doors you can pass through as well.

Defense:
Awareness

Eliciting information
Technique used to gather information without targets realizing they are providing it.

Examples: Talking a target through things, making incorrect statements so that they correct the person eliciting details

Identity Fraud and Impersonation

Identity fraud, or identity theft, is the use of someone else's identity.

It's the key tool in social engineering

Hoaxes, which are intentional falsehoods, come in a variety of forms ranging from virus hoaxes to fake news. They can be used by social engineers to assist in their social engineering attempts

Influence Campaigns

Online influence campaigns, which have traditionally focused on social media, email, and other online-centric mediums, have become part of what has come to be called hybrid warfare.

Influence campaigns themselves are not the exclusive domain of cyberwarfare, however. Individuals and organizations conduct influence campaigns to turn public opinion in directions of their choosing.