Chapter 4 Social Engineering and Password Attacks

# Social Engineering

Practice manipulating people through a variety of strategies to accomplish desired actions.

## Principles

* Authority: The fact that most people will obey someone who appears to be in charge or knowledgeable.
* Intimidation: Relies on bullying an individual into taking a desired action.
* Consensus-based: The fact that people want to do what everyone else is doing and using that as a form of persuasion.
* Scarcity: The situation that something looks desirable because it may be the last one.
* Familiarity-based: Relies on the victim liking the social engineer or what they claim to represent.
* Trust: Relies on the connection between the social engineer and the target.
* Urgency: Relies on the idea that an action needs to be done asap.

## Techniques

* Phishing
* Vishing
* Smishing: Phishing through SMS.
* Spear phishing: phishing a specific target.
* Whaling: phishing a target with a high status.
* Misinformation and Disinformation
  + Misinformation: Incorrect information from getting facts wrong.
  + Disinformation: Incorrect, inaccurate, or false information that serves a goal.
  + Malinformation: Facts that are out of context.
  + CISA 5 steps of TRUST to counter misinformation and disinformation:
    - Tell your story.
    - Ready your Team.
    - Understand and assess MDM.
    - Strategize response.
    - Track outcomes.
* Impersonation
* Business Email Compromises (BEC): Relies on using apparently legitimate email addresses to conduct scams and other attacks.
  + Methods:
    - Using compromised accounts.
    - Sending spoofed emails.
    - Using common fake but similar domain techniques.
    - Using malware or other tools.
* Pretexting: Process of creating made up scenario to justify why an attacker is approaching the target.
* Watering Hole Attacks: Targeting a frequently used website and attacking it.
* Brand Impersonation: Also known as brand phishing or brand spoofing, it’s the impersonation of a brand’s email handle and email format.
* Typosquatting: Use of misspelled and slightly similar to legitimate URLs.
  + Pharming: Relies on changing a system’s host file or active malware on the system that changes the system’s DNS servers.

# Password Attacks

3 types of password-related attacks:

* Brute-force attacks: Iterating through passwords until one works.
* Password Spraying attacks: like brute-force but uses a single password or small set of passwords on multiple accounts.
* Dictionary attacks: Like brute-force but uses a list of words for attempts.