**Social Engineering**

1. An attacker employs various means of gathering information about a target company, organization, or person. These techniques may range from using telephones, gathering trash or other discarded information, intrusion within company property, using the Internet for research, to querying individuals under false or misleading pretenses. A social engineer can use many small pieces of information to combine into a useful vulnerability of a system. Information can be important whether it comes from the janitor's office or from the CEO's office; each piece of paper, employee spoken to or area visited by the social engineer can add up enough information to attain access to sensitive data and resources of the company. The lesson here is all information, no matter how insignificant the employee believes it to be, may assist in creating a vulnerability for a company and an entrance for a social engineer. While the ultimate goal of the attacker may vary the purpose of these attacks is usually to gain access to computer systems or facilities [1].
2. An adversary exploits inherent human psychological predispositions to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the attackers' interests. Many interpersonal social engineering techniques do not involve outright deception, although they can; many are subtle ways of manipulating a target to remove barriers, make the target feel comfortable, and produce an exchange in which the target is either more likely to share information directly, or let key information slip out unintentionally. A skilled adversary uses these techniques when appropriate to produce the desired outcome. Manipulation techniques vary from the overt, such as pretending to be a supervisor to a help desk, to the subtle, such as making the target feel comfortable with the adversary's speech and thought patterns [2].
3. In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility. [3].

**REFERENCES**

1. <https://capec.mitre.org/data/definitions/404.html>
2. <https://capec.mitre.org/data/definitions/416.html>
3. <https://www.us-cert.gov/ncas/tips/ST04-014>