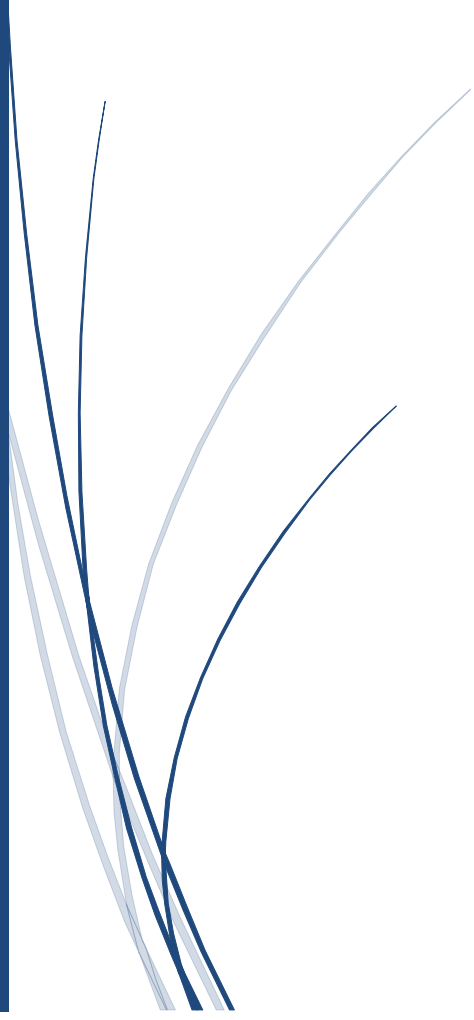
Chapter 9

Social Engineering

Theory



Ethical Hacking

Social engineering

Social engineering is an art of exploiting humans to gain sensitive information. This technique involves tricking people into breaking standard security procedures. It is a most significant threat in any organization. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.

Types of Social engineering

Social engineering is classified based on the techniques used to attack or commit fraud on the victim to steal the sensitive information. Types of social engineering attacks are:

- Human-based
- Computer-based
- Mobile-based

Human-Based

In human-based social engineering attacks, the social engineer interacts directly with the target to get sensitive information by performing the various techniques such as

- Shoulder surfing
- Dumpster diving
- Tailgating
- Piggybacking

Computer Based

Computer-based social engineering attacks are carried out with the help of computer software to gain access to the desired information. Some of these attack types are listed as follows:

- Phishing
- Spam mail
- Popup windows

Mobile Based

In mobile-based social engineering attacks, attackers take advantage of malicious mobile applications to gain access to the desired information. Some of the attack types are listed as follows:

- SMishing
- Publish malicious apps
- Repacking legitimate apps

Exploiting Human Using Social engineering

Social engineering and the human element are common ways to gain access to a network, database, or building. Major cyber incidents happen as the result of an attacker gaining initial access using social engineering technique, usually by convincing an insider to unwittingly download or install a piece of malware that opens up the target network to the attacker.

Attackers employ many tricks to try to get a human target to provide them with information or access. They appeal to ego, financial need, curiosity, humanity, or job duties all with the goal of getting the target to either click on a link that redirects the target to a malicious website or opens an attachment that contains malware.

Humans continue to be the weak link. No matter how secure a network, device, system, or organization is from a technical point of view, humans can often be exploited.

- Individuals should be vigilant regarding emails
- unsolicited phone calls that attempt to get people to reveal sensitive information.
- Companies should regularly provide security awareness training to employees.
- Lack of the security policies
- Unregulated access to information

Eavesdropping

Eavesdropping is a technique used by attackers to intercept unauthorized and private communication, such as a phone call, instant message, video conference or fax transmission. This is done by directly listening to digital or analog voice communication or by intercepting or sniffing data relating to any form of communication.

Dumpster diving

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container). In Information Technology, dumpster diving refers to a technique used to retrieve information that could be used to perform attacks on a computer network. Dumpster diving is not limited to searching through the trash for information like access codes or passwords written down on sticky notes

Shoulder Surfing

Shoulder surfing is noting but direct observation, such as looking over someone's shoulder, to grab sensitive details. It is commonly used while someone enters passwords, PIN numbers, security codes at ATMs or on their personal computers.

Tailgating and Piggybacking

A person tags himself with another person who is authorized to gain access into a restricted area, or pass a specific checkpoint is known as Tailgating/Piggybacking. Tailgating implies without consent while piggybacking means approval of the authorized person.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, financial information), often for malicious reasons, by masquerading as a trustworthy entity in electronic communication.

Spear phishing

Spear phishing is a variation on phishing in which hackers send emails to groups of people with specific common characteristics or other identifiers. Spear phishing emails appear to come from a trusted source but are designed to help hackers obtain trade secrets or other classified information.

Countermeasures

1. Employees in an organization should be aware of security policies and procedures.
2. Secure or shred all the documents containing private information.
3. Protect your personal information from being published.
4. Never store personal/banking information on the mobile device.

References:

1. Ablon, & Lillian. (2015, October 20). Social Engineering Explained: The Human Element in Cyberattacks. Retrieved from https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html
2. What is Spear Phishing? - Definition from Techopedia. (n.d.). Retrieved from https://www.techopedia.com/definition/4121/spear-phishing