IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 66-68
www.iosrjournals.org

Contrast Study of Social Engineering Techniques

Rohit Dhull[1], Prof. Sugandha Singh Hooda[2]
[1]*Research Scholars CE Department, PDM College of Engineering, Bahadurgarh, India*
[2]*Head, CSE Department, PDM College of Engineering, Bahadurgarh, India*

Abstract: *Social engineering has become a menace in our virtual world and is an effectual way to attack our systems. The objective of this study is to discuss different existing social engineering techniques and aspects of social engineering. This paper presents the various social engineering techniques and after the comparison among them a conclusion is drawn.*

Keywords:*Psychological Manipulation, Phishing, Spoofing, Social engineering*

I. Introduction

In this digital world every day we hear regarding virus and hackers. In spite of having antivirus and antispyware software the systems can't be protected. In our country, still the IT penetration is not up to that extent as in USA or Europe countries. [1] Computers get hijacked by hackers or infected by Virus, Worms and Spywares that can affect the working to a great extent. Nowadays, communication has distributed over a variety of online communication channels. In addition to E-mail and Instant Messaging, Web 2.0 services such as Instagram, Facebook, and other social networking sites are playing a major role. [2]Currently, communication via internet has some security loopholes and often been misused to purloin sensitive and confidential information. Security management of Information system (IS) is not only dependent on technological measures but also on managerial schemes. Technological methods are being developed to cop up various security issues but the human factor that contribute significant security breaches are neglected. The salient key to deal with potential aggressors is a combination of technical, behavioural, and procedural countermeasures. Social engineering is a process to manipulate a human being and exploit the human behaviour to retrieve sensitive data. [3]The positive result of this social engineering attack completely depends on the natural instinct of human. The working of social engineering is shown in Figure 1.

Figure 1: How Social Engineering works

II. Social Engineering Techniques

Social engineering techniques are categorized in two major categories: Human-based social engineering technique and Technology-based social engineering technique. Human-based refers to a human interaction to execute the suitable attack. Technology-based refers to interact with an electronic interface that attempts to perform the desired action.

A. Human-based Social Engineering Techniques

a) Shoulder Surfing: It is an effectual mean to obtain desired sensitive information as we can stand next to a person and watch as they enter any password, PIN number and use that data to breach the security. [10]
b) Hoaxing: It is a social engineering technique in which the social engineer provides a false information to the target in such a way that the target have to believe every word. [1]
c) Tailgating: Tailgating is a social engineering technique in which an unauthorized person follows an authorized personnel into a restricted location, usually to purloin confidential data. [11]
d) Creating Confusion: The Social engineer create a confusing scenario in a way that the target get confused and the social engineer grabs an opportunity from this confusion to retrieve sensitive data. [9]
e) Dumpster Diving: It is a technique is implemented to obtain confidential data that can be utilize to breach the security. The social engineer can get confidential information that can be used to assist an attacker to gain access to any restricted data or area. [11]
f) Impersonation: This technique is widely used to gain access to a computer system or network in order to commit fraud, industrial espionage or identity theft. There are basically five scenarios where impersonation can be used to create a successful social engineering attack: [12]

i. Helpdesk: Social Engineer calls the help desk pretending to be someone who already has authorizations to confidential information. Help desks are trained to be very helpful to their customers and often give out sensitive. [1]
ii. Authorization: The social engineer use the name of an employee of the organization who has the authority to authorize access to sensitive data. He/she may call the target and claims that the Senior Manager, Mr. Z, requested that information. [6]
iii. Tech Support: The social engineer pretend to be technical support executive. He/she can explain a false network problem that need troubleshooting and tells the target that he/she narrow down the problem to a certain computer. He/she asks for the user id and password of the computer. Unless the target has been properly educated in security practices, they will likely to give the sensitive information asked. [7]
iv. Technician: People usually don't suspect on telephone or computer technicians. Acting as a technician, the attacker can hide a snooping device or look around for passwords or other sensitive information without the permission of the owner. [8]
v. Mail: It is another effective means of social engineering to get sensitive information because it is not costly and people have tendency to trust the written word. The attacker can easily send the fake mail through any reputed postal service and ask for permission to get confidential information pretending to be the manager of his/her organization. [1]

g) Reverse Social Engineering: It is a human based attack in which an attacker persuades the target in believing he/she has a problem or might have a certain type of problem in the future and he can fix the problem and ask for the username or password to move forward with the solution.[1]

B. Technology-based Social Engineering Techniques

a) Pop-Window: The social engineer sends a software using physical storage disks or via internet on the target system, this software will open a dialog box on the screen with the message 'Network connection has been lost". The user is prompted to verify his/her username and password, then the program send the information back to the social engineer via internet. [4]
b) E-Mail Attachment: The attacker sends a spy software with the e-mail attachment that can be able to snoop on your computer and send the confidential information back to the attacker. [4]
c) Phishing: The social engineer form a fake login webpage of a website and lure the target using that. This fake login webpage seems very real to a normal person that's why most of the time target enter their credentials to get the access of their profile, but in real the credentials has been sent to the attacker by the fake login webpage. [1]
d) Brand Spoofing: The attacker spoofs any renowned brand by creating fake website or sending fake e-mails to the random people, then the people who are receiving the services from that company can reply with their confidential information. [1]
e) Baiting: It involves dangling something that excite you to take an action. Social engineer leaves any kind of storage device to be found by the target and once the person used that device using any computer then it infects the computer and the entire network of the company which allow the attacker to access the confidential data. [4]

III. Comparison of Social Engineering Techniques

A comparison of the social engineering techniques using seven different parameters on the basis of the advantages and disadvantages of all the techniques is done. Table 1 shows a tabular comparison of human based social engineering techniques and table 2 shows a tabular comparison of technology based social engineering techniques.

Seven parameters that are used to compare all the techniques are as follows:

1) Time Consumption: It defines how much time it will to execute the technique.
2) Information Provided: It defines information given to the target is true or false.
3) Role playing: It defines whether the attacker pretending to be someone else during executing the technique or not.
4) Intensity of Attack: It defines the intensity of technique in terms of risk factor involved.
5) Effectiveness: It defines the efficiency of the technique performed.
6) Targeted/Un-targeted: It defines whether the attack is for a specific person or not.
7) Direct/Mediated: It defines whether the attack is being performed directly on the target or performed indirectly.

Table 1: Human Based Social Engineering Techniques

Parameters → / *Techniques* ↓	**Time Consumption**	**Information Provided**	**Role Playing**	**Intensity of Attack**	**Effective-ness**	**Targeted/ Un-targeted**	**Direct/ Mediated**
1. Impersonation	Most	False	Yes	High	Most	Targeted	Direct
2. Hoaxing	Less	False	Yes	Low	Less	Targeted	Direct
3. Creating Confusion	Least	False	Yes	Moderate	Moderate	Un-targeted	Direct/ Mediated
4. Dumpster Diving	Moderate	No Need	No Need	Low	Less	Un-targeted	N/A
5. Reverse Social Engineering	Less	False	No Need	Moderate	Moderate	Targeted/ Un-targeted	Direct/ Mediated
6. Shoulder Surfing	Less	No Need	No Need	Low	Less	Targeted	N/A
7. Tailgating	Less	No Need	No Need	Low	Moderate	Targeted	N/A

Table 2: Technology Based Social Engineering Techniques

Parameters → / *Techniques* ↓	**Time Consumption**	**Informati on Provided**	**Role Playing**	**Intensity of Attack**	**Effective-ness**	**Targeted/ Un-targeted**	**Direct/ Mediated**
1. Pop-up Window	Less	False	No	Low	Moderate	Targeted	Direct
2. Mail Attachment	Least	False	No	Low	Moderate	Targeted	Direct
3. Phishing	Moderate	False	No	Moderate	High	Targeted/ Un-targeted	Direct
4. Brand Spoofing	Most	False	Maybe	High	Moderate	Un-targeted	Direct
5. E-mail Scam	Less	False	No	Low	Moderate	Un-targeted	Direct
6. Baiting	Moderate	False	No	Low	High	Targeted/ Un-targeted	Direct/ Mediated

IV. Conclusion

Companies might have the most secure network or clear policies still human are unpredictable due to curiosity and greed without concern for the consequences. A conundrum of social engineering is that human being is not only the biggest problem and security threat but also the optimum solution to defend against social engineering attacks. Policies and procedures must be established by the organizations that define the roles and responsibilities of an employee to defend against social engineering attacks. As well as organization must ensure that, these policies and procedure are executed by users properly hence regular training needs to be provided.

References

[1]. Mosin Hasan, Nilesh Prajapati and Safvan Vohara. "CASE STUDY ON SOCIAL ENGINEERING TECHNIQUES FOR PERSUASION," International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.2, June 2010.

[2]. Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl. "Advanced Social Engineering Attacks," Journal of Information Security and Applications, July 2014.

[3]. Xin (Robert) Luo, Richard Brody, Alessandro Seazzu, Stephen Burd. "Social Engineering: The Neglected Human Factor for Information Security Management," Information Resources Management Journal, 24(3), 1-8, July-September 2011.

[4]. P. S. Maan and Manish Sharma. "Social Engineering: A Partial Technical Attack," IJCSI International Journal of Computer ScienceIssues, Vol. 9, Issue 2, No 3, March 2012.

[5]. https://en.wikipedia.org/wiki/Social_engineering_(security)"Social engineering (security)".

[6]. Thomas R. Peltier. "Social Engineering: Concepts and Solutions,"Vol. 33, Issue 8, December 2006.

[7]. https://en.wikipedia.org/wiki/Technical_support_scam"Technical support scam".

[8]. Steven DeFino, Larry Greenblatt "Official Certified Ethical Hacker Review Guide: For Version 7.1," Cengage Learning, 2012.

[9]. White paper: Avoiding Social Engineering and Phishing Attacks,Cyber Security Tip ST04-014, by Mindi McDowell,Carnegie Mellon University, June 2007.

[10]. https://www.giac.org/paper/gsec/4202/social-engineering-information-bandits/106723 "Social Engineering: Information Bandits".

[11]. https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914"SocialEngineering: Manipulating the Source".

[12]. Alfred Basta, Nadine Basta, Mary Brown. "Computer Security and Penetration Testing," 2nd edition.