Social Engineering on Social Networking sites

M.Puneeth, Jasmine Shafi Farha, M.Yamini, N.Sandhya

Abstract— *The number of users will be more for social networking sites and its information base will be more, due to the more number of users there may be a more chances for exploitation for the people's vulnerabilities Influencing or making the people to perform some action that which is in favor of attacker or that which makes the attacker to attack is called as social engineering.In this journal we are going to describe about the social engineering and the attacks that which are possible on social networking sites*

Keywords— Decryption, Information Security, Privacy, Social Engineering

I. INTRODUCTION

In the information Security generally the threats are possible due to the vulnerabilities that which are on the sites or the vulnerabilities due to people. The threats that which are based on technology is discussed well and in many studies it is addressed well, for the researchers the threats that which are based on human are somewhat less attractive in the field of information technology. This is because it is very difficult to understand the human behavior and their mentality this leads to the human vulnerability [2]. Social Engineering attack is an attack that which helps the attacker to attack

The social networking sites are first appeared in 1997 with a social networking site named sixdegrees.com, so people are very much interested in creating their profile and to share the information with different types of people in different ways depended upon the nature of the website, these social networking sites started introducing the different types of features in their websites for attracting the people, institutions, organisations, companies etc. As the number of users are increasing day by day then the transmission of their secret and private message will also get increasing. These social networking sites will attract the people, companies and also the attackers to extract the information that which is shared by the people or companies [4]. Every time there will be a threat for the information so that the message can be modified or intercepted or exposed for preventing these things availability and confidentiality are the main principles for securing the information

II. STUDY OF SOCIAL ENGINEERING

Social engineering was reported as the top most security threat in the year 2005 by IOMA (Institute Of Management and Administration)[1].They said that the social engineering attack is the threat that which is based on the human. According to the survey that which has been done by the security professionals of Canada, USA, United Kingdom, Australia, New Zealand and Germany. The victims of the social engineering attacks are around 48% and they experienced twenty five more attacks in the years 2010,2011 .The social networking sites are the sites that which are most possible ways for the attackers or spammers or for the social engineers who will attack the users with their vulnerabilities. Studies said that the more number of users are sharing their secret or private messages through the social networking sites only so that their messages are exposed to the spammers and social engineers. ENISA (European Network and Information Security Agency) said that social engineering attacks are dangerous sites that which are the ways for the social engineers and attackers to extract the messages and the secret information that which is shared by the users or the organizations. The social engineers will take the advantage of irresponsibility of the users or organizations and they will start attacking their secret information due to the vulnerability of the users the social engineering attack is a low cost and it is also called as effective form for attack. Kowalski and Nohlberg proposed the Holistic model of the social engineering attacks[3]. The model that which is proposed by them was related to the situations of the real life There are some unique and specific characteristic's for social networking sites.The factors that which lead the users to take the decisions on poor security into the three categories Hardee, west, May horn and Mendel the three categories are user factors, technology factors, environmental factors.

2.1. User factors: The user factors like limitations for problem solving, experience and heuristic decision making

2.2. Technology Factors: The technology factors are the factors that which appear as credible and that which is relevant to personal email and a website that which is used to trick the users

2.3: Environmental Factors: Environmental factors are the factors that which involves time pressure, where the users cannot identify the details of the threat.

III. SOCIAL ENGINEERING MODELS IN SOCIAL NETWORKING SITES

3.1. Phase base model:

For the modelling of social engineering in the social networking sites we have to know how the social engineer influences the user to perform an action in his favors for attacking the victim. There are eight phases for a social engineer for influencing the user to perform an action the probability of the social engineering attack depends upon how well the eight phases are performed by the social engineer

3.1.1. Phase 1: For gathering the information the gates that which are suitable for Social Networking Sites. In case of Phase 1 the gathering of information about the victim takes place for understanding their vulnerabilities. The gathered information involves their interests, hobbies, name, age, work place, occupation .Some information that which is gathered may not be that much useful

3.1.2. Phase 2: In phase 2 the determination of tactic and the plan development takes place, the plan is developed by using the information that which is gathered in the phase 1.In this phase the techniques like phishing takes place that is sending a link to the victim and influencing or making the victim to open that link the social engineer should plan according to the interests of the victim so that he can easily open the link

3.1.3. Phase 3: In phase 3 the people are attracted to the wrong information that which is given by the social engineer because of their psychological characteristics and their interests so that they are attracted to the wrong information that which is given by the social engineer that which is based on their interests studies has proved that the social engineering attacks are mainly caused due to the psychological weaknesses of the victims

3.1.4. Phase 4: In phase 4 the gates that which are suitable for social networking sites are used for reaching the victim. This is an effective and cheapest means for reaching the victim

3.1.5. Phase 5: In this phase 5 the social engineer should act in some different manner he may act as a good friend, very poor person and based upon the information gathered about the victim he have to act in the suitable character that which may be helpful for the social engineer for reaching the victim easily

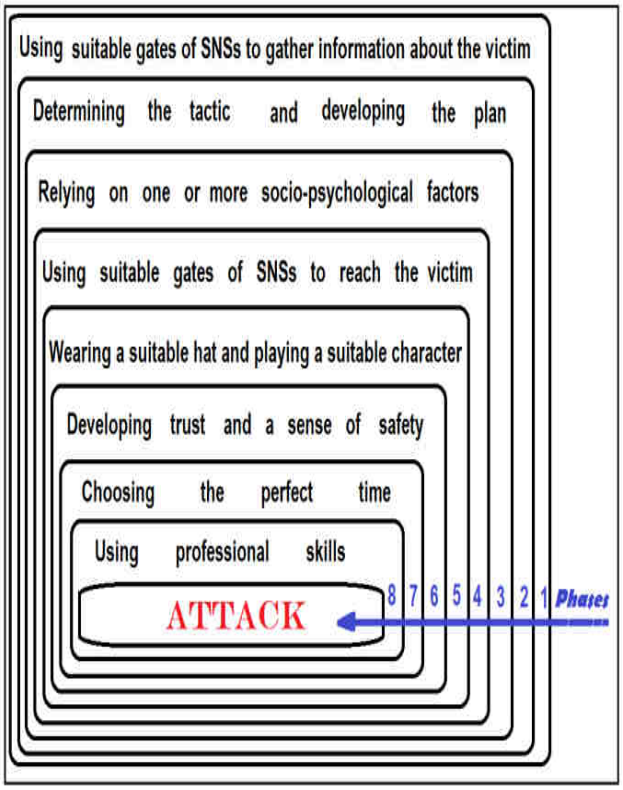

Fig. 1 social engineering attacks that which is based on phases

3.1.6. Phase 6: The social engineering is depended mainly upon the two factors they are trust and safety. These two factors are mainly depended upon the psychology of the victim and the victim experiences. When the victim trusts the social engineer then possibility of the attacks will be high on the victim

3.1.7. Phase 7: The perfect time should be chosen for attacking the user or victim so that the victim will be attacked by the social engineer when it is a perfect time for him to attack

3.1.8. Phase 8: In this last phase the professional skills of social engineer takes place so that in this final stage the social engineer should use all his professional skills for attacking the victim

3.2. Source Based Model:

There are three sources of threats for social networking sites they are insecure privacy settings, Friendship and connection with strangers, Insecure dealing with content

3.2.1: Insecure Privacy Settings: The classification of social networking sites takes place based on the relationships like friend, friend of friend etc. Firstly the phishing link will be sent to the friend and after the exploitation takes place then the link is sent to the friends of the victim and their accounts are exploited and the privacy will be modified

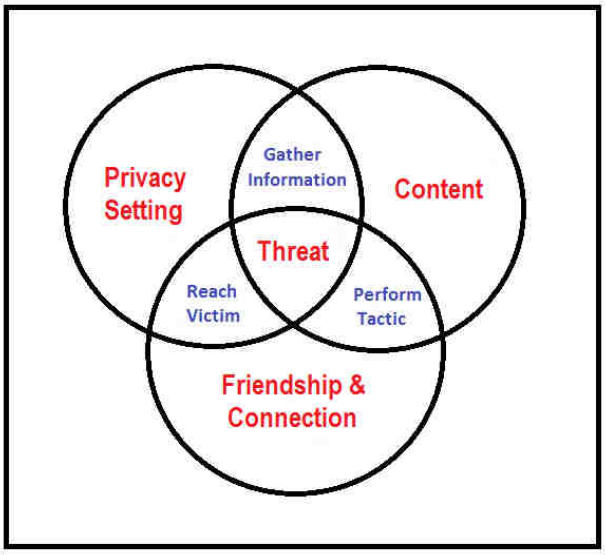

Fig. 2 Source based model for social engineering in Social Networking Sites

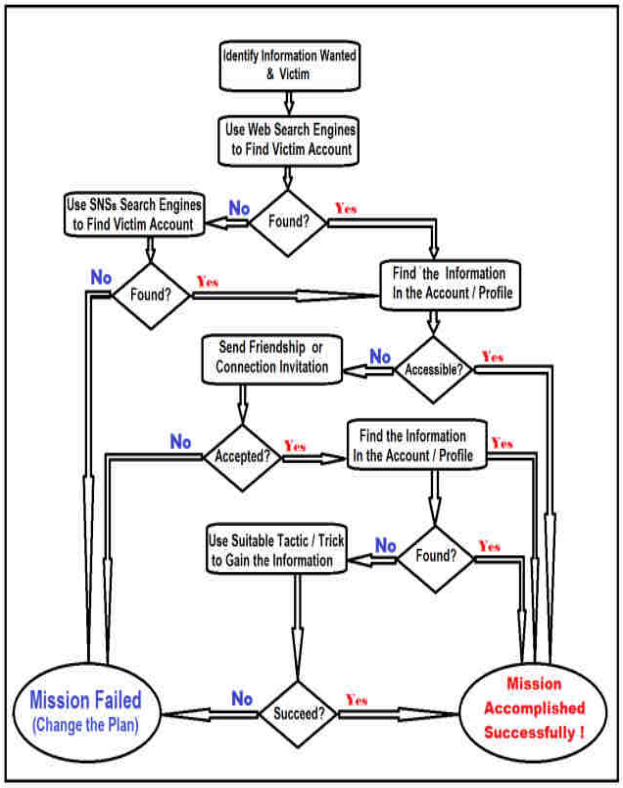

Fig. 3 Information gathering for social networking sites

3.2.2. Friendship and the connection with strangers:

In this case the human beings have some mentality or some type of psychological things that which makes them to make friendship with the strangers. Social engineer takes an advantage of these type of people's mentality and starts doing the exploitation by taking their character as an advantage

3.2.3. Insecure dealing with the Content:

In this model the insecurity of the victim causes for exploitation .The insecurity of the victim will be taken as advantage by social engineer and then he will attach a virus file or some threats to the photos or videos or for any other files then the exploitation starts after the file is executed

IV. CONCLUSION

We have studied about the social networking sites and the social engineering with the knowledge of social engineering on social networking sites we have applied this in social engineering by using se-tool kit in Kali Linux

V. RESULTS

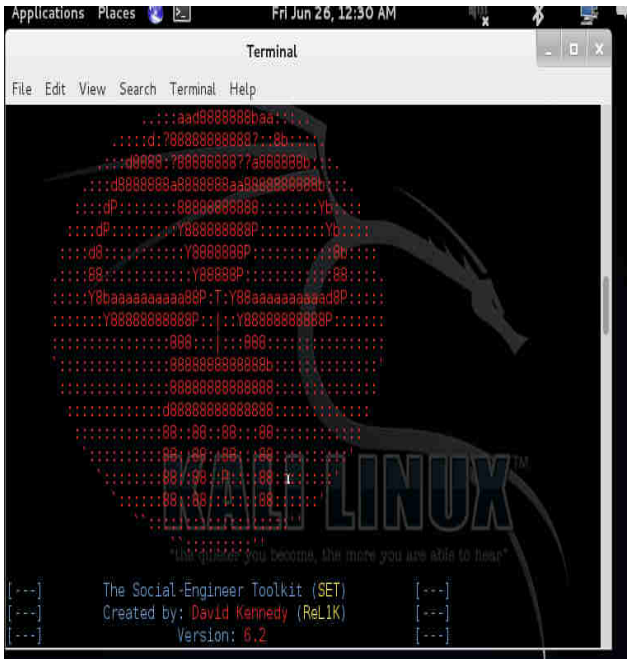

Fig. 4: se-tool kit in Kali Linux

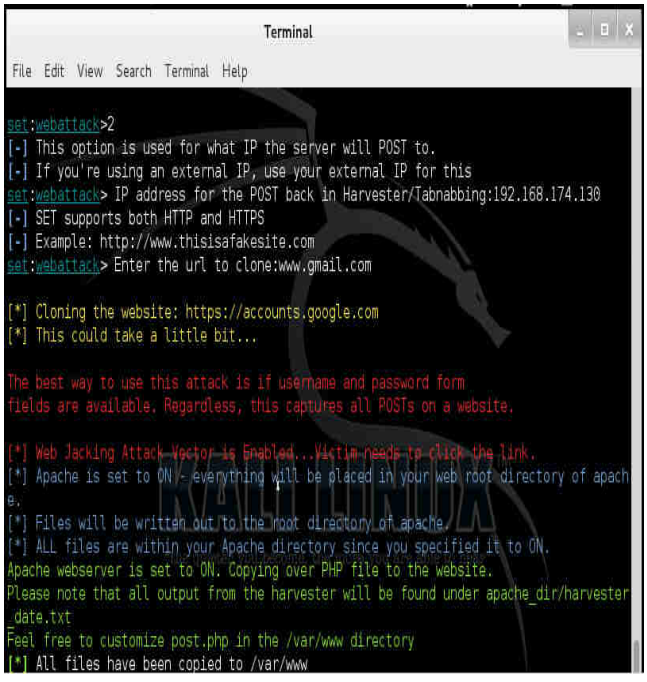

Fig. 5: An URL with 192.168.174.130 is created as a Gmail account

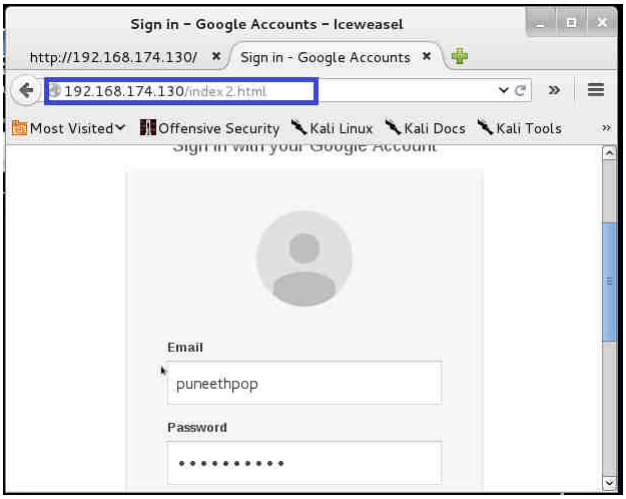

Fig. 6 when victim opens the URL that has been sent by the social engineer

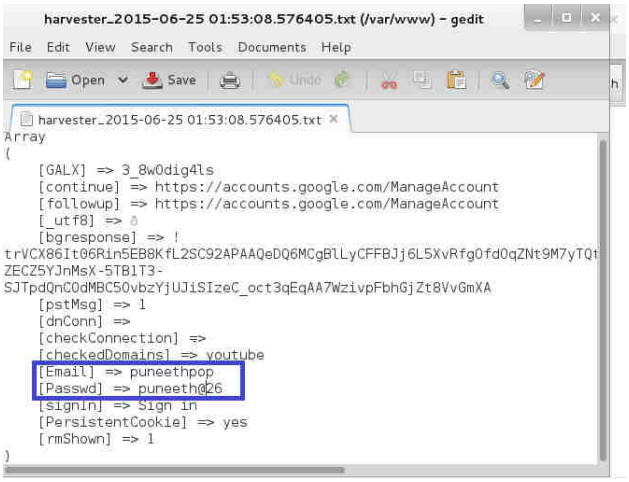

Fig. 7 victims Email ID and password exploited by social engineer

REFERENCES

[1] Abdullah Algarni and Yue Xu, "social Engineering in Social Networking Sites Phase-Based and Source-Based Models" International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 3, No. 6, December 2013

[2] Xin (Robert) Luo, Richard Brody, Alessandro Seazzu, Stephen Burd, "Social Engineering:

[3] The Neglected Human Factor for Information Security Management" Information Resources Management Journal, 24(3), 1-8, July-September 2011

[4] Brandon Atkins, Wilson Huang, "A Study of Social Engineering in Online Frauds", Open Journal of Social Sciences2013. Vol.1, No.3, 23-32 Published Online August 2013

[5] Dr. Saswati Gangopadhyay, Ms Debarati Dhar, "SOCIAL NETWORKING SITES AND PRIVACY ISSUES CONCERNING YOUTHS", Article - 2 Global Media Journal-Indian Edition, Summer Issue/June 2014/Vol. 5/No. 1