International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 01, January 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

HACKING: SOCIAL ENGINEERING ASPECT

Sukhminder Dass Bawa

Assistant Professor, Computer Science & I.T.

A.S.S.M. College Mukandpur(S.B.S. Nagar ,Punjab)

ABSTRACT

The human brain is not protected from hacking. Social engineering is the skill of trapping user into performing unsafe actions or revealing confidential information to attackers. Knowing the tricks used by hackers to trick users into releasing vital login information among others is fundamental in protecting computer systems.

In this research paper, the common social engineering attacks and the security measures to counter them have been explored.

Keywords: Authorized, Communication, Phishing, Security, Social engineering

I. INTRODUCTION

Social engineering is the art of manipulating people so they give up confidential information. The types of information the hackers are seeking can vary, but when individuals are targeted the hackers are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Hackers use social engineering tactics because it is usually easier to exploit your natural inclination to trust than to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Security is all about knowing who and what to trust. Knowing when, and when not to, to take a person at their word; when to trust that the person you are communicating with is indeed the person you think you are communicating with; when to trust that a website is or isn't legitimate; when to trust that the person on the phone is or isn't legitimate; when providing your information is or isn't a good idea.

Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. It doesn't matter how many locks and deadbolts are on your doors and windows, or if have guard dogs, alarm systems, floodlights, fences with barbed wire, and armed security personnel; if you trust the person at the gate who says he is the pizza delivery guy and you let him in without first checking to see if he is legitimate you are completely exposed to whatever risk he represents.

In this research paper following areas has been explored as-far-as social engineering is concerned

- What is social engineering?
- Social Engineering Cycle
- Popular types of social engineering attacks

ISSN (O) 2454-9665
ISSN (P) 2454-0663

- Social Engineering Counter Measures

II. WHAT IS SOCIAL ENGINEERING?

Social engineering is the art of psychologically manipulating users of a computing system into revealing confidential information that can be used to gain un-authorized access to a computer system. The term can also include activities such as exploiting human kindness, greed and curiosity to gain access to restricted access buildings or getting the users to install backdoor software.

III. SOCIAL ENGINEERING CYCLE:

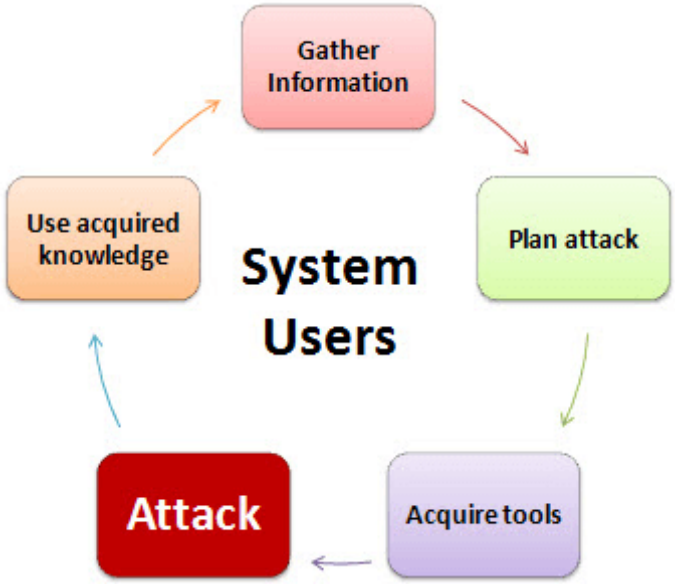

Fig: 3.1

Gather Information:

This is the first stage, the attacker learns as much as he can about the intended victim. The information is gathered from company web sites, other publications and sometimes by talking to the users of the target system.

Plan Attack:

The attacker outlines how he/she intends to execute the attack

Acquire Tools:

These include computer programs that an attacker will use when launching the attack.

Attack:

Exploit the weaknesses in the target system.

Use acquired knowledge:

Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders etc. is used in attacks such as password guessing.

IV. POPULAR TYPES OF SOCIAL ENGINEERING ATTACKS:

ISSN (O) 2454-9665
ISSN (P) 2454-0663

Social engineering attacks can take many forms. Following is the list of the commonly used attacks.

Familiarity Exploit:

Users are less suspicious of the people they are familiar with. An attacker can familiarize him/herself with the users of the target system prior to the social engineering attack. The attacker may interact with users during meals, social events etc. This makes the attacker familiar to the users. The attacker may ask for answers to questions such as where you met your spouse, the name of your high school maths teacher etc. The users are most likely to reveal answers as they trust the familiar face. This information could be used to hack email accounts and other accounts that ask similar questions if one forgets their password.

Tailgating: This practice involves following users behind as they enter restricted areas. As a human courtesy, the user is most likely to let the social engineer inside the restricted area.

Intimidating Circumstances:

People tend to avoid people who intimidate others around them. Using this technique, the attacker may pretend to have a heated argument on phone or with a co-conspirator. The attacker may then ask users for information which would be used to compromise the security of the users' system. The users are most likely to give the correct answers just to avoid having a confrontation with the attacker. This practice can also be used to avoid been checked at a security check point.

Phishing:

This practice uses deceit to obtain private data from users. The social engineer may try to impersonate a genuine website such as yahoo and then ask the unsuspecting user to confirm their account number and password. This practice could also be used to get credit card information or any other valuable personal data.

Spear phishing:

It is phishing, tailored for a specific individual or organization.

Exploiting human greed:

Using this practice, the social engineer may lure the user with promises of making a lot of money online by filling in a form and confirm their details using credit card details etc.

Baiting:

Baiting is exploiting human curiosity, using this practice; the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up. The user will most likely plug the flash disk into the computer. The flash disk may auto run the virus or the user may be tempted to open a file with a name such as Employees Revaluation Report 2017.doc which may actually be an infected file.

Scareware:

Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

V. SOCIAL ENGINEERING COUNTER MEASURES:

ISSN (O) 2454-9665
ISSN (P) 2454-0663

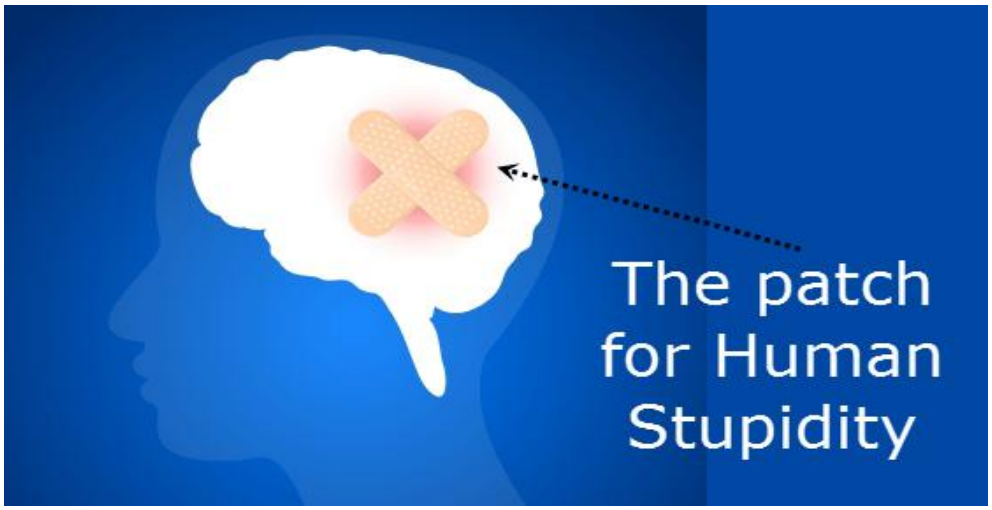

Fig:5.1

Educate yourself:

First mitigation is security through education, if people aren't educated to the types of attacks being used, and then they cannot possibly defend against them.

Be aware of the information you're releasing:

This tip encompasses both verbal and social media like Face-book or Twitter communication. Most of the social engineers would get deep background on their targets before moving.

Determine which of your assets are most valuable to criminals:

Determine which of your assets are most valuable to criminals. Focus on protecting those assets from social engineering attacks.

Write a policy and back it up with good awareness training:

Once you know which of your assets are most tempting to criminals and the pretexts they are most likely to use to pursue them. Write a security policy for protecting your data assets, then back up that policy with good awareness training.

Keep your software up to date:

Hackers using social engineering techniques are often seeking to determine whether you are running un-patched, out-of-date software they can exploit. Staying on top of patches and keeping your software updated can lessen a lot of risk.

Give employees a sense of ownership when it comes to security:

Security programs in India are failing miserably. The reason is that employees do not make security a personal thing. They need to feel a sense of ownership when it comes to security.

When asked for information, consider whether the person you are talking to deserves the information he/she is asking about:

Whenever you are in a conversation with someone you do not know, before you answer a question he/she asks, make sure he/she deserve to know the information that he/she is asking about.

Watch for questions that don't fit the pretext:

If a person asks a question that does not fit the persona he/she presents, it should set off alarm bells.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

Regularly carry out penetration tests:

Security experts recommend that IT departments should regularly carry out penetration tests that use social engineering techniques. This will help administrators learn which types of users pose the most risk for specific types of attacks while also identifying which employees require additional training. Security awareness training can go a long way towards preventing social engineering attacks. If people know what forms social engineering attacks are likely to take, they will be less likely to become victims.

VI. CONCLUSIONS

- Social engineering is the art of exploiting the human elements to gain access to un-authorized resources.
- Social engineers use a number of techniques to fool the users into revealing sensitive information.
- Social engineering poses a significant threat to individuals as well as to the firms of all sizes.
- The security risks of social engineering are significant, and organizations must address social-engineering threats as part of an overall risk-management strategy. The best way to mitigate the risk posed by rapidly evolving social-engineering methods is through an organizational commitment to a security-aware culture. Ongoing training will provide employees with the tools they need to recognize and respond to social-engineering threats, and support from the executive staff will create an attitude of ownership and accountability that encourages active participation in the security culture.

REFERENCES

[1] Petty, Richard E; Brinol, Pablo; Tormala, Zakary L. “Thought Confidence as a Determinant of Persuasion:The Self-Validation Hypothesis. Journal of Personality & Social Psychology: Vol. 82(5), May 2002, 722-741.

[2] Petty, Richard E.; Fleming, Monique A.; Priester, Joseph R.; Feinstein, Amy Harasty. “Individual versus group interest violation: Surprise as a determinant of argument scrutiny and persuasion.” Social Cognition: Vol. 19(4), Aug 2001, 418-442.

[3] Sagarin, Brad J.; Cialdini, Robert B.; Rice, William E.; Serna, Sherman B.“Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion.” The Journal of Personality & Social Psychology: Vol. 83(3), Sept 2002, 526-541.

[4] Rusch, Jonathan J. “The ‘Social Engineering’ of Internet Fraud.” United States Department of Justice . http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm.

[5] http://www.guru99.com/how-to-hack-using-social-enginering.html

[6] http://www.social-engineer.org/

[7] https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[8] http://www.darkreading.com/partner-perspectives/intel/techniques-lures-and-tactics-to-counter-social-engineering-attacks-/a/d-id/1319401