Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Real Time System for Phishing Attack and It's Safeguard

Puneet[1], Monica Goyal[2]
[1]Student, Department of Computer Engineering, GKU, Talwandi Sabo, Punjab, India
[2]Assistant Professor, Department of Computer Engineering, GKU, Talwandi Sabo, Punjab, India

Abstract: Social engineering is a hot spot in the field of information security. It is an Art of Manipulation to extract confidential information by using psychological triggers to stimulate emotions such as fear, greed, excitement or guilt that will lead the people to respond quickly without going in detail. The main difficulty in most of social engineering attacks is inability of victim to identify such attacks. No security will work if the person behind the system provides the security key to the hacker either intentionally or unintentionally.
This paper consists of study of social engineering attacks. Subsequently injection, detection and prevention techniques are outlined as a proof of concept and countermeasures. In today's internet world being attacked by viruses and hackers is very common but people are still not aware of dangerous effects of such activities. A tool using python has been designed to show hazardous effects of various attacks. It was observed that these attacks can exploit user's security information.

Keywords: Social Engineering (SE), Social Engineering Toolkit (SET), Phishing.

I. INTRODUCTION

Social engineering is a non-technical method to breach some useful information from the system or from the network. It was first introduced by Kevin D. Mitnick. The primary aim of Kevin D. Mitnick was to make an example of him-self. Working with social engineering is started in the age of seventeen. A book named *Art of deception* in the year 2002 about social engineering is published by Kevin. In this book human factor is the main reason of being victim of social engineering attack. Human factor is the weakest security link in social engineering attacks because people generally sympathize with anyone that claims to be in trouble or with those people whom they feel to be a trusted person. Mitnick said social engineer use this approach to exploit their victim. A social engineer will always use psychological triggers to stimulate emotions such as fear, Excitement or guilt that will lead the people to respond quickly without going in detail. There is no such technology as such that can prevent you from social engineering attacks. These can only be made difficult by keeping some security measures in account such as keeping the people out of decision making process, providing employees proper education and training. Decide some security policies for the employees to keep the information confidential and developing effective controls to counter potential security threats [1].

II. LITERATURE SURVEY

Social engineering is the technique which is used to gather information by exploiting system security. It is an illegal method of extracting some useful information from system or network. For performing social engineering attacks hacker firstly gathers information about victim and then start developing relationships with victim to gain their trust. After maintaining relationships hacker starts performing its objective and starts stealing information from victim [1]. A social engineering attack detection model (SEADM) for the workers to detect social engineering attacks who are working in the call centre environment. The proposed model is effective and efficient to determine if attacker tries to manipulate the worker for disclosing information to which the attacker does not have authorization. The proposed model detects the social engineering attacks by breaking the decision making process into manageable components [4]. To perform social engineering attacks SET has been developed to perform some social engineering attacks. Social Engineering Toolkit (SET) was designed by David Kennedy [3].
Hasan M. et. al. [6] discussed the inner working of social engineering it provided the case study of anti-virus for implementation of social engineering. He checked how effectively the social engineering works on the Linux. This paper concludes that an organization should establish security policies which define responsibilities of employees to avoid social engineering attacks. The proposed method provides 100% success using social engineering techniques. Techniques for defending social engineering were also introduced. On the basis of social engineering attack methodology two types of attacks are there: Computer based attacks are those attacks which are done through computer software for example Phishing, mass mailing attacks etc. Human based attacks are performed by interaction of persons to retrieve some useful kind of information. For example, asking a human being for their credit card number by making them a call that you are calling from a bank which is providing you the better loan facilities [8]. Client side attacks are those attacks which enter into system from applications on client's machine. Client side attacks are much famous than server side attacks as end user's machine is considerably less protective then server. In client side attacks the client initiates the connection that may cause an attack. In client side attacks if a server doesn't interact with client than it can't harm the system [9].

Till now lots of social engineering attacks are available. Among these attacks phishing is most common and popular attack these days. Phishing is a technique of creating a webpage that looks similar to original one .The link to that fake page is sent to victim by embedding in mail. When the user click on the link, a phished page appears. When user enters his/her details on phished page, information are directly stored to hackers database and redirect the victim to original page. Phishing is such a technique in which victim can't even think of that he/she has been phished [5]. A combination of social engineering and technical subterfuge for stealing the information of user is called phishing. According to Gartner, 2.4 million users were victim of phishing attacks. In May 2005, 34% of people reported to anti-phishing organization in the period of May 2005 to May 2006. To avoid such attacks Finjan introduced an anti-phishing behavior based technology which decides allowing, blocking or neutralization of contents [17]. An analysis of online behavior of 4000 students of carriage melon university students shows that the students have not been aware of the ways in which their personal information is being stolen [7]. Infectious media generator attack infects any removable media like USB and whenever that media will be connected to any system infectious material will automatically execute itself on the machine if autorun feature of windows is enabled. The infectious code in media may exploit any information. Such attacks may change the file formats in system or can cause many other events [16].

In summary, from the work done till now, we may say that phishing scams are increasing day by day after the year 2005.Most of the survey shows that people are not aware of the exploitation caused by such attacks. So people generally ignores some minor issues like checking the URL of website properly or people gets attracted towards some mails which are just meant to steal information. In our we are showing the proof of concept of mass mailer attacks which is enhanced to phishing attack. The main aim of our project is to make the victim aware of such attacks. So that in future the effect of such attacks may be reduced.

III. PROBLEM DEFINITION

Network based attacks are very common these days which can produce halting of services and stealing or misleading important information of network users. In this reserch we have defined two types of attacks: Phishing attack and mass mailing attack. These attacks are performed to show the hazardous effects of such attacks on user. By doing so, user can be made aware of staying away from such attacks. Detecting such attacks and preventing him from being the victim, counter measures for these attacks has been also proposed in our work.

IV. IMPLEMENTATION

In proposed approach client-server model has been used. Backtrack has been used to host server, and Window7 has been used as client side operating system. An environment of SET (social engineering toolkit) has been created in python script. When the user will start running the code a menu will appear showing various selections that user can make. It can be viewed as shown in figure 2

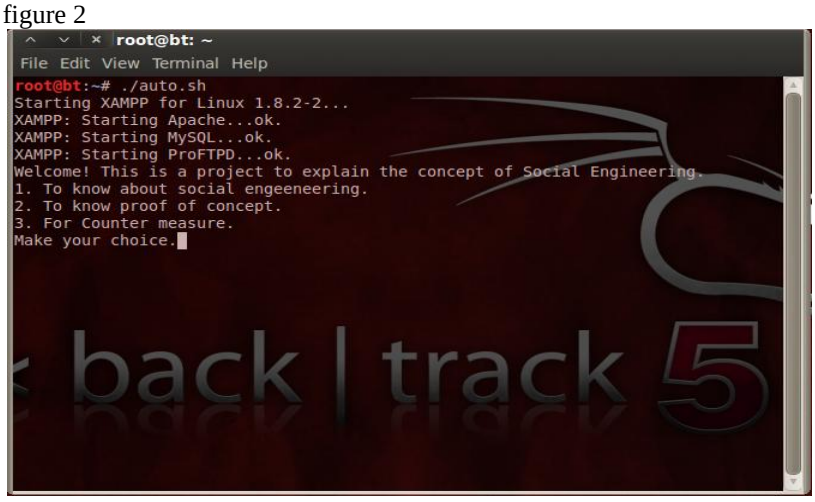

Figure 1*:* SET environment created in python

From above shown figure if user choose option 1 then it will give user the introduction of some popular client side attacks such as phishing, mass mailer attack etc. If user has chosen option 2: Proof of concept, then user can select either implementing phishing or mass mailer attack. If the client chooses option: Mass Mailer attacks then using python script mail will be sent to single user or to multiple users. Figure 3 shows the mail sent by mass mailor attack.

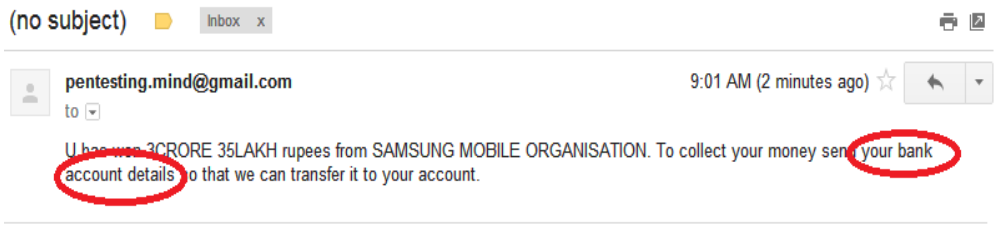

Figure 4: -Mail sent by mass mailer attack

The mail sent using mass mailer attack consists of phishing link. That mail consists of spoofed phishing page as shown in figure below. By clicking on this link client will be redirected to phished page and may lose his/her personal information.

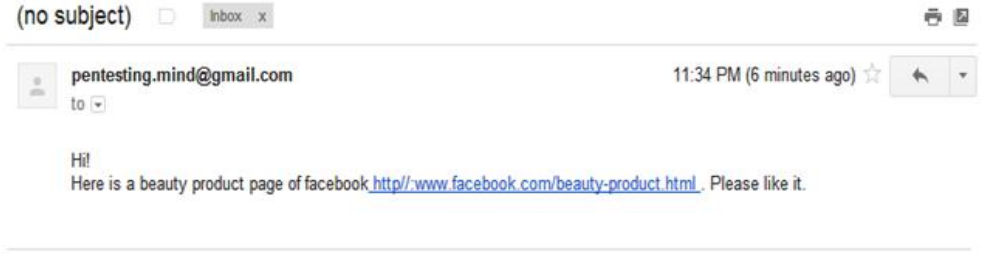

Figure 5: Phishing link embedded in email

When user receive that mail is in his/her inbox and click on phishing link then a phishing page appears.

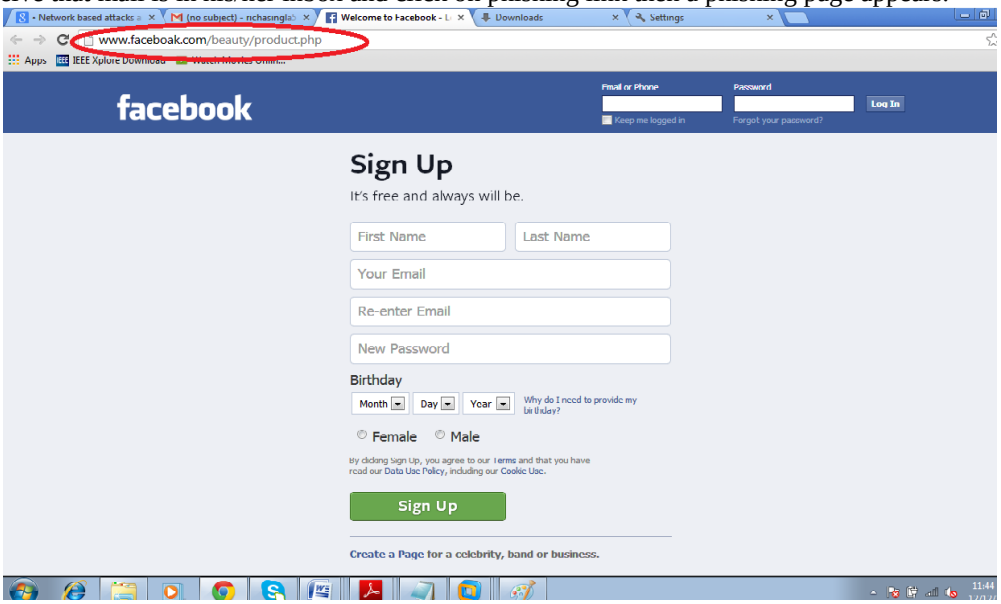

Figure 6: Phishing page

The information inputted by client, after pressing on Log in button will be stored to hacker's database. The figure shown below shows the server database containing the details of the victim.

Figure 4.8: Database containing stolen information

Mass mailer attack mails may consist of spam mails, worms, Trojan horses or any other spoofed object in it. The mails sent throw mass mailer attacks may contain message that attracts the victim easily. One of such mail has been shown in figure below. Many victim will send their credit card details to get their prizes and the hacker may use this information in one or another way.

Last but not least at the end to prevent user from these attacks countermeasures of attacks have been proposed by choosing option 3: Countermeasures. A python script has been used to locate the shell. After locating the shell, using a tool ns-lookup, client can check by setting the server type to name server, whether the requested page is authoritative or non-authoritative. If the answer is non-authoritative then the requested page can be the phished page.

V. CONCLUSION AND FUTURE WORK

Conclusion

Phishing is a famous online attack in today's internet world. Phishers use various social engineering tools to attract the victim. Most of people are not aware of such attacks and the dangerous activities caused by such attacks. So to understand the proof of concept of mass mailer attacks and phishing attacks both attacks has been implemented and hazardous results of these attacks has been described in section 4. Phishers use the resembled pages of some well known sites and acquire the secret information of user. In most of the cases victim may not even realize that he/she has been phished. So to keep user safe from such attacks countermeasure of attacks has been implemented. The tool designed works well for performing phishing attack and mass mailer attacks.

Future Scope

The implement proof of concept using social engineering which can further be enhanced to various other social engineering attack vectors like tabnabbing attack method, infectious media generator, etc. In this reserch nslookup tool had been used to demonstrate authoritative concept which can be enhanced to use Dig latest version of DNS query which can support IPv6.

REFERENCES

[1] Mitnick, Kevin D., and William L. Simon, "*The art of deception: Controlling the human element of security*" Wiley. com, 2001.

[2] Graves K., "*CEH certified ethical hacker study guide*" Wiley. com, 2010.

[3] Pavkovic N. Perkow L. , "Social Engineering Toolkit—A systematic approach to social engineering ." *MIPRO, 2011 Proceedings of the 34th International Convention*. IEEE, 2011.

[4] Bezuidedenhout M., Mouton F., "Social engineering attack detection model:SEADM.", *Information Security for South Africa (ISSA), 2010*. IEEE, 2010.

[5] Wenyin L., Fang N. "Discovering phishing target based on semantic link network.", *Future Generation Computer Systems*, vol.26, no.3, pp. 381-388, 2010.

[6] Hasan M. ," An attack vector for deception through persuasion used by hackers and crackers", Networks and Communications, 2009. NETCOM'09. First International *Conference on*. IEEE, 2009.

[7] Gross R., Acquisiti A., "Information revelation and privacy in online social network (the facebook case)", *Pre-proceeding version, ACM workshop on privacy in Electronic society (WPES)*, 2005.

[8] Arthurs, Wendy. "A proactive defense to social engineering", *SANS Reading Room,August* 2, 2001.

[9] Shimonski R., "Client Side attacks and defense", ELSEVIER, 2012.

[10] "Cyber Attacks Timeline Master Index", data available at http://hackmageddon.com/cyber-attacks-timeline-master-indexes/.

[11] "1-15 december 2013 cyber attacks timeline", data available at http://hacmageddon.com/category/security/cyber-attacks-timeline/.

[12] http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history.

[13] "History of cyber attacks-a timeline", data available at http://www.natint/docu/review/2013/Cyber/timeline/EN/index.htm.

[14] "Detection of phished page" figure available at http://www.phisnophish.com.

[15] "Social engineering" figure available at http://www.techrepublic.com/article change-your-companys-culture-to-combat-social-engineering-attacks/1047991.

[16] "In factious media genetrator", data available at http://www.socialengineerorg/framework/Computer_Based_Social_EngineeringTools:_Social_Engineer_Toolkit_(SET).

[17] "Phishing Threats and Countermeasure", finjan vital security, January 2007.

[18] Exploiting Cross-site Scripting Vulnerability on Facebook [Online]. Available: www.eweek.com/cloud/Facebook-Pursuing-Attackers-who-Exploited-XSS-Flaw-in-Massive-Spam-Attack/.

[19] Cross-site Scripting Worm Hits MySpace [Online]. Available: http://betanews.com/2005/10/13/cross-site-scripting-worm-hits-myspace/.

[20] Email attack exploits vulnerability in Yahoo site to hijack accounts [Online]. Available: http://www.pcworld.com/article/2026798/email-attack-exploits-vulnerability-in-yahoo-site-to-hijack-accounts.html.

[21] Cross-site Scripting Attack on Twitter [Online]. Available: http://www.pcmag.com/article2/0,2817,2369438,00.asp.

[22] Microsoft-patched HTML Sanitization Flaw Linked to Hotmail XSS Vulnerability [Online].Available: http://www.securityweek.com/recently-patched-html-sanitization-flaw-linked-hotmail-xss-vulnerability.

[24] Cross-site Scripting Vulnerability in TrueCaller[Online].Available: http://packetstormsecurity.com/files/108428/Truecaller.com-Cross-Site-Scripting.html.

[25] Skype: XSS Vulnerability is on the way [Online].Available:http://www.theregister.co.uk/2011/07/19/skype_xss_flaw_fix/.

