“The Effectiveness of Social Engineering using the Phishing method from an attackers view point”

Research to show how effective the phishing method type of social engineering has on capturing log in credentials of a victim.

Nsunga Innocent
School of Engineering
Department of Computer Forensics. ICU
Lusaka, Zambia
innocentnsunga@gmail.com

Dr. Silumbe Richard
School of Engineering
Department of Computer Forensics. ICU
Lusaka, Zambia
rsilumbe@gmail.com

***Abstract*— this paper explores more on the devastating method that crackers use to gain access to the information that is deemed private. The paper will address social engineering; in particular the social engineering committed through the phishing method with the use of a fake login page of any renowned website such as PayPal, Gmail, yahoo, Hotmail, twitter and the famous Facebook. The paper will afterwards propose some measures that can be put in place to reduce on the cases of computer social engineering using this type of attack. Regardless of the different motives that attackers carry in their minds, it is clear that these attackers are motivated differently, some attackers do this for fun, some for educational purposes and a large portion of them for financial gain especially those that attack websites that deal in financial transactions like PayPal. Unlike the other types of hacking methods that involves cracking passwords using different methods like the dictionary, hybrid and the brute force attacks that may take more time to accomplish; social engineering using the phishing method has proved to be very effective and efficient from an attacker’s view point as an attacker can get the information of their interest in a short time.**

Keywords: Social engineering, information systems, hacking, reconnaissance, phishing.

I. INTRODUCTION

Social Engineering has been in existence almost as far back as information technology has been enhanced, it keeps evolving with the technology, as systems become more and more complicated; the human beings also sharpen their social engineering techniques in order to gain the information of their interests in an enhanced way. Social Engineering may be carried out either by human beings or with the aid of a computer, regardless of any of the two afore-mentioned ways, social engineering’s purpose is known; it is sorely used for information gathering in a disguised way. With the human social engineering, an attacker works on the psychology of the victim resulting in the victim revealing the information that was not supposed to be given out. In today’s world of technology, social engineering is mainly carried out with the help of computers. The use of computers in carrying out social engineering involves the use of a computer as a perpetrating tool in carrying out an attack; the attackers’ computer is positioned in such a way that it is disguised to be the receiving computer of whatever information an attacker is interested in getting from the victim, this results in the loss of login information by the victim. The information sort after by an attacker is so sensitive that it can result in a big loss, this information may include among others, usernames, passwords to systems as well as PINs to the victims’ banking systems that they would never reveal intentionally.

Social Engineering can be defined as an art of manipulating someone in a disguised way for the purpose of obtaining information under pretense used to gain access to an unauthorized information resources. This act is mainly carried out through the use of computers, where a computer has been used as a perpetrating tool, at times human beings disguises themselves to be legitimate recipient of the desired information by working on the psychology of the victim. In order for this human hacking to pull through, an attacker must have observed the victim they would target, so by knowing little about the organization, an attacker would target an authorized employee of that organization into revealing sensitive information. An attacker can use a reconnaissance to get this information which they will use at the time they take an active attack of social engineering. After getting the information through reconnaissance, an attacker can physically visit the organization and disguise themselves to be a legitimate employee of that organization and ask for sensitive login credentials. At other times, an attacker can use other means like emailing or simply a phone call and pretends to be the manager asking for the login information from junior employees. Computers in this age are considered to be an effective way of social engineering; whenever a computer has been used to carry out social engineering, the computer is placed or positioned in as such a way that it is disguised to be the recipient of the incoming sensitive information from the victim’s computer, this positioning enables the attacker’s computer to receive information intended to go to the legitimate intended destination.

Information System as used in this paper refers to the interrelated components of the information communication technology that works with others in order to accomplish the designated task. Just like the human body has different systems that work together for the good being of the human, it has multiple organs that work in similar manner, systems like the vascular system, the circulatory system, the digestion system and the others, a computer system works in the exact way in processing information. A good illustration of an information system is the web page made in a PHP (hypertext processor) language interacting with the MySQL (query language) database in handling student requests like students registration, student banking transactions, result upload done by the administrator and viewing by the students; in this case the database is a component of management information system, equally the PHP web page being used as an interface in retrieving and submitting the requests can be referred to as an information system both working to accomplish the tasks of processing students requests.

Hacking is another terminology that is at many times misapplied; however, the term is nothing but an act of intruding into resources that are protected; it can be done either legally or illegally using their skills with the help of computers. That is to say hacking is a general term that can be used to refer to personnel that are able to access protected resources either legal or illegal. In this world of technology, many people with hacking abilities use their skills to attack others, and these people are referred to as perpetrators or crackers, on the other hand there are those with the same skills but use their skills to protect others from being victimized' and these personnel are known as the ethical hackers. Ethical hackers also help in legal courts in solving cybercrimes by using their hacking skills to prove the guilt crackers in courts.

Reconnaissance is part of social engineering; this reconnaissance is a pre-phase passive attack that an attacker carries out prior to the actual attack. It is said to be a pre-phase passive attack because it involves an attacker gathering information about the target organization or a person by passively observing the target and coming close to it in order to establish relationship with those so close to the target in order to improve the chances of attack. Among the information an attacker would gather at the reconnaissance phase may include and not limited to list of employees, the hierarchical structure of an organization, contact information and others in a case where an attacker has made an organization his target. In the case where an attacker wants to gather information on an individual victim, an attacker would establish a relationship with the target individuals themselves or use the people that are so close to the target in gathering information about them. Among the interesting information an attacker would get are things like email addresses, phone numbers and other things that the target person likes; because attackers are aware of the value that this information has more especially in emails where they ask the legitimate users to answer some questions as they are about to reset their email passwords in an event where a user forgets or just want to change for security reasons. All this information is gathered during the reconnaissance stage prior to the actual social engineering under human hacking. In the case where the computer has been used as a tool to carry out reconnaissance, there are special tools that are used across different platforms of computers that can carry out reconnaissance; tools like Nmap, Zen map and other can be used to gather information about the target organization; the information gathered by the computer among others include the operating system that is running on the target computer and the open ports that attackers can exploit later as they come to do the actual social engineering.

II. Phishing Using the Fake Login Credentials

Phishing using fake login page is one method of computer social engineering beside other methods like baiting and link manipulation. Phishing is a method that involves the presenting of a disguised component of an information system by an attacker as they wait for the victim to present their sensitive login information. This type of Phishing is effectively carried out by hackers who are well vested in programing languages like PHP and HTML. In this way an attacker may create an exact fake replicate of the login page but this login page redirects the user to something else instead of being where they intended to go, at times an attacker may just capture the login credentials of a victim hoping to login to their mails and lets the user connect back to the legitimate site so that they do not suspect anything illegal, in this manner the victim's credentials are captured in a short space of time. This method from an attackers' view point is very effective in that an attacker does not wait for long, as no cracking process of any sort is required. For this method to therefore work, at times an attacker has to carry out the two ways of social engineering, firstly the perpetrator carries out a human hacking, where they use their technique of tricking the victim into using certain channels to login their credentials, among the avenues used is an IP (Internet Protocol) address. This IP address is mainly the address of an attacker which directs the victim to a fake login page of the desired site, as such the victim's sensitive information such as those of Facebook, Twitter, Email or even financial websites like PayPal account's usernames and passwords remains with the attacker. These sites are then presented to the victim in a disguised way that is accomplished through the cloning of the site so that the victim cannot distinguish the difference between the legitimate and the fake website. Now this method cannot be accomplished without some form of human social engineering, therefore an attacker now uses his human social engineering techniques to make the victim login to the site of their choice using the attackers IP address either by sending the email having the attacker's IP address or by cell phone. At times an attacker will find a reason to give to get the victim to use their IP address to login to the site they want to get the information. As soon as an attacker gets the victim to login to the site using their IP address, let's say PayPal, the username

and the password of the victim is served on the computer of the attackers without the knowledge of the victim. With this information, an attacker can use the website as an authenticated user and they can even transfer the money because the server considers them to be legitimate users of the account. At this point the attacker will have full control to the victims account, they can even alter the password of the account thereby denying access to the legitimated user.

III. Methodologies of attack

For this type of social engineering to take place, let's take the side of an attacker and the ground work they do on their part so that they create this fake login page. Initially we said for this attack to succeed, an attacker has to be vested with programing languages like HTML, PHP as well as MySQL to create a database.

Firstly an attacker would choose which target website they would like to gain access to, we take PayPal for instance as our target we would like to get information about. It is worth noting that we would use this method to get login credentials of any website of our choice.

Secondly, the attacker would move on to the legitimate PayPal login web page and right click on the web page, they now go to view page source; this will give an attacker the source code of the page.

Thirdly, an attacker will copy the source code and save it in note pad with something like PayPal.html. They will next look for the form method to use; this form method is responsible for the defining of how information is supposed to be sent to the server. There are two ways to send the login credentials to the server; it is either the GET or the POST methods.

The POST method is the most secure and hence preferred when handling very sensitive information like credit cards and other personal information. This method is secured because the browser sends separate server request containing special server header then followed by the data intended to be sent afterwards.

It is most likely that after viewing the source code of the login information, an attacker will discover that the web page is using the POST method and hence attackers will change this method to the less secured type of GET. With this method, it is said less secured because the data is tacked right to the uniform resource locator (URL) being sent to the server.

The next phase is for the attacker to create a script in which the entered login credentials will be saved together with the redirected URL that the user will be redirected to after entering their username and the password, let's say this URL is www.google.com so that the victim does not have suspicions.

Finally the attacker will upload the two files, that of the legitimate PayPal website whose method had been changed and the PHP script for saving the captured credentials. The attacker will now send this fake login web page to the victim by mail or even via a phone message and once the victim logs in, their login credentials are sent to the attacker.

Another method similar to this fake login web page is that which is carried out with the aid of the computer using special social engineering tools more especially under the Linux distribution. This method involves the use of tools (SET tools). Under this method, an attacker does not need to create a fake login web page but using this tool has advantages in that an attacker can clone any login web page ranging from that of Facebook, twitter, Gmail, yahoo, Hotmail, PayPal and many more. The methodology of attack is similar to the first one but only differs on the aspect of creating and hosting the web page as well as on the avenues to present to the victim in luring them to login to their desired sites.

Firstly an attacker identifies the target website of their choice and goes to the attacker's Linux machine, opens the terminal and types; start apache server, then pressing enter o the keyboard.

Next an attacker specifies the attack they are to carry by typing setool kit; this gives an attacker multiple options from which to choose the mode of attack, among the options provided is that of social engineering, so an attacker chooses this option.

Now after choosing social engineering an attacker chooses web attack among other social engineering attacks. Afterwards credential harvester is chosen and website cloner as the final option of social engineering.

An attacker now opens another terminal and types "ifconfig" command in order to know the IP address on which their attacking computer is sited on the network.

After knowing their IP address they are using in accessing the network, an attacker then moves on entering the URL of the target website, in this case http://www.PayPal.com. At this point an attacker is set and ready to move on victimizing the person of their choice with the PayPal account.

But before an attacker presents this login page to the victim, they first enter the directory in which all the information about the victim will be saved. This directory is as follows in the case of a Linux machine running the 2.0 kali Linux Sana; Computer > Var > www. An html folder will be created together with the html login file that has to be presented to the victim; so the html file has to be put inside the html folder manually.

Finally the attacker will now move on to lure the victim into login using their IP address. An attacker at this point will find a reason to lure a victim to use the IP address instead of the victim going to the browser and typing www. PayPal.com, the attacker will tell them to use their IP address that might be something like 192.168.1.21 depending on the attackers IP address and once the victim logs in using this address, their usernames and password remains with an attacker and later on being directed to the legitimate website so that nothing is suspected by the victim without their knowledge.

To lure a victim in the trap more especially those with little or no much knowledge about the cyber threats we face in the world of information technology, the victim will login using the attackers IP address. Among the reasons, an attacker will use to lure victims may include time consumption to start typing the whole URL of the website instead of using the

direct simple IP address and this might seem appealing to the victim not knowing that they are being led into a very serious problem that might lead them into bankruptcy as an attacker can do anything in the victim's account once they get these login credentials.

IV. Conclusion

Social engineering has its root from far back decades when it was mostly carried out by humans themselves but it keeps getting enhanced more especially on the computer based; as technology advances, social engineering takes a new form too. There are a lot of literature that talks about the devastating effect of social engineering and therefore the vice cannot be over emphasized as its effect is widely known. It was stated that social engineering from an attacker's view point is effective because all the attacker needs to do is to make sure that the human social engineering part is successful and once successful this pull through, then the attacker has access to the information they seek. The paper's focus is on the social engineering that is computer based using the phishing method, the reason for the choice of this type of social engineering is to raise awareness of the threats that we face in the cyber space. A lot of people are quite aware about social engineering from the human aspect but the phishing method with the help of cloned fake login web page that an attacker gets the victim to login using their IP address has not been explored to the maximum in raising awareness to the public. The major points of this discussion is that as technology advances, social engineering like any other form of hacking also increases in sophistication, this is point for user now to know that social engineering has taken a widespread form, more than the general public knows about this act. Unlike the previous decades when it was in its infancy, social engineering is now not limited humans tricking others but that others methods like the ones discussed in this paper are being employed in getting sensitive information from users.

III. Recommendation

Social engineering can a devastating way of getting information and therefore appropriate measures are supposed to be put in place to reduce on the cases of the vice.
It is very difficult to pin point on the defenses that we can put across in order to safeguard ourselves from social engineering because no matter how much security we can put across, social engineers are sophisticated people that are not restricted to one type of method in getting information they want. Among the recommendations that can help reducing the likelihood of this attacker are the following and not restricted to:
(a) Using common sense among the workers in organizations by avoiding giving information to any user that is not an employees of an organization. From an individual's perspective, it is important to reduce on giving out contact detail such as phone numbers, email addresses and other personal information.
(b) From the fake login perspective of social engineering, it is important for users to avoid using IP addresses to login to any website as this is an avenue that hackers use to get users' login credentials. It is therefore recommended that users should go to the website's URL by typing it in the web browser and not any other methods in whatever circumstances.
(c)Users are also recommended to frequently change their login credentials from time to time, more especially to the sites that deal in financial transactions such as PayPal.

V. References

Allen, M. "Social engineering: A means to violet a computer system", 2006.

Guenther, M. "Social engineering: Security awareness series", 2001.

Robbins, J.N. "Learning Web design: A beginner' guide to (X)HTML, style sheets and Web graphics", 2007.

Rafay .B. "A beginner's guide to ethical hacking", 2010
URL: www.rafayhackingarticles.blogspot.com.

Shetty, D. Social engineering.