ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 1, pp: (22-35), Month: January - March 2019, Available at: www.researchpublish.com

Human firewall enterprise security framework to mitigate social engineering attacks within organizations in Botswana

June Jeremiah

PHD in Information Systems, Limkokwing University of Creative Technology

Abstract: **Social engineering attacks are by far the tremendously hard forms of cybersecurity and data privacy attacks since they focus on manipulating humans to become the weakest link in security. As per security data breach reports the existing security techniques are more focused into technology forgetting humans as the weak link in the security chain. As evidenced by the fact that penetration testing reports in today cyberspace keep proving hackers are gaining access to company networks mostly through social engineering attacks. In this research paper, we are going to assess various forms of social engineering attack concepts and their impact on organizations. The research will further identify attack stages and propose enterprise security framework to mitigate socially engineered attacks through building human firewall within organizations in Botswana. The proposed outcome of this research is the enterprise security framework to establish secure cyberspace through the creation of a human firewall within organizations and secure their digital assets from social engineering attacks in the wild in Botswana. The framework will provide security guidelines and cloud training platform to assist employees to be more aware while online. Furthermore, the framework will help organizations to build more secure human firewall through security assessment survey generated to provide graphical presentation report that can be used by security auditors to mitigate social engineering attacks in Botswana through effective security training and awareness while online. Thus the creation of a human firewall to fight against social engineering attacks can only be achieved through awareness and making use of technology to simulate real-life phishing camping within the workforce to filter weak link within employees in the security chain.**

Keywords: **Social Engineering, Human Firewall, Vulnerability, Exploitation, Cyber security, Hacker, Victim.**

1. INTRODUCTION

Over the last decades, the modern digitalized world has revolutionized how businesses operate today and the way we live our lives. Business communications and data sharing now fully depends on connected devices in the internet of things whereby business and customers can perform a various task such as shopping, paying bills and even perform bank transactions just by few clicks on the world wide web. However, with the ease of internet connected world comes along cyber threats and vulnerabilities which have been exploited and affected so many businesses globally. A survey by Price Waterhouse Cooper (PWC), reported that 93% financial intuitions fall prey for security data breaches in 2016, with this figure indicating the exponential growth in cyber-attacks in the wild. Today cyber-attacks towards nations, businesses and individuals have become so sophisticated that society is now at the edge to implement a strategic response plan to the sheer volume and acceleration of these cyber threats through the creation of human firewall.

According to a study by the Bank of America Merrill Lynch Global Research, cybercrime it is growing at rapid pace costing the global economy up to approximately 540 billion dollars annually. Furthermore, as the digital world continues to grow due to the inevitable rapid technology innovations securing our devices and data while online has become impressively impossible. The rise of cybersecurity attacks incidents continue to grow exponentially, both in frequency and damage, unfortunately, users and organizations have not yet adequately deployed strategic defense plan to combat human error security attacks. The latest cybersecurity attacks are more social engineered than technical making them more efficient in the fact that they exploit the human flaws which have supported some of the major cyber-attacks in today cyberspace. Socially engineered attacks use the art of exploiting human errors to gain access to secure and protected data to achieve cybercriminals' malicious objective.

2. BACKGROUND

2.1 Botswana Cyber Security

Botswana is one of the developing countries in Africa with new technology such as the internet with internet users are now at the benefiting from the wide range of services and products offer them. With this new amazing services that come along with the internet it is also a good practice to always remember the threats of malicious activities in the digital world. Based on previous research conducted by the United Nations on cybersecurity issues within African countries. It is in this research it was found that Botswana is striving to ensure secure cyberspace through legal measures such as the introduction of the Cybercrime and Computer-Related Crimes Act, Electronic (Evidence) Records ACT 2014, Electronic Commerce and Signatures Bill and Law on data protection which is still under review. However, all these legal measures and regulations are only implemented to govern cybersecurity agencies and law enforcement to adhere and follow certain protocols in regard to cybersecurity issues within the country**.**Therefore leaving the users still at high risk of attacks within an organization as there no proper means of awareness and training provided to users to create a strong secure human firewall. According to a review paper by ITU in the year 2012, it was stated that Botswana lacks national governing body that will train and develop cybersecurity frameworks to be used by both private and public sector to mitigate cybersecurity challenges. Botswana is already exposed to cyber-attacks taking a look at the hacking incident of University of Botswana website as reported by Sunday Standard 20th February 201. The hacking attack occurred during the week the university was under devastating turmoil strike from the students leading to the destruction of campus properties. It is not a shock to find that the attack that defaced the university website by changing logo content to the image of the anonymous mask. Hackers have different objectives they aim to achieve through cyber-attacks the hack of the University of Botswana website is in form of hacktivism attacks which normally launched by anonymous in demand of justice, political stability, economic growth or even anti-terrorism attacks.

Despite the fact that Botswana has not yet encountered major cybercrime data breach it is not an assurance that organizations in Botswana are secure. In today globalized world of new technology and connected devices security is now just illusion. The worry is no longer be how secure how secure are we but the main question is when are we going to be compromised therefore the creation of human firewall wall within the organization in Botswana can by far assist to reduce and avoid the occurrence of social engineered attacks incidents. The human firewall can be achieved only through awareness, policies, monitoring, train, and development with assessments to identify the weak links within organizations.

2.2 Why Botswana is a potential target to cyber attacks

- Botswana as a developing country internet technology is still at its infant stage and many users still lack awareness on security measure to take while online.
- Lack of computer literacy, technology is something complex and challenging to use Botswana as a developing country have many commiserate therefore making it even easier for attackers to target them.
- Poor rules, regulation and policies to govern individuals and organizations on cybersecurity matters.
- Economy, Botswana by far is one of the peaceful stable countries with promising economy as one of the attacker's objective is personal financial gain, therefore, leaving Botswana citizen exposed to high risk of financial loss targeting government and organizations.
- Lack of educating and training users on cybersecurity issues.

2.3 Social Engineering Attacks Taxonomy

According to Hadnagy (2001), the term social engineering is defined as the art of human exploitation to manipulate users to take actions that may help cyber criminals achieve their objective to compromise and gain access to valuable secure data. In contrast to this SANS Institute define social engineering as "a non-technical or low technology attacks that focus on tactic such as lies, impersonation, tricks, bribes, blackmail, and threats used to attack information systems". Therefore with these definitions above we can have insight into how socially engineered attacks fully depends on the human factor.

Today attackers are now finding it easy to use the benefit of human behavior as a tool to gain access to secured data by manipulating unaware user to perform various multifaceted social engineering attacks. Bisson (2015) further argue that social engineering is a low tech attacks that only depends on its success by manipulating victims to devour confidential secured data by its attempt to exploit human factor vulnerabilities.

Social engineering a tactic deploy technique used by attackers to exploit flaws in human logic known as cognitive biased has to lead various organizations into data breaches due to users fall prey to click and download malicious emails within the corporate network. In today digitalized and innovative world many organizations are investing heavily on security technology measures with the aim to improve security, however human factor vulnerability still continue to represent the weak link in the information security chain.

2.4 Steps involved in Social Engineering Attack

Social engineering attacks are identified as common social-technical attacks because they rely on the usage of technology to manipulate humans to gain access to secure protected data. Lou (2011) identifies various human and technical means such as phishing to dumpster diving as techniques used by attackers to gain access to secured data. For successful attacks to occur a synergy of both human and technology need to be deployed to assist attackers to trick victims to obtain an ambiguous amount of sensitive information that causes huge damage to individual and organizations. Luo (2011) identify the steps used by attackers in the social engineering attack process to ensure a high success rate to manipulate users to perform tasks assisting them to achieve the malicious objective. The below figure shows the various steps in the social engineering attack.

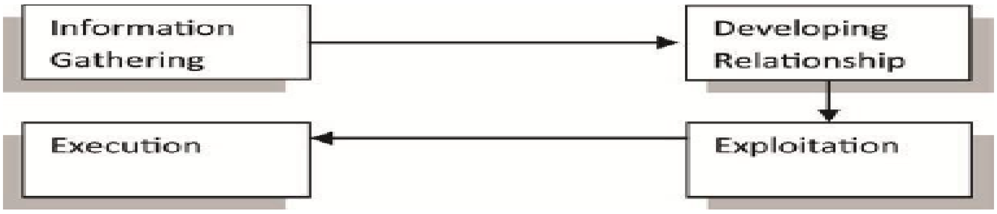


Figure 1: The stages in Social Engineered Attack

The above figure (Fig 1) graphically give insight into the steps attackers use to perform successfully social engineered attacks. The attack process begins with information gathering phase which assists the attacker to establish a fake legitimate relationship with the victim. Once the relationship is established exploitation phase take place resulting in relinquishes of sensitive information and the final stage the attack is implemented to achieve attacker objective. Social engineered attacks can be considered as social-technical attacks that focus more on human or technology deployment. The

human factor vulnerability stems out from an attacker who already has enough information about the target deploys a strategy of a known trusted party to trick victims to perform the task to exploit their networks; therefore contributing to complete the hackers puzzle to gain access to secured data.Social-technical attacks are by far sophisticated forms of attacks deployed through wide range of options such as email attachment, pop-up windows and websites to harvest user sensitive information by prompting victims to input user and password information in bogus malicious form pages in fake website and the malicious script embedded within windows pop-up notification manipulating victims run and install malicious backdoor software’s which give full access to hackers.

Social engineering a tactic deploy technique used by attackers to exploit flaws in human logic known as cognitive biased has to lead various organizations into data breaches due to users fall prey to click and download malicious emails within the corporate network. In today digitalized and innovative world many organizations are investing heavily on security technology measures with the aim to improve security, however human factor vulnerability still continue to represent the weak link in the information security chain.

2.5 Common Social Engineering Attacks in Today Cyberspace

Social engineering attacks encompass a wide range of malicious activities and in this research, we identify the five common types of attacks in the cyberspace today.

2.5.1 Vishing: is the form of socially engineered that the attacker makes use of phone call to trick a victim to reveal sensitive information such as SSN number, pin code, full names, and home address. Most of this attack manipulate users using IP (VOIP) technology to spoof caller id and remain anonymous.

2.5.2 Baiting/Trojan Horse: in this form of attack, attackers use digital devices such as USB, SD Cards, to gain victim attention to enable them to run malicious codes to penetrate cooperate networks. This attack fully relies on human curiosity to spread malware installed on their devices. As result the entire cooperate will be compromised by hacker having full control to the organization internal network.

2.5.3 Fraudulent Websites: With this social engineering attack the attacker exploits the human trust by leading them to access fake legitimates looking website which will automatically trigger a download of malicious code into the victim device. The executed file in this attack will give attackers full access to the device and enable them to harvest sensitive information within the victim device.

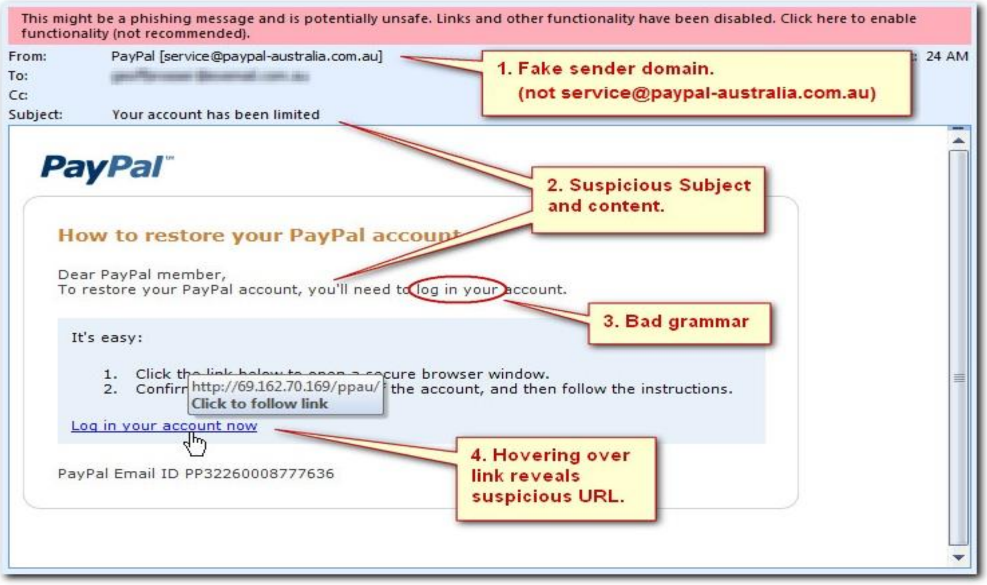
2.5.4 Pretexting: This is a human exploit that use legitimates scripted scenarios to allure the victim to reveal sensitive information or achieve other objectives of running malicious files unknowingly. The reverse social engineering is by so far the major example for pretexting, in which attackers impersonate scenario to be technical support by sending a malicious file through email advising victim to perform security upgrade on a new application and an innocent victim will believe that the security upgrade is needed trusting the new security update will solve the problem.

2.5.5 Phishing/Spear Phishing: Phishing the most tedious social engineering attack in the wild targeting users and organizations with the aid of using legitimate organization logos and trademarks to grab the attention of their target. The malicious email appears to be sent from a trusted sender such as bank requesting the customer to update account information details through bogus attachment or link. The malicious site leads to the installation of malicious code in the victim computer giving attackers access to secure sensitive information such as financial credentials.

Phishing is by far considered the most complex attack and technique as it involves manipulation of human flaws for the benefit of attackers. Spear-phishing, this is unique and consider impossible to stop as it is executed based on information gathered from the victim. Social media sites are widely used to harvest information that would be used to create customized fake email appearing to be from a legitimate friend, business partner or organization. This attack uses the information gathering process on potential target and creates a fake legitimate email with a high probability of success.

2.6 Example of Social Engineering Attack

Phishing attempts by far are the most dangerous forms of attack. In the below shown (Fig.1) it is an example of a phishing attack which is using social engineering attack impersonated to be a trusted party in this case PayPal. The attackers' objective is to harvest PayPal login credentials by tricking users to restore their account using a bogus link that will direct users to attacker a fake PayPal website.To avoid this form of attack users need to be alert at all time for a bogus link by verifying the sender email address, check for spelling errors, suspicious link or attachment and hovering over email links within email content can assist to expose the fake site. In the next section of the paper is an example of execution of a phishing attack.



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au]
To: [redacted]
Cc:
Subject: Your account has been limited

24 AM

PayPal

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirr the account, and then follow the instructions.

http://69.162.70.169/ppau/
Click to follow link

Log in your account now

PayPal Email ID PP32260008777636

1. Fake sender domain.
(not service@paypal-australia.com.au)

2. Suspicious Subject and content.

3. Bad grammar

4. Hovering over link reveals suspicious URL.

Figure 2: Phishing attack attempt explained

In this section, we will use social-technical attack using Social Engineer Toolkit that comes pre-installed with pen testing tool Kali Linux figure 2. Kali is a Debian Linux operating system widely adopted by penetration testers for testing purpose using a wide range of tools designed to analyses and identify system vulnerabilities. The offensive security fund and maintain Kali Linux as a renowned open sour project used by cybersecurity experts to tackle challenging cybersecurity challenges in today digitalized world.

The Social-Engineer Toolkit (SET) is widely adopted by cybersecurity experts to combat social engineering attacks. SET is now considered as the standard framework to assist cybersecurity experts to solve exponential rising of social engineered attacks.

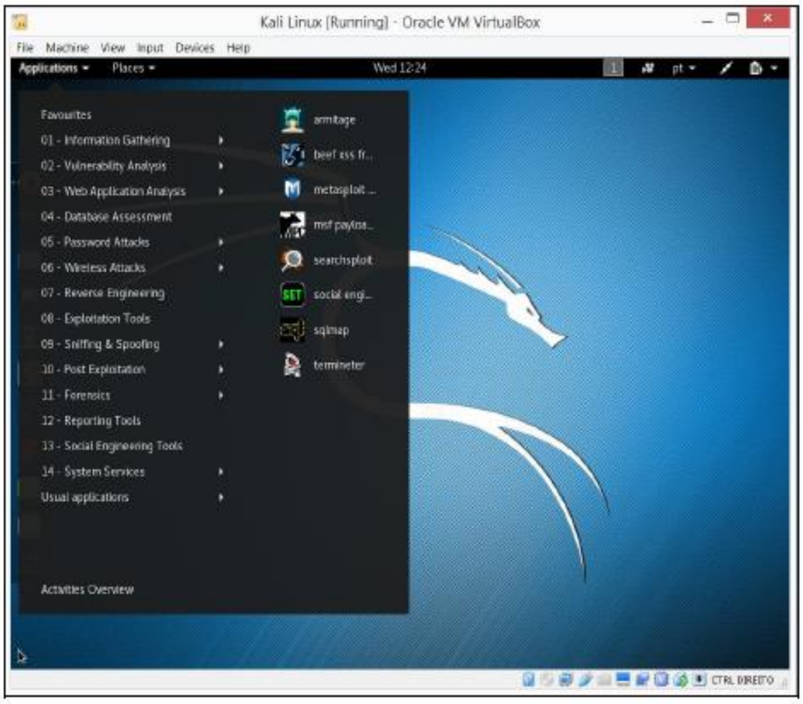
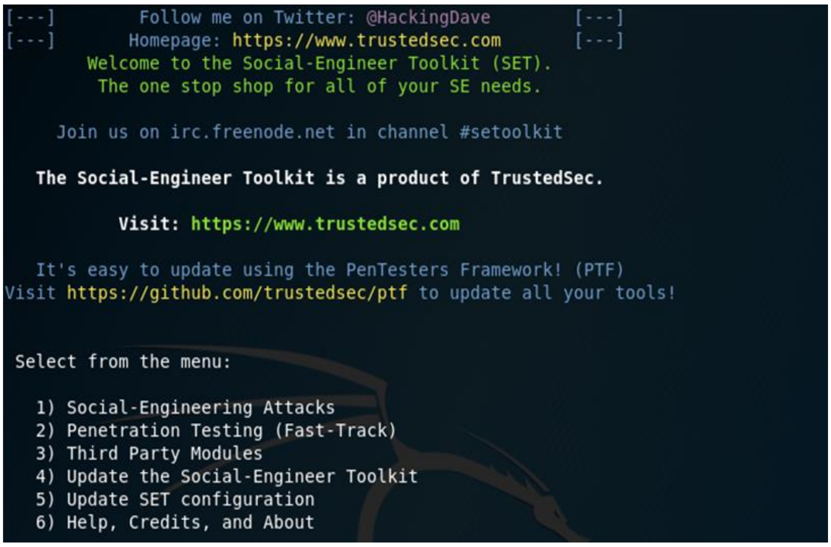


Figure 3: A few exploitation tools including the Social-Engineer Toolkit

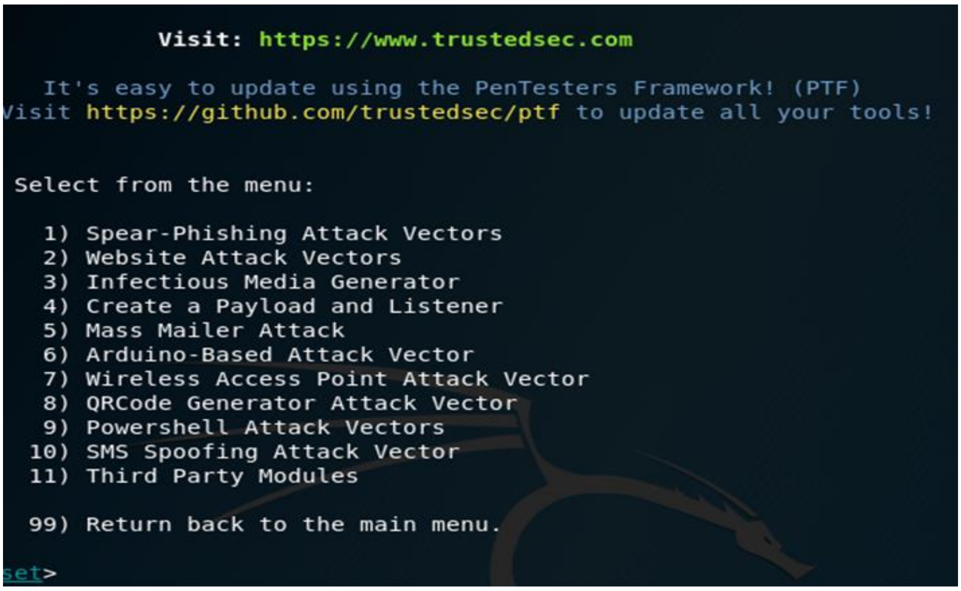
To demonstrate how attackers execute these forms of attacks using kali terminal simple type command “setoolkit”. This can also can be achieved by using the application menu as above figure. Once this command executes it will present a simple main menu to select the type of attack need to be launched as shown in following (Fig 3). Since this research paper is on social engineering we, therefore, select option one in (Fig 3) which is the kind of attacks we studying.



```
[---]         Follow me on Twitter: @HackingDave        [---]
[---]        Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About
```

Figure 4: Social Engineering Toolkit Menu

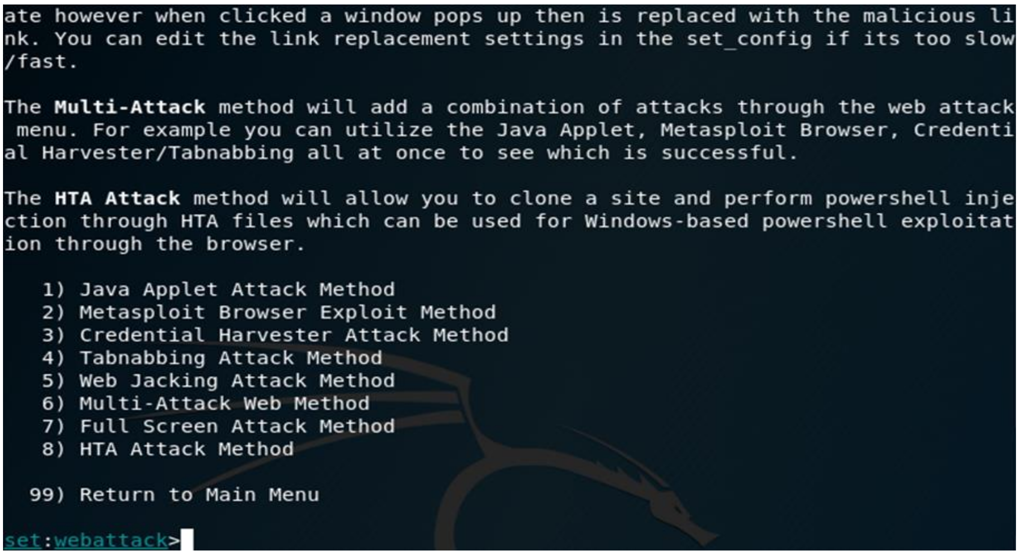
By selecting the social engineering option in the above figure a new menu will present a set of attacking vectors that attacker can launch to exploit users to gain access to sensitive data. In this example, we will use a website attack vector (Fig 5) which is web-based phishing attempts. Website vector attack facilitates multiple web-based attacks in order to exploit targeted victims, it is by far the common widely used attack vector due to its efficiency to harvest sensitive data at ease.



```
          Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set>
```

Figure 5: Social Engineering Attacks Menu

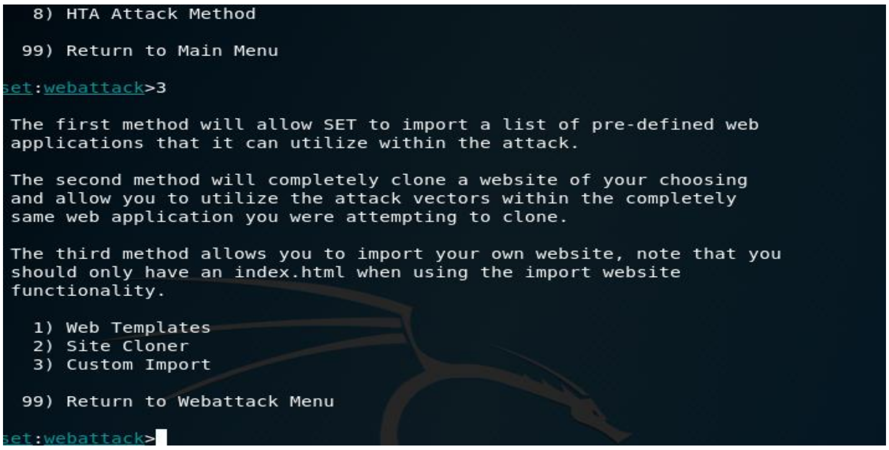
The attackers' objective is to harvest sensitive data such as passwords from the victim and to achieve this in Kali Linux we continue using the following menu by selecting the menu "Credential Harvester Attack Method" shown in (Fig 5) this method enables the attacker to harvest passwords from fake websites by manipulating users with using fake legitimate emails from trusted parties such as Banks, Friends or even PayPal phishing attempt example in (Fig 2) above.



```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

Figure 6: Figure 4: Website Attack Vectors Menu

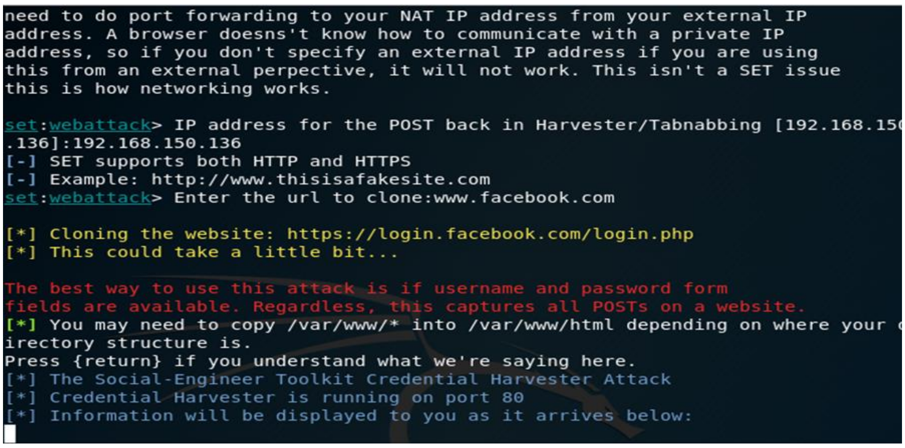
In a social engineering attack, the desired result by the attacker is to take advantage of the human factor vulnerability. Therefore by using fake legitimate trusted party websites to trick the user to reveal their credential is the main objective to be achieved by the attacker. To achieve this attacker's use site cloner attack vector method as shown in (Fig 7). This attack vector clone any website as desired, therefore attackers take advantage of this attack vector to direct users into a fake website which completely appear legitimate and trick users reveal their sensitive data.



```
  8) HTA Attack Method

 99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>
```

Figure 7: Figure 4: Website Attack Vectors Menu

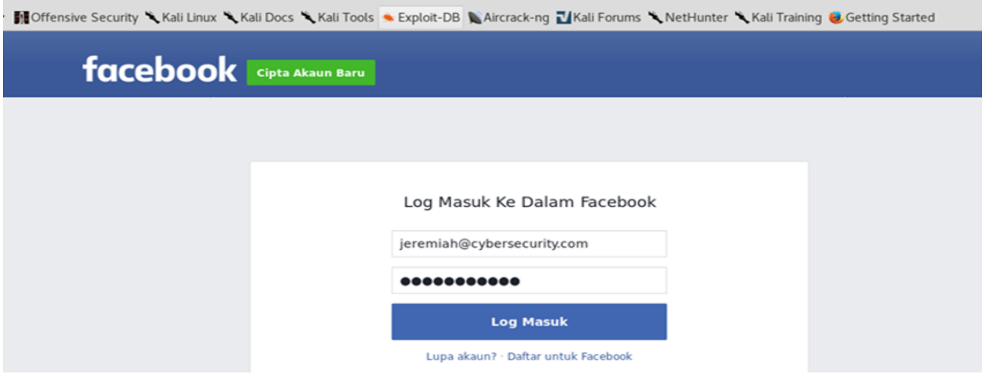
For phishing attack to be successful users are tricked to use fake websites to fill in sensitive data as personal information, pin codes, password, and usernames. To successfully harvest this information attacker need to receive generated report of login attempts. In Kali to achieve this, we need to configure our web server IP address to enable access of the fake cloned site and also receive harvested data. In the following (Fig 8) we use configure Kali Linux to set our local host IP address as our web server host and also insert the URL of the website attacker desire to clone in this example of phishing attack Facebook was used.



```
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.15
.136]:192.168.150.136
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your 
irectory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Figure 8: Site Cloner Vector Attack Configuration Menu

Once the attacker successfully clones the website the next stage is to deploy mean of transferring the bogus website to targeted users, usually email is the most widely used communication platform used by hackers to facilitate these attacks. Through applications of various social engineered attacks, human factor vulnerability is used to exploit users to mistakenly submit the targeted credentials in this example is Facebook email address and password as shown in Fig (9) user submitting sensitive data to a bogus website.



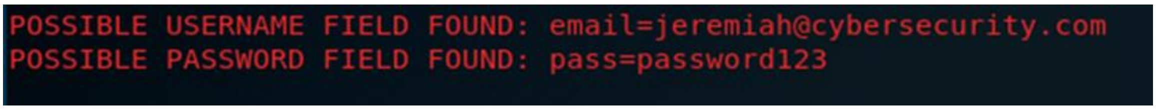
Log Masuk Ke Dalam Facebook

jeremiah@cybersecurity.com

●●●●●●●●●●●

Figure 9: Cloned bogus Facebook page

In the last stage of attack the malicious objective is achieved by harvesting Facebook credentials from the user by directing them to fake website which is cloned to perfection of not been noticed by victims and they reveal their sensitive data with the trust of the authenticity of the website. This form of attacks are by far most complex and challenging to deal with as controlling human nature has never been easy.



```
POSSIBLE USERNAME FIELD FOUND: email=jeremiah@cybersecurity.com
POSSIBLE PASSWORD FIELD FOUND: pass=password123
```

Figure 10: Harvested victim credentials on the terminal

With new technology evolving social engineering attacks will continue to take advantage of new technology to design new challenging phishing attempts. Furthermore, phishing is now used by attackers to bypass security perimeters to spread malware within organizations network such attacked is considered as an advanced persistent threat (APT). Malware attacks are persistent and hard to detect users can go for days even years without knowing they are compromised in such attacks organizations or individual typical sustain a severe financial loss in modern internet of things (IoT) world. Without proper security measures, phishing attempts will continue to escalate the rise of cyber and data breach incidents of which will always leave businesses in difficulty to survive in competitive digital markets. Therefore it is encouraged for organizations to be cyber aware and ensure secure human firewall in their daily business operations.

2.7 Impact of Social Engineering Attacks within Organizations

Every socially engineered attack is deployed with an objective to benefit the attacker, the goal can be multi-staged attacks such as harvesting administrative password to gain access to the entire cooperate network and compromise organization sensitive information. Therefore with this kind of attacks according to Thornburgh (2004) with each and every little information an attacker comprise it is crucial and significant to do enough damage from organization reputation to financial loss. The rapid growth and success of many social engineering attacks are ultimately after manipulating humans to perform legitimate transactions, download and install of malware to gain access to the entire network with all this leading to huge financial losses and exposure of sensitive data such as individual's personal information.

In a statement made by Home Depot Thursday, 18 September 2014, the company was hit by data breach attach compromising 56 million unique customer payment cards. The root cause of data breach was due to a customized unique malware installed in Home Depot PoS register which could be through social engineering attempts because the methods deployed by hackers to gain access was not disclosed by Home Depot. Due to the fact that Home Depot is a large nation trusted company, in today digital world of innovation different technologies such as anti-viruses, intrusion detection systems (IDS), firewalls and patch management systems are widely updated by organizations of their scale to mitigate more of technical attacks Twitchell (2006). As a result, the kind of malware attack used to compromise Home Depot PoS system is through employing social-technical attack targeting the human factor vulnerability and usage of new technology to make it unique. Manske (2000) further stated that social engineering attacks will continue to make severe damage to organization digital assets despite the invested amount in security architecture human error will still be the weakest link in cybersecurity.

Most cybersecurity study reports reveal that the exponential rise of social engineered attacks targeting individual and organizations should be considered as a national crisis because most attacks focus on the financial gain by the attacker which can cripple the economy. Any social engineering attack can affect any user even a bank employee leading to exposure of bank financial infrastructure to attackers. Insecurity breaches like this can result in significant damage to the nation's financial markets due to the interconnectedness they have with a nation's economy. In a survey report presented by Microsoft in 2008, prove that malicious phishing website related bank scams lead to financial loss amounting more than the US $5 billion. In another report, it was stated that Well Fargo Bank suffered a loss of US $ 2.1 million due to social engineered attacks with US bank credit card growing up to US$2.8 billion annually due to phishing attempts.

Social engineering attacks have a significant impact on the cost of reputation loss and goodwill which harm organization operation in the future. Taking the example of Home Depot data breach consumer can perceive company less secure resulting in bad reputation with their online business platform which can cripple business revenue cash flows. Therefore the impact of social engineering is by far most dangerous attacks, looking at the recent cyber-attack incident on Bangladesh's central bank that hackers transferred $80 Million from the institutes' Federal Reserve bank after social engineering attack was using to compromise employees system through a malware sent to employees email. The impact of such attacks are considered as a national crisis as the central bank losing such a huge amount of taxpayers can destroy the economy of the country in today global completive markets.

2.8 Addressing Social Engineering Attacks in Botswana through Human Firewall

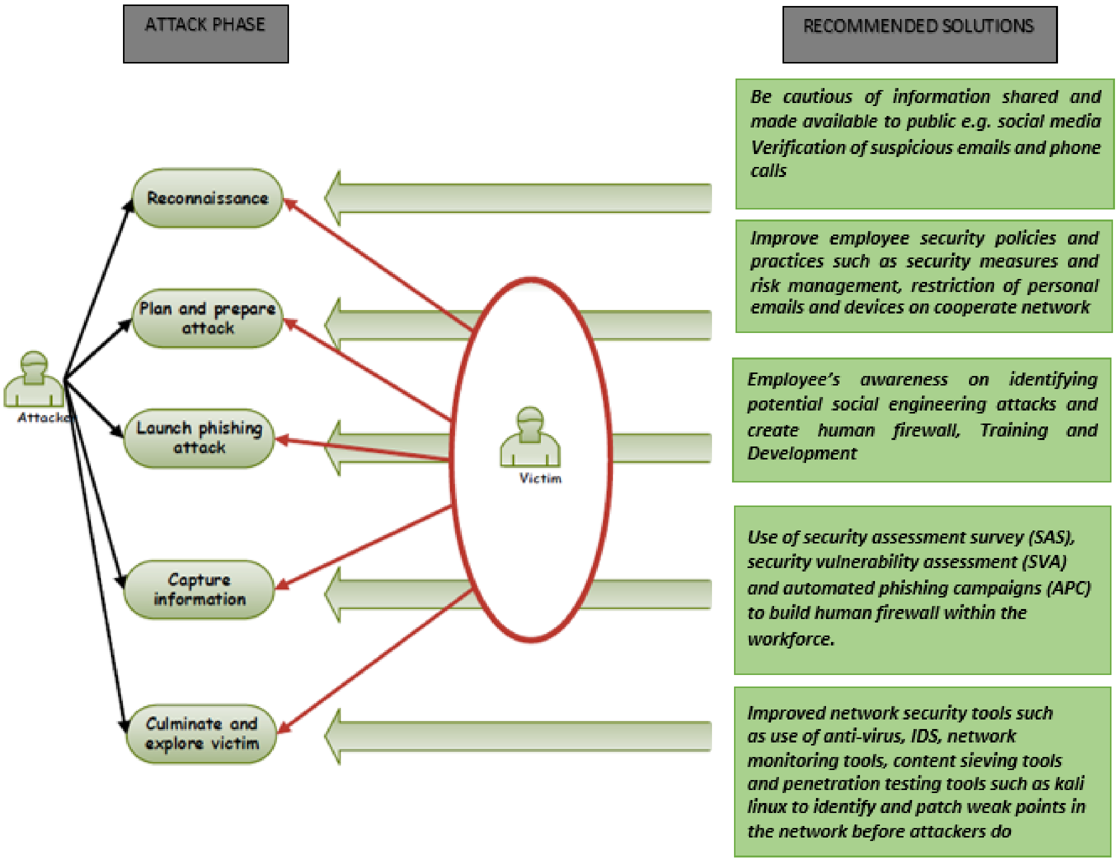
Despite the growing world of innovation and new security technologies, cyber-attacks are growing at exponential rate challenging the current complex secure architecture through social engineering attacks. To address these challenging attacks of social-technical deployment we propose in this research enterprise security frame to create a human firewall to combat challenging cybersecurity attacks. While many organizations are taking advantage of new innovative security technologies to protect their digital assets against attackers. It is, therefore, a good practice for organizations to implement strategic security plans considering humans as the weak link in security. Human firewall is by far the best-suggested method to mitigate social engineering attacks that bypass highly secure firewalls by exploiting human factor vulnerability Twitchell (2006). Social engineering attacks can be challenging since the attack depends on the successful manipulation of humans to achieve the attacker's objective

According to previous studies, it is advisable for organizations to adopt a new security measure of the creation of a human firewall from less crucial social attacks as denying an unauthenticated person entry into a premise. It is necessary for organizations to provide multiple security measures and strategies based on the attacks they are facing. Adams (2008) highlighted that technically oriented attacks have a limit in terms of data they can provide thus forcing hackers to deploy manipulative social engineering attacks to bypass security. This form of attacks assists attackers to access sensitive information such as passwords, security pin, account numbers and classified data that can put individual or organization at high risk of information theft and financial loss. Therefore to address these forms of attacks users need training and development to make them cyber aware by building a human firewall from top to lower management within originations Manske (2000). The human firewall in this context means good security practice measures by employees such as the use of strong passwords and be alert on email links or attachment as this is the major communication media used to compromise network using human factor vulnerability.

Furthermore, by implementing an enterprise security framework such as setting security policies to govern employee at the workplace it is a significant element in the creation of a human firewall to mitigate social engineering attacks. The compliance and relevance of security policy should be used to address social engineering attacks by making them clear and well distributed across the entire organizational chart within the company Thornburgh (2004). Such governing policies could be avoiding personal computers at the workplace or restrict accessing personal email account within cooperate network. This kind of policies has potential addressing challenging human vulnerability attacks threating users while online. The proposed outcome for this research is to come up with a security framework to address social engineering attacks deployed by cybercriminals, using the creative tactic to manipulate humans to gain access to sensitive information. This framework assists to address this form of attacks by identifying various steps used by attackers and thus when can implement effective counter security measures by building a human firewall through social engineering attack process stages.

3. HUMAN FIREWALL ENTERPRISE SECURITY FRAMEWORK TO MITIGATE SOCIAL ENGINEERING ATTACKS IN BOTSWANA

Most of the organizations in Botswana and globally are under war against astonishing social engineering attacks penetrating their network at ease. Manske (2000) previously presented that social engineered attacks are by far caused by human factor vulnerability which has led to a data breach in today cyberspace. Thus the creation of a human firewall could serve as the best strategic plan to mitigate social engineering attacks in Botswana. Human factor vulnerability has been proven to be the weakest link in information security chain compromising highly secured network infrastructures and security software, and yet it has often ignored and considered challenging to address Thornburgh (2004). The proposed framework is based on single-staged social engineering attack which consists of five stages: information gathering, planning and preparing the attack, execution of phishing attack, capturing sensitive data and lastly information exploitation. In every stage, the proposed framework will provide security recommendations guideline based on the attack phase to secure cooperate network against social engineering attacks while online. The proposed framework (Figure 3) could also be applied to multi-staged attacks since they both follow the same attack process cycle.



Be cautious of information shared and made available to public e.g. social media Verification of suspicious emails and phone calls

Improve employee security policies and practices such as security measures and risk management, restriction of personal emails and devices on cooperate network

Employee's awareness on identifying potential social engineering attacks and create human firewall, Training and Development

Use of security assessment survey (SAS), security vulnerability assessment (SVA) and automated phishing campaigns (APC) to build human firewall within the workforce.

Improved network security tools such as use of anti-virus, IDS, network monitoring tools, content sieving tools and penetration testing tools such as kali linux to identify and patch weak points in the network before attackers do

Figure 11: The proposed security framework to mitigate Social Engineering Attacks

The frameworks are designed to assist users to be alert and aware at every stage of social engineering attacks. In today connected world of internet of things, the question is no longer how secure are we? But how soon can we be compromised? Therefore the framework promotes the creation of a human firewall by training users in Botswana to be more aware to avert attacks in the wild. The framework proposed in this research figure 3 provides recommended solutions to mitigate possible social engineering attack in each stage of attack launched by the hacker. In case of a successful attack, the proposed framework provides the user with security countermeasure to appropriately take to mitigate further attacks depending based on the compromise stage they are in social engineering attack process.

The framework present in the following section five social engineering attack stages and the security countermeasure guidelines a user should follow to build a human firewall within an organization to mitigate social-technical attacks now and in the future.

Reconnaissance: This is the first stage of attack information gathering about the victim is done through public accessible information such as social media. To prevent this social engineering attacks the research framework proposes a limitation of accessible shared information on public, social media such as Facebook which give attackers so much information such as the targeted victim birthday, occupation, relatives and even disclosure of location to attacker based on check-in option in a Facebook status. This information can by far do damage allowing hackers to gain access to sensitive information by tricking individuals to bogus links and malicious attachments using fake legitimate emails based on information they gather about the victim and exploit human factor vulnerability. For instance, it's easy for attackers to impersonate trusted sender of the email or phone call based on the information gathered. According to Thornburgh (2004 limitation of public information alone cannot prevent reconnaissance therefore in the proposed framework we further recommend security verification measure to validate the attacker true identity. For instance, a customer receives a call from a restaurant he visited with checked in on Facebook telling him his payment is rejected and they need to take payment over the phone. The attack is already social engineered in the sense victim checked in location is used as attention picker making the user vulnerable and believe the caller is legitimate and provide card details to authorize payment without further verification of the called to identify first, leading sensitive financial information into wrong hands.

Plan and Prepare Attack: In this second stage of the attack process previously gathered information about the victim will be filtered and used to create manipulative attacks to gain access to cooperate networks and harvest sensitive data. The framework proposes security policies to govern how employees should interact with the internet of things (IoT) in Botswana's fast-growing digitalized world. These policies include verifying websites been accessed within corporate network as some email link could be bogus phishing emails socially engineered to trick users based on the information previously gathered. Thus exploiting human factor vulnerability. Through practicing good security measures within the organization the enterprise framework proposes users should make it a good practice to always verify the address bar of the website they are accessing to ensure the authenticity of the site certificate.

Conventionally, malicious sites do not have valid certificates, therefore, users should always take security measures to verify this sites as they are possible phishing attacks, and hence, by using recommended solutions of security risk management by mitigating social-technical attacks by avoiding such bogus sites.

To further ensure human firewall within the organization the proposed framework recommend a restriction on the use of personal email accounts at the workplace, and the restriction of connecting personal devices on the corporate network. To ensure human firewall at workplace employees should have governing rules to control what they do with the corporate network, in most cases, personal email accounts are easily attacked due to the low level of technical security as compare to highly secured cooperate network. Therefore in a case whereby users open their email accounts at work, there is a high chance they can open possible malicious link and attachments in their email compromising the entire cooperate network.

Launch Phishing Attack: Usually in this third stage the attacker's lunch the phishing attack which is sophisticated attacks which manipulate unaware users into phishing attempts through emails and phone calls. Lack of awareness within organizations has a significant impact on the exponentially increasing number of social engineering attacks in Botswana. Users are therefore recommended to be alert at all times of any suspicious email, phone calls and any social tactic that may be deployed by the attacker. Some of the proposed security countermeasures proposed by the framework are to ensure organizations and individual contributions to the awareness of social engineering attacks and the techniques to mitigate challenging attacks in today cyberspace. Provision of training and development with supporting material such as cybersecurity new reports and cooperate training on possible attacks can assist the creation of human firewall within the organization since by cyber aware workforce will find it easy to identify social engineering attacks and stay secure online Manske (2000). Furthermore, organizations need to make users more alert to any forms of attack by adequately sensitized with cybersecurity awareness measures and training. The framework proposes a general rule of thumb is awareness and training to ensure the non-disclosure of personal sensitivity data in public domains. Any personal information such as name, email address, the phone number must be handled with a high level of confidentially to avoid manipulative social engineering attacks. Any socially engineered attack should be reported to ensure such incidents are made known to security firms and originations to ensure secure network through awareness.

Capture Information: In this stage, the attacker harvests the data from previous phishing attempts made in the previous stage. Attackers are often looking for sensitive data such as password, pin codes, email address, security questions, and answers, therefore different forms of phishing attacks are launched targeting information needed by the attacker to breach systems security. To address this issue the proposed framework suggests the use of automated phishing campaign within the workforce to test the weak employees by failing to identify bogus emails and reveal sensitive data to attackers.However, the challenging part is that sometimes genuine emails may also be classified as malicious therefore it recommended for organizations to always run security vulnerability assessment to check where data could possible compromised. Security vulnerability assessment provide graphical present crucial security issues an organizations are facing by identifying the vulnerability within the network.Therefore by assessing possible means, an attacker can deploy to harvest data within the workforce can be controlled by the security assessment survey report used to assess individual weakness on social-technical attacks. The security assessment survey report includes a pop quiz, automated phishing campaigns, exams and certification of employees which can be used as a key performance indicator to determining weak employees likely to fall prey to social engineering attacks by testing general secure measures to be safe online.

Attack Culmination and Victim Exploitation: In this stage data collected from information gathering to recovery of sensitive information is now used to achieve the attacker s objective. It is in stage users need to take security countermeasures such as computer forensic investigation to perform penetration testing to identify and patch the weak links within cooperate network. Other high technology software can be used to detect phishing attacks such as Intrusion

Detection Software (IDS). Data protection software can also play a significant role in securing sensitive information such as passwords, credit card number, pin numbers and nation identify numbers. In a case of malware used in social engineering attack and the user is using data protection software it is unlikely for attackers to harvest data using remote access backdoor due to encryption with security protection software. Network monitoring tools such as Wireshark can be used to capture real network traffic to amylase any suspicious packets coming in the network to block and avoid further attacks. The proposed framework proposes the use of penetration testing tool Kali Linux (figure1) this toolkit is widely adopted by security experts to solve challenging security issues. With this tool kit, it is easy to assess vulnerabilities and generate reports to patch the weak holes within the organization network

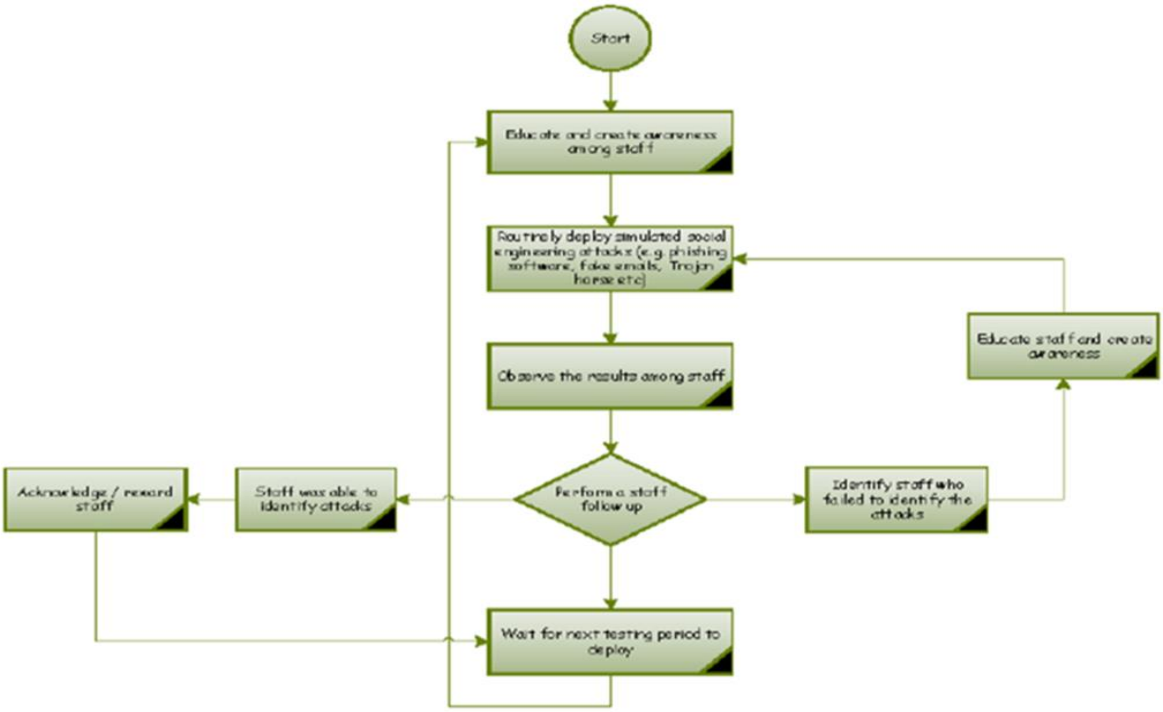

Start
Educate and create awareness among staff
Routinely deploy simulated social engineering attacks (e.g. phishing software, fake emails, Trojan horse etc)
Observe the results among staff
Educate staff and create awareness
Acknowledge / reward staff
Staff was able to identify attacks
Perform a staff follow up
Identify staff who failed to identify the attacks
Wait for next testing period to deploy

Figure 12: illustrate the proposed security framework for deployment of simulated social engineering attack campaigns within the organization to create human firewall.

The success of the proposed enterprise security framework depends on how much the workforce adhere to the specifics of the framework. To continuously engage users into cybersecurity awareness consistent educating users to alert them of social engineered attacks targeting them, can be by utilized as proposed in this framework through assessing activities done by the staff within cooperate network and requires monitoring to generate security assessment report to identify weak link within the workforce. To achieve human firewall IT personnel within the organizations in Botswana must periodically launch simulated social engineered attacks against staff members on a normal business day. The forms of attacks can vary from vishing to email phishing, once the simulated attack is launched results are observed and analyzed to identify weak staffs failing to identify launched malicious attacks. Identified weak link must be further trained and developed into a strong human firewall by being aware and alert all when performing their task online. In addition, to ensure strong human firewall employees who are able to be aware and secure online by identifying potential threats should be acknowledged as a means of motivation to empower the workforce and become more secure.

Education plays a significant role in making staffs aware and alert to current cyber-attacks possible targeting them. Education and training is by far a necessary action that management can take as a countermeasure to combat social-technical attacks in the wild. Each and every level in the organizational hierarchy should make it a good practice to secure and protect origination from social engineering attacks by avoiding actions that can lead to the divulging of company sensitive data such as customer data records, passwords or even sensitive financial details. Therefore staffs should be educated and trained to avoid revealing any sensitive information they are requested either through a phone call, in person and email communication and use recommended solutions in each stage of the attack. Finally, users are recommended to stay alert on activities that could compromise them and in case of such attacks they should report to the relevant department to monitor such attacks in the futures.

4. CONCLUSION

To conclude this research paper, challenging cyber threats such as social engineering attacks will continue to assist attackers to gain access to secured sensitive information through humans as the weak link in the security chain. Social engineered attacks use tactics to trick victims into submitting personal information, passwords and financial details since humans are easily manipulated based using less suspicious means of attacks to win the trust of users and achieve the core objective of mining credentials to bypass security. Social engineers are experts in network security and social skills which enables them to manipulate victims to gain access to cooperate networks and secured data without the user's knowledge that they are compromised. Phishing attempts are nothing but lies and scams fooling users to reveal credentials. Social engineering attacks are challenging and complex to solve because controlling human behavior is by far impossible task to do.Therefore, organizations in Botswana need to put in mind that, while investing on new advance cybersecurity technologies to mitigate cyber-attacks human factor vulnerably s by far the weakest link in the security chain. Furthermore to create strong human firewall organizations in Botswana need enterprise security framework which will provide adequate training of individual ongoing cybersecurity attacks. The is no obvious concrete solution to exponential rise of challenging cyber-attacks however change of governing policy within an organization can be used to restrict employee actions while using cooperate network. A lot of damage has been caused by human factor vulnerability resulting in devastating data breaches attacks. The complexity of social engineering attacks comes with the different multi-staged attacks launched against victims, it is hard to just use one method security to combat these attacks therefore by far the best solution is to prioritize awareness within the workforce by reporting any suspicious event to others to avoid them fall prey for such attacks in the future

REFERENCES

[1] Wenke Lee, Bo Rotoloni, "Emerging cyber threats, trends and technologies", Technical report,Institute for Information Security and Privacy, 2016.

[2] "Internet organized crime threat assessment", Technical report, Europol, 2016.

[3] James Comey, "Worldwide threats to the homeland: ISIS and the new wave of terror, statement before the house committee on homeland security", FBI, July 2016.

[4] "Internet security threat report", Technical report, vol. 21, Symantec, April 2016.

[5] Nahal Sarbjit, Ma Beijia, Tran Felix, "Global cybersecurity primer", Technical report, Bank of America Merrill Lynch, 2015.

[6] Nabie Y Conteh, Paul J Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks", International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016.

[7] "State of cyber security implications for 2016", Technical report, ISACA and RSA, 2016.

[8] "The human factor", Technical report, Proofpoint, 2016.

[9] Kevin D Mitnick, William L Simon, "The art of deception: Controlling the human element of security", John Wiley & Sons, 2011.

[10] "Hacking the human operating system: The role of social engineering within cybersecurity", Technical report, Intel Security, 2015.

[11] Prashant Kumar Dey, "Prashant's algorithm for password management system", International Journal of Engineering Science, pp.2424, 2016.

[12] Seppo Heikkinen, "Social engineering in the world of emerging communication technologies", Proceedings of Wireless World Research Forum, pp. 1-10, 2006.

[13] Rahul Singh Patel, "Kali Linux Social Engineering", Packt Publishing Ltd, 2013.

[14] Joseph Muniz, "Web Penetration Testing with Kali Linux", Packt Publishing Ltd, 2013.

[15] Andrea Cullen, Lorna Armitage, "The social engineering attack spiral (seas). In Cyber Security And Protection Of Digital Services (Cyber Security)", 2016 International Conference On, pp.1-6, IEEE, 2016.

[16] Mika Kontio et al, “Social engineering”, pp.101, 2016.

[17] “Social engineering fraud: questions and answers”,Technical report, Interpol, December 2015.

[18] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, “Advanced social engineering attacks”, Journal of Information Security and applications, Vol.22, pp.113-122, 2015.

[19] E Rutger Leukfeldt, Edward R Kleemans, Wouter P Stol, “Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks”, British Journal of Criminology, pp. azw009, 2016.

[20] Nalin Asanka Gamagedara Arachchilage, Steve Love, Konstantin Beznosov, “Phishing threat avoidance behaviour: An empirical investigation”, Computers in Human Behavior, Vol.60, pp.185-197, 2016.

[21] Parker Graeme, Shala Vlerar, “Social engineering and risk from cyber-attacks”, Technical report, PECB,February 2019

[22] “Kali Linux”, https://www.kali.org/. [Online; accessed on 04 Feburary 2019].