SOCIAL ENIGNEERING ATTACK USING SETOOLKIT PACKGES IN KALI LINUX - IP ADRESS APROACH

Ahmed Mohammd Al-tarawneh & Alaa H Al-Hamami
King Hussein Faculty for Computing Sciences, Princess Sumaya University for Technology, Amman, Jordan
amtcah@gmail.com

ABSTRACT: *One of the largest and fastest growing websites today are related to social networks such as Facebook and Twitter, where these websites provide the service of finding new friends and groups. Since they have a large amount of information and billions of users available made them critical with respect to the user security and privacy. In this paper, we will present one of the social engineering attacks, with an experiment on Kali Linux operating system using the Set package from the SetoolKit over Facebook. In this type of attack; attacker will collect the information from the victim device, login information and IP address.*

Keywords—Information Security, Information Assurance, Social E Toolkit (SET) engineering, penetration testing, reverse social engineering, Kali Linux, Facebook.

I. INTRODUCTION

Security is one of the most important factors for information system quality and robustness. Since most of people think that software and hardware bugs are the only reasons for making vulnerabilities in information systems. While in reality the human is causing more risk in the information systems [3].

No matter how much work and research have been done in the security field such as network holes, patches, and other kind of attacks to improve and resolve all holes in the systems, since security it's all about trust, blind trust in big names like twitter and Facebook encourages people to accept all updates or any new configurations. Trust generally leads to vulnerable systems in protection and authenticity [1].

Since people are easily manipulated, they are the weakest point in the security chain. Social engineering attacks based on this fact, where many attacks success because of human errors.

In this paper, we will discuss the concept and methods (attacks) of the social Engineering on social media platforms as (Facebook, twitter and Malicious software’s), the idea is how to convince the victim voluntary to give the attacker a critical information such as email, passwords or some personal information’s throw social media platforms. Which called Website cloning attack, where the user trust the mirror page link as if it’s a real page link, in this attack user provide a critical information easily, in this paper will present an experiment with solutions. In section 2 we are going to present related work , section 3 will be about social engineering attack and the set tool kit in Kali Linux, in section 4 experiment part, section 5 is about the results and eventually the conclusion will be presented in section 6.

2. RELATED WORK

Social engineering attacks appeared in early 90s'; so many tools are created with the fast growing in social media and networks. Social engineering in early stages started with phones, where the attacker call the victims and convince them that they have a power and privileges, so the victims give a sensitive information.

.

Nowadays social networks replaced by the traditional communication tools, which ease the mission to trick people, where a lot of users are connected and available online. Since Social E Toolkit (SET) package is used to implement one of the social engineering attacks on Gmail accounts, in this paper we will present same approach to trick people over Facebook, and collect more than login information, IP address and victim device information might be used in other attacks.

3. SOCIAL ENGINEERING TOOL KIT MODE OF ACTION

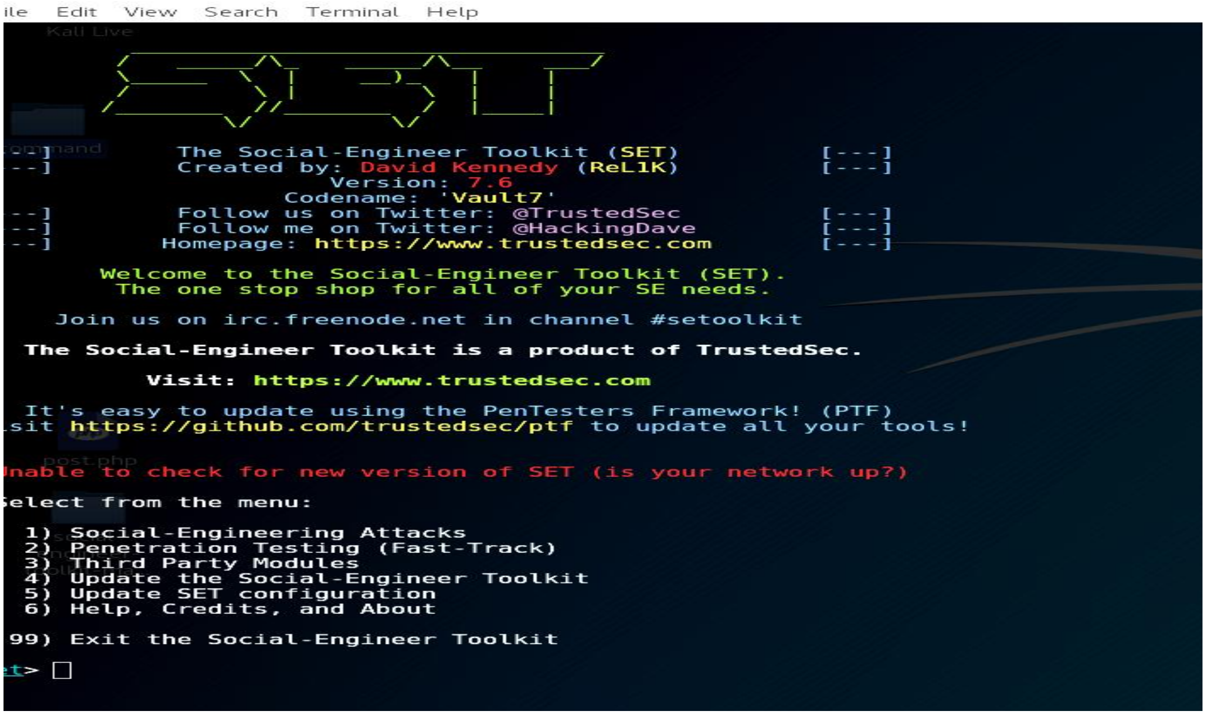
Social engineering is the art to trick people and make them share sensitive information voluntary. This is considered as one of the attack types. Attackers aimed to let people into giving up their confidential information such as their passwords or bank information, and in another cases attacker will gain the control to the victim computer [4].

Also, another notion for this type of attack attached to it called reverse social engineering attacks, where the attacker does not need to contact the victim; however, the victim tricked into contacting with the attacker. So, a high degree of trust build between them since it started from the victim side [5]. Most of victims are not aware about the methods are used to attack them, while there are many tool kits to implement these kinds of attacks; one of these kits is for social engineering attacks called Setoolkit over the Kali Linux operating system include the SET method.

SET is a software package to be used over Social engineering attacks, concentrates on attacking the human element of security. Also, it's the most complete and most advanced Social Engineering toolkit available as open source software [3].

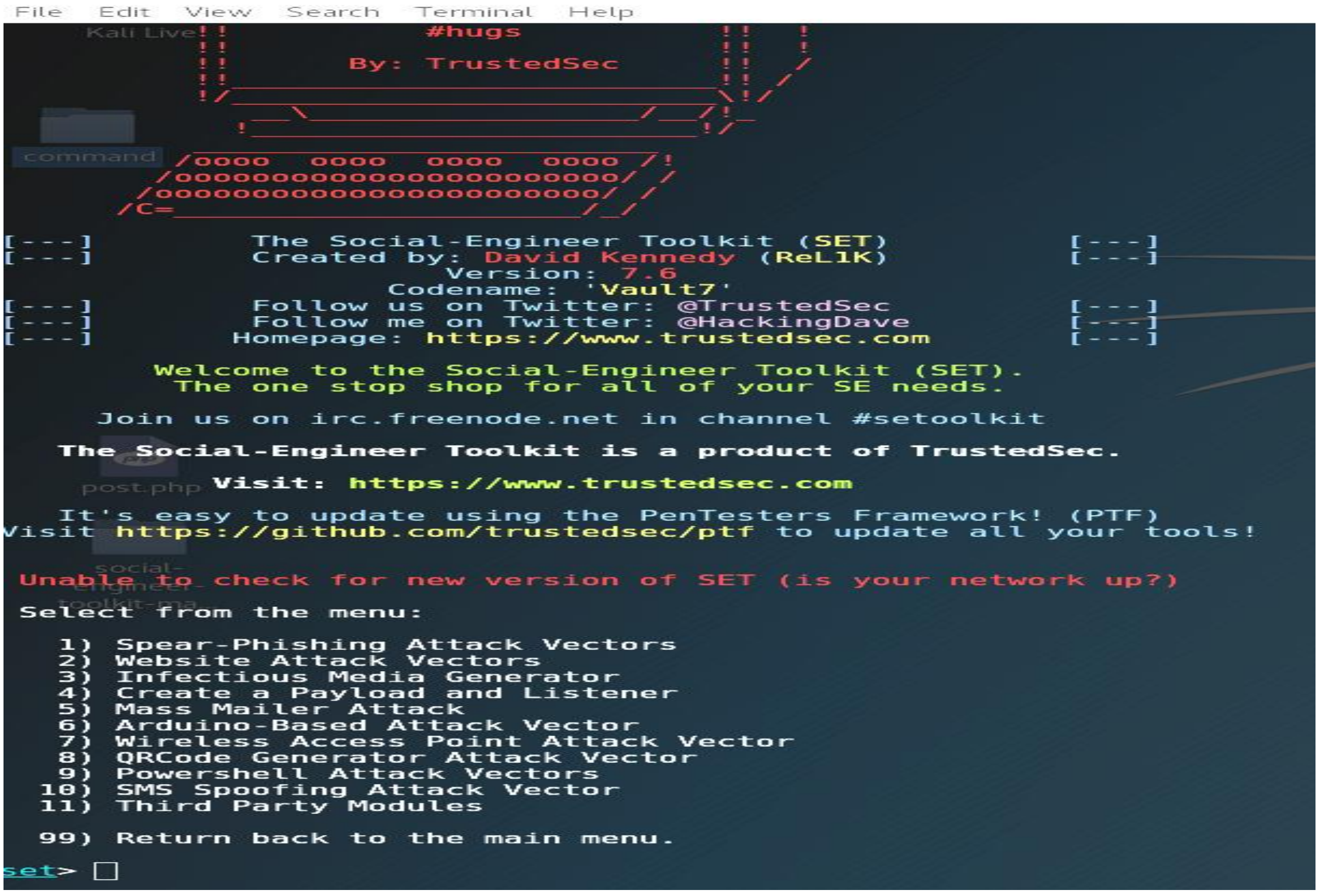
4. EXPERMINT

In this experiment, we are using the social engineering tool kit SetoolKit with SET package over Kali Linux OS. Kali aimed at advanced penetration testing, security auditing and contain hundred tools for information security tasks. SET tool is used to apply the web cloning attack. Figure 1 shows the user interface for the options supported with SET command and Figure 2 shows the Website Attack Vector



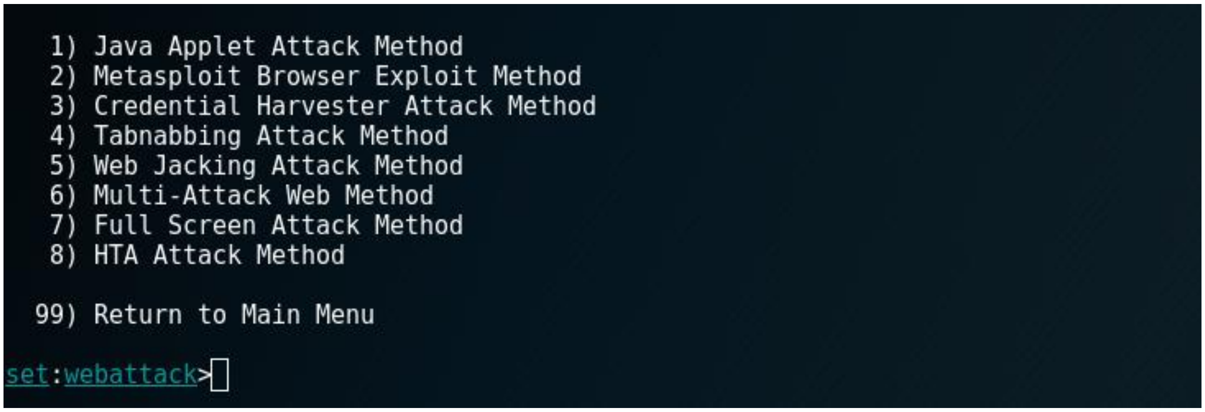
```
           The Social-Engineer Toolkit (SET)           [---]
           Created by: David Kennedy (ReL1K)           [---]
                   Version: 7.6
                Codename: 'Vault7'
           Follow us on Twitter: @TrustedSec           [---]
           Follow me on Twitter: @HackingDave          [---]
          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)
isit https://github.com/trustedsec/ptf to update all your tools!

nable to check for new version of SET (is your network up?)

elect 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

t>
```

Figure 1User Interface



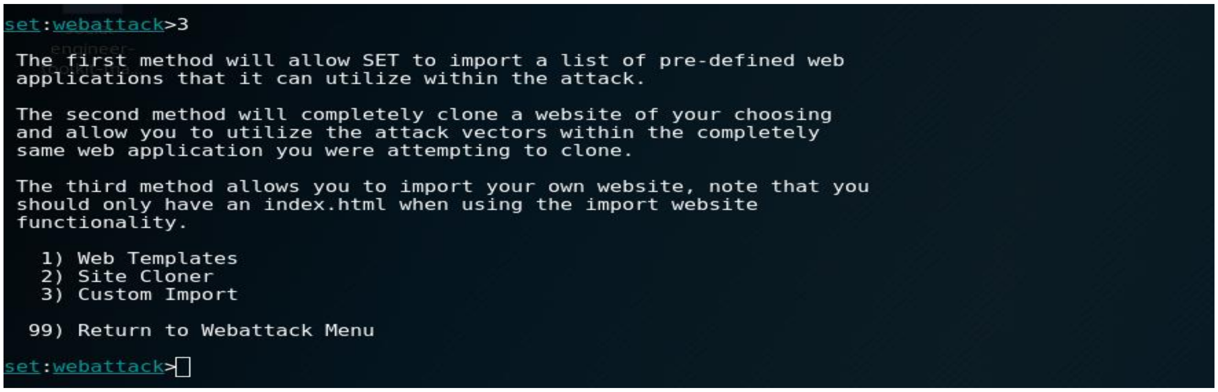
```
                  #hugs
              By: TrustedSec

[---]        The Social-Engineer Toolkit (SET)          [---]
[---]        Created by: David Kennedy (ReL1K)          [---]
                     Version: 7.6
                  Codename: 'Vault7'
[---]        Follow us on Twitter: @TrustedSec          [---]
[---]        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!

 Unable to check for new version of SET (is your network up?)

 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 2 Website Attack Vectors



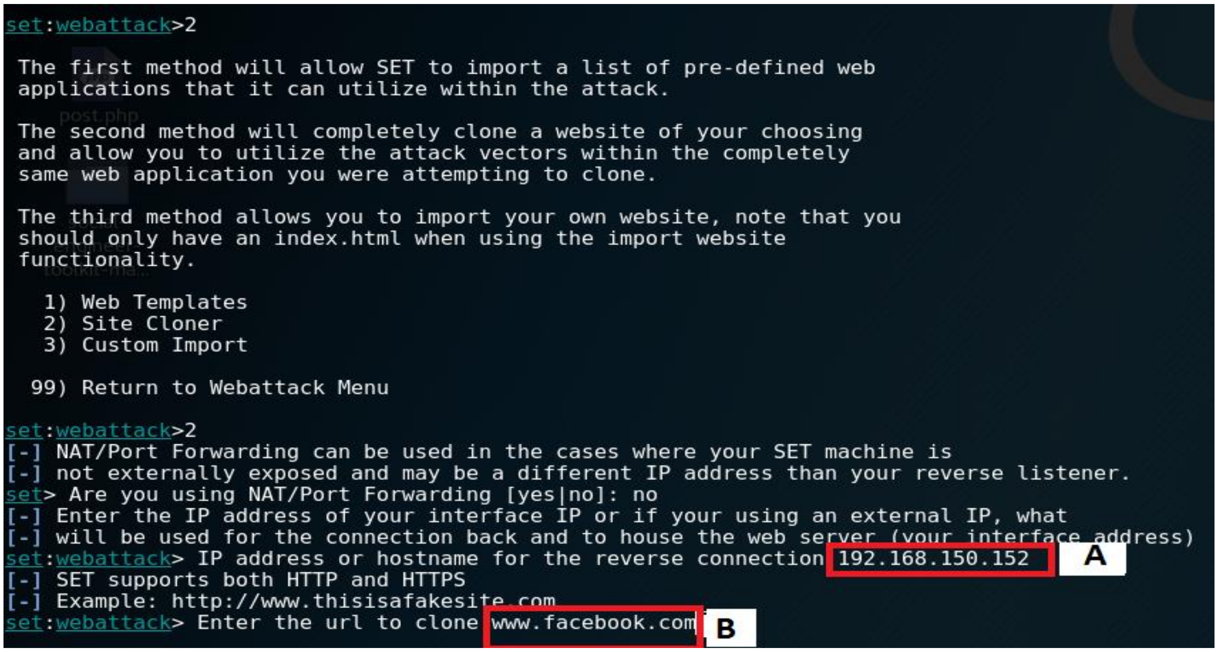
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

Figure 3 Credential Harvester Attack Method



```
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 4 Site Cloner



```
set:webattack>2

 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
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, what
[-] will be used for the connection back and to house the web server (your interface address)
set:webattack> IP address or hostname for the reverse connection 192.168.150.152
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone www.facebook.com
```

Figure 5 Add IP & URL

Provedas three options as in Figure 4, the second method will completely clone a website of your choosing and allow

This section will show an example where the attacker's goal is to collect login information and IP address for the victim over Facebook. After starting SET tool; you will choose from displayed menu in order as following; from SET

menu choose "Website Attack Vectors", this will have displayed another menu choose "Credential Harvester Attack Method", then choose "Site Cloner" from the new menu.

Since the site cloner method is chosen attacker needs to specify which site he/she wants to clone.

We will take a look at the third option, Credential Harvester Attack Method. Figure 3 shows the list of vectors available:you to utilize the attack vectors within the same web application that you were attempting to clone.

Add my IP address and the site we want to clone as in Figure 5.

A. My (Host) IP address

B. Website address to clone: www.facebook.com

Attacker will provide the host IP address and Facebook URL as the website to be cloned, and that will implicit starting the apache server (PHP). The victim start Adding his/her credentials to Facebook fake page [2] as in Figure 6.

After the victim receives the link many scenarios might occur:

(1) The victim discards it.

(2) The victim opened the link, however closed it.

(3) The victim opened the link, entered his/her credentials even if it's correct or not, then hit submit.

The attacker will use a Fake Facebook page as shown in Figure 6.

We are interested in the second and third scenario, where click in the link and the submission process will guarantee that the IP address will be collected. The specifications of the victim device in addition to the credential info that victim entered, whether he/she entered his/her login information or not. This is one of the main profit gained by this approach.While IP addresses can be used on other serious attacks.

The fake page will talk to POST.PHP and save the entered text (the login information) on a text file. Then victim will automatically have directed to a real page which is not noticeable.

There are several web sites used to hide and cover the attacker IP address. These websites create mock link for the IP address similar to other regular links, so the user can't distinguish it such as the website called TinyURL.

Example for fake URL using TinyURL website to cover IP address: 192.168.155.130.

Fake URL will appear as:

http://tinyurl.com/FacebookAppVistor

Since the real URL for Facebook real page

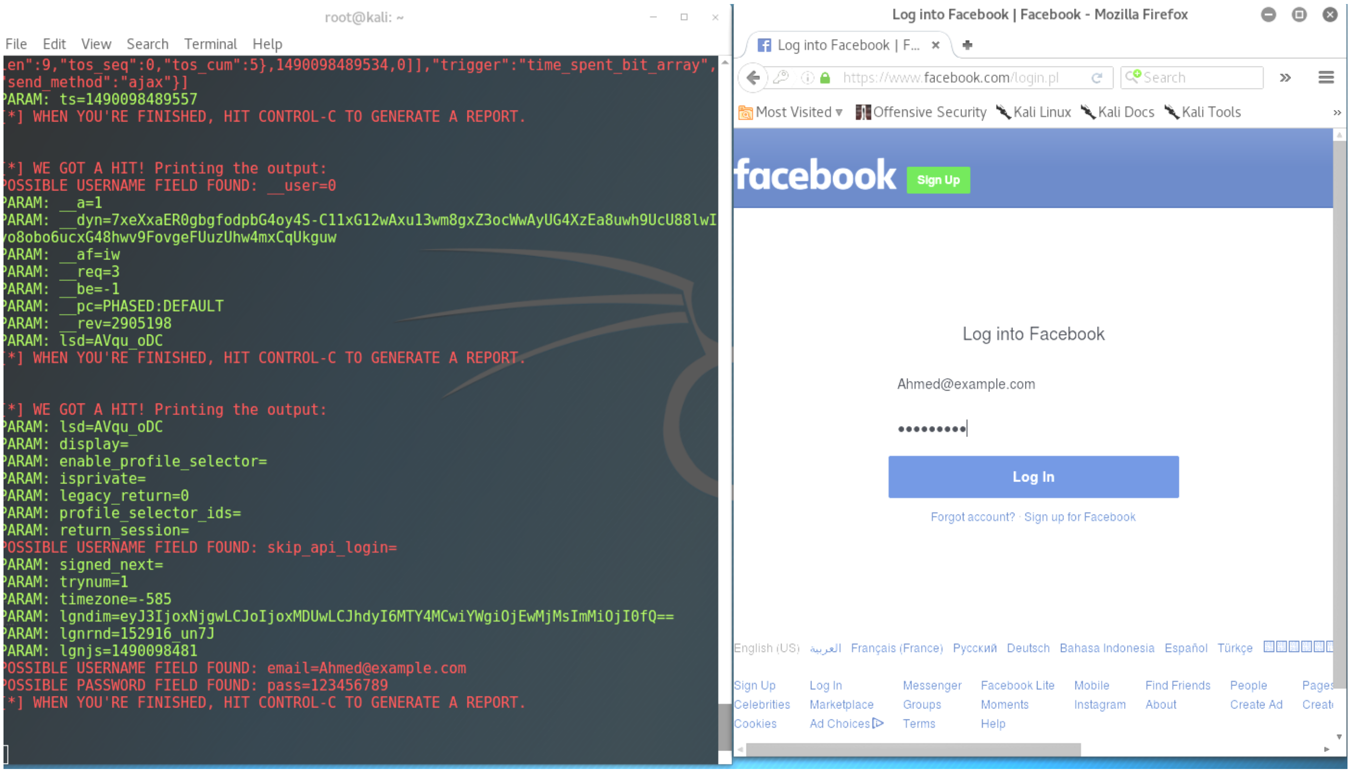
Real URL: https: //www.facebook.com/login.php?_rdr

When we got to the text file path, that post.php created, we will find the victim Email and the password he/she entered on the fake page login.

As we mentioned above this approach is successful in both ways, whether we got the login information or not. Anther types of attack could be implemented using IP address (ex. DOS Attack, Ping Sweep Attack, etc.).

5. RESULT AND DISCUSSION

As a result, for this experiment, the IP address, the specifications of the victim device (the type of browser, the operating system name and version) and the credential info that victim entered will be collected as shown in Figure 6. This will make the victim vulnerable for many attacks.


root@kali: ~
File Edit View Search Terminal Help
Log into Facebook | Facebook - Mozilla Firefox
Log into Facebook | F...
https://www.facebook.com/login.pl
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
facebook
Sign Up
Log into Facebook
Log In
Forgot account? · Sign up for Facebook
English (US) العربية Français (France) Русский Deutsch Bahasa Indonesia Español Türkçe
Sign Up Log In Messenger Facebook Lite Mobile Find Friends People Pages
Celebrities Marketplace Groups Moments Instagram About Create Ad Create
Cookies Ad Choices Terms Help

```
en":9,"tos_seq":0,"tos_cum":5},1490098489534,0]],"trigger":"time_spent_bit_array",
'send_method":"ajax"}]
PARAM: ts=1490098489557
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __dyn=7xeXxaER0gbgfodpbG4oy4S-C11xG12wAxu13wm8gxZ3ocWwAyUG4XzEa8uwh9UcU88lwI
yo8obo6ucxG48hwv9FovgeFUuzUhw4mxCqUkguw
PARAM: __af=iw
PARAM: __req=3
PARAM: __be=-1
PARAM: __pc=PHASED:DEFAULT
PARAM: __rev=2905198
PARAM: lsd=AVqu_oDC
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVqu_oDC
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-585
PARAM: lgndim=eyJ3IjoxNjgwLCJoIjoxMDUwLCJhdyI6MTY4MCwiYWgiOjEwMjMsImMiOjI0fQ==
PARAM: lgnrnd=152916_un7J
PARAM: lgnjs=1490098481
POSSIBLE USERNAME FIELD FOUND: email=Ahmed@example.com
POSSIBLE PASSWORD FIELD FOUND: pass=123456789
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Ahmed@example.com

•••••••••

Figure 6 victim credential info

5.1 PREPARATION OF THE TARGET PACKAGE USING SOCIAL ENGINEERING

Recently, more countries and governments have started to use social engineering methods to gather information about dangerous far targets. Using social engineering methods enables us to minimize risks by not exposing intelligence sources on the ground.

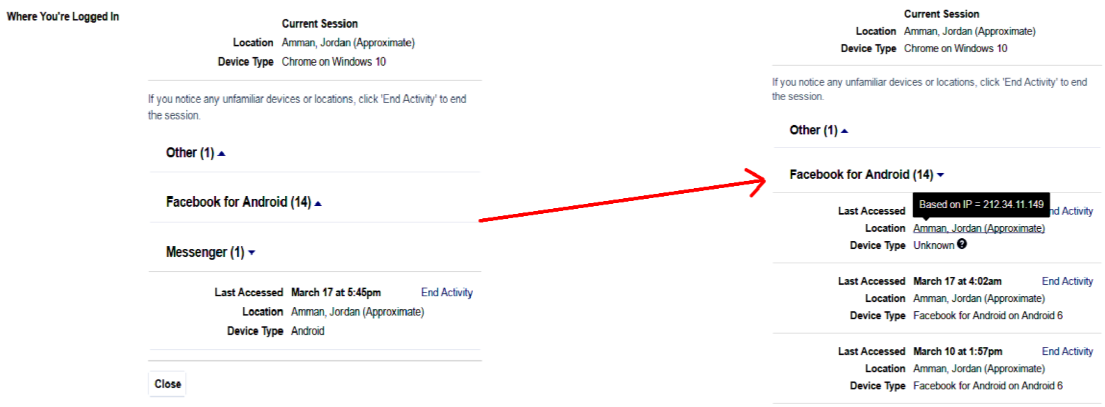
In this part of study, the gathered data were proceed by analysts to produce the target package that hold an important data without being at the place of mission such as Facebook.

The first scenario, which was mentioned above, if we got IP address, the following information, can be obtained:

1. Geographic location using this website : (https://www.ip2location.com/)
2. The company that operate the network.
3. Doing another attack such as metasploit software from SetoolKit to create payload and send it to target to get a full access from victim devises and more over about metaspolit that has many capability features for example run vnc, keylogger and dumphash.

The second scenario, if the victim entered his/her credentials, firstly, we can get full access in victim account and obtain the following information as in Figure 7:

1. Login Approvals like phone number and email address that guide us to a lot of information.
2. Trusted Contacts from (list of friends, massages).
3. Where the victim was Logged In and this feature can give many information such as Last Accessed, Device Type, and IP addresses of location.



Where You're Logged In

Current Session
Location Amman, Jordan (Approximate)
Device Type Chrome on Windows 10

If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Other (1) ▲

Facebook for Android (14) ▲

Messenger (1) ▼

Last Accessed March 17 at 5:45pm End Activity
Location Amman, Jordan (Approximate)
Device Type Android

Close

Current Session
Location Amman, Jordan (Approximate)
Device Type Chrome on Windows 10

If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Other (1) ▲

Facebook for Android (14) ▼

Last Accessed Based on IP = 212.34.11.149 nd Activity
Location Amman, Jordan (Approximate)
Device Type Unknown

Last Accessed March 17 at 4:02am End Activity
Location Amman, Jordan (Approximate)
Device Type Facebook for Android on Android 6

Last Accessed March 10 at 1:57pm End Activity
Location Amman, Jordan (Approximate)
Device Type Facebook for Android on Android 6

Figure 7 current session

4. The analysts can study the target behavior from the posts where shared on victim Facebook profile.

5.2 SOCIAL ENGINEERING AND OPEN SOURCE INELLIGENCE

After gathered basic critical information about the victim and applied into open source intelligence tools, it could lead to more critical information about the victim as shown in Figures, 8, 9, 10 & 11 [6].

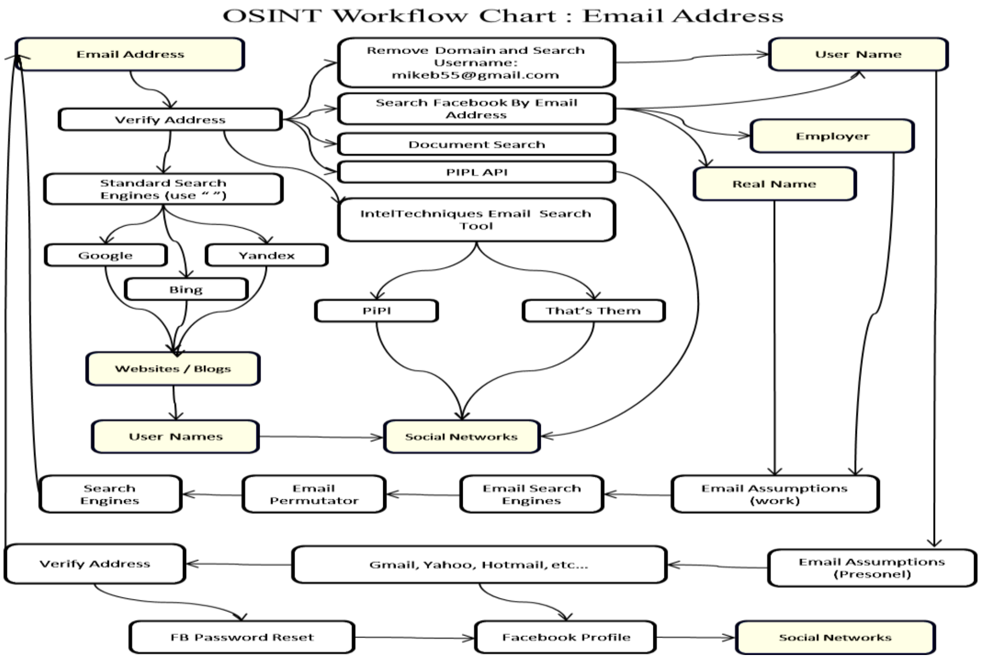


Figure 8 Email Address

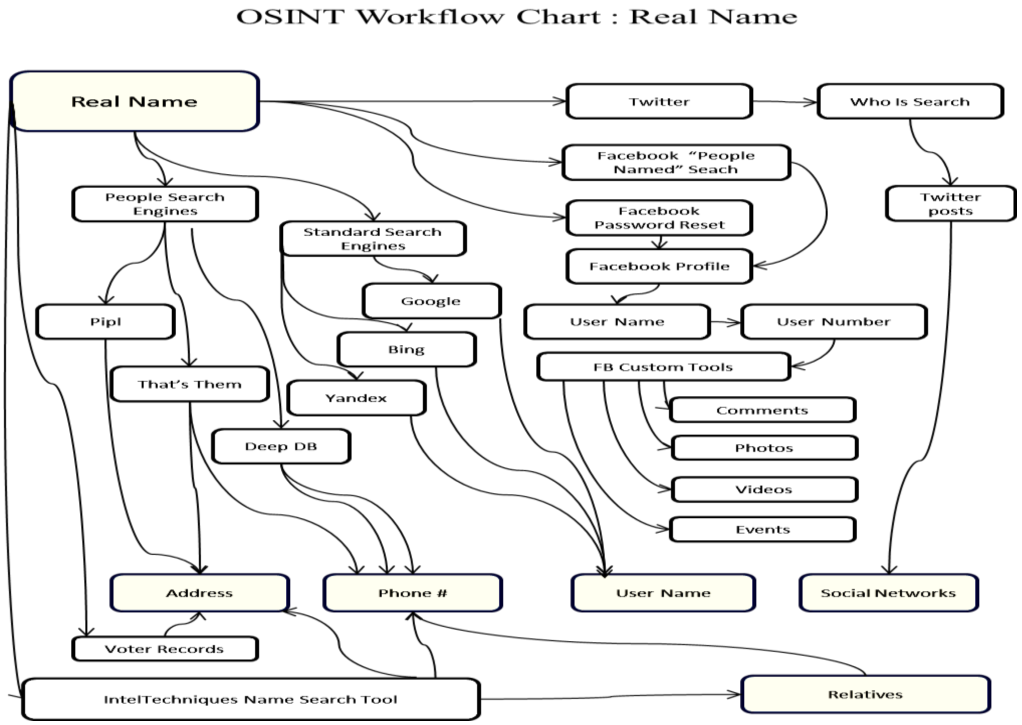


Figure 9 Real Name

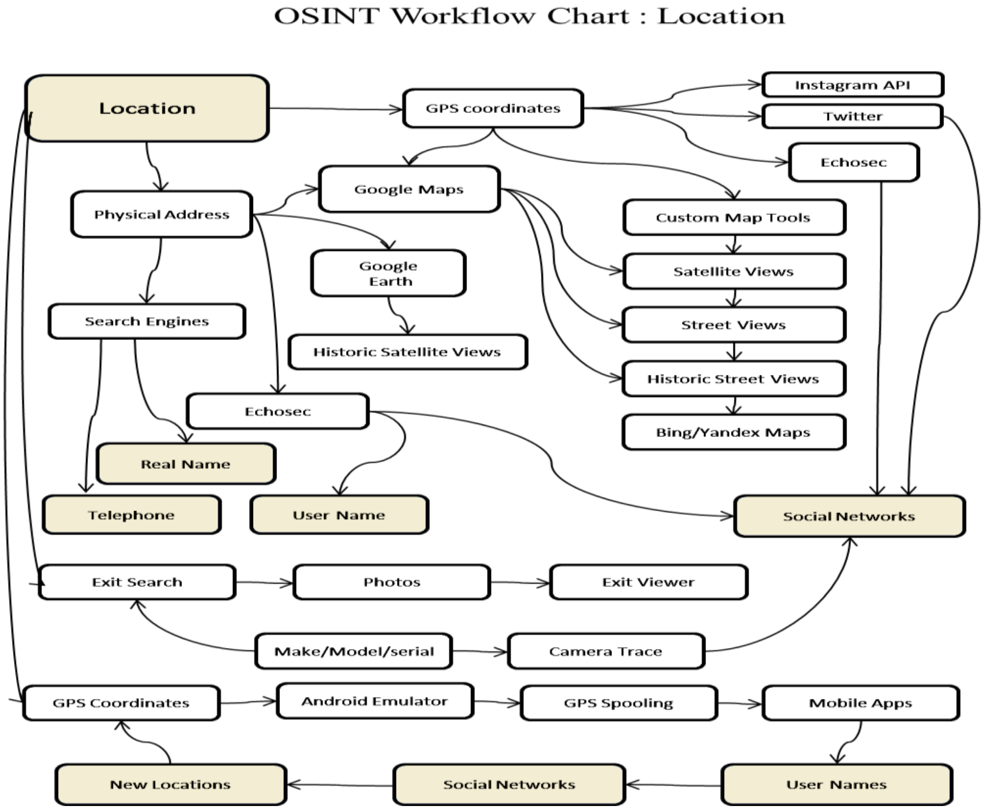


Figure 10 Location

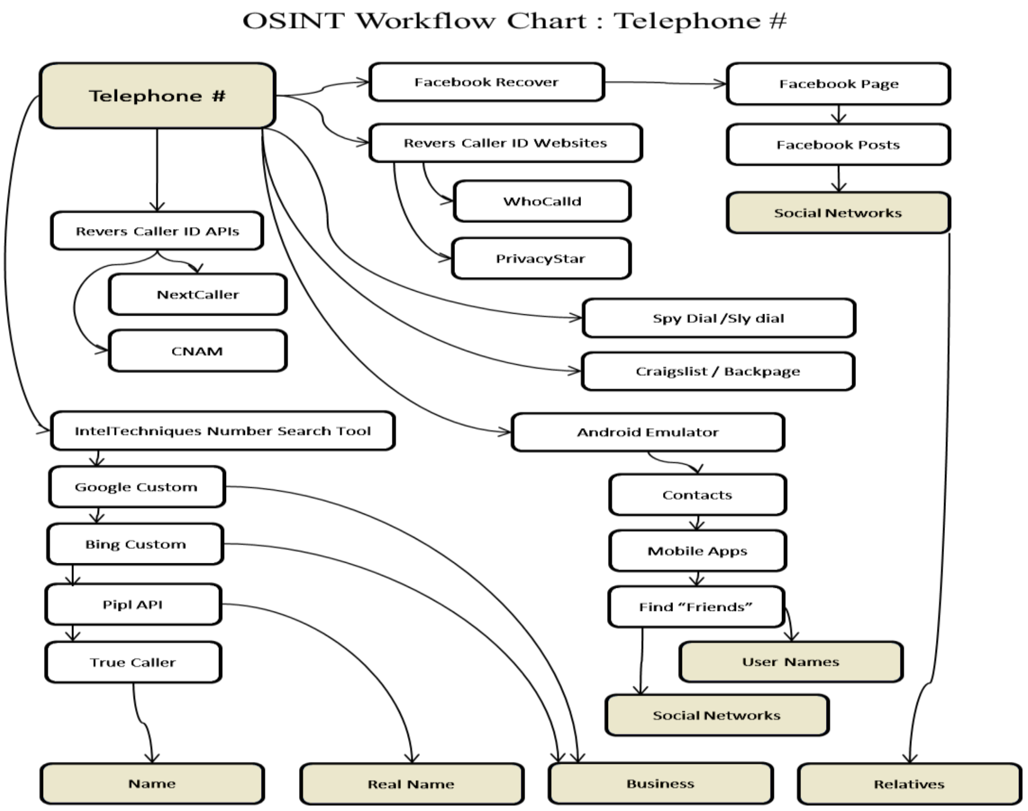


Figure 11 Telephone

6. CONCLUSSION

One of the most important methods that used in evaluation of information security is penetration testing including social engineering. Since the user is the weakest in the security chain.The main characteristic of SET is its one of the open source code packages, where a lot of developers can always add more and make it easy to use and provide a new functionality.

Rapid developing system for penetration testing will be more open for creating new and advanced attack vectors.

REFERENCES

[1] Granger, Sarah. "Social engineering fundamentals, part I: hacker tactics." Security Focus, December 18 (2001).

[2] Pavković, Nikola, and Luka Perkov. "Social Engineering Toolkit—A systematic approach to social engineering." MIPRO, 2011 Proceedings of the 34th International Convention. IEEE, 2011.

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

[4] Power, Richard, and Dario Forte. "Social engineering: attacks have evolved, but countermeasures have not." Computer Fraud & Security 2006.10(2006):17-20.

[5] Irani, Danesh, et al. "Reverse social engineering attacks in online social networks." International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer Berlin Heidelberg, 2011.

[6] MICHAEL BAZZELL. "OSINT WORKFLOW PROCESSES." Open Source Intelligence Techniques. 5th Edition ed. USA: Library of Congress Cataloging-in-publication Data, 2016. 394-99. Print.