RESEARCH ARTICLE OPEN ACCESS

Exploring the Social Engineering Toolkit (Set) Using Backtrack 5R3

Talatam. Durga Rao*, Vankayalapati. Sai Madhav**
*(Department of Electronics and Computers, KL University, Guntur, India)
** (Department of Electronics and Computers, KL University, Guntur, India)

ABSTRACT
Linux Operating System is being reverenced by many professionals because of its versatile nature. As many network security professionals ,particularly those of ethical hackers use linux in an extensive way, did we ever observe how and why the number of hackers were enhancing day to day. Not only professionals ,every one are unleashing their hacking potentials with the help of Backtrack5R3 operating system which is a comprehensive tool kit for security auditing. This paper emphasizes on the so called SET (Social Engineering Toolkit).In a pen-testing scenario, alongside uncovering vulnerabilities in the hardware and software systems and exploiting them ,the most effective of all is penetrating the human mind to extract the desire information. Such devious technics are known as social engineering ,and computer based software tools to facilitate this form the basis of Social Engineering Toolkit

Keywords: Backtrack5 R3,Ethical hackers,Metasploit Framework ,Pentesting , Security auditing ,Social Enginneering Toolkit,Website Attack Vectors.

I. INTRODICTION:

TrustedSec is considered as a doyen of Social Engineering toolkit(SET) ,which is the only founder of SET.An open source Python-driven tool aimed at penetration testing around social engineering is SET.It is a standard for social-engineering penetration tests and supported heavily with in the security community[1].Social Engineering Toolkit has over elusive number of downloads and is aimed at literally enhancing attacks in social engineering type environment. Many consulting companies believe that social engineering is one of the hardest attacks to protect against and now one of the most prevalent . In that way this is considered as the potential for network intruders.

II.SYSTEM REQUIREMENTS:

2.1 SOFTWARE REQUIREMENTS:

- Backtrack5 R3 Operating system
- Social Engineering Toolkit(SET)
- Metasploit Framework

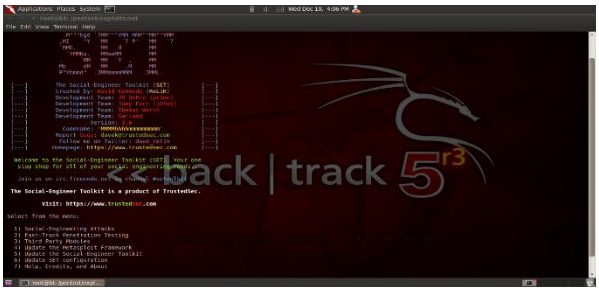
2.2 HARDWARE REQUIREMENTS:

- Intel i-3 Processor
- 2GB RAM
- 36GB Hard Disk

III.METHODOLOGY:

Firstly we need to install Backtrack5 R3 .In order to explore the various options of SET we should give the followng commands of cd /pentest/exploits/set and ./set in terminal. Then it gives an extensive list of options which have unique functionality for unique operations. Of all these options, Social Engineering Attacks plays a prominent role for the purpose of intrusion which is so called hacking.

However each option has its own significance ,and let us see how the options we displayed in the terminal:



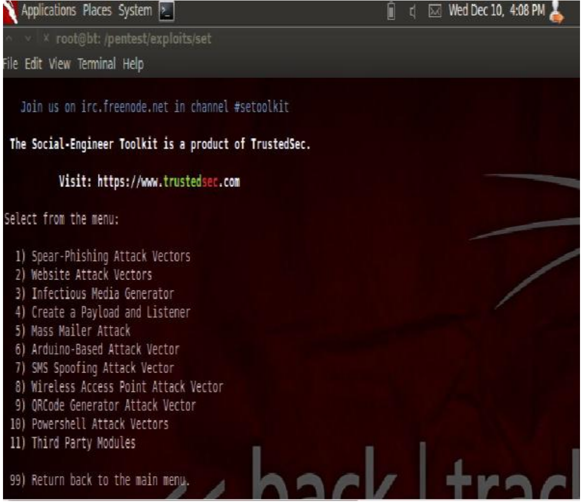
Applications Places System
Wed Dec 10, 4:06 PM
root@bt: /pentest/exploits/set
File Edit View Terminal Help
<< back | track 5 r3

```
[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
[---]        Development Team: JR DePre (pr1me)       [---]
[---]        Development Team: Joey Furr (j0fer)      [---]
[---]        Development Team: Thomas Werth           [---]
[---]        Development Team: Garland                [---]
[---]                  Version: 3.6                   [---]
[---]          Codename: 'MMMMhhhhmmmmmmmmm'          [---]
[---]        Report bugs: davek@trustedsec.com        [---]
[---]        Follow me on Twitter: dave_rel1k         [---]
[---]        Homepage: https://www.trustedsec.com     [---]

 Welcome to the Social-Engineer Toolkit (SET). Your one
  stop shop for all of your social-engineering 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 Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About
```

Fig:1

3.1.Social engineering attack is the art of manipulating people so they give up confidential information. The types of information these attackers are seeking can vary, but when individuals are targeted the attackers are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Attackers use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak). Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. It doesn't matter how many locks and deadbolts are on your doors and windows, or if have guard dogs, alarm systems, floodlights, fences with barbed wire, and armed security personnel; if you trust the person at the gate who says he is the pizza delivery guy and you let him in without first checking to see if he is legitimate you are completely exposed to whatever risk he represents[2].


Applications Places System
Wed Dec 10, 4:08 PM
root@bt: /pentest/exploits/set
File Edit View Terminal Help

```
  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) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.
```

Fig:2

From the displayed options of given commands in the terminal ,if option 1 that is pointing to Social Engineering attacks is chosen, it again gives above set of extensive fields(given in Fig:2). They are:

A. Spear-Phishing Attack Vector:

The Spear Phishing menu is used for performing the targeted email attacks against a victim.You can send multiple emails based on what you have harvested or you can send it to individuals.You can also utilize file format(for example a PDF bug) and send the malicious attack to the victim in order to hopefully compromise the system.

B.Website Attack Vectors:

Using this,the task simply is to attack victim via the internet browser.In this we will attack in such a way that we will attack via website generated by Social Engineering Toolkit to open by victim. The web attack vector, simply saying , is used by performing the phishing attacks against the victim in hopes they click the link. There is a wide variety of attacks that can attack once they click the link.

C.Infectious Media Generator:

The Infectious USB/DVD creator will develop a Metasploit based payload for you and craft an auto run.inf file that once burned or placed on a USB will trigger an autorun feature and hopefully compromise the system. This attack vector is relatively simple in nature and relies on deploying the devices to the physical system.

D.Create a payload and Listener:

The create payload and listener is an extremely simple wrapper around metasploit to create a payload,export a exe for you and generate a listener.You need to transfer the exe on to the victim machine and execute it in order for it to properly work.

E.Mass Mailer Attack:

The mass mailer attack will allow you to send multiple emails to victim and customize the messages. This option does not allow to create payloads, so it generally used to perform a mass phishing attack.

F. Arduino-Based Attack Vector:

The Arduino-Based Attack Vector utilizes the Arduin-based device to program the device. You can leverage the Teensy's, which have onboard storage and can allow for remote code execution on thephysical system. Since the devices are registered as USB Keyboard's it will bypass any autorun disabled or endpoint protection on the system.

G. SMS Spoofing Attack Vector:

The SMS module allows you to specially craft SMS messages and send them to a person. You can spoof the SMS source.

H. Wireless Access Point Attack Vector:

The Wireless Attack module will create an access point leveraging your wireless card and redirect all DNS queries to you. The concept is fairly simple, SET will create a wireless access point, dhcp server, and spoof DNS to redirect traffic to the attacker machine. It will then exit out of that menu with everything running as a child process.

I.ORcode Generator Attack Vedio:

The QRCode Attack Vector will create a QRCode for you with whatever URL you want. When you have the QRCode Generated, select an additional attack vector within SET and deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet and send the QRCode via a mailer.

J. Powershell Attack Vector:

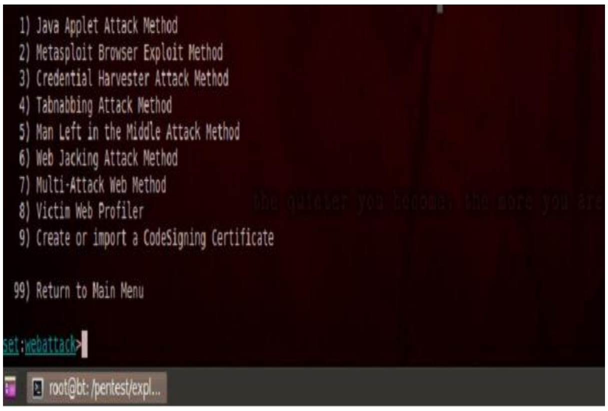
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.

K. Third Party Modules:

This attack vector consists of Third party module-RATTE(Remote Administration Tool Tommy Edition)which is a HTTP tunneling payload .This can be used in the same way as website attack vectors but with an added advantage of beating security mechanisms like local firewall and IPS.

3.2 Website Attack Vectors:

Now, in order to conceive or conspire the username and password details in social networks ,the attackers usually opt the second option which is Website Attack Vectors. After choosing option 2 in the terminal the following set of options is displayed as below:



```
 1) Java Applet Attack Method
 2) Metasploit Browser Exploit Method
 3) Credential Harvester Attack Method
 4) Tabnabbing Attack Method
 5) Man Left in the Middle Attack Method
 6) Web Jacking Attack Method
 7) Multi-Attack Web Method
 8) Victim Web Profiler
 9) Create or import a CodeSigning Certificate

99) Return to Main Menu

set:webattack>
```

the quieter you become, the more you are
root@bt: /pentest/expl...

Fig:3

The displayed options can be described as follows:

a. Java Applet Attack Meathod:

The Java Applet Attack considers as one of the most successful and popular methods for compromising a system.Popular because we can create the infected Java applet very easily,we can clone any site we want that will load the applet very fast and successful because it affects all the platforms

b. Metasploit Browser Exploit Method:

Metaspoit Framework is a open source penetration tool used for developing and executing exploit code against a remote target machine it, Metasploit frame work has the world's largest database of public, tested exploits. In simple words, Metasploit can be used to test the Vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems[3].The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

c. Credential Harvester attack Method:

The credential harvester attack method is used when you don't want to specifically get a shell but perform phishing attacks in order to obtain username and passwords from the system. In this attack vector, a website will be cloned, and when the victim enters in the user credentials, the usernames and passwords will be posted back to your machine and then the victim will be redirected back to the legitimate site.

d. Tabnabbing Attack Meathod:

Tabnabbing is a computer exploit and phishing attack, which persuades users to submit their login details and passwords to popular websites by impersonating those sites and convincing the user that the site is genuine. The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

e. The Man Left in the Middle Attack method:

The man left in the middle attack utilizes HTTP REFERERS on an already compromised site or XSS vulnerability to pass the credentials back to the HTTP server. In this instance if you find a XSS vulnerability and send the URL to the victim and they click, the website will operate 100 percent however when they go to log into the system, it will pass the credentials back to the attacker and harvest the credentials[4].

f. Web jacking Method:

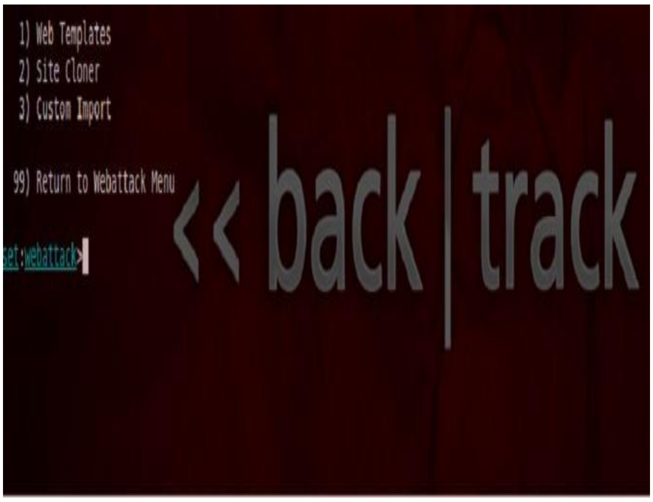
The Web Jacking Attack Vector is another phishing technique that can be used in social engineering engagements. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another link.If the victim clicks the link that looks real he will redirected to a fake page.

g. Multi - Attack Web Method:

The multi-attack web vector is new and will allow you to specify multiple web attack methods in order to perform a single attack. In some scenarios, the Java Applet may fail however an internet explorer exploit would be successful. Or maybe the Java Applet and the Internet Explorer exploit fail and the credential harvester is successful. The multi-attack vector allows you to turn on and off different vectors and combine the attacks all into one specific webpage. So when the user clicks the link he will be targeted by each of the attack vectors you specify. One thing to note with the attack vector is you can't utilize Tabnabbing, Cred Harvester, or Web Jacking with the Man Left in the Middle attack. Based on the attack vectors they shouldn't be combined anyways. In the scenario of Multi –Attack web method, we are going to turn on the Java Applet attack, Metasploit Client-Side exploit, and the Web Jacking attack. When the victim browses the site, he/she will need to click on the link and will be bombarded with credential harvester, Metasploit exploits, and the java applet attack.

3.3 Tabnabbing nethod:

If the Network Intruder uses the Tabnabbinng method,the following set of options will be displayed:



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

99) Return to Webattack Menu

set:webattack>
```

Fig:4

*** Web Templates:**

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

***Site Cloner:**

This 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**.**

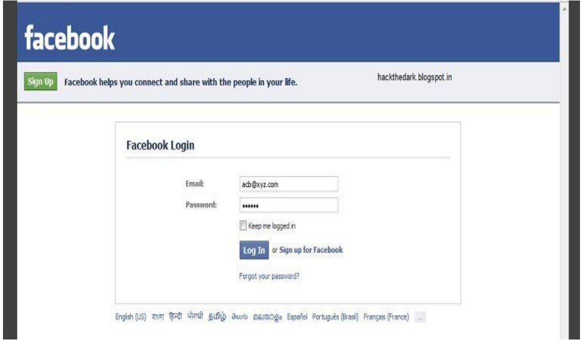
***Custom Import:**

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

Now,undoubtdedly the Network Intruder will opt the Site Cloner .So, that it will ask the IP address for the post back in Harverster/Tabnabbing.After that it'll ask you to Enter the url to clone. Here, I'm using www.facebook.com for demonstration but you can use the url of gmail or yahoo or whatever you want. After writing the URL hit Enter.

When its done with cloning again press Enter. Don't close this terminal because it'll display the password later. Now our site clone is ready all you need to do is to send its link to the victim who's account you want to hack. The IP address of the Backtrack will be treated as the address of the clone site.

So grab the IP address of Backtrack. Open a new terminal and shoot the command ifconfig and get its IP address. It'll look something like inet addr: 192.168.1.4. Now, send your IP address directly to the victim or you can spoof it by shrinking the url using many online services like adf.ly or goo.gl or any similar one. Send the generated link to the Victim via chat or Email or by any means.When the user click on the link, it'll redirect to the facebooks cloned login page.



Facebook helps you connect and share with the people in your life.

hackthedark.blogspot.in

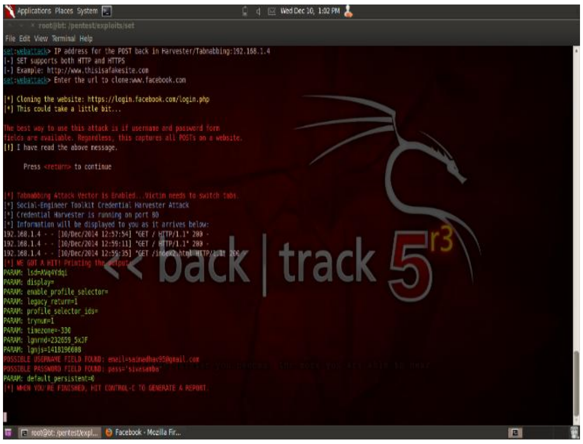
Facebook Login

Email: acb@xyz.com
Password: ••••••
☐ Keep me logged in

facebook
Sign Up
Log In
or Sign up for Facebook
Forgot your password?
English (US) বাংলা हिन्दी ਪੰਜਾਬੀ தமிழ் తెలుగు മലയാളം Español Português (Brasil) Français (France) ...

Fig:5

Now after the filling of username and password it will displayed on the terminal of the Network Inruder.So,it will be displayed as below



Applications Places System
Wed Dec 10, 1:02 PM
root@bt: /pentest/exploits/set
File Edit View Terminal Help

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.4
[-] 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.
[!] I have read the above message.

    Press <return> to continue


[*] Tabnabbing Attack Vector is Enabled...Victim needs to switch tabs.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.4 - - [10/Dec/2014 12:57:54] "GET / HTTP/1.1" 200 -
192.168.1.4 - - [10/Dec/2014 12:59:11] "GET / HTTP/1.1" 200 -
192.168.1.4 - - [10/Dec/2014 12:59:35] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVq4Ydqi
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgnrnd=232659_5xJF
PARAM: lgnjs=1418196608
POSSIBLE USERNAME FIELD FOUND: email=sainadhav95@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass='sivasamba'
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fig:6

IV.CONCLUSION:

The versatility of Backtrack operating system is always known and has always been proved by many network professionals.And so Backtrack is considered as a comprehensive toolkit for security auditing but the actual thing is Backtrack operating system is also exceptionally good in its inbuilt Forensic capabilities. Backtrack5r3 operating system has a stupendous structure as it has humongous number of tools ,on using which we get prolific results.

REFERENCES:

[1]. https://www.trustedsec.com/social-engineer-toolkit/

[2]. http://www.webroot.com/in/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering
[3]. http://www.webopedia.com/TERM/M/Metasploit.html
[4]. http://theonemarch.wordpress.com/2011/11/14/man-left-in-the-middle-attack-method/