Social Engineering Toolkit - A Systematic Approach To Social Engineering

Nikola Pavković, Luka Perkov
Ruđer Bošković Institute
Bijenička cesta 54, 10000 Zagreb, Croatia
E-mail: nikola.pavkovic@irb.hr, luka.perkov@irb.hr

***Abstract*—Social engineering techniques, exploiting humans as information systems' security weakest link, are mostly the initial attack vectors within larger intrusions and information system compromises. In order to practically evaluate the risks of information leakage trough the target organizations' employees, when performing a penetration test, an ethical hacker must consider social engineering as a very important aspect of the performed test.**

Social Engineering Toolkit (SET) is an integrated set of tools designed specifically to perform advanced attacks against the human element, and is the most advanced, if not the only toolkit of such kind that is publicly available as open source software. Incorporating many social engineering attack vectors, it heavily depends on Metasploit, an integrated penetration testing framework.

This paper gives a brief introduction to the Social Engineering Toolkit software architecture, and provides an overview of supported attack vectors.

I. Introduction

Security, as one of the most important criteria for information system quality assessment, depends on many technical and non-technical factors. Contrary to popular belief that vulnerabilities in information systems are mostly contained in software, actually it's the human factor that poses the most significant security risk. [1]

Social engineering represents the art of exploiting humans' characteristics in order to elicit information, valuable in further stages of system penetration. Since the first stage of penetrating the target organization's security perimeter is usually done through attacker's interaction with organization's staff, penetration testing that involves methods of social engineering becomes extremely important when evaluating an organization's information system security.

II. Penetration testing through SE

In order to penetrate the perimeter of a company's information system, an attacker is likely to begin with collecting valuable information about the target company, it's information system architecture, security countermeasures etc. The vast resource of such highly valuable information are the employees of the target company who often pose an easy target for an experienced social engineering practitioner. Very few surveys regarding SE have been publicized, one of which, [2] implies that when employees do not have clear guidelines set in place in response to a given situation, they will default to actions that they perceive as being helpful, passing confidential information to the attacker conducting SE attacks.

III. State of the art

When conducting a SE attack, the attacker's best tools are actually his own skill in human-to-human communication, understanding of human behavioural characteristics and knowledge how to exploit them. However, in order to ease the process of eliciting information from the victim, specialized SE oriented software tools are of great value. Up to date, the only publicly available software product in SE domain, within the open source community, is the Social Engineering Toolkit which is described in following sections.

IV. SET software overview

SET is a software package, specially designed to perform social engineering (SE) attacks [3], i.e. attacks against the human element, and is the most complete and most advanced SE toolkit available as open source software. Author David Kennedy released the SET software package[1] under the GNU GPL license[2] which provided the public with the ability to join the development of it's core components. This resulted in a very dynamic development process and release of new functionalities almost on a daily basis.

The main feature of SET is the ability to launch technically sophisticated social engineering attacks while providing the attacker with a simple, menu driven user interface. For launching particular attacks, SET heavily depends on the Metasploit framework[3] which provides means of payload generation and listener setup.

A. Software dependencies

SET software is written in Python programming language. Although SET should work on a variety of operating systems, the natural execution environment is Linux OS for it's openness and flexibility. Software dependencies that SET relies on are shown as follows:

- Metasploit framework
  - used for payload generation and listener setup.
- Java Development Kit

[1] http://www.secmaniac.com/download/
[2] http://www.gnu.org/licenses/gpl.html
[3] http://www.metasploit.com/

  - used for Java-based payload generation
  - OpenJDK[4] or commercial version applicable
- Ettercap[5]
  - used for launching a DNS spoofing attack if the attacker already resides within the victim's network
- Sendmail (or other MTA)
  - used for spoofing sender's E-mail address
- Apache web server[6]
  - not a necessity but, compared to the built-in web-server, improves performance of some attack vectors

B. Configuration file

Configuration parameters of SET are contained in the main configuration file located at `config/set_config` within the directory of SET installation. The configuration parameters are defined as variable definitions:

`VARIABLE="value"`

Some of the configuration variables with corresponding explanations are shown as follows:

METASPLOIT_PATH - path to Metasploit framework installation

ETTERCAP - enable/disable usage of Ettercap tool for DNS spoofing

ETTERCAP_PATH - path to Ettercap installation

SENDMAIL - enable/disable usage of local Sendmail installation

JAVA_SIGNED_APPLET - enable/disable self-signing of Java applets which enables forging the the Applet author

JAVA_ID_PARAM - message to be shown within the Java applet execution info-dialog

JAVA_REPEATER - enable/disable repeating the dialog for approving the Java applet execution

WEB_PORT - TCP listening port for internal web-server

CUSTOM_EXE - executable file to which the Metasploit payload is to be merged

APACHE_SERVER - enable/disable usage of local Apache installation

APACHE_DIRECTORY - path to the DocumentRoot directory of local Apache installation

WEBATTACK_SSL - enable/disable usage of SSL while performing web-based attacks

SELF_SIGNED_CERT - enable/disable usage of a self-signed SSL certificate

COMMAND_CENTER_PORT - TCP listening port on which the SET web-interface is to be run

COMMAND_CENTER_INTERFACE - IP address on which the SET web-interface is to be run

AUTO_MIGRATE - enable/disable automatic payload migration after successful exploitation

AUTO_REDIRECT - enable/disable automatic redirection to authentic web-site once the credentials have been captured using the Credential harvester method

[4]http://openjdk.java.net/

[5]http://ettercap.sourceforge.net/

[6]http://apache.org/

C. User interface

The textual user interface consists of a system of multi-level menus which are shown within the terminal window where the tool is being run. A typical example is shown in fig. 1.

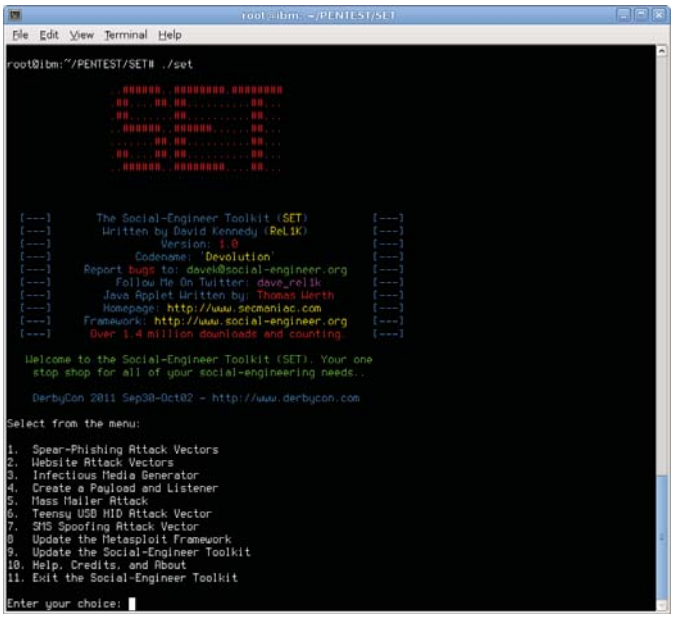

Fig. 1. SET textual user interface

After the attack vector has been chosen, the system of menus guides the attacker through various configuration options of particular attack. Eventually, the attacker is given the choice of different payloads to deliver to the victim.

SET also provides a web-based user interface which is run at the TCP port defined in the `COMMAND_CENTER_PORT` variable within the configuration file. A typical example is shown in fig. 2.

Fig. 2. SET web user interface

V. Attack vectors

SET provides different attack vectors which are used to deliver a victim the payload that is chosen and configured in the attack configuration process. Once the exploitation is successfully finished and the payload is delivered to the victim's computer, a connection to the attacker's computer is being established. This provides the possibility for the attacker to perform various actions on the victim's computer.

A. E-mail based attack vectors

E-mail is the most used communication system on the Internet. [5] Choosing the right subject, sender address and content of an E-mail message, an attacker can easily deceive the victim into believing that the message originates from a valid source. In such circumstances, victim is likely to open the attached file which holds the malicious payload that is to be executed. SET provides means to generate such E-mail messages, to generate and attach the payload and eventually, start a listener on the attacker's computer to which the exploited system will try to establish connection.

B. Web based attack vectors

1) Java applet attack: This kind of attack provides the possibility to setup a fake web-interface on the local web server. The web-interface, although looking authentic, asks the victim to run a malicious Java applet. If the victim accepts it's execution, the previously configured payload is being delivered and executed. For the purpose of setting up a fake web-interface, SET provides various templates for popular web sites (Gmail and others), but also provides the possibility to clone an existing web site or use an externally prepared template.

2) Metasploit browser exploit: As in the previous case, a fake web-interface is being started on the local web server, but in this case SET will try different exploits available for popular web browsers. Besides the fake web-interface a hidden iframe containing malicious code is being created. If the victim's browser has one of the vulnerabilities unpatched, control over his computer is being established.

3) Credential harvester method: This kind of attack is not aimed at taking control over the victim's computer. Instead, through a fake web-interface, it captures victim's credentials when trying to authenticate. If any of the POST variables have been captured, SET will display them in the console window.

4) TabNabbing method: This method is effective when the victim has several tabs open in the web browser. As the victim clicks on the link leading to the fake web-interface, a "Please wait while the site loads..." message is displayed. Meanwhile, waiting for the site to load, the victim will probably switch to another tab and at that moment the fake web-interface is loaded to the, now inactive, tab. After some time, when the victim reopens the tab containing the fake web-interface, it will show the default login window, misleading the victim to believe that the authentication has been timed-out. When the victim enters the login credentials, SET captures them and displays them in the console window while redirecting the victim to the authentic web-interface.

5) Man left in the middle: 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 a URL containing the XSS vulnerability is sent to the victim and when the victim clicks on it, the web site will operate 100 percent however when the victim goes to log into the system, SET will pass the credentials back to the attacker and harvest the credentials.

6) Web jacking method: Web jacking uses the Credential harvester method to capture victim's login credentials, but instead of providing a fake web-interface, it presents the victim a link stating that the web site has moved. When the victim hovers over the link, a valid URL will be shown, not the actual URL pointing to the attacker's computer. When the victim, believing it is a valid link pointing to the authentic web-interface, clicks on it, the attacker's malicious site is being opened.

7) Multi-attack: Multi-attack method combines all of the above referenced web based attack vectors. For example, in some cases the Java applet method might not be successful while the Metasploit browser attack might succeed. SET provides means to enable or disable particular attack vectors and to setup a fake web-interface which contains all of the chosen attacks. This way, the attacker raises the probability for the attack to be successful in only one step.

C. Malicious media generator

Delivering the payload to the victim's computer can be done using a physical media, i.e. a CD/DVD media or a USB memory device. The attacker labels the media and leaves it where the victim can find it. As the victim finds the media and tries to explore it's contents by inserting it into his computer, the payload is run for example through the Autorun system in Windows OS. This attack vector exploits curiosity as a general characteristic of humans. [4]

D. Creating payload and listener

In some scenarios, the attacker wants to deliver the payload by other methods than described above. SET provides means to simply create the payload and the corresponding listener to which the payload will connect once run. This method actually represents a simple wrapper around the Metasploit framework.

E. Teensy USB HID Attack Vector

HID *(Human Interface Device)* devices are used for direct interaction of the computer system with the user. Examples for such devices are the computer mouse or the keyboard. Specially designed device called "Teensy"[7], when connected to the USB port of a computer, is recognized as keyboard, thus providing means to emulate real user's usage of the keyboard. As such, it enables automation of various tasks aiming at compromising the target computer system, for example by downloading and executing a malicious executable or opening a malicious web page within the browser. SET provides the

[7] http://www.pjrc.com/teensy/

functionality to configure the Teensy device by preparing the `.pde` file that is to be uploaded to the device. Contrary to the other attack vectors, this attack would be successful in case where automatic running of `autorun.inf` file is disabled on the victim's computer.

F. Example SET usage – Credential harvester

In this section an example attack walkthrough is shown. Attacker goal is to collect login information of specific web page, in this example `gmail.com`. After starting SET following is displayed:

```
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.  Teensy USB HID Attack Vector
7.  SMS Spoofing Attack Vector
8   Update the Metasploit Framework
9.  Update the Social-Engineer Toolkit
10. Help, Credits, and About
11. Exit the Social-Engineer Toolkit

Enter your choice: 2
```

In the next step *credential harvester* method is chosen.

```
1. The Java Applet Attack Method
2. The 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. Return to the previous menu

Enter your choice (enter for default): 3
```

In the next section attacker can choose to use existing web page template, clone a web site or import custom template in order to continue with attack.

```
1. Web Templates
2. Site Cloner
3. Custom Import
4. Return to main menu

Enter number (1-4): 2
```

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

```
Email 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.

SET supports both HTTP and HTTPS
Example: http://www.thisisafakesite.com
Enter the url to clone: www.gmail.com
```

After attacker submits all requested parameter attack platform is launched.

```
[*] Cloning the website: www.gmail.com
[*] 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.

[*] SET Credential Harvester Attack
[*] Credential Harvester is
    running on port 80
[*] Information will be displayed
    to you as it arrives below:
```

After the credentials have been entered attacker can see it in the console.

```
[*] Information will be displayed
    to you as it arrives below:
[*] WE GOT A HIT! Printing the output:
PARAM: ltmpl=default
PARAM: ltmplcache=2
PARAM: continue=http://google.com/mail/?
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=-3099857175512610860
PARAM: ltmpl=default
PARAM: ltmpl=default
PARAM: scc=1
PARAM: timeStmp=
PARAM: secTok=
PARAM: GALX=AHbFmLnJf3I
POSSIBLE USERNAME FOUND: Email=john.doe
POSSIBLE PASSWORD FOUND: Passwd=123456
PARAM: rmShown=1
PARAM: signIn=Sign+in
PARAM: asts=
[*] WHEN YOUR FINISHED.
    HIT CONTROL-C TO GENERATE A REPORT
```

As shown an attacker can easily get correct victims credentials. Upon successful capture victim is redirected to authentic site.

VI. Conclusion

Information security of an organization depends on various factors, one of which is appropriate consciousness and education of it's staff. As humans are often the weakest link in the security chain, penetration testing involving social engineering

methods is one of the most important categories in evaluation of information security. Social Engineering Toolkit represents a very important tool for such evaluation because it provides to the penetration tester a convenient, easy to use set of tools aimed at exploiting the human element.

Important characteristic of SET is it's openness of the source code, which enables the broad security research community to join the development force, providing the rapid growth of SET's functionalities. SET's tight dependence on the Metasploit framework, also a very rapidly developing system for penetration testing, provides a solid base for creating new advanced attack vectors.

REFERENCES

[1] R Gulati, *The Threat of Social Engineering and Your Defense Against It*, SANS InfoSec reading room, SANS Institute, 2003.

[2] C. J. Hadnagy, M. Aharoni, J. O'Gorman, *Social Engineering Capture the Flag Results*, DEFCON 18

[3] *http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_(SET)*

[4] F. Stajano and P. Wilson, *Understanding scam victims: seven principles for systems security*, Cambridge, 2009.

[5] S. Radicati, *Email statistics report, 2010*, The Radicati Group, Inc, Palo Alto, 2010.