Social Engineering Toolkit

Author: 3psil0nLaMbDa a.k.a Karthik R, INDIA

http://www.epsilonlambda.wordpress.com

The social engineering toolkit is a project named **Devolution,** and it comes with Backtrack as a framework used for penetration testing. This framework has been written by David Kennedy nick named as ReL1k. For more information about Social Engineering Toolkit (SET), please visit the official page at http://www.social-engineer.org

Why am I writing on this framework?

Usually in a Pen-Testing scenario, alongside finding of vulnerabilities in the hardware and software systems, and exploiting them, the most effective of all is penetrating the Human mind and get all information needed first hand. This is the secret art called Social Engineering. The computer based software codes and tools that facilitate this using a computer system is called as SET.

What can you expect from this article?

Well, this article covers on backdooring executables, and also evade antivirus that is implicitly taken care by few scripts in this framework. We shall also touch upon on a scenario in pen testing where we see if the employees of the organization are well aware of the security threats they face by the art of Social engineering.

Introduction

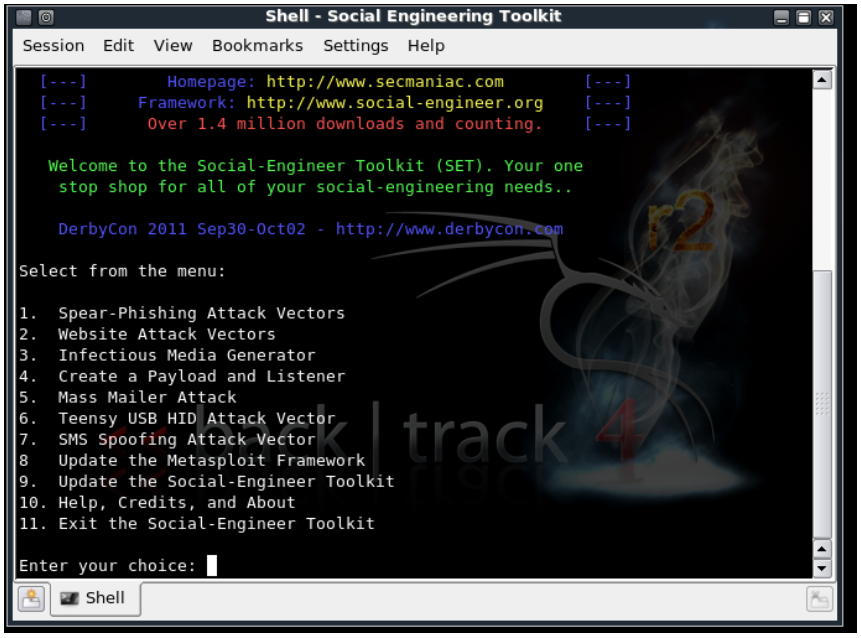

Figure1 – This is the opening menu of the SET framework.

We shall cover the spear phishing attack vectors and Website Attack Vectors in detail in this article.

As the term suggests, spear is defined as "a weapon consisting of metal point attached to the end."

Phishing is defined as a crackers way to fool the individual in believing that what he is seeing is true, by creating fake contents on the web.

Spearphishing is a special type of an attack where you target a particular victim and not the mass, analogous to the spear which can be used to attack only one person at any given point of time. Let's move on with this attack using SET.

On choosing 1 in the menu, we get another menu, where I shall be choosing 1, which is perform a mass mailer attack. This attack send an email to the victim with a content that we want to deliver.

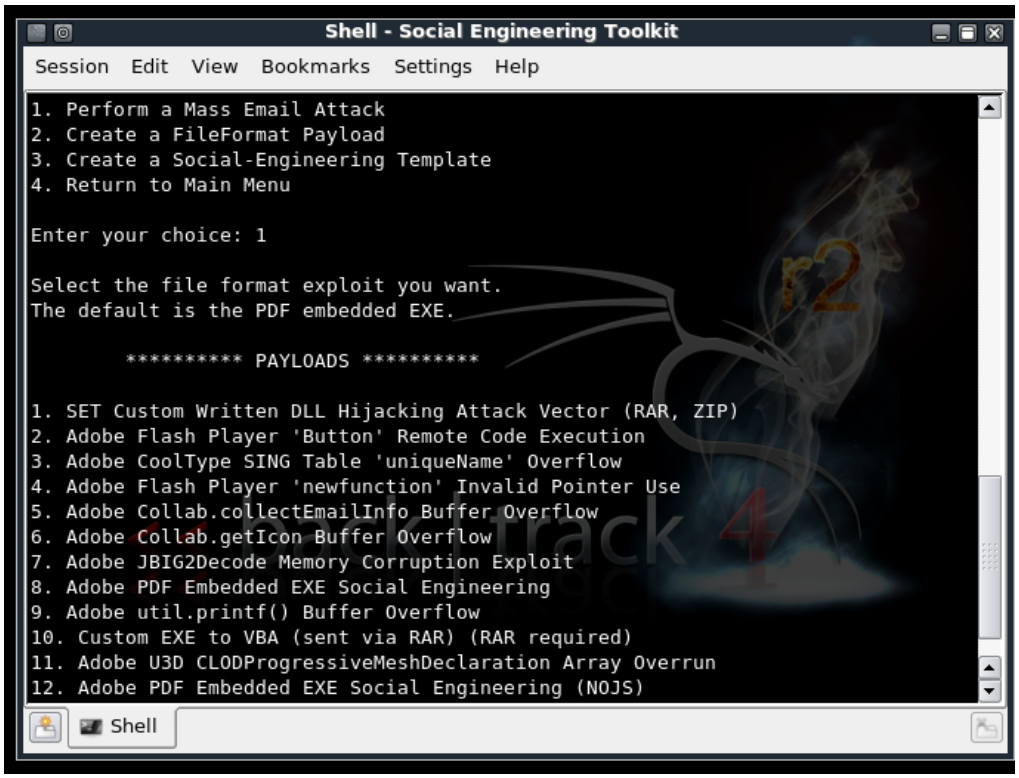

Figure2: different payloads available for the mass mailer attack.

I choose option 10, which tells, Custom exe to vba (sent via RAR). This tells that we would be sending the victim a Backdoored rar file.

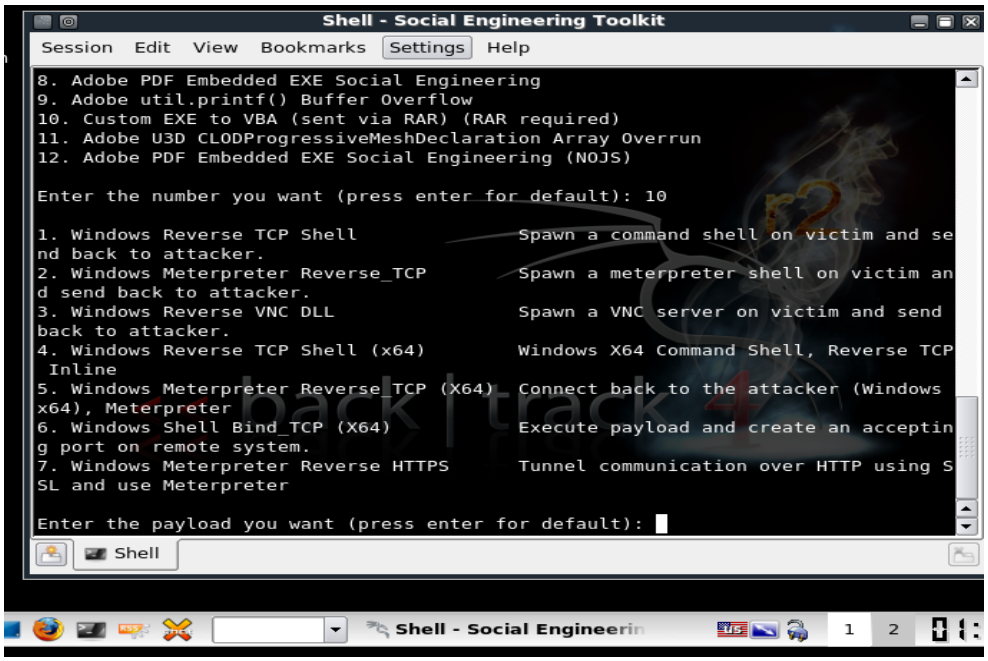

Figure 3: This shows the different payload options available and we can also observe how SET uses the support from metasploit's meterpreter extension, in pwning a shell and then controlling it in remote system.

Once you choose the pay load to send to the victim, it will ask for the victim's email id. And it ll also ask you to provide a valid gmail account and login to it, so that the mail is sent via this gmail account. There is a provision for using your own SMTP server for emails also. The choice is left to the individual as to how he would like to perform this attack.

There are ready made templates to choose from. Figure 4shows the templates available to be sent in the form of a mail. There is always an option of creating your own template for the attack and save it for future use. Creating your own template has its own advantage, that is, it ll evade the spam filters and manage to reach to the inbox of the victim where he feels that the mail is from a legitimate source.

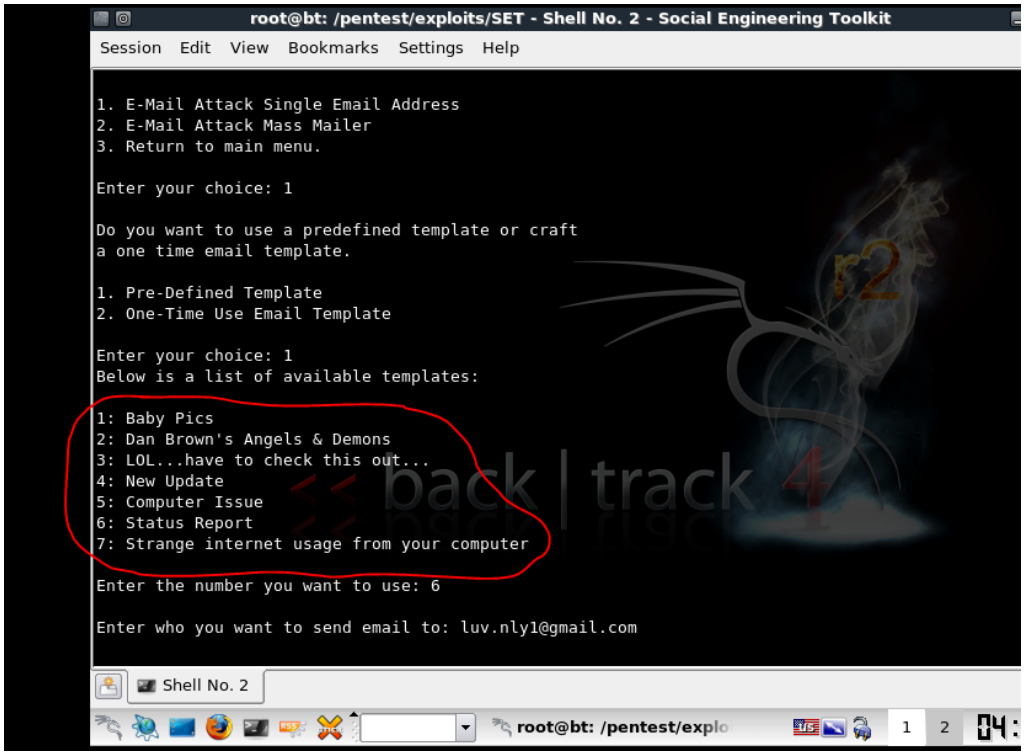

Figure4; SET Templates, which may or may not evade spam filters. But using a custom template always had higher chances of evading spam.

Website Attack Vectors:

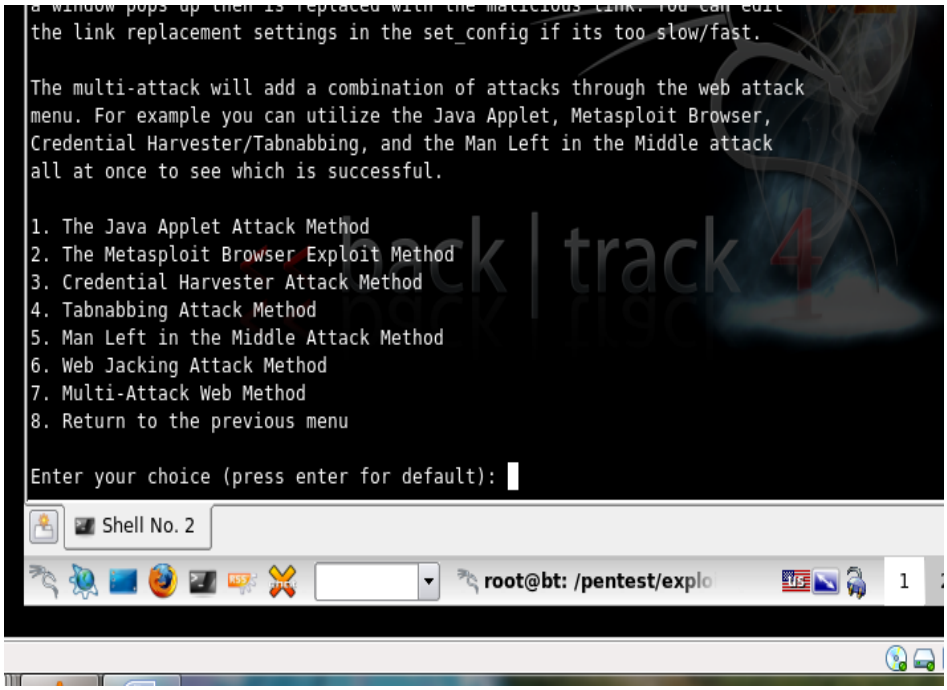

Figure5: List of options available for website attack vectors. We shall be seeing the JAVA applet method in detail.

The tabnabbing attack method is the one in which you can clone the entire website and harvest the keystrokes on that webpage on the fake server hosted by SET. Usually happens when the user changes his tabs, he sees the login page and falls prey to the attack by giving out his actual details, to the attacker without his knowledge. Other attacks like metasploit browser exploit method exploits the browser vulnerabilities and pwns a meterpreter shell in the victim machine there by giving complete access to the system. Credential harvester method as the name suggests helps in stealing the credentials of the victim.

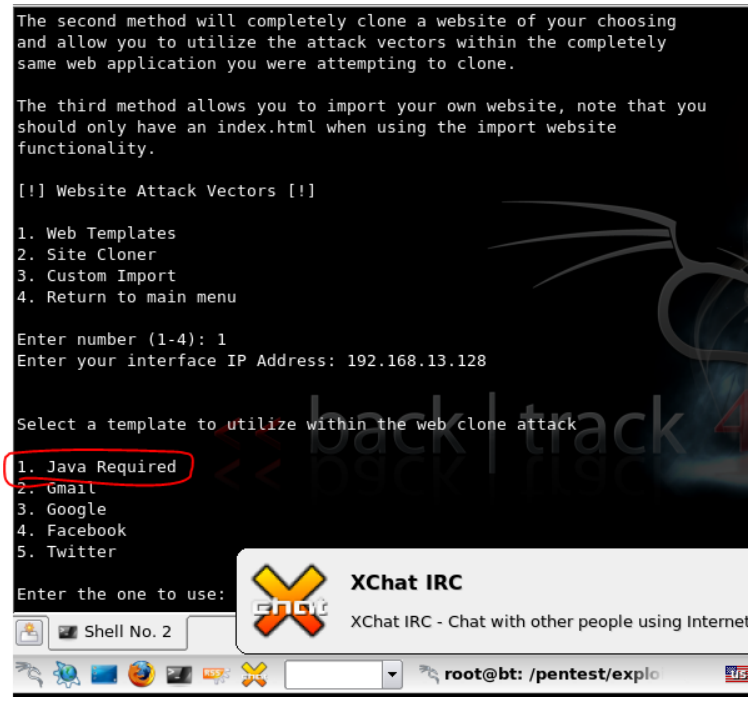

Figure6: Shows the Java applet options available under webtemplates.

We choose the template that asks the user for a JAVA plugin required. In the subsequent menus, we choose the backdoored executable **shikata_ga_nai**. Its rated very good, because it evades anti-virus effectively, and it's quite powerful in pawning a meterpreter shell in the victim.

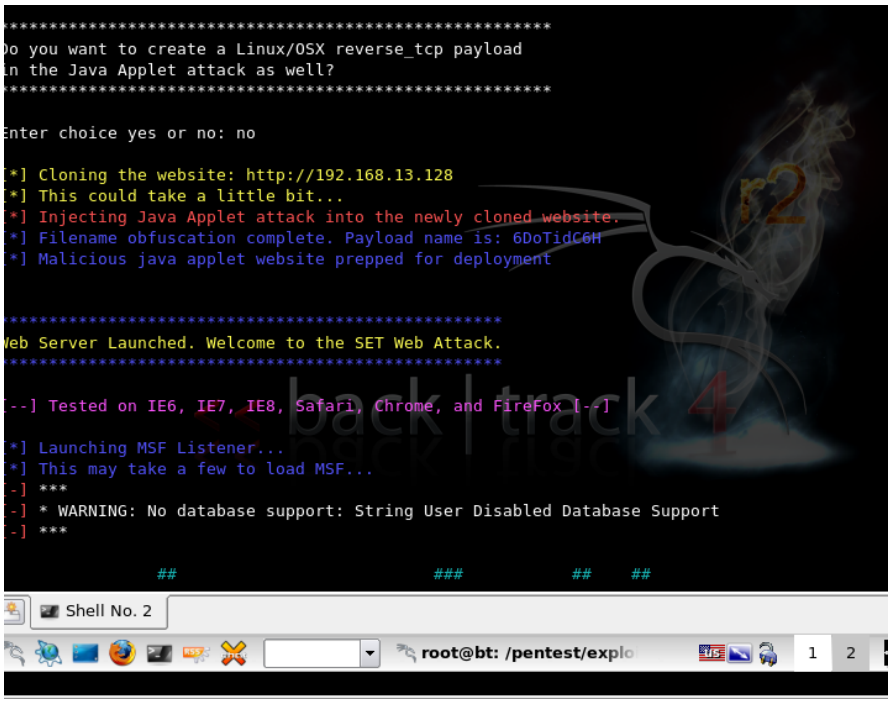

Figure7: This shows the web attack vector being cloned at IP 192.168.13.128. And it also tells us that this attack works successfully and is tested on IE6, IE7, Safari and Firefox. Again we see an influence of Metasploit in this toolkit, in pwning the victim.

Figure8 shows the pop-up window in the browser, when the URL browsed is http://192.168.13.128

This can be used to test the awareness of the employees within the organization during the Pen-test phase, to social engineering threats.

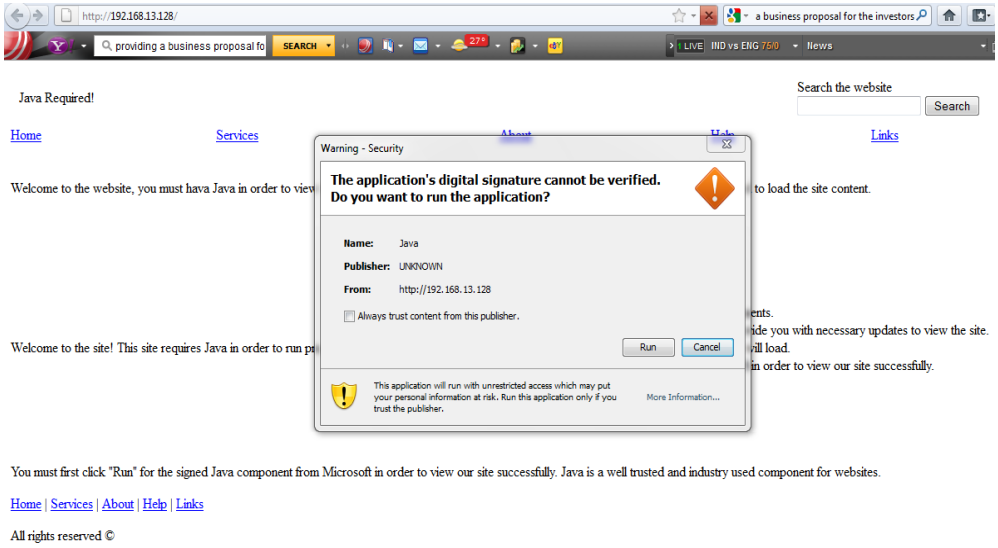

Figure8: the following pop-up tells the user to install a JAVA Applet but, when the user clicks OK, a meterpreter shell is pwned in the system giving access to the attacker over the victims machine.

This covers a brief about Social Engineer's Toolkit. In subsequent articles different forms of attacks shall be covered in future. If the readers have any requests on a particular topic or an attack to be covered, feel free to contact me, anytime.