

Forum:[Hack Forums](#)

Thread: [\[EASY TUTORIAL\] SET Social Engineering Toolkit Tutorial \[PART 1\]](#)

slober - December 31, 2011, 11:59 am

SET Social Engineering Toolkit Tutorial

Introduction

Requirement

Explanation [SET]

Useful links

Outro

Sources

1. Introduction

first the definition of social engineering From wikipedia.org

Social engineering is commonly understood to mean the art of manipulating people into performing actions or divulging confidential information.

While it is similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.

"Social engineering" as an act of psychological manipulation was popularized by hacker-turned-consultant Kevin Mitnick. The term had previously been associated with the social sciences, but its usage has caught on among computer professionals.

ok and SET??? ?

set is an tool that can help you performing an SE attack

i will explain ho you can fake a web page like Facebook, gmail,...

if you combine SET with a wifi-hack or with an DNS-spoof or..

ok let's go on to the next part ?

2. Requirement

Some SE knowledge

Backtrack5 or

ettercap

SET

Virtualbox (if you're on a windiws machine)

3. Explanation

ok SET is really easy to use so let's start.

start backtrack and go to SET

Applications -> Backtrack -> Exploitation tools ->

Social engineering Tools -> SET

[IMG]<http://img651.imageshack.us/img651/8066/18540368.png>[/IMG]

then press 2 or chose a different attack 2 is for websites =)

[IMG]<http://img198.imageshack.us/img198/9053/46201498.png>[/IMG]

we are almost done now you can chose a more detailed attack do you want a backdoor or just a fake gmail, facebook,.... site? i pressed 3 =)

[IMG]<http://img845.imageshack.us/img845/9092/49319321.png>[/IMG]

now you can chose to copy a login (paypal, game,....) or you can use the themes pre-difined by SET

i taked 1 and the theme of gmail

[IMG]<http://img28.imageshack.us/img28/4429/27009126.png>[/IMG]

[IMG]<http://img534.imageshack.us/img534/3230/82708879.png>[/IMG]

now it's done ? you can dns-spoof your target or use some other attack the lure him when the pass is entered you can view it trough set

[IMG]<http://img585.imageshack.us/img585/1408/98994285.png>[/IMG]

[IMG]<http://img39.imageshack.us/img39/6619/75474149.png>[/IMG]

[IMG]<http://img24.imageshack.us/img24/5704/65135144.png>[/IMG]

Notice.

You learn more by trying yourself

4. Useful Links

<http://www.youtube.com/watch?v=---X87jRK7o> [Video]

[http://en.wikipedia.org/wiki/Social_engineering_\(security\)](http://en.wikipedia.org/wiki/Social_engineering_(security))

<http://www.backtrack-linux.org/>

<http://shadeshroud.be> [my site with some other tutorial]

<https://hackforums.net/showthread.php?tid=1402415> [DNS spoofing]

5. Outro

ok this was my tutorial i hate outro's XD
please comment =)

ow if i missed something spelled something wrong just say i'm quite new to English tutorials ;)

6. Sources<http://www.social-engineer.org/>

[http://en.wikipedia.org/wiki/Social_engineering_\(security\)](http://en.wikipedia.org/wiki/Social_engineering_(security))

Interesting tutorial you have here.

Reading is a pleasure ;)

I33t10n9 - December 31, 2011, 1:00 pm

Nice tut here, great and HQ post
3535355353535

slober - January 1, 2012, 4:12 am

Thx,
trying to make a series of this next is set and metasploit =)

bernardbear - January 1, 2012, 9:20 am

thanks for sharing bro, but may you help me pivoting internet cafe client pc ?
i already backdoored 1 pc :D but armitage + metasploit still cant exploit it. OS is sp2 ! lol
if yes may you pm me with your msn or ym ?

BeggFoMercy - January 1, 2012, 9:36 am

Great TUT it seems awesome ill try it
just when i kno what is back track :D

slober - January 1, 2012, 1:00 pm

(Jan 1, 2012 10:36 AM)BeggFoMercy Wrote: [\[CITE\]](#) Great TUT it seems awesome ill try it
just when i kno what is back track :D backtrack is an "hacking os" you can download it from there
official website if you need an tutorial on how to install it i will soon post one here =) just keep
watching for a few days ;)

(Jan 1, 2012 10:20 AM)bernardbear Wrote: [\[CITE\]](#) thanks for sharing bro, but may you help me
pivoting internet cafe client pc ?
i already backdoored 1 pc :D but armitage + metasploit still cant exploit it. OS is sp2 ! lol
if yes may you pm me with your msn or ym ?
use an dns spoofing attack and a java drive by =) or the java applet in SET 100% working =) [not
elegant but working =)]

you can ad me just sent me pm (don't give it here or i get spammed lol)

BeggFoMercy - January 1, 2012, 2:07 pm

(Jan 1, 2012 02:00 PM)slober Wrote: [\[CITE\]](#) backtrack is an "hacking os" you can download it from
there official website if you need an tutorial on how to install it i will soon post one here =) just keep
watching for a few days ;)

use an dns spoofing attack and a java drive by =) or the java applet in SET 100% working =) [not
elegant but working =)]

you can ad me just sent me pm (don't give it here or i get spammed lol)

Well alright ill be waiting for that so do i have to burn it on a CD etc? and setup like a new OS ?
and i need a list of commands that will help me doing things with that OS

bernardbear - January 2, 2012, 11:26 am

thanks for pm guys, i will be waiting for you online ?

Fr0st_Byte - January 2, 2012, 5:15 pm

This is a lot like my tutorial I wrote last year. The one in my sig.
Good job.

haris013 - January 6, 2012, 1:58 pm

hi guys! I wanted to ask if someone can help me to build a phishing site for fun :P
i need more details and tips, if someone can help me plz pm me. i have already read this tut and i have some previous experiences with backtrack but i am still a noob :D

slober - January 6, 2012, 4:55 pm

(Jan 6, 2012 02:58 PM)haris013 Wrote: [\[CITE\]](#) hi guys! I wanted to ask if someone can help me to build a phishing site for fun :P
i need more details and tips, if someone can help me plz pm me. i have already read this tut and i have some previous experiences with backtrack but i am still a noob :D
making a phishing site is not that hard i made a tutorial on how to do it on my website:
<http://shadeshroud.be/moderate-tutorials-phishing/>
the problem with SET and backtrack is that the tools are primarily used for local purposes so i suggest you take a look to this =)

wellager - January 6, 2012, 6:05 pm

Good job & thanks for your hard work.

haris013 - January 7, 2012, 2:20 am

(Jan 6, 2012 05:55 PM)slober Wrote: [\[CITE\]](#) making a phishing site is not that hard i made a tutorial on how to do it on my website: <http://shadeshroud.be/moderate-tutorials-phishing/>
the problem with SET and backtrack is that the tools are primarily used for local purposes so i suggest you take a look to this =)
thx :D
so if backtrack and set are for local area network can i do something to a public hotspot or a cracked wireless network?

slober - January 7, 2012, 6:40 am

(Jan 7, 2012 03:20 AM)haris013 Wrote: [\[CITE\]](#) thx :D
so if backtrack and set are for local area network can i do something to a public hotspot or a cracked wireless network?
yes if you are on some free wifi then you can dns-spoof all of the persons on it and if they surf to facebook, gmail, paypal yahoo,.... you can hack (phish, hack based on your settings with set) them with set

Adolf Hipster - January 7, 2012, 7:03 am

Thanks for this.

Going to see if I can put this into action.

haris013 - January 7, 2012, 2:02 pm

so guys r any other tuts or some books with more details about various attacks, phishing etc?
i am interested in a deeper knowledge, for example a complete hack at free wifi.. how i can do a dns spoof, get some accounts etc?
and finally which is the best way to hide my tracks? i think that i should learn this first and then proceed to hacking experiments :P

kauris - January 21, 2012, 12:34 pm

in order for this to work your suppose to be connected to the same network as the victim right???

i tried hacking facebook accounts i tired it on my sister and it worked but when i tried it on my friend who was a few miles away it didnt work
so is there a way to hack facebook accounts and not be in the same network as the slave
if there is i want to know

BTW i was using SET when i was experamenting

Dragon Siege - March 24, 2012, 3:05 am

Looks Like a Pretty Good Tutorial, Didn't Read it All But what I read looked good. Great Job :)

BomBas - February 28, 2013, 8:25 am

I don't understand how it's possible to hack a WINDOWS system just by getting the victi m to enter a site. (I saw a video doing it with SET - Java Applet)

BTW, what's a slave?

sccsc69uk - April 23, 2013, 9:25 am

good posting - tonight's job - seein what trouble I can get into

rfdp - April 23, 2013, 9:37 am

Great tutorial but phishing is not allowed :/

The Sailor ? - April 23, 2013, 12:04 pm

COOI thanks alot for sharing, have to try this out later today.

chippydog - April 23, 2013, 2:42 pm

Great tutorial, you can also make the url into a more trustworthy link instead of numbers at, www.goo.gl etc.

Sir SkinowZ - April 23, 2013, 4:26 pm

Good job bro very great tutorial ?

calbus - June 22, 2013, 11:54 am

This is a cool tutorial, thank you!