

Forum:[Hack Forums](#)

Thread: [Metasploit and Social Engineering Toolkit on iPhone](#)

D4T4B4S3 - August 3, 2014, 1:32 pm

Hey Hack Forums,

This is my first post and it will be about getting Metasploit on iPhone. I successfully installed it on my iPhone 5 running ios 7.1. To install it follow these steps[needs jailbreak]: First of all Install SBSettings from Cydia

1-On Cydia go to Sources, click Edit - Add and add these repos "<http://ininjas.com/repo/>" and "<http://cydia.myrepospace.com/Boo/>"

2-Now go to Search on Cydia and install MobileTerminal.

3-Okay now we have to get the "wget" command on our terminal. Type in "su" and "alpine" as password to gain Root access. Now, in these steps, we will be building our own terminal. Type these commands on your terminal:

```
"apt-get update"
```

```
"apt-get dist-upgrade"
```

```
"apt-get install wget subversion"
```

4-Now we have successfully installed the "wget" command on our mobile terminal ?

5-Here comes the boring+harder parts. On you device, go to Settings>Wifi and connect to your wifi.

6-After connecting to your WiFi, on your device open SBSettings by swiping right on the clock area and write that Wi-Fi IP Address somewhere as shown below.

7-Now if you have a Mac OSX, your work will be alot easier. If you don't, you do not need to do part 8.

8-From OSX terminal make a SSH connection to your iDevice like this:

9-Now we are going to download the correct version of ruby. Type these commands in:

```
"wget http://ininjas.com/repo/debs/iconv\_1.14-1\_iphoneos-arm.deb"
```

```
"wget http://ininjas.com/repo/debs/zlib\_1.2.3-1\_iphoneos-arm.deb"
```

```
"wget
```

```
http://apt.saurik.com/dists/tangelo-0.9/main/binary-iphoneos-arm/debs/ruby\_1.8.6-p111-5\_iphoneos-arm.deb"
```

```
"wget
```

```
http://apt.saurik.com/dists/tangelo-0.9/main/binary-iphoneos-arm/debs/rubygems\_1.2.0-3\_iphoneos-arm.deb."
```

10-After downloading all of the deb files, we need to install them:

```
"dpkg -i iconv_1.14-1_iphoneos-arm.deb"
```

```
"dpkg -i zlib_1.2.3-1_iphoneos-arm.deb"
```

```
"dpkg -i ruby_1.8.6-p111-5_iphoneos-arm.deb"
```

```
"dpkg -i rubygems_1.2.0-3_iphoneos-arm.deb"
```

11-And after we install all of the files inside the .deb's, we do not need the .deb files any more. Lets delete them:

```
"rm -rf *.deb"
```

12-Now we have to cd to our Pentest file. (/var/mobile/pentest - If you do not have that file cd to here /private/var).

13-We are going to get Metasploit from github, with the "git" command and name it framework3 (this command will do it):

"git clone git://github.com/rapid7/metasploit-framework framework3"

14-It gives a empty git error at start sometimes, but it will continue, give it like 5-10 minutes to fully download+install required files.

15-Now in your Pentest file, cd to Exploits and you should see a file named framework3, thats Metasploit! But no, we are not done yet ?

16-Go to Cydia and install the file named Metasploit (6mb). This file will add the command "msfconsole" on your mobile terminal.

17-After doing that on your framework3 folder type in "msfconsole". It will give an error. (Illegal instruction: 4) To fix this error on your framework3 folder, type in "which ruby" and it will show you where ruby is installed.(lets say /usr/local/bin/ruby)

18-Now type or paste this while you are on the framework3 folder:

```
"sed -i" ' s/\x00\x30\x93\xe4/\x00\x30\x93\xe5/g;s/\x00\x30\xd3\xe4/\x00\x30\xd3\xe5/g;' /usr/local/bin/ruby"
```

19-After all this work, Metasploit should be working fine! ?

20-If you want S.E.T aswell, go on Cydia and Search for SET. Install it and you should see SET file on your /pentest/exploits file too. CD into that file and try running set like this: "./set". If it says Illegal Instruction:4, paste the code above on your SET file aswell.

21-You are done, i will be happy to help any errors! ?

-Fortune@Chaos Hackerz-

NarwhalTusks - August 3, 2014, 1:34 pm

First post and it actually looks pretty great. Good job man, keep being HQ :D

EDIT: No idea if this works, just commenting on the look of the thread and all that jazz.

D4T4B4S3 - August 3, 2014, 1:36 pm

Thank you very much bro ? I am trying to figure this website out and i will post alot more ?

NarwhalTusks - August 3, 2014, 1:46 pm

(Aug 3, 2014 01:36 PM)Fortune-ChaosHackerz Wrote: [\[CITE\]](#) Thank you very much bro ? I am trying to figure this website out and i will post alot more ?

No worries man, I know what it's like to be new. ? Just keep reading and posting and try to soak up as much as you can. ?

D4T4B4S3 - August 3, 2014, 1:48 pm

(Aug 3, 2014 01:46 PM)NarwhalTusks Wrote: [\[CITE\]](#) No worries man, I know what it's like to be new. ? Just keep reading and posting and try to soak up as much as you can. ?Thanks man, yeah i will try my best ?

Grin - August 14, 2014, 11:16 am

You don't have to do all that. Just use iNinjas repos and download said packages. ???

D4T4B4S3 - August 14, 2014, 1:47 pm

(Aug 14, 2014 11:16 AM)Grin Wrote: [\[CITE\]](#) You don't have to do all that. Just use iNinjas repos and download said packages. ???

Nope, that doesn't work. I have tried installing this for like 10 hours. Ininjas repo will give error if one of the steps above was passed mate :P

Private Parts - August 17, 2014, 1:07 am

Wow, a way to do this on IOS 7... I've seen this on some older versions of IOS, but it stopped working on IOS 7. I will definitely check this out later.

D4T4B4S3 - August 17, 2014, 2:14 am

(Aug 17, 2014 01:07 AM)Private Parts Wrote: [\[CITE\]](#) Wow, a way to do this on IOS 7... I've seen this on some older versions of IOS, but it stopped working on IOS 7. I will definitely check this out later. Hehe, thanks mate ask questions here if any errors appear :P

D4T4B4S3 - August 17, 2014, 9:24 am

(Aug 17, 2014 07:52 AM)NoCheat Wrote: [\[CITE\]](#) Very good encrypt I recommend it very well! Thank you very much ? Hope I could've helped!

viewsonic1970 - September 3, 2014, 4:34 pm

Once I master metasploit on my pc, then I will try this...lol could be a while :)

D4T4B4S3 - September 3, 2014, 5:12 pm

(Sep 3, 2014 04:34 PM)viewsonic1970 Wrote: [\[CITE\]](#) Once I master metasploit on my pc, then I will try this...lol could be a while :)

Good luck mate, I am pretty sure you will somehow figure it all out ?

Storm- - September 4, 2014, 10:17 am

Are you aware of any limitations to the IOS version of Metasploit?

D4T4B4S3 - September 4, 2014, 11:16 am

(Sep 4, 2014 10:17 AM)Storm- Wrote: [\[CITE\]](#) Are you aware of any limitations to the IOS version of Metasploit?

Yeah, there are actually many limitations ?

But still there are things you can do :)

???? - January 25, 2015, 11:55 am

This was really fun doing it ? and hard ?

Hydra935 - October 28, 2016, 12:36 pm

Can you update your tutorial please ?

ininjas repo is down, and i've got "no module named pexpect" error in the SET in the cra.cn repo