

Forum:[Hack Forums](#)

Thread: [\[*TUT*\] Metasploit, S.E.T., and compatible Terminal on iPhone 4\[*TUT*\]](#)

Fr0st Byte - October 16, 2010, 11:11 am

I'm sharing this with HF because I noticed on my iPhone 4, I couldn't get these working correctly, but here is how to do it if any of you struggle with it.

You'll need: Jailbroken iPhone 4 (might work on other generations, not sure though)

Install 'OpenSSH', 'nano', and 'APT 0.7 Strict' via cydia

Make sure you have installed 'OpenSSH', 'nano', and 'APT 0.7 Strict' via cydia before you begin.

It's much faster to do this via SSH, so I'd download PuTTY: [DOWNLOAD HERE](#). For the Terminal part of this tutorial, I suggest using WinSCP or FileZilla, you chose.

Metasploit

SSH into your iPhone, (user = root, password = alpine, unless changed with "passwd root" command) and use these commands:

```
Code cd /private/var/
```

```
apt-get install subversion nano ruby rubygems wget python
```

```
apt-get clean
```

```
wget http://www.metasploit.com/releases/framework-3.4.1.tar.bz2
```

```
tar jxpf framework-3.4.1.tar.bz2
```

```
cd msf3
```

```
svn update
```

Social Engineering Toolkit; S.E.T.

```
Code cd /private/var/
```

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

```
cd SET/
```

```
./set
```

Agree to install the pexpect and soup python modules

Edit your set config file found at config/set_config and change the msf path to /private/var/msf3

```
Code cd config
```

```
nano set_config
```

to save your changes, press Ctrl+o, then Ctrl+x, confirm all

[img]http://i55.[censored].com/25quhad.png[/img]

IMPORTANT!!

A few days after I did this tutorial, the Cydia repos got an updated ruby 1.9 package, which breaks metasploit completely. To resolve this, uninstall ruby 1.9, and rubygems, and install the older packages (ruby_1.8.6-p111-5_iphoneos-arm.deb and rubygems_1.2.0-3_iphoneos-arm.deb) manually with dpkg. Here are the commands, once again I suggest doing this with putty through

SSH:

```
Code cd /private/var
```

```
apt-get remove ruby rubygems
```

```
wget
```

```
http://apt.saurik.com/dists/tangelo-0.9/main/binary-iphoneos-arm/debs/ruby_1.8.6-p111-5_iphoneos-arm.deb
```

```
dpkg -i 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
```

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

```
rm ruby*
```

iPhone 4 Terminal

This terminal is somewhat laggish, but, it does work, and if you're an iPhone 4 user like me, you'll know that the terminal in Cydia doesn't work for you.

Download [Mobile Terminal 4.26](#). SSH into your phone (this is why I suggest WinSCP, easier to drag and drop for people) and drop the .deb into:

```
Code /private/
```

If you're using WinSCP, hit Ctrl+T, or click the Black Terminal icon, and run the command "dpkg -i MobileTerminal-426.deb"

After it gets to "setting up mobileterminal (426)", close out the window, respring your phone and the icon should show up.

If it appears as a blank icon, drop [This Terminal Icon](#) into /private/var/stash/applications/terminal.app and rename it icon.png
You may need to reboot your phone once or twice for the icon to show up.

TEST!

Now, open up your terminal, and run these commands:

```
Code cd /private/var/
```

```
ls
```

You should see two directories, 'SET', and 'msf3'.

You can now CD into SET via your mobile terminal and run

```
Code su (enter root password, default is alpine)
```

```
./set
```

To open the SET.

Alternatively, from /private/var/, you could cd to msf3, and run

```
Code ./msfconsole
```

to open Metasploit (if you fixed the Ruby errors I posted above)

If you have any questions, feel free to PM me, I hope this works for you like it did me.

Cylay - October 16, 2010, 11:33 am

Wow thank you very much !

Fr0st_Byte - October 16, 2010, 11:37 am

(Oct 16, 2010 11:33 AM)Cylay Wrote: [\[CITE\]](#) Wow thank you very much !

Very welcome, This is a compilation of sources online, I just put them all together for HF.

FadeCity - October 16, 2010, 11:38 am

Nice tut bro. Gonna look into this, sounds like fun.

Fr0st_Byte - October 16, 2010, 12:02 pm

(Oct 16, 2010 11:38 AM)Fade Wrote: [\[CITE\]](#) Nice tut bro. Gonna look into this, sounds like fun.

It is =]

I'm trying to find a better terminal for the iPhone atm, the one here won't scroll up to let you see things past the screen, which if anyone has used metasploit, you know "show exploits" is gonna need that feature.

SkylarTheFox - October 16, 2010, 12:53 pm

(Oct 16, 2010 12:02 PM)Kotto*N[ix]mouth Wrote: [\[CITE\]](#) It is =]

I'm trying to find a better terminal for the iPhone atm, the one here won't scroll up to let you see things past the screen, which if anyone has used metasploit, you know "show exploits" is gonna need that feature.

MobileTerminal 4.26 is the only Terminal that supports iOS 4.

Fr0st_Byte - October 16, 2010, 1:24 pm

(Oct 16, 2010 12:53 PM)FrostyFoxxy Wrote: [\[CITE\]](#) MobileTerminal 4.26 is the only Terminal that supports iOS 4.

For now lol. Thanks though I won't bother for a while then.

skull2006 - October 21, 2010, 1:11 am

thank you man..everything is okay

Fr0st_Byte - October 21, 2010, 7:38 am

I hope it worked out well for you. Only thing I don't like about this is that after installing the older ruby and rubygems packages Cydia keeps wanting you to update =/

dubshah - October 21, 2010, 11:38 pm

I've followed the tutorial closely, and tried looking up the solution to this error but have not had any luck. I was wondering if you would have any insight?

Im running cydia on the most recent Iphone 4 OS.

```
home:/private/var root# cd msf3
home:/private/var/msf3 root# ./msfconsole
/private/var/msf3/data/msfweb/vendor/rails/activesupport/lib/active_support/dependencies.rb:440:in
`load_missing_constant': uninitialized constant Rex::Zip::Jar (NameError)
    from
/private/var/msf3/data/msfweb/vendor/rails/activesupport/lib/active_support/dependencies.rb:80:in
`const_missing'
```

```
from /private/var/msf3/lib/msf/core/payload/java.rb:24:in `tcp_stager_jar'
from (eval):49:in `generate_jar'
from (eval):42:in `generate'
from /private/var/msf3/lib/msf/core/payload.rb:163:in `size'
from /private/var/msf3/lib/msf/core/payload_set.rb:168:in `recalculate'
from /private/var/msf3/lib/msf/core/payload_set.rb:113:in `each_pair'
from /private/var/msf3/lib/msf/core/payload_set.rb:113:in `recalculate'
... 7 levels...
from /private/var/msf3/lib/msf/base/simple/framework.rb:70:in `create'
from /private/var/msf3/lib/msf/ui/console/driver.rb:85:in `initialize'
from ./msfconsole:112:in `new'
from ./msfconsole:112
home:/private/var/msf3 root#
```

Fr0st_Byte - October 22, 2010, 2:14 pm

(Oct 21, 2010 11:38 PM)dubshah Wrote: [\[CITE\]](#) I've followed the tutorial closely, and tried looking up the solution to this error but have not had any luck. I was wondering if you would have any insight?

Im running cydia on the most recent Iphone 4 OS.

```
home:/private/var root# cd msf3
home:/private/var/msf3 root# ./msfconsole
/private/var/msf3/data/msfweb/vendor/rails/activessupport/lib/active_support/dependencies.rb:440:in
`load_missing_constant': uninitialized constant Rex::Zip::Jar (NameError)
from
/private/var/msf3/data/msfweb/vendor/rails/activessupport/lib/active_support/dependencies.rb:80:in
`const_missing'
from /private/var/msf3/lib/msf/core/payload/java.rb:24:in `tcp_stager_jar'
from (eval):49:in `generate_jar'
from (eval):42:in `generate'
from /private/var/msf3/lib/msf/core/payload.rb:163:in `size'
from /private/var/msf3/lib/msf/core/payload_set.rb:168:in `recalculate'
from /private/var/msf3/lib/msf/core/payload_set.rb:113:in `each_pair'
from /private/var/msf3/lib/msf/core/payload_set.rb:113:in `recalculate'
... 7 levels...
from /private/var/msf3/lib/msf/base/simple/framework.rb:70:in `create'
from /private/var/msf3/lib/msf/ui/console/driver.rb:85:in `initialize'
from ./msfconsole:112:in `new'
from ./msfconsole:112
home:/private/var/msf3 root#
Try running it as root:
Code su (enter password)
cd /private/var/msf3/
./msfconsole
```

TyggerBob - November 2, 2010, 7:34 pm

This works well for me. Thanks for bringing everything together.

I wanted to mention that for those who are having problems with MobileTerminal on IOS4, PodZombie has a repository with a working version.

The information can be found here:

<http://www.podzombie.com/2010/08/learn-how-to-install-mobileterminal-v4-2-6-the-easy-way-ios4-compatible-version/>

I actually prefer iSSH with a localhost connection. I like having the easy access to the control and

alt keys and the key pie rocks!

Tyg

Fr0st_Byte - November 7, 2010, 7:25 pm

(Nov 2, 2010 07:34 PM)TyggerBob Wrote: [\[CITE\]](#) This works well for me. Thanks for bringing everything together.

I wanted to mention that for those who are having problems with MobileTerminal on IOS4, PodZombie has a repository with a working version.

The information can be found here:

<http://www.podzombie.com/2010/08/learn-how-to-install-mobileterminal-v4-2-6-the-easy-way-ios4-compatible-version/>

I actually prefer iSSH with a localhost connection. I like having the easy access to the control and alt keys and the key pie rocks!

Tyg

You're welcome, and thanks for the extra info for others.

Stocking - November 7, 2010, 7:28 pm

I've been trying to get SET on my iPhone!

Thanks man!

Fr0st_Byte - November 7, 2010, 7:33 pm

(Nov 7, 2010 08:28 PM)moosefaux Wrote: [\[CITE\]](#) I've been trying to get SET on my iPhone!

Thanks man!

No problem dude, glad you enjoyed it.

Sir SkinowZ - November 8, 2010, 1:04 pm

Very good man

Thanks you

Fr0st_Byte - November 9, 2010, 10:03 am

No problem guys, glad you enjoyed it.

If you have any questions suggestions or comments let me know.

StaTiX - November 9, 2010, 10:04 am

thanks but is it possible to do this on HTC wildfire ?

Fr0st_Byte - November 9, 2010, 7:41 pm

(Nov 9, 2010 11:04 AM)StaTiX Wrote: [\[CITE\]](#) thanks but is it possible to do this on HTC wildfire ?

Idk the method but I'm sure there is a way. All I can tell you there is <http://www.google.com/> lol. Sorry.

mrprez - November 19, 2010, 8:33 pm

How bout using TouchTerm for this, would it work? I will try when I get home..

Fr0st_Byte - November 20, 2010, 10:05 pm

Idk, try it and report back. Are you trying it with an iPhone 4?

Pvsxe - November 21, 2010, 3:00 am

works to on ipod 3gs

thank you very much :D

Fallenbot - November 21, 2010, 9:22 am

The images in the main topic are deleted. Can you re-upload it mate?

Thanks in advance. Appreciated.

Fr0st_Byte - December 22, 2010, 10:36 am

I will try to get the posts fixed with the images asap. If anyone has any questions about this without the pictures feel free to contact me. I may be working on a tutorial for the same thing with Android based phones soon; not 100% sure though.

I will try to get the posts fixed with the images asap. If anyone has any questions about this without the pictures feel free to contact me. I may be working on a tutorial for the same thing with Android based phones soon; not 100% sure though.

Fr0st_Byte - December 22, 2010, 2:18 pm

Images fixed. If they go back down again, please let me know, someone.

Thanks; hope you enjoy the tutorial.

skull2006 - January 7, 2011, 3:54 pm

but there is problem with fasttrack and msf3

because when i start fasttrack and make autopwn it look for sqlite database

is there any help for that problem.

tnx

Fr0st_Byte - January 7, 2011, 4:12 pm

You'd need that database on the phone. This is a tutorial for strictly installing SET and using it with Metasploit.

This reminds me though that I need to update the commands; the SET as been moved in location.

skull2006 - January 8, 2011, 7:23 am

yes we need DB to make it run.

but how to install sqlite in iphone?

tnx

Fr0st_Byte - January 8, 2011, 8:45 am

(Jan 8, 2011 08:23 AM)skull2006 Wrote: [\[CITE\]](#) yes we need DB to make it run.

but how to install sqlite in iphone?

tnx

I don't think this is what everyone is looking for, but this is all I could find:

<http://dblog.com.au/iphone-development-tutorials/iphone-sdk-tutorial-reading-data-from-a-sqlite-database/>

IDK what you all need this for...I use the S.E.T. and Metasploit on my iPhone every day or so with no problem. The only problem I have at all is using Metasploit listener, and that can easily be resolved via WiFi or VPN connections.

Freezer - February 9, 2011, 7:58 am

when i type tar pxpf framework-3.4.1.tar.bz2 . It says low disk space even though i have 18GB free.

and then the step results in error and doesn't complete.
what should i do ?

dixonkyleard - April 11, 2011, 7:00 pm

(Oct 16, 2010 11:11 AM)Kotto*N[ix]mouth Wrote: [\[CITE\]](#) I'm sharing this with HF because I noticed on my iPhone 4, I couldn't get these working correctly, but here is how to do it if any of you struggle with it.

You'll need: Jailbroken iPhone 4 (might work on other generations, not sure though)

Install 'OpenSSH', 'nano', and 'APT 0.7 Strict' via cydia

Make sure you have installed 'OpenSSH', 'nano', and 'APT 0.7 Strict' via cydia before you begin.

It's much faster to do this via SSH, so I'd download PuTTY: [DOWNLOAD HERE](#). For the Terminal part of this tutorial, I suggest using WinSCP or FileZilla, you chose.

Metasploit

SSH into your iPhone, (user = root, password = alpine, unless changed with "passwd root" command) and use these commands:

```
Code cd /private/var/  
apt-get install subversion nano ruby rubygems wget python  
apt-get clean  
wget http://www.metasploit.com/releases/framework-3.4.1.tar.bz2  
tar jxpf framework-3.4.1.tar.bz2  
cd msf3  
svn update  
Social Engineering Toolkit; S.E.T.
```

```
Code cd /private/var/  
svn co http://svn.secmaniac.com/social_engineering_toolkit SET/  
cd SET/  
./set  
Agree to install the pexpect and soup python modules
```

Edit your set config file found at config/set_config and change the msf path to /private/var/msf3

```
Code cd config  
nano set_config  
to save your changes, press Ctrl+o, then Ctrl+x, confirm all
```

[img]http://i55.[censored].com/25quhad.png[/img]

IMPORTANT!!

A few days after I did this tutorial, the Cydia repos got an updated ruby 1.9 package, which breaks metasploit completely. To resolve this, uninstall ruby 1.9, and rubygems, and install the older packages (ruby_1.8.6-p111-5_iphoneos-arm.deb and rubygems_1.2.0-3_iphoneos-arm.deb) manually with dpkg. Here are the commands, once again I suggest doing this with putty through SSH:

```
Code cd /private/var
```

```
apt-get remove ruby rubygems
```

```
wget
```

```
http://apt.saurik.com/dists/tangelo-0.9/main/binary-iphoneos-arm/debs/ruby_1.8.6-p111-5_iphoneos-arm.deb
```

```
dpkg -i 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
```

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

```
rm ruby*
```

iPhone 4 Terminal

This terminal is somewhat laggish, but, it does work, and if you're an iPhone 4 user like me, you'll know that the terminal in Cydia doesn't work for you.

Download [Mobile Terminal 4.26](#). SSH into your phone (this is why I suggest WinSCP, easier to drag and drop for people) and drop the .deb into:

Code /private/

If you're using WinSCP, hit Ctrl+T, or click the Black Terminal icon, and run the command "dpkg -i MobileTerminal-426.deb"

After it gets to "setting up mobileterminal (426), close out the window, respring your phone and the icon should show up.

If it appears as a blank icon, drop [This Terminal Icon](#) into

/private/var/stash/applications/terminal.app and rename it icon.png

You may need to reboot your phone once or twice for the icon to show up.

TEST!

Now, open up your terminal, and run these commands:

Code cd /private/var/

ls

You should see two directories, 'SET', and 'msf3'.

You can now CD into SET via your mobile terminal and run

Code su (enter root password, default is alpine)

./set

To open the SET.

Alternatively, from /private/var/, you could cd to msf3, and run

Code ./msfconsole

to open Metasploit (if you fixed the Ruby errors I posted above)

If you have any questions, feel free to PM me, I hope this works for you like it did me.

Do you happen to have Ruby 1.8.7? its required to install db_driver sqlite3 which would be very handy for backdoor exploits on xp. I've searched everywhere and even tried compiling my own with

no luck.