

Forum:[Hack Forums](#)

Thread: [Antagonism | Install & Config -> Metasploit * PostgreSQL * GIT * SET |](#)

?Dante - January 25, 2013, 7:00 am

[img]http://desmond.imageshack.us/Himg515/scaled.php?server=515&filename=antagonism.jpg&res=medium[/img]

INTRODUCTION-

Metasploit Framework or MSF is a famous 'penetration testing suite' which is used by 'pentesters' worldwide and it's almost their first choice to start a 'pentest'. This pentesting suite consists of thousands of 'exploits' which actually are scripts or codes written in some 'scripting languages' like python, perl, ruby etc.

SHORT DEFINATIONS-

Pentesting: A penetration test or pentesting is a typical 'test' the most effective way to detect and identify the vulnerabilities in programs, operating systems, networks etc. so that the system/network wouldn't get compromised by the BH (black hat) hackers and doing so will ensure the system/network is up-to-date in terms of 'security'.

Vulnerability: It's basically a weakness in programs, OS modules, and even human mind (in terms of 'social engineering' which isn't covered in this thread) which can be used to exploit a system and network etc.

Exploit: Exploit is a piece of 'code' which, when executed on a 'vulnerable' machine/system compromises that system. In general, that system would be in hands of the attacker/pentester.

DOWNLOADS AND INSTALLATIONS-

NOTE: All codes should be entered in TERMINAL.

Metasploit Framework (community edition)

To download it, you may need to goto the link provided below and select the appropriate download either Linux or Windows (Linux recommended) as this tutorial will focus on debian Linux i.e. [Ubuntu](#). So download the '.run' file.

[Metasploit Framework 4.5](#)

Once downloaded, move that file into this directory-

`"/home/your_username_here/Downloads/"`

So it'd look like-

`"/home/your_username_here/Downloads/metasploit-4.x.x.run"`

Then you need to move the file metasploit-4.x.x.run which is actually a GUI installer by the way, to the ROOT directory i.e. `" / "` (the forward slash) and also set the file's attributes to be executed by ROOT and THEN execute the installer. But you'll need to be ROOT user. To do that either use the 'sudo' or login as ROOT.

Login as ROOT-

Code `sudo su`

`mv /home/your_username_here/Downloads/metasploit-4.x.x.run /`

`chmod +x metasploit-4.x.x.run`

`./metasploit-4.x.x.run`

Using SUDO-

Code `sudo mv /home/your_username_here/Downloads/metasploit-4.x.x.run /`

`chmod +x metasploit-4.x.x.run`

`./metasploit-4.x.x.run`

You'll be greeted with the cool logo of Metasploit. Further, click forward. Accept the license agreement and click forward. Select the folder where you wanna install MSF and click forward. Recommended location is in the image.

Spoiler [\(Click to View\)](#)

Now, click yes on the next prompt to 'register Metasploit as a service' and add it to the startup and click forward. Select the desired SSL port (default: 3790 is recommended) and click forward Name your server e.g. "dante-pc" (you can pick any) and click forward.

Installation should start now. It wouldn't take much long, just stare at it and it'll complete. :P

Sooner you'll see installation is finalizing.

Make sure the checkbox is ticked and click finish-

Spoiler [\(Click to View\)](#)

Your browser should open a link i.e. "https://localhost:3790/license/offline_activation" and you'll see a warning page like shown below. Don't panic! Simply click proceed anyway (on chrome) or I understand the risks, add an exception (in firefox) and add this page's certificate to your exception list and you'll be good.

Spoiler [\(Click to View\)](#)

Then, you'll see a page like shown below. Just wait some seconds and you'll be redirected to another page.

Spoiler [\(Click to View\)](#)

Now, as you're installing MSF for the first time, you've to activate it by registering and making a personal-use account. Simply click on Create Account and follow on-screen instructions.

Spoiler [\(Click to View\)](#)

Fill-up this simple form-

Spoiler [\(Click to View\)](#)

Now, click on the get activation key and follow the on screen steps to get the key on your e-mail that you'd provide and login using the user-password you made-

Spoiler [\(Click to View\)](#)

After logging in, you'll be there which you can call ADMIN-CP of your own MSF. :D You can manage many things from here. Just explore, they're self explicit. Then logout and get ready to see more interesting things. :)

Spoiler [\(Click to View\)](#)

Open-up a terminal by CTRL+ALT+T or by any means then get ROOT and update the MSF by entering following commands in the terminal-

```
Code sudo su  
msfupdate
```

After the update is complete, you can launch the MSF by following command.

```
Code msfconsole
```

Wait for about 30 seconds or more to let MSF load all its exploits and scripts etc. into memory. After that, you shall see something what's called the text version of MSF :D with cool ASCII art banner.

Enter the following command to check whether or not the database is connected to MSF-. B-)

```
Code db_status
```

If your output matches the image below then everything is fine. If not so, then read further- :)

Spoiler ([Click to View](#))

Now, if your database isn't connected by any cause then what you have to do is, connect MSF to the 'postgresql database'.

NOTE: Read the next section below on how to configure 'postgresql database'.

```
Code db_connect
```

```
postgre_username:postgre_user_password@127.0.0.1/postgresql_database_name
```

Further reading:

[Metasploit Unleashed](#)

[Metasploit Wiki](#)

[Metasploit Community](#)

[Metasploit Help](#)

And you're done!

PostgreSQL 9.1

We need it as it's the only database which is supported by MSF as of now. We need database to store 'informations' on our pentests, IP scans, vulnerability scans, etc.

```
Code sudo apt-get install postgresql-9.1 libpq-dev
```

After installing it, you've to make sure of two settings in the "postgresql.conf" as below-

```
Quote:listen_addresses = 'localhost'
```

```
or
```

```
listen_addresses = '127.0.0.1'
```

```
and
```

```
password_encryption = on
```

If not so, change them by editing the configuration file-

```
Code sudo nano /etc/postgresql/9.1/main/postgresql.conf
```

Now we need to create a postgresql user, password, database and set the ownership of the postgresql database to the user we created. While this part is kinda not needed to be configured as the latest version of MSF i.e. 4.5 comes preconfigured with postgresql database so whenever you run MSF, you can always check the status of 'driver' being used and the database is connected to it (that'd be postgresql for sure) by the entering the following command in MSFCONSOLE terminal-

```
Code db_driver
```

```
db_status
```

If, by any cause, the output of these two commands shown above is like- database not connected, or no driver specified or something like that; then you need to continue with the next piece of code written below. But, if everything seems fine, then you can completely skip this 'postgresql' part and

head towards 'git'.

Code `sudo su postgres -c psql`

`postgres=# CREATE USER desired_postgres_user_name WITH PASSWORD 'desired_password';`

`postgres=# CREATE DATABASE desired_database_name OWNER postgres_user_name;`

`postgres=# \q`

Now we need to set password authentication to access the postgres on localhost (127.0.0.1). For that, we need to edit the configuration file located in `"/etc/postgresql/9.1/main/pg_hba.conf"`

Code `sudo nano /etc/postgresql/9.1/main/pg_hba.conf`

Now press CTRL+W and enter 'IPv4 local connections:' without quotes and press 'enter' to search where it is. When you get to that line, you have to change the two fields JUST below this line 'IPv4 local connections:'. Change:

Quote: `host all all 127.0.0.1/32 md5`

to

`host "your_postgres_database" "your_postgres_user" 127.0.0.1/32 md5`

Commands when you're a postgres user-

Code `\h` for help with SQL commands

`\?` for help with PSQL commands

`\g` or terminate with semicolon (;) to execute query (just like in C++ :P)

`\q` to quit

Commands to manage postgresql server-

Code `/etc/init.d/postgresql start`

`/etc/init.d/postgresql stop`

`/etc/init.d/postgresql restart`

`/etc/init.d/postgresql status`

And you're done with postgresql!

GIT

It's a program which will be used to update the MSF database as well as SET too so we need it.

Code `sudo apt-get install git`

SET (Social Engineering Toolkit) *optional*

It's a set of techniques and exploits of MSF which mainly targets the human mind to exploit and compromise a system/network. It isn't used in MSF but SET itself uses exploits of MSF.

Code `git clone https://www.github.com/trustedsec/social-engineer-toolkit/` set/NOTE: Mind the SPACE before set

Now move that downloaded directory named set to `"/opt/pentest/set/"`

and then UPDATE the set-

Code `sudo su`

`cd /opt/pentest/set/`

`./set-update`

You can RUN the set in terminal by moving into the set folder and then running it as-

Code `sudo su`

`cd /opt/pentest/set/`

`./setSpoiler` [\(Click to View\)](#)

Noticed the warning? Sure you do. So what we've to do is simply edit the configuration file located at `"/opt/pentest/set/config/set_config"`. Issue the command as ROOT (`sudo su`)-

Code `nano /opt/pentest/set/config/set_config`

Goto line highlighted in the image below and edit as it's in the image. Then press CTRL+O (to save) and CTRL+X (to exit) and your're done. :D

Spoiler ([Click to View](#))

You may need to update it as well by command-

Code ./set-update

But you must not be running set when you update it.

Spoiler ([Click to View](#))

Try running it again-

Code ./setSpoiler ([Click to View](#))

Further reading:

[SE Blog](#)

And we're done with set too!

And that's it! That's it for now guys. :D

More tutorials are coming. :D Stay tuned and do post your feedback, I'd love to see that. :D

-Dante ?

-?Divine- - January 25, 2013, 7:07 am

Well made Dante. Thanks for posting this.

?Dante - January 25, 2013, 7:10 am

(Jan 25, 2013 08:07 AM)-?Divine- Wrote: ([CITE](#)) Well made Dante. Thanks for posting this.

Glad you liked it D. ? This thread has made me starve, god I need something to eat NOW! ?

Keeper - January 25, 2013, 7:12 am

Nice, hope somebody find it useful. Good job.

?Dante - January 25, 2013, 7:14 am

(Jan 25, 2013 08:12 AM)Keeper Wrote: ([CITE](#)) Nice, hope somebody find it useful. Good job.

Thanks keeper. :3 Sure this'll be useful. ?

Dyme - January 25, 2013, 7:15 am

Really good tut for people new to *nix and have trouble with stuff like this. Nice contribution!

?Dante - January 25, 2013, 7:18 am

(Jan 25, 2013 08:15 AM)Dyme Wrote: ([CITE](#)) Really good tut for people new to *nix and have trouble with stuff like this. Nice contribution!

Yea Dyme, this thread is pretty much needed to be posted too. Also, thanks ?

supracontra - January 25, 2013, 7:49 am

(Jan 25, 2013 08:15 AM)Dyme Wrote: ([CITE](#)) Really good tut for people new to *nix and have trouble with stuff like this. Nice contribution!

People who can't even use their operating system shouldn't be using Metasploit.

shellfu - January 25, 2013, 7:52 am

Great tutorial! Looking forward to even more things from you :)

-Maxi

?Dante - January 25, 2013, 7:53 am

(Jan 25, 2013 08:52 AM)Maxi Wrote: [\[CITE\]](#) Great tutorial!Thanks Maxiii :3

(Jan 25, 2013 08:52 AM)Maxi Wrote: [\[CITE\]](#) Looking forward to even more things from you :)Sure! More are coming ASAP. ? ?

/Ninja - January 25, 2013, 8:57 am

Awesome tut man! looks sweet! Another Tut from an Antagonism :D

?Dante - January 25, 2013, 9:57 am

(Jan 25, 2013 09:57 AM)/Ninja Wrote: [\[CITE\]](#) Awesome tut man! looks sweet! Another Tut from an Antagonism :D

Thanks Ninja! nice to see you like it too. ? And yea, <3 Antagonism ?

Bohemia - January 26, 2013, 5:22 am

This is one hell of a tutorial. Just read through pretty quick, but bookmarked it for later ;) Keep up this HQ Work buddy.

?Dante - January 26, 2013, 5:59 am

(Jan 26, 2013 06:22 AM)vi5hal Wrote: [\[CITE\]](#) This is one hell of a tutorial. Just read through pretty quick, but bookmarked it for later ;) Keep up this HQ Work buddy.

Nice to see that you liked it so much. ? Thanks bhai! ? More tutorials are coming. ?

SIM-111414 - January 26, 2013, 6:24 am

Awesome tut bro.

Thanks for sharing it.

Its really detailed. :)

?Dante - January 26, 2013, 7:24 am

(Jan 26, 2013 07:24 AM)harsh_0707051 Wrote: [\[CITE\]](#) Awesome tut bro.

Thanks for sharing it.

Its really detailed. :)

Yaa! I know that it's awesome ? (my bad :P)

I was just getting tired of replying to same old questions so I made it. I'll be posting more threads/tutorials as I feel they're needed as hell. ?

Glad that this tutorial or mine is serving its cause. ?

Kindly DO post your feedback if you read this tutorial, that'd mean a lot to me.?

I <3 Python. :D

cronic_hack - January 27, 2013, 9:18 am

good work bro! really nice to see ya post! :)

?Dante - January 28, 2013, 3:22 am

(Jan 27, 2013 10:18 AM)cronic_hack Wrote: [\[CITE\]](#) good work bro! really nice to see ya post! :)

Thanks for liking the thread. I posted for a reason. And posting the thread was a success and an

accomplishment for me too. As I've become more HQ than before. ?

AlKapone - January 28, 2013, 6:24 am

Nice Tut - Thanks - Gotta love metasploit although i prefer mysql over any database software

?Dante - January 28, 2013, 6:55 pm

(Jan 28, 2013 07:24 AM)AlKapone Wrote: [\[CITE\]](#) Nice Tut - Thanks - Gotta love metasploit although i prefer mysql over any database software

MySQL is good, I used it in past many times. But now, PostgreSQL is recommended by the makers/coders of MSF and it comes pre-configured now so, better get used to it. Also, thanks for taking your time to post your feedback. Much appreciated. ?

ambujagrawal - January 30, 2013, 5:18 am

vouch!!

this tutorial got everything One will probably need.

Nice Work Keep it Up man

!!

Evanescence - January 30, 2013, 5:52 am

Awesome TUT Dante keep it up with such TUTs.

?Dante - January 30, 2013, 6:00 am

(Jan 30, 2013 06:18 AM)ambujagrawal Wrote: [\[CITE\]](#) vouch!!

this tutorial got everything One will probably need.

Nice Work Keep it Up man

!!

Thanks for the vouch bhai. ?

-Dante ?

(Jan 30, 2013 06:52 AM)D|Known45 Wrote: [\[CITE\]](#) Awesome TUT Dante keep it up with such TUTs. Thanks for your feedback mate. Really happy to see that community is liking it. But NOT posting the feedback MUCH. ? This thread of mine has 240+ views and not even 50% of replies. LOL It doesn't matter much though as people like you are posting on a regular interval. ?

Van1la - January 31, 2013, 5:50 am

Thank You Bro,
Very Good Tutorial....

?Dante - January 31, 2013, 6:16 am

(Jan 31, 2013 06:50 AM)Van1la Wrote: [\[CITE\]](#) Thank You Bro,
Very Good Tutorial....

Thanks Van1la! ? I worked out ma time on this thread. ?

DiamondHacking - April 29, 2013, 2:06 am

Very HQ, plan to use this a lot in the future. Keep this stuff up.

4bh1 - April 29, 2013, 7:28 am

Nice one bro great HQ tutorial.

GO get some energy drink

N1T3ST4LK3R - April 29, 2013, 4:12 pm

Now this is some HQ work. Cheers mate.

super_haker2002 - February 27, 2014, 8:31 pm

Well made Dante. Thanks for posting this.