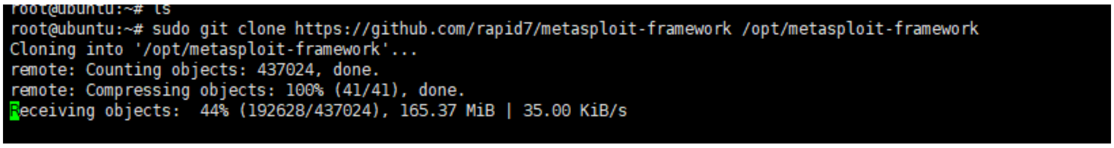
metasploit5 安装与配置

--By Menthol

1， 首先 git

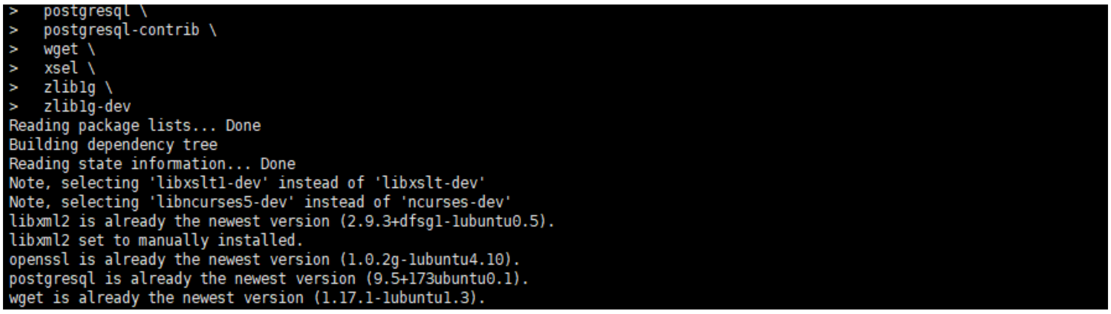
sudo git clone https://github.com/rapid7/metasploit-framework /opt/metasploit-framework



```
root@ubuntu:~# ls
root@ubuntu:~# sudo git clone https://github.com/rapid7/metasploit-framework /opt/metasploit-framework
Cloning into '/opt/metasploit-framework'...
remote: Counting objects: 437024, done.
remote: Compressing objects: 100% (41/41), done.
Receiving objects:  44% (192628/437024), 165.37 MiB | 35.00 KiB/s
```

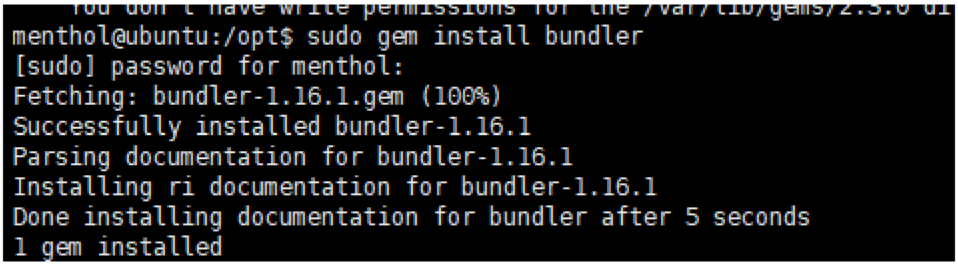
2， 安装所需要的依赖

sudo apt-get -y install \autoconf \bison \build-essential \curl \git-core \ libapr1 \ libaprutil1 \ libcurl4-openssl-dev \ libgmp3-dev \ libpcap-dev \libpq-dev \ libreadline6-dev libsqlite3-dev \ libssl-dev \ libsvn1 \ libtool \ libxml2 \ libxml2-dev \ libxslt-dev \ libyaml-dev \ locate \ ncurses-dev \ openssl \ postgresql \postgresql-contrib \ wget \ xsel \zlib1g \zlib1g-dev

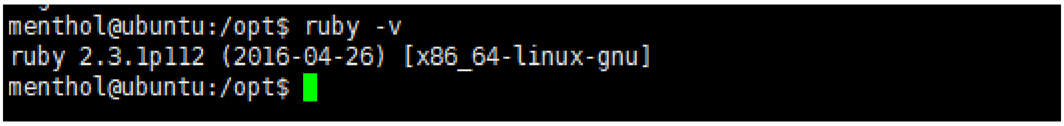


```
>   postgresql \
>   postgresql-contrib \
>   wget \
>   xsel \
>   zlib1g \
>   zlib1g-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libxslt1-dev' instead of 'libxslt-dev'
Note, selecting 'libncurses5-dev' instead of 'ncurses-dev'
libxml2 is already the newest version (2.9.3+dfsg1-1ubuntu0.5).
libxml2 set to manually installed.
openssl is already the newest version (1.0.2g-1ubuntu4.10).
postgresql is already the newest version (9.5+173ubuntu0.1).
wget is already the newest version (1.17.1-1ubuntu1.3).
```

3， 安装 Ruby 和 bundler

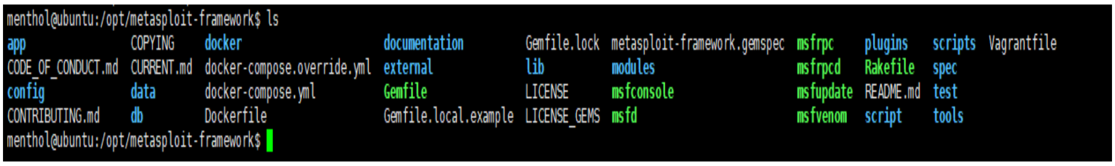


```
  You don't have write permissions for the /var/lib/gems/2.3.0 di
menthol@ubuntu:/opt$ sudo gem install bundler
[sudo] password for menthol:
Fetching: bundler-1.16.1.gem (100%)
Successfully installed bundler-1.16.1
Parsing documentation for bundler-1.16.1
Installing ri documentation for bundler-1.16.1
Done installing documentation for bundler after 5 seconds
1 gem installed
```



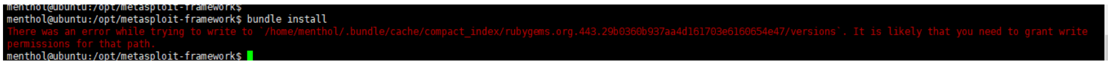
```
menthol@ubuntu:/opt$ ruby -v
ruby 2.3.1p112 (2016-04-26) [x86_64-linux-gnu]
menthol@ubuntu:/opt$ 
```

4， 切换到 metasploit-framework 目录下



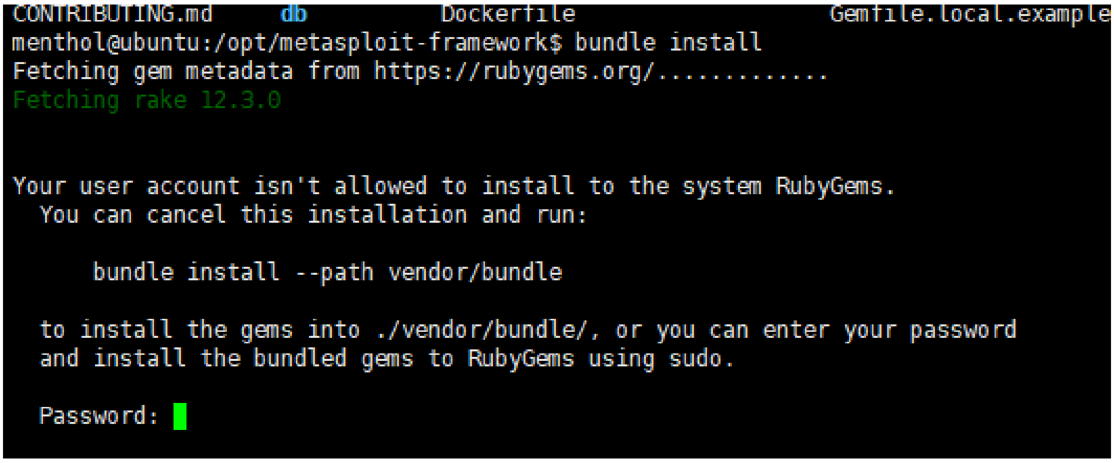
```
menthol@ubuntu:/opt/metasploit-framework$ ls
app              COPYING      docker                     documentation          Gemfile.lock  metasploit-framework.gemspec  msfrpc     plugins   scripts  Vagrantfile
CODE_OF_CONDUCT.md  CURRENT.md  docker-compose.override.yml  external           lib           modules                       msfrpcd    Rakefile  spec
config           data         docker-compose.yml         Gemfile                LICENSE       msfconsole                    msfupdate  README.md test
CONTRIBUTING.md  db           Dockerfile                 Gemfile.local.example  LICENSE_GEMS  msfd                          msfvenom   script    tools
menthol@ubuntu:/opt/metasploit-framework$
```

5， 执行 bundle install，可能会报错，你要确定是否有权限。并且最好不使用 root 权限执行。这里要对执行该操作的用户的家目录下的.bundle 目录有完全的写权限。

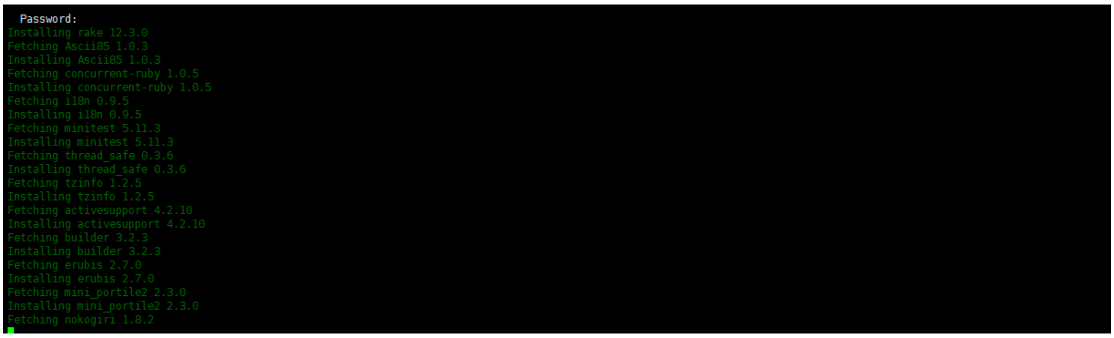


```
menthol@ubuntu:/opt/metasploit-framework$
menthol@ubuntu:/opt/metasploit-framework$ bundle install
There was an error while trying to write to `/home/menthol/.bundle/cache/compact_index/rubygems.org.443.29b0360b937aa4d161703e6160654e47/versions`. It is likely that you need to grant write
permissions for that path.
menthol@ubuntu:/opt/metasploit-framework$
```

需要特殊权限时会自己申请

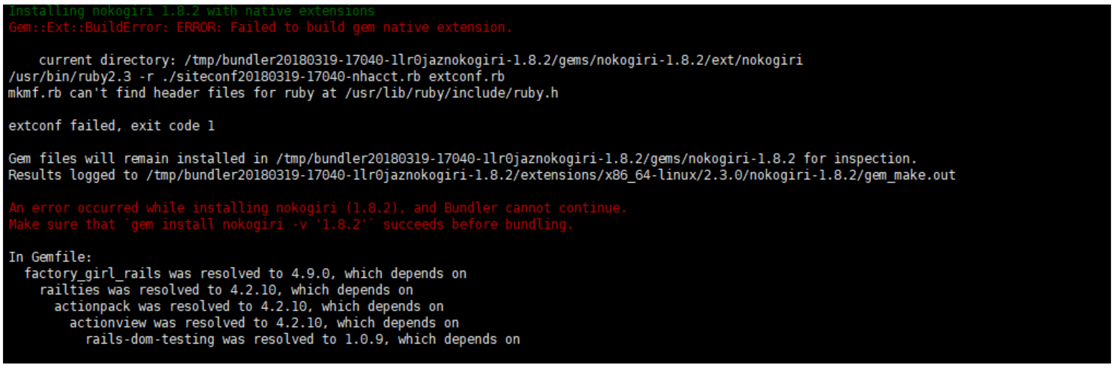


```
CONTRIBUTING.md      db          Dockerfile                Gemfile.local.example
menthol@ubuntu:/opt/metasploit-framework$ bundle install
Fetching gem metadata from https://rubygems.org/.............
Fetching rake 12.3.0


Your user account isn't allowed to install to the system RubyGems.
  You can cancel this installation and run:

      bundle install --path vendor/bundle

  to install the gems into ./vendor/bundle/, or you can enter your password
  and install the bundled gems to RubyGems using sudo.

  Password:
```



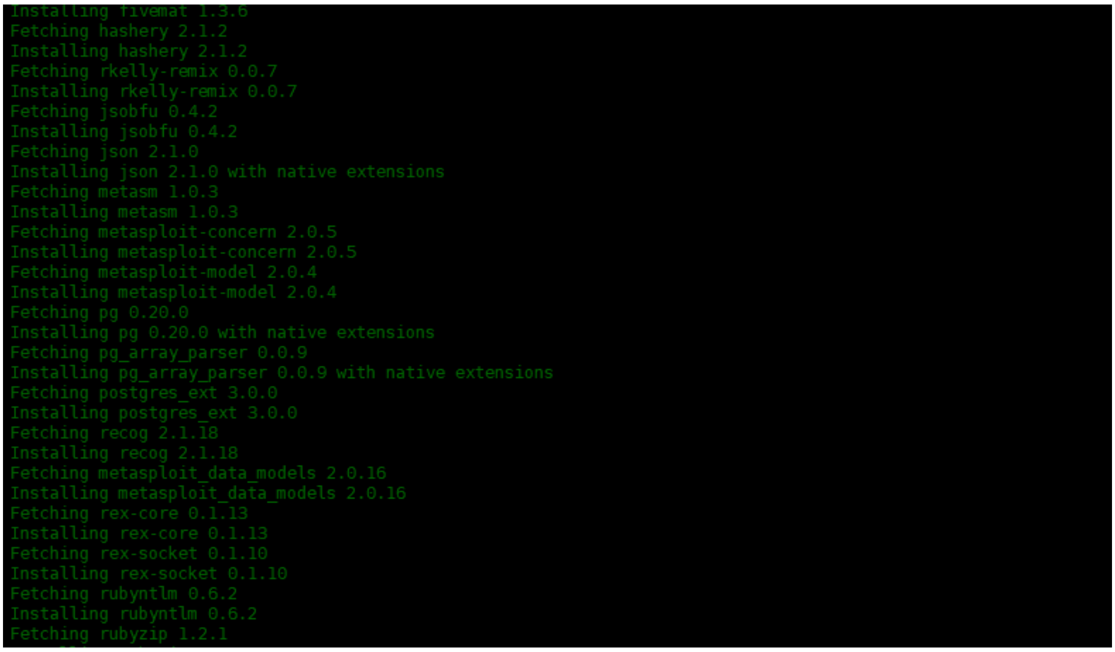
```
  Password:
Installing rake 12.3.0
Fetching Ascii85 1.0.3
Installing Ascii85 1.0.3
Fetching concurrent-ruby 1.0.5
Installing concurrent-ruby 1.0.5
Fetching i18n 0.9.5
Installing i18n 0.9.5
Fetching minitest 5.11.3
Installing minitest 5.11.3
Fetching thread_safe 0.3.6
Installing thread_safe 0.3.6
Fetching tzinfo 1.2.5
Installing tzinfo 1.2.5
Fetching activesupport 4.2.10
Installing activesupport 4.2.10
Fetching builder 3.2.3
Installing builder 3.2.3
Fetching erubis 2.7.0
Installing erubis 2.7.0
Fetching mini_portile2 2.3.0
Installing mini_portile2 2.3.0
Fetching nokogiri 1.8.2
```

6， 可能还会报一下的错误信息



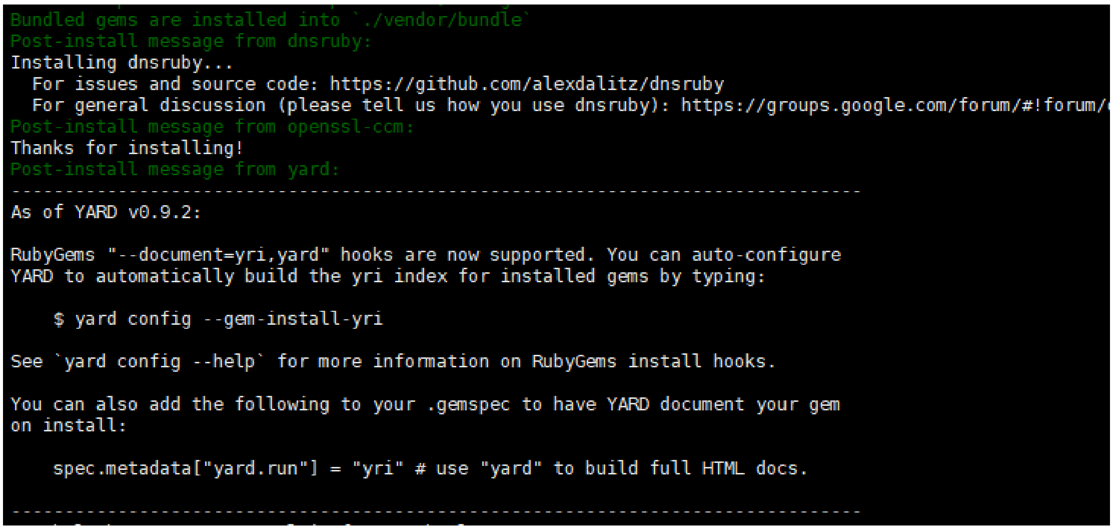
```
Installing nokogiri 1.8.2 with native extensions
Gem::Ext::BuildError: ERROR: Failed to build gem native extension.

    current directory: /tmp/bundler20180319-17040-1lr0jaznokogiri-1.8.2/gems/nokogiri-1.8.2/ext/nokogiri
/usr/bin/ruby2.3 -r ./siteconf20180319-17040-nhacct.rb extconf.rb
mkmf.rb can't find header files for ruby at /usr/lib/ruby/include/ruby.h

extconf failed, exit code 1

Gem files will remain installed in /tmp/bundler20180319-17040-1lr0jaznokogiri-1.8.2/gems/nokogiri-1.8.2 for inspection.
Results logged to /tmp/bundler20180319-17040-1lr0jaznokogiri-1.8.2/extensions/x86_64-linux/2.3.0/nokogiri-1.8.2/gem_make.out

An error occurred while installing nokogiri (1.8.2), and Bundler cannot continue.
Make sure that `gem install nokogiri -v '1.8.2'` succeeds before bundling.

In Gemfile:
  factory_girl_rails was resolved to 4.9.0, which depends on
    railties was resolved to 4.2.10, which depends on
      actionpack was resolved to 4.2.10, which depends on
        actionview was resolved to 4.2.10, which depends on
          rails-dom-testing was resolved to 1.0.9, which depends on
```

此时执行 sudo apt-get intall ruby-dev bundle install --path vendor/bundle gem install nokogiri -v '1.8.2'



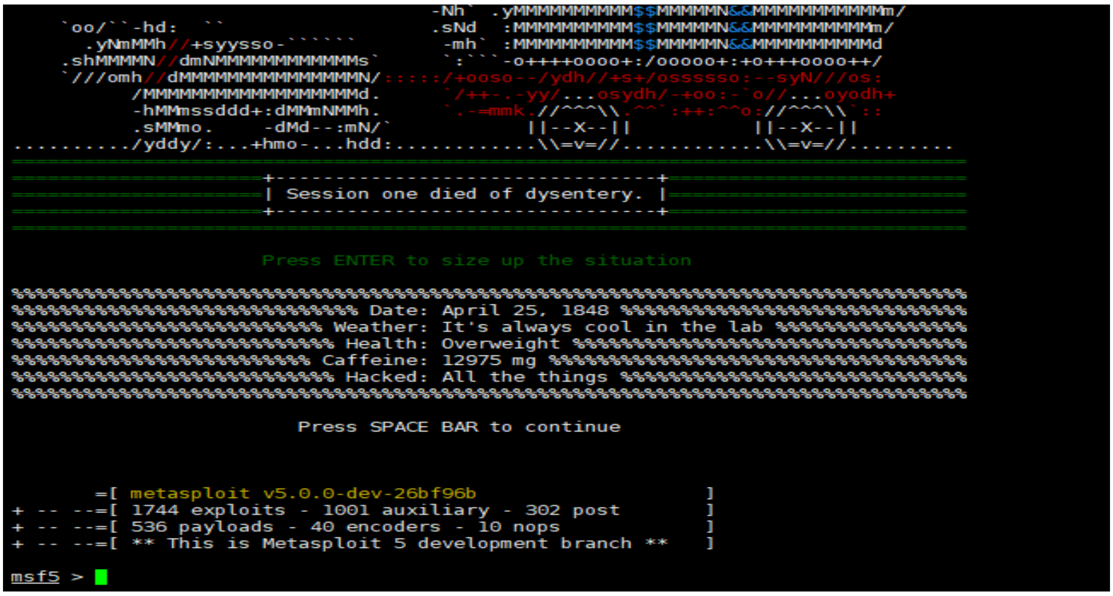
```
Installing fivemat 1.3.6
Fetching hashery 2.1.2
Installing hashery 2.1.2
Fetching rkelly-remix 0.0.7
Installing rkelly-remix 0.0.7
Fetching jsobfu 0.4.2
Installing jsobfu 0.4.2
Fetching json 2.1.0
Installing json 2.1.0 with native extensions
Fetching metasm 1.0.3
Installing metasm 1.0.3
Fetching metasploit-concern 2.0.5
Installing metasploit-concern 2.0.5
Fetching metasploit-model 2.0.4
Installing metasploit-model 2.0.4
Fetching pg 0.20.0
Installing pg 0.20.0 with native extensions
Fetching pg_array_parser 0.0.9
Installing pg_array_parser 0.0.9 with native extensions
Fetching postgres_ext 3.0.0
Installing postgres_ext 3.0.0
Fetching recog 2.1.18
Installing recog 2.1.18
Fetching metasploit_data_models 2.0.16
Installing metasploit_data_models 2.0.16
Fetching rex-core 0.1.13
Installing rex-core 0.1.13
Fetching rex-socket 0.1.10
Installing rex-socket 0.1.10
Fetching rubyntlm 0.6.2
Installing rubyntlm 0.6.2
Fetching rubyzip 1.2.1
```

7， 完成安装



```
Bundled gems are installed into `./vendor/bundle`
Post-install message from dnsruby:
Installing dnsruby...
  For issues and source code: https://github.com/alexdalitz/dnsruby
  For general discussion (please tell us how you use dnsruby): https://groups.google.com/forum/#!forum/
Post-install message from openssl-ccm:
Thanks for installing!
Post-install message from yard:
--------------------------------------------------------------------------------
As of YARD v0.9.2:

RubyGems "--document=yri,yard" hooks are now supported. You can auto-configure
YARD to automatically build the yri index for installed gems by typing:

    $ yard config --gem-install-yri

See `yard config --help` for more information on RubyGems install hooks.

You can also add the following to your .gemspec to have YARD document your gem
on install:

    spec.metadata["yard.run"] = "yri" # use "yard" to build full HTML docs.

--------------------------------------------------------------------------------
```

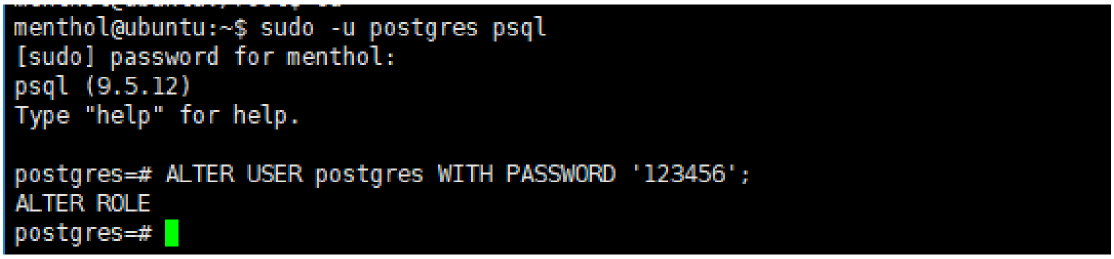
8， 启动界面



```
                                                -Nh`  .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
     `oo/``-hd:  ``                             .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
       .yNmMMh//+syysso-``````                   -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
     .shMMMMN//dmNMMMMMMMMMMMMs`                 `:```-o++++oooo+:/ooooo+:+o+++oooo++/
     `///omh//dMMMMMMMMMMMMMMMN/:::::/+ooso--/ydh//+s+/ossssso:--syN///os:
            /MMMMMMMMMMMMMMMMMMd.                `/++-.-yy/...osydh/-+oo:-`o//...oyodh+
            -hMMmssddd+:dMMmNMMh.                `.-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
            .sMMmo.    -dMd--:mN/`                     ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.........
================================================================================
=====================+--------------------------------+=========================
=====================| Session one died of dysentery. |=========================
=====================+--------------------------------+=========================
================================================================================

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v5.0.0-dev-26bf96b                   ]
+ -- --=[ 1744 exploits - 1001 auxiliary - 302 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ ** This is Metasploit 5 development branch **   ]

msf5 >
```

9，配置 PostgreSQL 数据库，启动并设置密码

启动 sudo -u postgres psql　　设置密码 ALTER USER postgres WITH PASSWORD '123456';



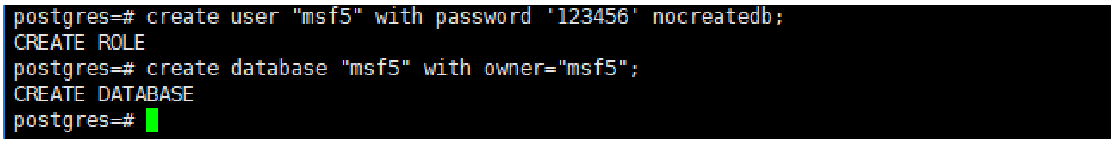
```
menthol@ubuntu:~$ sudo -u postgres psql
[sudo] password for menthol:
psql (9.5.12)
Type "help" for help.

postgres=# ALTER USER postgres WITH PASSWORD '123456';
ALTER ROLE
postgres=#
```

10，　创建新用户和新数据库

create user "msf5" with password '123456' nocreatedb;

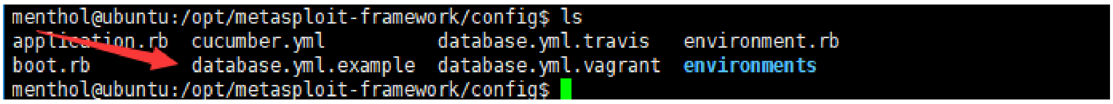
create database "msf5" with owner="msf5";

按\q 退出。

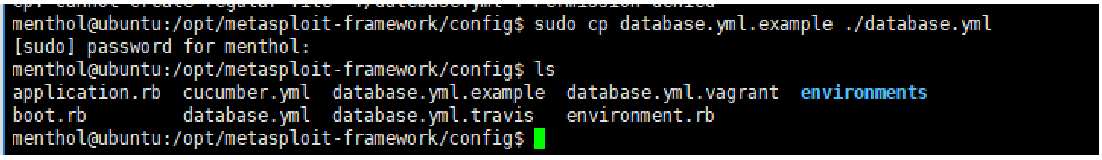


```
postgres=# create user "msf5" with password '123456' nocreatedb;
CREATE ROLE
postgres=# create database "msf5" with owner="msf5";
CREATE DATABASE
postgres=#
```

11，　编辑 database.yml

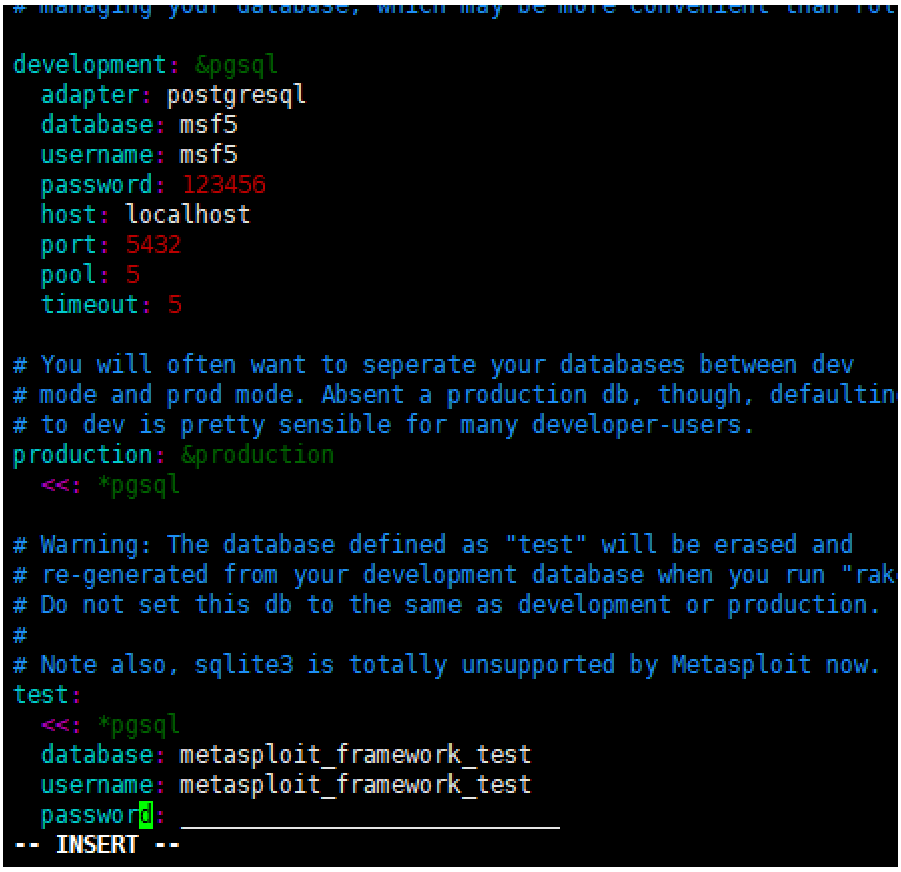


```
menthol@ubuntu:/opt/metasploit-framework/config$ ls
application.rb  cucumber.yml          database.yml.travis   environment.rb
boot.rb         database.yml.example  database.yml.vagrant  environments
menthol@ubuntu:/opt/metasploit-framework/config$
```



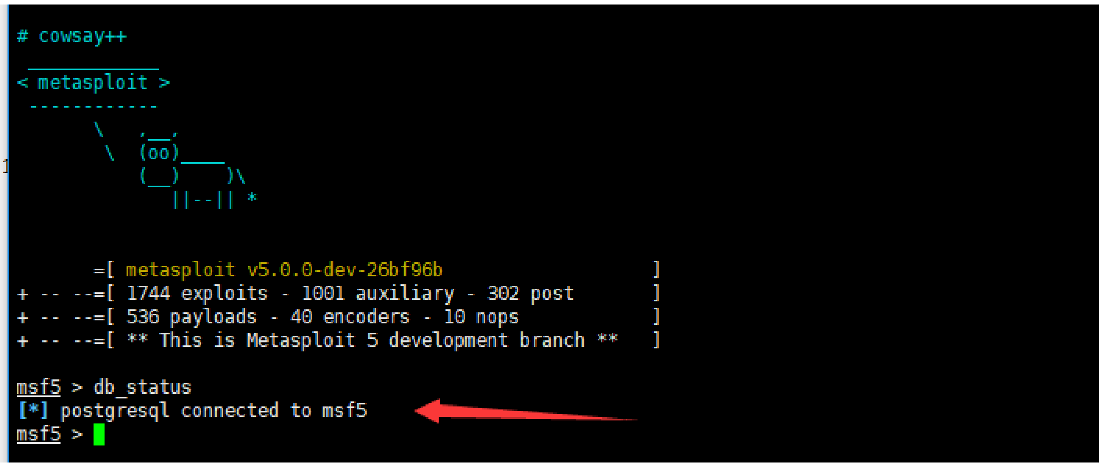
```
menthol@ubuntu:/opt/metasploit-framework/config$ sudo cp database.yml.example ./database.yml
[sudo] password for menthol:
menthol@ubuntu:/opt/metasploit-framework/config$ ls
application.rb  cucumber.yml  database.yml.example  database.yml.vagrant  environments
boot.rb         database.yml  database.yml.travis   environment.rb
menthol@ubuntu:/opt/metasploit-framework/config$
```

按照以下的配置填写



```
# managing your database, which may be more convenient than rol

development: &pgsql
  adapter: postgresql
  database: msf5
  username: msf5
  password: 123456
  host: localhost
  port: 5432
  pool: 5
  timeout: 5

# You will often want to seperate your databases between dev
# mode and prod mode. Absent a production db, though, defaultin
# to dev is pretty sensible for many developer-users.
production: &production
  <<: *pgsql

# Warning: The database defined as "test" will be erased and
# re-generated from your development database when you run "rak
# Do not set this db to the same as development or production.
#
# Note also, sqlite3 is totally unsupported by Metasploit now.
test:
  <<: *pgsql
  database: metasploit_framework_test
  username: metasploit_framework_test
  password: ___________________________
-- INSERT --
```

12，　　保存退出，启动 msf5 查看数据库的连接状态，正常连接。



```
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v5.0.0-dev-26bf96b                  ]
+ -- --=[ 1744 exploits - 1001 auxiliary - 302 post      ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops           ]
+ -- --=[ ** This is Metasploit 5 development branch **  ]

msf5 > db_status
[*] postgresql connected to msf5
msf5 > 
```

---END 2018.03.19