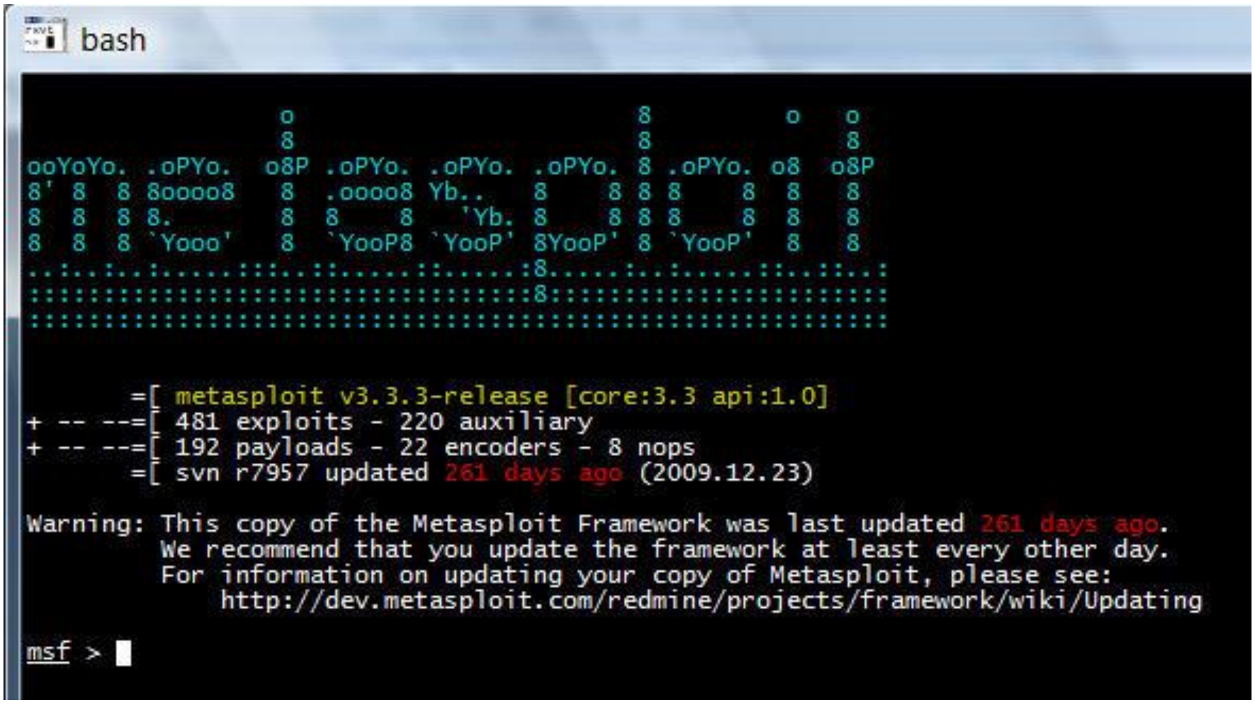
Metasploit Framework



```
                o                       8         o   o
                8                       8             8
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8  8  .oooo8 Yb..   8    8 8 8    8  8   8
8  8  8 8.      8  8    8   'Yb. 8    8 8 8    8  8   8
8  8  8 `Yooo'  8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:.....:::..::.....::.....:8.....:..:.....::..::..:
::::::::::::::::::::::::::::::::::8:::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[ 481 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops
       =[ svn r7957 updated 261 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 261 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
```

Hey all, Today I will be talking about Metasploit Framework. The Metasploit Framework is a modular, Ruby-based penetration testing platform that lets you write, test, and run exploit code. You may use the Metasploit Framework to test security vulnerabilities, enumerate networks, execute attacks, and elude detection. The Metasploit Framework is, at its core, a collection of widely used tools that provide a full environment for penetration testing and exploit creation.

The Metasploit framework is a sophisticated tool that can be used by both cybercriminals and ethical hackers to investigate network and server vulnerabilities. It's easy to customize and use with most operating systems because it's an open-source framework.

Installing Metasploit Framework

- Installing the Metasploit Framework on Unix

Extracting the tarball, shifting into the generated directory, and running your favorite user interface are all it takes to install the Framework. We strongly advise you to use a version of the Ruby interpreter that includes support for the GNU ReadiLine library. If you're running Mac OS X 10.5.1 or earlier, you'll need to install GNU ReadiLine first, then recompile the Ruby interpreter. The console interface can be tab completed if you use a version of Ruby that supports ReadiLine. For regular use, the msfconsole user interface is preferred, however the msfweb user interface might be handy for live demos.

- Installing the Metasploit Framework on Windows

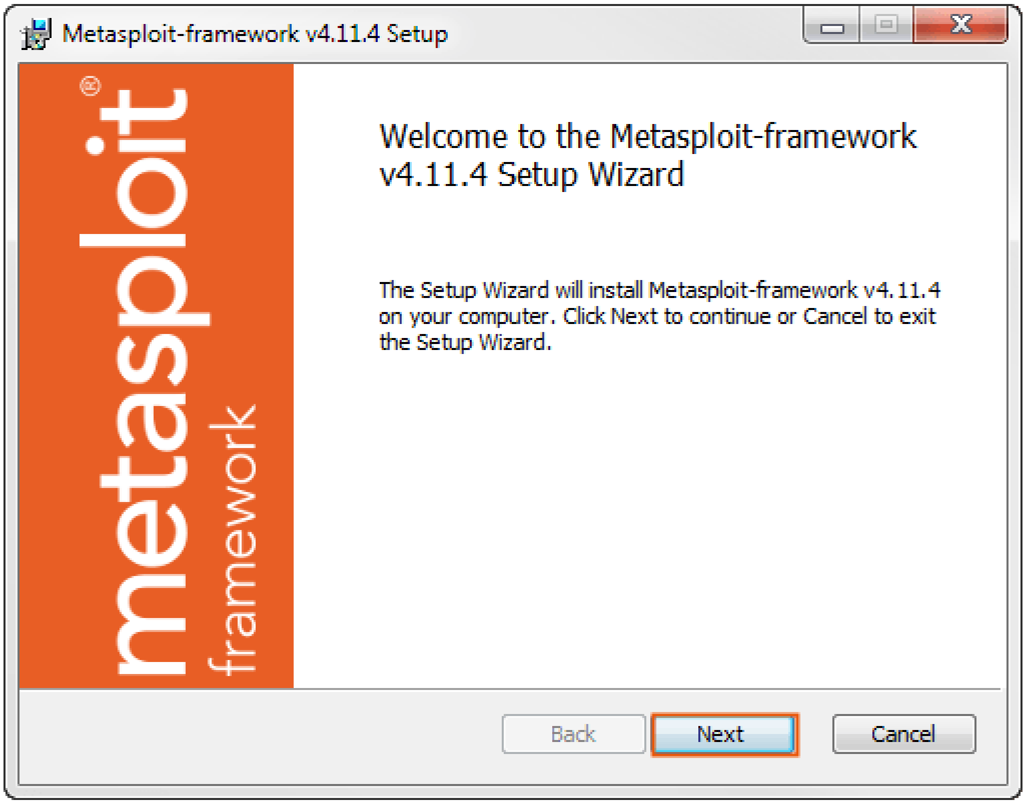
On the Windows platform, the Metasploit Framework is fully supported.

http://framework.metasploit.com/ - Download Link

Download the newest version and do an online update

After you download the installer, locate the file, and double-click the installer icon to start the installation process.

When the Setup screen appears, click Next to continue.

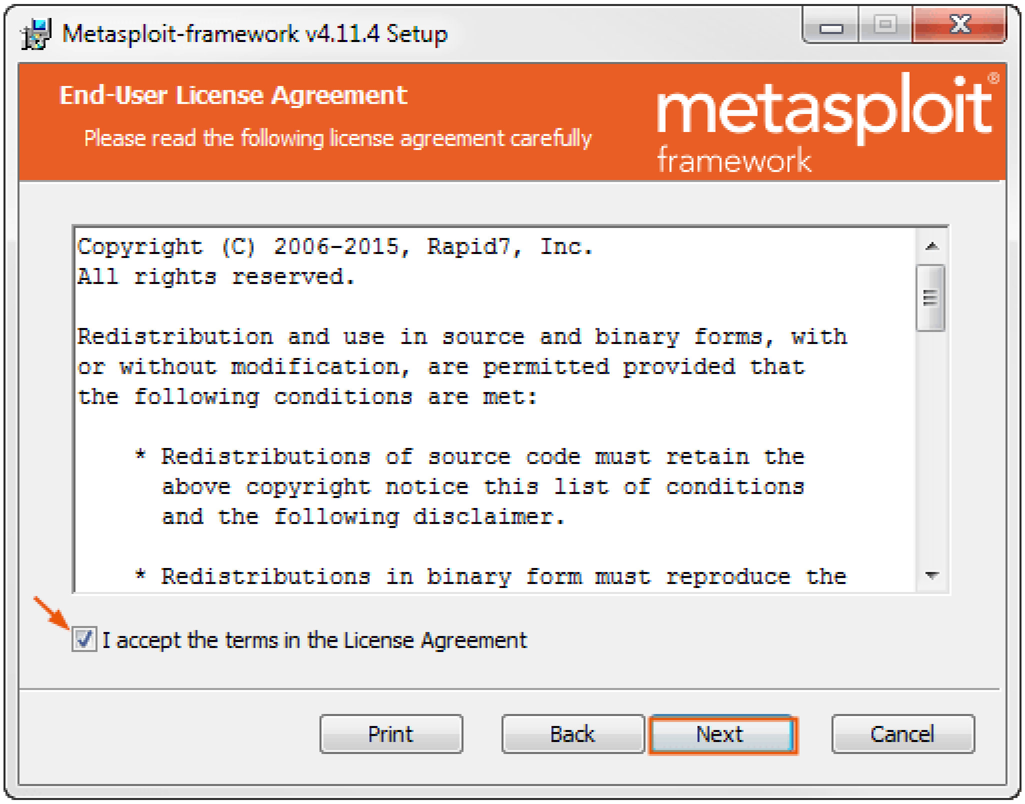


Metasploit-framework v4.11.4 Setup

Welcome to the Metasploit-framework v4.11.4 Setup Wizard

The Setup Wizard will install Metasploit-framework v4.11.4 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Read the license agreement and select the I accept the license agreement option. Click Next to continue.



End-User License Agreement

Please read the following license agreement carefully

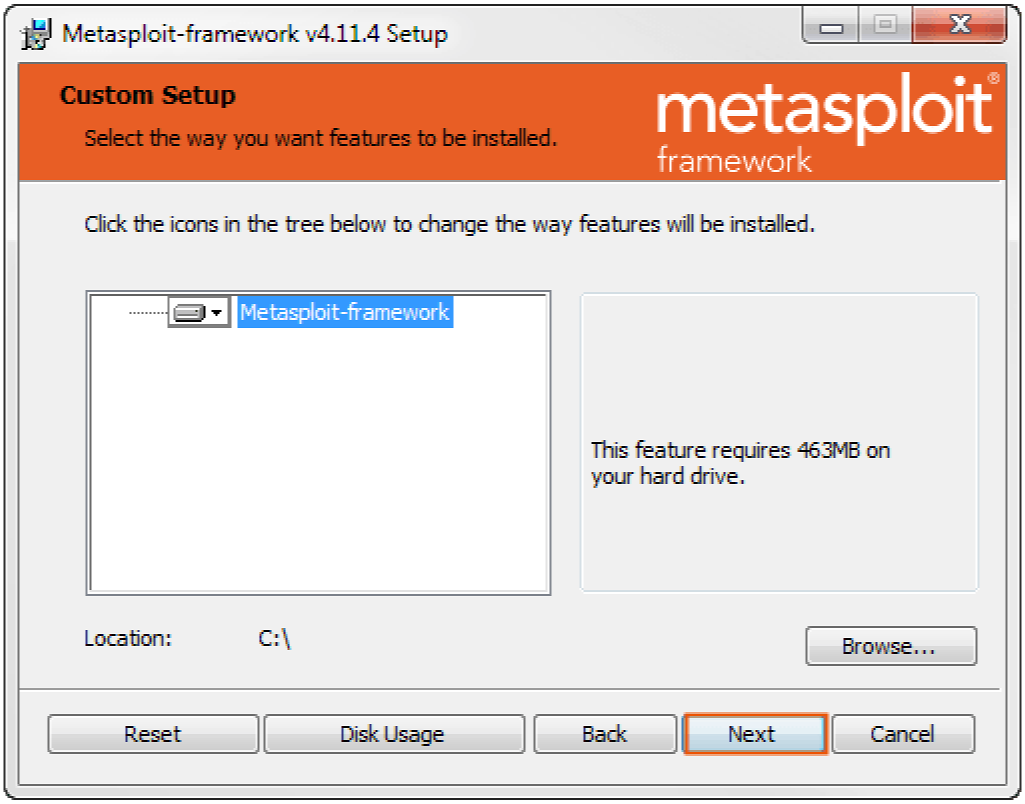
```
Copyright (C) 2006-2015, Rapid7, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with
or without modification, are permitted provided that
the following conditions are met:

    * Redistributions of source code must retain the
      above copyright notice this list of conditions
      and the following disclaimer.

    * Redistributions in binary form must reproduce the
```

☑ I accept the terms in the License Agreement

Browse to the location where you want to install the Metasploit Framework.

By default, the framework is installed on the C:\ Metasploit-framework directory.

Click Next to continue.


Metasploit-framework v4.11.4 Setup

Custom Setup

Select the way you want features to be installed.

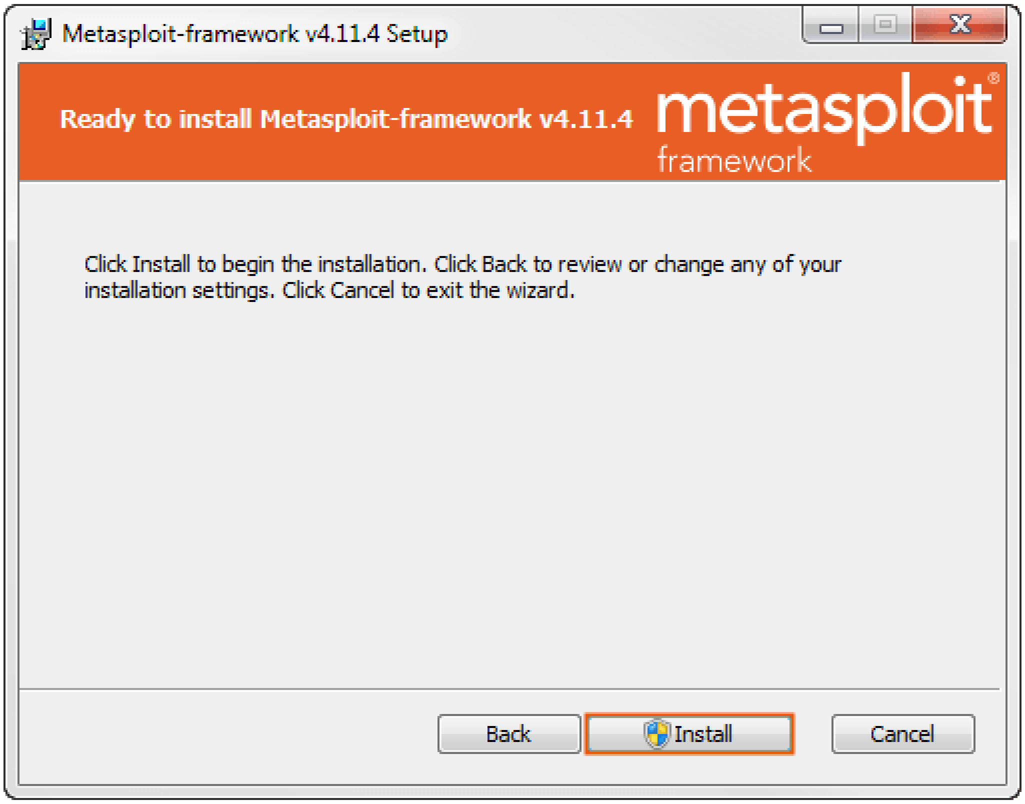
Click the icons in the tree below to change the way features will be installed.

This feature requires 463MB on your hard drive.

Location: C:\

Click Install.

The installation process can take 5-10 minutes to complete. When the installation completes, click the Finish button.



Ready to install Metasploit-framework v4.11.4

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

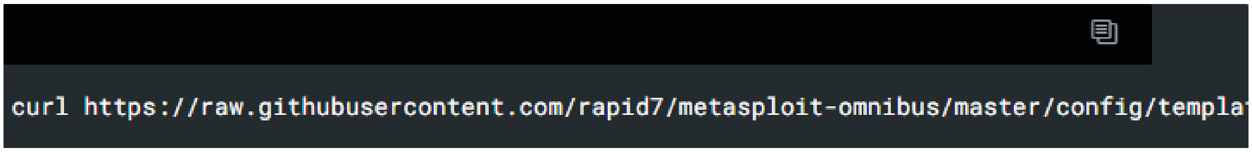
To launch msfconsole after the installation completes, run the following from the command line:

```
$ msfconsole.bat
```

- ## Installing the Metasploit Framework on Linux

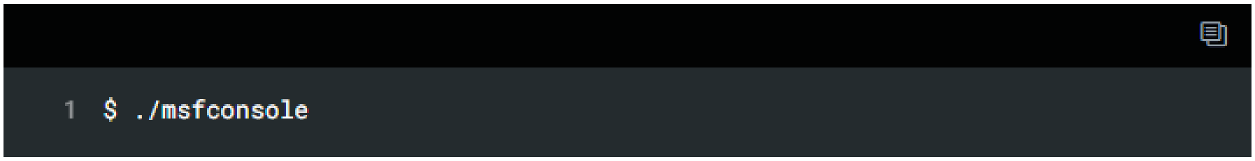
Open the terminal.

Enter the following command to add the build repository and install the Metasploit Framework package:



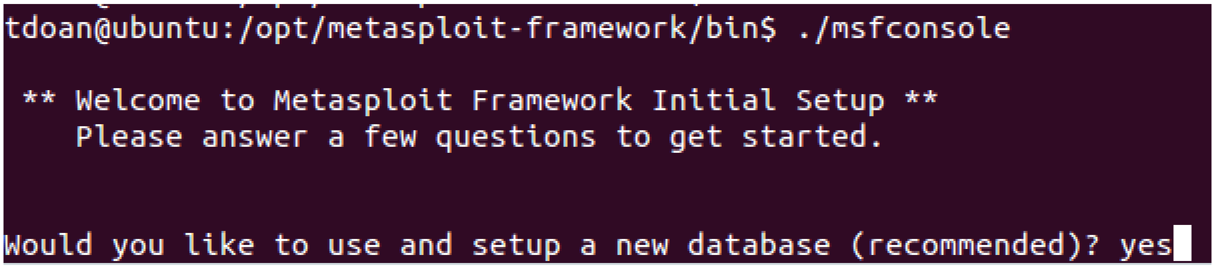
```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templa
```

After the installation completes, open a terminal window, and type the following to start msfconsole:

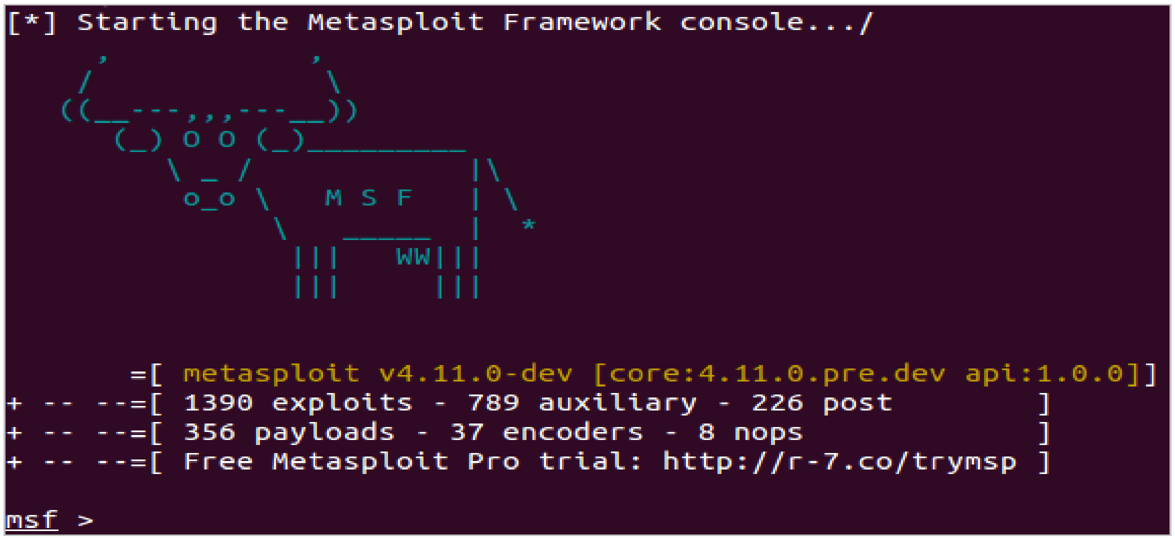


```
$ ./msfconsole
```

The prompt asks you if you want to use and set up a new database. Type y or yes to run the initial configuration script to create the initial database.

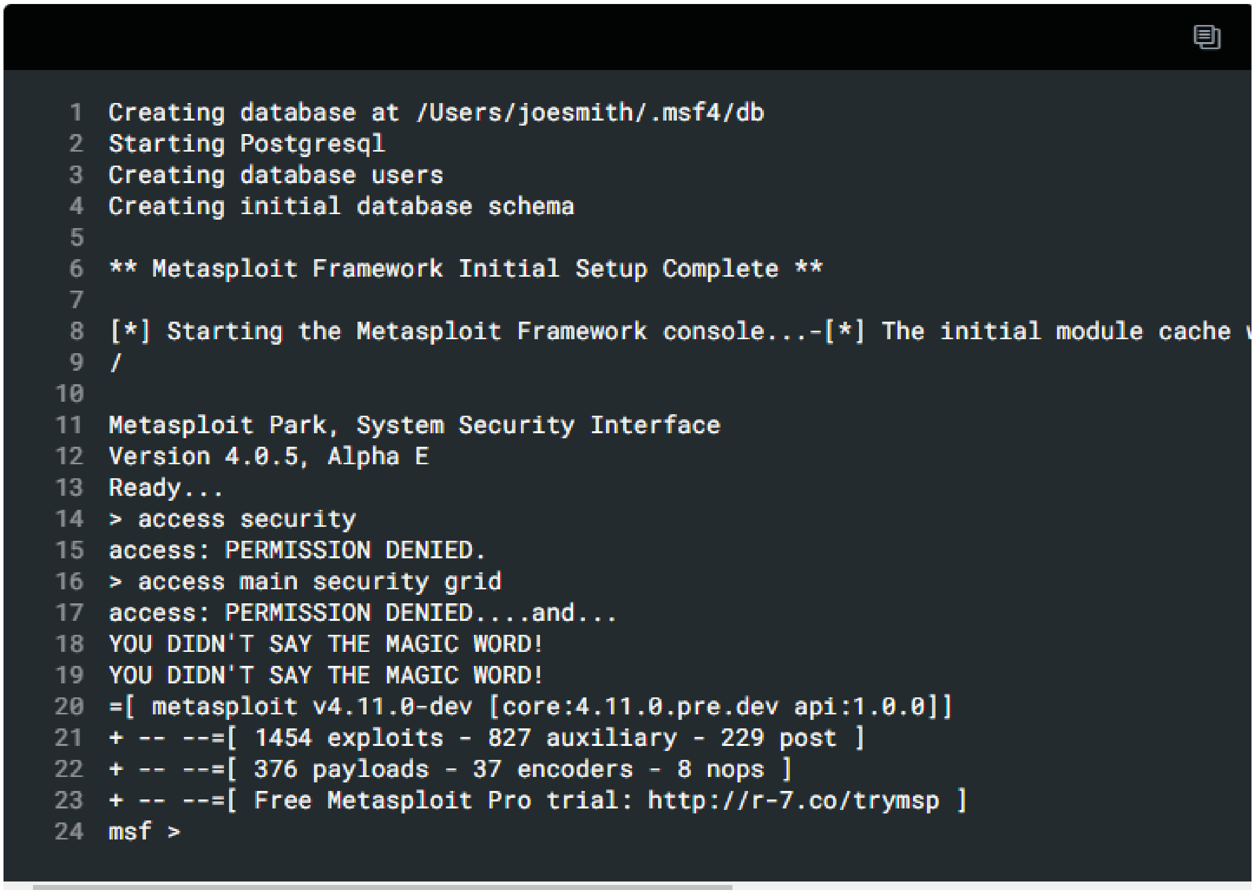


```
tdoan@ubuntu:/opt/metasploit-framework/bin$ ./msfconsole

 ** Welcome to Metasploit Framework Initial Setup **
    Please answer a few questions to get started.


Would you like to use and setup a new database (recommended)? yes
```



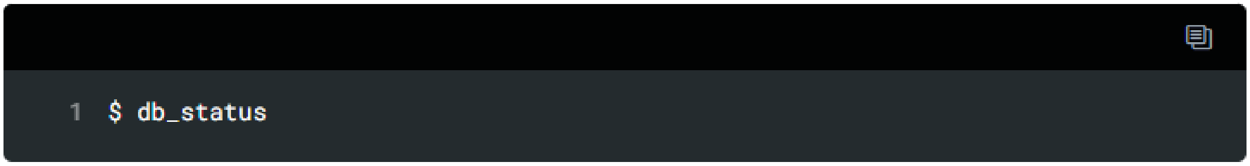
```
[*] Starting the Metasploit Framework console.../
     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

If all goes well, the console starts and displays the following:



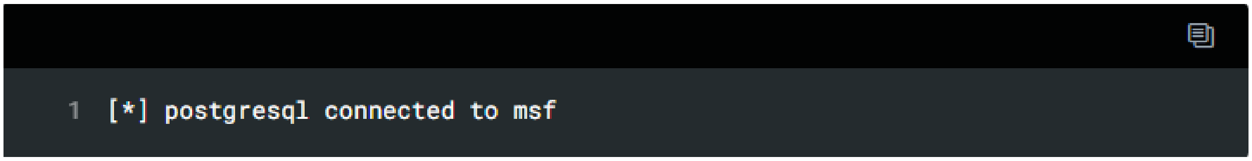
```
Creating database at /Users/joesmith/.msf4/db
Starting Postgresql
Creating database users
Creating initial database schema

** Metasploit Framework Initial Setup Complete **

[*] Starting the Metasploit Framework console...-[*] The initial module cache
/

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
=[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1454 exploits - 827 auxiliary - 229 post ]
+ -- --=[ 376 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf >
```

To check to see if the database was set up, run the following command:



```
$ db_status
```

If the Metasploit Framework successfully connected to the database, the following status displays:



```
[*] postgresql connected to msf
```

Interfaces in Metasploit Framework

1. The Console Interface
   After you've installed the Framework, double-check that everything is operating as it should. The msfconsole user interface is the simplest way to do this. If you're using Windows, open the msfgui interface and go to the Window menu and select the Console link.

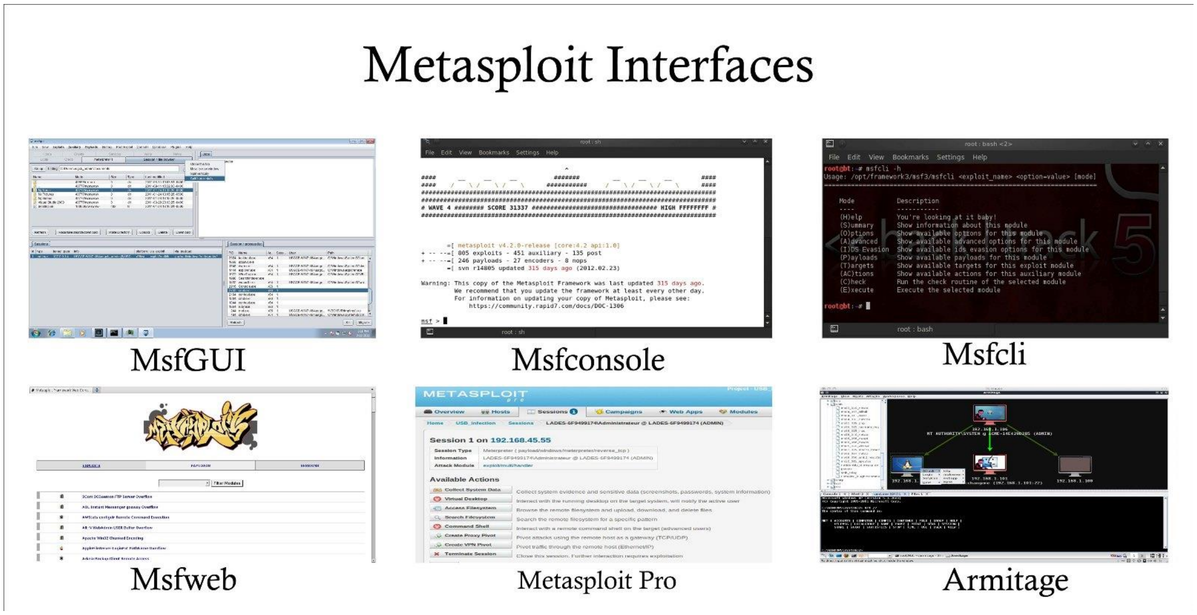
2. The GUI Interface
   The msfgui interface debuted in version 3.1, and it has many new capabilities in addition to the functionality of msfconsole. Select the Console option from the Window menu to enter a msfconsole shell. Enter a string or regular expression in the search field and hit the Find button to find a module within the module tree.

3. The Command Line Interface

   If you want to automate exploit testing or just don't want to use an interactive interface, msfcli could be the answer. The first parameter in this interface is the module name, followed by the options in VAR=VAL format.

4. The Web Interface

   The msfweb interface is based on Ruby on Rails. Start the server with msfweb to have access to this interface. The WEBrick web server is used by the msfweb interface to handle requests. By default, msfweb listens on port 55555 on the loopback address (127.0.0.1). A log message indicating that the service has begun should be displayed.



```
       =[ metasploit v4.2.0-release [core:4.2 api:1.0]
+ -- --=[ 805 exploits - 451 auxiliary - 135 post
+ -- --=[ 246 payloads - 27 encoders - 8 nops
       =[ svn r14805 updated 315 days ago (2012.02.23)

Warning: This copy of the Metasploit Framework was last updated 315 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf >
```

```
root@bt:~# msfcli -h
Usage: /opt/framework3/msf3/msfcli <exploit_name> <option=value> [mode]
==========================================================================

    Mode           Description
    ----           -----------
    (H)elp         You're looking at it baby!
    (S)ummary      Show information about this module
    (O)ptions      Show available options for this module
    (A)dvanced     Show available advanced options for this module
    (I)DS Evasion  Show available ids evasion options for this module
    (P)ayloads     Show available payloads for this module
    (T)argets      Show available targets for this exploit module
    (AC)tions      Show available actions for this auxiliary module
    (C)heck        Run the check routine of the selected module
    (E)xecute      Execute the selected module

root@bt:~#
```

Home › USB_infection › Sessions › LADES-6F9499174\Administrateur @ LADES-6F9499174 (ADMIN)

Session 1 on 192.168.45.55

Session Type	Meterpreter (payload/windows/meterpreter/reverse_tcp)
Information	LADES-6F9499174\Administrateur @ LADES-6F9499174 (ADMIN)
Attack Module	exploit/multi/handler

Available Actions

Collect System Data	Collect system evidence and sensitive data (screenshots, passwords, system information)
Virtual Desktop	Interact with the running desktop on the target system, will notify the active user
Access Filesystem	Browse the remote filesystem and upload, download, and delete files
Search Filesystem	Search the remote filesystem for a specific pattern
Command Shell	Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot	Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot	Pivot traffic through the remote host (Ethernet/IP)
Terminate Session	Close this session. Further interaction requires exploitation

How to Get Metasploit Framework?

Metasploit can be downloaded from the Rapid7 website using open-source installers. In addition to the most recent versions of Chrome, Firefox, and Explorer. The following are the minimal system requirements:

- Operating Systems:
    - Ubuntu Linux 14.04 or 16.04 LTS (recommended)
    - Windows Server 2008 or 2012 R2
    - Windows 7 SP1+, 8.1, or 10
    - Red Hat Enterprise Linux Server 5.10, 6.5, 7.1, or later

- Hardware:
    - 2 GHz+ processor
    - Minimum 4 GB RAM, but 8 GB is recommended
    - Minimum 1 GB disk space, but 50 GB is recommended

Before you begin, make sure your device is free of antivirus and firewall software, and that you have administrative capabilities. When you install the framework, the installer is a self-contained entity that is set up for you. If you need to configure specific dependencies, you can also use the manual installation option. The Metasploit Pro edition is pre-installed with the Kali Linux distribution. The install shield wizard will be used for Windows users.

After installation, upon startup, you'll be faced with these choices:

- Creating database at /Users/joesmith/.msf4/db
- Starting Postgresql
- Creating database users
- Creating an initial database schema

For what this Metasploit Framework use ?

It’s an essential tool for discovering hidden vulnerabilities using a variety of tools and utilities. Metasploit allows you to put yourself in the mind of a hacker and utilize their methods to probe and infiltrate networks and services.

Core components of the Metasploitable Framework

Finding Modules

The Metasploit Framework's fundamental components are modules. A module is a component of software capable of carrying out a certain task, such as scanning or exploiting. Each task that the Metasploit Framework may do is defined by a module. There are a few types of modules. The module type depends on the purpose of the module and the type of action that the module performs.

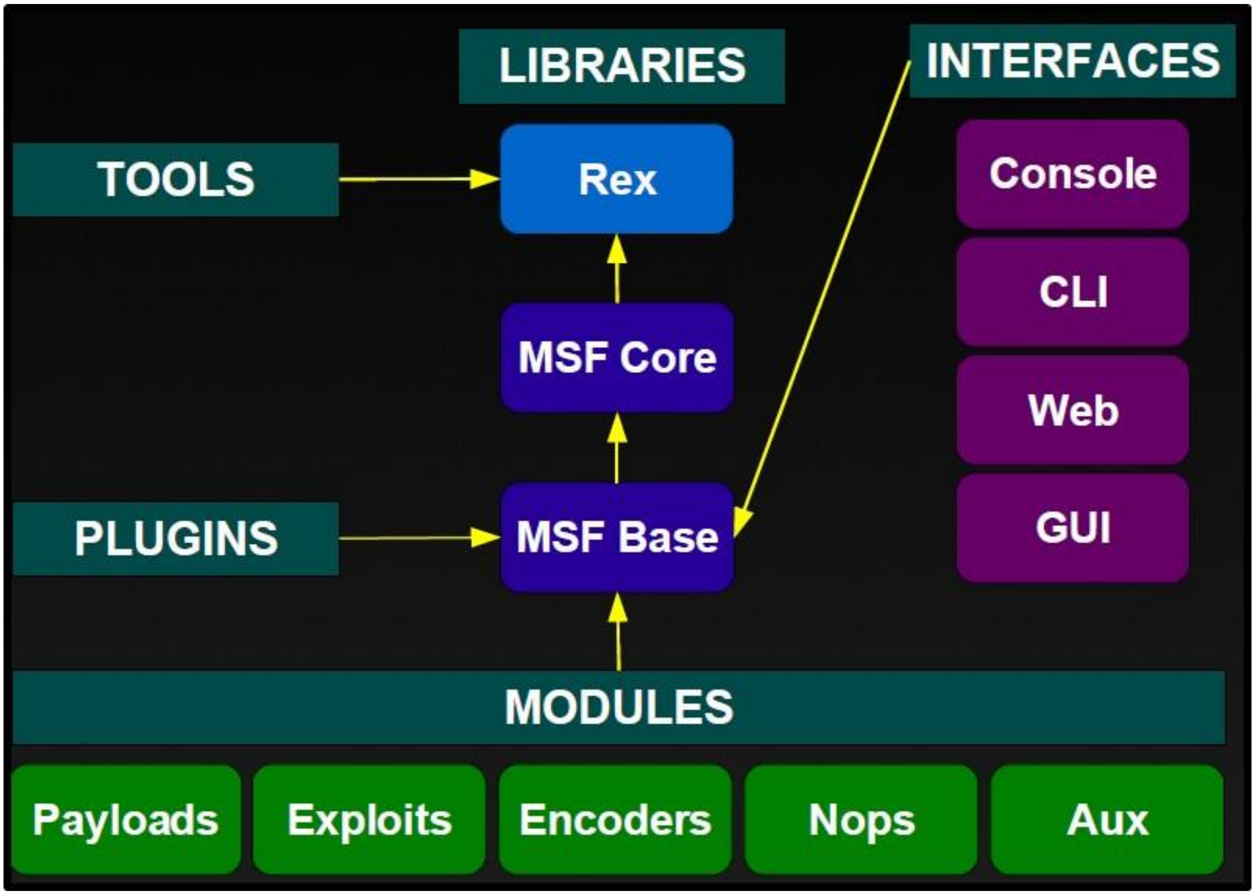
- Exploit
- Auxiliary
- Post-Exploitation
- Payload
- NOP generator

Datastore

The Metasploit Framework's datastore is an essential component. The datastore is a table of named values that allows you to customize the behavior of Metasploit Framework components. The datastore allows interfaces to set parameters, payloads to patch opcodes, and exploits to specify parameters. The datastore also makes it possible for the Metasploit Framework to pass settings across modules internally.

- Global datastore
- Module datastore
- Saved datastore

Metasploit Architecture



Advanced Features

This section goes over some of the more sophisticated features in this edition. These functionalities can be used in any compatible exploit, emphasizing the value of using an exploit framework to write attack code.

1. The Meterpreter
    - The Meterpreter is an advanced multi-function payload that can be dynamically expanded at any moment during operation.

2. PassiveX Payloads
    - Any ActiveX controls can be loaded into a target process using the Metasploit Framework. This feature operates by modifying the target

system's registry and causing the attacked process to open Internet Explorer with a URL that points back to the Framework.

3. Chainable Proxies
   - TCP proxies are transparently supported by the Framework, and handler functions for HTTP CONNECT and SOCKSv4 servers are included in this release. The Proxies environment variable must be set in order to use a proxy with a specific exploit. This variable's value is a comma-separated list of proxy servers, with each server's type:host:port format.

4. Win32 UploadExec Payloads
5. Win32 DLL Injection Payloads
6. VNC Server DLL Injection

We've reached the conclusion of today's session. I hope you enjoy reading it as much as I liked writing it. The tool is described in detail in this article. Now that you've been exposed to this technology, you may utilize your newfound knowledge to begin learning more about it.

“When solving problems, dig at the roots instead of just hacking at the leaves.”

Stay home, stay safe!

Written by Osuni Abeywickrama — 2nd Year 2nd Semester -Cyber Security Student-SLIIT