

Forum:[Hack Forums](#)

Thread: [Metasploit Tutorial 1:Msf Console](#)

Xinapse - March 18, 2010, 10:18 am

Metasploit Tutorial 1:Msf Console

[Download Here](#)

This tutorial will cover all the information needed to find your way around the MSF console.

Part 1: Command List

? - Shows Help Menu

back - Move back from the current context

banner - display the metasploit banner

cd - change the directory

color - toggle color

connect - communicate with a host

exit - exit the console

help - help menu

info - displays information about one or more modules

irb - enter irb scripting mode

jobs - displays and manages jobs

kill - kill a job

load - load a framework plugin

loadpath - Searches and loads modules from a path

quit - exit the console

resource - run the commands stored in a file

route - route traffic through a session

save - saves the active datascores

search - searches the module names and descriptions

sessions - dump session listings and displays info on them

set - Sets a variable to a value

setg - sets a global variable to a value

show - displays modules of a given type, or if not specified , all of them

sleep - do nothing for the specified number of seconds

unload - unload a framework plugin

unset - unsets one or more variables

unsetg - unsets one or more global variables

use - selects a module by name

version - shows the framework version

db_connect - connect to an existing database

db_create - create a new database

db_destroy - delete an existing database

db_disconnect - disconnect from the database

db_driver - specify the database driver

Part 2: Choosing Your Exploit

To do this we will be using the "show" command. So enter in to the console, show exploits

This will return a full list of all the exploits in the database. For example..

```
msf > show exploits
```

Exploits

=====

Name	Description
----	-----
aix/rpc_ttdbserverd_realpath	ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer
Overflow	
bsdi/softcart/mercantec_softcart	Mercantec SoftCart CGI Overflow
-----Cut off point-----	

Once you have found which exploit you want, we will use the "use" command to set it as the exploit. We do this by typing use (exploit name) for example:

```
msf > use hpux/lpd/cleanup_exec
msf exploit(cleanup_exec) >
```

Part 3:Configuring Your Exploit

We now need to configure the exploit to work in the current scenario. So we will do this by using the "show options" command, for example

```
msf exploit(cleanup_exec) > show options
```

Module options:

Name	Current Setting	Required	Description
----	-----	-----	-----
RHOST	yes		The target address
RPORT 515	yes		The target port

Exploit target:

Id	Name
--	----
0	Automatic Target

```
msf exploit(cleanup_exec) >
```

We now need to set the options by using the "set" command, so we will type:
set RHOST 192.168.2.2

We may also other options to our exploit such as payloads. These are chosen in the same way as before. We can view the payloads by typing:

```
show payloads
and then once you have found the correct payload type,
set payload bla,bla,bla
```

Part 4:Exploiting the System

Once you have configured your exploit correctly you simply, type:
exploit
or
run

This will now run your exploit, it may return an error if it is not configured correctly or if the system is not vulnerable, if not congratulations!

Part 5:Finishing Up

Once you have finished with your exploit in the current module, you can simply type
back
and it will return to the original metasploit console.

Part 6: Scripting Mode

You can drop into scripting mode by typing,
irb
Now you can type and execute commands and create scripts!

Xinapse - March 18, 2010, 10:23 am

Yeap i will do a section on that :)

d4t4st34l - March 18, 2010, 10:25 am

thanks i was shearching a tut about it :-D

bikezone - March 18, 2010, 11:15 am

thanks dear its realy very helpful to noobs

imAcarrot - March 18, 2010, 11:33 am

Very nice tutorial Xinapse! Good job!

@@1cu1@te - March 20, 2010, 9:31 pm

This is a good intro for beginners who are trying out metasploit for the first time.

K0FIN - June 25, 2010, 11:18 pm

About fucking time lol

It took me a long time of fucking around to get metasploit for Ubuntu, and I've been needing a tutorial fr the console. Thanks dude. :D

Oh yeah, it would be good to mention nmap in there lol

Prank Calling - June 25, 2010, 11:32 pm

Thank You for this Tut man i have been looking for this.

MainHacker - June 26, 2010, 1:19 am

Thanks :) >:D< .. will help me a lot ;) :D

Xinapse - September 27, 2010, 1:07 pm

No problem glad you enjoyed it :)

