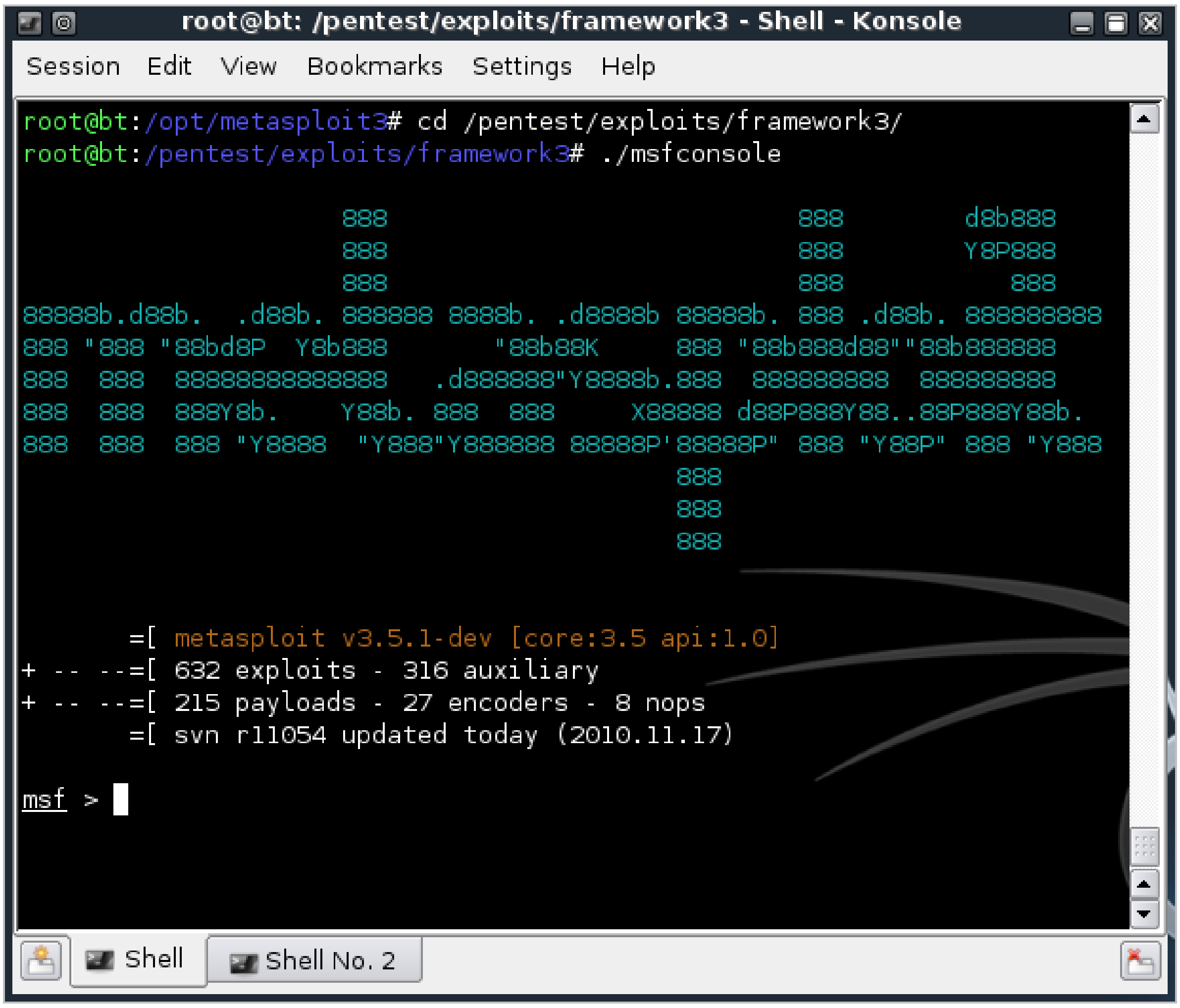
MSFconsole Commands Cheat Sheet

pentestlab.blog/category/general-lab-notes/page/19

March 13, 2012

Here is a list with the most often used commands of Metasploit Framework console.



```
root@bt:/opt/metasploit3# cd /pentest/exploits/framework3/
root@bt:/pentest/exploits/framework3# ./msfconsole

                     888                           888        d8b888
                     888                           888        Y8P888
                     888                           888           888
88888b.d88b.  .d88b. 888888 8888b. .d8888b 88888b. 888 .d88b. 888888888
888 "888 "88bd8P  Y8b888       "88b88K     888 "88b888d88""88b888888
888  888  88888888888888   .d888888"Y8888b.888  888888888  888888888
888  888  888Y8b.    Y88b. 888  888     X88888 d88P888Y88..88P888Y88b.
888  888  888 "Y8888  "Y888"Y888888 88888P'88888P" 888 "Y88P" 888 "Y888
                                           888
                                           888
                                           888


       =[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ -- --=[ 632 exploits - 316 auxiliary
+ -- --=[ 215 payloads - 27 encoders - 8 nops
       =[ svn r11054 updated today (2010.11.17)

msf >
```

Metasploit Framework Console Commands List

show exploits

Show all exploits of the Metasploit Framework

show payloads

Show all payloads

show auxiliary

Show all auxiliary modules of the Metasploit Framework

search *name*

Search for exploits or modules

info

Load information about a specific exploit or module

use *name*

Load an exploit or module

LHOST

Your local IP address if you are on the same network with the target or the public IP address when you are not

RHOST

The IP address of the target

set *function*

Set a specific value (for example RHOST or LHOST)

setg *function*

Set a specific value globally (for example RHOST or LHOST)

show options

Shows the options that are available for module or exploit

show targets

shows which platforms can be attacked by the exploit

set target *num*

specify a target index if you know the OS and the service pack

set payload *payload*

Specify the payload that it will be used

show advanced

Show advanced options

set autorunscript migrate -f

Automatically migrate a separate process upon exploit completion

check

Determine if the target is vulnerable to an attack

exploit

Execute the module or exploit and attack the target

exploit -j

Run the exploit under the context of the job

exploit -z

Do not interact with the session after successful exploitation

exploit -e encoder

specify the payload encoder to use (example:exploit -e shikata_ga_nai)

exploit -h

Display help for the exploit command

sessions -i

List available sessions

sessions -i -v

List all available sessions and show verbose fields,such as which vulnerability was used when exploiting the system

sessions -s *script*

Run a specific Meterpreter script on all Meterpreter live sessions

sessions -K

Kill all live sessions

sessions -c *cmd*

Execute a command on all live Meterpreter sessions

sessions -u *sessionID*

Upgrade a normal Win32 shell to a Meterpreter console

db_create *name*

Create a database to use with database-driven attacks (example:db_create autopwn)

db_connect *name*

Create and connect to a database for driven attacks (example:db_connect autopwn)

db_nmap

Use nmap and place results in database

db_autopwn -h

Display help for using db_autopwn

db_autopwn -p -r -e

Run db_autopwn against all ports found,use a reverse shell and exploit all systems

db_destroy

Delete the current database

db_destroy *user:password@host:port/database*

Delete database using advanced options