Bushra Akter

Class: 15

Terminal

Core Commands

==========

Command	Description
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
debug	Display information useful for debugging
exit	Exit the console
features	Display the list of not yet released features that can be opted in to
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu

```
    history          Show command history
    load             Load a framework plugin
    quit             Exit the console
    repeat           Repeat a list of commands
    route            Route traffic through a session
    save             Saves the active datastores
    sessions         Dump session listings and display information about sessions
    set              Sets a context-specific variable to a value
    setg             Sets a global variable to a value
    sleep            Do nothing for the specified number of seconds
    spool            Write console output into a file as well the screen
    threads          View and manipulate background threads
    tips             Show a list of useful productivity tips
    unload           Unload a framework plugin
    unset            Unsets one or more context-specific variables
    unsetg           Unsets one or more global variables
    version          Show the framework and console library version numbers
```

```
┌──(shariful㉿kali)-[~/Desktop]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands
```

```
  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
```

```
 > access security
 access: PERMISSION DENIED.
 > access security grid
 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!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.32-dev                          ]
+ -- --=[ 2459 exploits - 1266 auxiliary - 430 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > help

Module Commands
===============

    Command           Description
    -------           -----------
```

advanced	Displays advanced options for one or more modules
back	Move back from the current context
clearm	Clear the module stack
favorite	Add module(s) to the list of favorite modules
favorites	Print the list of favorite modules (alias for `show favorites`)
info	Displays information about one or more modules
listm	List the module stack
loadpath	Searches for and loads modules from a path
options	Displays global options or for one or more modules
popm	Pops the latest module off the stack and makes it active
previous	Sets the previously loaded module as the current module
pushm	Pushes the active or list of modules onto the module stack
reload_all	Reloads all modules from all defined module paths
search	Searches module names and descriptions
show	Displays modules of a given type, or all modules
use	Interact with a module by name or search term/index

Job Commands

==========

Command	Description
handler	Start a payload handler as job
jobs	Displays and manages jobs
kill	Kill a job
rename_job	Rename a job

Resource Script Commands

==========

Command	Description
makerc	Save commands entered since start to a file
resource	Run the commands stored in a file

Database Backend Commands

==========

Command	Description
analyze	Analyze database information about a specific address or address range
db_connect	Connect to an existing data service
db_disconnect	Disconnect from the current data service
db_export	Export a file containing the contents of the database
db_import	Import a scan result file (filetype will be auto-detected)
db_nmap	Executes nmap and records the output automatically
db_rebuild_cache	Rebuilds the database-stored module cache (deprecated)
db_remove	Remove the saved data service entry
db_save	Save the current data service connection as the default to reconnect on startup
db_stats	Show statistics for the database
db_status	Show the current data service status
hosts	List all hosts in the database
klist	List Kerberos tickets in the database
loot	List all loot in the database
notes	List all notes in the database

services List all services in the database

vulns List all vulnerabilities in the database

workspace Switch between database workspaces

Credentials Backend Commands

==========

Command Description

------- -----------

creds List all credentials in the database

Developer Commands

==========

Command Description

------- -----------

edit Edit the current module or a file with the preferred editor

irb Open an interactive Ruby shell in the current context

log Display framework.log paged to the end if possible

pry Open the Pry debugger on the current module or Framework

reload_lib Reload Ruby library files from specified paths

time Time how long it takes to run a particular command

DNS Commands

==========

Command Description

------- -----------

dns Manage Metasploit's DNS resolving behaviour

For more info on a specific command, use <command> -h or help <command>.

msfconsole

==========

`msfconsole` is the primary interface to Metasploit Framework. There is quite a lot that needs go here, please be patient and keep an eye on this space!

Building ranges and lists

Many commands and options that take a list of things can use ranges to avoid having to manually list each desired thing. All ranges are inclusive.

Ranges of IDs

Commands that take a list of IDs can use ranges to help. Individual IDs must be separated by a `,` (no space allowed) and ranges can be expressed with either `-` or `..`.

Ranges of IPs

There are several ways to specify ranges of IP addresses that can be mixed together. The first way is a list of IPs separated by just a ` ` (ASCII space),

with an optional `,`. The next way is two complete IP addresses in the form of `BEGINNING_ADDRESS-END_ADDRESS` like `127.0.1.44-127.0.2.33`. CIDR specifications may also be used, however the whole address must be given to Metasploit like `127.0.0.0/8` and not `127/8`, contrary to the RFC. Additionally, a netmask can be used in conjunction with a domain name to dynamically resolve which block to target. All these methods work for both IPv4 and IPv6 addresses. IPv4 addresses can also be specified with special octet ranges from the [NMAP target specification](https://nmap.org/book/man-target-specification.html)

Examples

Terminate the first sessions:

```
    sessions -k 1
```

Stop some extra running jobs:

```
    jobs -k 2-6,7,8,11..15
```

Check a set of IP addresses:

```
    check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255
```

Target a set of IPv6 hosts:

```
    set RHOSTS fe80::3990:0000/110, ::1-::f0f0
```

Target a block from a resolved domain name:

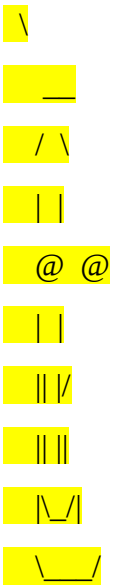
```
   set RHOSTS www.example.test/24
msf6 > hashdump
[-] Unknown command: hashdump. Run the help command for more details.
msf6 > exit

┌──(shariful㉿kali)-[~/Desktop]
└─$ sudo -i
[sudo] password for shariful:
┌──(root㉿kali)-[~]
└─# meterpreter
meterpreter: command not found

┌──(root㉿kali)-[~]
└─# meterpreter
meterpreter: command not found

┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

       _____________________________________
      / it looks like you're trying to run a \
      \ module                               /
       -------------------------------------
              \
```



=[metasploit v6.4.32-dev]

+ -- --=[2459 exploits - 1266 auxiliary - 430 post]

+ -- --=[1471 payloads - 49 encoders - 11 nops]

+ -- --=[9 evasion]