Cheatography

Metasploit 4.5.0-dev.15713 Cheat Sheet by TerrorByte (huntereight) via cheatography.com/1810/cs/560/

Database Commands	
Connect	db_connect
Disconnect	db_disconnect
Export Database	db_export
Import Scan Result	db_import
Status of Database	db_status
Display Hosts	hosts
Display Loot	loot
Display Notes	notes
Display Services	services
Display Vulnerabilities	vulns
Switch Between Workspaces	workspace
NMAP Scan into Database	db_nmap

Core Commands	
Display Help	? or help
Go Back	back
Change Directory	cd
Toggle Color	color
Communicate with a Host	connect
Exit Metasploit	exit
Display Info of Module	info
Go into irb	irb
Display and Manage Jobs	jobs
Stop a Job	kill
Load a Plugin	load
Load a Plugin from Path	loadpath
Print Commands Entered to a Path	makerc
Set Previous Module as Current Module	previous
Pops the Latest Module Off of the Module Stack and Makes it Active	popm
Pushes the Active or List of Modules onto the Module Stack	pushm
Quit the Console	quit
Run Commands Stored in a File	resource

Core Commands (cont)	
Route Traffic Through a	route
Connection	
Save Datastores	save
Search for Modules	search
Dump Session Listings and Display Information about Sessions	sessions
Set Variable of a Module	set
Set a Global Variable	setg
Display Modules of a Type, or All Modules	show
Do Nothing for X Seconds	sleep
Write All Output to a Files	spool
Manipulate Threads	threads
Unload a Plugin	unload
Unset a Variable	unset
Unset a Global Variable	unsetg
Use a Module (by Name)	use
Show Metasploit Info	version

Meterpreter Core and File System	
Background the Current Session	background
Kill a Background Meterpreter Script	bgkill
Displays Info About Active Channels	channel
Close a Channel	close
Disables Encoding of Unicode Strings	disable_unicode_e ncoding
Enable Encoding of Unicode Strings	enable_unicode_e ncoding
Exit Meterpreter Shell	exit
Display Help	help
Display Info About Active Post Module	info
Interact with a Channel	interact
Drop into irb Scripting Mode	irb

Load One or More Meterpreter ExtensionsloadMigrate the Server to Another ProcessmigrateTerminate the Meterpreter SessionsquitReads Data from a ChannelreadRun the Commands Stored in a FileresourceExecutes a Meterpreter Script or Post ModulerunWrite Data to a ChannelwriteRead the Contents of a File to the ScreencatChange DirectorycdDownload File to Your ComputerdownloadEdit a FileeditPrint Local Working DirectorygetlwdPrint Working DirectoryIcdDirectoryIpwdList FilesIsMake DirectorypwdDelete the Specified FilermRemove Directoryrmdir	Meterpreter Core and File System	(cont)
Terminate the Meterpreter Sessions Reads Data from a Channel read Run the Commands Stored in a File Executes a Meterpreter Script or Post Module Write Data to a Channel write Read the Contents of a File to the Screen Change Directory cd Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory lcd Change Local Working Directory lpwd List Files Is Make Directory pwd Delete the Specified File read	•	load
Reads Data from a Channel read Run the Commands Stored in a File Executes a Meterpreter Script or Post Module Write Data to a Channel write Read the Contents of a File to the Screen Change Directory cd Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory getwd Change Local Working Directory lpwd List Files Is Make Directory pwd Delete the Specified File run read read read read resource read read resource run existency guite Locat run Print Local Working Directory pwd List Files Is		migrate
Run the Commands Stored in a File Executes a Meterpreter Script or Post Module Write Data to a Channel write Read the Contents of a File to the Screen Change Directory cd Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory lcd Change Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File run	·	quit
File Executes a Meterpreter Script or Post Module Write Data to a Channel write Read the Contents of a File to the Screen Change Directory cd Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory getwd Change Local Working Directory lcd Directory Print Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Reads Data from a Channel	read
Post Module Write Data to a Channel write Read the Contents of a File to the Screen Change Directory cd Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory getwd Change Local Working Directory lcd Directory Print Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File rm		resource
Read the Contents of a File to the Screen Change Directory cd Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory getwd Change Local Working Directory lcd Directory Print Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	, ,	run
the Screen Change Directory cd Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory getwd Change Local Working Directory lcd Directory Print Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Write Data to a Channel	write
Download File to Your Computer download Edit a File edit Print Local Working Directory getlwd Print Working Directory getwd Change Local Working lcd Directory Print Local Working Directory lpwd List Files Is Make Directory mkdir Print Working Directory pwd Delete the Specified File rm		cat
Edit a File edit Print Local Working Directory getlwd Print Working Directory getwd Change Local Working lcd Directory Print Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Change Directory	cd
Print Local Working Directory getlwd Print Working Directory getwd Change Local Working lcd Directory Print Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Download File to Your Computer	download
Print Working Directory getwd Change Local Working lcd Directory Print Local Working Directory lpwd List Files ls Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Edit a File	edit
Change Local Working Directory Print Local Working Directory List Files Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Print Local Working Directory	getlwd
Directory Print Local Working Directory Ipwd List Files Is Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Print Working Directory	getwd
List Files Is Make Directory mkdir Print Working Directory pwd Delete the Specified File rm		lcd
Make Directory mkdir Print Working Directory pwd Delete the Specified File rm	Print Local Working Directory	lpwd
Print Working Directory pwd Delete the Specified File rm	List Files	Is
Delete the Specified File rm	Make Directory	mkdir
·	Print Working Directory	pwd
Remove Directory rmdir	Delete the Specified File	rm
	Remove Directory	rmdir
Search for Files search	Search for Files	search
Upload File to Target upload	Upload File to Target	upload



By **TerrorByte** (huntereight) cheatography.com/huntereight/

Published 5th September, 2012. Last updated 5th September, 2012. Page 1 of 2. Sponsored by **CrosswordCheats.com** Learn to solve cryptic crosswords! http://crosswordcheats.com



Metasploit 4.5.0-dev.15713 Cheat Sheet by TerrorByte (huntereight) via cheatography.com/1810/cs/560/

Meterpreter User Interface Commands	
List All Accessible Desktops and Window Stations	enumdeskt ops
Get the Current Meterpreter Desktop	getdesktop
Display the Amount of Time the User has been Idle	idletime
Start Capturing Keystrokes	keyscan_st art
Stop Capturing Keystrokes	keyscan_st op
Dump the Keystroke Buffer	keyscan_d ump
Screenshot of the GUI	screenshot
Change the Meterpreters Current Desktop	setdesktop
Control Some of the User Interface Components	uictl

Meterpreter System Commands	
Clear the Event Log	clearev
Relinquishes Any Active Impersonation Token	drop_token
Execute a Command	execute
Get the Current Process Identifier	getpid
Attempt to Enable All Privileges Available to the Current Process	getprivs
Get the User that the Server is Running as	getuid
Terminate a Process	kill
List Running Processes	ps
Reboots the Remote Computer	reboot
Interact with the Remote Registry	reg
Calls RevertToSelf() on the Remote Machine	rev2self
Drop into a System Command Shell	shell

Meterpreter System Commands (c	ont)
Shuts Down the Remote Computer	shutdown
Attempt to Steal an Impersonation Token from the Process	steal_toke n
Gets Information About the Remote System	sysinfo

Meterpreter Priv Commands	
List Webcams	webcam_li st
Take a Snapshot from the Specified Webcam	webcam_s nap
Attempt to Elevate your Priviledge to that of Local System	getsystem
Dumps the Contents of the SAM Database	hashdump
Manipulate MACE Attributes	timestomp

