Metasploit Cheat Sheet

comparitech

Framework Components

Metasploit Meterpreter	Run as a DLL injection payload on a target PC providing control over the target system
Metasploit msfvenom	Help create standalone payloads as executable, Ruby script, or shellcode

Networking commands

ipconfig:	Show network interface configuration
portfwd:	Forward packets
route:	View / edit network routing table

Meterpreter commands

Basic and file handling commands

sysinfo	Display system information
ps	List and display running processes
kill (PID)	Terminate a running process
getuid	Display user ID
upload or download	Upload / download a file
pwd or lpwd	Print working directory (local / remote)
cd or lcd	Change directory (local or remote)
cat	Display file content
bglist	Show background running scripts
bgrun	Make a script run in background
Bgkill	Terminate a background process
background	Move active session to background
edit <FILE Name>	Edit a file in vi editor
shell	Access shell on the target machine
migrate <PID>	Switch to another process
idletime	Display idle time of user
screenshot	Take a screenshot
clearev	Clear the system logs
? or Help	Shoes all the commands
exit / quit:	Exit the Meterpreter session
shutdown / reboot	Restart system
use	Extension load
channel	Show active channels

Process handling commands

Command	Description
getpid:	Display the process ID
getuid:	Display the user ID
ps:	Display running processes
kill:	Stop and terminate a process
getprivs	Shows multiple privileges as possible
reg	Access target machine registry
Shell	Access target machine shell
execute:	Run a specified
migrate:	Move to a given destination process ID

Interface / output commands

enumdesktops	Show all available desktops
getdesktop	Display current desktop
keyscan_start	Start keylogger in target machine
keyscan_stop	Stop keylogger in target machine
set_desktop	Configure desktop
keyscan_dump	Dump keylogger content

Password management commands

hashdump	Access content of password file - Hash file

Msfvenom command options

Switch	Syntax	Description
-p	-p (Payload option)	Display payload standard options
-l	-l(list type)	List module type i.e payloads, encoders
-f	-f (format)	Output format
-e	-e(encoder)	Define which encoder to use
-a	-a (Architecture or platform	Define which platform to use
-s	-s (Space)	Define maximum payload capacity
-b	-b (characters)	Define set of characters not to use
-i	-i (Number of times)	Define number of times to use encoder
-x	-x (File name)	Define a custom file to use as template
-o	-o (output)	Save a payload
-h	-h	Help