Cheatography

Metasploit Mystery Cheat Sheet

by matsho via cheatography.com/27317/cs/7817/

MSFConsole Basics

msf > help	Help menu
msf > back	Move back from the current context
msf > exit	Exit the console
msf > search [regex]	Searches module names and descriptions
msf > use exploit/[exploitpath]	Specify exploit to use
msf > show options	Shows options for the current module
msf > set [option] [value]	Sets a context-specific variable to a value. E.g. set RHOST 10.201.84.110
msf > set payload [payloadpath]	Specify a payload to use
msf > exploit	Start exploit
msf > grep	Grep the output of another command

Meterpreter Commands

? / help	Display a summary of commands
<Ctrl + Z> / background	Backgrounds the meterpreter session
exit / quit	Exit the meterpreter session
sysinfo	Show the system name and OS type
cd	Change directory
lcd	Change directory on local (attacker's) computer
ls	Show contents of directory
download / upload	Move files to/from target machine
edit	Open a file in the default editor

Note:
'meterpreter >' will be the terminal context for all these commands, not 'msf >'

MSFConsole Sessions

msf > sessions -h	Display help
msf > sessions -l	List all backgrounded sessions
msf > session -i [SessionID]	Interact with backgrounded session
<Ctrl+Z>	Background the current interactive session
msf > exploit -z	Run the exploit expecting a single session that is immediately backgrounded
msf > exploit -j	Run the exploit in the background expecting one or more sessions that are immediately backgrounded
msf > sessions -u	Upgrade a shell to a meterpreter session

nmap (a very small subset of available options)

-h	Displays help information
-sV	Probe open ports to determine service/version info
-p <port ranges>	Only scan specified ports

Example usage:
nmap -sV -p0-3000 10.201.84.110
Type 'nmap -h' or 'man nmap' for extended help

By **matsho**
cheatography.com/matsho/

Published 13th April, 2016.
Last updated 13th April, 2016.