Metasploit

Basic Commands:

Task	Command
Start Metapsloit	msfconsole
Search Modules	search [QUERY]
Exit Metasploit	exit
Select a module	use [MODULE]

Example:

```
use exploit/windows/smb/ms17_010_eternalblue
```

or:

```
use 1
```

Module Information

Task	Command
Display info about a specific module	info
List module options you can set	options
Show advanced options for a module	advanced
Show options in a specific category	show

Setting Module Options

Task	Command
Set module options	set [OPTION NAME] [VALUE]
Set target host(s)	set RHOSTS [IP]
Set target port	set RPORT [PORT NO]
Set the architecture of the target	arch
Set the payload to be sent to target	set payload [PAYLOAD NAME]

Running the module

Task	Command

Task	Command
Run the exploit	exploit
Run the exploit in the background	exploit -j
Run the exploit and background session	exploit -z

Sessions

Task	Command
List all sessions	sessions
Interact with a session	session -i [Session No]

Meterpreter

Task	Command
Download files from the target	download [FILE NAME]
Upload files to the target	upload [FILE NAME]
List all the running processes	ps
Change your process	migrate
List files in current directory	ls
Execute a command on the remote host	execute
Start an interactive shell on remote host	shell
Get the contents of a file	cat
Put the meterpreter shell in the bg	background
Dump the user account hashes	hashdump
Run the privilege escalation module	use priv