Medusa — Professional Cheat Sheet

> **One-page professional reference** for **Medusa** — speedy, parallel, modular login brute-forcer. Commands, flags, examples, tuning, and OPSEC notes for red-team and pentest use.

---

1) At-a-glance

- **Tool:** Medusa — parallel network login auditor (author: JoMo-Kun).
- **Primary uses:** Online password guessing against network services (SSH, FTP, RDP, SMB, HTTP auth, MSSQL, MySQL, POP3, IMAP, SMTP, and many others via modules).
- **Design:** Thread-based, module architecture (`*.mod`), flexible input (single entry, files, combo files).

---

2) Install / quick check

```
# Debian / Kali
sudo apt update && sudo apt install medusa

# From source
git clone https://github.com/jmk-foofus/medusa.git
cd medusa
./configure && make && sudo make install

# Quick help
medusa -h
```

---

3) Basic syntax

```
medusa [-h host|-H hostfile] [-u user|-U userfile] [-p pass|-P passfile] [-C
combofile] -M module [OPTIONS]
```

- `-M` selects the module (service) to test — **without** the `.mod` extension.

---

4) Core options (essentials)

- `-h TEXT` : target hostname or IP.

- `-H FILE` : file containing target hosts (one per line).
- `-u TEXT` : single username.
- `-U FILE` : username file.
- `-p TEXT` : single password.
- `-P FILE` : password file.
- `-C FILE` : combo file (user:pass entries).
- `-M TEXT` : module/service to use (e.g., `ssh`, `ftp`, `rdp`).
- `-n NUM` : non-default TCP port number.
- `-s` : enable SSL/TLS (if module supports it).
- `-g NUM` : give up after trying to connect for NUM seconds (connect timeout, default 3).
- `-r NUM` : sleep NUM seconds between retry attempts (default 3).
- `-R NUM` : attempt NUM retries before giving up (total attempts = NUM + 1).
- `-t NUM` : total number of logins to test concurrently (threads for login attempts).
- `-T NUM` : total number of hosts to test concurrently (scale across hosts).
- `-L` : parallelize by assigning one username per thread (alternative threading model).
- `-f` : stop scanning host after first valid credential found.
- `-F` : stop audit after first valid credential found on any host.
- `-O FILE` : append log info to FILE.
- `-d` : dump all known modules.
- `-q` : display module usage/help.
- `-v NUM` : verbosity (0–6).
- `-w NUM` : error debug level (0–10).
- `-Z TEXT` : resume scan from a saved map.

---

5) Module examples (common targets)

- `ssh`, `ftp`, `telnet`, `smtp`, `pop3`, `imap`, `http`, `http_form`, `mssql`, `mysql`, `rdp`, `smb`, `vnc`, `postgres`, `oracle` (support varies by build & version).
- Use `medusa -d` to list installed modules on your binary.

---

6) Practical examples

6.1 Single host, single username, password list (FTP)

```
medusa -h 192.168.1.50 -u alice -P /usr/share/wordlists/rockyou.txt -M ftp -t 6
-f
```

6.2 Multiple hosts, username list, password list (parallel)

```
medusa -H hosts.txt -U users.txt -P pass.txt -M ssh -T 10 -t 20 -F -O medusa.log
```

- `-T 10` tests up to 10 hosts concurrently; `-t 20` runs 20 login threads total.

6.3 Use non-default port and SSL

```
medusa -h target -u admin -P pass.txt -M http_form -n 8443 -s
```

6.4 Combo file (user:pass entries)

```
medusa -h 10.0.0.5 -C combos.txt -M smb -t 10
```

6.5 Resume a previous scan

```
medusa -h 10.0.0.0/24 -U users.txt -P pass.txt -M ftp -Z medusa.map
```

---

7) Tuning for effectiveness & stealth

- **Threading:** Lower `-t` and `-T` to reduce load/noise for targets with lockouts or IDS.
- **Retries/timeouts:** increase `-g`, `-r`, and `-R` for unstable networks; decrease for speed when reliable.
- **Parallelization mode:** use `-L` when you want one username per thread (helps with some services).
- **Stop flags:** `-f` / `-F` quickly reduce noise once a valid credential is discovered.
- **Module tuning:** use module `-m` option(s) to pass module-specific parameters (e.g., target domain or extra flags) — see module help with `-q`.

---

8) Logging, output & reporting

- Use `-O logfile` to append structured logs.
- Capture terminal output and `-O` logs for evidence and reporting.
- Combine with `tee` and timestamped filenames for audit trails.

---

9) Troubleshooting & common pitfalls

- `-e` **extra checks:** `-e n/s/ns` controls trial of no-password or username==password checks (where supported).
- **Module missing:** ensure your medusa build includes the module required; run `medusa -d` to inspect available modules.
- **Lockouts & rate limits:** slow down threads or add sleeps; coordinate with target owner.

- **False positives:** verify credentials manually after discovery; some services may accept partial auth or behave unusually.

---

10) OPSEC & legal (must read)

- Only use Medusa against systems you own or have explicit, written permission to test.
- Brute-force testing generates noisy logs and can trigger account lockouts or service disruption — coordinate with stakeholders and defenders.
- Store discovered credentials securely and include them in reports with minimal exposure (redact in public artifacts).

---

11) Quick one-liners (copy-paste)

```
# Fast FTP check (stop at first success)
medusa -h 10.0.0.5 -u admin -P /path/rockyou.txt -M ftp -t 8 -f

# Multi-host SSH test with userlist + passlist
medusa -H hosts.txt -U users.txt -P pass.txt -M ssh -T 20 -t 40 -F -O
medusa_results.log

# Use combo file against SMB
medusa -h target -C combos.txt -M smb -t 10
```

---

12) Alternatives & when to use them

- **Hydra:** broader community examples and active maintenance; similar feature set.
- **Ncrack:** modern redesign focused on speed & parallelism (Nmap project).
- **Custom scripts:** use when specific authentication flows or rate controls are required.

This cheat sheet is intended for authorized penetration testing and defensive assessments only.