Hydra Cheat Sheet

Installation

```
sudo apt install hydra

sudo snap install seclists
```

Basic Usage

Command	Description
hydra <target> <service>	Brute-force a single host
hydra -h	Show help message
hydra <service> -U	Show service module usage

Target specification

Option	Description
<target> <service>	Target host and service
<service>://<host>	Target host and service
-s <port>	Target port
-M <file>	Load targets from a file

Common services

Service	Description
http[s]-{head|get|post}	Basic HTTP(S) authentication
http[s]-{get|post}-form	HTTP(S) login form
ftp[s]	FTP login
ssh	SSH login
mongodb	MongoDB
mysql	MySQL
postgres	PostgreSQL
redis	Redis

Use hydra -h to see a full list of supported services.

Username and password specification

Flag	Description
-l <username>	Login with username
-L <file>	Load usernames from a file
-p <password>	Try password
-P <file>	Load passwords from a file
-C <file>	Load usernames and passwords from a file ("login:password")

Brute force password generation

Option	Description
-x 3:5:a	Generate passwords of 3 to 5 lowercase letters
-x 5:8:A1	Generate passwords of 5 to 8 uppercase letters and numbers

Output

Option	Descripton
-o <file>	Write found login/password combinations to file
-b <format>	Switch between text, json or jsonv1
hydra -v	Verbose mode
hydra -V	Show all attempts

Performance

Flag	Description
-u	Loop around users, not passwords
-f	Exit after first match

Examples

```
hydra -l admin -P passwords.txt <target> http-get
/admin

hydra -l admin -P passwords.txt <target> https-post-
form
"/login.php:username=^USER^&password=^PASS^:F=incorr
ect"

hydra -L users.txt -P passwords.txt -u -f
ssh://<target> -t 4

hydra -l admin -P passwords.txt ftp://<target>
```

Personalized wordlists

Command	Description
sudo apt install cupp	Install CUPP
cupp -i	Create a custom wordlist interactively