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

For this deployed machine, here are the commands to use Hydra on SSH and a web form (POST method).

SSH

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

hydra -l <username> -P <full path to pass> MACHINE\_IP -t 4 ssh

For example, hydra -l root -P passwords.txt MACHINE\_IP -t 4 ssh will run with the following arguments:

* Hydra will use root as the username for ssh
* It will try the passwords in the passwords.txt file
* There will be four threads running in parallel as indicated by -t 4

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. You can use your browser’s network tab (in developer tools) to see the request types or view the source code.

sudo hydra <username> <wordlist> MACHINE\_IP 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 |
| <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> MACHINE\_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V

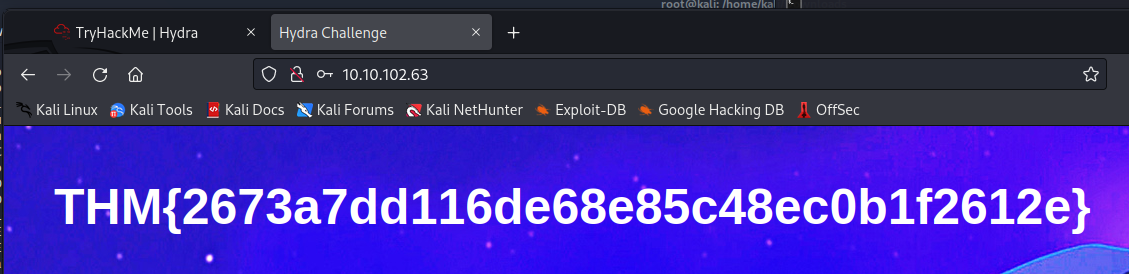
* The login page is only /, i.e., the main IP address.
* The username is the form field where the username is entered
* The specified username(s) will replace ^USER^
* The password is the form field where the password is entered
* The provided passwords will be replacing ^PASS^
* Finally, F=incorrect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

You should now have enough information to put this to practice and brute force your credentials to the deployed machine!

Use Hydra to bruteforce molly's web password. What is flag 1?

hydra -l molly -P rockyou.txt 10.10.102.63 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect" -V





Use Hydra to bruteforce molly's SSH password. What is flag 2?

hydra -l molly -P rockyou.txt 10.10.102.63 -t 4 ssh

