

MATA KULIAH
KEAMANAN SISTEM DAN JARINGAN KOMPUTER



Disusun oleh:

Nama : Yoki Rahmada

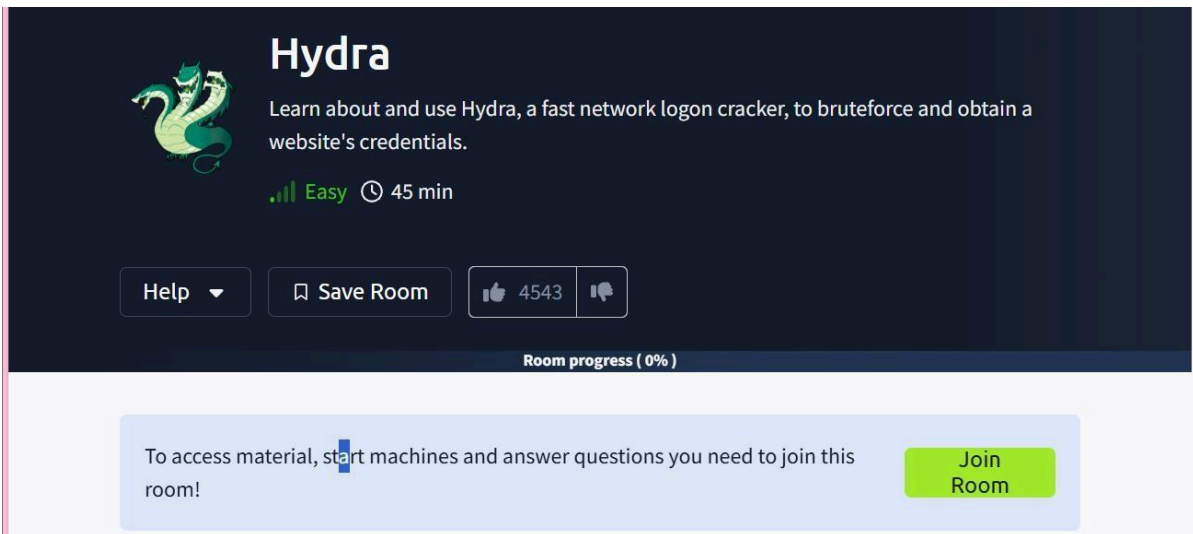
NIM : 2231740012

Kelas : 3B-Teknologi Informasi

PRODI D3 TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG

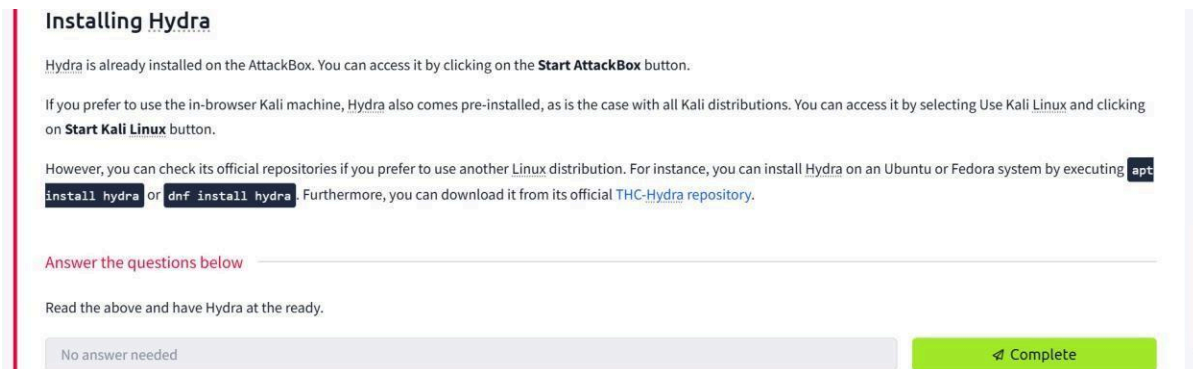
2025

1) Pertama yang harus kita lakukan adalah “Klik Join room.”



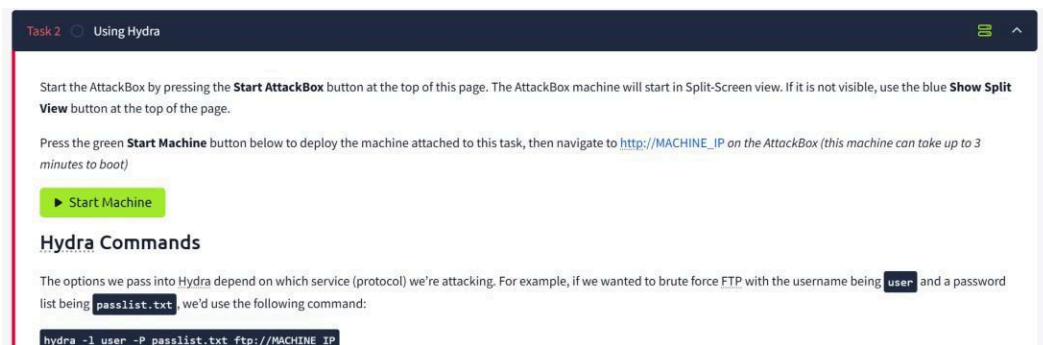
The image shows the Hydra room interface. At the top, there's a Hydra logo (a green dragon) and the text "Hydra". Below it, a description says "Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials." There's a difficulty indicator "Easy" with a green bar and a timer "45 min". Below this are buttons for "Help", "Save Room", and a thumbs up/down icon with "4543". A progress bar at the bottom says "Room progress (0%)". A light blue box contains the text "To access material, start machines and answer questions you need to join this room!" and a green "Join Room" button.

2) Task 1 : Introduction.



The image shows the "Installing Hydra" task page. It has a title "Installing Hydra" and a sub-header "Hydra is already installed on the AttackBox. You can access it by clicking on the **Start AttackBox** button." Below this, it explains how to use Hydra on Kali Linux or other Linux distributions. It provides commands like `apt install hydra` or `dnf install hydra`. There's a section "Answer the questions below" with a text input field and a "Complete" button.

3) Task 2 : Using Hydra. Klik tombol “Start Machine”.



The image shows the "Using Hydra" task page. It has a title "Task 2 Using Hydra". The instructions say to start the AttackBox by pressing the "Start AttackBox" button. It also mentions navigating to `http://MACHINE_IP` on the AttackBox. There's a green "Start Machine" button. Below this, it shows "Hydra Commands" and explains how to use Hydra with a command: `hydra -l user -P passlist.txt ftp://MACHINE_IP`.

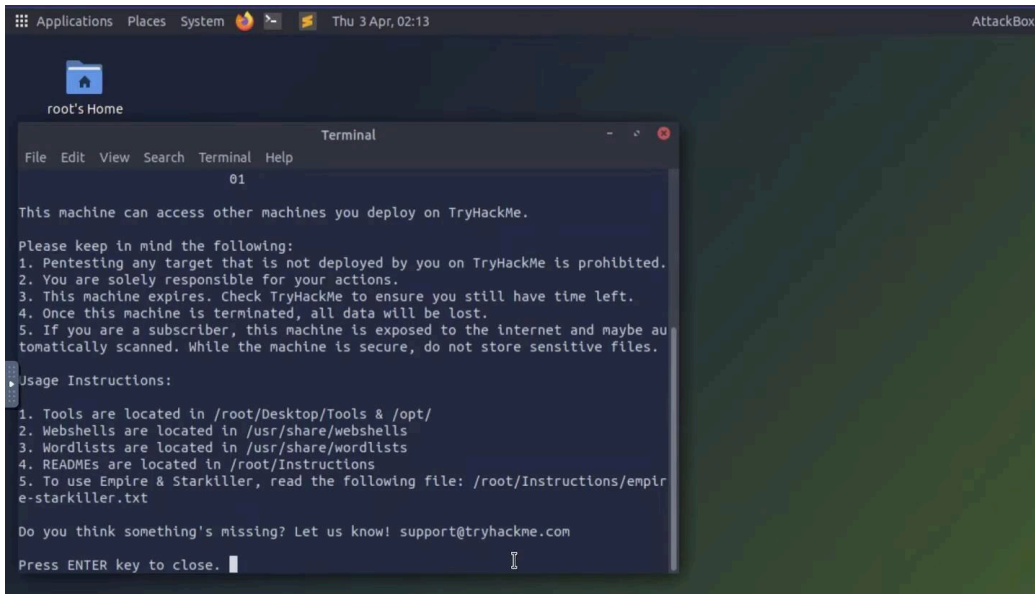
Setelah tombol “Start Machine” di klik, Maka akan muncul tampilan seperti berikut:



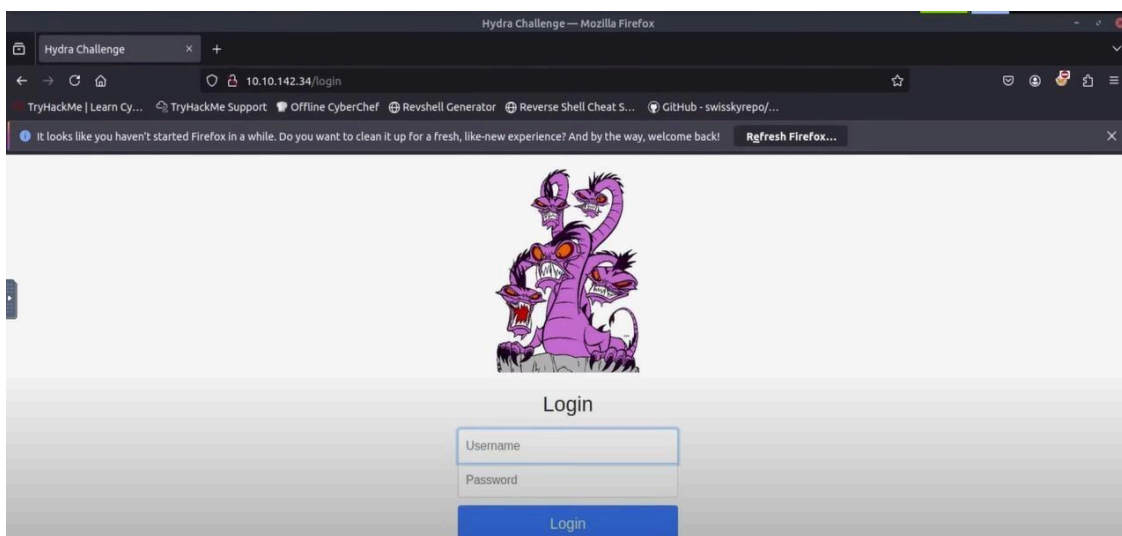
Target Machine Information		
Title	Target IP Address	Expires
Hydra Challenge	10.10.142.34	1h 56min 39s

Buttons: ? Add 1 hour Terminate

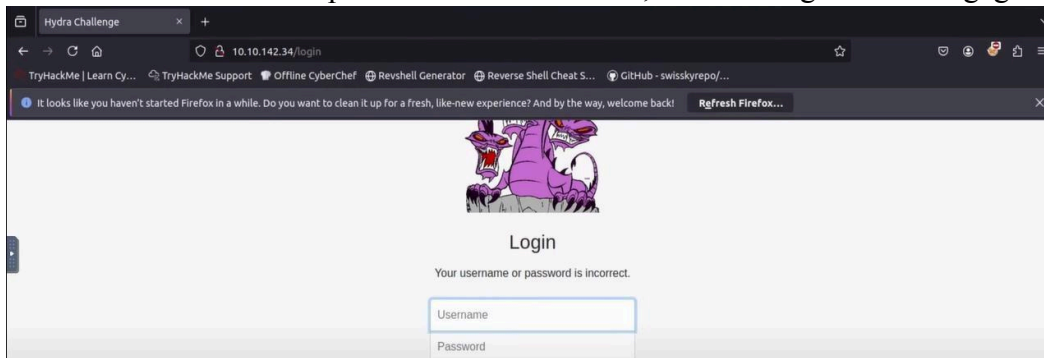
Setelah itu, klik tombol “**Start AttackBock**” yang ada di bagian atas Lalu, akan muncul seperti tampilan berikut ini:



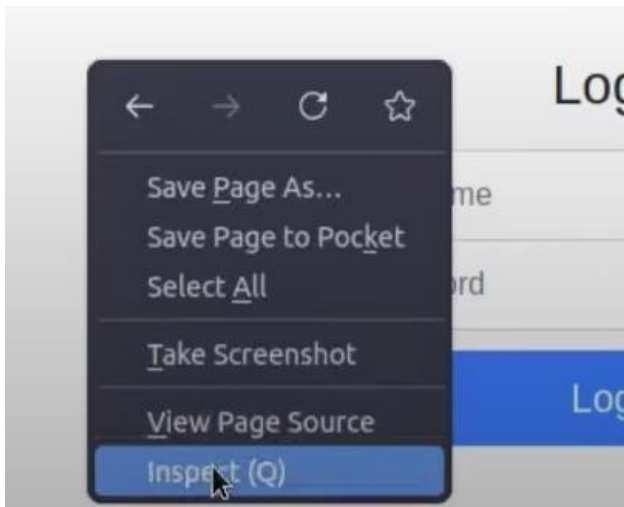
- 4) Selanjutnya bisa buka browser Mozilla Firefox dan masukkan IP Address yang tertera diatas tadi sehingga akan tampil halaman seperti berikut:



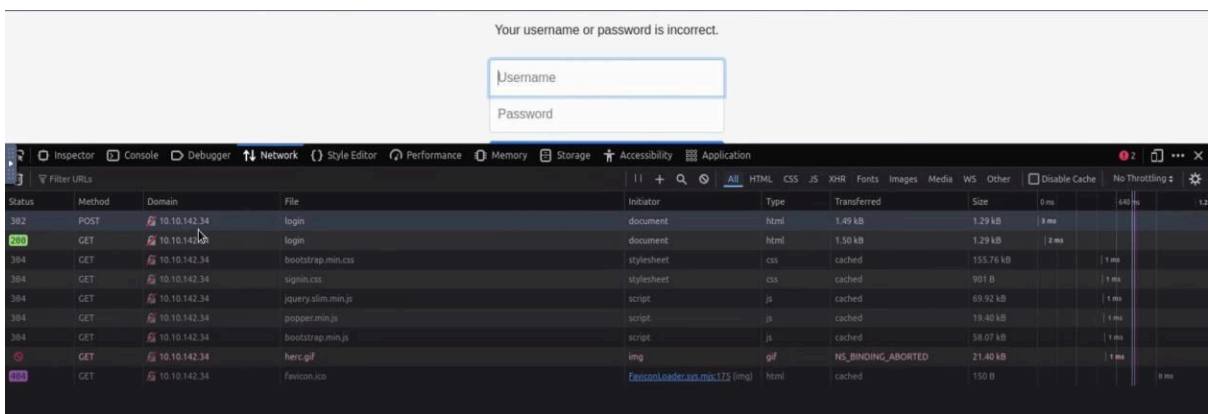
- 5) Masukkan username dan password secara random, dan kemungkinan akan gagal login.



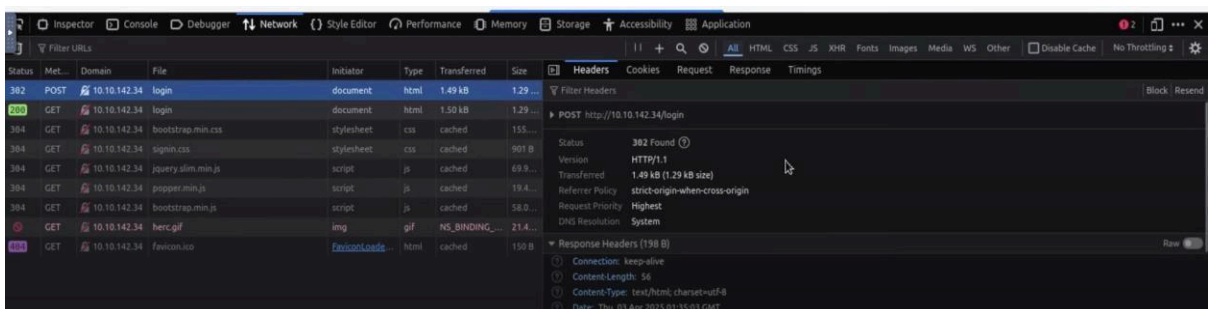
6) Lakukan inspect dengan cara klik kanan dan pilih inspect.



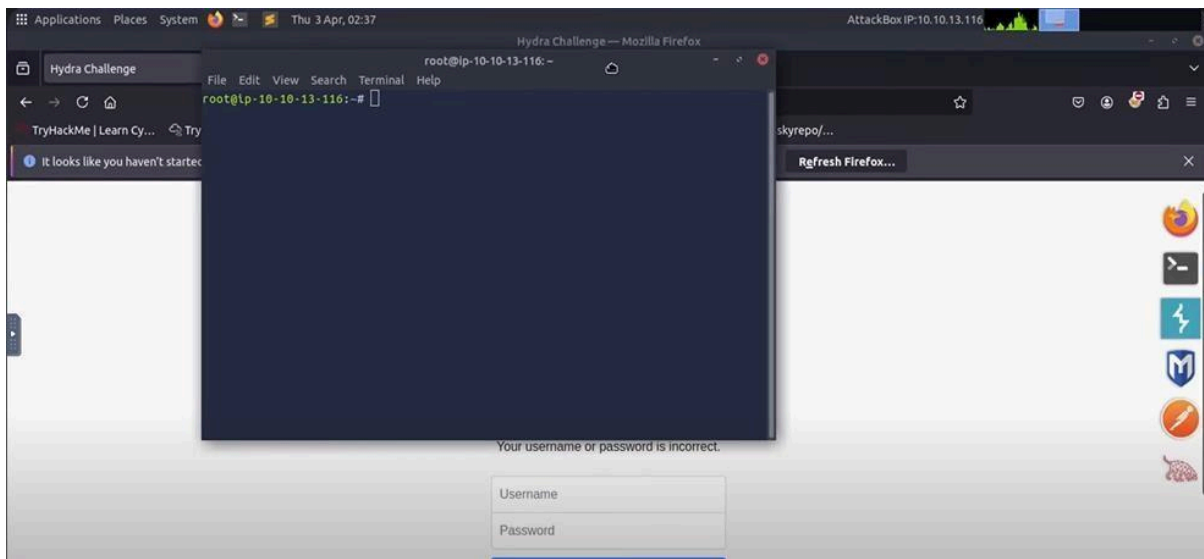
7) Pilih Network, and klik pada bagian yang method nya berupa POST.



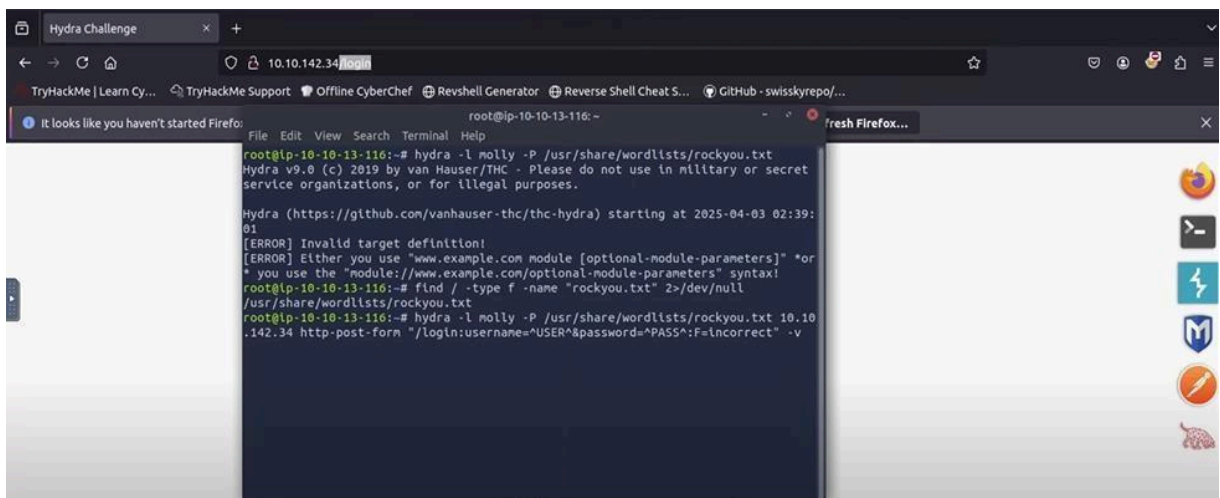
Sehingga akan menampilkan seperti berikut ini:



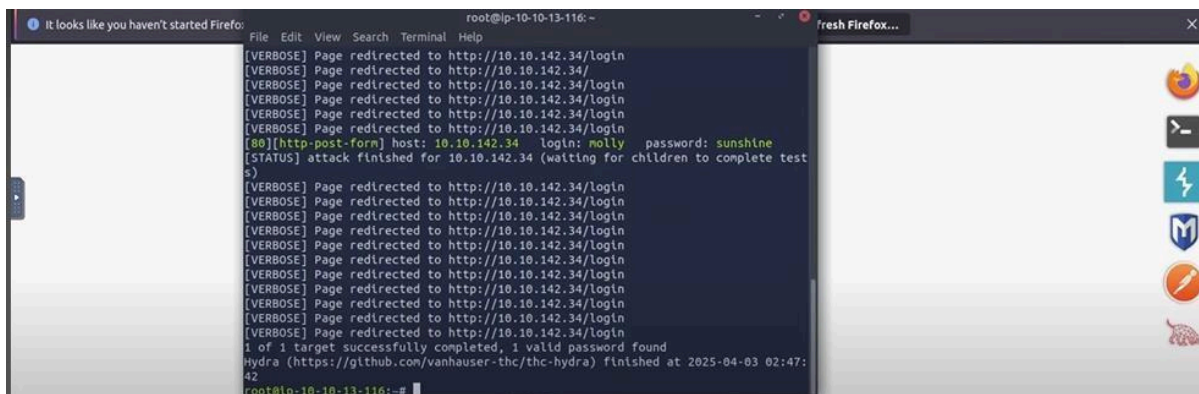
- 8) Percobaan menggunakan terminal untuk melakukan serangan pada situs web. Mulai dengan membuka terminal terlebih dahulu.



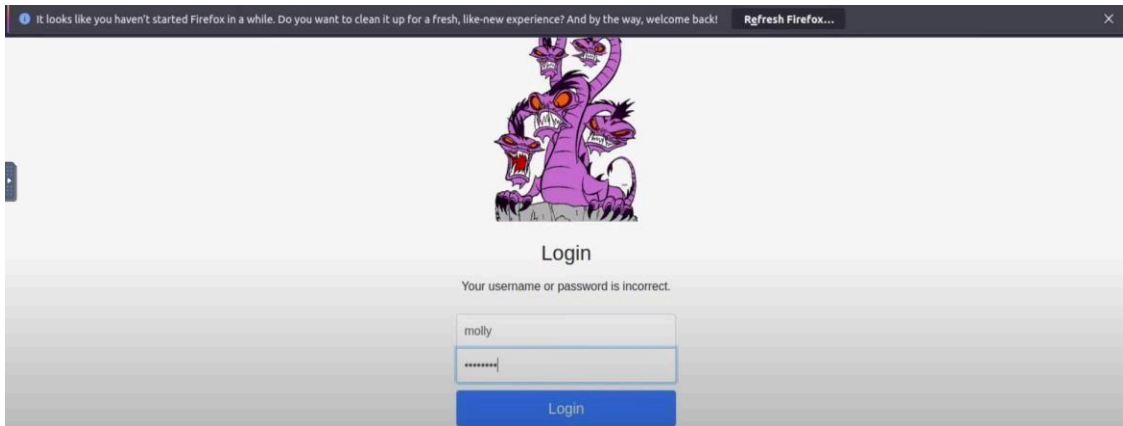
- 9) Kemudian masukkan perintah Hydra untuk melakukan brute force pada form login POST seperti format berikut & sesuaikan berdasarkan perintah: hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V



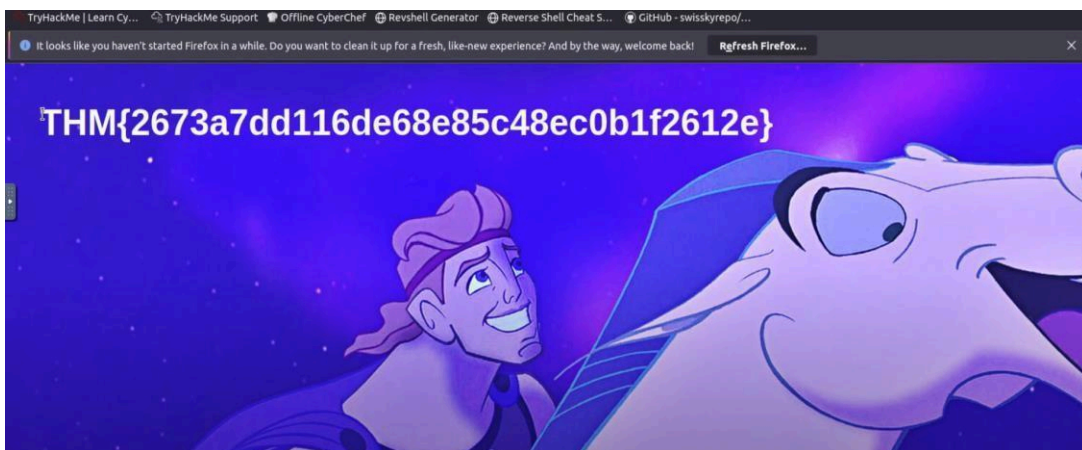
- 10) Apabila berhasil, maka akan menampilkan seperti berikut:



- 11) 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 username “molly” dan password “sunshine”.
- 12) Masukkan kembali username dan password yang sudah kita ketahui.



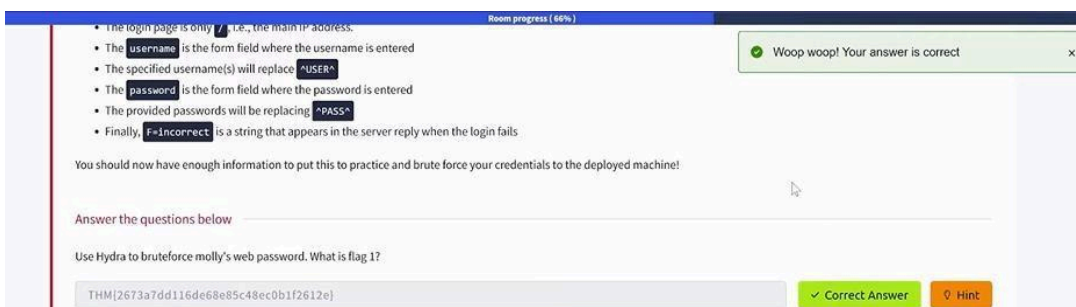
Maka kita akan diarahkan ke halaman baru yang menampilkan seperti berikut:



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

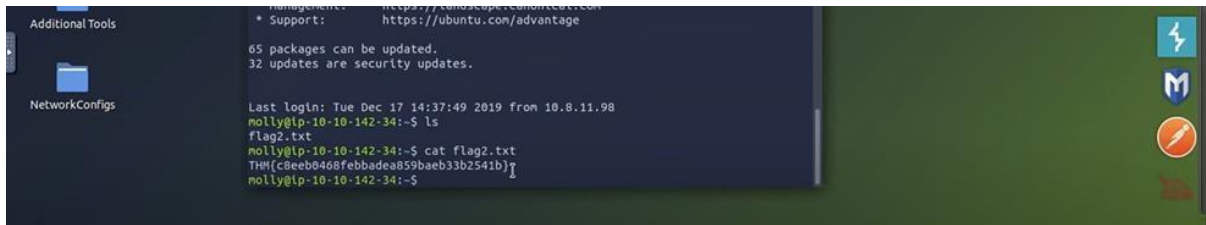


Setelah berhasil di submit, maka akan menampilkan pesan “your answer is correct”



- 13) Kembali lagi pada terminal, lakukan perintah berikut:

- 17) Masukkan perintah “ls” untuk menampilkan daftar file. Dan untuk mengakses dan melihat isi konten didalam file tersebut, gunakan perintah “cat filename”, maka akan muncul seperti berikut:



```
Additional Tools
NetworkConfigs

* Support: https://landscape.canonical.com
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@tp-10-10-142-34:~$ ls
flag2.txt
molly@tp-10-10-142-34:~$ cat flag2.txt
THM(c8eeb0468febbadea859baeb33b2541b)
molly@tp-10-10-142-34:~$
```

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



Room completed (100%)

Answer the questions below

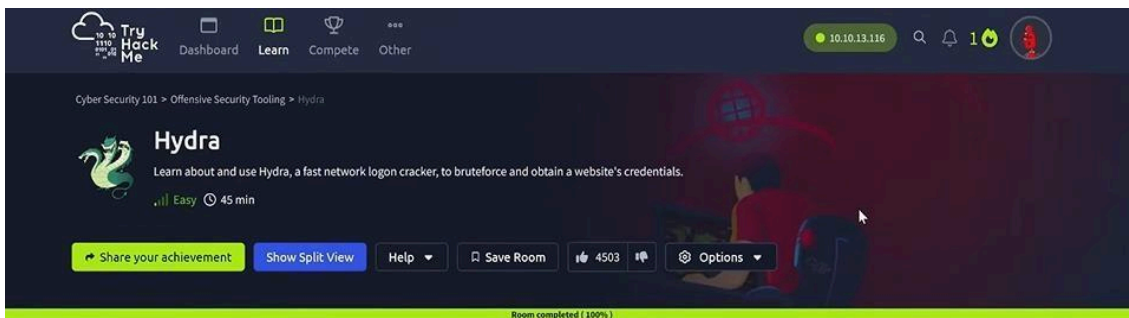
Use Hydra to bruteforce molly's web password. What is flag 1?

THM(2673a7dd116de68e85c48ec0b1f2612e) ✓ Correct Answer [Hint](#)

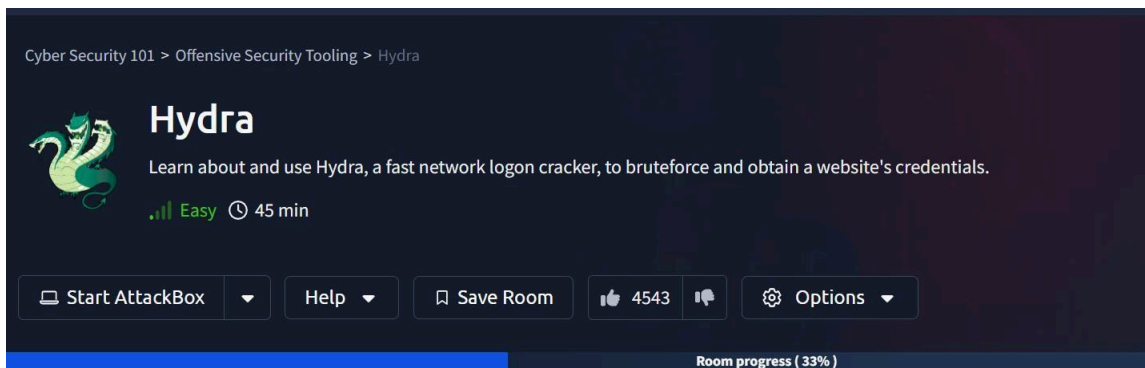
Use Hydra to bruteforce molly's SSH password. What is flag 2?

THM(c8eeb0468febbadea859baeb33b2541b) ✓ Correct Answer

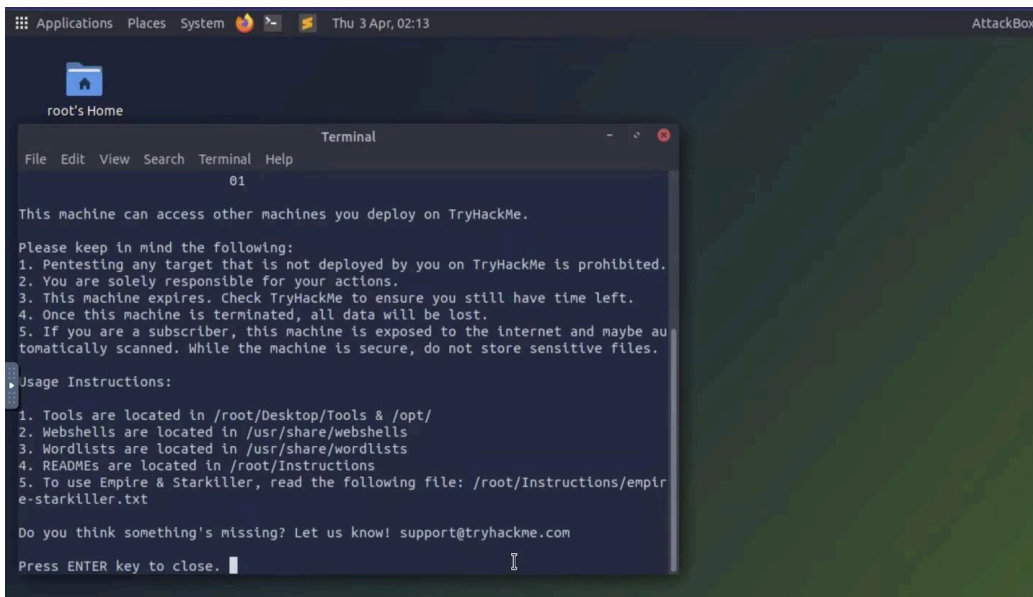
- 19) Setelah semuanya telah dilakukan maka progress menjadi 100%



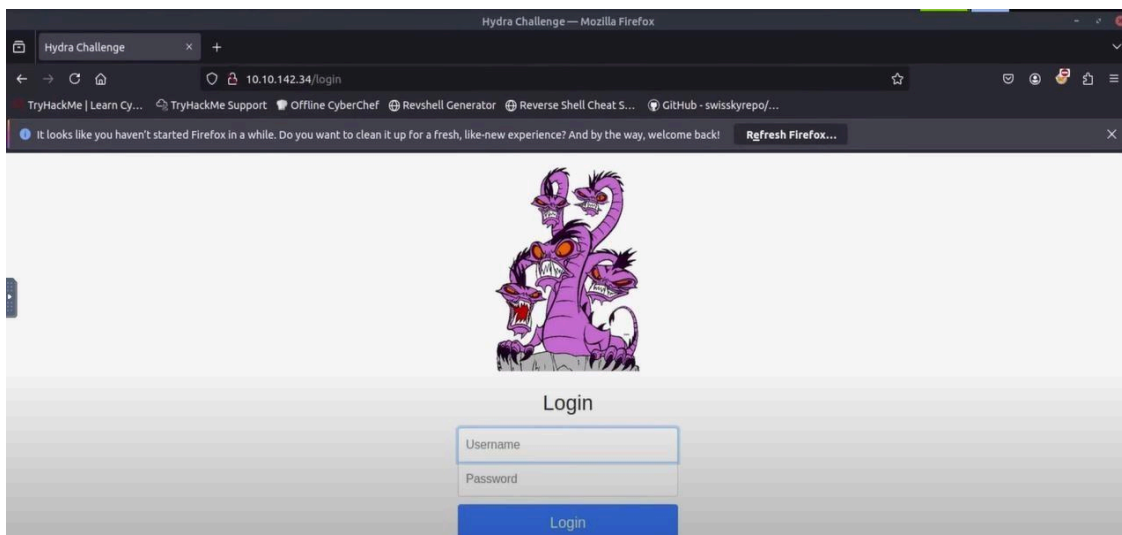
- 20) Selesa



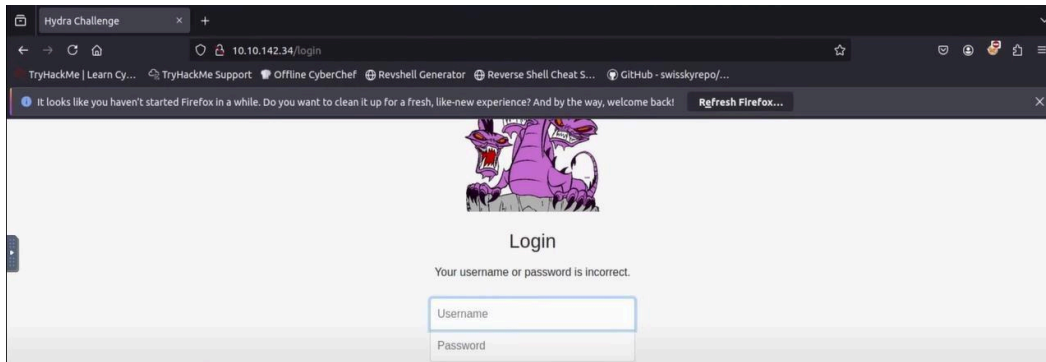
Lalu, akan muncul seperti tampilan berikut ini:



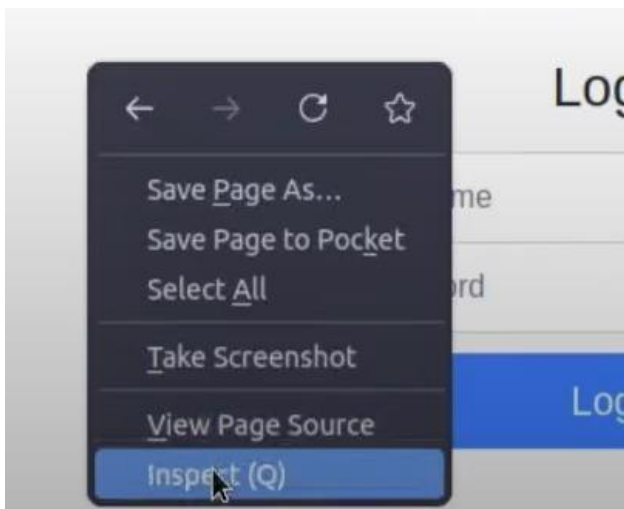
21) Selanjutnya bisa buka browser Mozilla Firefox dan masukkan IP Address yang tertera diatas tadi sehingga akan tampil halaman seperti berikut:



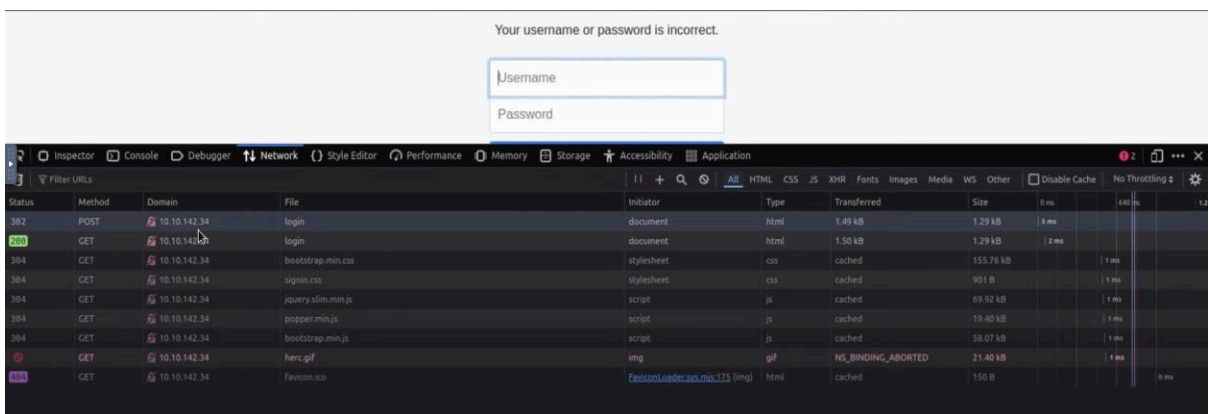
22) Masukkan username dan password secara random, dan kemungkinan akan gagal login.



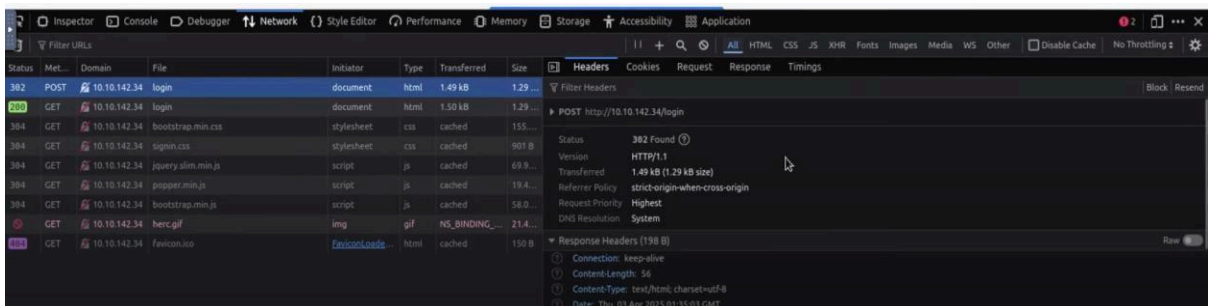
23) Lakukan inspect dengan cara klik kanan dan pilih inspect.



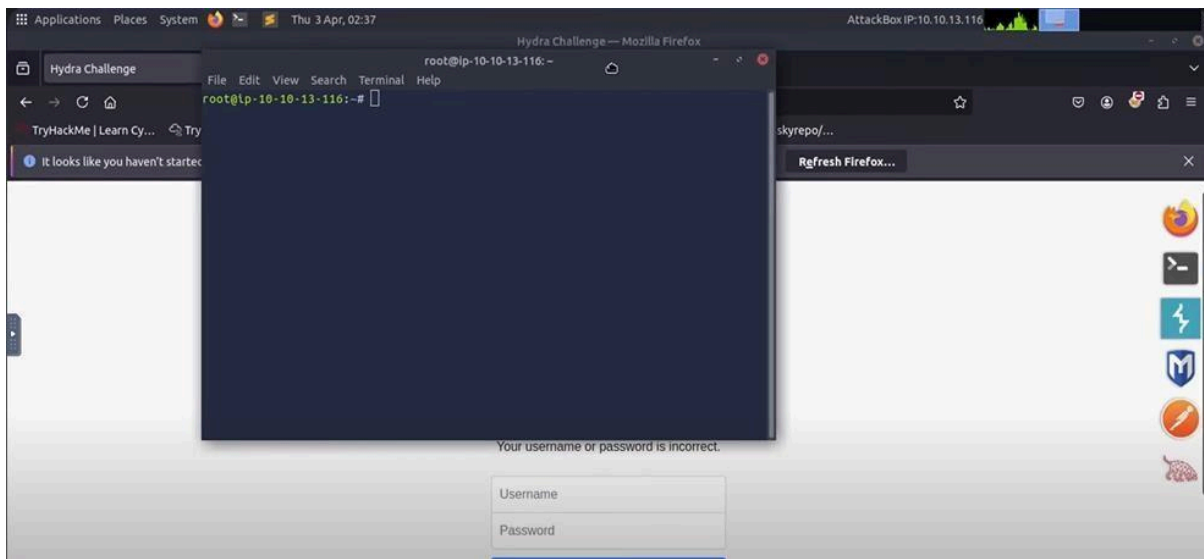
24) Pilih Network, dan klik pada bagian yang method nya berupa POST.



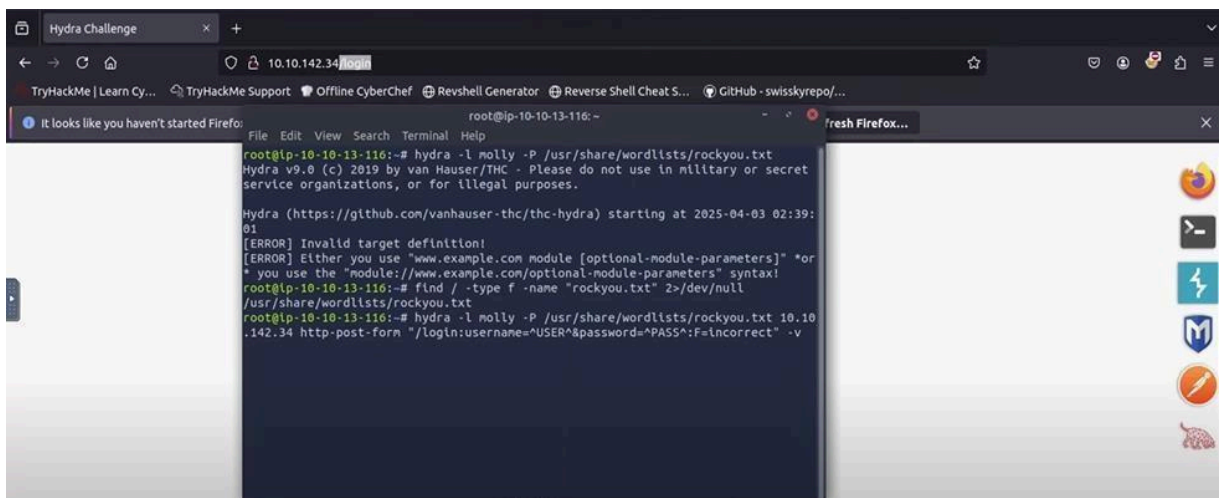
Sehingga akan menampilkan seperti berikut ini:



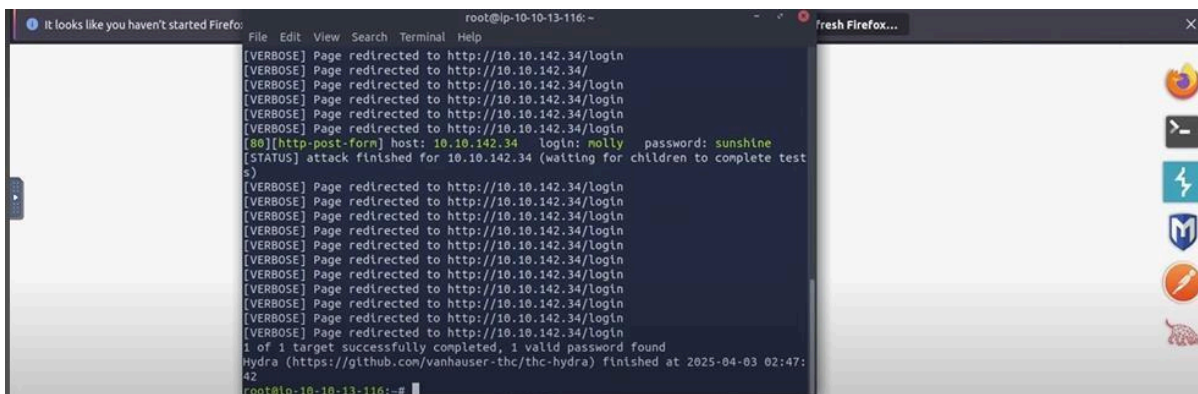
- 25) Percobaan menggunakan terminal untuk melakukan serangan pada situs web. Mulai dengan membuka terminal terlebih dahulu.



- 26) 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`

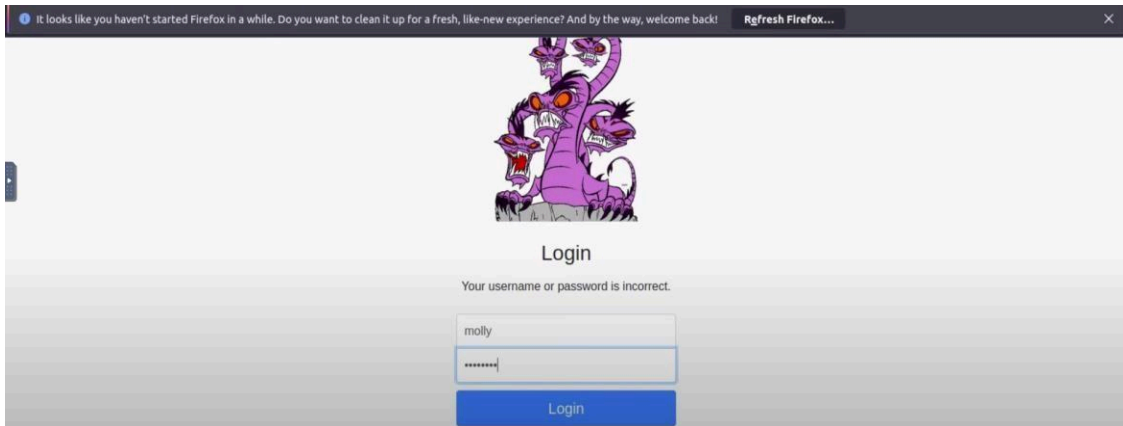


- 27) Apabila berhasil, maka akan menampilkan seperti berikut:

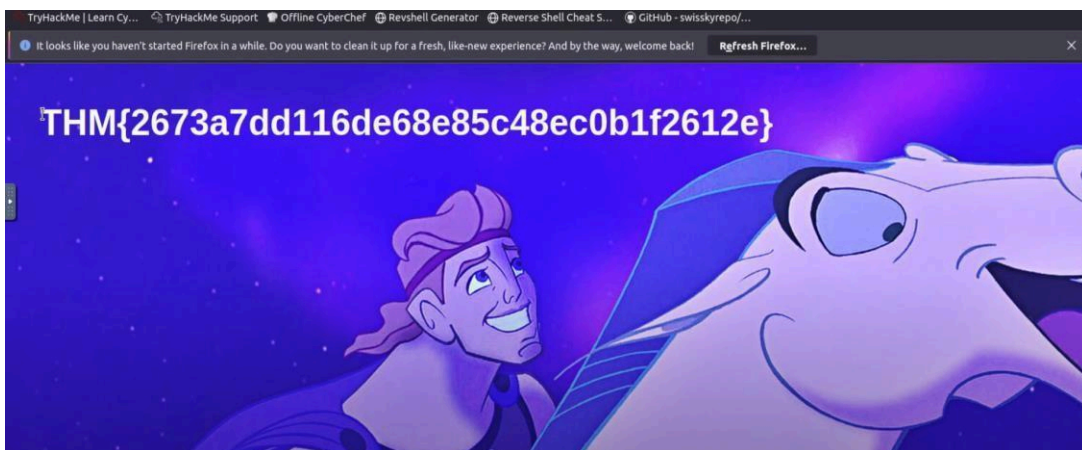


28) Perhatikan gambar diatas, dan terlihat pada bagian yang menampilkan bahwa layanan (protocol) HTTP-POST-FORM dengan host IP Address 10.10.142.34 menunjukkan bahwa username “molly” dan password “sunshine”.

29) Masukkan kembali username dan password yang sudah kita ketahui.



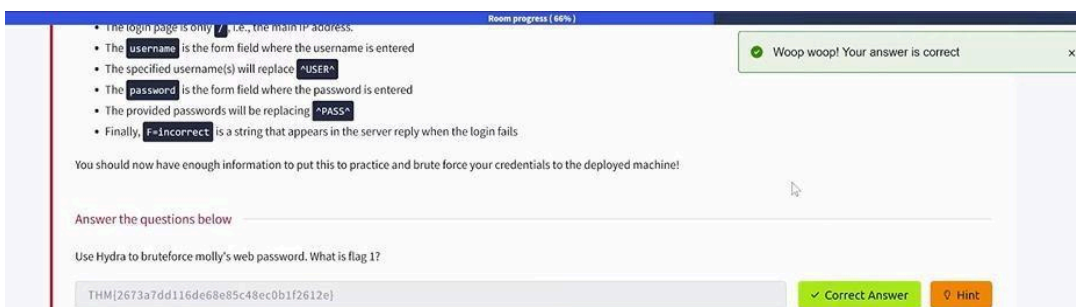
Maka kita akan diarahkan ke halaman baru yang menampilkan seperti berikut:



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

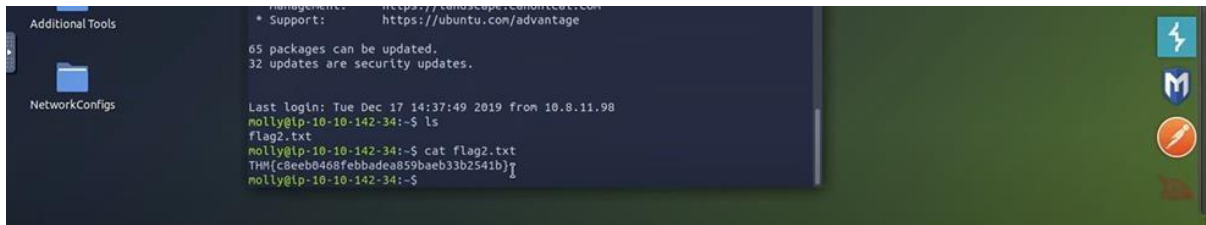


Setelah berhasil di submit, maka akan menampilkan pesan “your answer is correct”



30) Kembali lagi pada terminal, lakukan perintah berikut:

- 34) Masukkan perintah “ls” untuk menampilkan daftar file. Dan untuk mengakses dan melihat isi konten didalam file tersebut, gunakan perintah “cat filename”, maka akan muncul seperti berikut:



```
Additional Tools
NetworkConfigs

* Support: https://landscape.canonical.com
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@tp-10-10-142-34:~$ ls
flag2.txt
molly@tp-10-10-142-34:~$ cat flag2.txt
THM(c8eeb0468febbadea859baeb33b2541b)
molly@tp-10-10-142-34:~$
```

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



Room completed (100%)

Answer the questions below

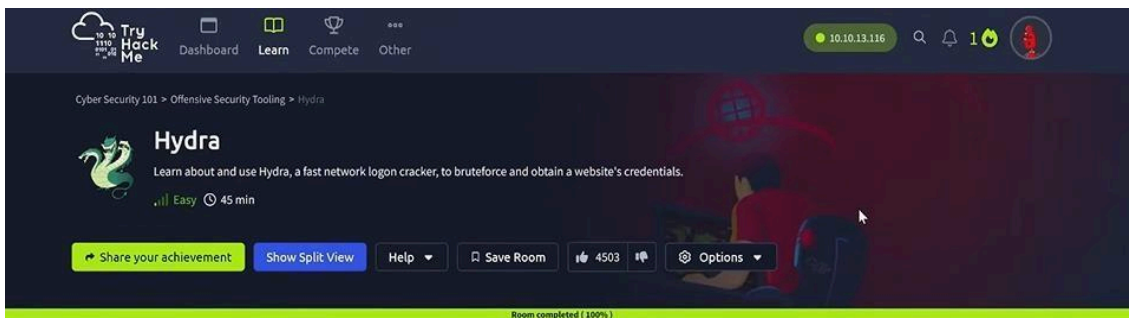
Use Hydra to bruteforce molly's web password. What is flag 1?

THM(2673a7dd116de68e85c48ec0b1f2612e) ✓ Correct Answer Hint

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

THM(c8eeb0468febbadea859baeb33b2541b) ✓ Correct Answer

- 36) Setelah semuanya telah dilakukan maka progress menjadi 100%



- 37) Selesai.