

# **KEAMANAN SISTEM DAN JARINGAN KOMPUTER**



**Disusun oleh:**

**Nama : Abdul Mun'im**

**NIM : 2231740015**

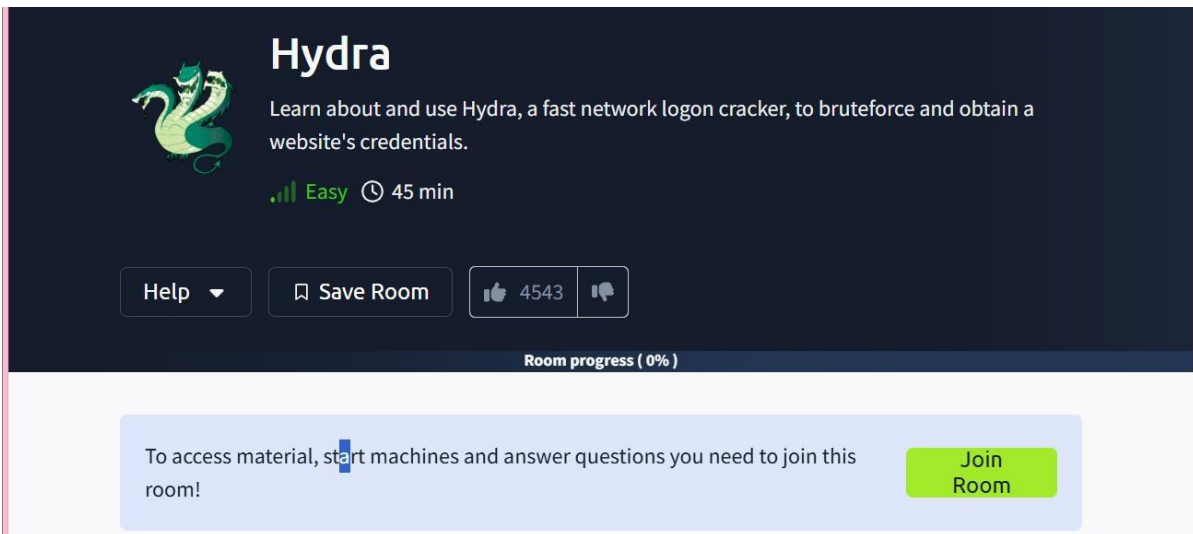
**Kelas : 3B-Teknologi Informasi**

**PRODI D3 TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI MALANG**

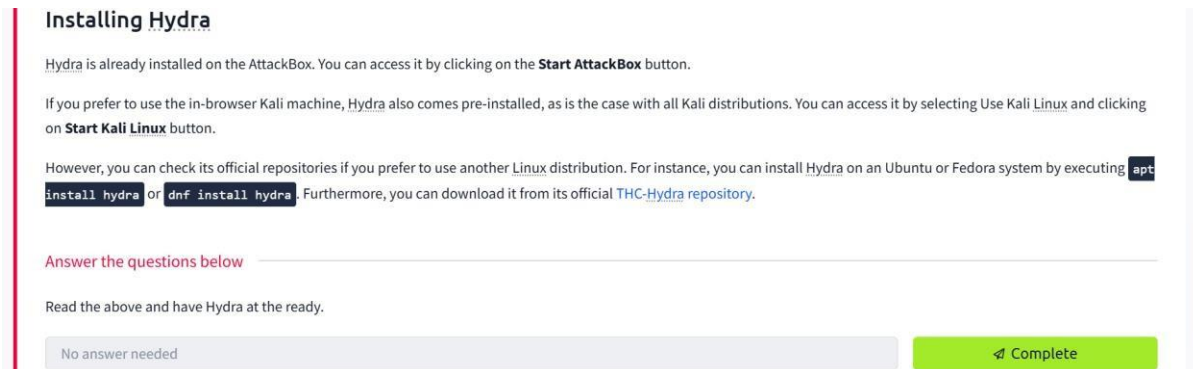
**2025**

1) Klik Join room.



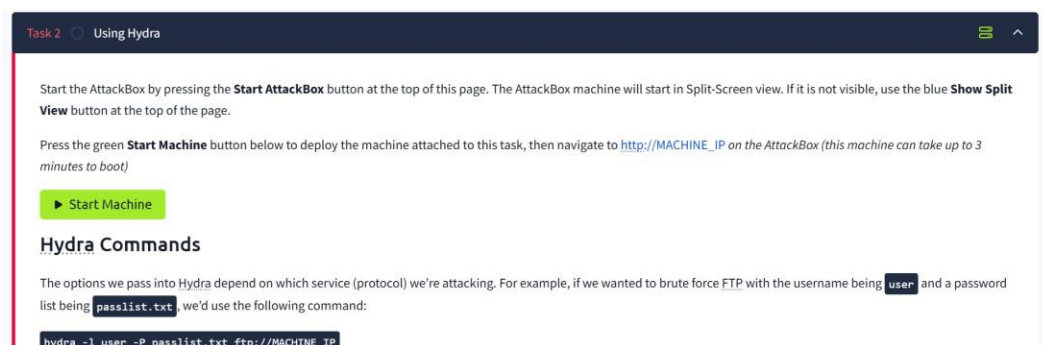
The image shows the Hydra room interface. At the top, there's a Hydra logo (a green dragon) and the title "Hydra". Below it, a description says "Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials." There's a difficulty indicator "Easy" with a clock icon and "45 min". Below this are buttons for "Help", "Save Room", and a thumbs up icon with "4543". A progress bar at the bottom indicates "Room progress ( 0% )". A large 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) Introduction.



The image shows the "Installing Hydra" section. It starts with the title "Installing Hydra". The text explains that Hydra is already installed on the AttackBox and can be accessed by clicking the "Start AttackBox" button. It also mentions that Hydra is pre-installed on Kali Linux. A code block shows the command to install Hydra on other Linux distributions: `apt install hydra` or `dnf install hydra`. Below this, there's a section "Answer the questions below" with a text input field and a "Complete" button.

3) Klik start machine



The image shows the "Task 2 Using Hydra" interface. It contains instructions on how to start the AttackBox and how to use the "Start Machine" button. Below the instructions, there's a green "Start Machine" button. The section "Hydra Commands" explains how to use Hydra with a specific command: `hydra -l user -P passlist.txt ftp://MACHINE_IP`.

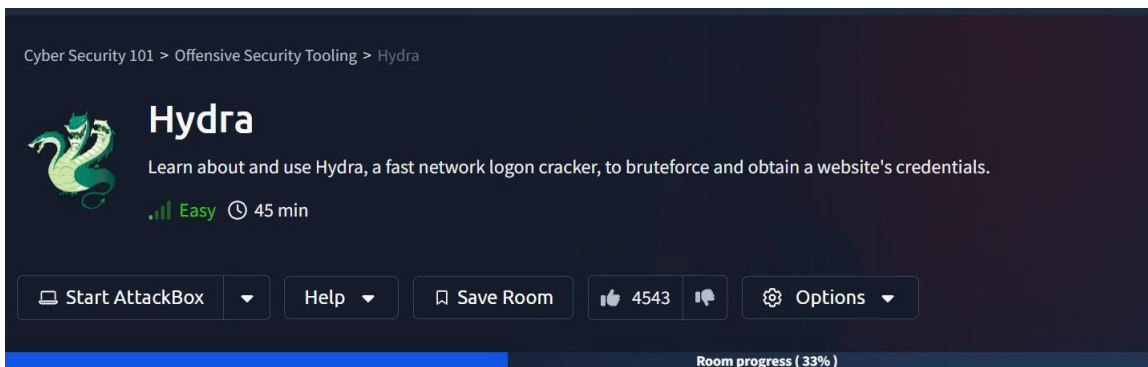
4) Maka akan muncul tampilan seperti berikut:



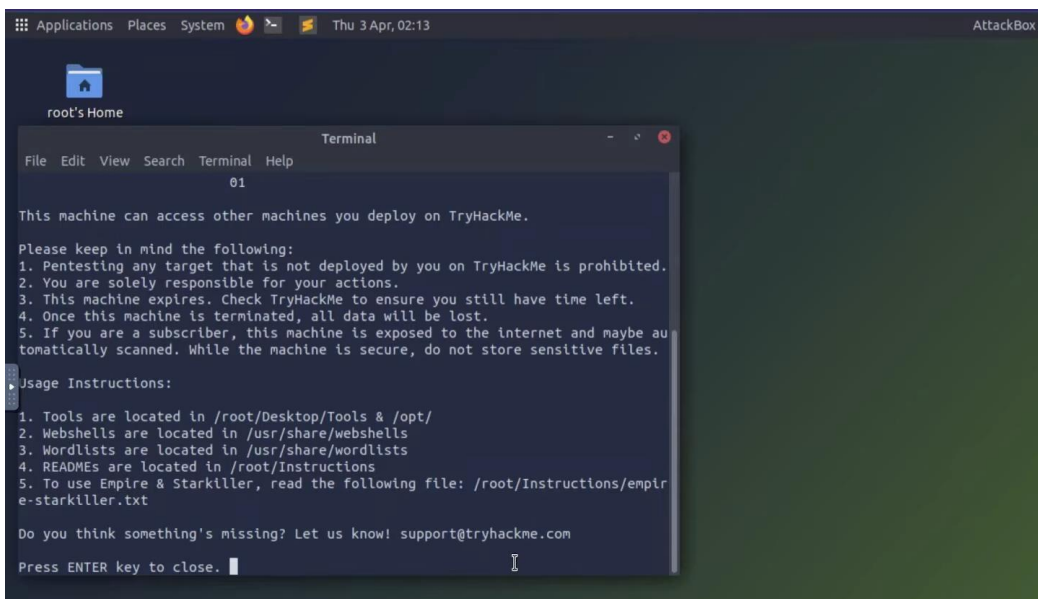
The image shows a table titled "Target Machine Information". The table has three columns: "Title", "Target IP Address", and "Expires". The first row shows "Hydra Challenge", "10.10.142.34", and "1h 56min 39s". There are buttons for "?", "Add 1 hour", and "Terminate" to the right of the table.

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

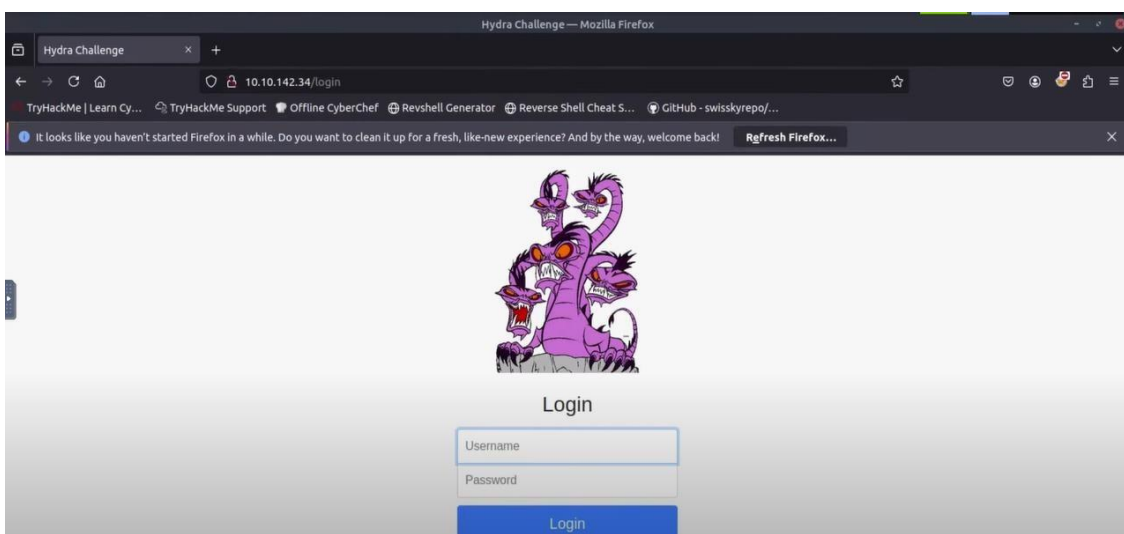
5) Setelah itu, klik Start AttackBock yang ada dibagian atas



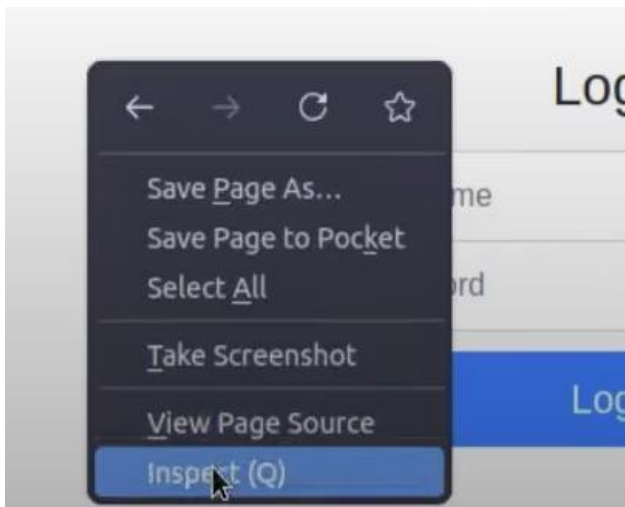
6) Lalu, akan muncul seperti tampilan berikut ini:



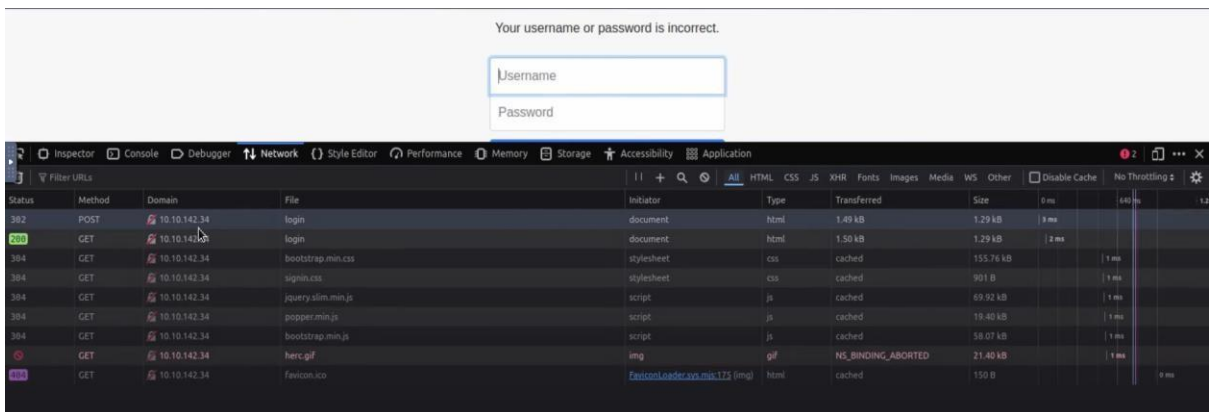
7) Selanjutnya bisa buka browser Mozilla Firefox dan masukkan IP Address yang tertera diatas tadi sehingga akan tampil halaman seperti di bawah dan masukkan username dan password secara random, dan kemungkinan akan gagal login:



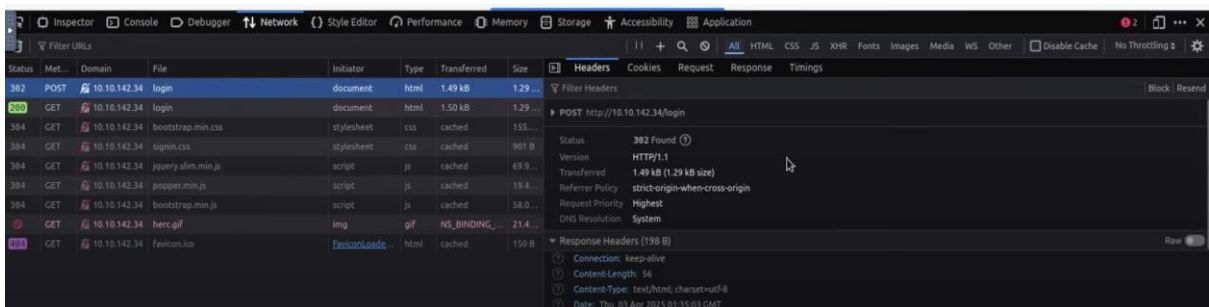
8) Lakukan inspect dengan cara klik kanan dan pilih inspect.



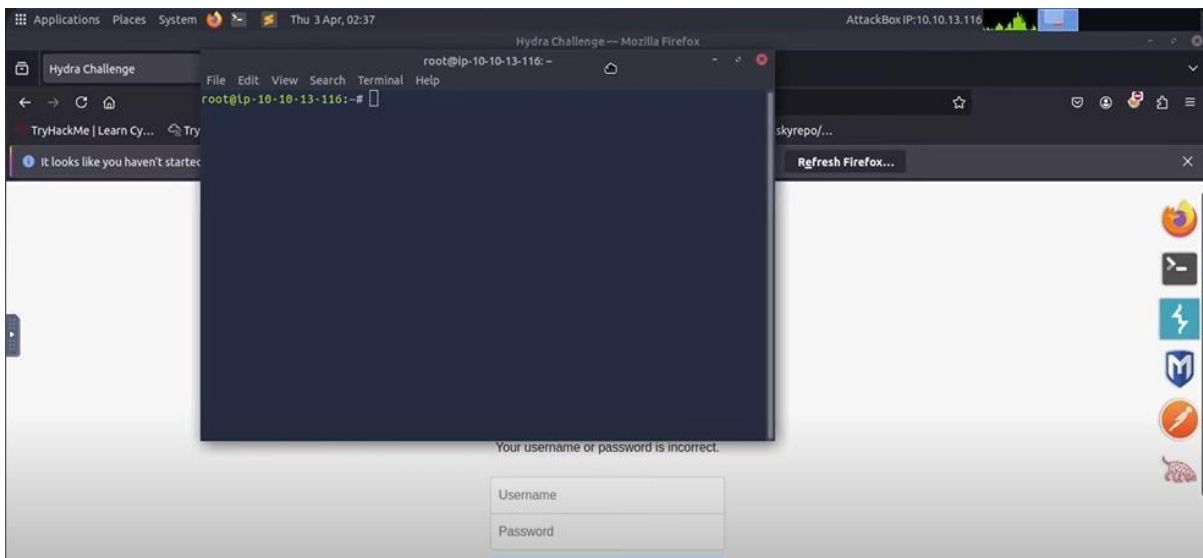
9) Pilih Network, and klik pada bagian yang method nya berupa POST.



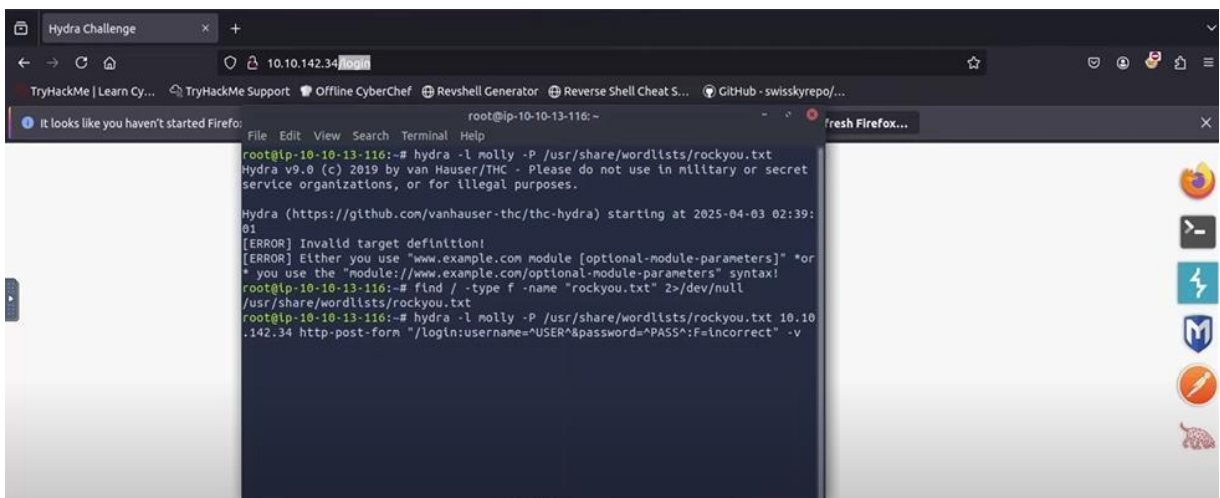
Sehingga akan menampilkan seperti berikut ini:



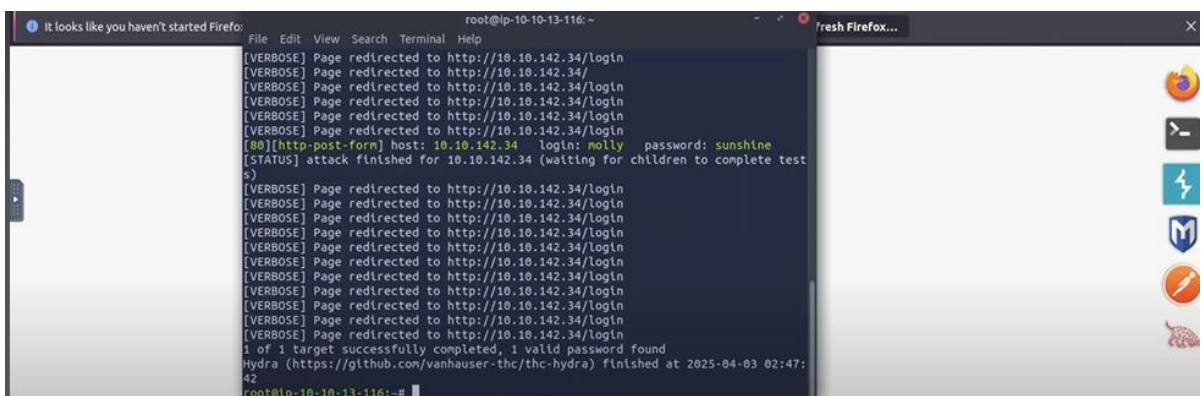
- 10) Mulai dengan membuka terminal terlebih dahulu untuk melakukan percobaan pada situs web.



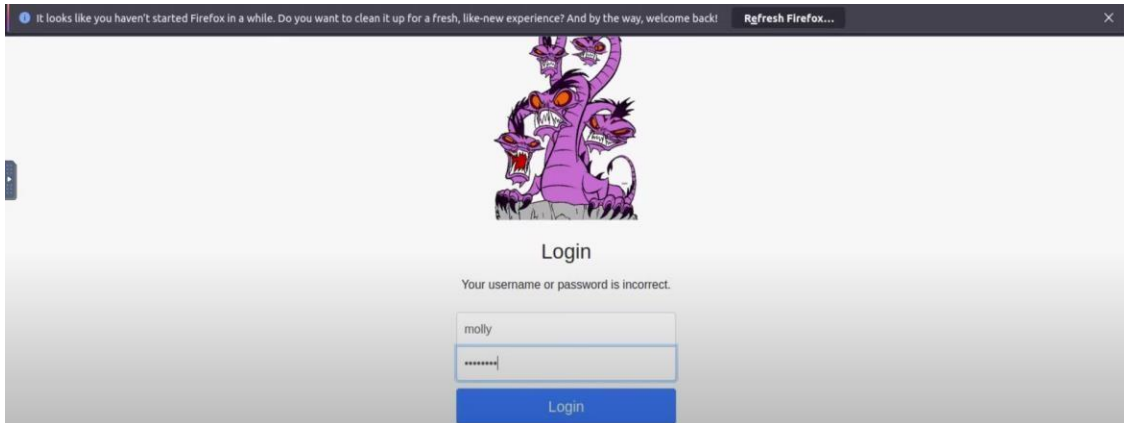
- 11) Kemudian masukkan perintah Hydra untuk melakukan brute force pada form login POST seperti format berikut & sesuaikan berdasarkan perintah: `hydra -l <username> -P <wordlist> MACHINE_IP http-post-form '[:username=^USER^&password=^PASS^:F=incorrect' -V`



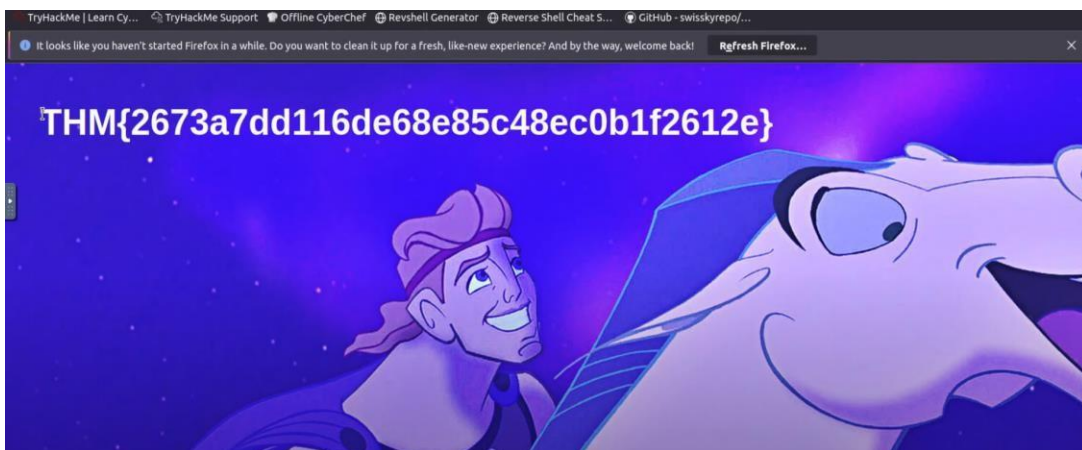
- 12) Jika berhasil, maka akan menampilkan seperti berikut:



- 13) Perhatikan gambar diatas, 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”.
- 14) Masukkan kembali username dan password yang sudah kita ketahui.



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



- 16) 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 1?

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

Room progress (66%)

Woop woop! Your answer is correct

- The login page is only `10.10.142.34`, 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, `!Incorrect` is a string that appears in the server reply when the login fails

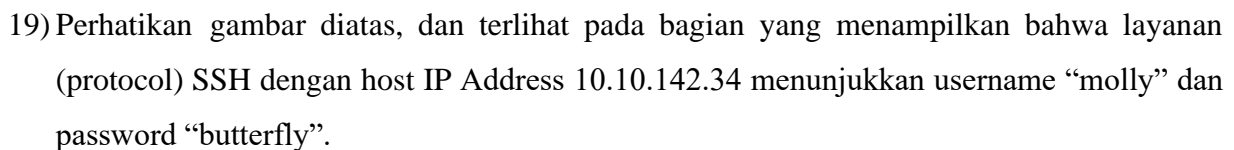
You should now have enough information to put this to practice and brute force your credentials to the deployed machine!

Answer the questions below

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

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

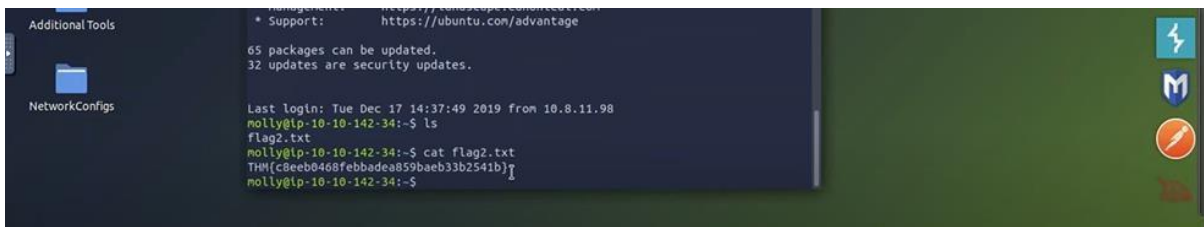




A screenshot of a Kali Linux desktop environment. The desktop background is dark blue. On the left side, there is a vertical dock with icons for 'root's Home', 'Terminal', 'Tools', 'Additional Tools', and 'NetworkConfigs'. The 'Terminal' icon is highlighted. In the center, a terminal window is open, displaying a Hydra brute-force attack. The terminal title is 'molly@ip-10-10-142-34: ~'. The output shows that the attack was successful, finding the password 'butterfly' for the user 'molly' on host '10.10-142-34'. The terminal also shows the user's prompt 'root@ip-10-10-13-116:~#', a warning about the host's authenticity, and a list of known hosts. At the bottom, it shows the last login time and the current prompt 'molly@ip-10-10-142-34:~#'. On the right side of the desktop, there are several icons: a Firefox browser icon, a file manager icon, a terminal icon, a lightning bolt icon, a mail icon, and a terminal icon with a red lightning bolt.

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

22) 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:



```
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@10-10-10-142-34:~$ ls
flag2.txt
molly@10-10-10-142-34:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@10-10-10-142-34:~$
```

23) 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

24) Setelah semuanya telah dilakukan maka progres selesai.

