

Forum:[Hack Forums](#)

Thread: [Brute-Forcing Passwords Ethically with Hydra](#)

JoseMar - January 10, 2025, 2:49 am

Brute-Forcing Passwords Ethically with Hydra

Hydra is a powerful tool for performing brute-force attacks on login services, commonly used by ethical hackers to test system security. This tutorial explains how to use Hydra step by step, from installation to running an attack on a target system in a controlled environment.

Step-by-Step Guide to Using Hydra

1. What is Hydra?

Hydra is a fast and flexible brute-force password-cracking tool. It supports multiple protocols like SSH, FTP, HTTP, and more. Its primary purpose is to test password strength and identify weak credentials.

2. Setting Up Hydra

Install Hydra:

On Kali Linux, Hydra comes pre-installed. If it's not installed, use the command:

```
Code sudo apt-get install hydra
```

3. Creating a Wordlist

A wordlist is a file containing potential passwords. Use an existing wordlist (like /usr/share/wordlists/rockyou.txt) or create your own:

```
bash
```

```
Code echo -e "password123\nadmin\n123456" > mywordlist.txt
```

4. Running Hydra

Hydra requires you to specify the target, protocol, username, and wordlist. Here's a basic command:

Targeting SSH:

```
Code hydra -l username -P mywordlist.txt ssh://<target IP>
```

-l specifies the username.

-P specifies the wordlist.

ssh:// indicates the protocol.

5. Common Scenarios:

HTTP Login Forms:

To target a web form, identify the POST request format using tools like Burp Suite and use Hydra:

```
Code hydra -l admin -P mywordlist.txt <IP or URL> http-post-form
```

```
"/login:username=^USER^&password=^PASS^:Invalid login"
```

Replace /login with the actual login page path and Invalid login with the server's response for failed logins.

FTP Login:

```
Code hydra -l admin -P mywordlist.txt ftp://<target IP>
```

6. Advanced Hydra Options

Threading: Use -t to specify the number of threads for faster brute-forcing (e.g., -t 10).

Verbose Output: Add -v or -V to see the progress of each attempt.

Saving Results: Use -o to save results to a file:

```
Code hydra -l admin -P mywordlist.txt ssh://<target IP> -o results.txt
```

7. Understanding Results

Once Hydra completes its operation, it will display valid login credentials (if found). For example:

```
Code [22][ssh] host: 192.168.1.10 login: admin password: password123
```

8. Ethical Usage

Always ensure you have explicit permission to test a system. Never use Hydra on unauthorized systems, it's illegal and unethical.

BiNBo - January 10, 2025, 5:26 am

Love the thread, love the idea, we need more tutorials and stuff like that.

However, the style and format all scream LLM generated wall of text to me. IF this is the case, it would be nice to disclose that at the start. Otherwise it just seems like you're trying to pass it off as your genuine efforts. Though, again, IF that is the case.

7 - January 12, 2025, 2:44 am

I really appreciate the work you put into threads like these.

This is what I call HQ. Top man

Nightmare - January 12, 2025, 3:06 am

HQ stuff,i love it!!Good job my brother!

Bastille - January 13, 2025, 2:58 am

You have no idea how great it feels to see HF going back to its roots with this kind of content. Thanks for the hard work!

JoseMar - January 13, 2025, 3:09 am

(Jan 13, 2025 03:58 AM)Bastille Wrote: [\[CITE\]](#) You have no idea how great it feels to see HF going back to its roots with this kind of content. Thanks for the hard work!

Thanks, buddy! Yesterday, I tried creating a detailed thread about SQL Injection, including code and all the details, but unfortunately, HF's firewall blocked the code. Even simple examples wouldn't go through.

For example:

Bypassing Login Forms

This is just one simple code , eliminate -->> *" OR* 1=1 --

So, I think I'll have to upload it as a PDF to Mega for download.

Bastille - January 13, 2025, 3:15 am

(Jan 13, 2025 04:09 AM)JoseMar Wrote: [\[CITE\]](#) Thanks, buddy! Yesterday, I tried creating a detailed thread about SQL Injection, including code and all the details, but unfortunately, HF's firewall blocked the code. Even simple examples wouldn't go through.

For example:

Bypassing Login Forms

This is just one simple code , eliminate -->> *" OR* 1=1 --

So, I think I'll have to upload it as a PDF to Mega for download.

Interesting, did it happen if you place the commands inside a too ?

Generally, we get more activities / replies when content is behind an attachment or a download link, than when we post content in direct access in threads like what we do for the hacking tutorials.

I'm curious to see how it will go for your thread with the PDF file, if we observe the same behavior it might be interesting to think about a feature such as "Hiding content" and people will have to reply to un-hide it. But maybe Omni didn't put it for SEO reasons

JoseMar - January 13, 2025, 3:35 am

(Jan 13, 2025 04:15 AM)Bastille Wrote: [\[CITE\]](#) Interesting, did it happen if you place the commands inside a too ?

Generally, we get more activities / replies when content is behind an attachment or a download link, than when we post content in direct access in threads like what we do for the hacking tutorials.

I'm curious to see how it will go for your thread with the PDF file, if we observe the same behavior it might be interesting to think about a feature such as "Hiding content" and people will have to reply to un-hide it. But maybe Omni didn't put it for SEO reasons

Try pasting that SQL injection code and pressing *Preview*, you'll see what I mean.

For a tutorial, it's much better to have everything in one thread instead of requiring a download. It's not just better for SEO but also makes it easier for people to find it. They can simply read it without downloading. However, if it's a long course with videos and extensive content (What I will upload in few minutes), then I agree, downloads make more sense in that case.

JoseMar - January 15, 2025, 1:58 pm

(Jan 12, 2025 03:44 AM)7 Wrote: [\[CITE\]](#) I really appreciate the work you put into threads like these.

This is what I call HQ. Top man

Thanks so much: [BiNBo](#) @7@ @Bastille@ [Nightmare](#)

If someone need anything special, just let me know, and I'll do my best to create a thread if I can

and also if I know.?

Best Regards!

??Mirai - September 24, 2025, 11:20 pm

(Jan 10, 2025 03:49 AM)JoseMar Wrote: [\[CITE\]](#) Brute-Forcing Passwords Ethically with Hydra

Hydra is a powerful tool for performing brute-force attacks on login services, commonly used by ethical hackers to test system security. This tutorial explains how to use Hydra step by step, from installation to running an attack on a target system in a controlled environment.

Step-by-Step Guide to Using Hydra

1. What is Hydra?

Hydra is a fast and flexible brute-force password-cracking tool. It supports multiple protocols like SSH, FTP, HTTP, and more. Its primary purpose is to test password strength and identify weak credentials.

2. Setting Up Hydra

Install Hydra:

On Kali Linux, Hydra comes pre-installed. If it's not installed, use the command:

```
Code sudo apt-get install hydra
```

3. Creating a Wordlist

A wordlist is a file containing potential passwords. Use an existing wordlist (like `/usr/share/wordlists/rockyou.txt`) or create your own:

```
bash
```

```
Code echo -e "password123\nadmin\n123456" > mywordlist.txt
```

4. Running Hydra

Hydra requires you to specify the target, protocol, username, and wordlist. Here's a basic command:

Targeting SSH:

```
Code hydra -l username -P mywordlist.txt ssh://<target IP>
```

-l specifies the username.

-P specifies the wordlist.

ssh:// indicates the protocol.

5. Common Scenarios:

HTTP Login Forms:

To target a web form, identify the POST request format using tools like Burp Suite and use Hydra:

```
Code hydra -l admin -P mywordlist.txt <IP or URL> http-post-form
```

"/login:username=^USER^&password=^PASS^:Invalid login"

Replace /login with the actual login page path and Invalid login with the server's response for failed logins.

FTP Login:

Code `hydra -l admin -P mywordlist.txt ftp://<target IP>`

6. Advanced Hydra Options

Threading: Use -t to specify the number of threads for faster brute-forcing (e.g., -t 10).

Verbose Output: Add -v or -V to see the progress of each attempt.

Saving Results: Use -o to save results to a file:

Code `hydra -l admin -P mywordlist.txt ssh://<target IP> -o results.txt`

7. Understanding Results

Once Hydra completes its operation, it will display valid login credentials (if found). For example:

Code `[22][ssh] host: 192.168.1.10 login: admin password: password123`

8. Ethical Usage

Always ensure you have explicit permission to test a system. Never use Hydra on unauthorized systems, it's illegal and unethical.

This thread is pretty cool, very clear and brief information, I will study it more thoroughly, thanks.

alachner - October 12, 2025, 8:41 am

Thanks you bro

zeealive - November 23, 2025, 12:47 am

Thank you. Good tutorial.