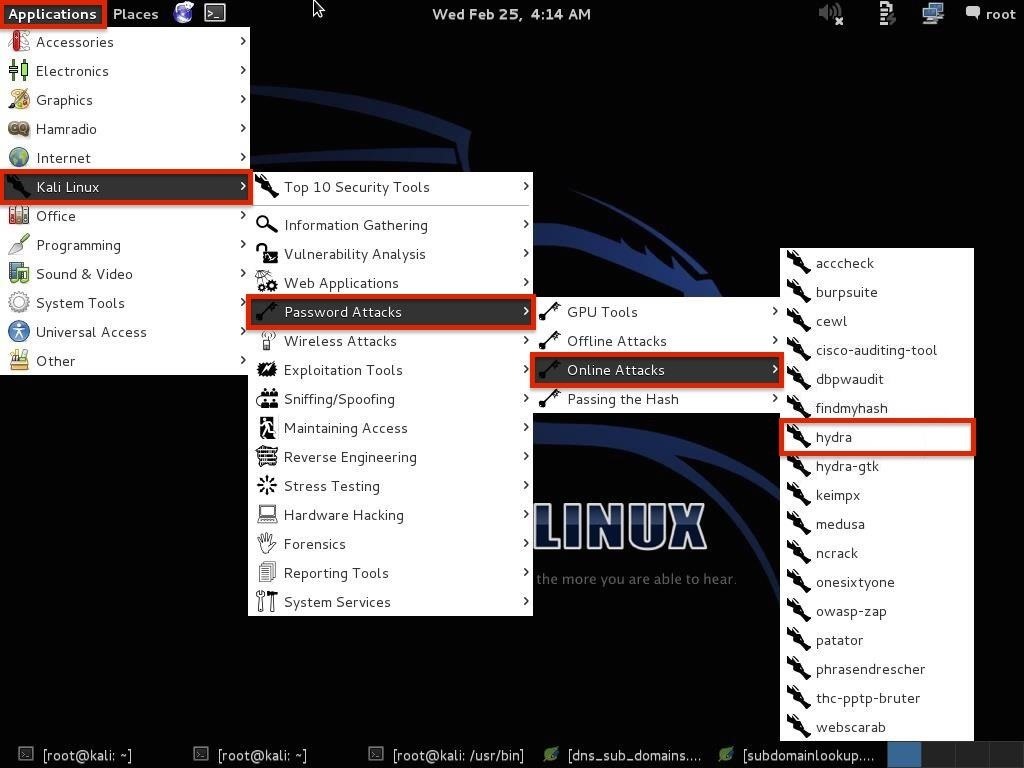
**Hydra Tool** is a password detection **tool** (cracking) that can be used in a wide range of situations, including authentication-based forms commonly used in web applications. ... When you need brute force cracking remote authentication, **Hydra Tool** is a service often a **tool** of choice.

<https://www.concise-courses.com/what-is-hydra/>

Step 1Open THC-Hydra

So, let's get started. Fire up [Kali](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-kali-your-new-hacking-system-0151631/) and open THC-Hydra from Applications -> Kali Linux -> Password Attacks -> Online Attacks -> hydra.

[](https://img.wonderhowto.com/img/original/39/40/63561584064222/0/635615840642223940.jpg)

Step 2Get the Web Form Parameters

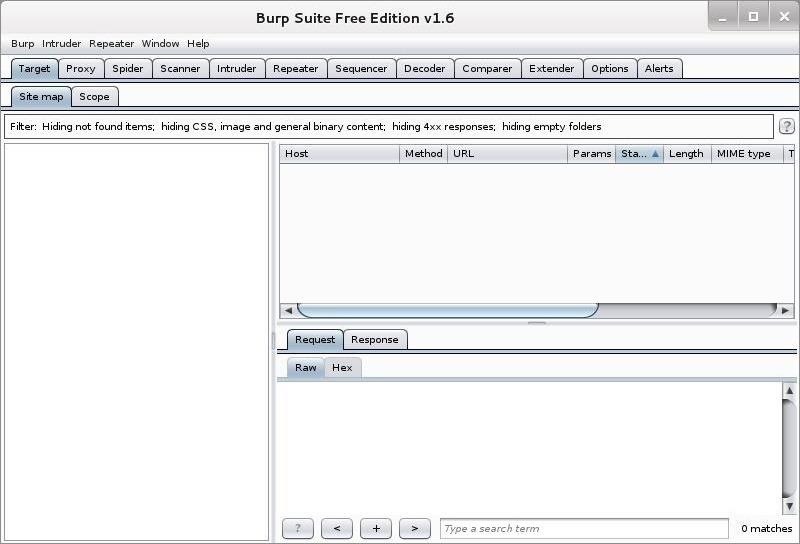
To be able to hack web form usernames and passwords, we need to determine the parameters of the web form login page as well as how the form responds to bad/failed logins. The key parameters we must identify are the:

* IP Address of the website
* URL
* type of form
* field containing the username
* field containing the password
* failure message

We can identify each of these using a proxy such as Tamper Data or Burp Suite.

Step 3Using Burp Suite

Although we can use any proxy to do the job, including Tamper Data, in this post we will use Burp Suite. You can open Burp Suite by going to Applications -> Kali Linux -> Web Applications -> Web Application Proxies -> burpsuite. When you do, you should see the opening screen like below.

[](https://img.wonderhowto.com/img/original/48/12/63561584079675/0/635615840796754812.jpg)

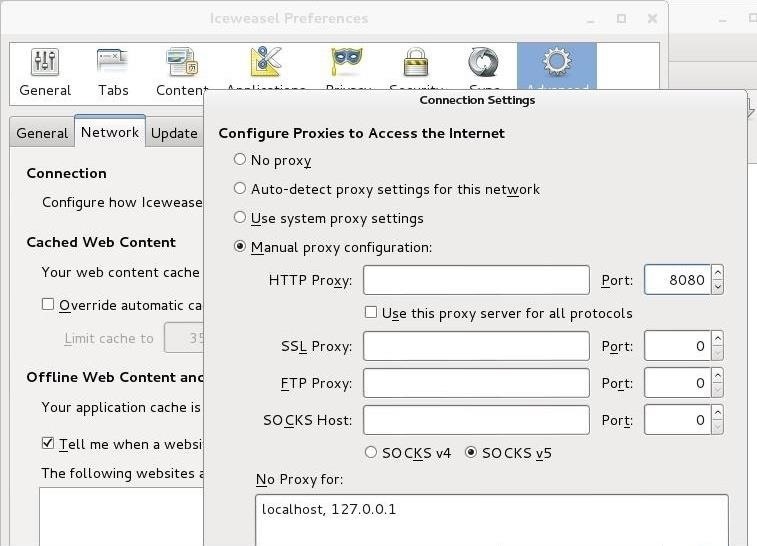
Next, we will be attempting to crack the password on the Damn Vulnerable Web Application (DVWA). You can run it from the Metasploitable operating system ([available at Rapid7](https://information.rapid7.com/metasploitable-download.html)) and then connecting to its login page, as I have here.

[](https://img.wonderhowto.com/img/original/93/87/63561584110612/0/635615841106129387.jpg)

We need to enable the *Proxy* and *Intercept* on the Burp Suite like I have below. Make sure to click on the *Proxy* tab at the top and then *Intercept* on the second row of tabs. Make certain that the "Intercept is on."

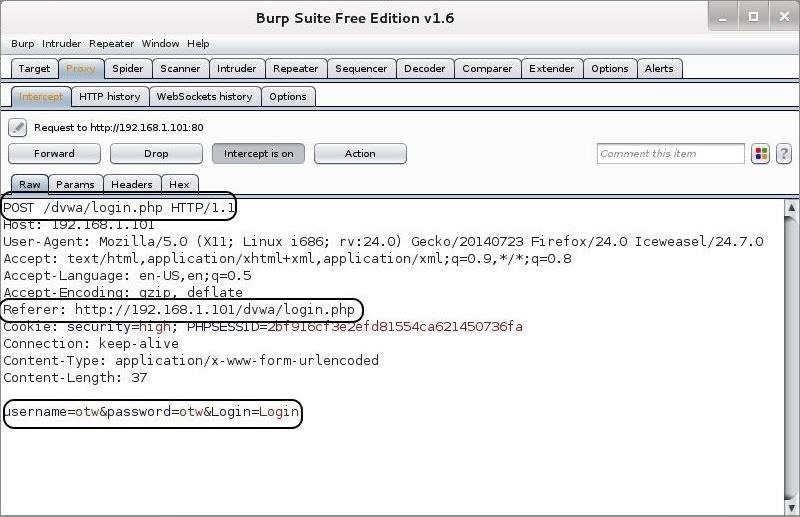
[](https://img.wonderhowto.com/img/original/10/87/63561584124441/0/635615841244411087.jpg)

Last, we need to configure our IceWeasel web browser to use a proxy. We can go to Edit -> Preferences -> Advanced -> Network -> Settings to open the Connection Settings, as seen below. There, configure IceWeasel to use 127.0.0.1 port 8080 as a proxy by typing in 127.0.0.1 in the *HTTP Proxy* field, 8080 in the *Port* field and delete any information in the *No Proxy for* field at the bottom. Also, select the "Use this proxy server for all protocols" button.

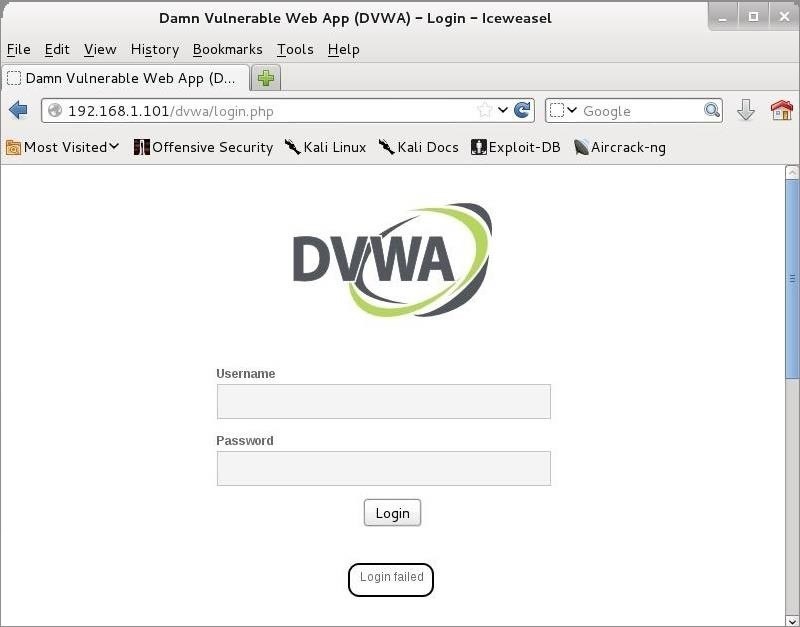
[](https://img.wonderhowto.com/img/original/95/31/63561584136862/0/635615841368629531.jpg)

Step 4Get the Bad Login Response

Now, let's try to log in with my username OTW and password OTW. When I do so, the BurpSuite intercepts the request and shows us the key fields we need for a THC-Hydra web form crack.

[](https://img.wonderhowto.com/img/original/61/28/63561584149378/0/635615841493786128.jpg)

After collecting this information, I then forward the request from Burp Suite by hitting the "Forward" button to the far left . The DVWA returns a message that the "Login failed." Now, I have all the information I need to configure THC-Hydra to crack this web app!

[](https://img.wonderhowto.com/img/original/05/04/63561584166035/0/635615841660350504.jpg)

Getting the failure message is key to getting THC-Hydra to work on web forms. In this case, it is a text-based message, but it won't always be. At times it may be a cookie, but the critical part is finding out how the application communicates a failed login. In this way, we can tell THC-Hydra to keep trying different passwords; only when that message does not appear, have we succeeded.

Step 5Place the Parameters into Your THC Hydra Command

Now, that we have the parameters, we can place them into the THC-Hydra command. The syntax looks like this:

***kali > hydra -L <username list> -p <password list> <IP Address> <form parameters><failed login message>***

So, based on the information we have gathered from Burp Suite, our command should look something like this:

***kali >hydra -L <wordlist> -P<password list>  
192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"***

A few things to note. First, you use the upper case "L" if you are using a username list and a lower case "l" if you are trying to crack one username that you supply there. In this case, I will be using the lower case "l " as I will only be trying to crack the "admin" password.

After the address of the login form (*/dvwa/login.php*), the next field is the name of the field that takes the username. In our case, it is "username," but on some forms it might be something different, such as "login."

Now, let's put together a command that will crack this web form login.

Step 6Choose a Wordlist

Now, we need to chose a wordlist. As with any dictionary attack, the wordlist is key. You can use a custom one made with [Crunch](https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817/) of [CeWL](https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-5-creating-custom-wordlist-with-cewl-0158855/), but Kali has numerous wordlists built right in. To see them all, simply type:

***kali > locate wordlist***

In addition, there are numerous online sites with wordlists that can be up to 100 GB! Choose wisely, my hacker novitiates. In this case, I will be using a built-in wordlist with less than 1,000 words at:

***/usr/share/dirb/wordlists/short.txt***

Step 7Build the Command

Now, let's build our command with all of these elements, as seen below.

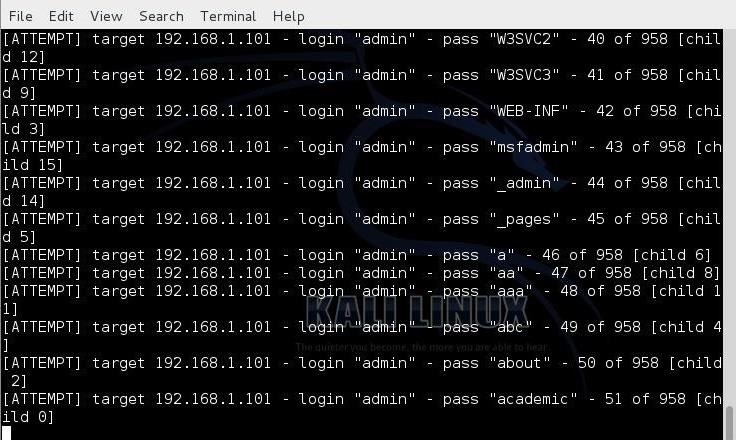
***kali > hydra -l admin -P /usr/share/dirb/wordlists/small.txt 192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V***

[](https://img.wonderhowto.com/img/original/50/71/63561584187175/0/635615841871755071.jpg)

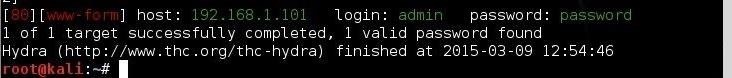
* **-l** indicates a single username (use **-L** for a username list)
* **-P** indicates use the following password list
* **http-post-form** indicates the type of form
* **/dvwa/login-php** is the login page URL
* **username** is the form field where the username is entered
* **^USER^** tells Hydra to use the username or list in the field
* **password** is the form field where the password is entered (it may be passwd, pass, etc.)
* **^PASS^** tells Hydra to use the password list supplied
* **Login** indicates to Hydra the login failed message
* **Login failed** is the login failure message that the form returned
* **-V** is for verbose output showing every attempt

Step 8Let Her Fly!

Now, let her fly! Since we used the ***-V*** switch, THC-Hydra will show us every attempt.

[](https://img.wonderhowto.com/img/original/86/89/63561584198909/0/635615841989098689.jpg)

After a few minutes, Hydra returns with the password for our web application. Success!

[](https://img.wonderhowto.com/img/original/28/14/63561584210316/0/635615842103162814.jpg)

Final Thoughts

Although THC-Hydra is an effective and excellent tool for online [password cracking](https://null-byte.wonderhowto.com/how-to/password-cracking/), when using it in web forms, it takes a bit of practice. The key to successfully using it in web forms is determining how the form responds differently to a failed login versus a successful login. In the example above, we identified the failed login message, but we could have identified the successful message and used that instead. To use the successful message, we would replace the failed login message with "S=successful message" such as this:

***kali > hydra -l admin -P /usr/share/dirb/wordlists/small.txt 192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&S=success message" -V***

Also, some web servers will notice many rapid failed attempts at logging in and lock you out. In this case, you will want to use the wait function in THC-Hydra. This will add a wait between attempts so as not to trigger the lockout. You can use this functionality with the ***-w*** switch, so we revise our command to wait 10 seconds between attempts by writing it:

***kali > hydra -l admin -P /usr/share/dirb/wordlists/small.txt 192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -w 10 -V***

I recommend that you practice the use of THC-Hydra on forms where you know the username and password before using it out "in the wild."

Keep coming back, my hacker novitiates, as we continue to expand your repertoire of hacker techniques and arts!

**John The ripper – kali Linux**

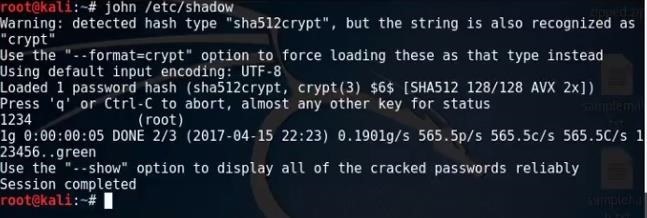
**1.Cracking Linux User Password**  
**2.Cracking Password Protected ZIP/RAR Files**  
**3.Decrypting MD5 Hash**  
**4.Using Wordlists To Crack Passwords**  
Lets begin.

## Cracking Linux User Password

The linux user password is saved in /etc/shadow folder.  
So to crack it, we simply type :

john /etc/shadow

It will take a while depending on your system.

[](https://img.wonderhowto.com/img/original/13/66/63647565251018/0/636475652510181366.jpg)

## Cracking Password Protected ZIP/RAR Files

First, go to the directory of the file.  
I will assume that everyone here can do that.  
After, use this command :

zip2john zipfile > output.txt

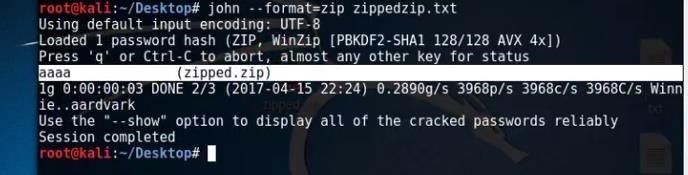
(If it is a RAR file, replace the zip in the front to rar.)

Replace the "zip file" with the name of the zip file you are trying to crack and replace the "output.txt" with any name that is a .txt format.

After that command, you will see that it would have marked a text file.  
The hashes are stored in that file.  
To crack the hash, type:

**john --format=zip hashfilepath**

Again, replace the "hashfilepath" to yours. Mine is just an example.  
Now, wait, and you can see it is cracked.

[](https://img.wonderhowto.com/img/original/83/85/63647566200084/0/636475662000848385.jpg)

Now go in the zip file and put the password.

## Decrypting MD5 Hash

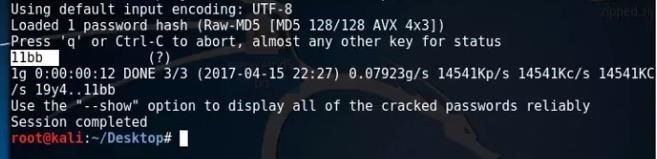
I have my Hash over here:

[https://img.wonderhowto.com/img/03/14/63647566548288/0/cracking-passwords-using-john-ripper.w1456.jpg](https://img.wonderhowto.com/img/original/03/14/63647566548288/0/636475665482880314.jpg)

Now, let’s use john to decrypt it.  
To decrypt it, use this:

**john --format=raw-md5 hashfilepath**

Again, repl......  
I won't say it.  
And now enter, and should take a while and it will decrypt it.

[](https://img.wonderhowto.com/img/original/75/47/63647566751928/0/636475667519287547.jpg)

And boom.

## Using Wordlists to Crack Passwords

I don't really recommend this one, but there are some peoples out there using this to crack...  
I will crack a hash that is inside a text file.  
I have a wordlist here, and I named it password.txt.  
To use the wordlist and crack the file, do :

**john --format=raw-shal --wordlist password.txt THEHASHFILE.txt**