**FFUF TOOL**

**‘ffuf’** tool (Fuzz Faster U Fool), which is a web fuzzing tool used for finding hidden web resources and vulnerabilities.

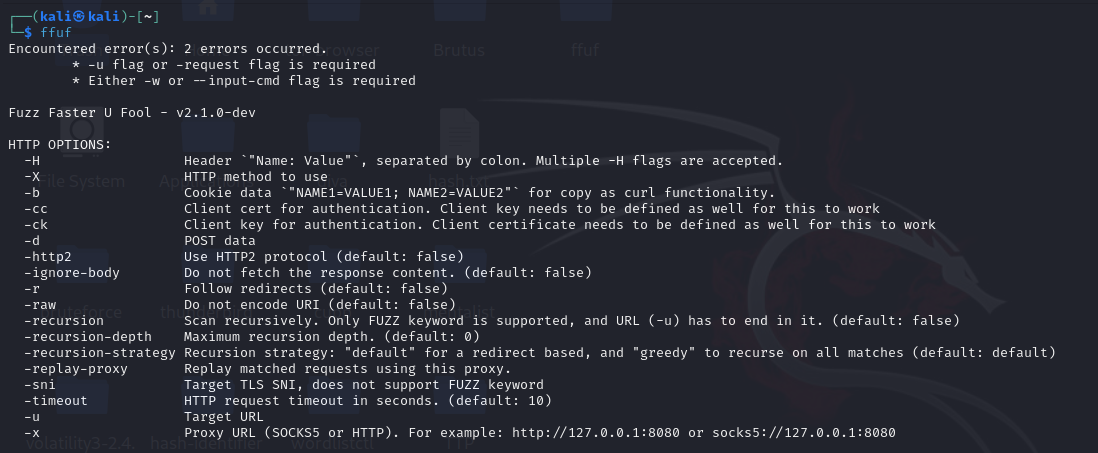
1. ‘ffuf’ is a web fuzzing tool written in Go
2. It is used for brute-forcing web applications.
3. It discovers hidden directories, parameters in web applications.

Installing fuff tool:

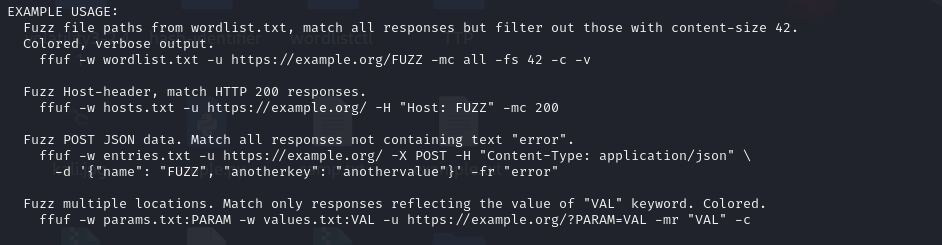
To install this ffuf tool we have the following command:

**sudo apt install ffuf -y**

After installation, to work with it type ffuf.



It shows multiple options. If we scroll down to the bottom we can see the example usage.



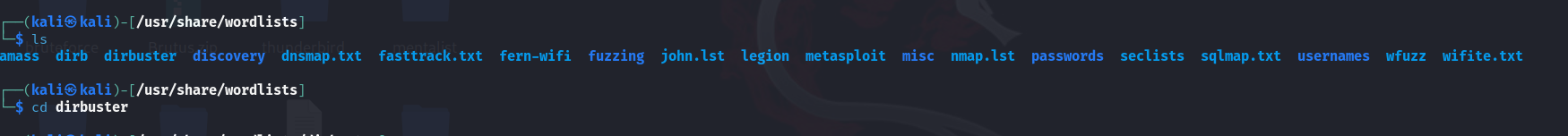
If we look in to the above image clearly we can see it requires a wordlist.

In kali linux we will get inbuilt wordlist. If we don’t have any wordlist we can install from google.

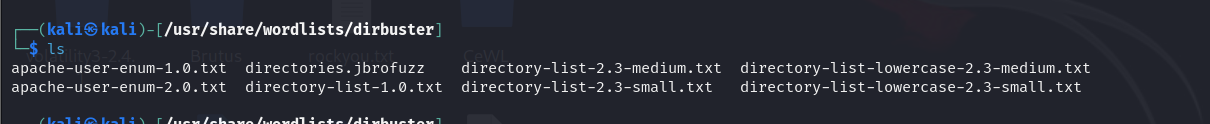
<https://github.com/danielmiessler/SecLists> -- SECLISTS

Follow this repository to install secLists [word lists for different purposes].

We will the wordlists for linux in path as shown in below image.



In the above image, you can see there are multiple word lists present. Since we are working ffuf[fuzzing] to find out the directories we are moving to dirbuster. These are the list of words that are available.



So now we will proceed with medium wordlist.

We need a target site which followed by “–u”.

-u 🡪 url

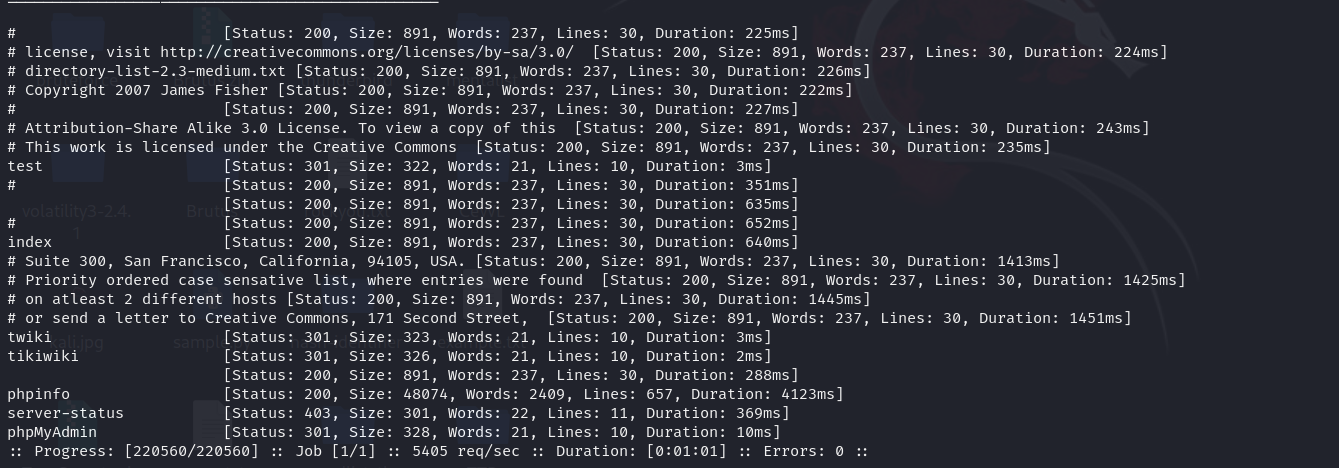
-w 🡪 wordlist.

I am currently using my metasploitable as my url.

Now, if we start ffuf tool, we can find the following



The above image describes the interface working with ffuf. The result will be



We can find the above directories along with their response codes.

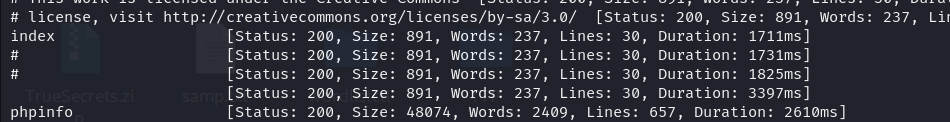
* **200:** OK - Request succeeded.
* **201-299:** Success - Request processed successfully.
* **301:** Moved Permanently - Resource has been permanently moved to a new URL.
* **302:** Found - Resource temporarily moved to a new URL.
* **307:** Temporary Redirect - Resource temporarily moved, repeat request to new URL.
* **401:** Unauthorized - Authentication required.
* **403:** Forbidden - Server refuses to fulfill the request.
* **405:** Method Not Allowed - Request method is not supported by the resource.
* **500:** Internal Server Error - Generic server error.

We can also filter using response codes.



-mc 🡪 Match HTTP status codes, or "all" for everything. (default: 200-299,301,302,307,401,403,405,500)

So I filtered only 200 which says ok.



So, in the output we only got the response codes saying 200.