🕵️🌐 Subdomain Identification

Intro

The attack surface in a Web audit is not reduced to the main domain, but in an organization, whether large or medium, a domain will be made up of several **subdomains** where *you will host your own web applications*. This is why it is very important to identify all the subdomains that exist, because they are **potential points of attack.**

This is very useful if we see that the main web application we are auditing has no faults or is protected with a *waf.* Many companies, in order to save costs, prefer not to put waf on a subdomain in a commercial waf and to save costs they prefer to put these measures only on their main page.

On many occasions they can leave subdomains or applications that are not included in these security tools. It's also possible that they forgot that applications exist on a subdomain and didn't update.

This greatly expands the attack surface of the organization we are auditing.

⚙️ Tools for Subdomain Identification

👩‍🎨 Subfinder

Intro
Tool to discover validated subdomains of a web page using **passive sources of information**. This means that we will not interact directly with the organization's systems.

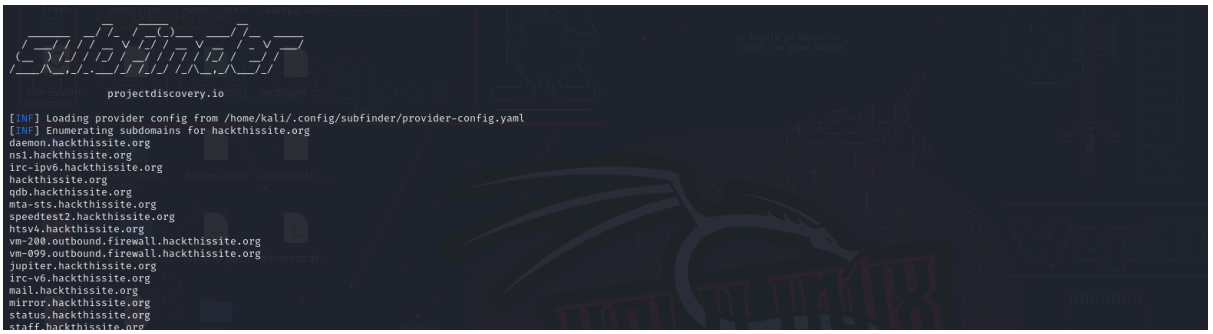
This tool does not come pre installed in Kali so you have to install it with the command:

sudo apt install subfinder

To put it to work **Subfinder** we just put the domain of the organization with the command

subfinder -d sitioweb.com

And the result would be something like:



Also, if we want to save the result in a .txt file we can do it with the command:

subfinder -d sitioweb.com > document.txt

Also We can add indicating API keys using entering from a text editor, be it nano or whatever we prefer, to the address **.config/subfinder/provider-config.yaml** and we can add APIs like those of **Shoda, Censys** or those that we want

🕵️📜 Sublist3r

Intro

This, like subfinder, is responsible for searching for web application subdomains in public places. But it also incorporates a second tool, SubBrute**,** which lists made requests to *name servers* public, which means it is more active than subfinder.

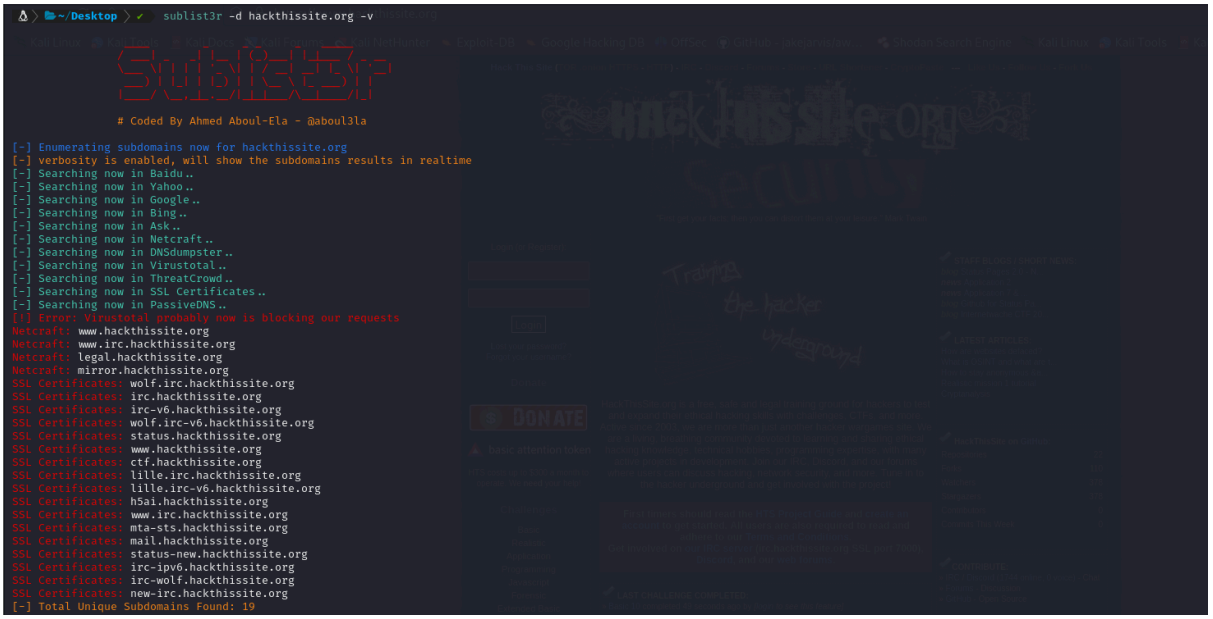
This does not come pre-installed in 🐉 kali either, but just run the following command to install it:

sudo apt install sublist3r

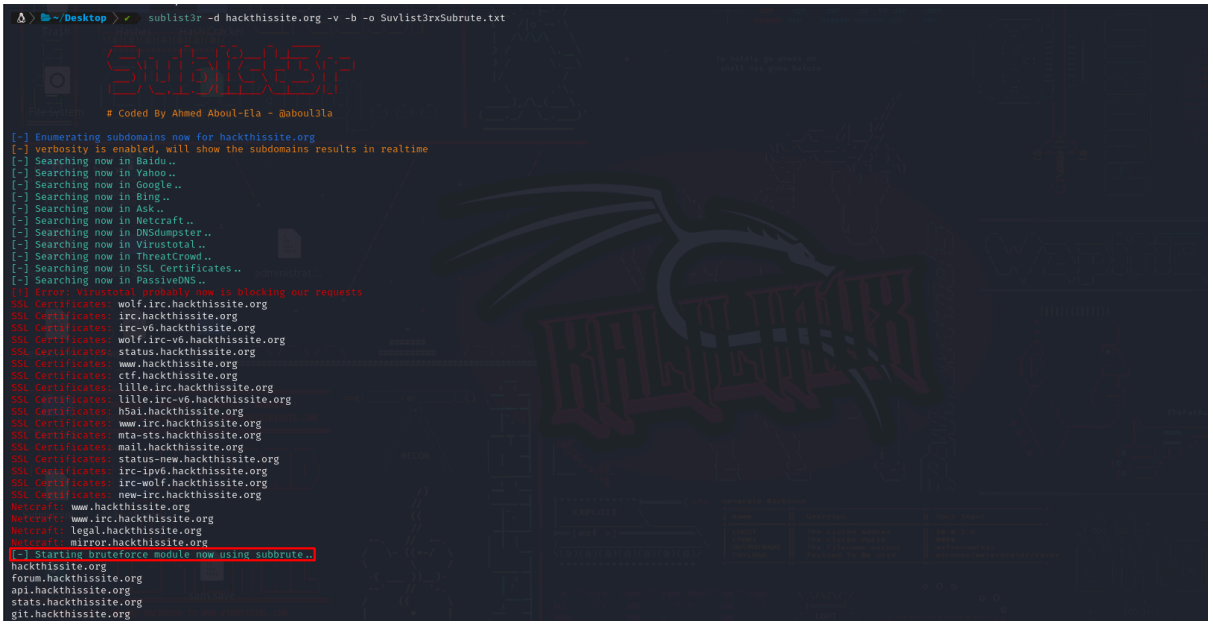
To use it we just have to use the command

sublist3r -d sitioweb.com -v

And the result would be something like this



We can also use the option **SubBrute** with the **-b** to the previous sentence and the result would be something like this:



Remember that this SubBrute module is more intrusive, it must be done with caution and only used in consensual audits

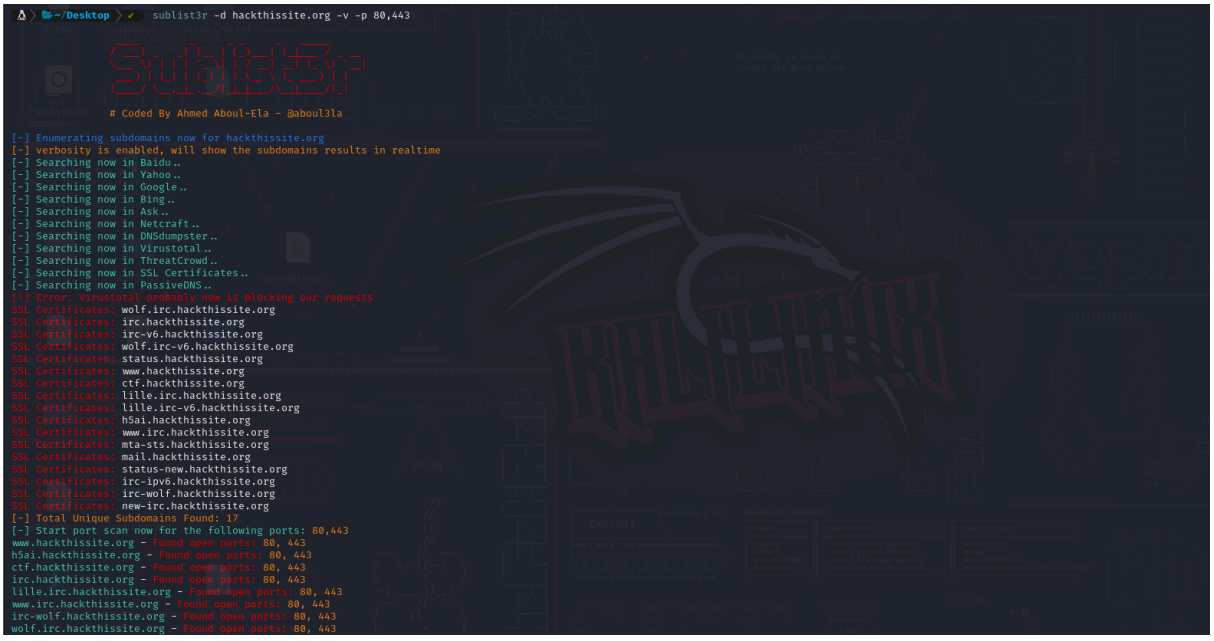
Interaction with web application port with

Another way to interact with it would be to do the normal command **sublist3r** and with the -p command plus placing the ports we can make an active scalene interacting with the machines that host said subdomains to the TCP ports

Example

sublist3r -d hackthissite.org -v -p 443,80

And the result would be something like this:



With **wireshark**🦈 we can see the network traffic it generates and you can even see the IP address.

📝**Note:** Adding the command **-o** we can create an output file with the extension we want as **txt**