

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.

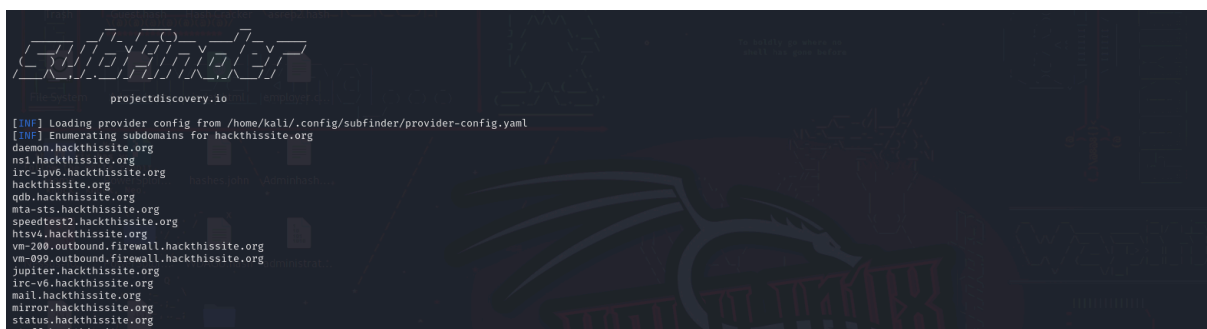
This tool does not come pre installed in Kali so you have to install it with the command:

sudo apt install subfinder

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

subfinder -d target.website

And the result would be something like:



```
Subfinder
projectdiscovery.io

[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for hackthissite.org
daemon.hackthissite.org
ns1.hackthissite.org
irc-ipv6.hackthissite.org
hackthissite.org
qdb.hackthissite.org
mta-sts.hackthissite.org
speedtest2.hackthissite.org
https4.hackthissite.org
vm-200.outbound.firewall.hackthissite.org
vm-099.outbound.firewall.hackthissite.org
jupiter.hackthissite.org
irc-v6.hackthissite.org
mail.hackthissite.org
mirror.hackthissite.org
status.hackthissite.org
staff.hackthissite.org
```

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



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 target.website -v
```

And the result would be something like this

```

┌─> ~/Desktop > ./sublist3r -d hackthissite.org -v
Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for hackthissite.org
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
Netcraft: www.hackthissite.org
Netcraft: www.irc.hackthissite.org
Netcraft: legal.hackthissite.org
Netcraft: mirror.hackthissite.org
SSL Certificates: wolf.irc.hackthissite.org
SSL Certificates: irc.hackthissite.org
SSL Certificates: irc-v6.hackthissite.org
SSL Certificates: wolf.irc-v6.hackthissite.org
SSL Certificates: status.hackthissite.org
SSL Certificates: www.hackthissite.org
SSL Certificates: ctf.hackthissite.org
SSL Certificates: lille.irc.hackthissite.org
SSL Certificates: lille.irc-v6.hackthissite.org
SSL Certificates: h5ai.hackthissite.org
SSL Certificates: www.irc.hackthissite.org
SSL Certificates: mta-sts.hackthissite.org
SSL Certificates: mail.hackthissite.org
SSL Certificates: status-new.hackthissite.org
SSL Certificates: irc-ipv6.hackthissite.org
SSL Certificates: irc-wolf.hackthissite.org
SSL Certificates: new.irc.hackthissite.org
[-] Total Unique Subdomains Found: 19
```

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

```

[~] Desktop > sublist3r -d hackthissite.org -v -b -o Sublist3rxSubBrute.txt

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for hackthissite.org
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Error: Virustotal probably now is blocking our requests
SSL Certificates: wolf.irc.hackthissite.org
SSL Certificates: irc.hackthissite.org
SSL Certificates: irc-v6.hackthissite.org
SSL Certificates: wolf.irc-v6.hackthissite.org
SSL Certificates: status.hackthissite.org
SSL Certificates: www.hackthissite.org
SSL Certificates: ctf.hackthissite.org
SSL Certificates: lille.irc.hackthissite.org
SSL Certificates: lille.irc-v6.hackthissite.org
SSL Certificates: h5ai.hackthissite.org
SSL Certificates: www.irc.hackthissite.org
SSL Certificates: mta-sts.hackthissite.org
SSL Certificates: mail.hackthissite.org
SSL Certificates: status-new.hackthissite.org
SSL Certificates: irc-ipv6.hackthissite.org
SSL Certificates: irc-wolf.hackthissite.org
SSL Certificates: new-irc.hackthissite.org
Netcraft: www.hackthissite.org
Netcraft: www.irc.hackthissite.org
Netcraft: legal.hackthissite.org
Netcraft: mirror.hackthissite.org
[-] Starting bruteForce module now using subbrute..
hackthissite.org
forum.hackthissite.org
api.hackthissite.org
stats.hackthissite.org
git.hackthissite.org

```

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 target.website -v -p 443,80

And the result would be something like this:


```


[~] Desktop > sublist3r -d hackthissite.org -v -p 80,443

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for hackthissite.org
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Error: Virustotal probably now is blocking our requests
SSL Certificates: wolf.irc.hackthissite.org
SSL Certificates: irc.hackthissite.org
SSL Certificates: irc-v6.hackthissite.org
SSL Certificates: wolf.irc-v6.hackthissite.org
SSL Certificates: status.hackthissite.org
SSL Certificates: www.hackthissite.org
SSL Certificates: ctf.hackthissite.org
SSL Certificates: lille.irc.hackthissite.org
SSL Certificates: lille.irc-v6.hackthissite.org
SSL Certificates: h5ai.hackthissite.org
SSL Certificates: www.irc.hackthissite.org
SSL Certificates: mta-sts.hackthissite.org
SSL Certificates: mail.hackthissite.org
SSL Certificates: status-new.hackthissite.org
SSL Certificates: irc-ipv6.hackthissite.org
SSL Certificates: irc-wolf.hackthissite.org
SSL Certificates: new-irc.hackthissite.org
[-] Total Unique Subdomains Found: 17
[-] Start port scan now for the following ports: 80,443
www.hackthissite.org - Found open ports: 80, 443
h5ai.hackthissite.org - Found open ports: 80, 443
ctf.hackthissite.org - Found open ports: 80, 443
irc.hackthissite.org - Found open ports: 80, 443
lille.irc.hackthissite.org - Found open ports: 80, 443
www.irc.hackthissite.org - Found open ports: 80, 443
irc-wolf.hackthissite.org - Found open ports: 80, 443
irc-wolf.hackthissite.org - Found open ports: 80, 443
wolf.irc.hackthissite.org - Found open ports: 80, 443

```

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**