Hunting Subdomains

Part 1

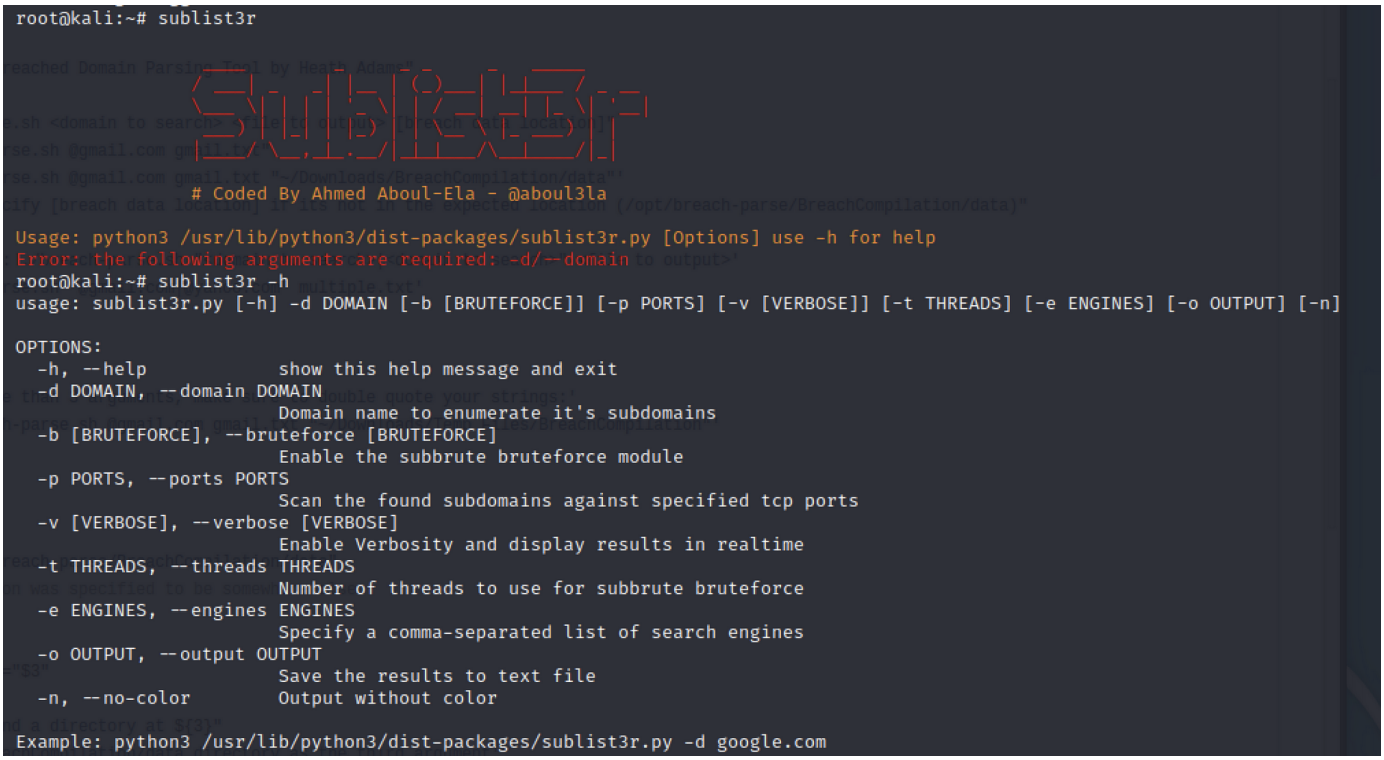
Sometimes, we might be tasked with finding information on subdomains of websites and domains. This is because we might find websites and subdomains that should not be found on the internet. For example a "Top-Secret" domain.

We will be using a tool called `sublist3r` to search for subdomains. We need to manually install this tool using the following command: `apt install sublist3r`.

Once it is installed we can use it to search for subdomains.

To use `sublist3r` we need to use the following syntax:

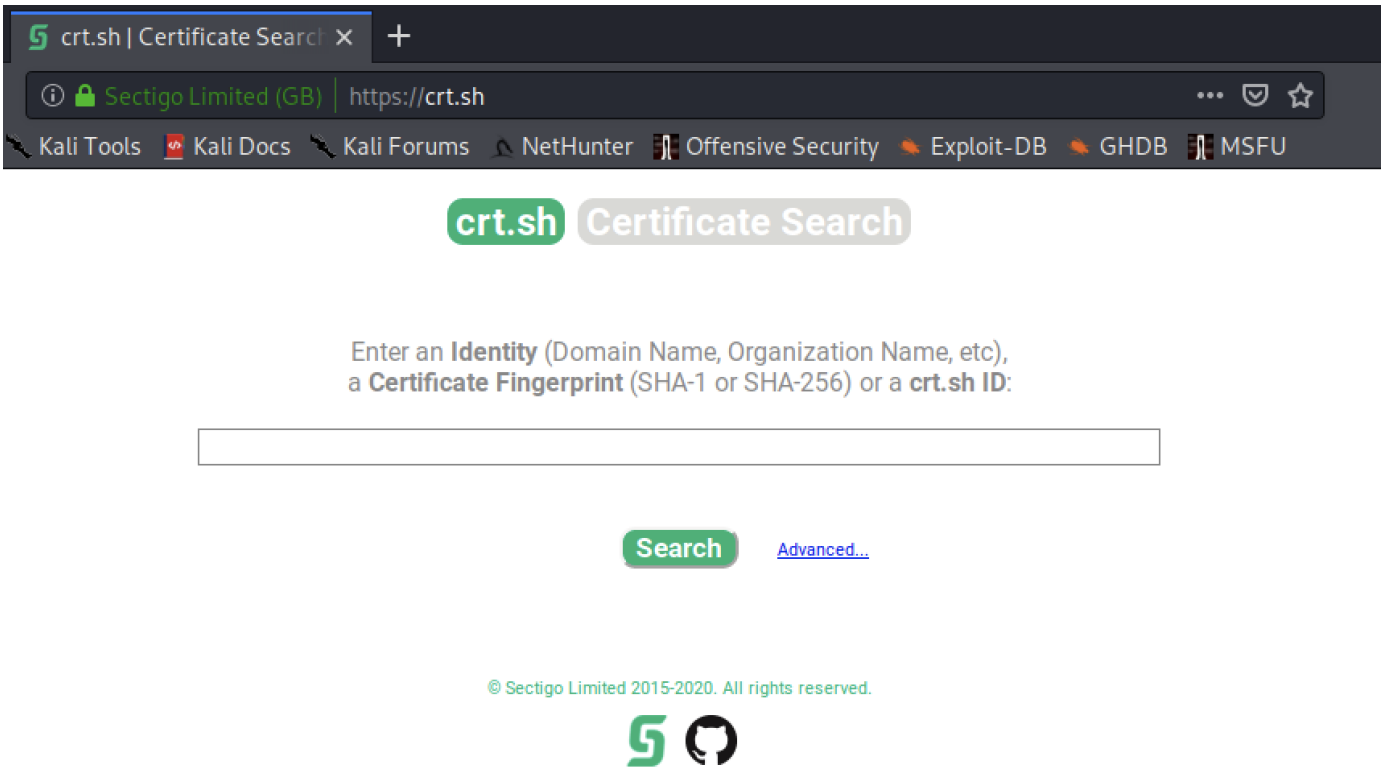
1. `sublist3r -h` for help as shown below:



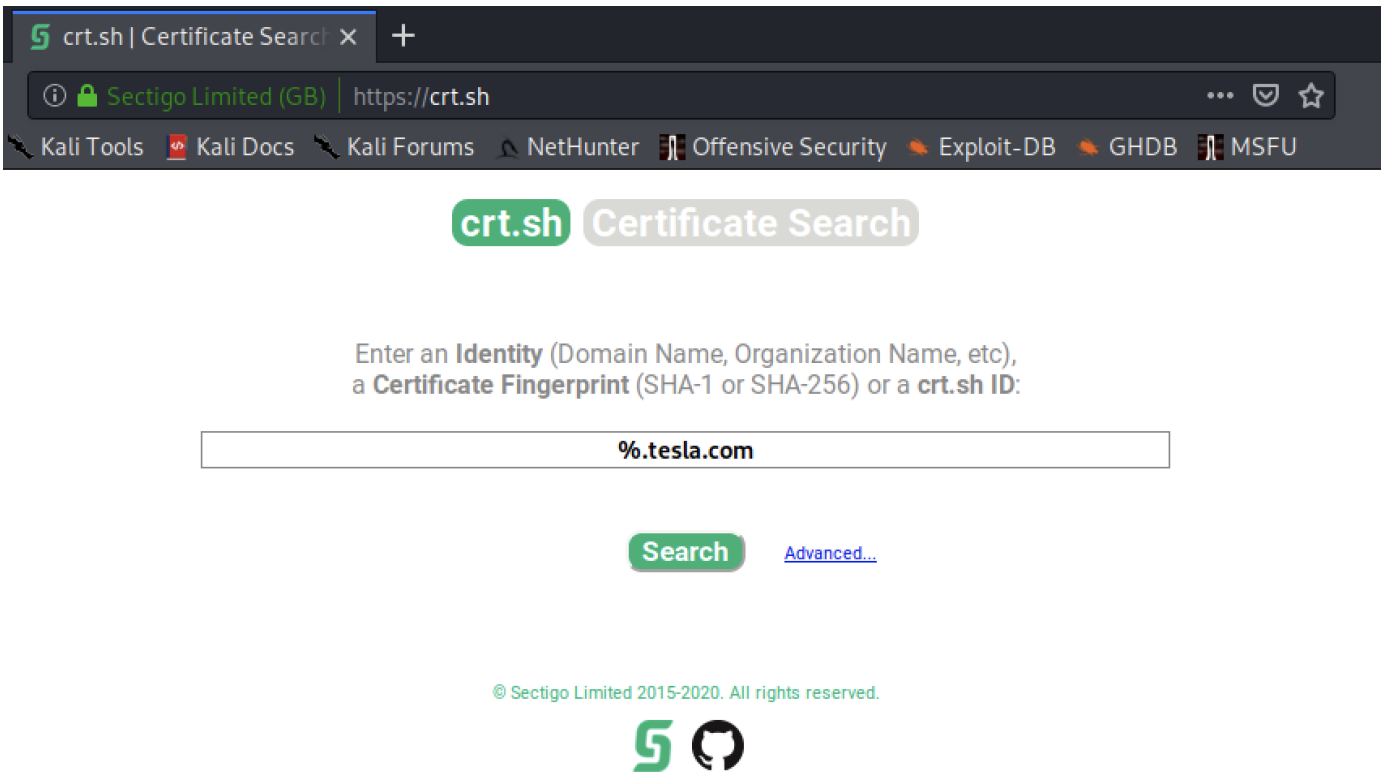
2. `sublist3r -d tesla.com` for a subdomain search on the `tesla.com` domain as shown below:

In this scenario, it gave many results (not all are shown).

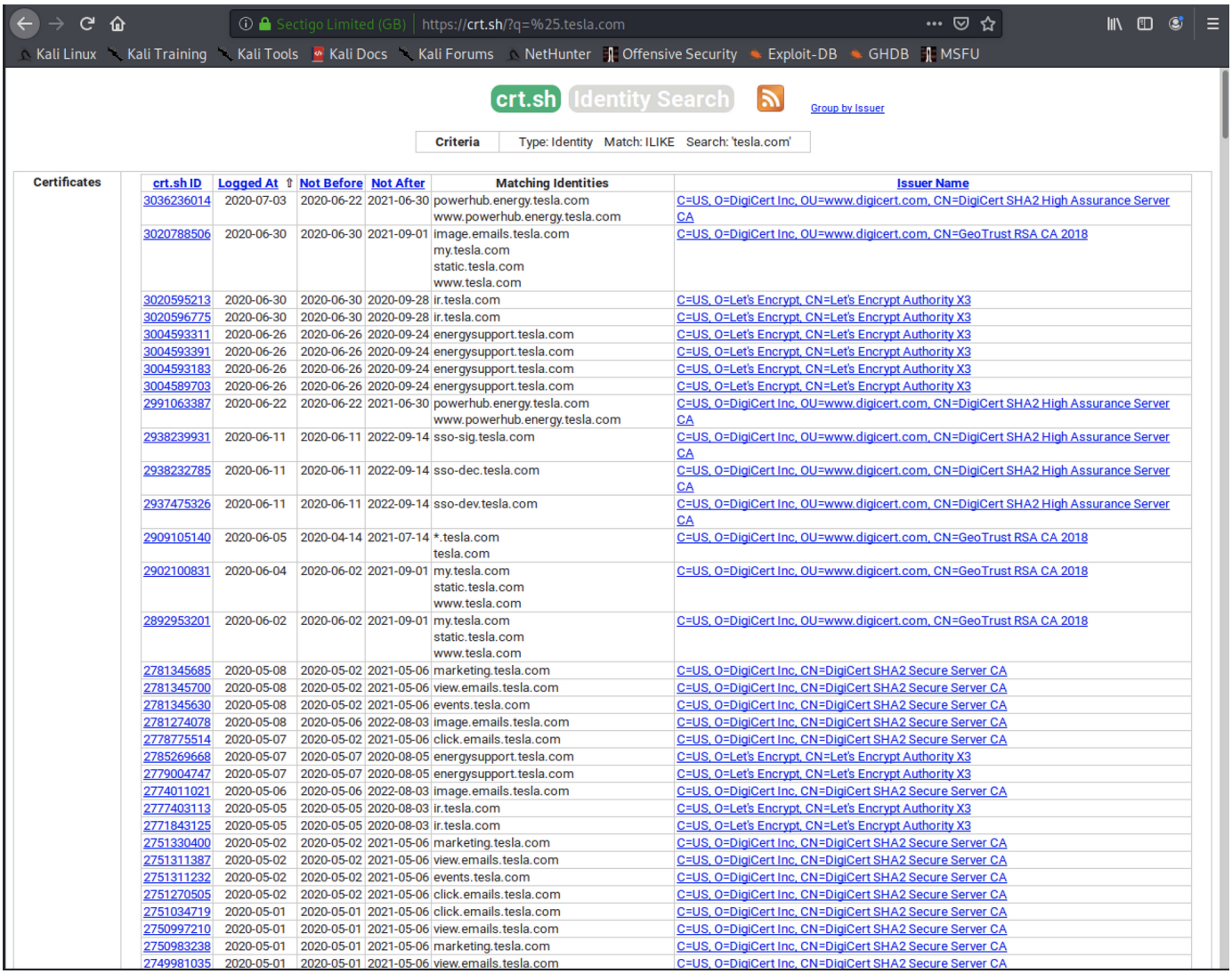
Another tool that we use is a web tool called `crt.sh`. It can be found at https://crt.sh as shown below:



We can do a "wildcard" search for a domain. In our case, the syntax is: `%.domain.com` as shown below:



These are the results from that search:



crt.sh ID	Logged At ⇧	Not Before	Not After	Matching Identities	Issuer Name
3036236014	2020-07-03	2020-06-22	2021-06-30	powerhub.energy.tesla.com www.powerhub.energy.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
3020788506	2020-06-30	2020-06-30	2021-09-01	image.emails.tesla.com my.tesla.com static.tesla.com www.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
3020595213	2020-06-30	2020-06-30	2020-09-28	ir.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3020596775	2020-06-30	2020-06-30	2020-09-28	ir.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3004593311	2020-06-26	2020-06-26	2020-09-24	energysupport.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3004593391	2020-06-26	2020-06-26	2020-09-24	energysupport.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3004593183	2020-06-26	2020-06-26	2020-09-24	energysupport.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3004589703	2020-06-26	2020-06-26	2020-09-24	energysupport.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2991063387	2020-06-22	2020-06-22	2021-06-30	powerhub.energy.tesla.com www.powerhub.energy.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2938239931	2020-06-11	2020-06-11	2022-09-14	sso-sig.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2938232785	2020-06-11	2020-06-11	2022-09-14	sso-dec.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2937475326	2020-06-11	2020-06-11	2022-09-14	sso-dev.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2909105140	2020-06-05	2020-04-14	2021-07-14	*.tesla.com tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
2902100831	2020-06-04	2020-06-02	2021-09-01	my.tesla.com static.tesla.com www.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
2892953201	2020-06-02	2020-06-02	2021-09-01	my.tesla.com static.tesla.com www.tesla.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
2781345685	2020-05-08	2020-05-02	2021-05-06	marketing.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2781345700	2020-05-08	2020-05-02	2021-05-06	view.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2781345630	2020-05-08	2020-05-02	2021-05-06	events.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2781274078	2020-05-08	2020-05-06	2022-08-03	image.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2778775514	2020-05-07	2020-05-02	2021-05-06	click.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2785269668	2020-05-07	2020-05-07	2020-08-05	energysupport.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2779004747	2020-05-07	2020-05-07	2020-08-05	energysupport.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2774011021	2020-05-06	2020-05-06	2022-08-03	image.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2777403113	2020-05-05	2020-05-05	2020-08-03	ir.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2771843125	2020-05-05	2020-05-05	2020-08-03	ir.tesla.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2751330400	2020-05-02	2020-05-02	2021-05-06	marketing.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2751311387	2020-05-02	2020-05-02	2021-05-06	view.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2751311232	2020-05-02	2020-05-02	2021-05-06	events.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2751270505	2020-05-02	2020-05-02	2021-05-06	click.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2751034719	2020-05-01	2020-05-01	2021-05-06	click.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2750997210	2020-05-01	2020-05-01	2021-05-06	view.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2750983238	2020-05-01	2020-05-01	2021-05-06	marketing.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
2749981035	2020-05-01	2020-05-01	2021-05-06	view.emails.tesla.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

This tool uses a concept called "Certficate Fingerprinting" to find the certificates of sites registered to that domain.

We can also find sub-subdomains (4 domain levels).

Part 2

One of the most popular tools to use is called OWASP Amass which can be found on github here: https://github.com/OWASP/Amass. It is a fairly complex tool

Another tool that helps with subdomain probing is called `httprobe` it was made by tomnomnom. It can be found here: https://github.com/tomnomnom/httprobe. It's a fairly easy tool to use. Once you generate a list of subdomains, you'll generally need to check them and see which ones work and don't work. This tool makes that task of checking a lot easier by checking them for you.
