Hunting Subdomains Part 1

Passively gathering information.

The first thing is finding subdomains for websites.

subdomains are ex: "dev.tesla.com", or "test.tesla.com".

Sublist3r is an awesome tool to find the subdomains.

#apt install sublist3r

Usage: #sublist3r -d tesla.com

This will passively search the subdomains for the website specified.

Another tool we can use is the " https://crt.sh"

Usage: "%.tesla.com"

Use the wildcard to identify all subdomains. We are looking for sso, vpn, dev, epi-toolbox, sso-dev.....

Hunting Subdomains Part 2

Owasp amass - is another tool to find subdomains. Seems to be the latest and greatest. We need to install it on our kali linux.

Another one is the : tomnomnom httprobe which is a probe tool. It is going to probe the different subdomains for a website to assess if they are alive or not.