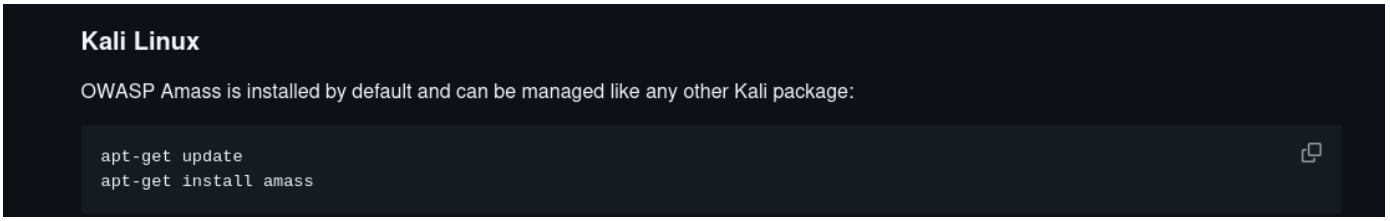
03 - Amass - Finding Subdomains

So, the idea here to learn another subdomain tool is that it uses other methods to find the subdomains for the domain name, so we could get different results with it, results that we did not pick up before with other tools.

So, we can make one script, run all the tools available, or the ones we want to run in the script, go through the list, rm the duplicate ones, and keep the rest.

https://github.com/owasp-amass/amass

Reading the repo:



We do not need to install.

To run:

"#amass enum -d tesla.com"

So, the script we had, we are going to be incrementing on the same code. We want to have a single file with no duplicates, and we are going to use that file to probe the subdomains to see if they are alive using http