🕐

Day 6

`Day 6 was all about Passive Recon.`

`Learned many thing as I’m weak at my Recon Skills.`

`Learned about Google Dorking.`

`Learned about Github Dorking.`

`Learned about Using Httprobe.`

`Learned about using Subfinder and Sublist3r.`

`Learned about Using EyeWitness for ScreenShot.`

`Learned about using Subjack.`

`Made a Report on all the Process just main points and details.`

I started with DNS recon and used dnsrecon -d target.com.

Then I moved to OSINT part and used Harvester to harvest online available details regarding our target.

Then I used WhatWeb to discover the Web Technologies.

After that I moved to Subdomains part and Used Sublist3r and SubFinder to Find Subdomain of our target.

Saved the result of both scan to a File and then Probbed them seprately for alive domains.

Then I tested the Probbed Result for Duplication and found that both tools gave totally different results.

After that I merged both results and put them into single file and Put the burden on Eyewitness to check for working domains.

And then final thing I tested all subdomains for the SubDomain TakeOver.

🪔 RECON https://www.maynoothuniversity.ie/

📻 Google Dorks