With this guide, you should improve your recon skills and explore some tools.

1 - Picking a target

Please go to http://100.101.228.35:7000/ and get your random target domain for this assignment (💡 hint: turn on Tailscale VPN if you can't connect)

2 - Required tools

- `nmap`
- `subfinder` (https://github.com/projectdiscovery/subfinder)
- `assetfinder` (https://github.com/tomnomnom/assetfinder)
- `httprobe` (https://github.com/tomnomnom/httprobe)
- Content discovery tools: dirsearch, ffuf, gobuster or kiterunner.
- `dnsx`
- `httpx`
- `nuclei`

3 - Tasks

Submit your solution for the following tasks in **Moodle**. The solution should be a ZIP file with a brief report describing your findings and the files created during the execution of these tasks. The report must be in one of the following formats: txt, markdown, or PDF and should be submitted **until the next class date** - 23:59. If all tasks are completed successfully, you'll get the points for the `Lab 02` challenge on https://tpas-desafios.alunos.dcc.fc.up.pt (**250 points**). This is a solo lab exercise, so **each student must** have a submission.

EN

After retrieving the target at http://100.101.228.35:7000:

1. Conduct passive subdomain enumeration with `subfinder`, `assetfinder` or both. Save the output in a file `subs.txt`. If more than one tool is used, merge them in to one file to obtain a unique list of subdomains. 💡 Hint: use the `sort` command with the appropriate flag.

2. Conduct active subdomain enumeration using `dnsx` or `massdns` with a wordlist of your choice. If you find new subdomains, that weren't found with the step before, **make note of those**. 💡 Hint: https://github.com/danielmiessler/SecLists or https://wordlists.assetnote.io are good places to look for a wordlist.

3. Find active `http` and `https` services, with the `httpx` or `httprobe` tool, by providing as input the subdomains gathered from steps 1 and 2. Save the result in a file, `urls.txt`. **Important:** Remove out of scope domains from `subs.txt`.

4. URL scanning: Choose one url that you think might be interesting to look at from `urls.txt` (pick a subdomain and not the apex/root domain, e.g. something.acme.com instead of acme.com);
   4.1. Identify the technologies (top 5) used in that subdomain. Can be useful for technology identification: Wappalyzer, nuclei technology templates - to be used with nuclei. 💡Hint: use the -tags flag
   4.2. Run one or more content discovery tools against at the web service (e.g. `ffuf` or `dirsearch`) to discover exposed files or available endpoints. Adjust the file extensions according to the technologies used by the asset. 💡Hint: typically you should only get a hit or 200 in a dozen files/endpoints, more than that probably indicates false positives.

5. Special tasks (optional):

   - 6.1 (50 points) - Use Google dorks to try and find sensitive files/endpoints of the target. Useful link: https://www.exploit-db.com/google-hacking-database
   - 6.2 (50 points) - Research potential sensitive, interesting or vulnerable endpoints identified on task (if the URL(s) you used above didn't yield anything, try another subdomain or domain altogether)