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

- `dig`
- `traceroute`
- `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.
- Optional: 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 27/09 - 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
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. Email reconnaissance

    - 1.1 - What are the email providers used by the target organization?
    - 1.2 - Are those correctly configured? (e.g., SPF headers, DKIM?). Useful commands and tools: `dig MX`, `dig TXT`, https://toolbox.googleapps.com/apps/checkmx/

2. 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.

3. Execute `traceroute` for a subdomain of your choice. Track the location of **all** IP addresses on the obtained route. Can be helpful: https://www.ip-tracker.org, https://github.com/mitsuhiko/python-geoip

4. Find active `http` and `https` services, with the `httprobe` tool, by providing the file `subs.txt` as input. Save the result in a file `urls.txt`. **Important:** Remove out of scope domains from `subs.txt`.

5. URL scanning: run one or more content discovery tools against at least one web service of the attack surface. Adjust the file extensions according to the technologies used by the asset (specify the top 5 technologies being run). Can be useful for technology identification: Wappalyzer, nuclei technology templates - to be used with nuclei. Note: typically you should only get a hit or 200 in a dozen files/endpoints, more than that probably indicates false positives.

6. Special tasks (optional):

    - 6.1 (50 points) - Use google dorks to 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 5.

PT

Depois de ser alocado um domínio de http://100.101.228.35:7000:

1. Levantamento de email

    - 1.1 - Quais os serviços de email utilizados pela organização alvo?
    - 1.2 - Estão correctamente configurados (e.g. SPF, DKIM)? Comandos e ferramentas úteis: `dig MX`, `dig TXT`, https://toolbox.googleapps.com/apps/checkmx/

2. Realizar a enumeração de subdomínios passiva com o `subfinder` e/ou `assetfinder`. Guardar o output num ficheiro `subs.txt`. Se ambas as ferramentas foram utilizadas, fundir o resultado dos dois num único ficheiro para obter uma lista de subdomínios sem duplicados. Dica: usar o command `sort` com a flag apropriada.

3. Executar `traceroute` para um subdomínio à escolha e obter a localização geográfica de **todos** os endereços IP da rota obtida. Pode ser útil: https://www.ip-tracker.org, https://github.com/mitsuhiko/python-geoip

4. Verificar quais os subdomínios que têm serviços `http` ou `https` activos com a ferramenta `httprobe`, passando o ficheiro `subs.txt`. Armazenar o resultado num ficheiro `urls.txt`. **Importante:** Remover subdomínios out of scope do ficheiro `subs.txt`.

5. Levantamento de URLs: correr uma ou várias ferramentas de content discovery, contra pelo menos um serviço web da superfície de ataque já identificada. Ajustar as extensões de acordo com as tecnologias utilizadas por cada asset (especificar o top 5 tecnologias corridas nesses serviços). Podem ser úteis para perceber quais as tecnologias: Wappalyzer, Templates de tecnologias do Nuclei - devem ser utilizados com o Nuclei. Nota: tipicamente só devem conseguir descobrir uma dúzia de ficheiros/endpoints, mais que isso provavelmente indica falsos positivos. Verificar.

6. Tarefas extra (opcional):

    - 6.1 (50 pontos) - Usar google dorks para tentar encontrar ficheiros sensíveis pertencentes ao target. Link útil: https://www.exploit-db.com/google-hacking-database
    - 6.2 (50 pontos) - Investigar possíveis endpoints sensíveis, interessantes ou vulneráveis identificados pelas ferramentas de content discovery na tarefa 5.