In this assignment, you should improve your network scanning skills and explore `nmap` and other tools.

1 - Tools

Please install:

📝 note: check the official install instructions for each tool, as the commands above may not apply to your system

- `nmap` > `sudo apt-get install nmap`
- `wireshark` > `sudo apt-get install wireshark`
- `scapy` > `sudo apt-get install python3-pip; pip3 install scapy`

2 - Tasks

Submit your solution in the appropriate form. Your submission must consist in a brief report about the tasks you did and the output of the tools you ran. The report must be in TXT, Markdown or PDF. If all tasks are completed successfully, you'll get points for the `Lab 03` challenge on https://tpas-desafios.alunos.dcc.fc.up.pt.

1. Banner grabbing: use `nc`, `telnet`, `curl -v` (for HTTP/HTTPS), or a similar tool. Pick one asset identified on Lab 02 - `subs.txt` - and disclose a technology (product) and version (if possible) of any one service (e.g. SSH, HTTP/HTTPS, etc).

2. Explore `nmap`, making use of the manual (`man nmap`) or the `-h` flag. Use `100.101.228.35` **OR** any asset from the scope identified on Lab 02 (In this case you shouldn't choose an asset hosted on a CDN).

   📝 note: if 100.101.228.35 check Tailscale dashboard for an IP

   - 2.1 - How to perform a ping scan?
   - 2.2 - How to perform an aggressive scan? What information can we get?
   - 2.3 - How to perform a scan for a given port range? E.g. scanning all TCP ports between port `1` and `1000`.
   - 2.4 - How to perform a list scan? For this task, it's recommended to scan your home network.

3. Open Wireshark and start capturing network packets from the previous task. What was the scan option that leads to less network traffic (i.e. from ping scan, aggressive, port range or list scan)? Useful Wireshark display filter `ip.addr == X.X.X.X`, with `X.X.X.X` as your local IP address or target IP address.

4. Solve the `secret-service` challenge on https://tpas-desafios.alunos.dcc.fc.up.pt (Regular flag submission - no need to send the solution for this one).

5. Special tasks (extra):

    - 5.1 (50 points) - Perform banner grabbing and nmap scanning on other hosts from *Lab 02* - `subs.txt`, save identified products and versions, and search for CVEs on https://nvd.nist.gov/products/cpe/search > `View CVEs`. CPE format example: `cpe:2.3:a:openbsd:openssh:8.4:p1:*:*:*:*:*:*`. Are any exploitable? Can be useful for `nmap`: `-oX` includes CPEs on the output XML.

    - 5.2 (50 points) - With `scapy`, code a script that parses an exported capture file from Wireshark `.pcapng` and extracts all IP addresses.

    - 5.3 (50 points) - With `scapy`, code a script that performs a **SYN port scan** against a given IP address or hostname.