Instructions

With this guide, you should learn how to access the CTF challenges, hosted in the TPAS server (https://tpas-desafios.alunos.dcc.fc.up.pt). We will also configure and install the required tools for the classes.

1. Network configuration

Any challenge that requires a network port is only available via VPN.

The VPN is powered by Tailscale, and you must install it on the machine you'll be using during classes. Limited to one machine per student.

1. Follow the link: https://login.tailscale.com/start and signup with one of the available providers (Google, Github, Microsoft, etc) - register with any email **EXCEPT** anything ending in up.pt (e.g. up.pt, fc.up.pt); in short, use your personal email address just for this one step
2. Follow the onboarding instructions and install the Tailscale client on your machine
3. Click “Skip this introduction”
4. Follow the link to get access to the TPAS server: https://login.tailscale.com/admin/invite/TF64H34N1fV96sZnrUbD51
5. Open the Tailscale app in your machine and turn it on (it should say **connected**)
6. Try to ping the TPAS server by running the commands: `ping 100.101.228.35` / `ping tpas-be`

Notes for the lab machines

If you're using the lab computers, it's possible that the challenge server does not resolve correctly. If necessary, please configure an alternative DNS server on your network settings, such as 8.8.8.8 (edit /etc/resolv.conf in Mac/Linux). Please remember to click Apply or restart the network adapter after changing your network settings. You should now have access to https://tpas-desafios.alunos.dcc.fc.up.pt

2. Account creation

Create an account on https://tpas-desafios.alunos.dcc.fc.up.pt with your preferred 1337 hacker username, but please remember to sign up with your student email.

3. Installing software that we’ll need

- nmap
- wireshark
- exiftool
- Metasploit framework (https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers)
- aircrack-ng (https://www.aircrack-ng.org/doku.php?id=install_aircrack#installing_pre-compiled_binaries)
- john-the-ripper
- exiftool
- gdb-gef (https://github.com/hugsy/gef)
- pwntools (https://github.com/Gallopsled/pwntools)
- Ghidra (https://ghidra-sre.org/)
- relative-url-extractor (https://github.com/jobertabma/relative-url-extractor)
- waybackurls (https://github.com/tomnomnom/waybackurls)
- Dirsearch (https://github.com/maurosoria/dirsearch)
- Ffuf (https://github.com/ffuf/ffuf)
- Sublist3r (https://github.com/aboul3la/Sublist3r)
- subfinder (https://github.com/subnder/subnder)
- Aquatone (https://github.com/michenriksen/aquatone)
- Nuclei (https://github.com/projectdiscovery/nuclei)
- Caido (https://caido.io) - Basic or Student plan https://caido.io/student-plan
- Gowitness (https://github.com/sensepost/gowitness)

4. Exploring tools and solving challenges

After installing tools, you can start exploring features or go ahead and try solving a few basic challenges on the tpas-desafios platform.

⚠ **Important:** Don't target any public IP address, but feel free to scan the host `100.101.228.35` / `tpas-be` (e.g. with nmap). **Scanning unauthorized hosts is strictly prohibited.**