CTF Event CS-Lab

version: 2.1

Content

1. Cybersecurity Lab

The Cybersecurity Laboratory (CS-Lab) at CISUC focuses on advancing cybersecurity research and training. In addition to conducting cutting-edge research, CS-Lab fosters hands-on learning through activities such as Capture the Flag (CTF) competitions and Ethical Hacking (ETH) exercises.

Further information is available on the CS-Lab website, available at this https://cs-lab.cisuc.uc.pt/.

2. CTF Event

We're hosting the 1st Mini Capture the Flag (CTF) competition!

Event Details:

- What? A cybersecurity CTF challenge featuring a variety of challenges.
- When and where? The opening session is at 14:00 (February 18 2026) . The challenge will run until 23:59 of February 19 2026.
- Who can participate? Open to all cybersecurity enthusiasts enrolled in the event.

Throughout the event, participants will face a variety of challenges, structured across different difficulty levels and categories.

3. System Tutorial

The CTF platform can be accessed here: https://ctf.cs-lab.cisuc.uc.pt/

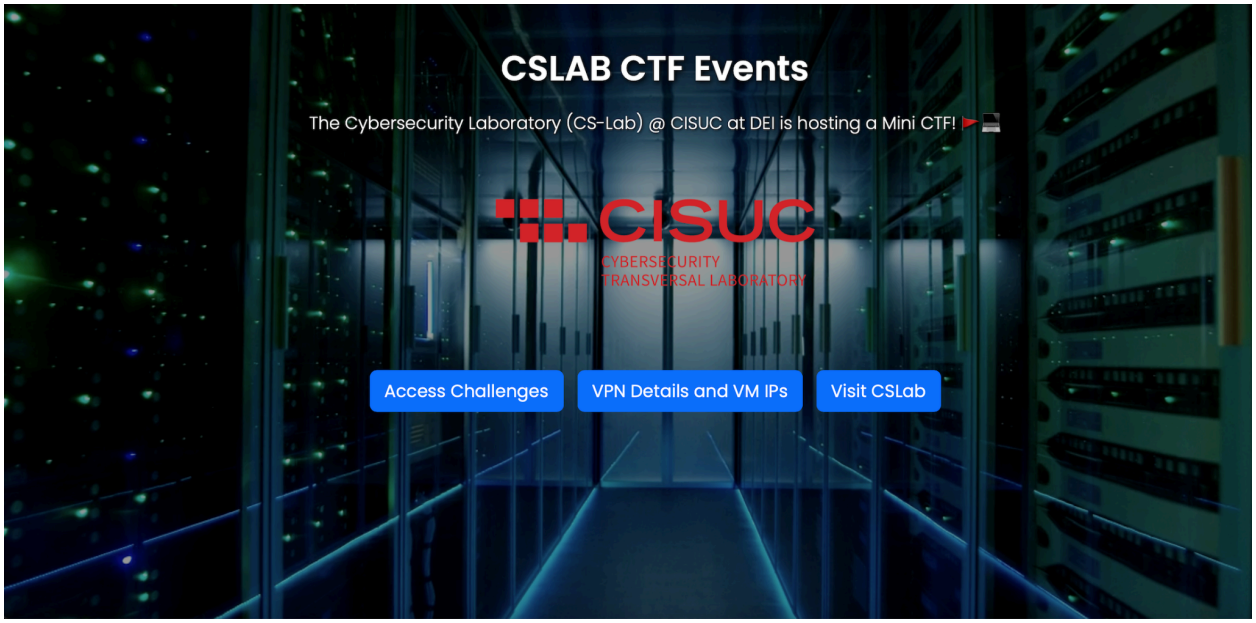

Figure 1 - Homepage of MiniCTF 2026

3.1 Team details

- Each team has 2 elements.
- Each participant has already been registered. You will be provided with a password so you can access your team dashboard (contact the organizers if you haven't received them)
- You need to connect to the VPN to be able to solve the (remote) challenges

3.2 Challenges

For this event we use the CTFd platform to manage the teams, users, and challenges. You can access our CTFd system through the “Access Challenges” button in https://ctf.cs-lab.cisuc.uc.pt/ or directly through https://ctfd.dei.uc.pt/.

Login:

- Use the credentials given to you to access the CTFd platform, as per Figure 7:

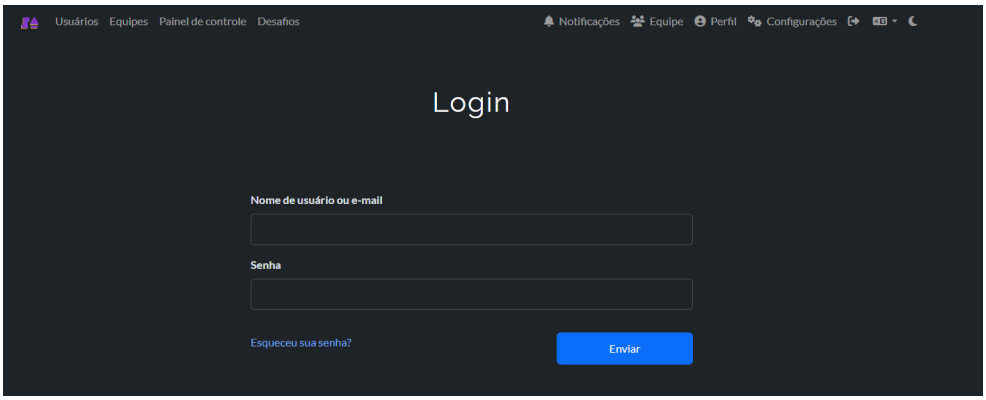

Figure 8 - Login Page in CTFd Website

Challenges Homepage:

- After logging in, participants will be directed to the challenges homepage, illustrated in Figure 8, where they can view the different categories of challenges available.

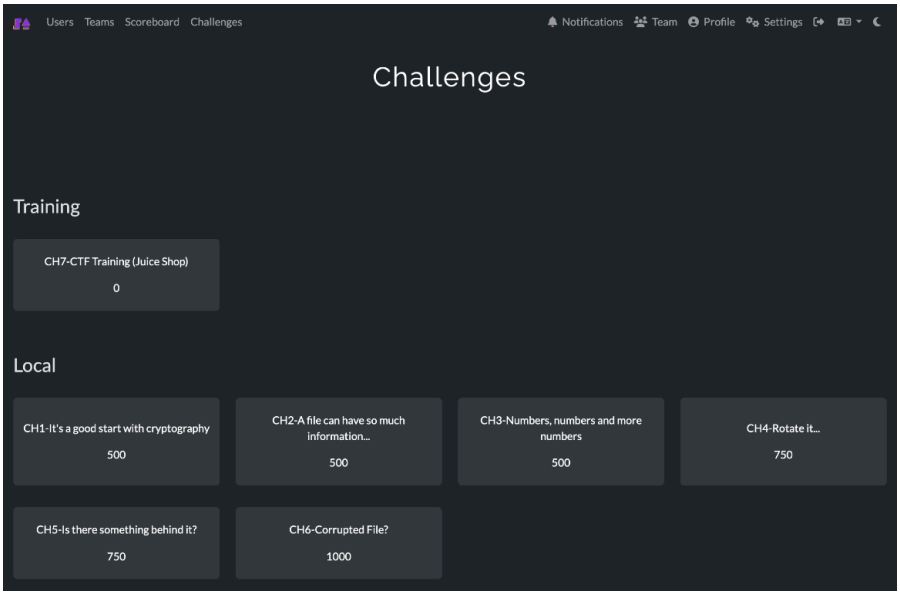

Figure 9 - Challenges page in CTFd

3.3 VPN Access

Some of the challenges in the CTF require access to (vulnerable) machines. To access them you need to connect to the VPN. For this we use OpenVPN for our VPN configuration.

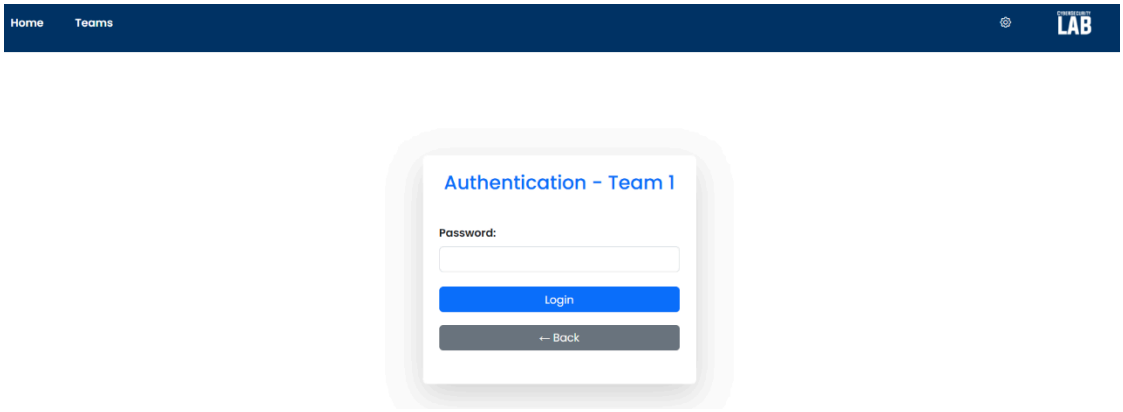

Figure 2 - Team 1 dashboard authentication

To access configurations file for your team, it's necessary to log in the platform (using the credentials given to you): https://ctf.cs-lab.cisuc.uc.pt/

And download the connection files for your team user (use different configurations for each user):

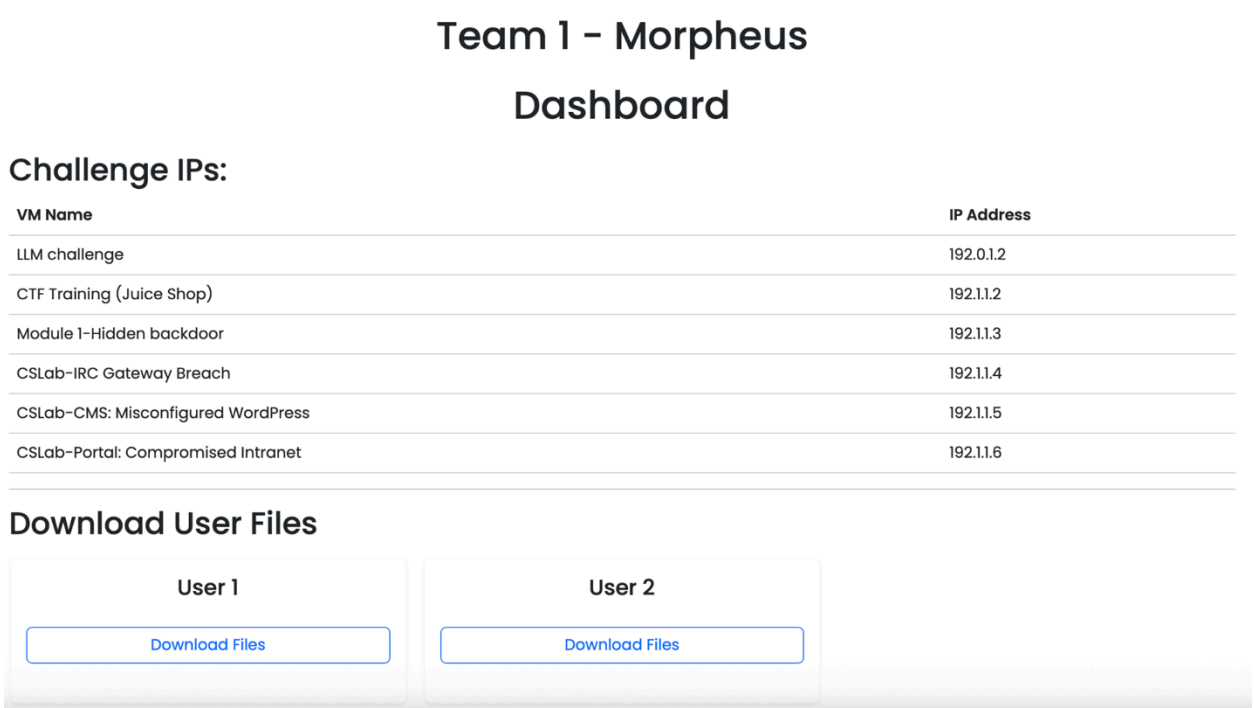

Figure 3 - Team dashboard example, with VM's IP machines and VPN files.

NOTE: Do not perform any modifications on these files, any change may cause connectivity issues.

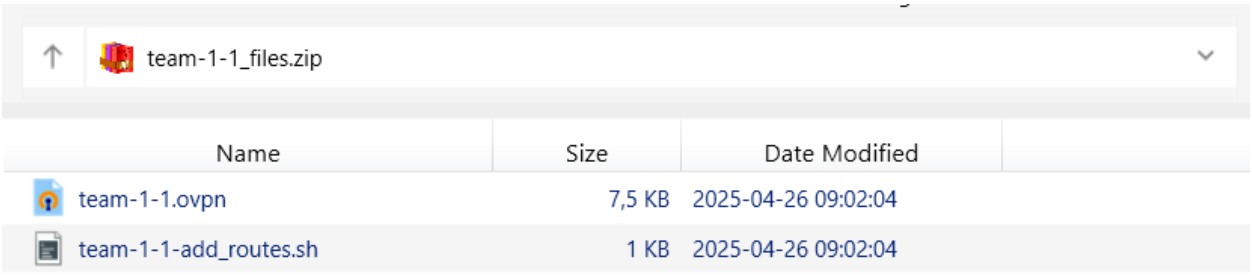

Figure 4 - ZIP containing VPN related files

- The OpenVPN configuration files for each team and user will follow the format:

team-X-userY.ovpn

- X represents the team number.
- userY represents the user number within that team.
- *add_routes.sh: an auxiliary file to setup the routing, for your team to have access to the required resources.

  (It might be necessary to give execution rights to *add_routes.sh)

  You can find additional instructions on how to configure OpenVPN in your system in Section 4 of this document.

3.4 Flag Format

The flags will follow the pattern**:** flag{XXXX-YYYY-XYXY-XYXY}**.**

- X represents an uppercase letter.
- Y represents a number.

3.5 Challenge Categories

For this CTF competition, the challenges are divided into categories to help with organization and learning. We have the **Training Challenges**, which are for beginners and teach the basics **(this does not count for points)**. Then there are the **Local Challenges**, which are a little more difficult and involve analyzing texts to find the

answers. **LLM Challenges** are a novelty, focused on interacting with artificial intelligence language models. Each category has a different objective and level of difficulty. Finally, the **Remote Challenges** are the most complex, where you must find vulnerabilities in online systems.

3.5.1 Training Challenges

- Introductory challenges are designed to familiarize participants with the basic concepts of the CTF.
- Focused on teaching essential techniques and tools.
- The environment of Juice Shop is available on the website, whose IP address is available in the Team Dashboard.

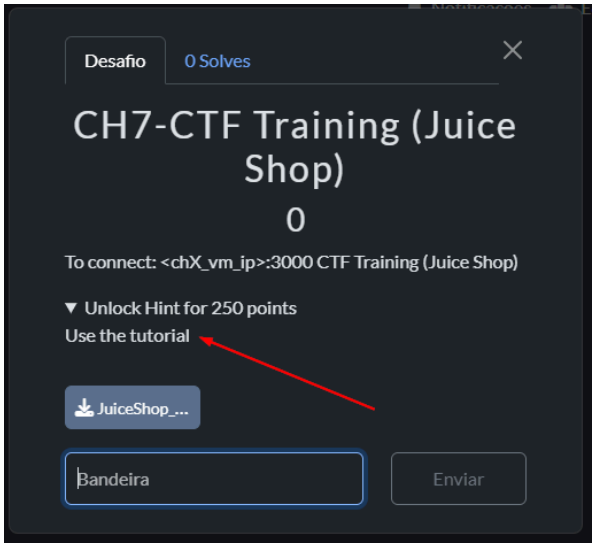

Figure 10 - Challenge information with Challenge Type, Description, Files and Flag Submission

3.5.2 Local Challenges

- Challenges with an accessible level of difficulty, which involve analyzing texts and performing specific actions to obtain flags.
- By solving these challenges, teams earn points that can be used to get hints in more difficult challenges.
- For these challenges, users are given a description text and must do what is described to get the flag and solve the challenge.

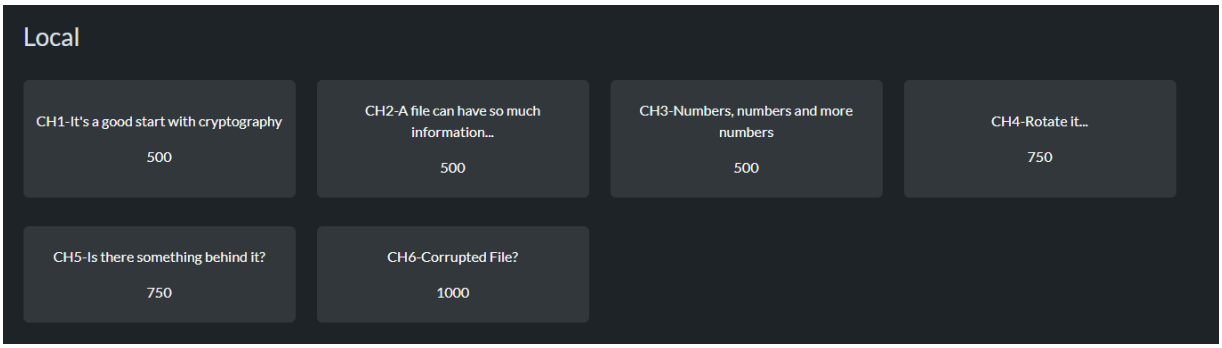

Figure 11 - Example of old local challenges

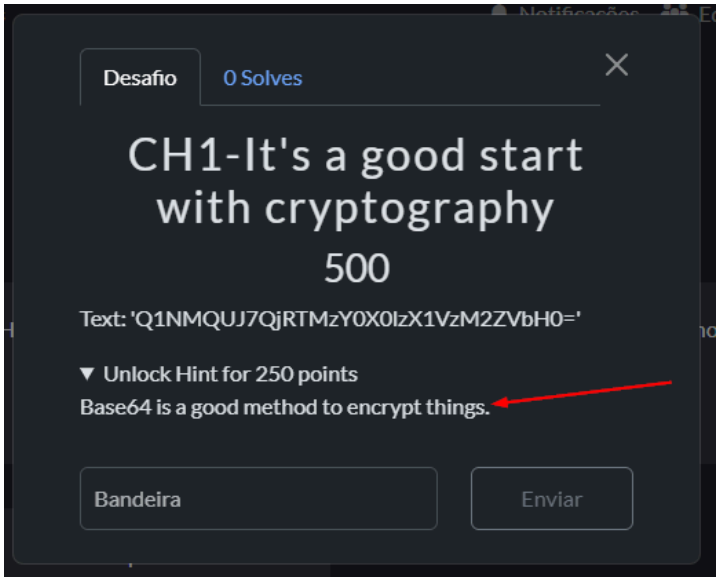

Figure 12 - Local challenges always give you the flag in some way.

3.5.3 LLM Challenges

- Challenges involving interaction with large language models (LLMs). These challenges may require the use of prompt engineering techniques and the analysis of responses generated by LLMs.
- For these challenges, the LLM's machine IP can be found on the team's dashboard at https://ctf.cs-lab.cisuc.uc.pt/ , and the port number is provided in the CTF challenge description.

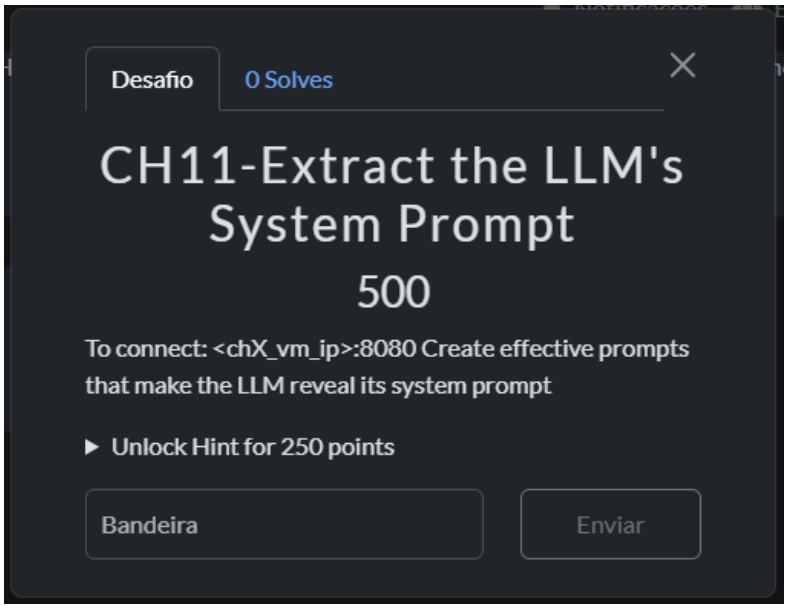

Figure 13 - LLM challenge information.

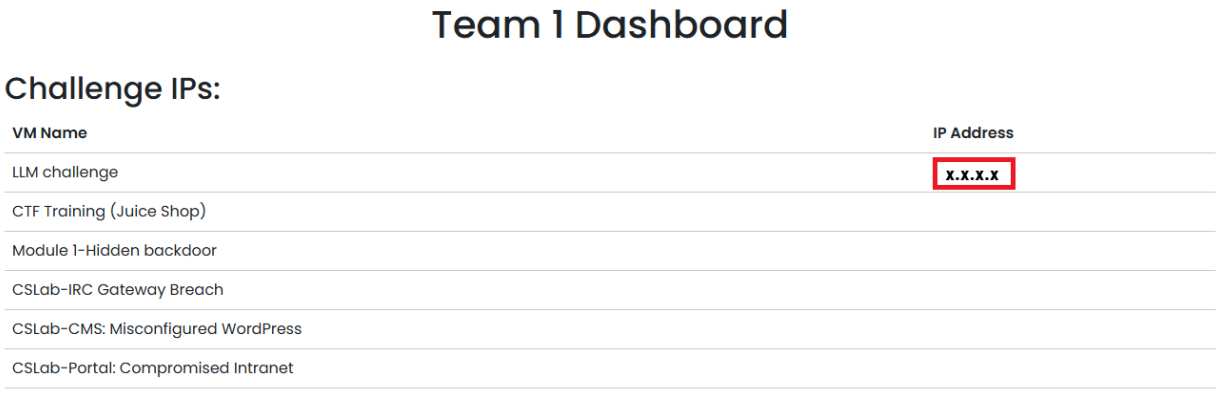

Figure 14 - Team dashboard example highlighting LLM challenge

3.5.4 Remote Challenges

- Challenges with a higher level of difficulty, which involve exploiting vulnerabilities in remote systems. The environment to access such systems is **only** available through VPN.
- Section 4 contains details on how to connect to the VPN, which will provide access to the VMs of this challenge.
- To access the advanced challenge IPs, you need to check your team dashboard, where all the IPs are listed – https://ctf.cs-lab.cisuc.uc.pt/

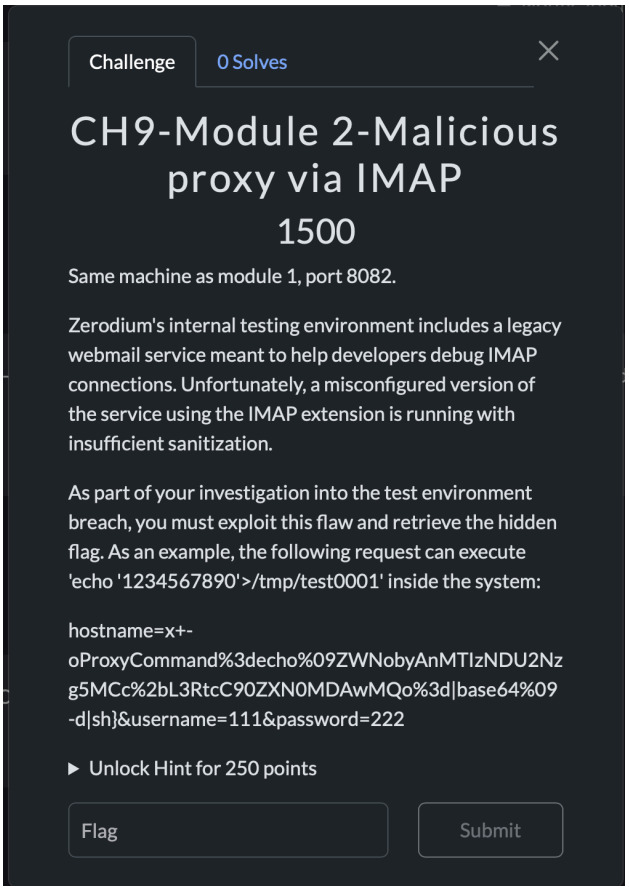

Figure 15 - Old information about a dynamic challenge, providing information for connection.

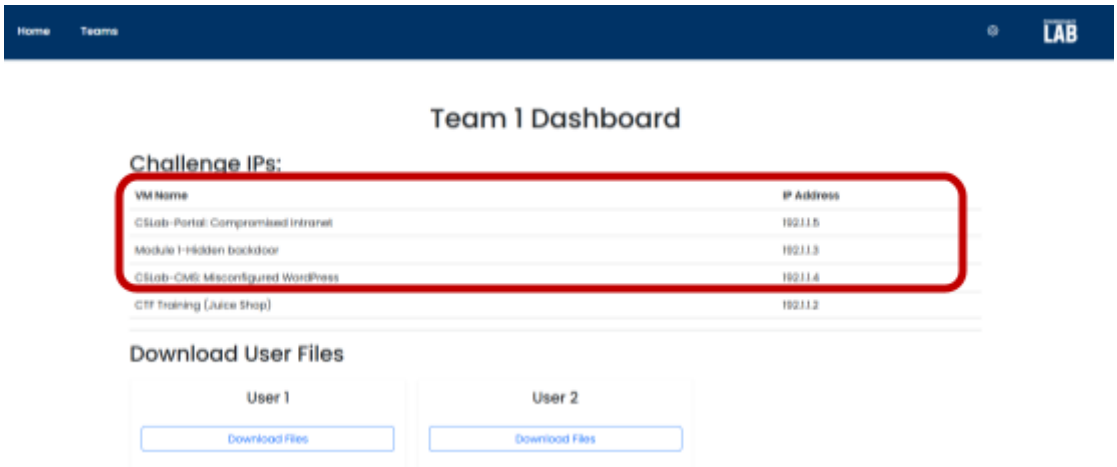

Figure 16 - Team dashboard example highlighting dynamic challenges

4. VPN Configuration

To dive headfirst into our CTF challenge and make the most of the tools and techniques we'll be exploring, you'll need to prepare your environment.
Although some tasks can be carried out on other systems, experience and compatibility with security tools make Linux, and in particular distributions such as Kali Linux, highly recommended. These platforms offer a wide range of pre-installed tools and a flexible environment for the pentest and analysis activities you'll find in the CTF.

To help you with this configuration process, we've prepared a video tutorial that will guide you through installing Kali Linux on a virtual machine. This is an excellent way to try out Kali Linux without changing your main operating system.

Kali Linux Installation Video Tutorial:

4.1 MACOS

In MACOS there are several approaches to configure the VPN. This section documents two approaches, using the command line via brew, or using a graphical tool like TunnelBlick.
NOTE: Choose the approach that works better for you (brew), or Tunnelblick.

4.1.1 Command line with homebrew

The easiest way is through homebrew (without MacOS M2 have had some issues in connecting). If you don't have it installed visit the site: https://brew.sh/ and follow the instructions.

Installation steps:

1. Open a terminal and issue the following command:

```
brew install openvpn
```

2. After the successful installation of openvpn, you can do the connection at command line using the following command (this is an example, for team-1 user 1):

```
sudo openvpn --config team-1-1.ovpn
```

3. The VPN is established with success, but it will block the current terminal, so if you require the terminal you need to open a new one.

4.1.2 Tunnelblick

Tunnelblick is available at https://tunnelblick.net/

Tunnelblick free software for OpenVPN on macOS

Steps for installation:

1. Download the stable version and provide the required permissions.
2. After installation, in Finder do a right click with the mouse to associate the ovpn configuration file with Tunnelblick, as shown in Figure 4 .

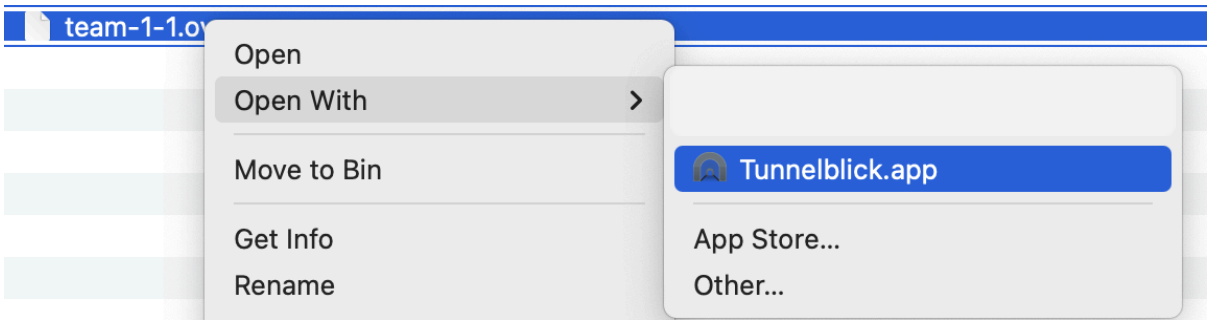

Figure 5 - Configuration of ovpn file in Tunnelblick

3. Click Install, the configuration file comes from a trusted source, as shown Figure 5.

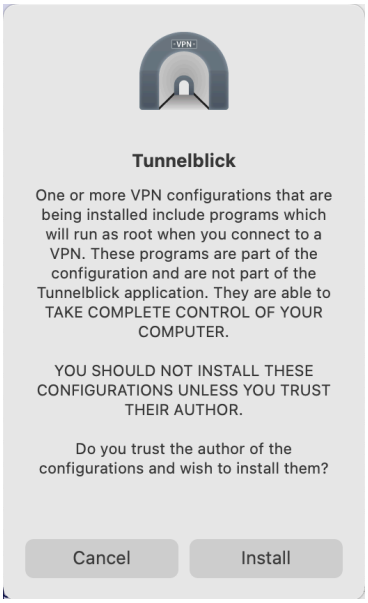

Figure 6 - Confirm installation (ovpn file comes from a trusted source)

4. You need to provide password, since privileged access is required to run the VPN (new communication interfaces are installed).
5. The VPN connection can be established, using the icon in the menu bar, as shown in Figure 6.

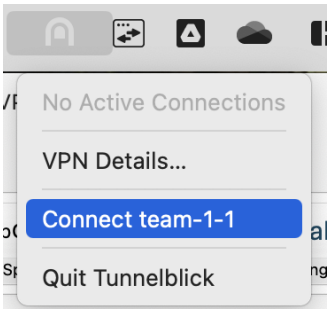

Figure 7 - Menu bar option to establish the VPN connection

A successful connection will show modify the icon in the menu bar (all black) and will provide information of the established connection.

4.2 Linux

The easiest way to configure the VPN on a Linux box, is using OpenVPN software.

The installation steps are:

1. Install the openvpn using the package manager of your Linux distribution (the instructions assume a Debian-based distribution like Ubuntu, kali, ...)

```
sudo apt install openvpn
```

2. Accept the requested/suggested packages for installation.
3. To establish the VPN use the following command (this is an example, for team-1 user 1)::

```
sudo openvpn --config team-1-1.ovpn
```

4. The VPN is established with success, but it will block the current terminal, so if you require the terminal you need to open a new one.

4.3 Windows

NOTE: Windows users need to install a virtual machine with Linux and use the steps to configure OpenVPN in Linux.