

B4 - Web Security

B-SEC-400

Hydra

Boot2Root networking challenges





INTRODUCTION

This project is designed to teach you network exploits in the form of **Boot2Root** challenges. As the name suggests, **Boot2Root** just means “boot it to root it”, which is a kind of challenge involving launching VMs to connect to a specific service, find weaknesses to access the system, then escalate your privileges to become root.

As a variant of the **Capture-The-Flag**, you will find in the VM token in the form of `EPI{Th1s_iS_4_T0k3N}`. You must find those to validate the challenges.

The **Hydra project** is composed of 15 different challenges that get gradually harder. You can use any tools / techniques you want to solve the challenges, although none of them require Metasploit.

Since you're on the second year course, the challenges are designed to be of medium difficulty, not too easy, but not too hard either. All of them are loosely based on privilege escalation, custom vulnerabilities exposures, reversing and bruteforcing with tools such as Gobuster, John the Ripper or Hydra.

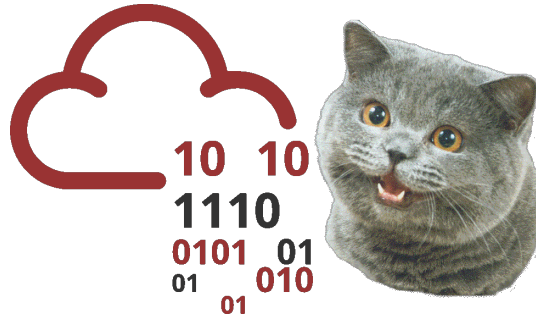


Some keywords are: Bruteforce, Reversing, Hashes, CVE, etc.
Google Them, or better yet, use TryHackMe to learn how to do it !



The challenge are sorted by difficulty, be sure to do the easier ones first before moving onto the harder ones

I CAN HAZ CHALLENGES ?



The challenges are on a specific platform for our partner : TryHackMe !

It is a website specifically designed to learn and practice hacking in all kind of shapes and forms, and is the perfect place to improve your skills.

You can join our custom learning path on the [Hydra interface](#)

If you don't have a TryHackMe account, you will need to register on the platform **using your epitech email**. If you already have an account and you want to keep it, just make sure that you your email address on TryHackMe is your epitech email.

Once done, just click the link above and get hacking!



Each time you start a machine, it takes around 1-3 minutes to boot, be patient!



It is still mandatory to register your group on the intranet.
The challenges need to be completed by at least one member of the team

SOME RULES

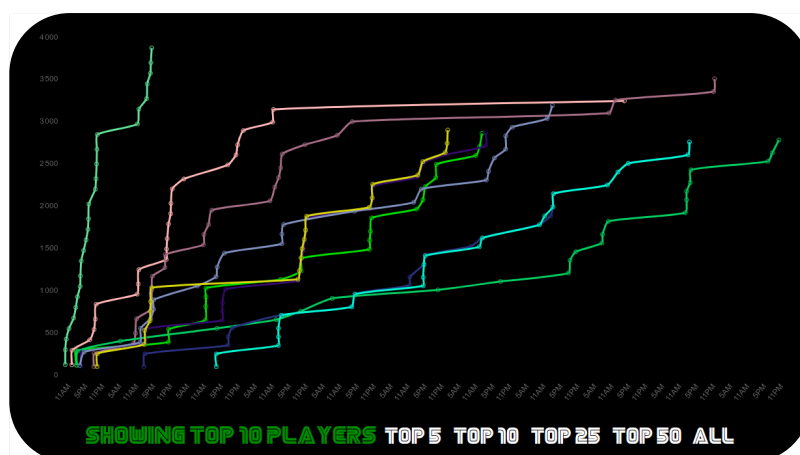


- You **MUST** register on <https://intra.epitech.eu> your group **BEFORE** the deadline.
- You **MUST NOT** submit write-ups, solutions, or flags anywhere online
- You **MUST** be able to explain every challenge that you succeed
- You **MUST NOT** share flags between teams, it will be considered cheating and will result in -42
- You **MUST** abide by the site rules (no attacking the main platform, no ddos, etc.)



Failure to follow those rules may result in -42, be careful !
Be sure to read it ALL !

NOW THE FUN PART



During this project, you will be graded according to the number of challenges you finish, and number of flags you find.

To add more spice to it, you will have a dashboard on [This website](#)

You will find a graph showing your score earned by collecting flags, finishing rooms and being the fastest



possible for each flag. You will have both a local ranking and (inter)national ranking.

Points are calculated this way:

- 100 points per flag
- 50 points per room fully completed
- up to 10 bonus points per flag depending on your speed

Prizes will be delivered to the best hackers of each city, the best hackers of all students, and their name will forever be in [the Hall of fame!](#)

Do your best to shine in this competition!

FINAL DEFENSE



The **Final Defense** will be a mandatory review that occurs right after the end of the Hydra project. The format will be that of a proper Review/Keynote, where you will have to explain the ins and outs of your project.

The pedagogical team will ask **each member** of the group to explain **one challenge each** that you manage to solve. You will have to go into detail on how you did it, which technique / tool you used, etc.
The choice of the challenge you'll be questioned on will be at your reviewer's discretion.

Some theoretical questions will be asked to be sure that you fully understand the core concepts of Reversing, CVE and bruteforcing.



Be careful, this defense is **MANDATORY** and will be crucial for the validation of your module!