B5 - Advanced Security

B-SEC-500

Chisel

Boot2Root networking challenges

Chisel

- The totality of your source files, except all useless files (binary, temp files, obj files,...), must be included in your delivery.

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 king 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.

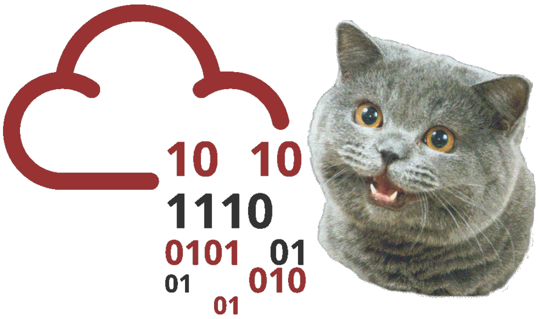
The Chisel project is composed of 10 different challenges that get gradually harder.
You can use any tools / techniques you want to solve the challenges, although none of them require Metasploit.

Since you're on the Advanced course, the challenges are designed to be tougher than you're used to. All of them are loosely based on privilege escalation and finding hidden internal port, that you can tunnel on your machine using tool such as Socat, SSHuttle or `Chisel`.

Some keywords are: Networks, Pivot, Tunneling, Reverse Proxy, Port Forwarding, 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 plateform 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 Chisel 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!

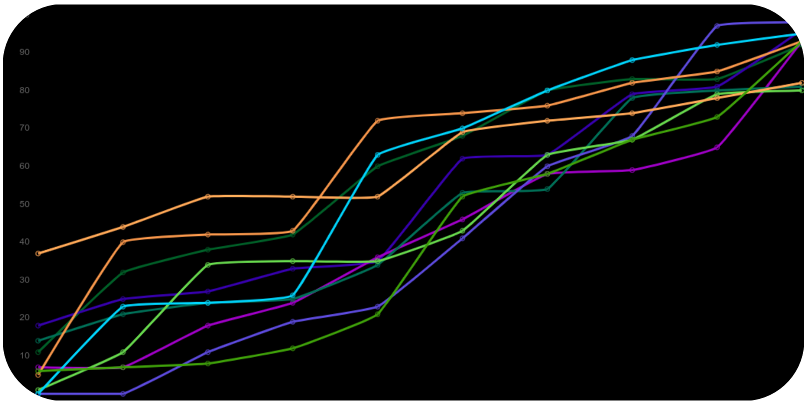
It is still mandatory to register your group on the intranet.
The challenges need to be completed by at least one member of the team

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 maye 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 by flags, rooms and speed of completion campus-wise and national-wise.

Prizes will be delivered to the best hackers of each city, the best hackers of all the Epitech nationally, 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 Chisel 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 questionned 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 SSH tunneling and port forwarding.

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