TP évalué, Sécurité des Systèmes

Hugo Blanc - Université Lyon 1
LP ESSIR 2024-2025

April 10, 2025

Le TP est à rendre obligatoirement avant le **dimanche 4 mai 2025 à 23h59** (Europe/Paris).
Attention au respect des consignes de rendu (voir Chapitre 2).

Table des matières

1. Énoncé 4
   1.1. Lancer les challenges 4
   1.2. État des challenges 4
2. Rendu 5
   2.1. Format du rendu 5
   2.2. Méthode de rendu 5
3. Critères de notation 6
4. Licence 7

1. Énoncé

Le but de ce TP noté est de résoudre 5 challenges de sécurité. Chaque challenge demandera des compétences différentes (sécurité web, cryptographie, …). Pour résoudre un challenge, il faut trouver un **FLAG**, qui commence par `FLAG:` ou `CTF{`.

1.1. Lancer les challenges

Afin de faciliter leur utilisation, les challenges sont hostés sur un serveur dédié, dont le domaine est `pwnthe.net`.

Les challenges seront disponibles aux adresses:

- challenge1.pwnthe.net
- challenge2.pwnthe.net
- challente3.pwnthe.net:3333
- challenge4.pwnthe.net
- challenge5.pwnthe.net
- etc.

Pour s'authentifier, utilisez les credz suivants:

- `essir` / `zkHdNVbLp3qv`

Le challenge 3 ne nécessite pas d'authentification.

1.2. État des challenges

Si jamais vous pensez qu'il y a un souci avec un des challenges (le serveur ne répond pas, vous avez des erreurs étranges…), vous pouvez vous rendre sur https://status.pwnthe.net/status/essir° pour en être sûr.e. Si les serveurs sont verts ici, cela signifie qu'ils sont fonctionnels.

Si jamais ils sont rouges, contactez moi par mail.

2. Rendu

2.1. Format du rendu

Un rapport de type *write-up* est attendu **format PDF**, contenant:

- le flag de chaque challenge;
- la réflexion, les outils et les méthodologies pour le trouver;
- toute autre information pouvant mener lieu à une évaluation.

2.2. Méthode de rendu

- Une archive **au format zip** est attendue, contenant votre rapport et tout autre fichier additionnel qui fera l'objet d'une notation (images, exploits, ...).
- Le nom de l'archive devra **impérativement** respecter la convention de nommage suivante: `NOM_PRENOM_SEC25.zip`.
- Cette archive devra m'être envoyée par mail. Le sujet du mail devra suivre la convention de nommage suivante: `[ESSIR] Rendu Sec 2025 NOM PRENOM`.
- La date de rendu maximale est précisée en début de document.

> ⚠ **Avertissement**
>
> - Veillez à respecter la casse des conventions de nommage.
> - Tout rendu ne respectant pas **tous** ces points **ne sera pas évalué**.
> - En cas de retard, un malus de −1 point par heure de retard sera appliqué à la note finale (heure de réception du mail faisant foi).

3. Critères de notation

Chaque challenge est noté sur 4 points. La notation se fera selon le barème suivant, pour chaque challenge:

- Flag correct: **1 pt**.
- Explication de la méthode de résolution: **3 pts**.

Les fautes d'orthographe et de grammaires ne seront pas prises en compte dans l'évaluation, **dans une moindre mesure**.

La mise en page du rapport devra être soignée, sous peine de pénalité également.

4. Licence

© Hugo Blanc, 2025

Ce document peut être distribué librement, selon les termes de la version 4.0 de la licence Creative Commons Attribution-ShareAlike: http://creativecommons.org/licenses/by-sa/4.0/°.

Vous êtes libres de :

- reproduire, distribuer et communiquer ce document au public;
- modifier ce document.

Selon les conditions suivantes :

- **Paternité**. Vous devez citer le nom de l'auteur original.
- **Partage des Conditions Initiales à l'Identique**. Si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.
- A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.
- Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.