

# Examen

## Éléments de cyber-sécurité

13 avril 2023

### I. (20 points) **Test d'intrusion sur un parc informatique**

L'examen consiste en un TP rassemblant des notions abordées lors des TP précédents mais également des techniques nouvelles qui n'ont pas été abordées en cours.

Le principe consiste à valider les connaissances et savoir-faire acquis tout au long du module, et aussi de vous placer dans des situations nouvelles qui requièrent de votre part imagination et ingéniosité.

La plateforme de l'examen est composée de 4 systèmes Linux dont il faut prendre le contrôle complet. Le principe se rapproche d'un *escape game*, à la différence qu'il s'agit ici de réaliser l'intrusion de chacun des systèmes, et non pas de s'évader.

À partir du tunnel VPN :

- Récupérer la configuration sur le site du cours <sup>1</sup>
- Lancer la commande suivante :
  - `sudo openvpn cours.ovpn`
- Les serveurs sont accessibles sur le sous-réseau 10.129.42.0/24
- Chaque compte compromis dispose d'un fichier nommé `trophee.trp` dont le contenu contient une chaîne de caractère du type 5593cff70d66403597a736208f8004a9. Il y a 10 trophés à récupérer sur la plateforme.

Vous pouvez travailler en groupe, mais le compte-rendu doit être personnel.

Le compte-rendu attendu devra expliquer les différentes vulnérabilités exploitées, ainsi que les valeurs des trophés, et les recommandations que vous formuleriez pour protéger de ces vulnérabilités.

Il est fortement conseillé de prendre des impressions d'écrans, ce qui permet d'expliquer plus facilement qu'un long paragraphe.

Vous pouvez me contacter en cas de blocage, ou si certains éléments de la plateforme sont non-fonctionnels à l'adresse suivante :

- philippe@pelicanux.net

Bon courage!

---

1. <https://cours.pelicanux.net/static/conf/cours.ovpn>