1- Contexte
Le dépôt https://github.com/vulhub/vulhub contient des environnements vulnérables organisés par dossier (outil, protocole, etc.). Chaque dossier regroupe une ou plusieurs vulnérabilités et fournit une démonstration de la manière d'exploiter chacune.

2- Objectif
Chaque étudiant·e choisit et corrige **deux vulnérabilités**. Vous êtes libres de choisir comment.

3- Contraintes
- Il est interdit de choisir deux vulnérabilités issues du même dossier.
- Une vulnérabilité ne peut être réservée qu'une seule fois par groupe (G1, G2, G11).
- Mettre à jour le logiciel ne compte pas comme une solution. Il faut supposer que c'est la version la plus récente.

4- Démarche
Pour réserver une vulnérabilité, envoyer un courriel à Samuel : s6desbie@uqac.ca (premier·e arrivé·e, premier·e servi·e).

5- Évaluation
Vous serez notés individuellement. Cependant, vous pouvez vous entraider.
Pour chaque vulnérabilité, le livrable est une vidéo unique**,** enregistrée en une seule prise, sans coupures ni montage, d'une durée **maximale de 10 minutes** contenant, dans l'ordre :

#	Critère	Points
1	Chargement de l'image Vulhub utilisée	10
2	Présentation de la vulnérabilité	10
3	Démonstration de l'exploit	10
4	Explication de la raison pour laquelle l'exploit fonctionne	20
5	Proposition justifiée d'un correctif	20
6	Application du correctif	20
7	Démonstration que l'exploit ne fonctionne plus	10

Chaque vidéo sera évaluée individuellement. Votre note sera la moyenne des deux notes.

<u>Exceptions pour exécutions longues</u>
Si l'application d'un correctif inclut une étape d'exécution qui prend beaucoup de temps, marquez, dans le courriel de remise du travail, le début et la fin de cette étape (p. ex. « minute 6

à minute 16 : exécution longue ») ; On va ignorer cette partie. Si plusieurs pauses existent, indiquez-les toutes dans le même courriel.

ATTENTION: Pour votre sécurité, lisez le pdf ‘Vérification_Vulhub.pdf’. Vous pouvez utiliser une VM pour avoir une double couche de protection.