# Sécurité informatique INF36207

## Travail Pratique #3 – Partie #2 sur Packet Tracer

### SESSION HIVER 2023

| | |
|---|---|
| Date limite de remise du TP | 11 avril 2023 à 19h00 |
| Équipe | Individuel ou en équipe de 2 ou 3 étudiants. |
| Pondération | 15% (partie 1 + 2) |

## Mise en contexte

Vous êtes le spécialiste en sécurité d'une organisation et votre équipe TI vous amène un comportement étrange qui s'est produit sur le poste d'un dirigeant. Les pare-feu ont levé des alarmes et des tentatives de connexion envers son poste.

Par la même occasion, nous avons reçu des plaintes d'un organisme externe qui pointait vers le poste du dirigeant. Ces derniers mentionnaient que quelqu'un aurait tenté de se connecter à plusieurs reprises sur le site forum.radioamateur.ca. Ils nous demandent d'investiguer.

À la lumière de ces informations, vous devez investiguer le fichier de capture du dirigeant en question que nous avons capté dans la dernière heure.

Pouvez-vous confirmer ces éléments :

1. Que s'est-il passé sur le poste du dirigeant à son insu ?
2. Qu'est-ce que le dirigeant a fait sur le site forum.radioamateur.ca ?
3. Pouvez-vous d'écrire la séquence des évènements qui se sont produits ?
4. Est-ce qu'il y a eu des attaques et dans la positive, d'où provenait les attaques
    - Adresses IP
    - Adresses MAC
    - Hostname
    - Etc.
5. Est-ce que de l'information a fuité à partir du poste du dirigeant ?

Quelles sont vos conclusions finales sur cet incident et quel serait le plan d'action à adopter ?

## Livrable pour l'évaluation du travail pratique

Pour que votre travail pratique puisse être évalué par l'enseignant, vous devez déposer un rapport écrit en format PDF à l'emplacement approprié sur le portail. Ce document doit comporter les réponses à l'ensemble des cinq (5) questions présentes. Vous devez également répondre à la question de conclusion.

Merci et bonne chance!