Cours 420-331-SF **Télécommunications et réseaux I** **Automne 2015** **Cégep Sainte-Foy** **Département d'informatique** **François Gagnon** **Catherine Boileau**	**TP 2** **25 %**

Contexte:

La NSA traque un dangereux criminel au Québec, M. Regit. Sachant que vous avez suivi le cours de réseau 420-331 au Cégep Ste-Foy, la NSA vous demande votre aide pour traquer ce M. Regit[1]. Votre contact à la NSA vous remet[2] 6 traces de trafic pour analyse[3]. Vous devez extraire le maximum d'information sur le criminel et transmettre un rapport en format PDF à votre contact (ça tombe bien, le « dead drop » se trouve justement dans LÉA).

Voici l'information que vous avez concernant les traces de trafic :

- Les traces TP2X_IP où X est une lettre (a, b, c ou d) ont été enregistrées directement dans le réseau personnel de Regit. Chaque trace a été capturée sur une machine différente; la trace est nommée avec l'IP de la machine sur laquelle elle a été capturée. Ces 4 captures de trafic ont été réalisées dans la même fenêtre de temps. Ces 4 traces doivent être traitées et analysées ensemble.
- La trace TP2_ Misc a aussi été enregistrée dans le réseau personnel de Regit, mais pas en même temps. Cette trace doit être traitée à part et toute l'information que vous réussissez à y extraire doit être consignée dans une section à cet effet de votre rapport.
- La trace TP2_ XiVO a été enregistrée grâce à l'infiltration d'un organisme dont Regit est client. Cette trace ne doit pas être traitée comme les autres, on cherche simplement à y extraire de l'information personnelle. Étant donné qu'elle a été capturée à l'extérieur du domicile de Regit, l'information sur le réseau et sur les activités réseaux ne sont donc pas pertinentes.
- Le réseau personnel de Regit est, somme toute, assez gros. Il a suffisamment d'argent pour se payer plusieurs ordinateurs.

À remettre:

- Un rapport en format PDF décrivant toute l'information que vous avez ramassez durant votre analyse.

---

[1] Ça se peut ça !!!

[2] Les traces de trafic seront disponibles pour téléchargement jusqu'au vendredi 20 novembre 23h59

[3] Comme la NSA prend la sécurité très au sérieux, l'archive zip qui vous ait remise est protégé par un mot de passe : le nom du criminel en minuscule dans l'ordre inverse ;)

- Pour chaque élément d'information que vous donnez, ajoutez une brève description du raisonnement vous permettant d'en venir à votre conclusion. Par exemple, si vous indiquez que la machine X offre le service Y, vous pourriez indiquer que les paquets 1, 56, 99 de la trace T vous mène à cette conclusion car « blablabla on a vu ça dans le cours blablabla… ». Cet élément sera particulièrement important pour l'établissement de la topologie du réseau, donc prévoyez un bon gros paragraphe pour justifier votre schéma de topologie.

Critères d'évaluation :

Information sur le réseau • **Topologie (schéma détaillé)** • **IP, MAC, OS, nom des machines** • **Services disponibles sur chaque machine** • **…**	**10 pts**
Information sur les activités durant l'enregistrement • **Actions faites par l'usager** • **Services utilisés** • **Sites visités** • **Séquencement des actions** • **…**	**8 pts**
Information personnelle simple sur l'usager • **Nom d'usager/mot de passe et service/serveur** • **Numéro de carte de crédit ou autres données financières** • **« Responsible Disclosure »**	**4 pts**
Information personnelle[4] complexe sur l'usager [Défi]	**3 pts**

Notes :

- Merci à l'équipe de XiVO (xivo.io), particulièrement à « Gregory Fodé ... Sanderson », pour leur aide dans la réalisation de ce travail, notamment au niveau de la trace TP2_ XiVO.pcap
- Ce travail est un travail ouvert. C'est-à-dire qu'il n'y a pas une solution complète attendue. Certains éléments clés sont attendus, d'autres sont souhaités, d'autre sont difficiles à obtenir et il y a certainement des éléments présents dont nous ignorons la présence. En ce sens, peu importe le nombre d'heures que vous mettrez sur le TP, certains éléments vous échapperons. Le conseil : débuter le TP tôt, travaillez-y régulièrement (n'attendez surtout pas à la dernière minute), et essayer de vous amuser (en travaillant sur le TP).

[4] Pour ce travail, le trafic a été capturé dans un environnement réel. Bien que beaucoup d'information fausse ait été introduite volontairement dans le trafic (pour rendre le TP intéressant), il est fort possible (pour être vraiment intéressant) que certaines informations vraiment personnelles apparaissent dans les traces. En suivant le modèle « Responsible Disclosure », il est de votre devoir d'informer votre professeur par MIO **DÈS QUE** vous trouvez de l'information personnelle (mot de passe ou autre), et ce même si vous croyez que l'information est fausse. De plus, il est strictement interdit de parler des éléments spécifiques que vous avez trouvé durant ce travail à d'autres personnes à l'intérieur ou à l'extérieur du cours (la NSA n'aime pas ça quand on parle du travail qu'ils nous donnent).