# 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

Cet exercice présente un exemple de simulation d'un réseau comportant un agent malveillant ayant infiltré un réseau d'entreprise et ayant déployé plusieurs services malveillants. Le fichier Paquet Tracer (PKT) présente un réseau comportant un agent malveillant.

## Attaque malveillante par DHCP Snooping et autres types

Pour réaliser cet exercice, vous devez avoir installé la version 8.2.1 du logiciel Packet Tracer disponible sur le lien OneDrive déposé sur le portail du cours. Une fois installé, lancez le fichier de simulation Packet Tracer (Exercice DHCNP Snooping) et attendez deux minutes avant de réaliser les exercices mentionnés dans les questions suivantes.

Ce délai de 2 minutes est nécessaire afin de permettre aux services de bien s'exécuter.

Vous devez ensuite répondre aux questions à joindre avec votre partie #1.

**Question #1**

Le site web du cours est en ligne et répond à l'intérieur du simulateur aux noms de domaine **inf362.ca** ou encore **www.inf362.ca**.

Ouvrez le PC #1, à partir du « Web Browser » disponible dans l'onglet « Desktop », rendez-vous sur le site web du cours à partir des adresses spécifiées.

A. Que pouvez-vous constater en visitant le site ?

Toujours sur le PC #1, lancez un ping vers le serveur Web avec l'adresse inf362.ca à partir de l'outil « Command Prompt » disponible dans l'onglet Desktop.

B. Quelle adresse IP est résolue par le ping ?
C. Que pouvez-vous constater ?

**Question #2**

Ouvrez le PC #2 et réalisez les mêmes opérations qu'aux questions #1 et #2

A. Que pouvez-vous constater en visitant le site ?
B. Quelle adresse IP est résolue par le ping ?
C. Que pouvez-vous constater ?

## Question #3

Ouvrez le PC #3 et réalisez les mêmes opérations qu'aux questions #1 et #2

A. Que pouvez-vous constater en visitant le site ?
B. Quelle adresse IP est résolue par le ping ?
C. Que pouvez-vous constater ?

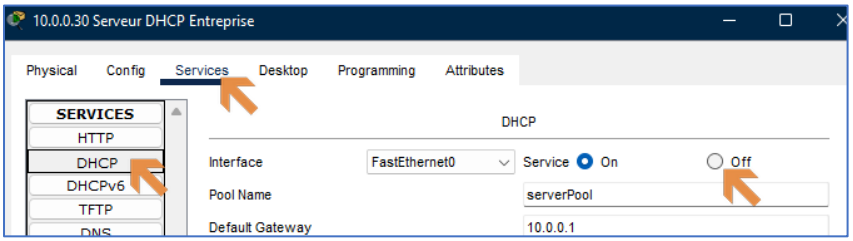
## Question #4

Ouvrez le PC #3 et réalisez les mêmes opérations qu'aux questions #1 et #2

A. Que pouvez-vous constater en visitant le site ?
B. Quelle adresse IP est résolue par le ping ?
C. Que pouvez-vous constater ?

## Question #5

Rendez-vous sur le « Serveur4 ». Dans l'onglet « Service », cliquez sur le bouton « DHCP » dans le menu de gauche et désactivez le service via le bouton à droite « Service = OFF ».



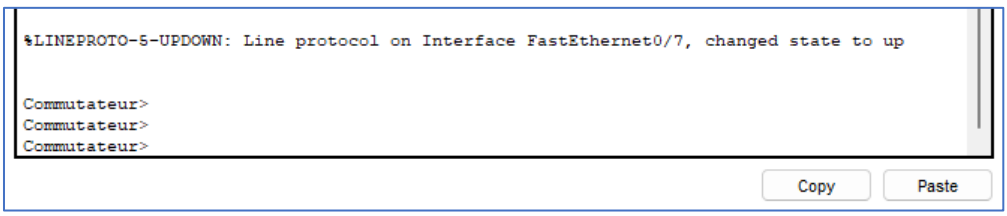

Attendez une minute que le service cesse de fonctionner. Rendez-vous ensuite sur le PC #2, dans le « Command Prompt » et lancez la commande : **`ipconfig /renew`**. Le PC devrait obtenir une adresse dans le réseau **10.200.0.x**.

Rendez-vous ensuite sur le site inf362.ca dans le « Web Browser ».

Que pouvez-vous conclure à la suite de ces tests ?

## Question #6

Rendez-vous sur le commutateur dans l'onglet « CLI ». Cliquez dans l'écran « IOS Command Line Interface » et donnez quelques coups de « Enter » sur le clavier. Vous devriez obtenir cette vue :




Entrez en mode privilégié dans le commutateur en saisissant la commande **`enable`** suivie d'un coup de « enter ».

Vérifiez si le commutateur est protégé contre le DHCP Snooping en lançant la commande : **`show ip dhcp snooping`**.

A. Est-ce que le commutateur est protégé contre le DHCP Snooping, détaillez votre réponse ?
B. À l'aide d'une recherche sur internet, que permet l'option 82 du service DHCP ?

## Question #7

Dans l'écran de configuration du commutateur en « Command Line », entrez en mode de commande en plaçant la commande **`conf T`**. Vous devriez voir le prompt du CLI afficher ceci :

```
Enter configuration commands, one per line.  End with CNTL/Z.
Commutateur(config)#
```

Lancez alors la commande : **`ip dhcp snooping`** et reprenons les précédentes questions.

A. Est-ce que le commutateur est protégé contre le DHCP Snooping, détaillez votre réponse ?
~~B. À l'aide d'une recherche sur internet, que permet l'option 82 du service DHCP ?~~

Retournez dans le « Command Prompt » des PC #1 et #2 et relancez la commande **`ipconfig /renew`** sur les deux PC.

C. Que pouvez-vous conclure ?

## Question #8

Le DHCP Snooping est un service que nous pouvons activer par VLAN. Par conséquent, nous devons définir ici le VLAN. Dans le CLI du commutateur, assurez-vous que vous êtes toujours en mode « configuration ». Le prompt du CLI devrait afficher « Commutateur (config) # ». Lancez la commande **`ip dhcp snooping vlan 1`**.

Il faut ensuite mettre un port du commutateur à « trust » afin de garantir que le trafic DHCP venant de ce port est bien autorisé et qu'il ne s'agit pas d'un agent malveillant tentant de débloquer compromettre votre infrastructure. Vous devez vous rendre sur la configuration du port Fa0/10 qui est le port sur lequel est raccordé le serveur DHCP officiel. Alors que vous êtes toujours en mode configuration, lancez la commande **`int fa0/10`**. Vous devriez être en mode configuration d'interface :

```
Commutateur(config)#int fa0/10
Commutateur(config-if)#
```

Lancez alors la commande **`ip dhcp snooping trust`** qui permettra alors le trafic DHCP sur le port désigné.

Remettez le service DHCP actif sur le « Serveur4 ». Référez-vous à la question #5 pour faire le chemin inverse.

Rendez-vous ensuite sur le PC #1 et #2, dans le « Command Prompt » et lancez la commande : **`ipconfig /renew`**. Les PC devraient obtenir des adresses dans le réseau **10.0.0.x**.

Retourner en mode privilégié dans le commutateur en saisissant la commande **`enable`** suivie d'un coup de « enter ». Si vous êtes en mode configuration, entrer la commande **`exit`** pour revenir au mode précédent.

Vérifiez si le commutateur est protégé contre le DHCP Snooping en lançant la commande : **`show ip dhcp snooping`**.

A. Est-ce que le commutateur est protégé contre le DHCP Snooping, détaillez votre réponse ?
~~B. À l'aide d'une recherche sur internet, que permet l'option 82 du service DHCP ?~~

**En conclusion :**

En guise de conclusion, répondez aux questions suivantes :

1. À la lumière de cet exercice, pouvez-vous identifier quels sont les services malveillants présents sur le réseau ? et où se trouvent-ils ?
    a. Décrivez votre démarche qui vous mène à ce constat ?

2. Que pouvez-vous conclure de ce type d'attaque ?

3. Que pouvez-vous conclure sur la protection appliquée et quelles sont les informations que l'administrateur réseau doit détenir afin d'assurer une configuration de la protection adéquate ?

## 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 huit (8) questions présentes. Vous devez également répondre aux questions incluses dans la conclusion.

Merci et bonne chance!