Université de Strasbourg

UFR de Mathématiques et d'Informatique

Licence Professionnelle ARS

Année 2018/2019

Réseaux Locaux

TP 1 : Analyse de trafic et prise en main Cisco

Introduction

Ce TP est à réaliser en binôme et sera évalué sur la base d'un compte-rendu à envoyer sur la plate-forme Moodle. Ce rapport devra se présenter sous la forme d'un document PDF et contenir les réponses aux questions posées dans le présent sujet ainsi que les commandes utilisées. Il devra en outre être agrémenté de captures d'écran et/ou d'extraits de fichiers de configuration.

1 Analyse de trafic

Afin d'analyser les flux entrant et sortant de notre machine, nous allons notamment utiliser l'analyseur de trafic *Wireshark*. Avec cet outil il est possible de capturer des trames directement sur les interfaces du système utilisé et/ou de lire des fichiers de captures sauvegardées. Wireshark tout comme *tcpdump* est basé sur la librairie *libpcap*. Cette librairie offre deux modes de fonctionnement :

- Le mode **normal :** permet uniquement d'analyser les trames à destination de la machine effectuant l'analyse.
- Le mode **promiscuous :** permet d'analyser tous les trames passant sur le bus. Cela même si les trames ne sont pas à destination de la machine effectuant l'analyse.
  Dans tous les cas, il faut avoir les droits d'un utilisateur privilégié pour analyser les trames circulant sur vos cartes réseau : par défaut, un utilisateur lambda ne pourra pas accéder à ces données sensibles.

1.1 Premier contact

Pour cela, effectuez les actions suivantes :

1. Identifiez l'interface de votre machine vous reliant à Internet ainsi que son adresse Ethernet

   ```
   ip -s link
   ```

2. Avec Wireshark, démarrez une capture sur l'interface repérée précédemment.

3. Lancez un navigateur Web et allez sur le site de votre choix. Une fois la page complètement

chargée, arrêtez la capture.

4. Relevez les valeurs des champs d'adresses sources et destinations dans les en-têtes Ethernet des trames capturées. Que pouvez-vous en dire ?
5. Identifiez le constructeur de votre carte réseau et le préfixe Ethernet qui lui est associé.
6. Créez un filtre permettant de n'afficher que les trames à destination de votre machine.
7. Après avoir repéré une trame contenant des données HTTP, observez le modèle d'encapsulation et les protocoles utilisés sur chaque couche. Comparez-le au modèle OSI.

1.2 Récupération d'information

Analyser les trames en mode promiscuous permet notamment de trouver des informations qui auraient dû rester confidentielles :

1. Repérez l'interface correspondant à votre machine dans la baie de brassage (numéro sur le câble bleu à l'arrière de la tour) et reliez-la au répéteur (hub) présent dans l'armoire.
2. Configurez votre machine pour utiliser cette interface pour accéder à Internet à l'aide de la commande `ip`.

   Désactiver l'ancienne interface de sortie :

   ```
   ip link set ethA down
   ```

   Où A est le numéro de l'interface vous reliant au réseau universitaire

   Activer la nouvelle interface :

   ```
   ip link set ethB up
   ```

   Où B est le numéro de l'interface reliée à l'armoire de brassage

   Assigner une adresse IP à l'interface

   ```
   ip addr add 10.0.0.X/8 dev ethB
   ```

   Où X correspond au numéro de votre machine

   Configurer la passerelle par défaut

   ```
   ip route add default via 10.0.0.254
   ```

3. Démarrez une capture sur la nouvelle interface en appliquant a priori un filtrage par adresse Ethernet ne gardant que les trames émises par votre voisin.
4. Demandez maintenant à votre voisin de lancer un navigateur Web, d'aller à l'adresse http://clarinet.u-strasbg.fr/~schreiner/teaching/rl/tp1.html et de renseigner un identifiant et un mot de passe factices. Une fois la page complètement chargée, arrêtez la capture.
5. Appliquez un filtre ne montrant que les messages HTTP et trouver celui qui contient les données POST avec l'identifiant et le mot de passe. Vérifiez que ceux-ci sont bien diffusés en clair.
6. Refaites la même manipulation sur le site :
   - https://clarinet.u-strasbg.fr/~schreiner/teaching/rl/tp1.html . Que remarquez-vous ?

1.3 Exercice

En conservant la configuration réseau précédente, démarrez une nouvelle capture n'affichant que les trames générés par la commande ping puis, en utilisant cette commande, déterminez les adresses Ethernet de toutes les machines reliées au répéteur. Vous pouvez vous référer au manuel pour apprendre comment utiliser et filtrer cette commande.

2 Prise en main des commutateurs Cisco

Les équipements de commutation que vous utiliserez en C315 sont des équipements de niveau 2/3 (commutateurs supportant le routage IP). Ces ponts/routeurs "Cisco" présentent plusieurs modes de fonctionnement :

- Le mode connecté ou utilisateur, accessible dès que vous êtes connectés.
- Le mode **monitoring** ou **privilégié** permet de consulter les fichiers de configurations, les tables de routages, de faire des ping, etc. Pour y accéder, tapez `enable` en étant en mode connecté.
- Le mode **configuration** permet de configurer les interfaces et les services du commutateur. Pour y accéder, tapez configure terminal en étant en mode monitoring.
  Pour retourner à un mode de configuration moins spécifique, de configuration à monitoring par exemple, vous pouvez utiliser les commandes exit (remonte d'un niveau) et end (retourne au mode monitoring).
  Vous pouvez à tout moment obtenir de l'aide sur les commandes en tapant "`?`". Utilisé seul, il affichera la liste des commandes disponibles dans le mode actuel ; à la fin d'une commande, il indiquera comment la compléter. Une complétion est également disponible via la touche de tabulation.
  Remarque : Pour gagner du temps, il est possible d'abréger la plupart des commandes en ne tapant que les premières lettres de chaque mot (juste assez pour que le système puisse reconnaître la commande). Par exemple, vous pouvez remplacer `enable` par `en`, `configure terminal` par `conf t` ou encore `show` par `sh`.

2.1 Configuration des commutateurs

Avant toute chose, vous allez devoir repérer un commutateur disponible et inscrire vos noms au tableau à côté de son numéro. Déplacez ensuite les câbles que vous aviez branché sur le concentrateur vers ce commutateur et ajoutez un troisième câble pour relier le concentrateur au commutateur.

1. Connexion à distance : Habituellement, la configuration de tels équipements se fait via une connexion série sur le port console du commutateur et un logiciel tel que "minicom". Une configuration à distance, plus simple, est cependant possible en salle C315. Il vous suffit donc de taper dans un terminal la commande :

   ```
   telnet console-api 200X
   ```

   où X représente le numéro de votre commutateur.

   Identifiez-vous ensuite à l'aide du mot de passe habituel de la salle (dans les champs login et password). Si une procédure d'auto-installation vous est proposée, refusez- la.

2. Réinitialisation de la configuration : Une fois connecté, passez en mode monitoring et entrez

les commandes suivantes :

```
show interface description
show running-config
```

3. Configurer les interfaces : En mode de configuration, vous pouvez sélectionner l'interface que vous souhaitez modifier avec la commande :

   ```
   interface FastEthernet 0/X
   ```

   où X correspond au numéro de l'interface.

   Éditez les interfaces sur lesquelles vous avez connecté vos câbles pour n'utiliser que du half duplex et limiter leur vitesse à 10Mb/s.

   Vérification : Vous devez ensuite vérifier que vos modifications ont bien été prises en compte (en mode monitoring) avec :

   ```
   show running-configuration
   ```

   Il peut parfois être fastidieux de devoir systématiquement sortir du mode de configuration pour utiliser des commandes de monitoring telles que celle-ci. Pour palier à ce problème, l'IOS de Cisco intègre une fonctionnalité permettant de taper ces commandes directement depuis un mode de configuration. Quelle est-elle ?

   Vérifiez également, à l'aide de la commande ip, que ces changements ont bien été répercutés sur les interfaces de vos machines.

2.2 Sauvegarder et charger des configurations

La configuration que vous avez effectuée est volatile. C'est-à-dire qu'elle n'est pas sauve- gardée en cas de coupure de courant ou de redémarrage du commutateur. Afin de sauvegarder votre configuration et que ce dernier redémarre avec cette même configuration il suffit de la copier sur le fichier de configuration de démarrage :

```
copy running-config startup-config
```

Pour sauvegarder ou charger une configuration à distance, une solution peut être d'utiliser un démon tftp sur un PC et de copier le fichier de configuration sur ou depuis ce serveur. Décrivez la procédure d'installation de ce service sur une machine ainsi que les commandes à utiliser pour transférer des fichiers de configuration entre votre machine et le commutateur.

Bonus : Trouvez une solution plus simple, quoique moins propre, pour arriver au même résultat.