HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Laboratoire OSER

Hubs, Switchs et ARP

21 novembre 2018

Objectifs

A la fin de ce laboratoire, vous devriez être capables de :

- Lancer une capture Wireshark sur une interface
- Utiliser les filtres Wireshark
- Analyser des paquets, en particulier les trames Ethernet qu'ils contiennent
- Expliquer et illustrer le fonctionnement du protocole ARP
- Monter un réseau simple selon un schéma
- Démontrer la différence entre le fonctionnement des hubs et des switchs
- Mettre en place et illustrer une attaque réseau simple

Matériels/Logiciels

- HUBs et Switches
- Wireshark

Travail demandé

Première partie - Wireshark

Pour la première partie de ce laboratoire, vous devrez :

1. Vous connecter au réseau de l'école en utilisant le bornier
2. Lancer une capture Wireshark sur l'interface correspondante
3. Choisir un paquet et l'analyser
4. Appliquer un filtre pour ne montrer que les paquets correspondant au même protocole applicatif que le paquet du point 3.

L'analyse de paquet devrait contenir au minimum :

- Le format de la trame Ethernet, le contenu de ses champs et leur signification
- Le code correspondant au protocole de la couche supérieure (Réseau/Internet), ainsi qu'une courte description de ce protocole
- Les adresses IP sources et destination
- Le nom et une courte description du protocole utilisé pour la couche transport
- Le nom et une courte description du protocole utilisé pour la couche application

Deuxième partie – ARP

Dans cette deuxième partie, vous devrez découvrir et présenter le protocole ARP, en utilisant Wireshark pour illustrer son fonctionnement. Les tâches suivantes devront être réalisées :

1. Faire quelques recherches sur l'utilité et le fonctionnement du protocole ARP et présenter le fruit de vos recherches dans le rapport.
2. Mettre en place un exemple d'utilisation du protocole ARP en capturant les paquets correspondant. Exécuter la commande *arp* avant et après afin de montrer le résultat.
3. Représenter le fonctionnement du protocole ARP sous forme d'un diagramme en se basant sur l'exemple du point 2.

Troisième partie – Hubs et Switchs

Dans cette dernière partie, vous expérimenterez les différences entre hubs et switchs au travers des tâches suivantes :

1. Monter le réseau correspondant à la figure 1.
2. Attribuer une adresse IP à chaque machine de votre groupe.
3. Lancer une capture wireshark sur la bonne interface (l'interface connectée au switch) et envoyer des pings aux autres membres de votre groupe.
4. Observer les paquets correspondant à des pings et commenter le résultat.
5. Monter le réseau correspondant à la figure 2.
6. Lancer une capture wireshark sur la bonne interface (l'interface connectée au hub) et envoyer des pings aux autres membres de votre groupe.
7. Observer les paquets correspondant à des pings et commenter le résultat.
8. Expliquer en quoi un des deux réseaux montés dans cette troisième partie peut constituer une menace en termes de sécurité. Inventer et décrire un scénario **basique** d'attaque permettant à un utilisateur malveillant d'accéder à des informations qui ne lui sont pas destinées. Décrire également les conséquences que cette attaque pourrait avoir, et comment il serait possible de s'en protéger selon vous.
9. **Bonus :** Réaliser l'attaque décrite au point précédent. *Conseil :* Plutôt que d'utiliser ping, trouver un protocole permettant d'envoyer des messages simples afin d'avoir des résultats plus intéressants (p.ex. netcat).

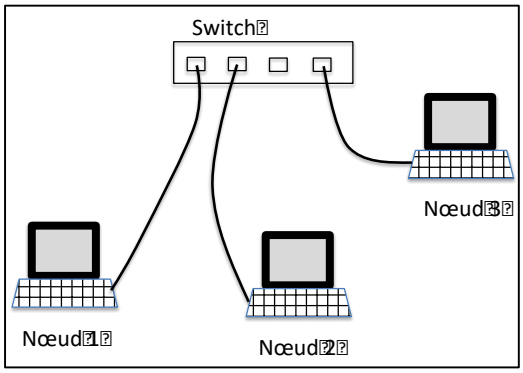

Figure 1

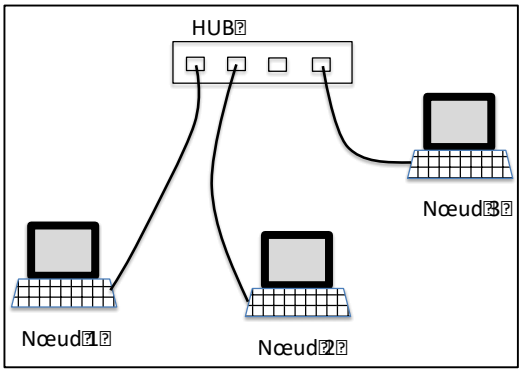

Figure 2

Rapport

Un rapport sera écrit par groupe de 4 étudiantes (à définir au début du laboratoire). Il contiendra :

- Une page de titre
- Une table des matières
- Une introduction (courte présentation du sujet, description des objectifs du laboratoire, structure du rapport)
- Une section montrant les tâches effectuées pendant la partie 1 et leur résultat
- Une section montrant les tâches effectuées pendant la partie 2 et leur résultat
- Une section montrant les tâches effectuées pendant la partie 3 et leur résultat
- Une conclusion (commentaires sur les résultats, difficultés rencontrées)

Détaillez les différentes manipulations que vous avez effectuées pour chaque partie. Illustrez vos explications avec des captures d'écrans ou des schémas. Gardez en tête qu'une personne ne connaissant que les bases du modèle OSI devrait être capable de comprendre ce que vous avez fait pendant le laboratoire et de le refaire elle-même par la suite.

Le nom du cours, la date, le numéro et le titre du laboratoire, ainsi que la date de rédaction, le numéro de groupe et le nom des membres du groupe devront également figurer sur le rapport.

Avant de rendre le laboratoire, relisez les objectifs et assurez-vous que votre rapport permet de voir que vous avez atteint ces objectifs. Si certaines manipulations n'ont pas fonctionné et que vous n'avez pas pu avoir de capture d'écran, expliquez le problème que vous avez rencontré et décrivez les étapes que vous auriez dû réaliser. Vous pouvez également ajouter des dessins ou des schémas pour présenter les résultats que vous auriez dû obtenir selon vous. Si vos explications sont justes, suffisamment claires et bien

illustrées, vous ne perdrez pas de points pour des problèmes techniques indépendants de votre volonté.

Rendu

Le rapport devra être envoyé par mail à lucie.steiner@heig-vd.ch avant le dimanche 16 décembre 2018 à 23h59. Le sujet du mail devra contenir le nom du cours, le numéro du laboratoire et le numéro de groupe.