Labo Réseau : Séance 1

Exercice

L'objectif de cet exercice est double. Premièrement il permettra de vous familiariser avec l'environnement Netkit et deuxièmement il vous permettra de comprendre le fonctionnement d'un switch.

A quelle couche du modèle OSI associe-t-on un switch ou commutateur ?

Couche 2 → liaison des données

1. Connectez-vous à une machine linux via le logiciel LeoStream
    1. login : votre login windows
    2. mdp : votre mdp windows
2. Téléchargez sur ecampus le labo netkit intitulé « netkit_lab_switch.tar.gz »
3. Décompressez le labo. (En ligne de commande pour faire remonter les souvenirs du cours de linux ...)
4. Lancez le labo (voir théorie)
5. Quelle est l'adresse IP du pc1 ? Quelle commande avez-vous utilisez ?

   10.0.0.1 → ifconfig

6. Quelle est l'adresse IP du pc2 ? Quelle commande avez-vous utilisez ?

   10.0.0.2 → ifconfig

7. Quelle est l'adresse MAC du pc1 ? Quelle commande avez-vous utilisez ?

   00:00:00:00:10:00 → ifconfig

8. Quelle est l'adresse MAC du pc2 ? Quelle commande avez-vous utilisez ?

   00:00:00:00:20:00 → ifconfig

9. Quel contient la table ARP du pc1 ? Quelle commande avez-vous utilisez ?

   arp

10. Tapez la commande suivante sur le switch1 : « brctl showmacs br0 » Que voyez- vous ?

    2 adresses MAC locales → c'est à dire celles du switch

11. Faites un ping de pc1 vers pc2 et refaites un « brctl showmacs br0 » sur le switch1. Que voyez-vous ?

    Le switch a mémorisé les adresses MAC du PC 1 et PC 2.

    Le PC 1 est branché sur le port 1 du switch, le PC 2 su le port 2.

12. Quel contient la table ARP du pc1 ? Quelle commande avez-vous utilisez ?

    L'adresse IP et MAC du PC 2.

13. Arrêtez le ping et relancez régulièrement le « brctl showmacs br0 ». Que se passe-t-il ? Essayez d'expliquer ce que vous venez de voir de la question 9 à 11.

    La table des adresses MAC du switch1 se vide après 10 secondes d'inactivité.

    La table ARP du PC 1 contient toujours l'adresse IP et MAC du PC 2.

14. Comment vider le cache ARP ? Quelle commande avez-vous utilisez ?

    Arp -d <<adresse IP>> → incomplete apparait

15. Réalisez une écoute sur le pc2 montrant un dialogue ARP **complet** (via une capture lisible dans wireshark). Réfléchissez à la meilleure manière d'obtenir ceci !

    1. **Vérifier que la table ARP du PC 2 est vide**
    2. **tcpdump -i eth0 -n -t -s 65535 -w capture.cap**
    3. **ping 10.0.0.1 depuis PC 1 (par exemple)**

16. Voyez-vous un problème de sécurité dans le protocole ARP ? Faites une recherche sur Internet et expliquez le problème.

    ARP spoofing → https://www.information-security.fr/attaque-man-in-the-middle-via-arp-spoofing/