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

Laboratoire OSER

Scénario d'attaque réseau

9 janvier 2020

Objectifs

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

- Mettre en place un réseau LAN basique avec des ordinateurs et un switch
- Communiquer entre deux ordinateurs en utilisant netcat
- Lancer un scan de ports TCP avec nmap et analyser le résultat
- Utiliser l'outil ettercap dans le cadre d'une attaque d'ARP Poisoning

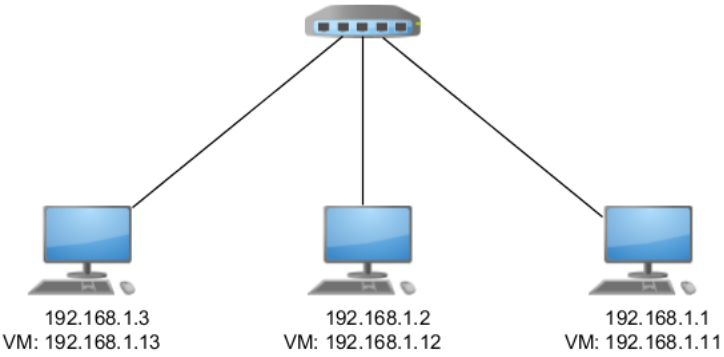
Matériel/Logiciels

- Machine virtuelle Kali
- Un switch par groupe

Travail demandé

Première partie – Mise en place d'un réseau

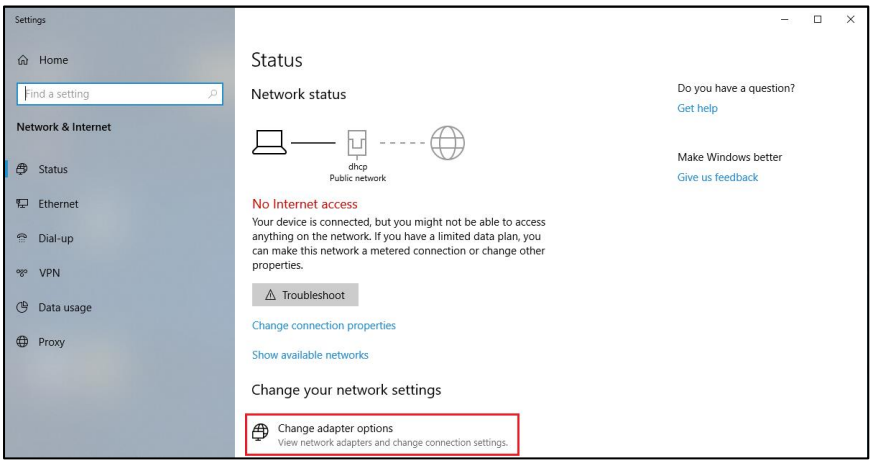
Pour ce laboratoire, vous devez créer un réseau avec 3 ordinateurs et un switch :

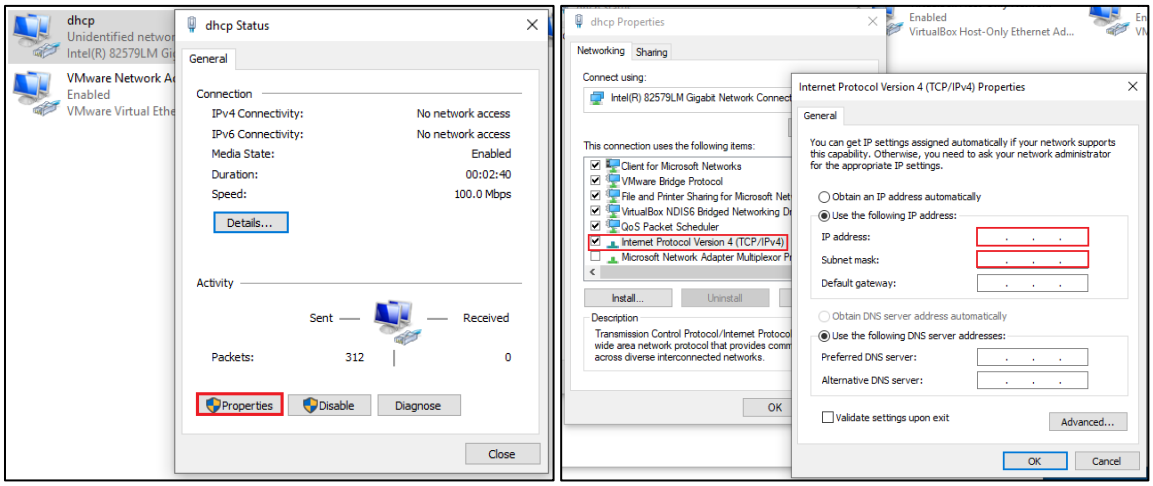


L'ordinateur avec l'adresse IP 192.168.1.3 représente l'attaquant et les deux autres seront les cibles de cet attaquant. Le masque de sous-réseau est 255.255.255.0

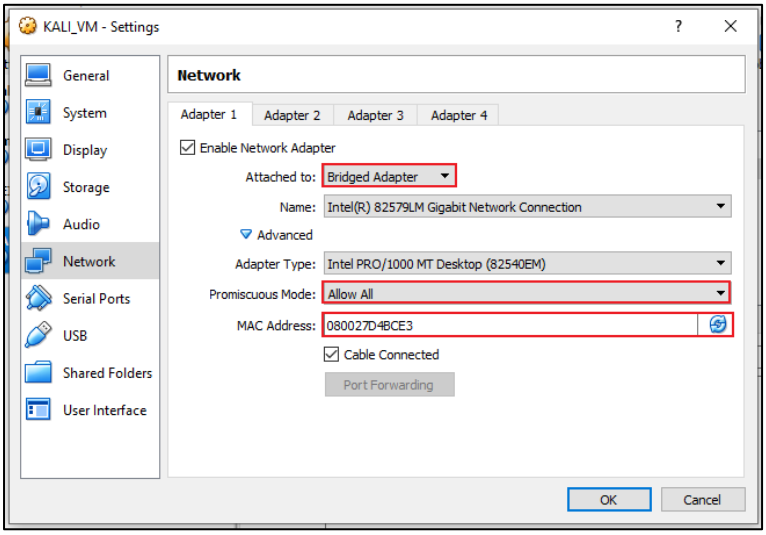
Pour mettre en place ce réseau, vous devez passer par les étapes suivantes:

1. Brancher les 3 ordinateurs sur le switch.
2. Attribuer manuellement des adresses IP aux ordinateurs selon le schéma (la première adresse IP est celle de l'ordinateur, la deuxième est celle qui sera attribuée à la machine virtuelle Kali). Les captures d'écran suivantes et les encadrés rouges montrent les étapes permettant d'attribuer manuellement des adresses IP.

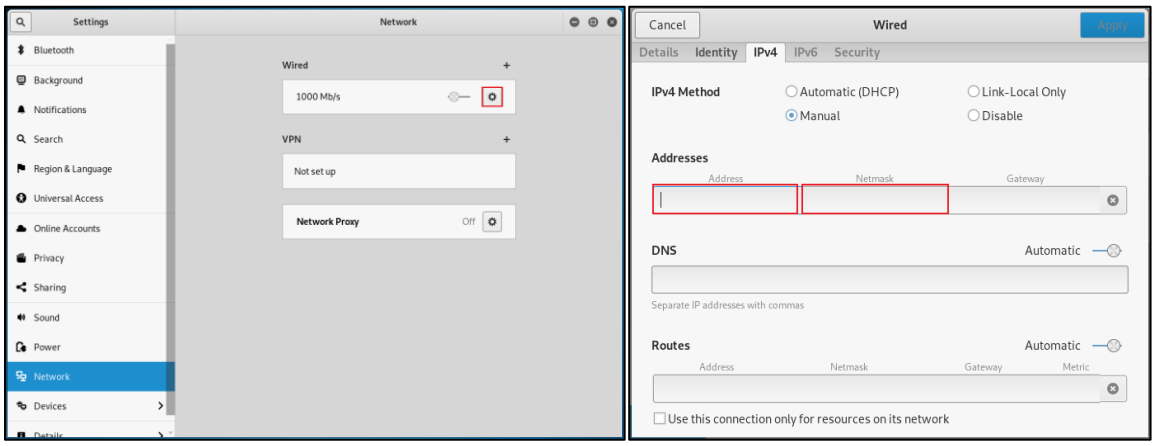




3. Lancer VirtualBox et modifier la configuration de la machine virtuelle Kali pour que le réseau soit en mode « Bridged ». Vérifier que les adresses MAC des 3 machines virtuelles sont différentes. Si ce n'est pas le cas, utiliser le bouton permettant d'en attribuer une nouvelle. Vérifier également que le mode « Promiscuous » est activé en sélectionnant « Allow All ».



4. Lancer la machine virtuelle Kali, et lui attribuer manuellement une adresse IP selon le schéma.



5. Vérifier que le réseau est configuré correctement en lançant des pings entre les différents ordinateurs et les différentes machines virtuelles. Pour lancer un ping, il suffit d'utiliser la commande suivante dans un terminal: ping <adresse_cible>, p.ex. ping 192.168.1.3.

Deuxième partie – Mise en place de la communication

Maintenant que le réseau est fonctionnel, les deux cibles doivent pouvoir s'échanger des informations. Elles vont donc se mettre d'accord sur un canal de communication secret sur lequel elles pourront s'échanger des informations secrètes. De son côté, l'attaquant va tenter de découvrir comment elles s'échangent ces fameuses informations.

1. Sur la machine virtuelle de l'ordinateur avec l'adresse IP 192.168.1.1, lancer la commande suivante : *nc -l -p <numéro_de_port>* en remplaçant *<numéro_de_port>* par un numéro de port de votre choix entre 1024 et 65535. Les deux cibles doivent se mettre d'accord sur le numéro de port sans en informer l'attaquant.
2. Sur la machine virtuelle de l'ordinateur avec l'adresse IP 192.168.1.2, lancer la commande suivante : *nc 192.168.1.11 <numéro_de_port>.* Vous devriez maintenant être en mesurer de communiquer en écrivant simplement du texte dans le terminal et en appuyant sur Enter.
3. L'attaquant doit maintenant tenter de découvrir comment les deux cibles communiquent. Pour ça, il doit lancer la commande suivante : *nmap 192.168.1.0-255 -sT*. Cette commande va lancer une attaque de port scanning TCP sur toutes les machines du réseau ayant une adresse IP entre 192.168.1.0 et 192.168.1.255, pour découvrir sur quels ports des applications tournent.

Troisième partie – Attaque

Maintenant que l'attaquant sait comment ses cibles communiquent, il va mettre en place une attaque lui donnant plus de pouvoir. Son but est d'arriver à intercepter le trafic entre les deux cibles, dans un premier temps juste pour lire les messages qui ne lui sont pas destinés.

1. Lancer l'outil ettercap, qui se trouve dans la catégorie « Sniffing & Spoofing » des applications.
2. Configurer ettercap pour une attaque d'ARP Poisoning à l'aide des étapes suivantes :
    a. Spécifier le masque de sous-réseau en allant dans le menu « Options > Set netmask ».
    b. Commencer à sniffer le trafic en allant dans le menu « Sniff > Unified Sniffing ».
    c. Récupérer les adresses IP des autres machines en allant dans le menu « Hosts > Scan for hosts ». Ils apparaitront sous « Hosts > Host List ».
    d. Les adresses IP des deux autres machines virtuelles correspondent à vos cibles. Pour les sélectionner utilisez les boutons « Add to Target 1 » et « Add to Target 2 »
3. Lancer une capture Wireshark chez l'attaquant, et laisser les deux cibles s'échanger des messages pendant un moment sans lancer d'attaque d'ARP Poisoning. Vérifier que l'attaquant n'intercepte pas les messages. Vérifier également que la table ARP des deux machines virtuelles cibles est correcte.
4. Lancer l'attaque d'ARP Poisoning avec ettercap en allant dans le menu « Mitm > ARP Poisoning » et en sélectionnant « Sniff remote connections ». Vérifier que l'attaquant peut maintenant voir le trafic avec Wireshark et que la table ARP des deux cibles contient des informations erronées.

5. **BONUS 1 :** Ettercap propose des filtres qui permettent de modifier ou de supprimer les paquets interceptés lors d'une attaque de type Man-in-the-middle. Vous pouvez les trouver sous « /usr/share/ettercap/ ». Le filtre etter.filter montre un filtre basique permettant de remplacer « ethercap » par « ettercap » dans les paquets qui sont interceptés. Créer une nouvelle version de ce fichier, qui permettra de remplacer des mots ou des lettres de votre choix et élaborer un scénario avec les cibles qui permet de montrer l'ampleur de cette attaque. Soyez créatives !

   Une fois que vous avez créé une nouvelle version du fichier etter.filter, vous devez le compiler en utilisant « etterfilter <nom_fichier> -o <nom_filtre>. Pour le nom du filtre, le mieux est d'utiliser etter.filter.<ce que fait votre filtre>, par exemple « etter.filter.modify »
6. **BONUS 2 :** Dans cette étape, il s'agira simplement de supprimer les paquets. Dans un premier temps, utiliser le fichier etter.filter.examples pour comprendre comment supprimer des paquets et créer votre propre filtre qui empêchera les deux cibles de communiquer.
7. **BONUS 3 :** Pour finir, créer un filtre qui ne supprime que les paquets contenant certains mots ou certaines lettres et imaginez un scénario avec les deux cibles pour montrer l'impact de cette attaque.

Rapport

Un rapport sera écrit par groupe de 4 étudiantes (à définir au début du laboratoire). L'écriture du rapport consiste à remplir les différentes sections du template fourni avec la donnée en tenant compte des différentes indications qui se trouvent dans la donnée. Les explications doivent être faites de la manière la plus claire possible et les exemples doivent être illustrés par des schémas ou des captures d'écran.

Rendu

Le rapport devra être envoyé par mail à lucie.steiner@heig-vd.ch avant le dimanche 19 janvier 2020 à 23h59. Le sujet du mail devra contenir le nom du cours, le numéro du laboratoire et le numéro de groupe.