Laboratoire de téléinformatique

Auteur : Romain Wenger, Gilles-Etienne Vallat
Assistante : Kenza Majbar
Professeur : Stephan Robert

5.12.2008

Version 1.2

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Introduction

Ce laboratoire se basera sur des attaques communes visant la couche MAC (ARP Spoofing et MAC Spoofing) dans le but de capturer un trafic réseau. Il présentera une méthode pour détecter ce type d'attaque (grâce à du logiciel) et de s'en prémunir efficacement (grâce à l'équipement matériel et logiciel).

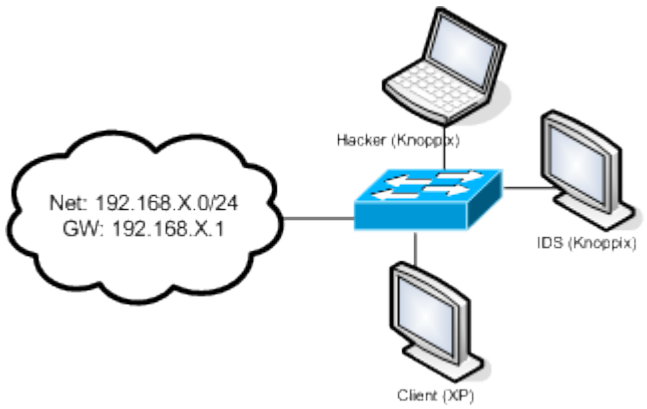
A chaque étape du laboratoire n'oubliez pas de présenter vos remarques ainsi que vos captures dans votre rapport.

Matériel

- 2 postes Linux à démarrer avec les CD de Knoppix (poste central 3xx et l'un des latéraux)
- 1 poste XP (installé un poste latéral 1xx ou 2xx)
- 1 switch CISCO 2900 ou 3500

Mise en place de l'infrastructure

Le schéma de votre réseau est le suivant:

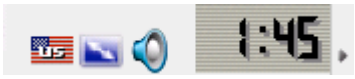


Le "X" est à remplacer par votre numéro de groupe.

Les trois machines recevront automatiquement une adresse par DHCP dès leur connexion au réseau. La passerelle permet l'accès à Internet par le réseau de l'école (attention au proxy).

Machines Linux

Le type de clavier ainsi que la résolution peuvent être modifiés en bas à droite de l'écran.



La carte marquée "DHCP" sur la machine centrale est normalement considérée comme l'interface eth2.

Il est possible que les machines Linux nécessitent l'activation de l'interface:
```
# sudo ifconfig eth0 up
```

La demande d'une adresse au DHCP peut aussi s'avérer utile:
```
# sudo pump –i eth0
```

Remarque: comme nous utilisons des LiveCD, toutes les captures seront perdues à l'arrêt de la machine. Il faut donc les sauvegarder sur une clé USB ou par Internet.

Tests

Contrôlez que les pings fonctionnent entre les machines et indiquez les adresses MAC et IP des machines sur le tableau.

Composant	IP	MAC
Gateway		
Client		
Attaquant		
IDS		

IP Forwarding

Sous Linux, le paramètre `/proc/sys/net/ipv4/ip_forward` définit la possibilité pour la machine de renvoyer un paquet qu'elle reçoit à la "bonne" destination.

Ce paramètre est à modifier après avoir choisi l'interface dans `ettercap`.

- Que se passe-t-il si l'IP Forwarding n'est pas activé sur la machine de l'attaquant lors d'une attaque ARP spoofing ?
- Créez un petit script (à nommer ~/`en-ip_forward`) activant cette fonction et le lancer grâce à `sudo ~/en-ip_forward`. Expliquez votre démarche.

Celui-ci doit être exécuté en tant que root après avoir activé les droits d'exécution.

1 ARP Spoofing

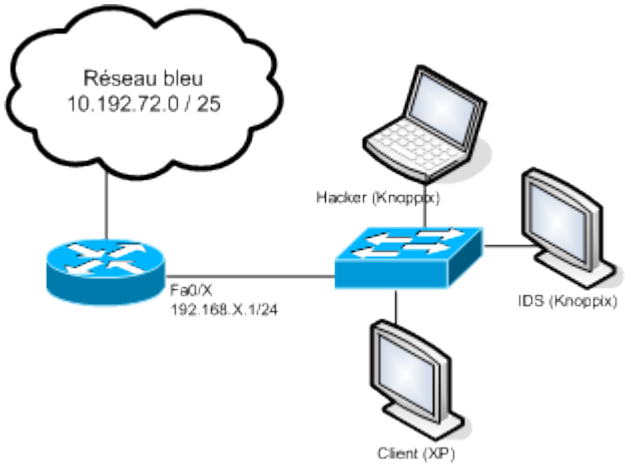
A partir de la machine attaquante, effectuer un ARP spoofing de type "one-way" entre la cible (Target 1) et la gateway (Target 2).

- Comment sont constitués les messages ARP (en précisant à quelles machines appartiennent les adresses) ?

Prenons l'exemple du trafic vers le Web; nous voulons voir les informations échangées entre la cible et les sites Web qu'elle visite.

- Que voyez-vous avec l'analyseur lorsque la cible charge une page Web ?
- Montrez que l'attaque est visible par la cible (cache ARP).

- Quels éléments réseau sont touchés par cette attaque ?
- Quel élément réseau s'est fait voler son identité ?
- Dessinez le chemin emprunté par les différents flux sur le schéma.

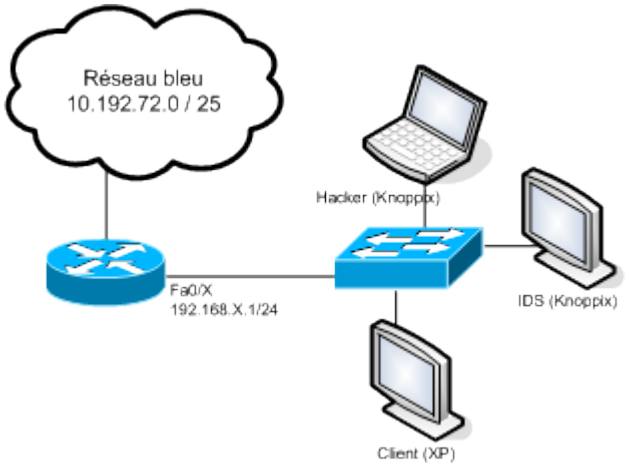


N'oubliez pas de stopper l'attaque par le menu Mitm à la fin de chaque attaque avec ettercap.

2 Man-in-the-middle

Effectuer maintenant une attaque de type "Man-in-the-middle".

- Que voyez-vous avec l'analyseur lorsque la cible charge une page Web ?
- Dessinez le chemin emprunté par les différents flux sur le schéma.



- Décrivez précisément l'attaque et représentez-la grâce à un diagramme en flèches.

Détection

Les risques de cette attaque maintenant démontrés, il est évident que des solutions permettant d'abord de la détecter puis de s'en prémunir devraient être mises en place.

De manière générale, l'intérêt d'une détection est double: en plus de voir qu'une attaque a été menée par la génération d'une alerte, cela permet d'en conserver une trace et ainsi souvent d'en connaître la source.

Le plus connu des outils de détection d'attaques ARP se nomme arpwatch. Il analyse le trafic réseau et indique tout message dont le but est potentiellement un spoofing d'adresse.

Port mirroring

La configuration d'un port mirroring sur le switch est nécessaire pour l'interface de la machine analysant le trafic. La commande permettant de le faire sur une interface d'un switch Cisco est `port monitor` (voir annexe).

- Décrivez cette fonction.
- Pourquoi notre IDS en a-t-il besoin pour détecter les ARP spoofing ?
- Activez cette fonction sur le switch.

arpwatch

Vous pouvez démarrer arpwatch sur l'IDS avec la commande suivante:

```
# sudo arpwatch -d
```

L'utilitaire arpwatch tient une table de correspondance entre les adresses MAC et IP du réseau. Pour que cette table dispose des adresses des différentes machines, effectuez un ping en direction de la passerelle depuis le poste client.

- Lancez l'attaque et expliquez les informations affichées.

Protection

Pour se protéger de ce type d'attaque, il faut que les machines ne changent pas leurs correspondances entre les adresses MAC et IP. Pour ce faire, il faut créer des entrées statiques dans la table ARP du système d'exploitation grâce à la commande:

`arp -s` *`[adresse IP] [adresse MAC]`*

Rentrez la correspondance entre l'adresse IP de la passerelle (192.168.X.1) et son adresse MAC dans le client et retestez l'attaque Man-in-the-middle.

- Est-ce que cette configuration suffit pour éviter les attaques vues précédemment ? Justifiez.

3 IP Spoofing & MAC Spoofing

Maintenant que l'attaque ARP Spoofing ne fonctionne plus, nous sommes obligés de changer l'adresse MAC de nos paquets émis pour correspondre avec l'adresse IP de la victime. Ainsi, l'attaquant va choisir les mêmes adresses MAC et IP que la passerelle afin d'en prendre sa place. Avant de changer ces adresses, il faut garder une trace de votre adresse MAC actuelle.

Pour changer son adresse MAC, vous pouvez utiliser la commande suivante:

```
ifconfig eth0 down hw ether [nouvelle adresse MAC]
ifconfig eth0 up
```

- Faites un ping sur la passerelle (192.168.X.1) depuis le client (avec l'option "`-t`" pour envoyer les pings en continu). Pendant que le client envoie ses pings, envoyez quelques pings depuis l'attaquant sur le client.
  Expliquez ce que vous voyez ainsi que ce qu'il s'est passé (sur le switch).

- Chargez une page provenant d'Internet et expliquez pourquoi la page ne peut pas être atteinte.

Protection

Cette manipulation est basée sur des switchs Cisco. Ces switchs ont plusieurs options de sécurité. Un guide de référence présentant ces commandes est disponible sur cette adresse:
http://www.cisco.com/en/US/docs/switches/lan/catalyst2900xl_3500xl/releasesa_sa1_sa2/cr/macrintr.html

port-security

Cette option permet de limiter le nombre d'adresses MAC sources utilisables sur un port donné. Cela signifie que l'on peut restreindre à n'utiliser qu'une seule adresse MAC source pour la machine connectée; ce qui l'empêcherait d'usurper celle d'un autre élément réseau.

Limiter le nombre d'adresse MAC par port à 1 sur les ports que vous utilisez.

- L'attaque fonctionne-t'elle toujours (justifiez) ?

Il est pourtant possible de changer son adresse MAC sur un port. Il suffirait d'attendre que le switch l'enlève de sa CAM ou, pour peu que l'on ait un accès à sa configuration ou que l'on puisse le redémarrer, d'effacer sa table CAM.

mac-address-table

Afin d'empêcher tout changement de MAC sur un port du switch, il faut l'empêcher d'enlever une MAC apprise. Pour y arriver, nous devons configurer le switch pour définir l'ajout des adresses MAC "secure" pour un port donné. Dans ce cas, il reste encore le moyen d'effacer sa table CAM ou de le faire redémarrer.

Pour garantir que la bonne adresse MAC soit connectée sur un port donné, il faut configurer le switch pour ajouter des adresses MAC "static" pour un port donné; cela ressemble un peu à l'ARP statique pour les postes.

Etablir la liste des MAC utilisables par port sur le switch et configurez-le.

Retestez l'attaque IP Spoofing et MAC Spoofing.

- Maintenant que votre infrastructure est sécurisée, critiquez-la en présentant ses avantages et inconvénients (en fonction de la sécurité ajoutée par rapport à la complexité d'utilisation).
- Donnez des exemples d'utilisation où nous devrions mettre en place ces solutions et où il serait peu envisageable de le faire; prenez des exemples réalistes pour une entreprise.