Laboratoire de téléinformatique

ANNEXE : ARP Spoofing et Man-in-the-middle

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

Cette annexe présente une méthode de mise en œuvre d'un attaque de type ARP Spoofing (ou ARP Poisoning) avec l'outil ettercap fonctionnant depuis le Live-CD Knoppix.

ARP Spoofing

L'élément de base d'un réseau informatique actuel est le switch. Plus évolué que le hub, il permet de diriger le trafic uniquement en direction de la bonne machine en se basant sur l'adresse MAC indiquée dans la couche Ethernet des paquets. De plus, cette méthode a l'avantage de permettre une largeur de bande maximale pour chaque port et non plus au niveau du concentrateur comme pour un hub.

Ainsi, lors d'une écoute du réseau via un analyseur, les messages n'étant pas destinés à sa propre machine ne sont pas visibles. Cependant, il existe une méthode bien connue pour "remédier" avec le protocole ARP.

Chaque machine conserve en cache une table de correspondance entre les adresses MAC et IP des correspondants connus. Il suffit alors d'envoyer des massages forgés indiquant l'adresse MAC de l'attaquant à la place d'une machine existante pour que ceux-ci lui soit envoyés. Il redirigera ensuite les messages au bon destinataire afin que la communication ne soit pas altérée.

Une évolution de ceci est l'attaque "Man-in-the-middle" qui permet de faire passer tout le trafic entre deux points par la machine de l'attaquant. Cette attaque est facilement réalisable avec l'aide d'un outil spécialisé comme par exemple ettercap, une application open-source disponible pour les principales plateformes actuelles.

IP Forwarding

Le "forwarding" des messages doit être activé au niveau de l'OS. En effet, comme les paquets destinés à la victime vont passer par l'attaquant, celui-ci devra les rediriger pour que la communication continue de fonctionner.

La commande suivante exécutée avec les droits root permet d'effectuer ceci:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Attention: cette commande doit être exécutée après le démarrage d'ettercap car ce dernier replace la valeur du paramètre à 0.

Ettercap NG

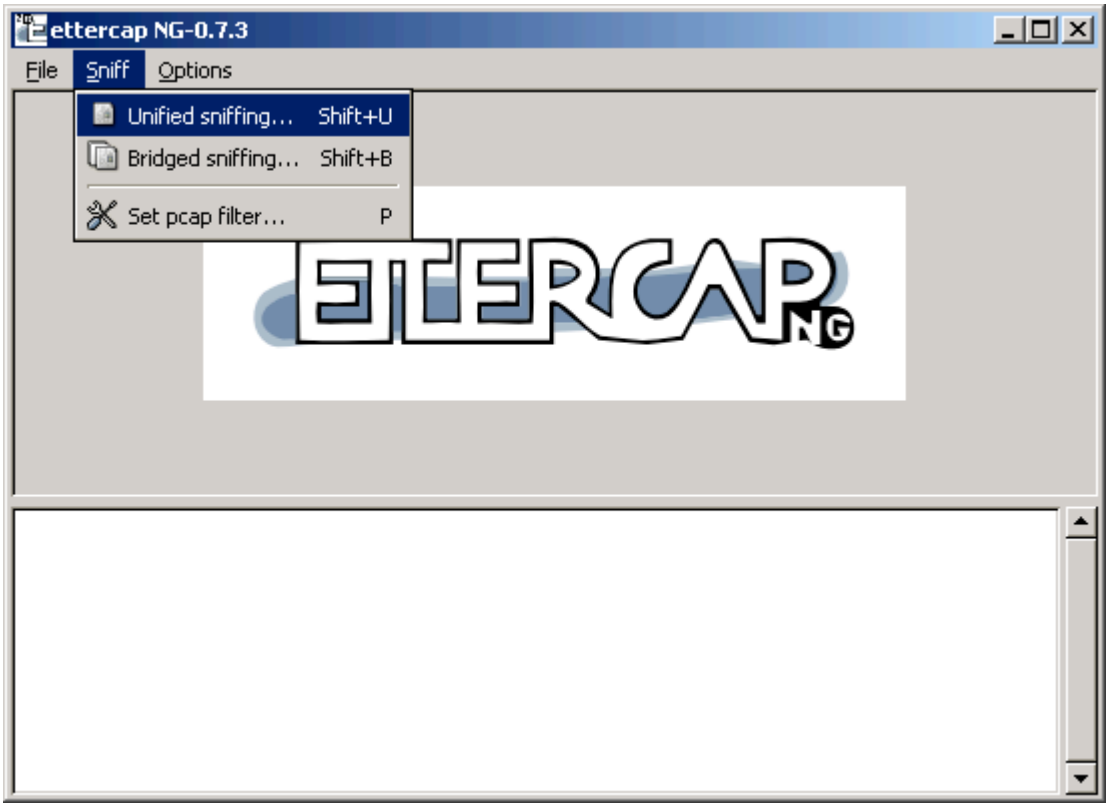
Le programme peut fonctionner en ligne de commande ou avec l'interface graphique.

La commande suivante permet de le démarrer:

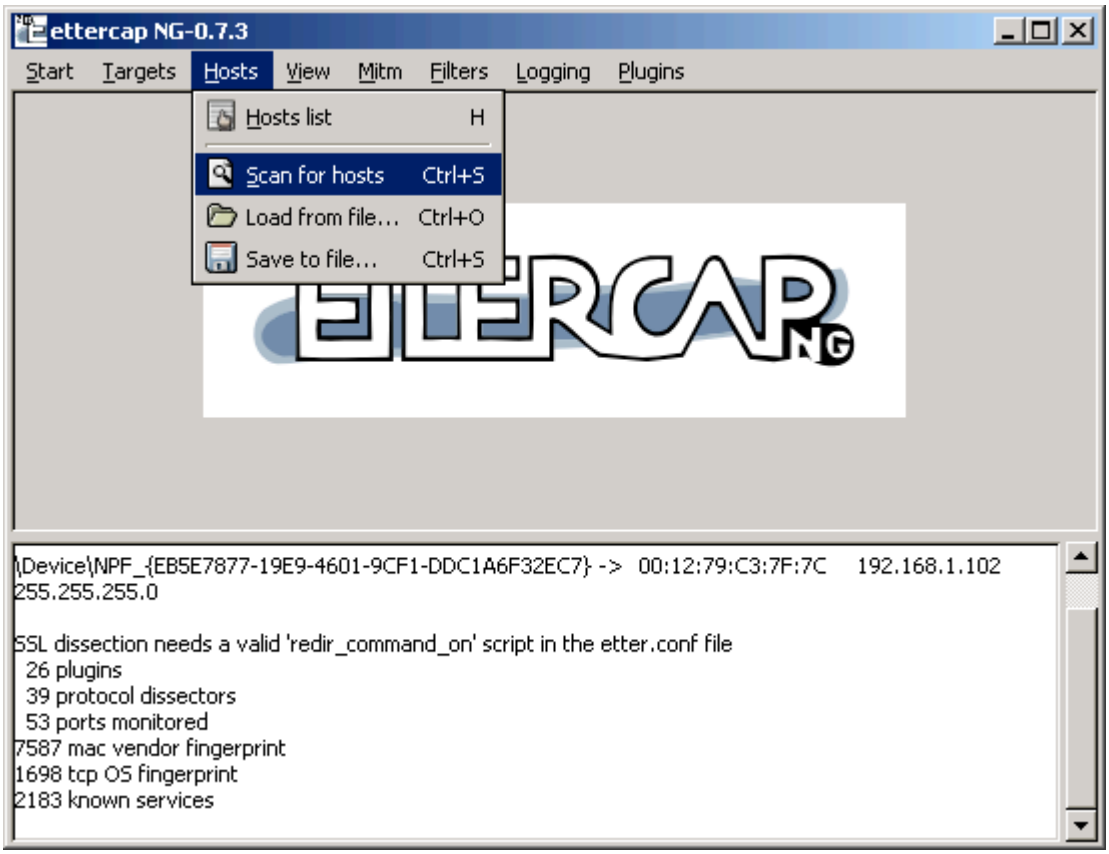
```
# sudo ettercap -G
```

Le "sudo" exécute la commande avec les droits root et le "-G" active l'interface graphique.

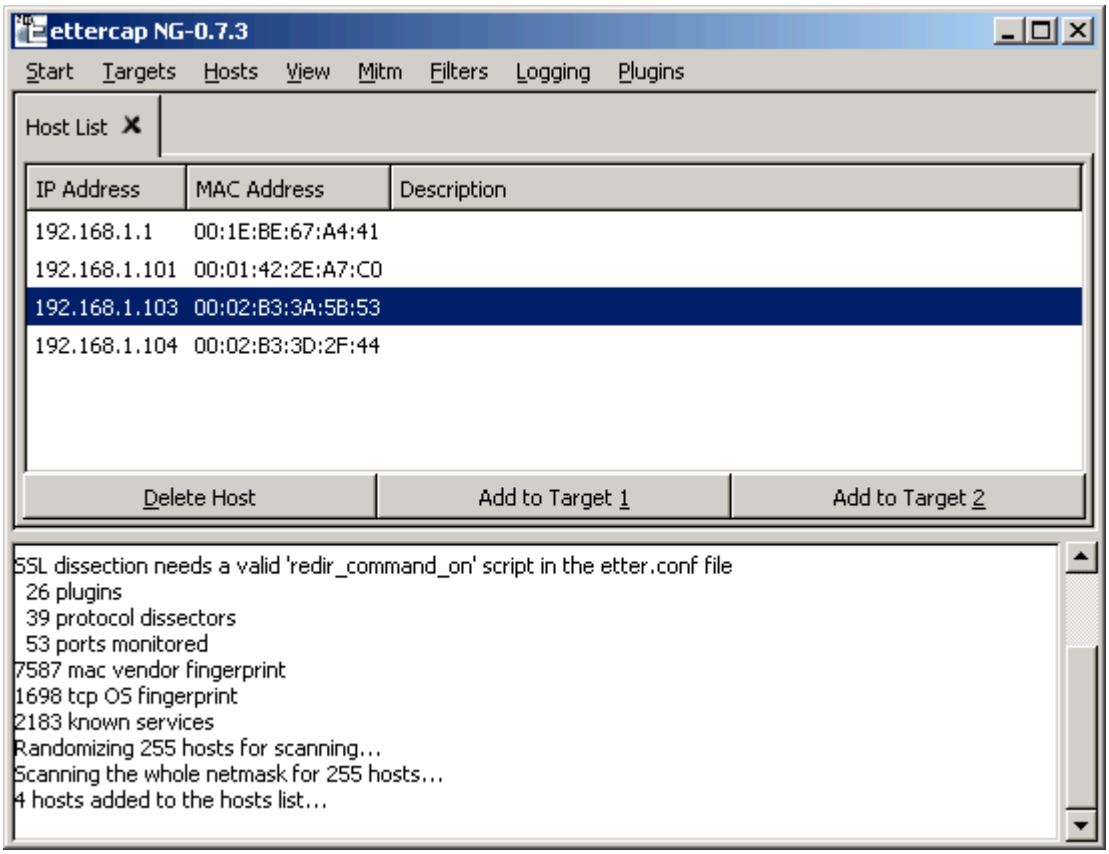
Aller ensuite dans "Sniff > Unified sniffing…" et choisir la bonne interface réseau à écouter.



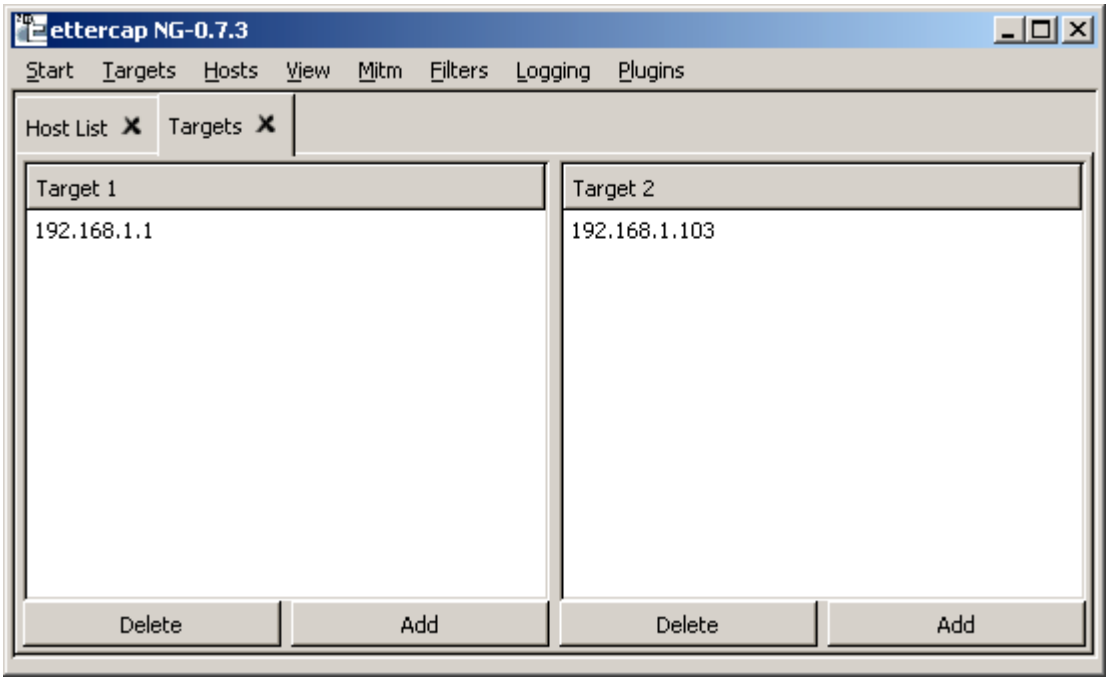
Puis choisir "Hosts > Scan for hosts" pour trouver les machines du réseau. Celles-ci sont alors listées par adresse IP en allant dans "Hosts > Hosts list".



L'idée consiste alors à définir deux targets entre lesquels nous voulons voir le trafic. Ceci s'appel un "Man-in-the-middle" ou MITM puisque l'attaquant se place entre les deux machines. Pour ce faire, il suffit de sélectionner la première machine puis la seconde pour les ajouter en tant que cible en cliquant respectivement sur les boutons "Add to Target".



Le menu "Targets > Current Targets" permet de voir les machines ajoutées.



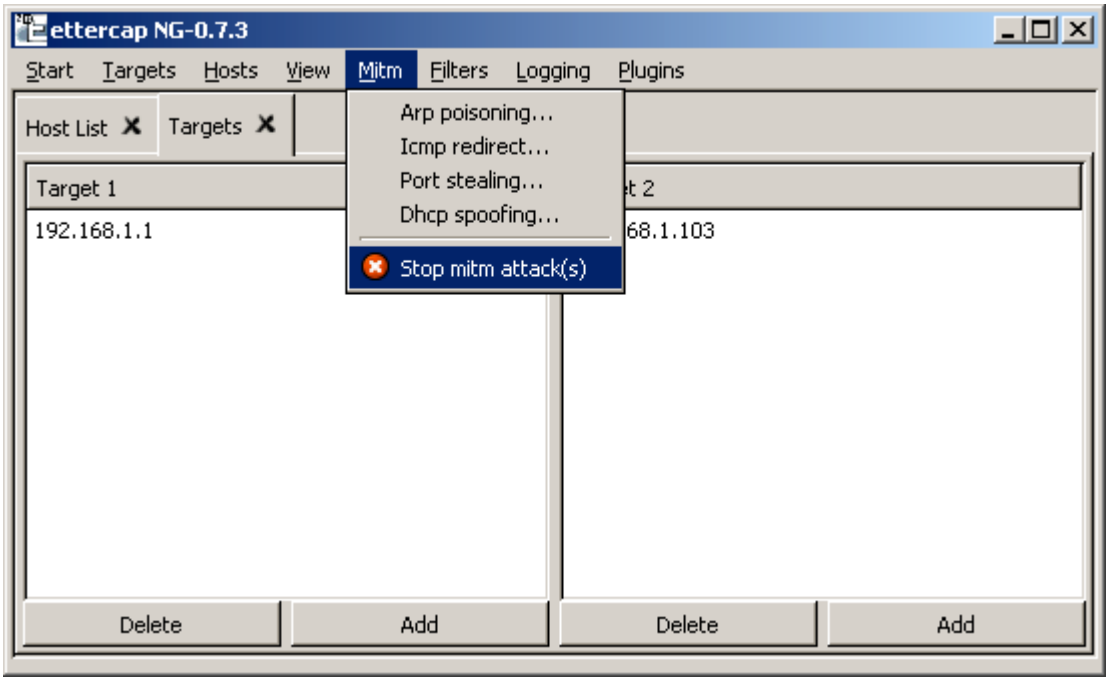
Attaque

L'attaque peut être exécutée de manière unique, on parle dans ce cas simplement d'ARP spoofing; ou bilatéralement, ce qui correspond alors au "Man-in-the-middle".

Choisir "Mitm > Arp poisoning…" pour lancer cette attaque.

A noter qu'un ARP spoofing simple du Target 2 est possible en cochant "Only poison one-way".

Remarque : afin d'éviter tout problème par la suite, il est important de désactiver l'attaque lorsque celle-ci n'est plus nécessaire en allant dans "Mitm > Stop mitm attack(s)". Ettercap enverra alors des messages ARP avec les adresses MAC correctes.


ettercap NG-0.7.3
Start
Targets
Hosts
View
Mitm
Filters
Logging
Plugins
Arp poisoning...
Icmp redirect...
Port stealing...
Dhcp spoofing...
Stop mitm attack(s)
Host List
Targets
Target 1
192.168.1.1
68.1.103
Delete
Add
Delete
Add