

SECURINETS



**CLUB DE LA SECURITE INFORMATIQUE
INSAT**

SECURILIGHT 2011

[Attaque MAN IN THE MIDDLE]

Chef Atelier : Fedi Boukhrouf (RT)

Soltani Nour (RT)

Sarah Thamine (GL)

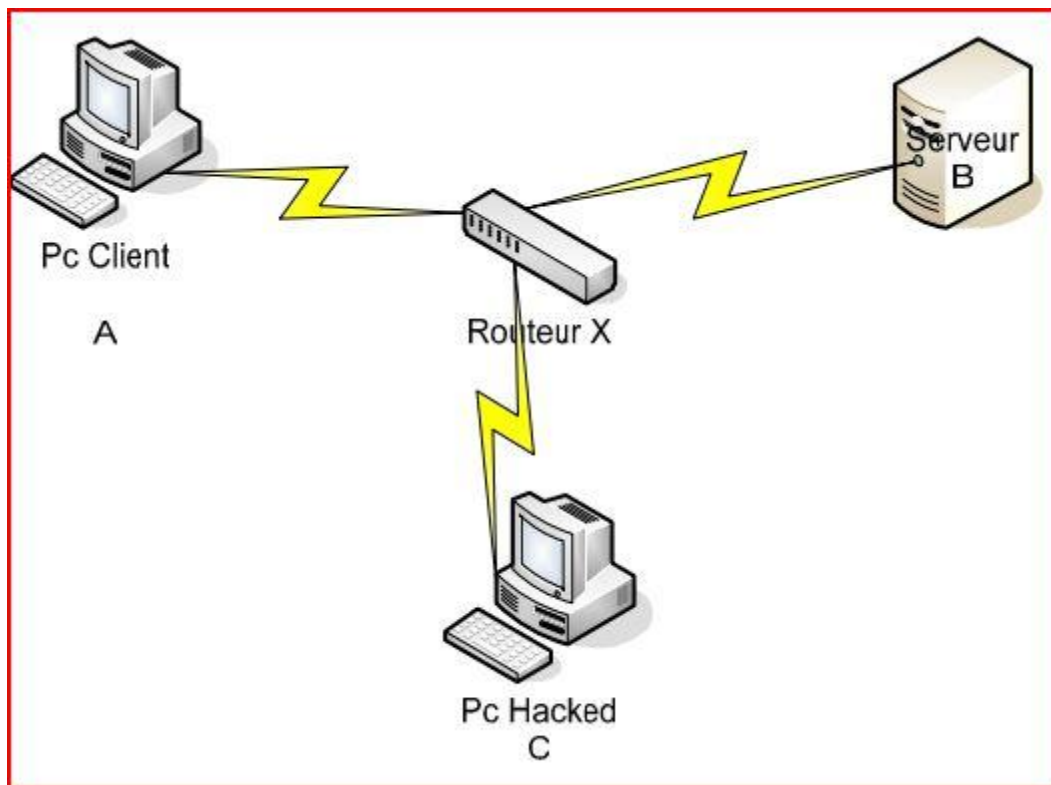
Faten Mkacher (RT)

30/11/2011

I. Définition de l'attaque MAN IN THE MIDDLE :

Man in the middle (l'attaque de l'homme de milieu) est une attaque qui a pour but de récupérer des données sensibles qui transitent sur le réseau local.

Cette attaque fait intervenir 3 ordinateurs : un serveur cible, un poste client et la machine où se trouve l'attaquant.



L'objectif de cette attaque est d'intercepter les communications par le pc C entre deux parties A et B, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

En effet, cette attaque exploite les failles du protocole arp.

En général, elle est menée pour des buts malveillants mais on la présentera lors de ce tuto pour pouvoir se protéger contre ce type d'attaque ☺

a. Présentation du protocole arp :

Les adresses IP sont attribuées indépendamment des adresses matérielles des machines. Pour envoyer un datagramme sur internet, le logiciel réseau doit convertir l'adresse IP en une adresse physique, utilisées pour transmettre la trame.

ARP(address resolution protocol) est un protocole qui fonctionne modèle TCP/IP à la couche Internet correspondant à la couche 3 du modèle OSI . L'objectif de ARP ,qui est un mécanisme de translation , effectue cette traduction entre le monde IP et Ethernet en s'appuyant sur le réseau physique. ARP

permet aux machines de résoudre les adresses sans utiliser de table statique répertoriant toutes les adresses des deux mondes. Une machine utilise ARP pour déterminer l'adresse physique du destinataire en diffusant dans le sous-réseau une requête ARP contenant l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique. Pour rendre ARP plus performant, chaque machinetient à jour en mémoire une table des adresses résolues et réduit ainsi le nombre d'émissions en mode diffusion.

i.les failles du protocole arp :

ARP est basé sur la confiance donc il n'y a aucun système d'authentification: il considère tous les messages reçus comme authentiques, qu'il provienne de la machine légitime ou pas et il n'intègre aucun moyen de vérification. La possibilité d'associer n'importe quelle adresse IP avec une adresse MAC permet à un pirate plusieurs vecteurs d'attaques.

En sachant que nous pouvons corrompre le cache arp de « n'importe » quelle machine connectée au

réseau, nous sommes en mesure de rediriger le trafic comme bon nous semble. Vous pouvez par

Exemple vous positionner entre un ordinateur et un routeurcomme c'est notre cas.Une fois placé entre ces deux machines, il est possible de déclencher une écoute passive du réseau(sniffing) à l'aide d'un analyseur de trames (sniffer). Je vous laisse imaginer les conséquences que cela pourrait avoir si toutes les informations recueillies tombaient entre les mains de personnes mal intentionnées.

b.ARP SPOFFING :

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.

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 messages 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

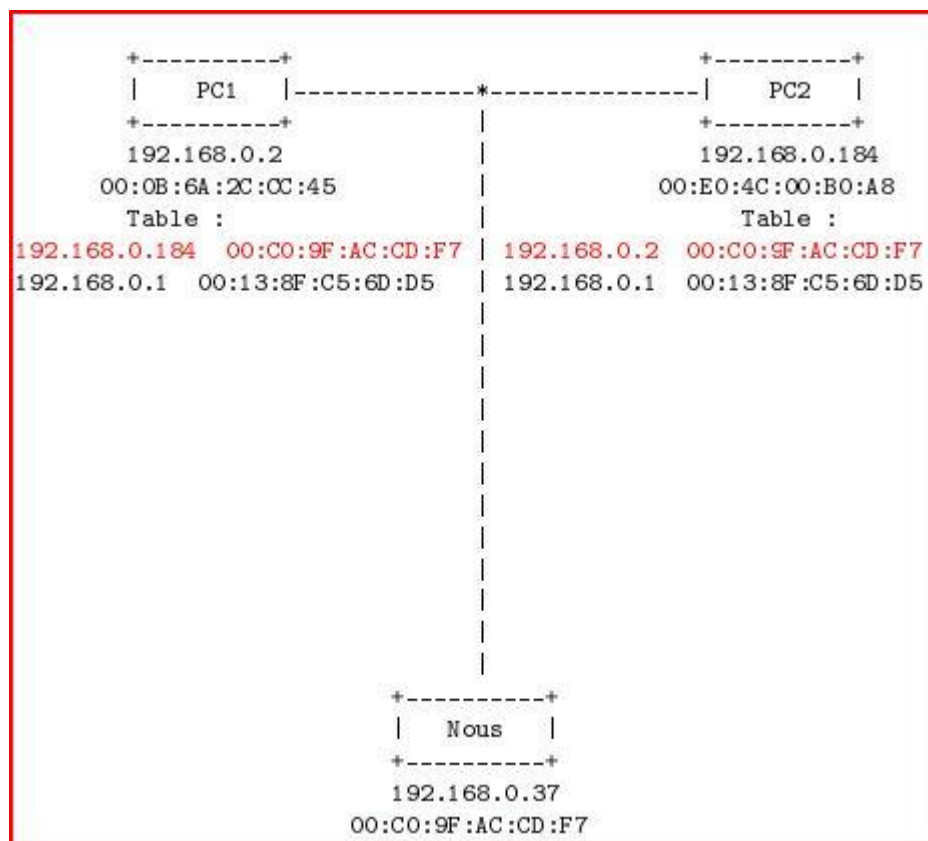
destinataire afin que la communication ne soit pas altérée.

=>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.

III/Etude pratique :

Lors de cet atelier on a utilisé le système BACKTRACK sur lequel est installé le logiciel Ettercap.

Pratiquement, on aura le schéma suivant :

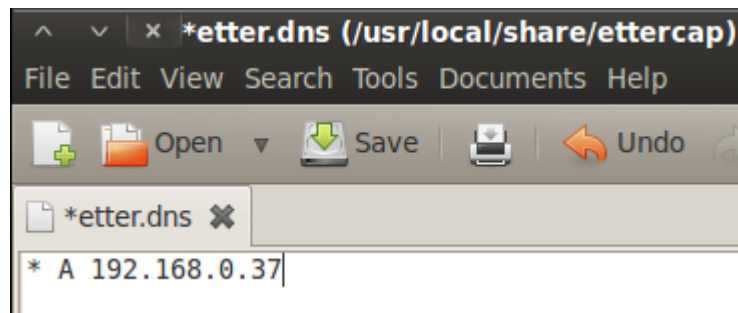


On remarque que l'adresse MAC des deux PC est celle de l'attaquant. Avec cette modification PC1 et PC2 nous enverront toujours les paquets quand ils voudront communiquer.

De cette façon, on peut appliquer toutes les règles de filtrage que l'on souhaite. Ci-dessous nous avons ce que voit 192.168.0.37 à travers le logiciel Ettercap. Comme nous le constatons, nous avons la main sur toutes les connexions, et même les paquets si on le souhaite

On redirigera toutes les requêtes adressées au serveur web vers une page statique qu'on a créée (sera jointe avec le tutorial) et qu'on a intégré sous le répertoire /var/www (qui représente le répertoire du serveur apache), sans oublier le fait qu'on a modifié le fichier etter.dns qui se trouve sous le

repertoire /usr/local/share/ettercap afin de preciser où le trafic sera redirigé(dans notre cas vers l'adresse ip de la machine du pirate :192.168.0.37)



=>signifie que toutes URL saisies par la victime sera spoofée vers l'adresse 192.168.0.37

On a utilise ettercap de mode console ,apres l'execution de cette commande l'outil ettercap va analyser l'infrastructure reseau et puis spoofer les requetes qui lui arrivent vers la page qu'on a crée.

```
root@bt:~# ifconfig
eth2      Link encap:Ethernet  HWaddr 00:0c:29:fc:a9:57
          inet addr:192.168.0.37  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5c:a957/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3694 (3.6 KB)  TX bytes:1948 (1.9 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1809 (1.8 KB)  TX bytes:1809 (1.8 KB)

root@bt:~# ettercap -T -q -i eth2 -P dns_spoof -M arp // //
```

VI)Comment se protéger de MITM :

Il faut savoir qu'il est difficile de se protéger contre l'attaque de man in the middle. Seulement on peut toujours prendre des mesures de sécurité.

Pour les petits réseaux ,On peut utiliser des ip fixes et des tables ARP statiques ainsi ils ne changeront jamais quel que soit les messages reçus. On peut mettre un contrôleur de domaine afin de définir un scripte de démarrage qui spécifiera ces adresses. Et de maintenir une liste.

Pour les grands réseaux, L'utilisation de switch cisco est fortement recommandée. Ils contiennent des options ports security qui permettent de définir une seule adresse mac par port. S'il y a changement d'adresse mac, le port se verrouillera.

Cela permet de limiter la plupart des attaques ARP.

=>La meilleure protection contre le MitM est la surveillance du réseau du fait que l'attaque ne peut pas passer inaperçu. En effet, il existe des outils qui permettent de détecter les messages ARP anormaux tel ARP watch.

De plus en aval d'une attaque MitM, il y a différentes solutions de protections tel la création d'une connexion SSH ou d'une connexion VPN qui sont cryptés et sécurisés.