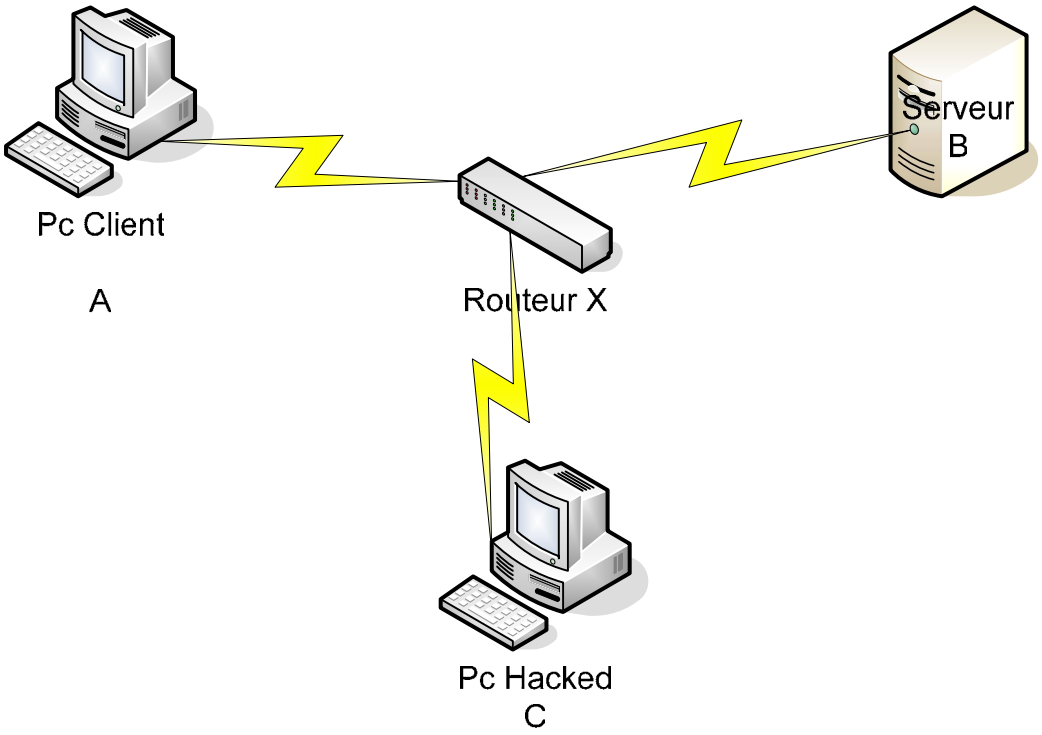
Man In The Middle

(MITM ou TCP hijacking)

Ce type d'attaque, traduit en français par « l'homme du milieu » est plus facile à comprendre qu'on ne le pense.

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

Schéma du réseau 1 :



Le but de l'attaque, est que le pc C (celui de l'attaquant) récupère les informations transitant entre A et B. Mais comme vous le savez dans un réseau switché ceci est plus difficile qu'avec un hub où toutes les informations sont envoyées à tous les ordinateurs connectés à celui-ci. Le Switch, lui, envoie seulement à la bonne personne.

Biensur, il y a la méthode agressive : l'ARP poisoning qui consiste à empoisonner tout le réseau ARP des requêtes ARP afin de se faire passer pour telle ou telle machine et récupérer les données. Mais cela est très voyant et provoque la plus part du temps voir tout le temps une coupure au niveau du réseau.

Maintenant, nous allons voir un peu de théorie sur l'ARP et les couches réseau.

Que signifie ARP ?
Address Resolution Protocol

Cela consiste à faire la correspondance entre les adresses MAC des machines et les IPs d'un réseau. Cette couche travaille au niveau 3 du modèle OSI, qui correspond à la couche réseau et dans la couche internet au niveau du modèle TCP/IP.

Plus d'infos ici :

http://www.commentcamarche.net/internet/tcpip.php3
http://www.frameip.com/entetearp/

Bon en fait je crois que je ne vais pas plus m'étendre sur la théorie car tout se trouve sur internet et en français, et je pense que la plupart connaissent en partie comment fonctionne le modèle TCP/IP.

Maintenant, il faut savoir que sur tout réseau Ethernet, il existe un cache ARP pour éviter de perdre du temps, et celui-ci est mis à jour régulièrement, toute les 30 ou 60s si je ne me trompe pas. Le but est donc de pouvoir convertir ce cache afin que nous nous fassions passer pour une autre machine. Le seul souci est que, si nous faisons seulement ceci, nous capturerons les paquets mais nous ne les renverrons pas à la bonne machine. Donc la subtilité est qu'il faut transmettre les paquets à la bonne machine de destination. Donc pour ce faire il suffit juste d'activer le forwarding. Toute de suite vous allez penser oui mais sous Windows ce n'est pas possible, il faudrait un iptable à la sauce Linux pour faire cela. Oui mais qui a dit que dans Windows, il n y avait pas un « iptable cache».

Conséquence, le site de Microsoft va nous être utile une fois de plus. Voici deux liens pour Windows XP et Windows 2K pour activer les forwarding dans windows.

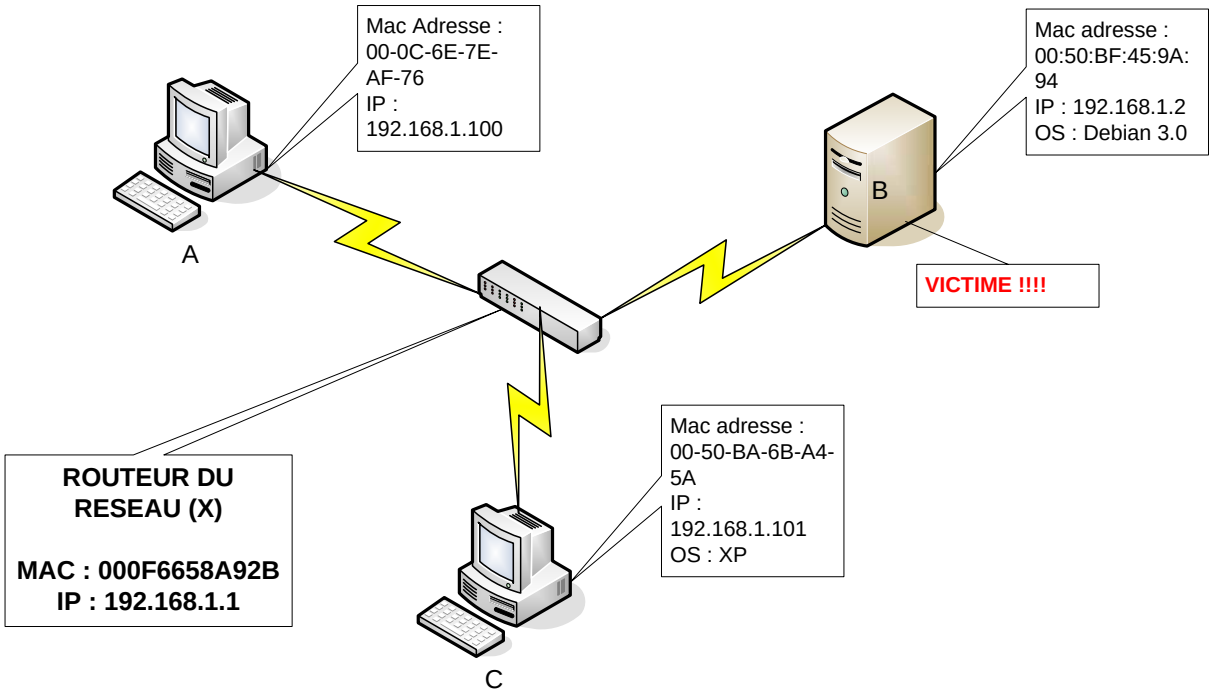
XP : http://support.microsoft.com/?kbid=315236
2K : http://support.microsoft.com/kb/230082/

Voilà ; plus qu'à modifier, relancer la machine pour être sur que cela fonctionne et hop nous pouvons passer à la suite.

Maintenant, il nous faut un logiciel qui va empoisonner notre cache ARP. Plusieurs possibilités s'offrent à nous : par interface graphique ou par fenêtre DOS. Bon sachant que tout le monde n'est pas forcément à l'aise sous DOS nous verrons les deux.

Avant tout regardez le schéma ci-dessous détaillant l'infrastructure IP du réseau (très simple, certes, mais c'est le principe de fonctionnement qui nous intéresse).

Schéma réseau 2 :



CACHE ARP Machine A: (avant attaque)

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:0F:66:58:A9:2B   C                     eth0
192.168.1.101            ether   00:50:BA:6B:A4:5A   C                     eth0
```

CACHE ARP Machine B: (avant attaque)

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:0F:66:58:A9:2B   C                     eth0
192.168.1.101            ether   00:50:BA:6B:A4:5A   C                     eth0
```

Donc, comme vous le voyez, tout pour le moment a l'air tranquille ☺
Alors là ca va être la partie qui je pense va le plus vous plaire, la partie démonstration de l'attaque.

Méthode n° 1 : Cain

Et oui Cain est un logiciel très très utile qui fait on va dire « presque tout tout seul ».
Donc premièrement téléchargez ce dont vous avez besoin.

Winpcap (indispensable) : toujours prendre la dernière version
http://winpcap.polito.it/install/bin/WinPcap_3_1_beta4.exe <= version non gui ☺

Cain : il vaut également mieux prendre la dernière version à jour avec les dernières techniques.
http://www.oxid.it/downloads/ca_setup.exe <= version 2.67

Et le plus indispensable, le petit fichier .reg pour modifier le registre.

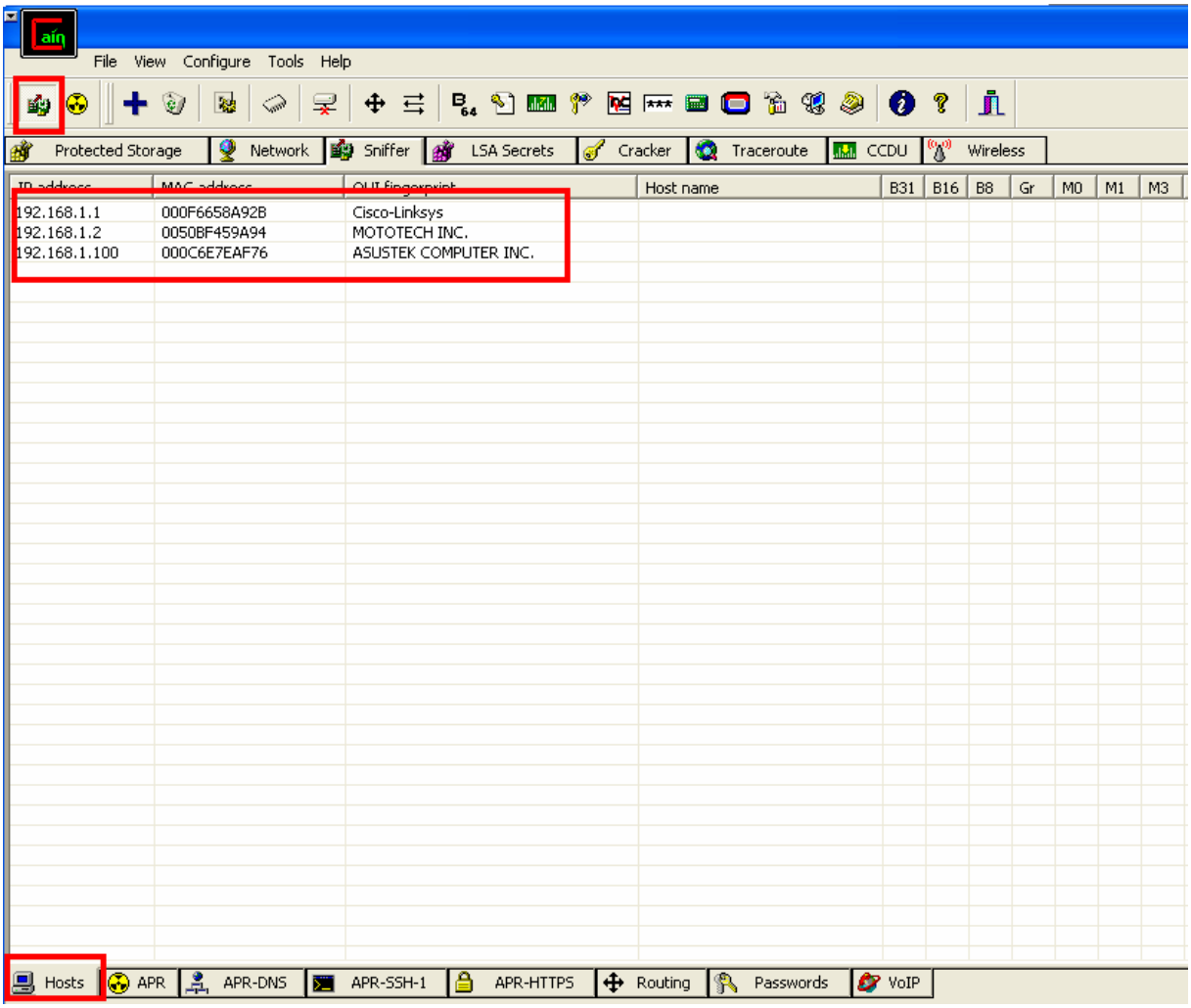
```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"IPEnableRouter"=dword:00000001
```

Ca marche pour XP et 2K ;)

Peut être qu'un petit reboot s'impose selon les machines…

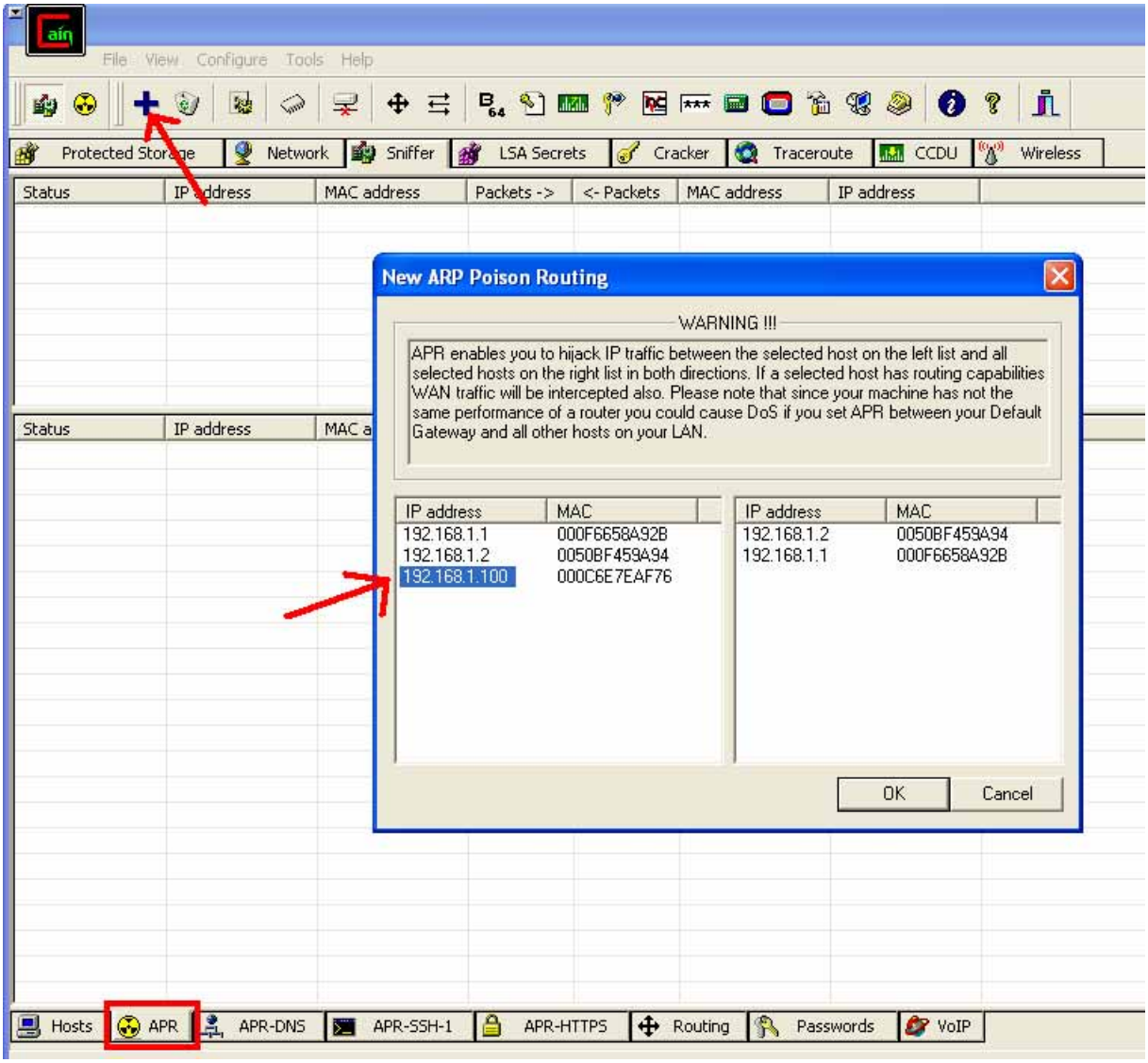
Ensuite vous ouvrez Cain bien gentiment.
Donc une petite fenêtre s'ouvre comme d'habitude :p, ensuite il vous faut cliquer sur ce qui ressemble a un icône d'une carte réseau en haut à gauche. Cela sert à sélectionner la carte réseau avec laquelle vous allez sniffer. Et vous vous positionnez dans l'onglet *sniffer*. A partir de là il vous faut ajouter les adresses entre lesquelles vous allez sniffer. Rien de plus simple avec Cain. Clic Droit => scan all MAC address in my subnet. Hop c'est fait il a tout scanné et vous avez juste à choisir l'IP a sniffer. (fig 1)

Figure 1 :



Rien de plus simple, vous allez dans l'onglet *ARP*, et vous cliquez sur la petite croix bleue en haut et vous choisissez l'host. (fig 2)

Figure 2 :



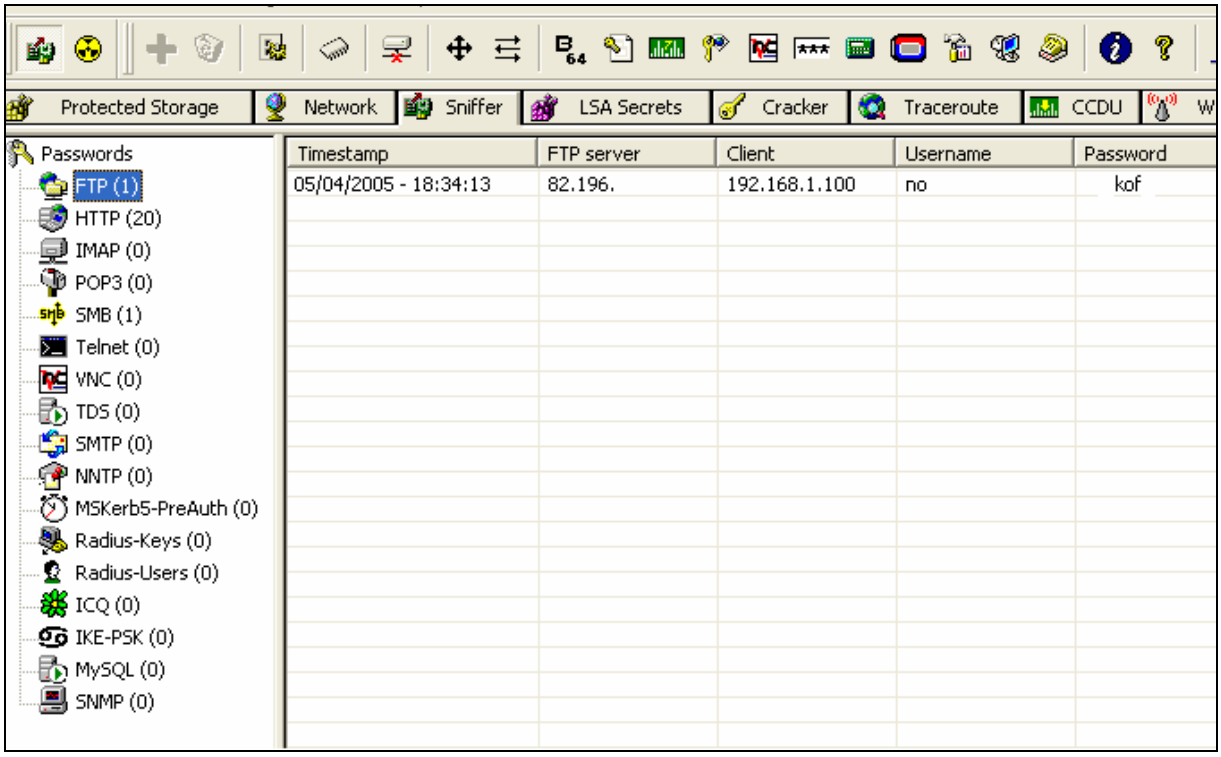
Nous allons donc écouter les connexions émises par le poste 192.168.1.100 (Machine A). Nous allons effectuer une connexion sur un serveur http qui demande une authentification par htaccess et sur un serveur ftp.

Donc comme vous les voyez sur la figure 2, en empoisonnant la machine 192.168.1.100 (A), nous avons le choix de nous faire passer pour 192.168.1.2 (B) ou 192.168.1.1(X).
Vous cliquez juste sur 192.168.1.1 et OK et vous pouvez lancer l'opération à l'aide de l'onglet jaune sniff à coté de celui du début.

Maintenant, la machine C (celle du hacker) va empoisonner le cache afin de se faire passer pour le routeur (ou gateway) du réseau afin de tout récupérer.

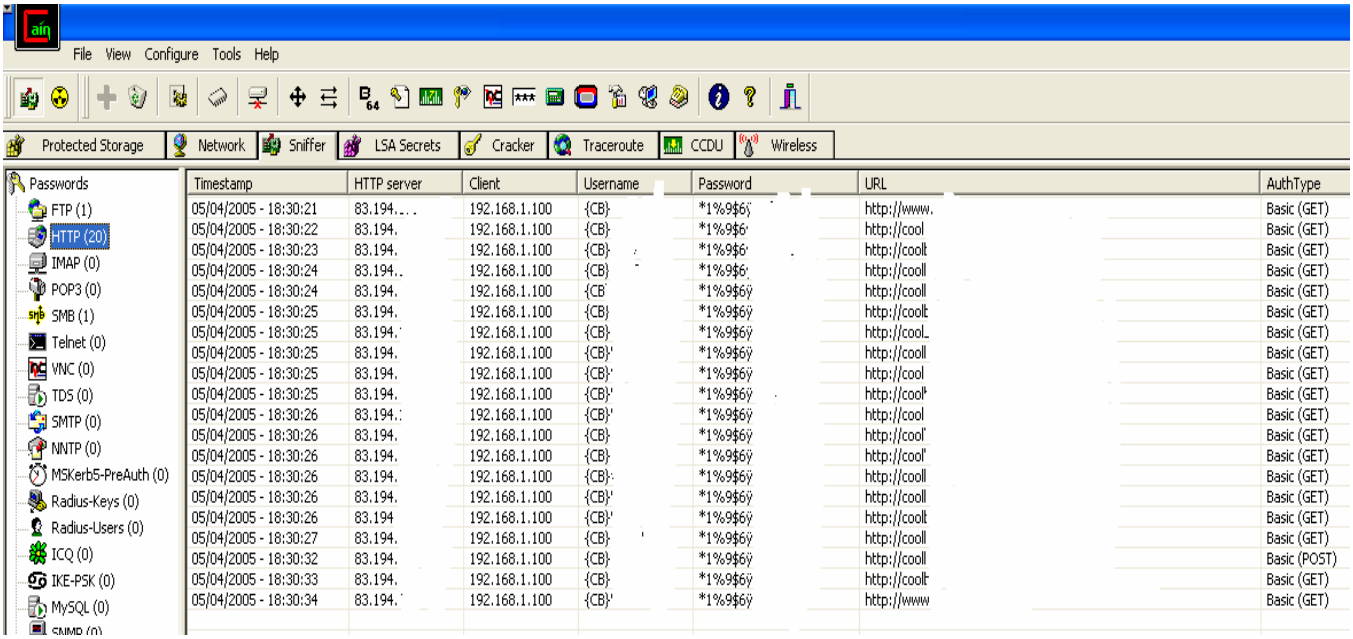
Et ensuite il suffit de faire les manipulations pour se connecter sur le site web avec htaccess et un serveur ftp distant et regarder dans la partie *password* de Cain. (fig 3 et 4)

Figure 3 (résultat FTP) :



Comme vous voyez, il y a le résultat de la connexion FTP (volontairement tronqué).

Figure 4 (résultat HTTP) :



C’est magique vous avez le login et password htaccess. ☺

Mais comme vous le voyez j'ai aussi capturé une session smb windows. Mais que je ne vais pas vous montrer car ca sert a rien ^^. Vous prenez les hashs un rainbowcrack et c'est parti ;). Vous avez biensur le droit de le faire avec les autres types de paquets que capture Cain. ☺

Et pour finir avec Cain, nous allons voir comment est maintenant le cache ARP des machines :

Machine A : Interface : 192.168.1.100 --- 0x2

Adresse Internet	Adresse physique	Type
192.168.1.1	**00-50-ba-6b-a4-5a**	dynamique
192.168.1.2	00-50-bf-45-9a-94	dynamique
192.168.1.101	**00-50-ba-6b-a4-5a**	dynamique

Machine B : Aucun changement

Machine C : Interface : 192.168.1.101 --- 0x2

Adresse Internet	Adresse physique	Type
192.168.1.1	00-0f-66-58-a9-2b	dynamique
192.168.1.2	00-50-bf-45-9a-94	dynamique
192.168.1.100	00-0c-6e-7e-af-76	dynamique

Donc comme vous le voyez sur la machine que nous avons empoisonnée, pour elle le routeur a la même adresse MAC que la machine 192.168.1.101. :p Donc à partir de là, la machine C n'a plus qu'à faire suivre au routeur les paquets, et personne n'a rien vu.

Méthode n° 2 : Dsniff

Et oui, il y a eu une version de dsniff adaptée sous windows.

Donc cette fois ci, il ne faut pas la dernière version de winpcap car cela ne va pas marcher du tout. Il vous faut la 2.3. Je vous laisse la prendre.

http://winpcap.mirror.ethereal.com/install/bin/

Ensuite, nous allons maintenant empoisonner sous DOS, il nous faut donc un outil pour cela.
Vous pouvez toujours tester arp-sk qui a été développé par des français.
Je vous conseille plutôt d'utiliser winarp_mim.

http://www.securiteinfo.com/download/wtk.zip

Donc là encore plus simple avec winarp, il ne vous suffit que d'indiquer les IP des deux machines entre lesquelles vous voulez intervenir.

Donc simple, on reprend nos IP indiquées plus haut.

1ère étape :

Sélection de l'interface : *dsniff –D*

```
Interface       Device          Description
----------------------------------------
1  \Device\Packet_NdisWanIp (Ndis
2 \Device\Packet_{881F994A-789D
3 \Device\Packet_NdisWanBh (NdisWan
```

2ème étape:

Lancement de winarp

⇨ *winarp_mim.exe -a 192.168.1.1 -b 192.168.1.100*

Il vous demande de sélectionner l'adaptateur. Et ensuite c'est bon. Vous devriez avoir un message du style :

```
Select the number of the adapter to open :
+ Sending 1 ARP REQUEST packet for each target

+ Sending ARP REPLY packets for each target

+ Start sending
```

Donc maintenant il ne suffit plus qu'à lancer Dsniff.

⇨ *Dsniff.exe –i 2*

Et magie!... Dsniff décrypte tout tout seul :

04/5/05 18:17:46 192.168.1.100 -> XP1 (ftp)
USER test
PASS test

Voila pour la démo, mais à savoir que la deuxième méthode est moins fiable si vous utilisez une vieille version de Dsniff.
Mais par contre, si vous avez un bon sniffer DOS qui décrypte les pass trames comme dsniff c bon ca marchera pareil.

En conclusion, il est certes difficile de faire une pratique en masse de l'attaque, mais sur une cible préalablement choisie, comme un serveur de messagerie ou un serveur d'authentification, on en voit vite l'utilité et les résultats. Maintenant, c'est à vous de tester, de voir et d'améliorer la chose.

Voila bonne chance, en espérant que ca n a pas été trop inintéressant pour vous.

Merci à Pro21 ;)

Jérome ATHIAS – http://www.athias.fr