Sniffing dans un réseau switché

-Une Recette Pour Hacker Un Switch Avec Ettercap et Ethereal

-Manu Garg
http://www.manugarg.com
manugarg at gmail dot com
-Version française:
Jérôme Athias

Enoncé du Problème-

Obtenir l’accès au switch principal de votre entreprise en utilisant une machine du même LAN.

Outils utilisés-

Ettercap, Ethereal

Techniques Utilisées-

Arp spoofing et Sniffing

Comment pouvons-nous arrivez à nos fins?

La plupart des administrateurs réseau utilisent telnet pour se connecter à un cisco.

Telnet est un protocole de données en-clair – ainsi, si vous pouvez sniffer les paquets vous pouvez savoir ce qu'une autre personne raconte au cisco.

Fastoche, je vais juste sniffer les paquets du cable et rentrer dans le switch.

Hey, je ne vois aucun trafic sur le cable. Pourquoi?

Vous êtes sur un réseau switché et les switchs ne font aucune faveur aux hackers. Ils ne transmettent les données qu'entre les machines qui dialoguent entre elles.

Mais c'est pas juste. Ils m'ont dit que j'étais sur ethernet. Ne sont-ils pas supposés utiliser CSMA/CD alors?

Ethernet a bien changé mon ptit. C'est 'ethernet switché' maintenant.

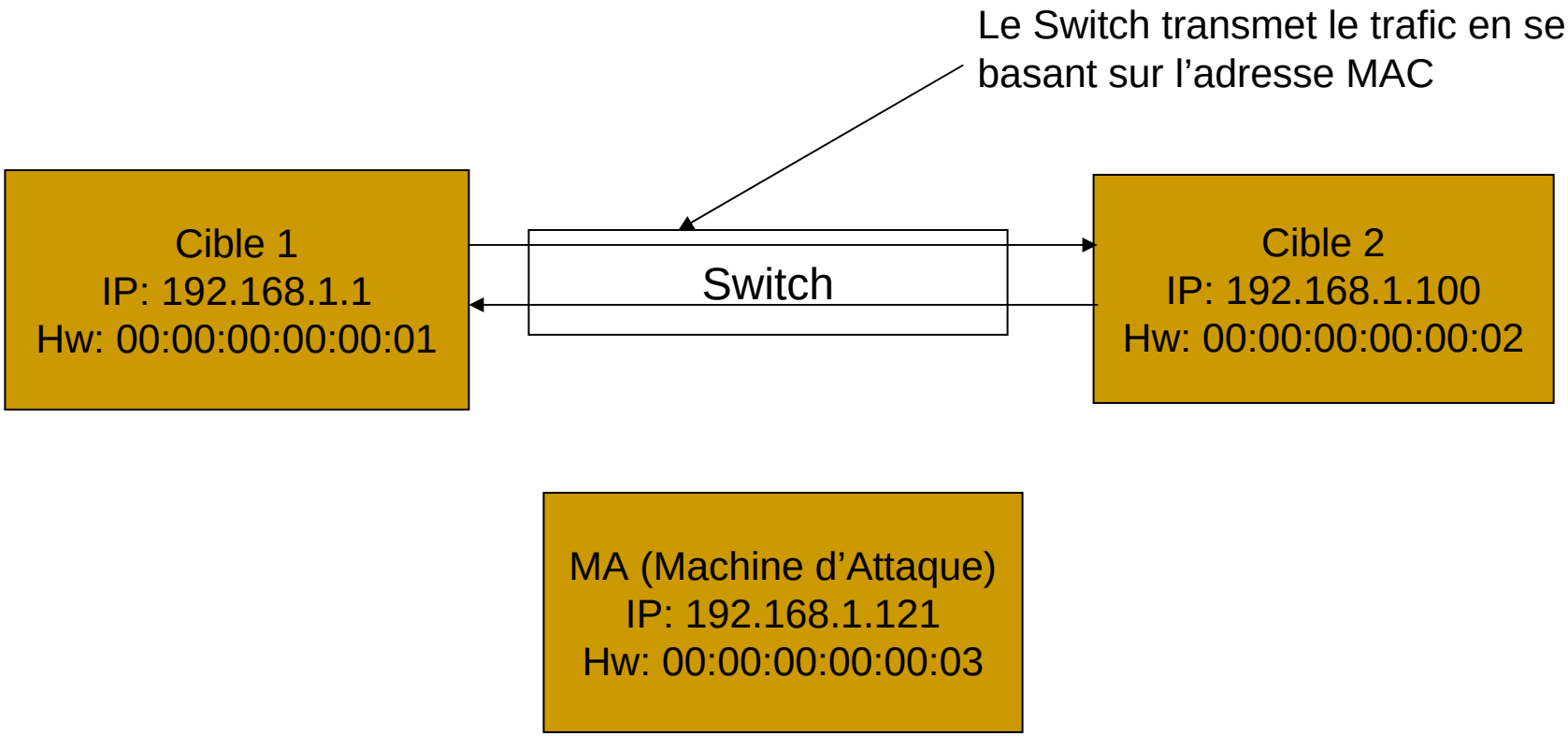
Attend! N'abandonne pas trop tôt. Nous les hackers ne sommes pas supposés être arrêtés par un switch. Pas vrai?

C'est vrai. Nos pères qui ont conçus les protocoles TCP/IP ne nous ont pas oubliés. Ils ont laissé un chemin invisible qui ne peut être vu que par leurs meilleurs étudiants.

Quel est donc ce chemin?

C'est le chemin du spoofing arp. En utilisant cette technique tu peux obliger tes machines cibls à envoyer des données à travers ta machine d'attaque, puis tu peux sniffer cela sur ta machine d'attaque.

SPOOFING ARP !!!
Comment ça marche?



Avant l'Attaque……..

Avant l'attaque, T1 et T2 ne parlent qu'entre elles. Voici la table arp de ces machines.

T1(192.168.1.1):

192.168.1.100	00:00:00:00:00:02
192.168.1.123	00:00:00:00:00:14

T2(192.168.1.100):

192.168.1.1	00:00:00:00:00:01
192.168.1.123	00:00:00:00:00:14

Le switch ne comprend que les adresses MAC et transmet les paquets aux machines correctes en se basant sur cette adresse MAC. C'est pour cela que si nous manipulons les tables arp (cela se nomme arp poisoning) sur T1 et T2 afin que l'adresse MAC cible dans tous les paquets soient échangée entre elles, et devienne l'adresse MAC de notre machine d'attaque. Et c'est gagné. Le switch transettra les paquets à la machine d'attaque.

Ainsi après l'attaque la table arp devrait ressembler à:

T1:

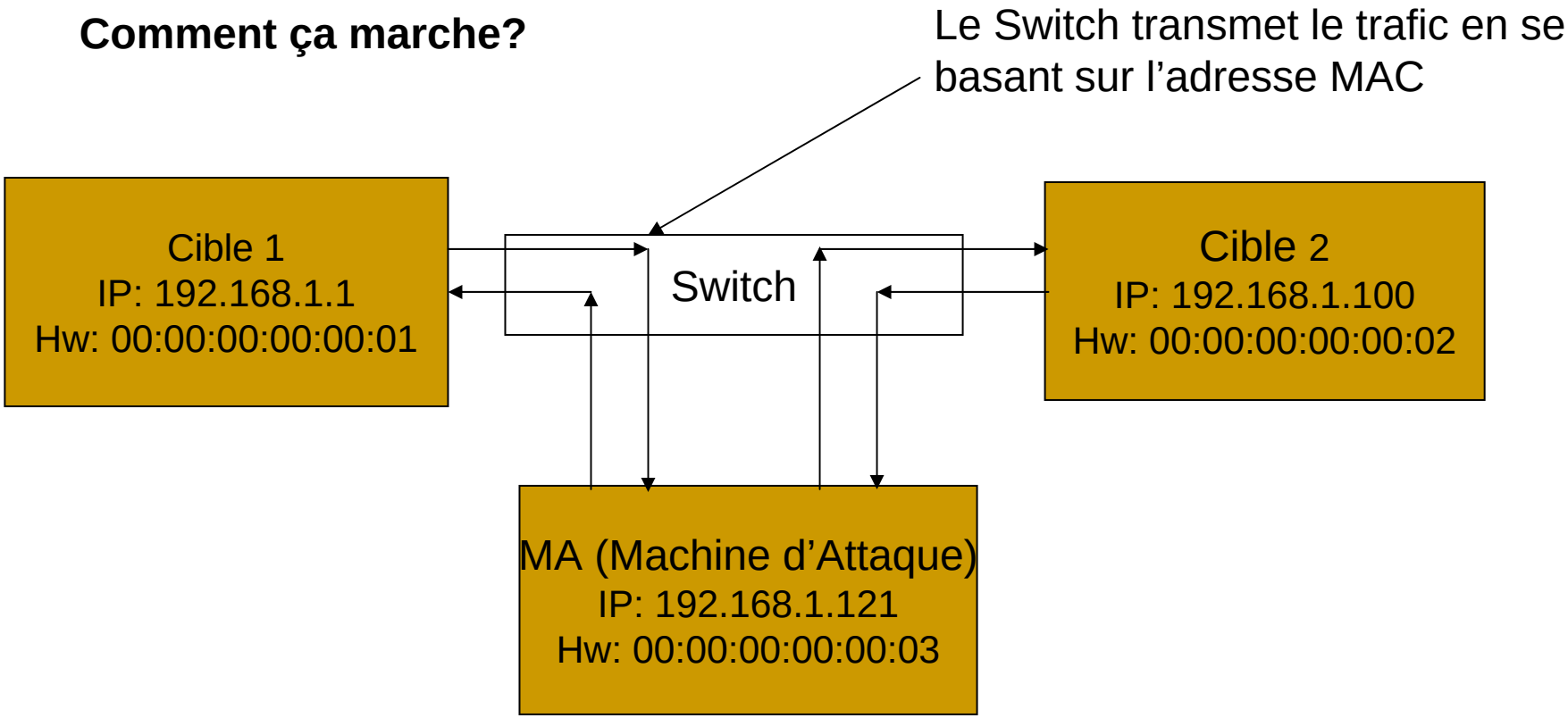
192.168.1.100	00:00:00:00:00:03
192.168.1.123	00:00:00:00:00:14

T2:

192.168.1.1	00:00:00:00:00:03
192.168.1.123	00:00:00:00:00:14

Où 00:00:00:00:00:03 est l'adresse MAC de la machine attaquante.

SPOOFING ARP !!!
Comment ça marche?



Après l'Attaque……..

Note: Ne pas oublier d'activer l'ip_forwarding sur la machine attaquante autrement vous empêcherez le trafic entre les 2 machines.

OK, maintenant vous savez ce qu'est l'ARP spoofing. Maintenant la plus grosse question – Comment allons-nous empoisonner la table ARP sur T1 et T2?

L'explication commence par une autre question. Comment les machines construisent cette table arp? Cette table est construite en utilisant le protocole arp. Le protocole ARP possède 2 types de paquets – ARP request et ARP reply.

Quant une machine (A) veux savoir l'adresse MAC d'une autre (B), elle envoie une requête ARP demandant "Qui a l'adresse IP B?". C'est un broadcast, envoyé par exemple à FF:FF:FF:FF:FF:FF. C'est recueilli par toutes les machines du LAN et seule la machine possédant l'adresse IP B va envoyer une réponse ARP. Elle est envoyée uniquement à la machine A. A enregistre cette adresse MAC dans sa table ARP.

Quelques indices... Oui, nous allons empoisonner la table ARP de T1 et T2 en envoyant des réponses ARP. La plupart des machines sont généreuses et respectent le paquet réponse ARP même quand il n'y a pas de requête particulière pour une IP.

Certaines machines, SunOS par exemple, ne créent une entrée ARP que si il y a eu une requête pour elle ou si cette IP est déjà dans la table arp. Nous pouvons les forcer à faire une requête pour une IP particulière en leur envoyant un paquet ICMP Echo depuis cette IP.

Ok. Donc tu veux que je créé ces réponses ARP moi-même et gère tout ca.

Non mon gars. Nous avons les bénédictions de nos camarades hackers.

Alberto Ornaghi (alias ALoR) et Marco Valleri (alias NaGA) de Milan ont créés un bel outil nommé **Ettercap** basé sur une belle librairie '**libnet**' de Mike.

Ettercap est assez versatile et un outil utile pour les attaques MITM comme l'ARP spoofing. Ettercap possède aussi des capacités de sniffing, mais je préfère l'utiliser seulement pour le spoofing. Pour le sniffing, je préfère **Ethereal**. La principale raison est l'utilisation du format pcap pour enregistrer les paquets par ethereal. Pcap est un format assez ancien et il y a beaucoup d'outils pour analyser les fichiers pcap.

Donc, utilise ettercap pour l'arp spoofing. Active l'ip forwarding dans le kernel pour maintenir lae connexion entre les victimes. Et commence à sniffer avec tethereal (interface texte ethereal).

Recette

Essayons de faire tout ce qu'on a vu. Voyons notre problème à nouveau

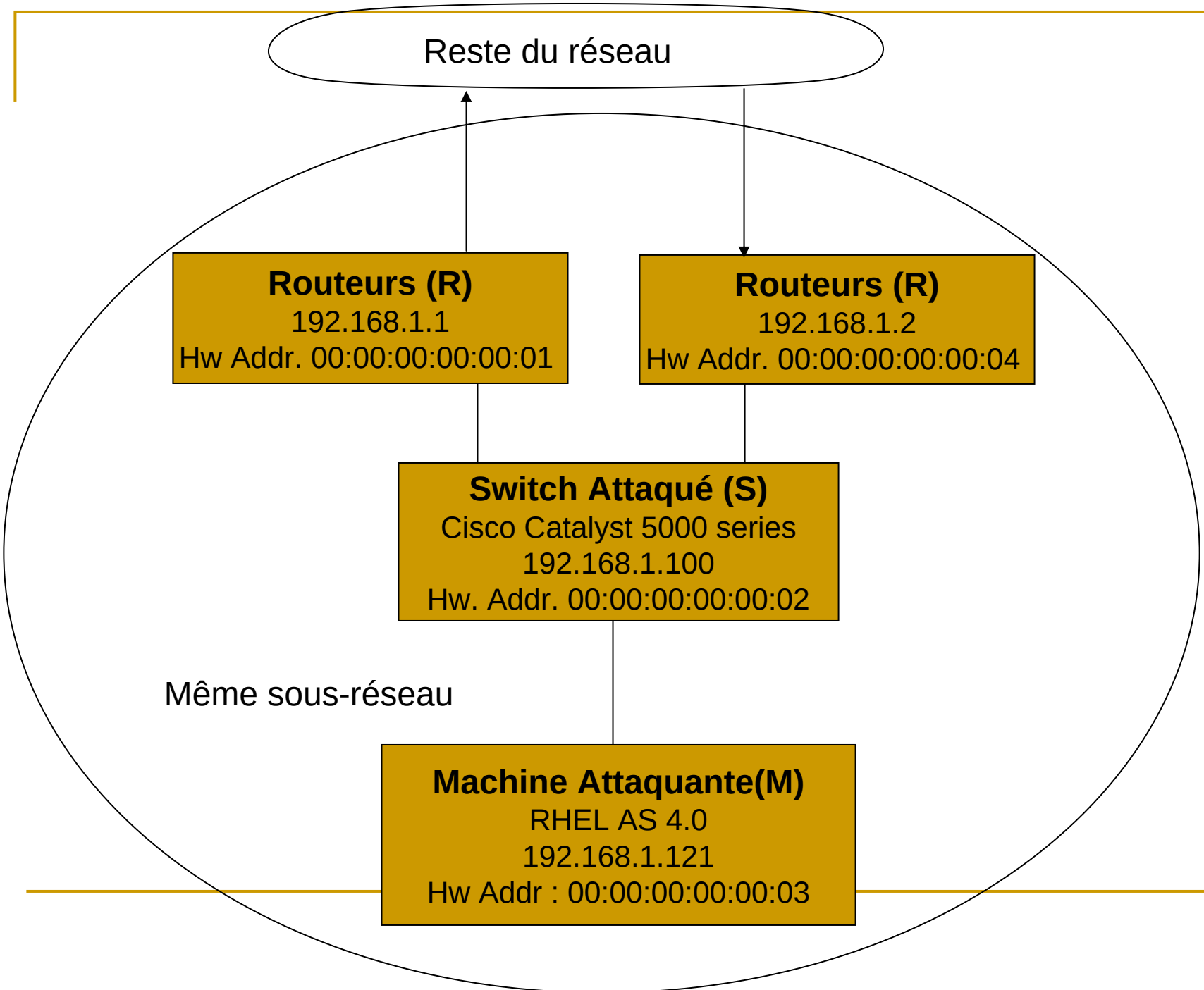
Nous voulons accèder au switch principal de notre entreprise. Cela va nous permettre de configurer les ports du switch à notre guise.

Première tâche, trouver l'IP du switch. Dans mon cas c'est 192.168.1.100. Vous pouvez utiliser la détection d'OS de Nmap pour la trouver.

Maintenant trouvons comment l'admin réseau communique avec le switch. Dans mon cas l'admin réseau n'est pas sur place. Il se connecte au switch par un WAN et les requêtes passent par la passerelle.

J'utilise une autre machine sur le même sous-réseau pour observer le trafic et trouver que tout le trafic entrant dans le sous-réseau arrive à travers le routeur 192.168.1.2 et tout le trafic sortant passe par le routeur 192.168.1.1.

Donc quand 192.168.101.34 s'authentifie à la consol du switche, les paquets sont routés à travers les routeurs 192.168.1.1 et 192.168.1.2.


Reste du réseau
Routeurs (R)
192.168.1.1
Hw Addr. 00:00:00:00:00:01
Routeurs (R)
192.168.1.2
Hw Addr. 00:00:00:00:00:04
Switch Attaqué (S)
Cisco Catalyst 5000 series
192.168.1.100
Hw. Addr. 00:00:00:00:00:02
Même sous-réseau
Machine Attaquante(M)
RHEL AS 4.0
192.168.1.121
Hw Addr : 00:00:00:00:00:03

Recette …

Comme vous pouvez le voir, je dois mettre ma machine d'attaque entre 192.168.1.1 et 192.168.1.100 pour marquer les paquets sortants et 192.168.1.2 – 192.168.1.100 pour marquer les paquets entrants.

Je dois donc dire au routeur 192.168.1.2 que 192.168.1.100 est en 00:00:00:00:00:03 qui est l'adresse MAC de la machine d'attaque. Et en même temps dire au switch par exemple 192.168.1.100 que 192.168.1.1 est en 00:00:00:00:00:03.

Avant d'inviter les paquets à votre machine, assurez-vous que vous avez le chemin pour qu'ils atteignent leur destination, par ex. N'oubliez pas d'activer ip forwarding. Sur Linux vous pouvez l'activer avec cette commande:

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

Lançons le spoofing….

Pouyr lancer l'arp spoofing avec ettercap:

ettercap -o -T -P repoison_arp -M arp:remote /192.168.1.100/ /192.168.1.1-2/

-o : que spoofing pas de sniffing.
-T : mode texte
-P repoison_arp

Demande de lancer le plugin repoison_arp. Il ré-empoisone la table arp régulièrement

-M arp:remote /192.168.1.100/ /192.168.1.1-2/

Demande de lancer une attaque MITMattack avec 192.168.1.100 dans le premier groupe cible et 192.168.1.1, 192.168.1.2 dans le second.

Je vous conseille de lancer ettercap dans un terminal.

J'ai utilisé "ettercap NG-0.7.2" disponible sur http://ettercap.sourceforge.com.

Lançons le Sniffing …

Utilisez la commande suivante pour lancer le sniffing et écrire les paquets dans un fichier:

 # tethereal -afilesize:100000 -w /tmp/cisco.pcap -f "host 192.168.1.100 and not arp and not icmp”

-afilesize:100000
limite la taille du fichier à 100Mo.
-w /tmp/cisco.pcap
écrit les paquets dans /tmp/cisco.pcap
-f “host 192.168.1.100 and not arp and not icmp**”**
est le filtre. Il demande de collecter les paquets provenant ou allant vers 192.168.1.100 et de ne pas collecter les paquets arp ou icmp.

Utilisez un peu de social engineering. Trouvez quand l’équipe réseau va travailler sur le switch ou une autre machine que vous voulez pénétrer. Lancez vos outils quand ils le feront.

Ensuite analysez le fichier de capture en l’ouvrant dans ethereal et suivez le flux telnet pour trouver le mot de passe.

C’est tout! ;-)

A *person* is smart. *People* are dumb, panicky, dangerous animals and you know it.
--Ed Solomon