Note technique

Address Resolution Protocol

- Rappels - Fonctionnement nominal

L'adresse IP est la donnée d'adressage couramment utilisée en programmation ou en configuration pour contacter une machine distance en passant par un réseau IP. Cependant cette adresse n'est pas suffisante : pour que deux machines puissent discuter sur un réseau local (ou qu'une machine puisse communiquer avec le routeur chargé de relayer les paquets) il faut une adresse de niveau 2, l'adresse MAC. L'ARP est un protocole qui se charge de trouver la correspondance IP_{dest} <-> MAC_{dest} (ou $MAC_{prochain\_routeur}$) de façon dynamique et automatique. Pour gagner en performance, les correspondances IP-MAC sont conservées localement par chaque machine dans une mémoire cache : le cache ARP.

Exemple : Remplissage du cache ARP de la machine attaquant

1) Au démarrage le cache est vide
2) La machine de l'attaquant ping l'IP du serveur et a donc besoin de connaître l'adresse MAC associée
3) Nouvel affichage de la table ARP après le ping cette fois
4) Le cache n'est plus vide et contient la correspondance IP <-> MAC (ici 192.168.2.1 <-> 08:00:27:8f:a6:b1)

```
dgsi@dgsi-VirtualBox:~$ arp -a 1
dgsi@dgsi-VirtualBox:~$ ping 192.168.2.1  2
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.454 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.236 ms
^C
--- 192.168.2.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.236/0.345/0.454/0.109 ms
dgsi@dgsi-VirtualBox:~$ arp -a  3
? (192.168.2.1) à 08:00:27:8f:a6:b1 [ether] sur eth0 4
dgsi@dgsi-VirtualBox:~$
```

De façon plus détaillée, deux types de trame ARP (encapsulées ensuite dans un protocole de niveau 2) existent :

- Les trames who-has : trames de requête envoyées à toutes les machines du réseau local (en broadcast) par la machine souhaitant connaitre la MAC associée à une IP.

Damien CASSU & Laura GRABOT
INSA TOULOUSE - TLS-SEC
2016/2017

ARP - who-has			
Adresse MAC émetteur	Adresse IP de l'émetteur	FF:FF:FF:FF:FF:FF Adresse MAC broadcast (Ce que l'on cherche)	Adresse IP du destinataire (IP dont la MAC est inconnue et recherchée)

- Les trames is-at : trames de réponse envoyées à la machine demandeuse (en unicast) en réponse à une requête who-has par la machine qui possède l'IP cherchée.

ARP - is-at			
Adresse MAC émetteur (L'adresse MAC cherchée)	Adresse IP de l'émetteur	Adresse MAC du destinataire	Adresse IP du destinataire (IP de la machine ayant émis le who-has)

Pour mettre à jour le cache ARP d'une machine plusieurs méthodes sont possibles :

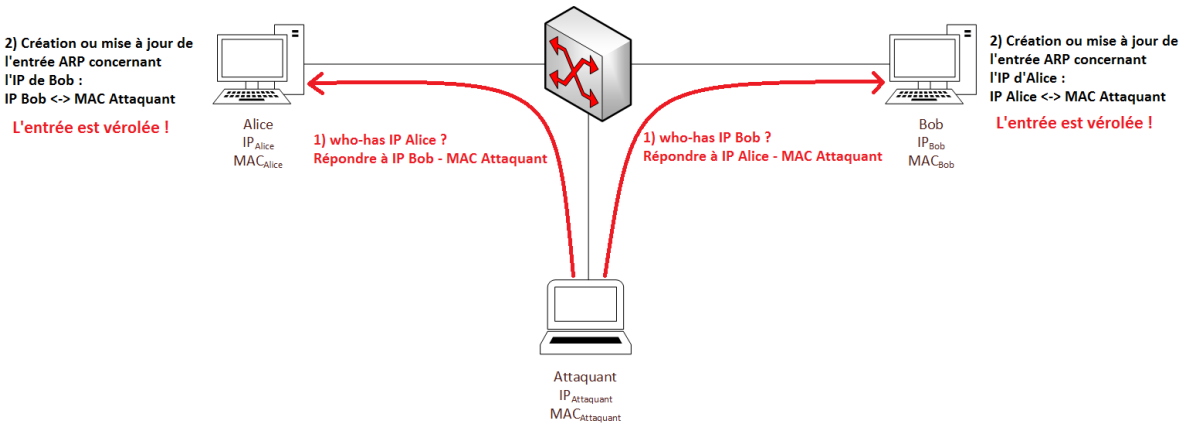
- Enregistrement du lien IP - MAC émetteur lors de la réception d'un is-at (en réponse à un who-has)
- Enregistrement liens IP - MAC émetteur lors de la réception d'un who-has
- Enregistrement du lien IP - MAC émetteur lors de la réception d'un is-at qui confirme une entrée déjà connue dans la table (même si le is-at ne répond pas à un who-has)
- Effacement du lien IP - MAC d'une entrée qui n'a pas été confirmée depuis longtemps

• ARP Poisoning : Un Man In The Middle Plug and Play

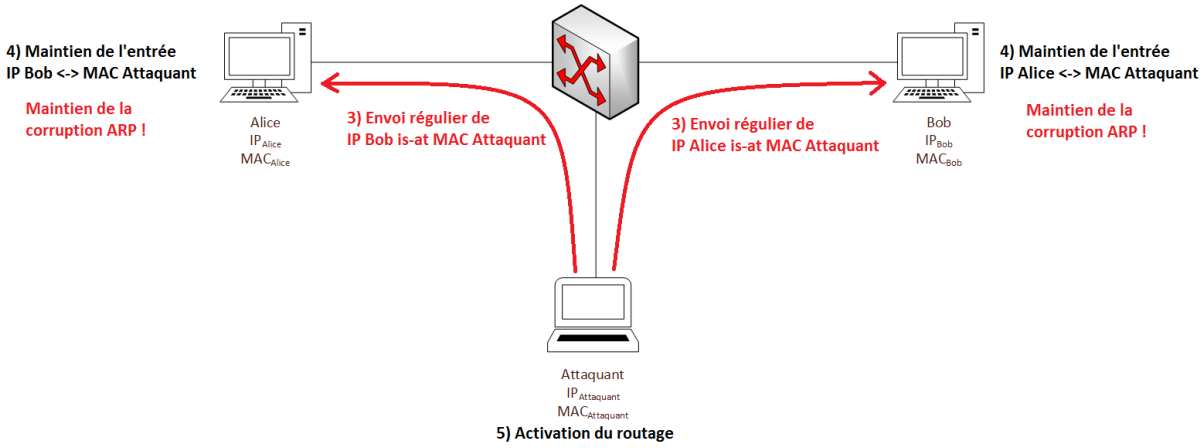
Le principe de l'ARP Poisoning est très simple : abuser des règles de mise à jour du cache ARP afin d'insérer de fausses entrées dans la table ARP d'une machine pour détourner les flux réseau qu'elle émet. En attaquant simultanément deux machines qui communiquent entre-elles via ce principe il est possible d'insérer une machine entre les deux interlocuteurs. Ainsi un attaquant peut écouter/modifier/stopper le trafic : c'est la position d'Homme du milieu (Man In The Middle en anglais).

Plusieurs étapes sont nécessaires pour mettre en place cette attaque, elles sont résumées dans les schémas ci-après :

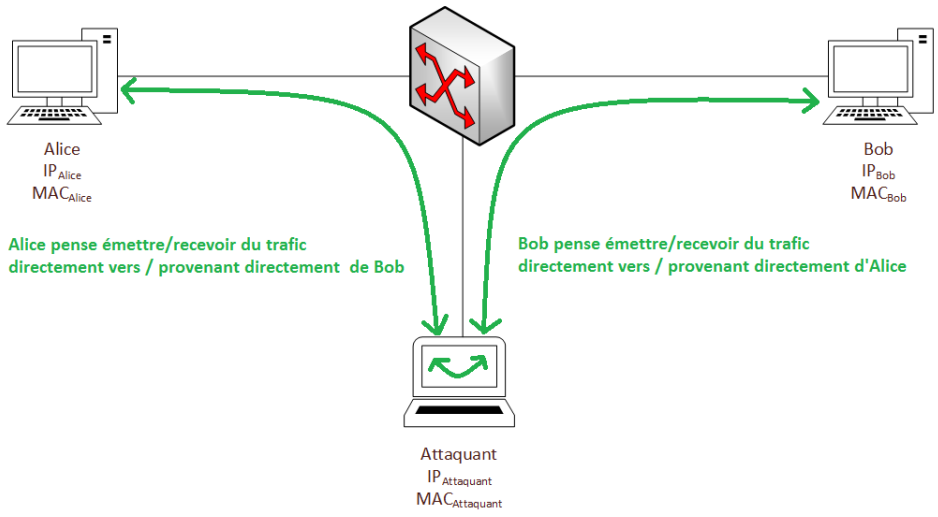
1) La compromission initiale des caches ARP des machines cibles :



2) Maintien de la corruption



3) L'exploitation



L'attaquant voit tout le trafic entre Alice et Bob et peut le modifier ou le bloquer avant de le router (l'attaquant possède une bonne table ARP !)

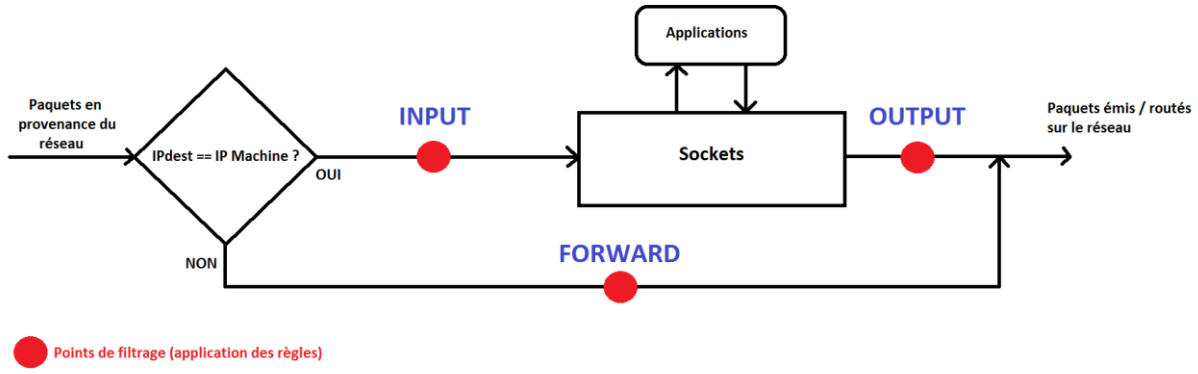
Damien CASSU & Laura GRABOT
INSA TOULOUSE - TLS-SEC
2016/2017

La base d'iptables et de la table filter

Iptables est utilisé pour l'inspection et la modification de paquets réseaux au moyen de règles de filtrage dans le noyau Linux. Ces règles de filtrage sont regroupées dans des tables en fonction de leur objectif : la table *nat* contiendra les règles relatives au NAT, la table *mangle* les stratégies de qualité de service par exemple… Dans la suite nous nous intéresserons à la table *filter* qui contient les règles de filtrage des paquets : c'est le firewall intégré de Linux.

Entrer une règle dans une table ne suffit pas. Il faut en effet préciser le moment de son application. Cette précision se fait au moyen de chaînes, il en existe trois dans la table *filter* :

- INPUT : Désigne les paquets destinés (au niveau IP) à la machine locale
- OUTPUT : Désigne les paquets émis par la machine locale
- FORWARD : Désigne les paquets transitant par la machine locale (si le routage est activé)



Enfin chaque règle doit préciser sa cible c'est-à-dire la décision à appliquer si un paquet correspond à la règle. La cible ACCEPT laisse passer le paquet, la cible DROP élimine le paquet et la cible REJECT élimine le paquet puis notifie l'émetteur de la suppression.

Le format général d'une règle iptables est donc le suivant :

iptables -t nom_table -A nom_chaine caracteristiques_paquet_a_filter -j cible

-t : nom de la table
-A : ajouter une règle dans la chaine nom_chaine
-j : nom de la cible

Caractéristiques des paquets :
-i : interface d'entrée
-s : source (IP ou réseau IP si le masque est précisé)
-d : destination (IP ou réseau IP si le masque est précisé)
-p : le protocole (tcp, udp, icmp…)
--dport : port de destination
--sport : port source

Quelques exemples :

iptables -t filter -A FORWARD -i eth1 -s 192.168.1.0/24 -d 192.168.2.2 -p tcp --dport 23 -j ACCEPT

- Les paquets routés par la machine rentrant par l'interface eth1, provenant du réseau IP 192.168.1.0/24 à destination de la machine 192.168.2.2 sur le port TCP 23 sont acceptés.

iptables -t filter -A INPUT -p udp --dport 80 -j DROP

- Tous les paquets à destination du port udp 80 de la machine locale sont rejetés.

iptables -t filter -L

- Affiche les règles courantes de la table *filter*

iptables -t filter -F

- Supprime toutes les règles de toutes les chaînes de la table *filter*