ARP Spoofing
ARP Cache Poisoning

Comprendre

Exploiter

Sécuriser

Théorie

Toute carte réseau dispose d'une adresse unique, appelée adresse MAC (Media Access Control) ou adresse physique que les ordinateurs utilisent pour communiquer.

Une adresse physique est codée sur 6 octets.

Ex. : 00:11:22:33:44:55

Windows : ipconfig /all

Unix-based : ifconfig

En pratique, en informatique, on utilise le protocole IP, beaucoup plus ergonomique, et permettant de plus grandes fonctionnalités.

Depuis l'arrivée des switchs, il est nécessaire de pouvoir traduire une adresse IP en adresse MAC. Pour cela, le protocole ARP (Address Resolution Protocol) a été créé.

MAC : nom et prénom

IP : numéro de téléphone

ARP : annuaire inversé

Différence Hub / Switch

Echanges

Je veux parler à 192.168.0.1.

Mais qui est 192.168.0.1 ?

Ah, on me répond que c'est 00:11:22:33:44:55 !

Cool, je lui envoie ma question.

Je vais noter sa MAC pour ne pas l'oublier.

Chaque fois qu'on veut envoyer un courrier à quelqu'un à partir de son numéro de téléphone, on doit récupérer son nom et son adresse via un annuaire inversé.

Windows et Linux : arp –a

Mise en pratique : Wireshark

Filtre Wireshark : arp

Ping 192.168.0.1

ARP Request : Who has 192.168.0.1 ?

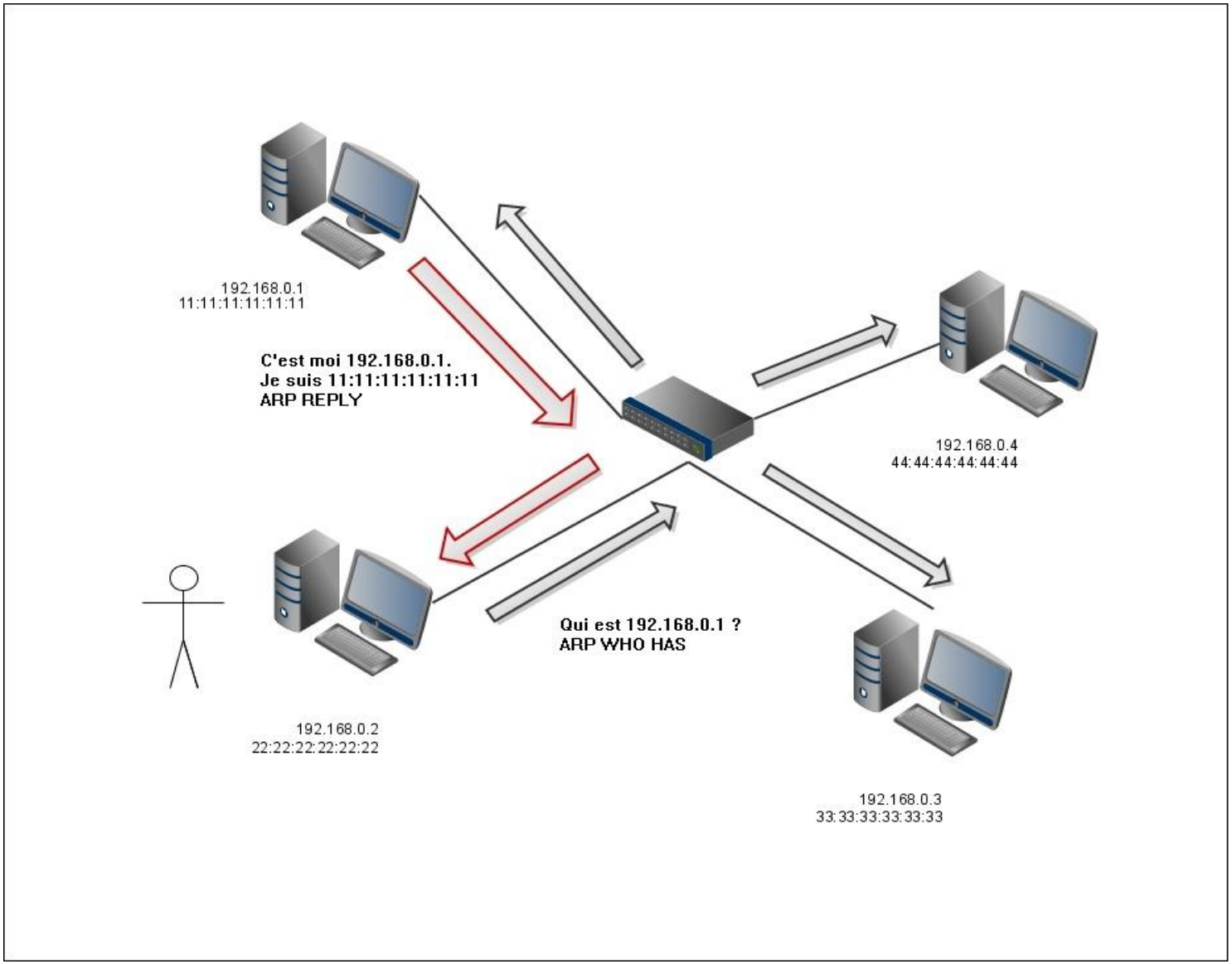
ARP Reply : 192.168.0.1 is at 00:11:22:33:44:55

/* Envoi des paquets réseau du ping */

/* Mise en cache de l'adresse MAC */

Chaque fois qu'on veut envoyer des paquets réseau à une machine à partir de son adresse IP, on doit récupérer son adresse MAC via ARP.

C'est toi le schéma



Sécurité

ARP n'a pas été pensé pour la sécurité. En effet, lorsqu'un ordinateur a mis en cache une adresse MAC, il ne la demande plus pour une durée limitée.

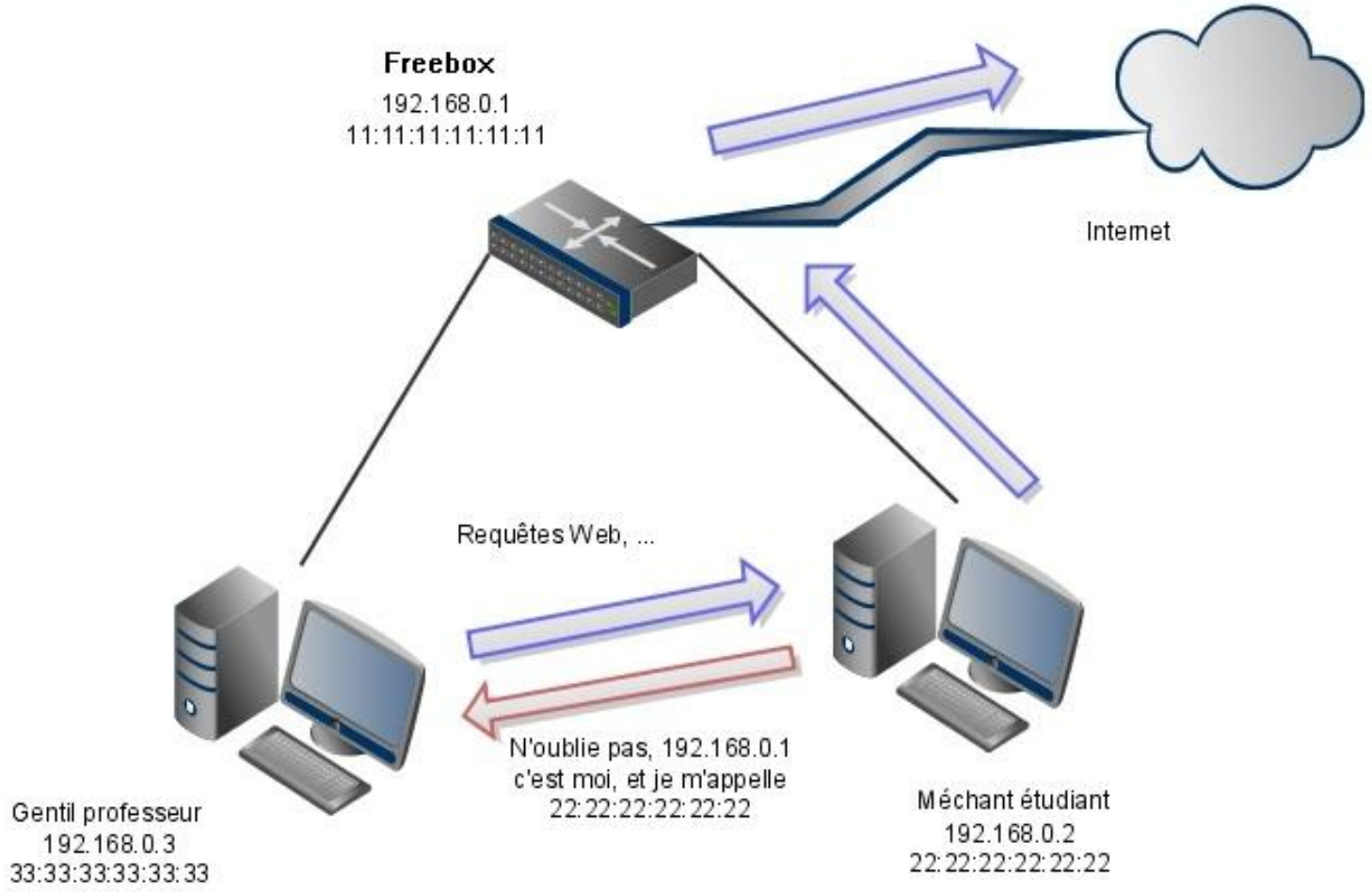
Le problème, c'est que lorsqu'un ordinateur reçoit un ARP Reply, il met en cache sans se poser de question, **même s'il n'a strictement**

.

Conséquence : On peut dire à n'importe quel ordinateur sur le réseau qu'une certaine adresse IP correspond à une certaine adresse MAC.

- Réponses ARP non vérifiées
- Empoisonnement de cache
- Détournement des paquets
- ☹

C'est toi l'autre schéma



Exploitation

Man-in-the-middle :

On se fait passer pour la passerelle.

nemesis arp -r -v -d etho -S ipSrc -D ipDst -h macSrc -m macDst

Résultat, ipDst va recevoir :

ARP-Reply : ipSrc is macSrc.

Il faut le faire en boucle !

Equivalent dsniff

arpspoof -i etho -t ipDst ipSrc

Pour Ettercap, voir le lien

http://wiki.backtrack-fr.net/index.php/Ettercap-ng

Nemesis : la base

Dsniff : le couteau suisse

Ettercap : le marteau

☺

Combler la faille

Plusieurs parades peu efficaces existent.

On peut mettre en cache des entrées ARP statiques au démarrage de la machine. Celle-ci ignorera alors toutes les réponses ARP.

On peut désactiver ARP. Ceci désactivera également IP.

On peut installer un système de monitoring qui détecte et avertit lors d'une réponse ARP non demandée.

Parfois peu fiable, et dépend de l'utilisateur

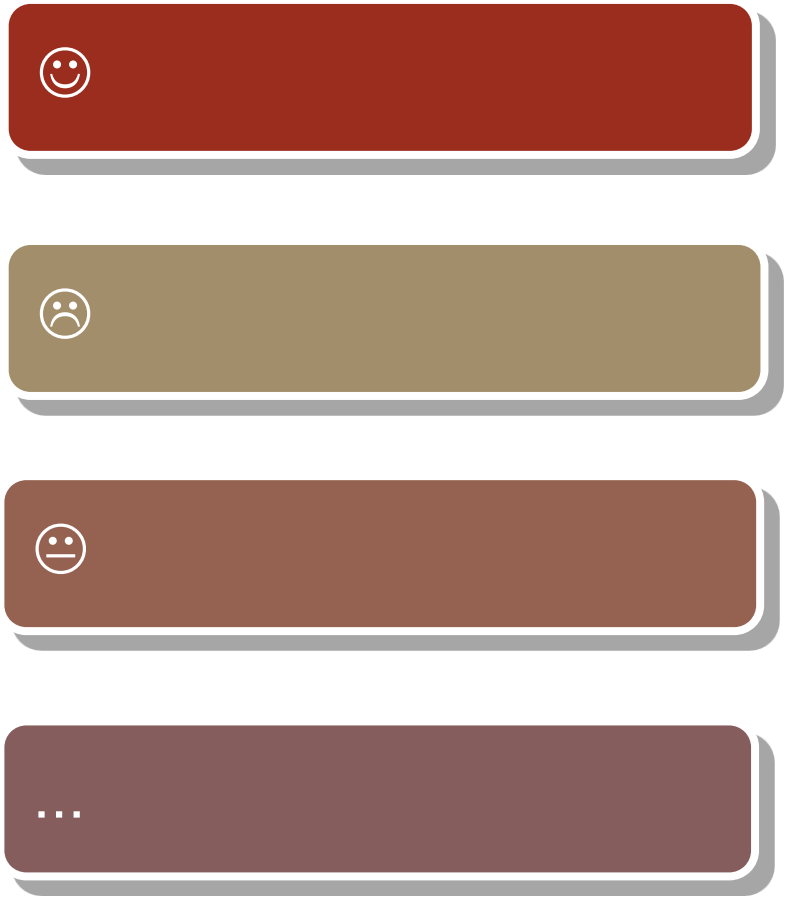
Cache statique

Désactiver ARP

Monitoring

😐

Références



ARP Spoofing
ARP Cache Poisoning

Comprendre

Exploiter

Sécuriser