

Le smart-spoofing IP

ou la sécurité relative du filtrage IP source

Althes (<http://www.althes.fr>)

Révision 1 – Octobre 2002

Laurent Licour (llicour@althes.fr)

Vincent Royer (vroyer@althes.fr)

Introduction

Cet article a pour but de présenter une nouvelle technique de spoofing IP réduisant de manière importante la confiance que l'on peut avoir dans les solutions de sécurité basées sur le filtrage IP source. Cet article ne présente pas une nouvelle vulnérabilité, le concept du spoofing IP existant depuis longtemps. Toutefois, la technique employée, basée sur de l'ARP cache poisoning associée à de la translation d'adresse, simplifie très nettement sa mise en oeuvre, rendant de ce fait les solutions de filtrage IP source incertaines, voire inutiles.

L'ARP cache poisoning

Cette technique vise à modifier le routage au niveau 2, et permet de jouer l'attaque de l'intercepteur (Man In The Middle) sur un LAN. Le protocole ARP est le protocole assurant la correspondance sur un LAN entre les adresses de niveau 2 (adresses Ethernet) et les adresses de niveau 3 (adresses IP). En modifiant les associations, il est possible de faire croire à une machine que l'adresse IP de son correspondant se trouve en fait à l'adresse Ethernet d'une machine pirate.

Le protocole ARP (RFC 826) a été créé sans prendre en compte les aspects d'authentification des machines, de sorte que n'importe quelle machine sur un réseau est capable de s'annoncer comme propriétaire d'une adresse IP.

L'utilisation d'un protocole non sécurisé, associé à de mauvaises implémentations dans les systèmes d'exploitation, fait qu'à ce jour, quasiment tous les systèmes sont vulnérables à de l'ARP cache poisoning.

Bien que la RFC définisse le format des messages, il est possible de les envoyer sous de multiples formes. Ainsi, une trame ARP peut être codée de 8 façons différentes (broadcast ou unicast, whois ou reply, gratuitous ou pas). Selon le résultat que l'on veut obtenir (création d'une entrée en table, mise à jour), il est possible d'employer ou de combiner ces messages. Des tests menés sur de nombreux OS (Unix, Linux, BSD, Windows, IOS, IPSO...) montrent qu'il existe toujours une forme de requête permettant de les "cache poisoner".

Sur certains OS, Windows 9x, NT et 2000, il est même possible de modifier des entrées définies en statique. Ce ne sont pas les seuls. Des tests menés sur un Solaris 8 ont permis d'identifier que cet OS était également vulnérable à de l'ARP cache poisoning sur des entrées définies en statique en utilisant des requêtes de type gratuitous.

Les attaques mettant en oeuvre le protocole ARP sont nombreuses et vont de l'écoute réseau sur un réseau switché au déni de service, en passant par le spoofing et l'attaque de l'intercepteur (<http://www.arp-sk.org/doc/arp.pdf>)

Le filtrage IP

Le filtrage IP consiste en la mise en place de règles de contrôle d'accès portant sur l'adresse IP source des paquets entrant dans un équipement ou une application, qui a alors la possibilité de comparer l'adresse IP source du paquet entrant avec une liste d'adresses autorisées (adresses unitaires ou réseau tout entier). Le paquet IP sera accepté seulement si l'adresse fait partie de cette liste. Dans le cas contraire, le paquet sera rejeté (émission d'un refus ou poubellisation). A noter que d'autres contrôles ou traitements sur le paquet peuvent être appliqués avant de l'accepter définitivement, mais ceci est hors de ce propos.

Le concept de filtrage IP est également à la base de la notion de cloisonnement des réseaux : telle machine ne peut communiquer qu'avec telle autre machine.

Le filtrage IP est donc un composant de sécurité de base, simple et performant, que l'on retrouve dans nombre d'équipements et de logiciels :

- Firewall avec utilisation de règles intégrant l'IP source
- Routeurs avec Access List (ACL)
- Filtres intégrés dans les piles IP des systèmes d'exploitation
- TCP Wrapper sur les systèmes unix
- Filtrage IP effectué au sein des applications afin de limiter les communications entre deux machines (transfert de zone pour un serveur DNS, relais SMTP, serveur Web...)
- ...

Le spoofing IP

La méthode du spoofing d'IP source permet de contourner ce filtrage. Elle existe depuis longtemps et certaines histoires célèbres font état de cette technique.

Le concept est simple, les techniques pour y parvenir plus complexes. Il suffit d'usurper l'adresse IP d'une machine autorisée pour profiter de ses privilèges.

Pour y parvenir, seules les techniques basées sur la construction manuelle de paquets IP étaient jusqu'alors connues. Jumelées à de l'écoute réseau, cela permettait au mieux de créer une pseudo communication avec la machine visée. La pile IP du système d'exploitation de la machine pirate était dans ce cas inutilisée. Des outils comme *dsniff* ou *ettercap* mettent en oeuvre ce principe.

Les mises en oeuvre de cette méthode sont les suivantes :

- Construction de paquets en aveugle. Les paquets sont construits et envoyés sur le réseau, sans savoir ce que l'autre machine va répondre. En TCP, cela nécessite de prédire les numéros de séquence échangés.
- Hijacking de connexion TCP. Il s'agit d'attendre l'établissement d'une connexion par une source autorisée, puis de la voler. Cela nécessite d'être sur le chemin réseau, d'écouter le trafic et de s'insérer dans la connexion. Cette méthode permet de profiter des privilèges de la source, le hijacking étant effectué après la phase d'authentification.
- Ecoute du réseau et construction de paquets. Il s'agit d'une méthode similaire au hijacking, mais en créant une nouvelle connexion. Les paquets sont écrits et lus sur le réseau sans passer par la pile IP de la machine, permettant de spoofer l'adresse de la source. Restera à jouer la phase d'authentification.

Cf l'article "IP-spoofing Demystified" (<http://www.phrack.com/phrack/48/P48-14>)

Les méthodes présentées ici sont possibles, mais difficilement exploitables, pour cause d'absence d'outillage évolué.

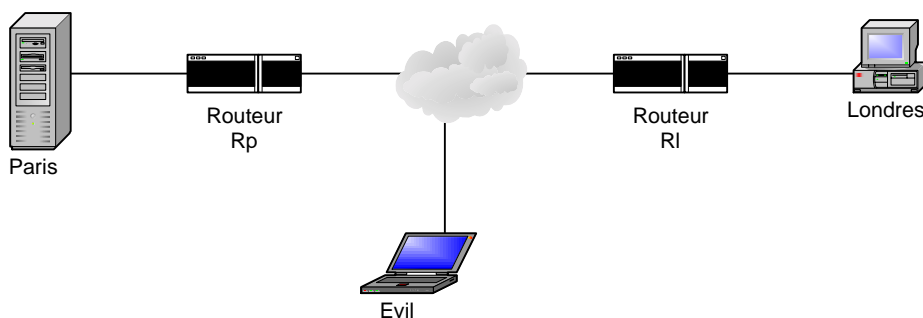
Le smart-spoofing IP

La technique présentée ici abandonne les principes d'écoute du réseau et de forgeage de paquets. Elle permet de spoofer une adresse IP de façon "propre", en permettant à n'importe quelle application exécutée de "profiter" de cette nouvelle identité. Cette méthode a été nommée le "smart-spoofing IP".

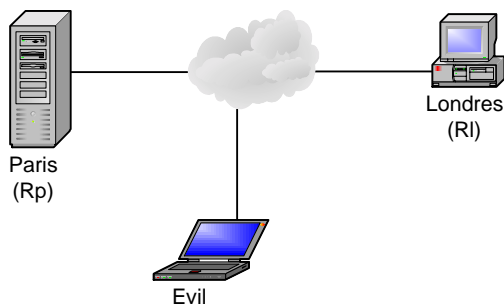
Dans la suite de l'article, nous appellerons "Paris" la machine sur laquelle le filtrage IP est effectué, "Londres" la machine autorisée à se connecter sur Paris et "Evil" la machine opérant le smart-spoofing IP. Evil se doit d'être sur le chemin réseau entre Paris et Londres.

Deux routeurs Rp et RI sont positionnés. Ils correspondent aux "next hops" permettant à Evil de joindre respectivement Paris et Londres. Selon que Evil se situe dans le même réseau que Paris ou Londres, Rp et RI pourront se confondre avec Paris ou Londres.

Les explications suivantes continueront à identifier Rp et RI afin de traiter le cas général.



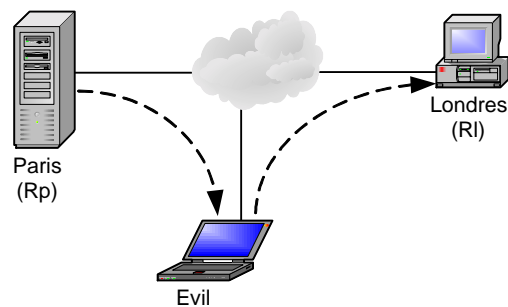
ou



Le smart-spoofing IP consiste à opérer dans un premier temps un ARP cache poisoning de Rp afin d'insérer dans la chaîne de routage niveau 2 des paquets circulant entre Londres et Paris. Il est nécessaire d'activer le routage sur Evil afin que Londres continue à recevoir les paquets qui lui sont destinés. Dans le cas où Evil se situe sur le même LAN que Paris, un blocage des ICMP redirect sur Evil empêchera de laisser trop de traces permettant une détection de l'attaque. Les ICMP redirect ne constituent toutefois pas une gêne fonctionnelle car le routage a seulement été détourné au niveau 2 (les ICMP redirect agissant au niveau 3).

Enfin, il est nécessaire d'empêcher RI d'effectuer des requêtes ARP en broadcast, vers d'autres machines. Ces broadcast auraient l'inconvénient de repositionner la véritable adresse ARP de RI dans le cache de Rp. Pour ce faire, on remplit le cache ARP de RI avec l'ensemble des adresses MAC pouvant se trouver sur le réseau.

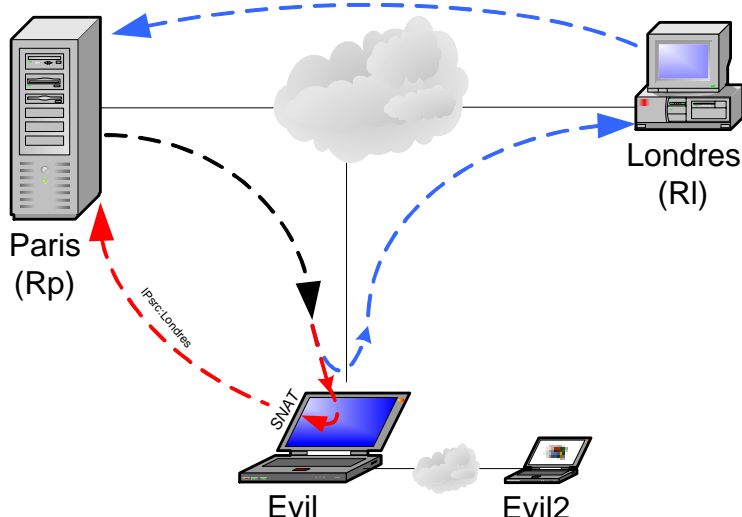
Il est à noter que seul l'ARP cache poisoning de Rp est nécessaire.



Une fois ceci réalisé, l'ensemble des paquets circulant de Paris vers Londres passera par Evil.

La deuxième étape consiste à mettre en place un mécanisme de translation d'adresse source (SNAT) sur Evil, de sorte que les connexions créées vers Paris le soit avec l'adresse source de Londres.

Les paquets en retour seront naturellement traités par le processus de SNAT et renvoyés dans la pile IP de Evil.



La dernière étape consiste à utiliser le logiciel client de l'application protégée par le filtrage IP source (telnet, browser, ftp, console d'administration...) afin d'accéder à Paris en se faisant passer pour Londres.

Le logiciel client peut être exécuté sur Evil lui-même ou sur Evil2, une machine sous Windows (pour profiter des GUI spécifiques à cet OS) située dans un réseau juste derrière Evil.

Ce concept a été mis en oeuvre sur une plate forme Linux 7.3 de base, équipée de l'outil *arp-sk* (<http://www.arp-sk.org>) pour opérer l'ARP cache poisoning ainsi que de *iptables* pour la gestion SNAT. L'outil *arp-fillup* est utilisé afin de saturer le cache ARP de RI. L'utilisation de VMWare (<http://www.vmware.com>) permet de créer sur Evil une machine Evil2 sous Windows, ainsi que le réseau dédié associé.

Cette méthode n'apporte rien de techniquement nouveau. Le spoofing IP était déjà réalisable auparavant. Les risques pour les systèmes étaient existants. La nouveauté réside ici dans la simplicité de sa mise en oeuvre, dans la souplesse d'utilisation qui en suit (utilisation d'une simple application cliente, telle un browser), et dans le nombre d'équipements contre qui cette

méthode peut être menée. L'utilisation du filtrage IP devient quasiment inutile compte tenu de la facilité de le contourner.

Un certain nombre de réflexions s'en suit, pouvant remettre en question quelques certitudes dans le domaine de la sécurité. Notamment la réponse à cette question :

Que vaut réellement une règle de filtrage IP source positionnée sur Paris (qu'il soit un firewall, un routeur, une application...) et n'autorisant que l'adresse IP de Londres ?

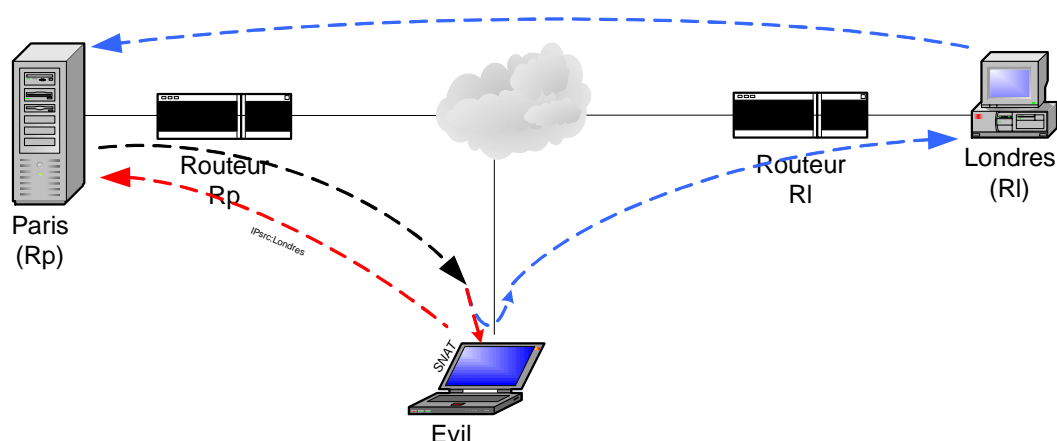
Globalement, il faut considérer que la règle en question correspond à autoriser toutes les machines des réseaux situés sur le chemin entre Paris et Londres.

Ces machines ont en effet la possibilité d'effectuer un ARP cache poisoning de leur Rp, et donc de se faire passer pour Londres.

Ce n'est sans doute pas ce que l'on vous avait expliqué lors de votre formation sur la création de règles sur votre firewall.

Ceci est d'autant plus inquiétant que les réseaux traversés ne sont pas tous sous votre contrôle (réseau du partenaire, réseau de l'opérateur...)

Il est à noter certaines techniques (par exemple le spoofing DNS) permettent de s'insérer sur un chemin réseau (modification du routage au niveau 3 cette fois ci)



Quelques cas de figure

- Votre architecture d'accès à Internet impose le passage par un proxy HTTP incluant des fonctions d'authentification, de filtrage d'URL, de contrôle de contenu, de contrôle anti-virus et de traçabilité.

Ce proxy est situé sur le réseau interne. Il est le seul à être autorisé à passer le firewall.

Pensez-vous encore maintenant que cet investissement en matière de sécurité soit le garant de votre politique de sécurité, alors qu'il est si facile de le contourner ?

Il est essentiel de reconsidérer son positionnement dans votre réseau (le placer dans une nouvelle DMZ par exemple). Le positionnement de telles passerelles ne devrait plus être préconisé sur le réseau interne.

- Le réseau de votre entreprise a été cloisonné pour des raisons de sécurité (présence de serveurs critiques, de bases de données sensibles, interconnexion avec un partenaire, client ou fournisseur...), de performance ou fonctionnelles (réseau de production, réseau de développement). Des routeurs équipés d'ACL "qui vont bien" permettent, selon vous, d'assurer la sécurité car ils contrôlent les flux échangés.

- Les équipements (routeurs, switches, firewalls, appliance...) de votre réseau sont administrables via telnet et HTTP. Des ACLs limitent l'accès depuis une machine bien précise située dans votre bureau, seule autorisée à s'y connecter.
En êtes-vous si sûr ? La récupération des mots de passe d'accès relève de la même technique (ARP cache poisoning). Dès lors, que reste-t-il à votre routeur pour se protéger si à la fois l'authentification et le filtrage IP sont tombés ?
- Il en va de même des applications protégées par un TCP Wrapper (SSH, Telnet, FTP...), d'un serveur Web possédant une arborescence spécifique, accessible uniquement depuis certaines adresses IP, d'un serveur DNS maître, n'autorisant le transfert de zone que depuis un serveur secondaire bien précis, d'un serveur de mail n'autorisant le flux incoming qu'en provenance d'un relais bien précis, du processus d'anti-relaying d'un relais de mails basé sur une résolution inverse de l'adresse IP source.

Il doit encore être possible de trouver bon nombre d'autres exemples plus inquiétants les uns que les autres.

Comment se protéger

Le filtrage IP n'a jamais été considéré comme un élément permettant de sécuriser un système. Tout au plus est-il un frein. Ce document a montré que ce frein est en fait virtuel dans bien des situations. Il n'est d'ailleurs jamais (est-ce bien sûr ?) considéré comme unique protection d'accès à un équipement ou une ressource. L'accès nécessite généralement une phase d'authentification (par mot de passe...).

Le problème posé ici est issu de l'aspect non sécurisé de la couche niveau 2 du réseau. Comme celui-ci n'a pas intégré lors de sa conception (RFC 826) de mécanisme d'authentification forte des extrémités, il est nécessaire de remonter cette sécurité dans les couches supérieures. L'authentification forte des extrémités doit donc être effectuée au niveau 3, ou au niveau applicatif.

L'utilisation systématique de protocoles comme IPSec, SSL, SSH et plus généralement les VPNs est donc le seul moyen efficace de protection contre le spoofing IP. Par ailleurs, le chiffrement induit par l'utilisation de ces technologies permet de supprimer le problème lié à l'écoute sur le réseau. Encore faut-il que cette cryptographie soit mise en oeuvre correctement, mais ceci est un autre débat.

Par ailleurs, il est également possible de renforcer la sécurité en empêchant l'ARP cache poisoning. Le seul moyen d'y parvenir est de travailler à partir d'un référentiel de ce que devraient être les associations adresses IP/MAC. Il s'agit en général de mesures lourdes à administrer, et dont l'efficacité est toute relative. Elle n'a comme portée que le segment réseau du LAN. Si le paquet a traversé un réseau non maîtrisé, alors rien ne vous prouve qu'il ne provient pas de la machine Evil.

Sécurité passive

Il s'agit de mesures visant à empêcher l'ARP cache poisoning, en figeant l'association IP/MAC sur les OS (utilisation des entrées statiques des tables ARP). Ceci est lourd et pratiquement inexploitable à grande échelle.

Qui plus est, certains OS gèrent mal ces entrées statiques qui peuvent être alors corrompues. C'est le cas des Windows 9x, NT et 2000 (XP a corrigé le problème). Ces OS sont donc fondamentalement vulnérables à ce type d'attaque et font profiter de leur faiblesse les logiciels (firewall, proxy, serveurs web...) qui leur sont dédiés.

Le verrouillage IP/MAC peut également être pris en charge au niveau applicatif. Par exemple, certains firewalls (dont *iptables*) sont capables de contrôler l'association IP/MAC des paquets entrants.

L'utilisation de commutateurs de niveau 3, capables de gérer l'association MAC/IP/port est également une solution au problème.

Sécurité active

Lorsqu'il n'est pas réaliste de verrouiller les entrées ARP de chaque machine, il est possible de mettre en oeuvre une solution de détection centralisée, qui agit comme une sonde de détection. Certaines sondes sont d'ailleurs capables de détecter des paquets ARP anormaux, susceptibles de signifier un ARP cache poisoning. Cependant, cette attaque étant réalisable avec des paquets normaux, la sonde n'a que peu d'intérêt.

L'utilisation de logiciels comme *arpwatch* permet de centraliser les associations MAC/IP, et de contrôler en temps réel les messages ARP pour vérifier qu'un poisoning n'est pas en cours.

Des alertes sont alors générées en cas de divergence.

Il pourrait même être envisagé un système de contre mesure consistant à repositionner la bonne association MAC/IP sur une machine venant de se faire poisons. Ce repositionnement pourrait s'effectuer par le même processus que celui qui a permis l'attaque : par ARP cache poisoning !