RÉGIS SENET

Attaque par IP Spoofing

Degré de difficulté

Comment obtenir l'acces non autorisé sur une machine ? La réponse est simple : usurpation d'adresse IP qui consiste à remplacer l'adresse IP de l'expéditeur d'un paquet par l'adresse IP d'une autre machine. Comment s'en défendre ? La réponse dans cet article.

Qu'est ce que l'IP Spoofing

La technique de l'IP Spoofing est une attaque informatique qui commence à dater mais elle demeure légendaire par l'utilisation qu'en a fait Kevin Mitnick en 1995 contre le Supercomputer Center de SanDiego protégé par Tsatumo Shimomura. Kevin Mitnick n'a fait que reprendre une faille connue depuis Février 1985 mais qui n'avait jamais été mise en place.

L'« usurpation d'adresse IP » (également appelée mystification ou en anglais IP Spoofing) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

Ce type d'attaque s'utilise de deux manières différentes :

- La première utilité de l'IP Spoofing est la falsification de la source d'une attaque. Par exemple, lors d'une attaque de type déni de service, l'adresse IP source des paquets envoyés sera falsifiée afin d'éviter de localiser la provenance de l'attaque permettant à l'attaquant d'être anonyme.
- La seconde utilisation de l'IP Spoofing permet de profiter d'une relation de confiance entre deux machines pour prendre la main sur l'une des deux.

Cet article vous présentera la seconde utilisation de l'IP Spoofing, utilisation qui peut avoir des retombées beaucoup plus désastreuses.

Certains tendent à assimiler l'utilisation d'un proxy (permettant de masquer d'une certaine façon l'adresse IP) avec de l'IP Spoofing. Toutefois, le proxy ne fait que relayer les paquets. Ainsi, même si l'adresse est apparemment masquée, un pirate peut facilement être retrouvé grâce au fichier journal (logs) du proxy.

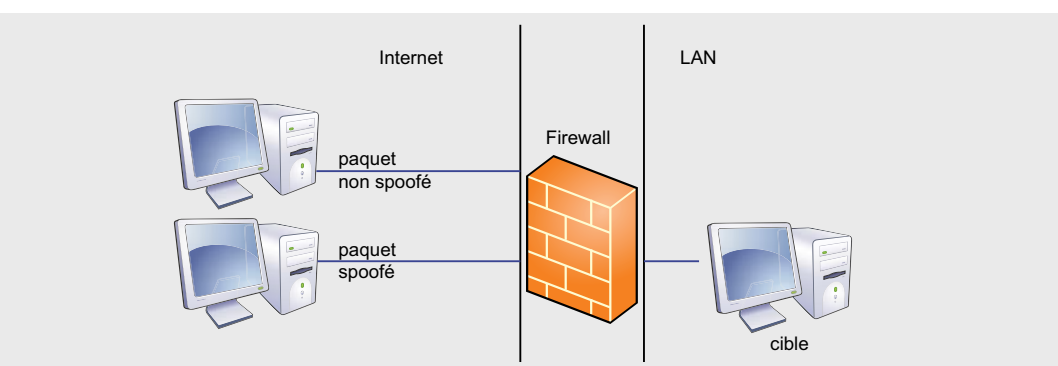

Figure 1. *Utilisation de paquets spoofé*

CET ARTICLE EXPLIQUE...

Ce qu'est l'IPSpoofing

Les risques encourus

Comment s'en protéger

CE QU'IL FAUT SAVOIR...

Connaissance en système d'exploitation Linux et les bases des réseaux

L'IP Spoofing a souvent lieu contre les services rlogin et rsh car leur mécanisme d'authentification est fondé sur l'adresse IP. Le principe est simple : dès qu'un client possède une connexion établie sur le serveur avec un mode d'authenfication fondé sur l'adresse IP, le pirate essaiera de se faire passer pour le client auprès du serveur. Pour cela, il empêchera le client de dialoguer avec le serveur et répondra à sa place.

Un peu de théorie ne fait jamais de mal

Le protocole IP est un protocole non-orienté connexion, il n'assure aucune vérification de la réception des paquets et ne se soucie que peu de la façon de les traiter. Le protocole IP n'assure qu'un routage d'une adresse vers autre. Il est donc aisé de duper le routage IP en injectant des paquets falsifiés ayant des adresses IP valides sur le réseau.

A l'inverse, le protocole TCP assure une fiabilité de la remise des paquets grâce à des numéros de séquences qui les distingue un à un. Chaque paquet TCP possède deux numéros, le numéro de séquence et le numéro d'acquittement. Ces deux nombres sont codés sur 32 bits. Ils sont uniques, afin de ne pas confondre les paquets lors de leurs traitements.

Nous décrirons l'attaque sur ces bases.

Imaginons que le *client A* est connecté grâce au protocole rsh sur le *serveur B*. Le *pirate C* tentera de voler la connexion au client.

En premier lieu, il réduira au silence le client en le saturant avec des attaques telles que le syn-flooding ou encore les attaques par *déni de service*.

La seconde partie de l'attaque est assez simple. Le pirate envoie une série de demandes de connexion au serveur en utilisant l'adresse du client A. Le serveur répond avec une série de paquets d'acquittement. C'est là que réside toute la finesse de l'IP Spoofing.

Rappels sur le protocole TCP

Afin de réaliser une connexion TCP, le client envoie un paquet avec un numéro de séquence initial (NS1). Le serveur répond avec un paquet d'acquittement ayant son propre numéro de séquence (NS2), mais ayant un numéro d'acquittement (NA1) égal au numéro de séquence initial incrémenté d'une unité (NA1=NS1+1). Ensuite, le client renvoie un paquet avec un numéro d'acquittement (NA2=NS2+1). Une connexion TCP s'établit donc en trois parties.

Ce principe de numéros de séquences et d'acquittement est utilisé durant toute la transaction pour en assurer la fiabilité. La subtilité de l'attaque réside dans le fait que le serveur génère la valeur NS2 suivant un cycle particulier. Il peut utiliser, par exemple, soit une fonction générant un nombre aléatoire, soit incrémenter une valeur initiale de 128 toutes les secondes et de 64 après chaque connexion. Tout dépend de l'implémentation de la pile TCP/IP du système.

Revenons à notre problème. Le pirate envoie un grand nombre de demandes de connexion dans un laps de temps déterminé et analyse les acquittements du serveur pour déterminer l'algorithme d'incrémentation. Si cet algorithme s'appuie sur la génération de nombres aléatoires, l'attaque a peu de chances d'aboutir. Mais si l'algorithme est facilement compréhensible, le pirate envoie alors une requête de connexion au serveur en utilisant l'adresse IP du client. Le serveur répond avec un paquet d'acquittement de numéro de séquence (NS). Le client mis hors service ne pourra répondre, le pirate le fera à sa place.

Pour cela, il doit injecter un paquet ayant un numéro d'acquittement de valeur NA = NS +1. Mais, ayant usurpé l'adresse du client, il ne peut intercepter les paquets lui étant destinés. Il ne peut donc pas connaître cette valeur NS. Il va donc la générer lui-même à partir de son analyse de l'algorithme d'incrémentation. C'est pourquoi cette attaque est aussi qualifiée «d'attaque aveugle». Si le numéro est valide, le pirate a établi la connexion au serveur en se faisant passer pour le client.

Le fait que l'attaque ne se restreigne qu'à une petite partie de système vient du fait que la plupart des piles TCP/IP utilisent des numéros de séquences fondés sur des nombres aléatoires. Certains systèmes comme BSD ou HP-UX connaissent de gros problèmes à cause de l'IP-Spoofing.

Dans le cadre d'une attaque par usurpation d'adresse IP, l'attaquant n'a aucune information en retour car les réponses de la machine cible vont vers une autre machine du réseau (il s'agit alors d'*attaque à l'aveugle*, en anglais *blind attack*).

Se défendre de l'IP Spoofing

Le filtrage IP n'a jamais été considéré comme un élément permettant de sécuriser un système. Tout au plus est-il un frein. Une authentification s'appuyant sur l'adresse IP peut être une bonne chose mais cette dernière doit être couplée avec un autre mécanisme d'authentification comme le classique couple nom d'utilisateur/mot de passe.

Comme indiqué précédemment, certains services comme rsh et rlogin ne se fondent que sur l'adresse IP, il est impératif de supprimer ces services pour les remplacer par, au pire du Telnet et au mieux du SSH avec login et mot de passe.

Listing 1. *Détermination de la difficulté de l'attaque*

```
nocrash:~# nmap -O -v 192.168.1.4

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
[…]
                    Remote operating system guess : Linux 2.1.19 - 2.2.19
Uptime 0.122 days (since Thu Mar 27 16 :02 :38 2003)
TCP Sequence Prediction : Class=random positive increments

Difficulty=4687481 (Good luck !)
IPID Sequence Generation : Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds

                    Les lignes intéressantes sont :
TCP Sequence Prediction : Class=random positive increments
Difficulty=4687481 (Good luck !)
```

Une solution consiste à refuser les paquets TCP SYN successifs depuis une même adresse pour éviter que le pirate prédise le comportement du générateur de numéros de séquences. Mais une telle restriction peut limiter la disponibilité du service (attaque par déni de service ou DoS).

Sous GNU/Linux, il existe des modules tels que rp_filter permettant de se défendre contre ces types d'attaques.

Il est maintenant possible de vérifier que son système n'a pas de numéro de séquence TPC facilement prédictible.

Prévenir l'IP Spoofing grâce à Nmap

Nmap invoqué avec l'option -O et -v vous fournit une indication sur la difficulté qu'aura le pirate à procéder à une attaque par IP Spoofing contre votre serveur.

Celles-ci nous renseignent sur la difficulté d'une attaque par IP-Spoofing. Plus le nombre associé à la valeur Difficulty est élevé, plus il est difficile d'entreprendre une attaque. Inversement, si lors d'un scan, vous obtenez un nombre très bas avec un message du type *Trivial Joke*, cela signifie que votre système est très vulnérable à une attaque par IP-Spoofing.

Conclusion

L'IP spoofing est une menace moins importante aujourd'hui en raison des patches de sécurité appliqués. La sécurité des syste`mes d'exploitation ainsi que l'utilisation étendue de séquence de nombre totalement aléatoire rend de moins en moins évident ce type d'attaque. Bien que cette attaque soit de plus en plus difficile à mettre en place, il est néanmoins nécessaire de la garder en tête et de tenter de l'éviter. Pour cela, la méthode la plus simple reste encore de désactiver l'ensemble des protocoles d'authentification ne se basant que sur l'adresse IP.

Auteur

Régis SENET, actuellement stagiaire pour la société JA-PSI, est étudiant en cinquième année à l'école Supérieure d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il s'oriente actuellement vers les certifications Offensive Security et CEH.

Contact : *regis.senet@supinfo.com*

Site internet : *http://www.regis-senet.fr*