COMMENT PRENDRE L'IP DE QUELQU'UN?

LE 31 AOÛT 2010 ***BRUNO***

Contrairement à ce qui a été dit pendant le débat sur l'Hadopi, c'est pas si facile que ça d'utiliser l'adresse IP d'un autre ordinateur. Petites explications sur comment fonctionnent les réseaux.

On entend beaucoup de bêtises, y compris dans l'hémicycle, ces temps-ci, à propos des adresses IP qui seraient de petites choses très faciles à usurper. Où est le vrai, où est le faux ?

Peut-on utiliser l'IP de quelqu'un d'autre?

La réponse est oui, mais pas sans conditions et certainement pas à l'aide d'un sabre et d'un perroquet.

Il existe trois grande familles de protocoles servant à faire voyager des données sur Internet (il y en a en réalité beaucoup plus, mais ces trois la représentent la majorité des applications)

ICMP, qui sert principalement aux machines elles-mêmes pour s'échanger des informations sur l'état du réseau et des autres machines (telle machine ne répond pas, tel portion du réseau réclame des paquets plus petits, …) et accessoirement permet de s'assurer qu'une machine répond un minimum.
UDP, qui sert principalement aux applications dites "temps réel" (la téléphonie, quelques applications de vidéo, …) et dont la particularité est de ne pas effectuer de contrôle d'intégrité de la transmission. En français, avec ce protocole, la machine qui reçoit un paquet n'a aucun moyen de savoir si un autre paquet aurait dû être reçu avant et si celui-ci s'est perdu en route.
TCP, qui représente l'immense majorité des usages (c'est là-dessus que voyagent le web, le mail, le FTP, les newsgroup, les vidéos Youtube, etc ..) qui, lui, dispose en interne d'un mécanisme de contrôle s'assurant que tous les paquets émis sont bien reçus et peuvent être remis dans le bon ordre à l'arrivée.
Un ordinateur peut envoyer sur le réseau un paquet avec n'importe quelle adresse IP comme source (de la même façon que n'importe qui peut envoyer un email venant de nicolas.sarkozy@elysee.fr).

Personne, en tout cas pas derrière une connexion ADSL, ne peut en revanche recevoir des données envoyées à une IP qui n'est pas la sienne (de la même façon que vous ne pouvez pas recevoir de réponse à votre mail envoyé depuis nicolas.sarkozy@elysee.fr)

Partant de la, ICMP et UDP n'ayant aucune notion de contrôle d'intégrité, on peut envoyer à peu près n'importe quoi à n'importe qui, mais les conséquences sont généralement minimes. Sauf envoi massif pour saturer la connexion de l'ordinateur cible, le seul dégât que vous pourriez peut-être causer, c'est de rompre une communication en cours qui se relancerait d'elle même quelques instant plus tard.

Avec TCP, par contre, pour établir une connexion avec une machine distante (par exemple avec le serveur de mail de votre fournisseur) vous devez envoyer une demande de connexion (SYN) qui contiendra un numéro de séquence à respecter et à laquelle, pour simplifier, l'autre va répondre (SYN/ACK) avec un autre numéro de séquence que vous allez devoir reprendre (ACK) pour pouvoir commencer la discussion et la poursuivre. Sans avoir le numéro de séquence envoyé par le serveur (puisque vous ne pouvez pas recevoir les paquets à destination de la fausse IP que vous voulez prendre), il est strictement impossible de maintenir une connexion TCP ouverte.

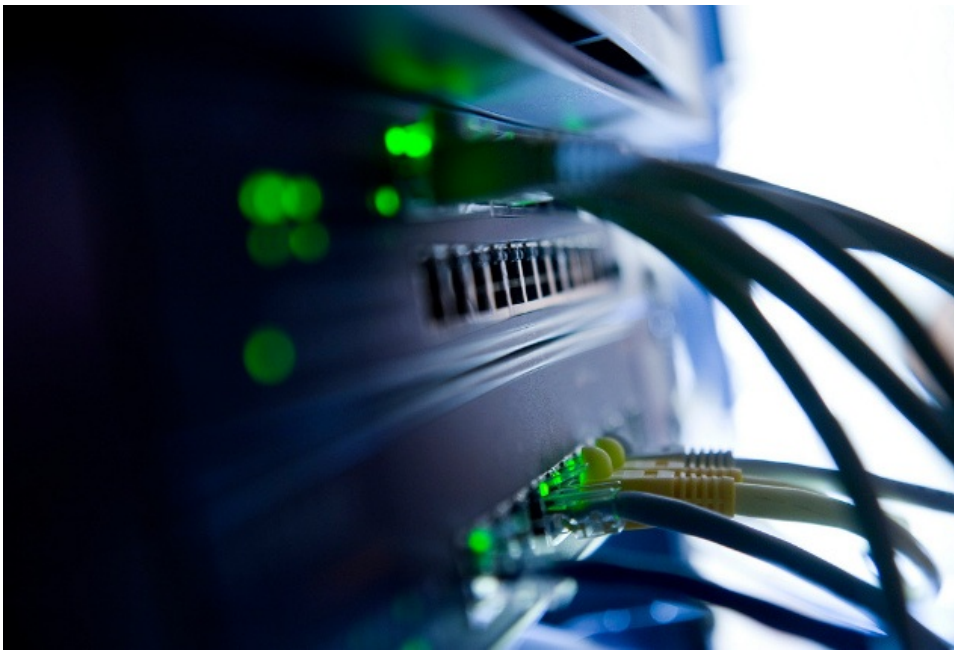
Il est éventuellement imaginable d'arriver par chance à deviner ce numéro de séquence (c'était plus facile il y a quelques années quand les système choisissaient des numéros de séquence avec un algorithme plus que douteux quant à sa faculté à générer du hasard) et donc de pouvoir envoyer des données, mais c'est sans compter sur la destination réelle des réponses de la cible de votre attaque qui se rebiffera rapidement en disant que "non, je n'ai jamais demandé à établir cette connexion, ferme la !". Tout ceci se jouant en quelques secondes, on peut valablement dire que "non, on ne peut pas prendre une IP au hasard", qui plus est pour télécharger un film sur un réseau P2P, chose qui, d'une part, prend généralement quelques heures au bas mot, et d'autre part nécessite de pouvoir

recevoir des données.

Ce qu'on peut faire

Ce qui est par contre possible de faire, c'est d'utiliser l'ordinateur de quelqu'un d'autre à son insu pour y faire passer ses propres données et, de fait, utiliser son IP. Pour cela, il faut l'avoir piraté d'une manière ou d'une autre (avec un virus envoyé par email que l'internaute à ouvert volontairement, pensant trouver des photos de sa femme, en exploitant une faille de sécurité, ou tout simplement en ayant l'occasion de s'assoir devant pour y installer discrètement un logiciel de prise en main à distance)

De même, avec un réseau wifi, on utilise l'IP du propriétaire de la connexion qui est au bout (exception faite du service Freewifi qui distribue une IP publique différente de celle de l'abonné dont on utilise la box).



Autre méthode, fortement conditionnée par le fait d'être sur un réseau de type réseau local d'entreprise, il n'est pas rare que les switchs reliant tous les ordinateurs ne soient pas configurés pour empêcher les postes de changer d'IP. Vous pouvez donc théoriquement, dans ce cas, utiliser n'importe quelle IP voisine de la vôtre (celle du collègue parti en vacances et qui a éteint son PC, deux machines avec la même adresse ne pouvant cohabiter). Même chose pour beaucoup de réseaux wifi publics couvrant les zones blanches ADSL.

Enfin, tous les services de VPN permettent, contre une obole mensuelle de l'ordre de 5 euro, de bénéficier d'une adresse IP complètement indépendante de son FAI mais vous ne la volez à personne puisqu'elle est là pour ça. Ceci dit, c'est au détriment de la vitesse et du débit de la connexion, toutes les données devant transiter par la plateforme VPN généralement située très loin et pratiquant le surbooking à outrance niveau bande passante pour être rentable.

Billet initialement publié sur **Turb(l)o(g)**

illustrations FlickR CC : **Darren Hester**, **splorp**

PMAUDUIT
le 31 août 2010 - 20:49 • SIGNALER UN ABUS - PERMALINK

"Un ordinateur peut envoyer sur le réseau un paquet avec n'importe quelle adresse IP comme source"

Une question qui me taraude : comment se fait-il que des vérifications ne soit pas faite du coté du fournisseur d'accès internet au niveau de ses équipements, pour ne pas jeter tout paquet "non légitime" (exemple concret : je suis chez free, je forge mes paquets en précisant une ip source Wanadoo) ? J'imaginais qu'un tel paquet ne ferait pas longue vie sur le réseau, au vu de l'aspect trivial de la vérification

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

BRUNOTURBLOG
le 31 août 2010 - 20:55 • SIGNALER UN ABUS - PERMALINK

Pas si trivial. Si en plus de devoir vérifier ou envoyer le paquet, le routeur doit regarder si la source est légitime, ça lui fait autant de temps en moins passé à router.

Accessoirement aussi, ça oblige à tenir à jour dans le routeur la liste de tous les préfixes qui peuvent passer par tel lien (ceux qui viennent de dedans et qui vont dehors) avec telles sources et, tant qu'a faire, avec telles destinations (ceux qui viennent de dehors et vont dedans).

Je ne sais en réalité pas si ça fonctionne encore chez les FAI connus, ça fait un moment que j'ai pas eu besoin d'essayer.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MARTIN
le 31 août 2010 - 21:41 • SIGNALER UN ABUS - PERMALINK

Les FAI pourraient intégrer cette vérification des paquets au niveau des box, puisqu'en général, du moins en France, celles-ci sont spécifiques à chacun des fournisseurs et appartiennent à ceux-ci. D'ailleurs, nul doute qu'à terme, on tende vers un filtrage au niveau de la box, que ce soit pour des raisons légitimes de sécurité du réseau (autant pour bloquer d'éventuelles intrusions sur le réseau local de l'abonné que pour l'empêcher à son tour de devenir l'agresseur, habituellement suite à un hack), ou pour des raisons plus discutables, sans rapport avec les intérêts de l'abonné ou du FAI (Hadopi en est un exemple).

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

HOMIE.IN
le 31 août 2010 - 22:44 • SIGNALER UN ABUS - PERMALINK

je ne suis pas du tout d'accord sur le fait que ce n'est pas si facile d'obtenir une autre IP. Bien au contraire, depuis que les lois se durcisse dans le monde entier, de nombreux fournisseurs d'IP et /ou VPN se créer tous les jours. Il n'y a qu'a voir la liste des fournisseurs: http://www.start-vpn.com/vpn-info/vpn-providers/

j'ai fait le test ce we, pour regarder un match de la Ligue 1 de foot sur Justin.tv avec une adresse IP américaine. Cela m'a pris 5 minutes montre en main entre le temps de choisir un fournisseur, m'abonner, installer le soft et choisir mon IP américaine.

et maintenant, a chaque fois que je me connecte sur Internet, je suis en IP étrangère.

rien d'aussi simple…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

BRUNOTURBLOG
le 31 août 2010 - 22:54 • SIGNALER UN ABUS - PERMALINK

@homiein : la moindre des choses lorsqu'on commente un article, c'est de le lire en entier avant de commenter.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

SID
le 1 septembre 2010 - 0:02 • SIGNALER UN ABUS - PERMALINK

Pour la vérification des IPs en sortie par les FAIs, certains le font pourtant…

Par contre, sur le fait que deux machines avec la même adresse ne peuvent pas cohabiter, dit comme ça, c'est vrai : on ne peut pas configurer deux machines sur le même LAN avec la même IP.
Par contre, on sait usurper depuis une machine A l'adresse IP d'une machine B elle

aussi active si ces deux sont sur le même LAN:

http://sid.rstack.org/static/articles/j/o/u/Jouer_avec_le_protocole_ARP_dadb.html

Ça marche aussi sur les réseaux Wi-Fi ouverts, sauf que là, on sait même usurper l'adresse MAC en même temps. Ça laisse rêveur quand on pense aux Hotspots ou aux accès genre FreeWiFi justement…

http://sid.rstack.org/pres/0602_ESW_CaptiveBypass.pdf

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GULFSTREAM
le 4 septembre 2010 - 12:12 • SIGNALER UN ABUS - PERMALINK

Un peu de clarification pour commencer

Tou d'abord on ne peut pas "envoyer un paquet avec n'importe quelle adresse source". Tous les routeurs de tous les ISP du monde et a fortiori les routeurs centraux des carriers appliquent par défaut une règle qui interdit le "source routing". Donc, pas de chance, si vous envoyez un paquet avec une adresse source différente de la votre il ira tout simplement à la poubelle sans bruit … Ca serait un peu trop facile quand même ;-)

Ensuite, à propos des fournisseurs de VPN, dont je fais partie, je l'avoue, la vitesse n'est pas un facteur pour les fournisseurs "sérieux". Nous prenons bien soin de ne jamais surbooker la bande passante de manière démesurée et proposons même des accès avec bande passante dédiée.

De plus, à moins que les plateformes d'accès de votre fournisseur VPN ne soient toutes situées en Asie ou en Afirque, les débits et le "lag" sont aujourd'hui tout à fait corrects, tant sur les points d'accès Europe que US … quand on prend soin de séléctionner son "peering" bien sur :-)

Nous avons de nombreux clients adeptes de jeux en ligne et les retours d'utilisation sont tout à fait positifs.

Enfin, et toujours à propos des VPN, il y a VPN et … VPN. Les accès PPTP sont dépassés, nous en proposons toujours bien sur pour rester "standard" mais l'avenir est à OpenVPN. PPTP est très facile à filtrer (ou plutot GRE) tandis qu'Open VPN peut se "dissimuler" sur n'importe quel port … Le notre utilise le port 443 (https) et passe aisément pour une connection http sécurisée … allez donc demander à un ISP de filtrer le port 443, il n'aurait plus beaucoup de clients … ;-)

Michael

http://www.anti-hadopi.com

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

BRUNO
le 4 septembre 2010 - 12:34 • SIGNALER UN ABUS - PERMALINK

Le source routing et le fait d'envoyer un paquet avec une IP forgée n'ont rien à voir.

Accessoirement, les carriers n'ont aucun moyen de connaitre l'IP d'un internaute lambda pour vérifier qu'elle n'est pas forgée dans un paquet qui passe. A la limite le fournisseur d'accès peut verrouiller ça dans sa bidulebox ou sur son réseau si ça l'amuse de perdre du temps, mais la dernière fois que j'ai essayé (ça remonte à 2 ans), ça fonctionnait très bien chez Free et Orange. Je ferais un article sur la question quand j'aurais pas la flemme de tout démonter chez moi pour faire un pilote chez moi, mais à l'instant, testé depuis le réseau TATA Telecom en inde vers une machine sur un autre réseau à Paris en forgeant une IP appartenant à Bouygues, ça passe sans problème, idem en partant d'une machine sur le réseau Free en allant chez orange avec une IP forgée appartenant à OVH.

Pour le reste, si vous le dites, je vous crois … Mais vous faites encore partie de ceux qui utilisent le mot peering à tord et à travers :)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

WILLEMIJNS

le 11 septembre 2010 - 7:30 • SIGNALER UN ABUS - PERMALINK

http://www.willemijns.com/dynip.php liste les VPN ;)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

KANIZE ALI
le 16 décembre 2010 - 13:02 • SIGNALER UN ABUS - PERMALINK

Bonjour .. ofait .. jaimerais demander une question je ne suis pas tres pro en informatique don comprendre l'article m'est un peu dur :S

Alors dans mon entourage , il y a u un certain incident comme suit : des foto de jeunes filles ont ete changer via photoshop et mise nude ds des sites porno …
*Apres la recherche de l'adresse IP on a pu deduire que cette c*nnerie a ete faite par un garcon appele X. et des photos du genre ont ete retrouvees sur le pC de X*

Donc voila ma question .. Est-ce que c'est possible que quelqu'un ai piater lordi de X et fait c sovageries ? et ensuite mi ces fotos ds son pC par le piratage ???

Votre aide me servira bcp svp

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

» Créer des paquets avec de fausses IP Turb(l)o(g) le 4 septembre 2010 - 16:05

[...] mon article expliquant comment prendre l'IP de quelqu'un, qui à lui même été repris sur OWNI, Michael de anti-hadopi.com indique qu'il est aujourd'hui impossible d'envoyer un [...]