RFC 5157 : IPv6 Implications for Network Scanning

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 mai 2008

Date de publication du RFC : Mars 2008

https://www.bortzmeyer.org/5157.html

Une technique classique des méchants craqueurs qui cherchent à pénétrer un gentil réseau est de **balayer** ("*to scan*") l'ensemble des adresses IP à l'intérieur du réseau, pour voir lesquelles répondent et ainsi trouver des cibles. Par exemple, Slammer l'utilisait. Mais en IPv6, où le nombre d'adresses possibles est infiniment plus grand, cette tactique est-elle encore efficace ? (Notez que ce RFC a, depuis, été remplacé par le RFC 7707 [1].)

Imaginons que le craqueur aie déterminé que le préfixe IP du réseau de sa victime est le 192.0.2.128/25. Il reste 7 bits pour les machines soit 128 victimes potentielles à interroger, ce qui ne prend que quelques secondes pour un programme comme fping. Cette technique est donc très utilisée pour avoir une liste des adresses IP utilisées... et donc des cibles possibles. Mais en IPv6, si la victime a le réseau de préfixe 2001:DB8:AF:42::/64, comment le balayer de manière efficace ? Cela fait 64 bits pour les machines donc 18446744073709551616 adresses à examiner, ce qui ne peut pas se faire en un temps raisonnable (sections 2.1 et 2.2 du RFC).

Certains en ont donc déduit que le balayage ("*scanning*") était impossible en IPv6 et que donc, sur ce point, IPv6 offrait davantage de sécurité qu'IPv4.

Mais notre RFC montre que ce n'est pas si simple et qu'il existe d'autres méthodes que la force brute pour trouver les machines allumées (un excellent article <http://www.cs.columbia.edu/~smb/papers/v6worms.pdf> de Steve Bellovin avait déjà déblayé ce terrain).

La section 2.3 parle par exemple de l'exploitation de conventions d'adressage. Si l'administrateur du réseau 2001:DB8:AF:42::/64 cité plus haut numérote ses machines 2001:DB8:AF:42::1, 2001:DB8:AF:42::2,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7707.txt

2001:DB8:AF:42::3, etc, l'attaquant n'aura à tester qu'une petite partie des adresses théoriques. Si au lieu d'adresses calculées ainsi, on utilise la traditionnelle autoconfiguration sans état d'IPv6 (RFC 4862), la connaissance du fournisseur des cartes Ethernet fournit déjà un bon moyen de sérieusement réduire l'espace de recherche.

Les sections 3 et 4 du RFC listent l'ensemble des techniques connues et que le méchant pourrait utiliser pour arriver néanmoins à balayer un réseau IPv6. La section 4 concerne les cas où l'attaquant est lui-même sur ce réseau et le problème est alors assez simple (il lui suffit d'espionner les paquets ND ("*Neighbor Discovery*", cf. RFC 4861). La section 3 parle des cas où l'attaquant n'est pas sur le réseau. Sa tâche est alors plus difficile mais reste faisable : par exemple la section 3.3 détaille l'information qu'on peut tirer d'un transfert de zone DNS <https://www.bortzmeyer.org/recuperer-zone-dns.html>, et la 3.4 l'intérêt qu'on peut trouver à regarder les journaux d'un gros serveur, journaux où on trouvera les adresses de clients qui sont autant de cibles potentielles.

Plus moderne est l'observation des pairs dans un réseau P2P (section 3.5). La plupart des protocoles de P2P, par exemple BitTorrent, mettent en rapport direct les « offreurs » et les « preneurs » et, en offrant du contenu intéressant, on peut récolter beaucoup d'adresses IP de machines.

La section 5 passe aux recommandations et contre-mesures : utilisation d'adresses « vie privée » (RFC 8981), dont la durée de vie est limitée, utilisation d'adresses EUI-64 (RFC 4291, cf. section 5.1) mais sans l'adresse MAC (section 5.3), configuration du serveur DHCP (RFC 8415) pour ne pas attribuer les adresses séquentiellement à partir de ::1 (section 5.4), etc.

Enfin, en guise de synthèse, la section 7, qui résume le problème et les moyens de le limiter, rappelle que dissimuler les adresses IP des machines est de la Sécurité par l'obscurité : cela peut ralentir l'attaquant, mais cela ne doit certainement pas être utilisé comme unique moyen de défense, car, tôt ou tard, l'attaquant trouvera ces adresses.

Un nouveau RFC, plus détaillé, a remplacé celui-ci, le RFC 7707.