B

L'attaque ARP

Objectif

L'une des attaques de sécurité les plus appréciées actuellement exploite l'*Address Resolution Protocol* (protocole de résolution d'adresse, ou ARP). Du fait de son importance, de sa simplicité et parce qu'elle illustre bien les ruses par lesquelles un pirate peut prendre le contrôle de votre réseau, nous avons choisi de vous la présenter brièvement ici.

B.1 L'ARP EN BREF

Lorsqu'une station doit envoyer un paquet IP vers une autre station, dont elle connaît l'adresse IP, mettons par exemple 10.0.0.2, elle commence par rechercher cette station sur le réseau local. Pour cela, elle doit trouver l'adresse physique (c'est-à-dire l'adresse MAC) correspondant à ladite adresse IP. C'est le rôle du protocole ARP, comme nous l'avons vu dans l'annexe A : une requête ARP de type *broadcast* (envoyée à tout le monde) demande, en somme, « qui possède l'adresse IP 10.0.0.2 ? ». Le propriétaire de l'adresse IP en question répond alors, par exemple, « c'est moi, et mon adresse MAC est 00:0E:A6:5C:80:37 ». La première station est alors en mesure d'envoyer le paquet IP vers la deuxième station, en encapsulant le paquet IP dans un paquet Ethernet adressé à la bonne adresse MAC.

Pour éviter d'avoir à envoyer des requêtes ARP sans arrêt, chaque station conserve en mémoire une table d'associations entre adresses IP et adresses MAC : cette table s'appelle naturellement la table ARP. Le principe d'ARP est donc très simple et très efficace. Mais il y a un « hic ».

B.2 L'EMPOISONNEMENT

Le problème provient du fait qu'aucun mécanisme n'est défini pour sécuriser le protocole ARP. En particulier, un pirate peut très bien envoyer une réponse ARP à une station en lui disant que, dorénavant, l'adresse IP 10.0.0.2 correspond à sa propre adresse MAC ou à n'importe quelle autre adresse MAC de son choix ! On dit alors que la station a été « empoisonnée ».

L'empoisonnement est rendu d'autant plus facile que la plupart des stations acceptent des réponses ARP alors même qu'elles n'ont envoyé aucune requête ARP : le protocole est dit « sans état » (*stateless*).

B.3 LES ATTAQUES POSSIBLES

L'attaque ARP permet de réaliser plusieurs types d'attaques sérieuses :

- En associant à une adresse IP une adresse MAC inexistante sur le réseau, le pirate interdit à la station empoisonnée tout trafic en direction de l'adresse IP choisie. C'est une attaque de type déni de service (DoS), qui a l'avantage de pouvoir être assez sélective.
- Si le pirate associe sa propre adresse MAC à une adresse IP, il peut espionner tout le trafic envoyé par la station empoisonnée vers l'adresse IP choisie.
- Une fois que le pirate a détourné le trafic vers lui-même, il peut choisir de répondre à la place de la station à qui le trafic était destiné, la station empoisonnée n'y voyant que du feu.
- S'il ne veut pas que l'on puisse détecter sa présence, le pirate doit rediriger tout le trafic qu'il reçoit vers le destinataire légitime. Pour pouvoir également intercepter les réponses, le pirate doit empoisonner le destinataire de la même manière. Il se retrouve alors entre les interlocuteurs, à leur insu : toutes les attaques de type *Man in the Middle* lui sont alors permises. Il peut par exemple espionner tous les paquets échangés, les modifier ou encore tenter de prendre le contrôle d'une session ouverte.
- Enfin, le pirate peut bombarder un commutateur (*switch*) avec des milliers de réponses ARP dans le but de saturer sa table ARP. Dans ce cas, certains commutateurs réagissent par la suite en retransmettant tous les paquets qu'ils reçoivent sur tous leurs ports ! En d'autres termes, ils se comportent alors en simples répétiteurs : leur fonction d'isolation des communications est éliminée. C'est le cas également avec certains commutateurs de type VLAN : c'est alors particulièrement grave car un pirate situé sur un

VLAN donné peut attaquer une station sur un autre VLAN. Preuve, s'il en est, qu'il est important de toujours bien vérifier la qualité du matériel que l'on achète.

B.4 LE NETTOYAGE

Dans le cas d'une attaque ARP de type MiM, deux précautions s'imposent pour le pirate :

- Lorsqu'une station ne détecte aucun trafic réseau vers une adresse IP donnée pendant un certain temps (en général, environ deux minutes), elle « nettoie » sa table ARP en enlevant l'association IP/MAC correspondante. Ainsi, pour pouvoir effectuer une attaque ARP sans heurts, le pirate doit fréquemment empoisonner la station ou s'assurer qu'un trafic régulier a lieu.
- Si le pirate s'en va, l'ensemble du trafic qui passait par lui est perdu dans le néant. Le trafic ne passant plus (au moins pour quelques minutes), l'utilisateur piraté risque alors de se rendre compte que quelque chose ne va pas et de donner l'alerte. Si le pirate ne souhaite pas que l'on sache qu'une attaque a eu lieu, en particulier s'il veut revenir plus tard, il doit, avant de partir, penser à remettre en place les bonnes associations dans les tables ARP des stations empoisonnées.

B.5 LA PORTÉE DES ATTAQUES

L'attaque ARP se déroulant au niveau de la couche 2, un pirate peut attaquer l'ensemble du réseau de niveau 2 auquel il appartient, c'est-à-dire l'ensemble des équipements qu'il peut atteindre par un broadcast. Rappelons qu'un broadcast est relayé par les répétiteurs et les commutateurs, et ne s'arrête qu'au niveau des passerelles qui délimitent deux (ou plusieurs) réseaux ou sous-réseaux. Par exemple, si l'entreprise a découpé son réseau en deux sous-réseaux en plaçant une passerelle entre les deux, un pirate pourra attaquer toutes les stations situées du côté où il se trouve, même si son sous-réseau est parsemé de répétiteurs, de commutateurs ou même… d'AP !

En effet, la plupart des AP se comportent comme des répétiteurs ou des commutateurs (à l'exception bien sûr des routeurs Wi-Fi). Ainsi, un pirate connecté sans fil à un AP peut réaliser une attaque ARP à l'encontre de toutes les stations de son sous-réseau, qu'elles soient connectées sans fil au même AP, à un AP différent (dans le même sous-réseau) ou même sur le réseau filaire ! Bref, c'est une raison de plus de sécuriser son réseau sans fil.

B.6 LES PARADES

B.6.1 Empêcher la connexion

L'attaque ARP suppose que le pirate soit capable de se brancher au réseau. La première parade consiste donc à l'en empêcher. Pour un réseau filaire, il faut empêcher l'accès physique au réseau. En Wi-Fi, avec le WEP, tous les paquets sont rejetés par l'AP si le pirate ne connaît pas la clé secrète. Malheureusement, nous avons vu qu'il n'était pas très compliqué pour un pirate de trouver la clé WEP d'un AP (en utilisant des outils disponibles gratuitement sur Internet), donc de profiter pleinement de la connexion Wi-Fi. En revanche, le WPA et le 802.11i offrent une protection très efficace : un pirate peut bien s'associer à un AP, mais l'ensemble des paquets qu'il émet est rejeté par l'AP tant qu'il ne s'est pas identifié avec le protocole 802.1x.

B.6.2 Installer un pare-feu

Si un pirate parvient bel et bien à se connecter au réseau sans fil, il peut en principe lancer une attaque ARP contre toutes les stations dans son sous-réseau. Toutefois, certains pare-feux savent détecter ces attaques et les empêcher : l'idéal est que ce type de pare-feu soit intégré à chaque AP, de sorte que le pirate ne puisse même pas attaquer les autres stations associées au même AP. Sinon, on devra se contenter d'un pare-feu installé entre l'AP et le réseau filaire, pour au moins protéger le réseau filaire contre les attaques provenant du réseau sans fil.

B.6.3 Des tables ARP statiques

Une autre parade, assez contraignante, consiste à interdire qu'une association de la table ARP puisse être modifiée. En supposant que les tables ARP soient déjà figées au moment où le pirate arrive, il ne pourra empoisonner aucune station. Malheureusement, il est souvent nécessaire que les associations changent : en particulier, si les stations obtiennent leur adresse IP dynamiquement (par DHCP), alors il peut arriver fréquemment qu'une même adresse IP soit attribuée à un moment donné à une station, et un peu plus tard à une autre (avec une autre adresse MAC). Dans ce cas, il faut que toutes les stations du réseau mettent à jour leur table ARP pour prendre en compte ce changement.

B.6.4 L'analyse des historiques

Enfin, les stations peuvent souvent conserver un historique de leur table ARP. On peut alors analyser les historiques ARP des stations (manuellement ou grâce à un logiciel spécialisé) dans le but de trouver les traces d'attaques passées, pour mieux prévoir et prévenir les prochaines.