Déni de service sur des téléphones Cisco

Régis Deldicque (regis.deldicque@orange.com)

(3/7/2017)

Résumé : cet article présente une attaque déni de service réalisée sur des postes téléphoniques IP modèle CP-7821 de la marque CISCO. L'objectif de cette expérimentation est de montrer qu'il existe différentes manières de nuire à une entreprise sans spécialement attaquer une application informatique mais en ciblant le fonctionnement d'une entité de cette dernière à travers la paralysie de son réseau téléphonique via un déni de service mis en œuvre à travers une attaque TCP/SYN flood. L'article conclue sur l'extension de ce type d'attaque à d'autres périphériques tout aussi utilisées au sein d'une entreprise comme les imprimantes réseau.

Définition de l'attaque : l'attaque TCP/SYN flood est une attaque réseau par saturation exploitant le mécanisme de poignée de mains en trois temps (Three-ways handshake) du protocole TCP.

Le mécanisme de poignée de main en 3 temps est la manière selon laquelle toute connexion « fiable » à Internet (utilisant le protocole TCP) s'effectue (cf. fig.1).

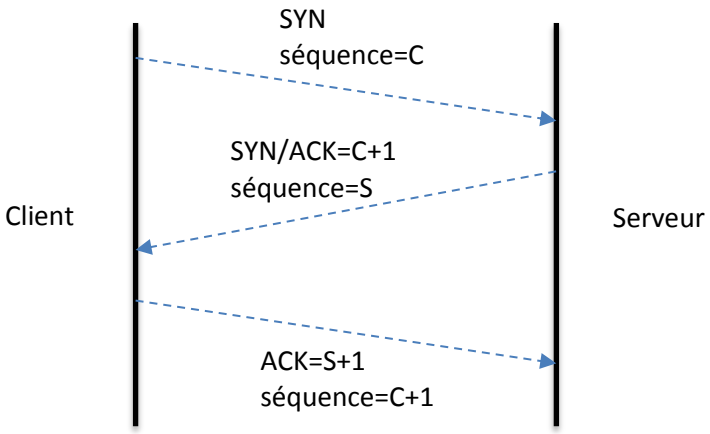

Fig. 1 : Three-ways handshake

Lorsqu'un client établit une connexion à un serveur, le client envoie une requête SYN, le serveur répond alors par un paquet SYN/ACK et enfin le client valide la connexion par un paquet ACK.

Une connexion TCP ne peut s'établir que lorsque ces 3 étapes ont été franchies. L'attaque TCP/SYN flood consiste à envoyer un grand nombre de requêtes forgées avec le flag SYN à un hôte avec une adresse IP source inexistante ou invalide (partenaire fantôme). Ainsi, il est impossible que la machine cible reçoive un paquet ACK (cf. fig.2).

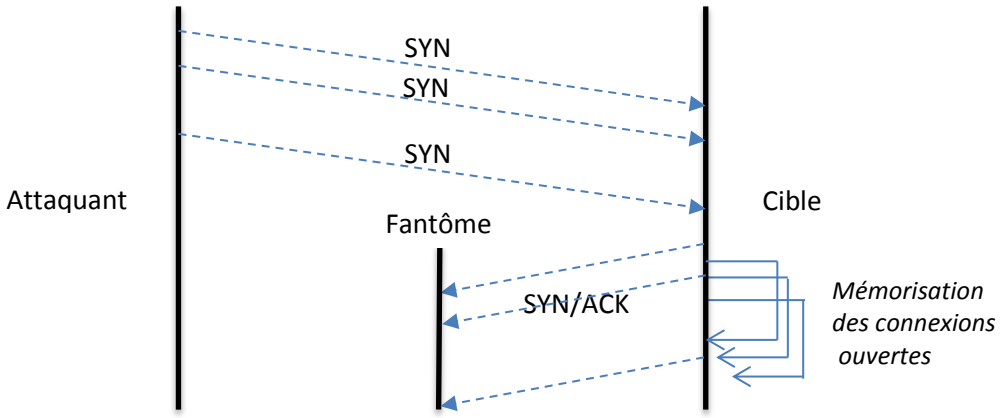

Fig. 2 : principe de l'attaque TCP/SYN flood

Les machines vulnérables aux attaques mettent en file d'attente les connexions ainsi ouvertes, en mémoire, et attendent de recevoir un paquet ACK. Il existe un mécanisme d'expiration permettant de rejeter les paquets au bout d'un certain délai. Néanmoins, avec un nombre de paquets SYN très important, si les ressources utilisées par la machine cible pour stocker les requêtes en attente sont épuisées, elle risque d'entrer dans un état instable pouvant conduire à un plantage ou un redémarrage.

Déclinaison de l'attaque dans un contexte entreprise : il semble donc intéressant pour ne pas fondamental de mettre en pratique cette attaque, non pas en prenant pour cibles les applications du SI d'une entreprise, qui sont pour la plupart protégées/supervisées à travers des solutions réseau (N-IDS, Load Balancer....), mais envers d'autres devices connectées telles que les postes téléphoniques qui si ils deviennent hors service peuvent freiner voire interrompre tout ou partie de l'activité d'une entreprise.

Une expérimentation a été menée à travers une attaque réalisée au sein d'une entreprise et plus précisément sur le téléphone de l'auteur de cet article. Ces devices sont connectées au même sous réseau. La configuration des postes de travail proposée est décrite dans le schéma ci-dessous. Le téléphone IP est directement raccordé au réseau local. L'ordinateur de l'utilisateur se connecte au réseau via une interface avec le téléphone IP ce qui implique qu'une mise hors service du téléphone IP implique une perte d'accès au réseau depuis l'ordinateur de l'utilisateur (cf. fig.3).

Fig. 3 : description du poste utilisateur

La préparation de l'attaque passe avant tout par la connaissance de l'adresse IP du poste téléphonique de la cible (cf. fig. 4) qui permet également d'orienter l'attaque vers une personne particulière.

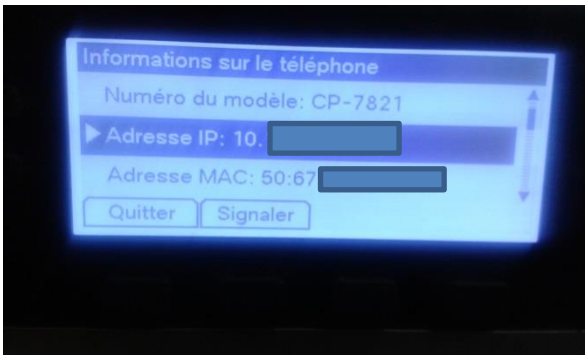

Fig. 4 : récupération de l'adresse IP du poste téléphonique

On peut également, collecter les adresses IP des postes en scannant le sous réseau concerné via la commande **nmap -sn --traceroute 10.xxx.xxx.0/24** qui permet d'énumérer tous les nœuds connectés à ce sous réseau. Dans ce cas les alias retournés et commençant par un préfixe spécifique**,** permettront de distinguer les postes Cisco, et donc les cibles potentielles, des autres devices (pc, serveurs....) et organiser ainsi une attaque en masse.

L'attaque a été lancée depuis une distribution Kali Linux qui propose un certain nombre d'outils de tests dont la commande **hping3** (http://tools.kali.org/information-gathering/hping3).

La commande hping3 a permis d'envoyer un grand nombre de paquets TCP/SYN vers le poste téléphonique IP Cisco afin d'inonder son interface réseau. De plus chaque paquet envoyé vers la cible l'a été avec une IP source inexistante ou invalide afin de conserver les connexions TCP initialisées à l'état actif pendant un certain temps propre à la cible (cf. fig. 5).

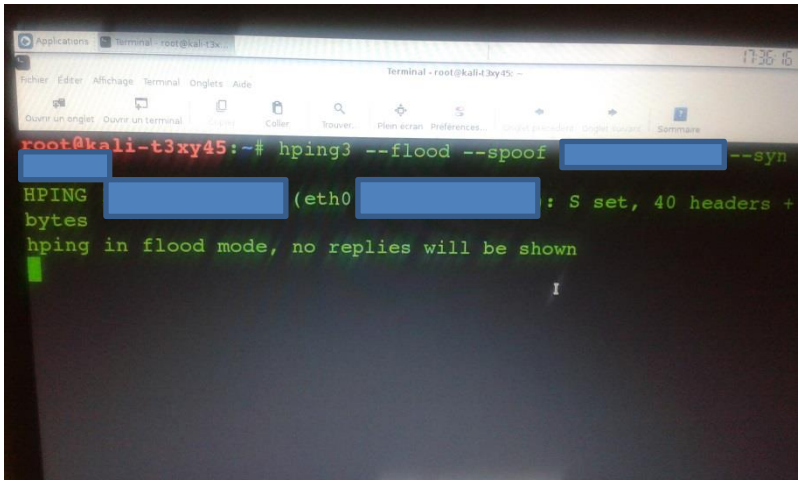

Fig. 5 : commande hping3 paramétrée pour le flood SYN

Au bout de 1 à 2 minutes le déni de service apparait sur le poste Cisco (cf. fig.6).

Fig. 6 : vue du poste téléphonique en déni de service

Si on arrête l'attaque, le rétablissement du poste est très rapide (~10 s) mais plus on laisse l'attaque s'exécuter et plus le rétablissement est long car les connexions initialisées côté tel Cisco sont plus nombreuses également et par conséquent l'engorgement de l'interface réseau est plus important.

Attention, si on utilise une même ip pour l'IP source et l'IP destinataire (i.e. l'IP de la victime) alors l'effet flood s'annule car il n'y a pas d'effet « attente réponse » pour les connexions initialisées.

Un deuxième effet qui est la conséquence du DoS précédemment décrit, est la mise hors service de l'interface réseau du PC portable connecté au téléphone IP Cisco (cf. fig. 7).

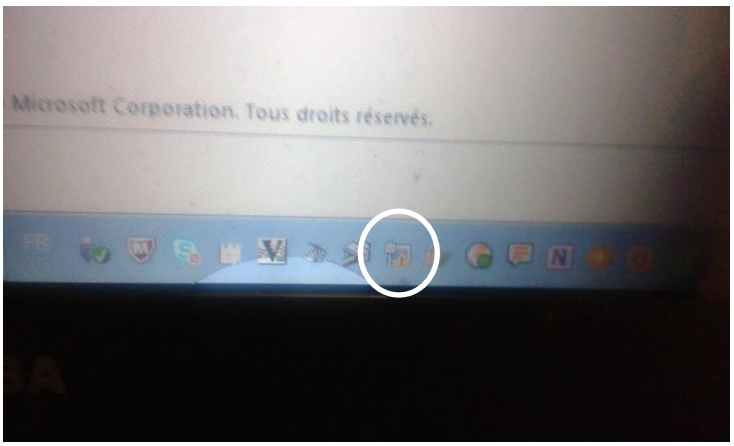

Fig. 7 : perte de connexion réseau pour le PC portable

On constate donc qu'une attaque de type déni de service sur un poste téléphonique IP est assez facile à réaliser et impacte également le PC portable associé via l'interface réseau. De cette manière on peut sans grande difficulté neutraliser, d'une certaine manière, une position de travail.

De la même manière, il est également tout à fait possible d'organiser le même type d'attaque sur une imprimante réseau avec pour résultat une mise hors service de toutes les fonctionnalités proposées par cette dernière le temps que dure le DoS (cf. fig. 8).

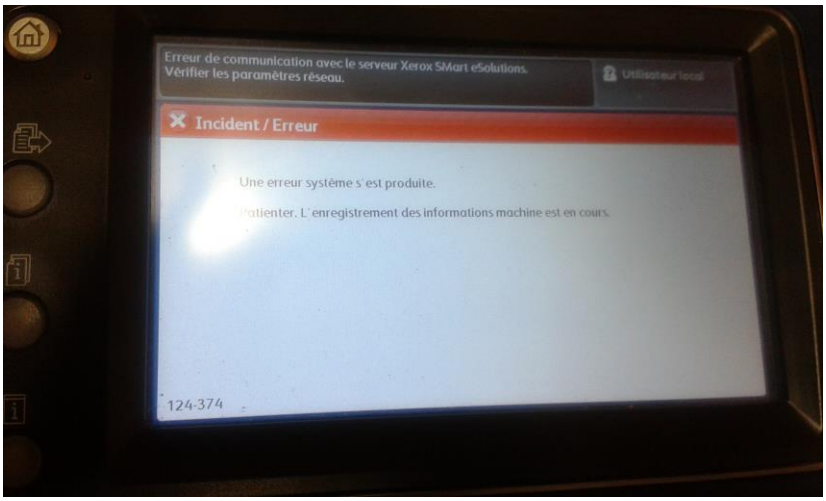

Fig. 8 : résultat d'un déni de service de type TCP/SYN flood sur une imprimante réseau

Conclusion : nous avons mis en œuvre une attaque TCP/SYN flood au sein du réseau téléphonique IP d'une entreprise. Nous avons pris soin de rester anonyme tant des responsables du site que des éléments de supervision réseau en « spoofant » l'adresse IP source à l'origine de l'attaque. A travers cette intrusion, nous nous sommes placés dans une situation où un utilisateur malveillant (salarié, assistance technique...) souhaite exercer un pouvoir de nuisance en exploitant une vulnérabilité des positions de travail et plus largement des ressources connectées sur le site de l'entreprise cible.

----------Fin du document----------