PROJET TRIBOX-2012-A

Auteur :
Groupe

Tutoriel d'installation et de configuration de Trixbox

Membres du projet:

GUITTON Jordan
MORELLE Romain
SECK Mbaye Gueye

Responsable de la formation:

MOTAMED Cina

Client:

DUSSART Dominique

CONTRÔLE DU DOCUMENT

Historique des versions :
Date de début : 20/03/2013
Auteur : GUITTON Jordan

Date	Version	Action/Modification apportée	Contributeur
20/03/13	1.0	Création de la première version du document	Jordan

Distribution :

Document destiné a être publié sur: http://tribox2012a.free.fr

État :
Terminé.

Sécurité et confidentialité :
Aucune

Responsabilité :
Ne s'applique pas.

Notes sur cette édition :
Cette publication concerne le projet tutoré Tribox-2012-a

TABLE DES MATIÈRES

I) PRÉSENTATION DU DOCUMENT

1) But

Ce document a pour but d'aborder les points essentiels sur la sécurité d'un réseau VoIP.

2) Cadre

Ce rapport est rédigé par GUITTON Jordan étudiant en licence professionnelle "Réseau et Système de Communication" et concerne le projet tribox2012-a.

3) Contenu

Se reporter à la table des matières.

II) LES ATTAQUES SUR UN RÉSEAU VOIP

1) Les interceptions d'appels

Avec la VoIP, les téléphones sont accessibles depuis l'extérieur de l'entreprise, les téléphones deviennent plus ou moins des serveurs. Les outils d'écoute du réseau, d'analyse de flux et d'injection de trafic IP sont donc utilisable sur un réseau VoIP (exemple : WireShark, VOMIT, SiVuS ...). Un pirate a donc la possibilité d'entrer ou de sniffer un réseau d'entreprise afin d'intercepter les communications du réseau.

2) Les attaques sur les couches basses

a) L'ARP spoofing ou ARP redirect

Cette attaque redirige le réseau d'une ou plusieurs machines vers la machine du pirate. Elle opère au niveau Ethernet et permet de spoofer le trafic IP et le trafic TCP.

Son fonctionnement est assez simple: Elle consiste faire correspondre son adresse IP à l'adresse MAC de la machine pirate dans les tables ARP des machines du réseau. Pour cela il suffit d'envoyer régulièrement des paquets ARP_reply en broadcast, contenant l'adresse IP cible et la fausse adresse MAC. Cela modifie les tables dynamiques de toutes les machines du réseau. Celles-ci enverront donc leurs trames Ethernet à la machine pirate tout en croyant communiquer avec la cible, et ce de façon transparente pour les switch. De son côté, la machine pirate stocke le trafic et le renvoie à la vraie machine en forgeant des trames Ethernet comportant la vraie adresse MAC.

b) L'ARP Cache poisoning

C'est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP. Cette technique peut permettre à l'attaquant de détourner des flux de communication transitant sur un réseau local commuté, lui permettant de les écouter, de les corrompre, mais aussi d'usurper une adresse IP ou de bloquer du trafic.

L'attaquant, en détournant le flux, peut ainsi voir les données qui transitent en clair entre les deux machines. L'ARP poisoning est notamment utile dans un réseau local, entre une victime B et un routeur A.

Source: http://fr.wikipedia.org/wiki/ARP_poisoning

3) Les dénis de service

Les attaques DoS (denial of service attack) n'a pas pour but de récupérer des informations ou prendre possession du réseau, mais juste de le mettre hors service.

Son principe est très simple : elle consiste à inonder le réseau de données inutiles. Par exemple un nombre trop important de messages SIP INVITE ou de simples messages ICMP peuvent créer un déni de service.

Les attaques DoS peuvent être provoquées par plusieurs machines simultanément pour plus d'efficacité, on parle de d'attaque DDoS (attaque distribuée).

A noter qu'il existe de nombreuses méthodes d'attaque DoS (les buffers overflows: mails, ping of Death, l'attaque SYN, l'attaque Teardrop, l'attaque SMURF, les virus etc …).

4) Le spoofing SIP

Il existe plusieurs types de spoofing sur le protocol SIP, la plus populaire consiste a forger un SIP INVITE (comportant un Call-ID, From, To et Cseq spécifique) pour faire sonner le téléphone distant. La conversation ne fonctionne que si le To est égal à celui qui est appelé, mais beaucoup de configuration n'utilise pas les Tags et sont donc vulnérable à ce type d'attaque, et dans le cas d'une LAN, il est possible de récupérer les Tags en sniffant le réseau. Avec cette attaque, il est possible d'écouter les conversations en temps réel et même de modifier les paquets de données envoyées (et donc usurper l'identité de l'utilisateur victime de l'attaque).

III) SÉCURISATION D'UN RÉSEAU VOIP

Comme vu précédemment, les possibilités d'attaques d'un réseau VoIP sont nombreuses, et la téléphonie a souvent un rôle très important dans les entreprises. La mise hors service du système de communication téléphonique d'une entreprise peut entraîner de grave dysfonctionnement, voir immobilité d'une entreprise. Pire encore : les interceptions d'appels.

Certaines conversations peuvent contenir des éléments confidentiels concernant la sécurité ou l'exclusivité inventive d'un projet. Il est donc très important de protéger un réseau VoIP convenablement, sous peine de graves conséquences pour l'entreprise.

1) Sécuriser les couches basses

a) La configuration des Vlan :

Il existe plusieurs types de Vlan, le choix dois se faire en fonction du besoin. Les Vlans permettent d'avantage de sécurité car les informations sont encapsulées dans un niveau supplémentaire, parfois analysées (pour un Vlan de niveau 3 par exemple) et réduis considérablement la diffusion du trafic sur le réseau.

b) Le filtrage des adresse mac :

Permet d'éviter que n'importe qui puisse se connecter sur les port d'un switch. Ainsi, seuls les périphériques ayant une adresse mac correspondante à la règle de filtrage sera capable d'accéder au switch.

c) La protection face aux attaques ARP :

- Pour faire une attaque ARP, il est nécessaire de pouvoir se brancher au réseau. Pour se protéger aux attaques ARP, il faut donc restreindre les possibilités de connexion. Pour un réseau Wi-fi, appliquer une protection par clé WPA ou supérieure, et la changer régulièrement. Pour un réseau filaire, restreindre l'accès physique au réseau.

- Installer un pare-feu maintenu à jour. La plupart des pare-feu sont capable de détecter et empêcher les attaques ARP.

- Implémenter des tables ARP statiques. Cette méthode consiste à interdire qu'une association de la table ARP puisse être modifiée. Ainsi, les pirates ne peuvent empoisonner aucune station (à condition que les tables ARP soient déjà figées à ce moment).

- Analyser les historiques des tables ARP. Cette méthode n'empêche pas directement le système d'être attaqué mais permet de chercher d'éventuelles traces d'attaques afin de les analyser, les comprendre, et s'en protéger a l'avenir.

2) Sécuriser le réseau

a) Le contrôle d'accès par filtrage IP

Les serveurs VoIP ont un grand nombre de port ouvert par défaut. Pour augmenter la sécurité du réseau, il est conseillé de veiller à la bonne configuration de politique de filtrage, afin de réduire au maximum les ports ouverts non utilisés.

b) L'utilisation de tunnels IPSec

L'utilisation de tunnel IPSec présente certains avantage, mais n'est pas sans inconvénient.

IPSec travaille sur la couche réseau et permet d'augmenter la fiabilité des informations (permet d'empêcher par exemple certaines modifications de donnés, et donc l'usurpation d'identité via le spoofing SIP). Cela dit, l'utilisation des tunnels IPSec est possible que sur des softphones suffisamment puissant et que sur des petites infrastructures car le coût de son utilisation est grand, et entraîne rapidement une surcharge du réseau.

c) La protection contre les attaques DoS

Les attaques DoS sont plus difficiles à contrer, car les dénis de services sont généralement provoqués sur des services et protocoles "normaux", couper ses services et protocoles reviendrait à à couper toute voie de communications avec internet. Il est donc impossible de bloquer toutes les attaques DoS, mais il existe tout de même certains outils de la marque Cisco permettant de les limiter :

Test de la taille des paquets :

- Test des adresses source et destination (ainsi que loop-back, unicast, multicast...)
- Test de la fragmentation
- Utilisation d'adresses IP virtuelles pour validation de sessions et ACK (contre attaques TCP)
- Test du nombre de SYN (contre attaques TCP)
- NAT d'adresses locales vers IP virtuelles basées sur IP globales
- Contrôles de flux
- Contrôles de contenus (port, tag, url, extensions de fichiers)
- Autres fonctions de Firewall, le tout basé sur du load-balancing et de la redondance

Source: http://nicolas.roux.pagesperso-orange.fr/securite/attaq/attaq_dos.htm

d) L'utilisation de SRTP

Le protocol *Secure Real-time Transport Protocol* définit un profil de RTP (Real-Time Transport Protocol) qui à pour but d'apporter le chiffrement (cryptage AES 128 bits), l'authentification (HMAC-SHA1) et la protection contre le replay de données RTP.

Source: http://fr.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol