## 1. S'adapter aux spammeurs

Supports de la présentation :

http://www.ba-cst.com/presentations/100p100/100p100.pdf

http://www.ba-cst.com/presentations/100p100/index.html

Les spammeurs sont constamment à la recherche de nouvelles méthodes pour nous faire parvenir leurs messages. Chaque méthode donne lieu à des contre-mesures dans les outils, selon la métaphore connue du bouclier et de l'épée.

Mais ils n'ignorent pas non plus certaines bonnes vieilles recettes, dont l'utilisation de dictionnaires.

Ainsi, on observe parfois des pics de réception (et rejets) de messages, pouvant aller jusqu'à presque 100% de messages rejetés pendant certaines périodes.

De telles valeurs de rejets de messages suggèrent une analyse du système, afin de déterminer s'il n'y a pas un dysfonctionnement dans la plate-forme de messagerie. En l'occurrence, pour les cas examinés, cela correspondait :

- A l'envoi de messages (probablement identiques : même adresse d'émetteur) à des destinataires choisis dans des listes de noms communs (jonh@domaine, henry@domaine, helen@domaine, etc.)
- Ces messages sont transmis en parallèle à tous les MX du domaine de destination.
- Ces messages sont expédiés à partir de sources (adresses IP) différentes.

La combinatoire est simple. Pour un domaine disposant de 3 MX, un dictionnaire de 5000 noms communs et un micro-réseau d'émission de spam de 10 sources, cela fait 150000 messages à recevoir sur un laps de temps court (une heure environ).

Si l'on met de côté l'engorgement que cela peut représenter au niveau de la bande passante et de la capacité de traitement des serveurs, quelle réponse peut-on apporter à cela ?

Il peut être intéressant :

- De s'assurer que tous les MX d'un domaine (y compris les secondaires même s'ils se trouvent sur d'autres sites) connaissent les adresses valides pour le domaine concerné (le rejet se fera alors au niveau du MX de réception, et non pas à celui du système gérant les boîtes à lettres).

- Voire de n'avoir qu'un seul MX, en se reposant sur le fait que les systèmes sont aujourd'hui stables et qu'en cas d'indisponibilité, les messages seront stockés sur les serveurs des émetteurs.
- Et d'éviter des structures d'adresses électroniques trop simples (du type prénom@domaine).

Le fait de n'avoir qu'un seul MX a déjà été évoqué au sujet du greylisting : cela permet de ne gérer qu'une seule base de triplets de listes grises, et donc d'éliminer les problèmes liés à des bases dissociées. En outre, c'est une méthode efficace pour s'assurer que « tous » les MX du domaine mettent en place les mêmes contrôles de sécurité.

## 2. Analyse des flux dans le moteur IPS-ASQ (NetASQ)

Supports de la présentation :
http://www.ossir.org/resist/supports/cr/20050404/MoteurIPS-ASQ-Netasq.pdf
http://www.ossir.org/resist/supports/cr/20050404/Netasq.pdf

Il existe plusieurs méthodes de détection de « problèmes » dans des flux IP :

- L'analyse protocolaire,
- Les signatures contextuelles, et
- Les statistiques et heuristiques.

Ces trois classes de méthodes sont mises en œuvre dans le moteur IPS-ASQ.

### *2.1. Analyse protocolaire*

Cela correspond à vérifier que les flux réseau « suivent bien » les spécifications attendues :

- Respect des RFCs
- Normalisation des flux

L'analyse protocolaire au niveau IP permet d'éliminer la mascarade d'adresses, de gérer les options IP (et d'éliminer les constructions n'ayant « aucun sens »), de s'assurer de la cohérence des données. Au niveau TCP, les flux sont reconstruits et nettoyés. Aucun paquet n'est réémis avant une défragmentation complète et la validation des données.

Par exemple, les attaques par insertion sont détectées. Un premier fragment peut être reçu, contenant GET /url-1. Un second fragment (qui peut recouvrir totalement le premier, comme s'il s'agissait d'une retransmission, ou ne le recouvrir que partiellement), contient GET /url-2. Le moteur d'analyse détecte cette incohérence des données, qui devraient être identiques, entre les deux fragments.

*Question* : Si le système fait la défragmentation avant de transmettre les paquets, il consomme des ressources mémoire pour stocker ces données. N'y a-t-il pas un risque de déni de service à ce niveau ?

*Réponse* : L'outil ne stocke les paquets en cours de reconstruction que pendant un certain laps de temps. Au-delà, il les efface et libère sa mémoire. Les éléments effacés étant retransmis par l'émetteur (puisqu'ils ne seront pas acquittés par le destinataire), il n'y a aucune perte de données.

*Question* : qu'en est-il des faux positifs, notamment des applications qui ne respectent pas (ou mal) les RFCs ?

*Réponse* : La rigueur du respect des RFCs est paramétrable, on peut mettre en place un « respect flou » pour les applications qu'il n'est pas possible de modifier. Il est aussi possible d'éliminer ce contrôle protocolaire s'il empêche l'analyse.

### *2.2. Signatures contextuelles*

Cette méthode est similaire à celle mise en place par les anti-virus ou les sondes de détection d'intrusion. Il s'agit d'une méthode permettant une réaction rapide à de nouvelles attaques : le téléchargement d'une nouvelle base de signatures est une opération bien plus facile que la mise à jour du firmware de l'outil. L'analyse des signatures est arborescente, plutôt que linéaire, afin de n'examiner que les branches « significatives » pour un paquet donné.

Cette méthode autorise des tests différents de ceux mis en place par l'analyse protocolaire (par exemple détection d'un User-Agent: particulier dans les données).

*Question* : Quel est le nombre de protocoles analysés ?

*Réponse* : Pour l'analyse protocolaire, 6 ou 7. Pour les signatures contextuelles, une quinzaine de protocoles.

*Question* : Les signatures contextuelles permettent-elles de détecter des spywares ?

*Réponse* : Une telle détection est partiellement du ressort de l'analyse statistique et heuristique des communications mises en place par les spywares (heures, types de flux, rapport émission/réception, etc.). Il existe aussi une base de signatures

permettant de détecter les communications des spywares et autres malwares avec l'extérieur.

### *2.3. Statistiques et heuristiques*

Des indicateurs statistiques, couplés à diverses heuristiques, permettent de détecter ou de qualifier des échanges pathologiques. Par exemple, un reverse shell dans des tunnels http aura un « aspect » statistique différent d'un échange http classique (taille des paquets, rapport des volumes d'émission et de réception, etc.). Certains de ces aspects statistiques permettent de qualifier une transaction comme étant « de nature interactive », alors que le protocole utilisé (http, DNS…) ne l'est pas.

*Question* : Est-ce que cela va jusqu'à permettre la détection d'IP encapsulé dans du DNS ou de l'ICMP ?

*Réponse* : S'il s'agit d'un tunnel interactif (de type reverse shell), les caractéristiques statistiques des échanges seront différentes de celles d'une utilisation légitime du DNS ou de l'ICMP. S'il s'agit d'un contournement de filtres (on utilise le port UDP/53 qui est autorisé en sortie pour tout le monde, mais ce n'est pas du DNS qui est transmis) l'analyse protocolaire le détectera.

## 3. Déploiement d'un réseau sans fil à l'échelle d'un campus

Support de la présentation :
http://www.ossir.org/resist/supports/cr/20050404/DeploiementWifiCampus.pdf

L'objectif du projet était d'augmenter le « service aux utilisateurs ». Cela signifiait notamment de coupler, autant que possible, l'équipement des salles de conférences (amphithéâtres) et des espaces ouverts ainsi que l'accès au réseau depuis les domiciles des étudiants (ou des enseignants).

Le cahier des charges comprenait les besoins suivants :

- Authentification de tous les utilisateurs
- Chiffrement des échanges
- Absence de contraintes sur les postes des utilisateurs
- Facilité d'administration
- Souplesse des politiques de sécurité, et possibilités d'adaptations rapides.
- Surveillance et détection des anomalies.

L'état de l'art concernant la connectivité sans fil est, globalement, le suivant :

- Pour des solutions de niveau 2 (au sens ISO) : 802.1X, WPA, 802.11i (WPA2). L'accès au réseau est impossible sans authentification. Chaque poste doit disposer de clients adéquats, qui sont parfois lourds à mettre en place et à configurer.
- Pour des solutions de niveau 3 : garde-barrière dynamique et VPN. L'accès au réseau est libre, mais on ne peut rien faire dessus tant que l'on ne s'est pas authentifié.

L'étude des solutions existantes (2004) a donné les « bilans » suivants :

- 802.1X et FreeRadius : l'administration de la solution est particulièrement lourde, ainsi que son installation sur certains types de postes.
- BlueSocket : Pas de gestion des accès à distance.
- Cisco : Pas d'administration centralisée (au moment où l'étude a été réalisée).
- Aruba : solution retenue, car la plus proche des besoins du cahier des charges.

Le principe est d'utiliser des bornes légères (24 bornes, dont 5 pour la surveillance de l'espace radio), configurées depuis un concentrateur Wireless Gateway. L'authentification passe par LDAP et Radius ou LDAP seul.

Le nomadisme régional (un membre d'une des écoles concernées se déplaçant sur le campus d'une des autres écoles doit pouvoir se connecter au réseau sans fil) est géré par le biais de Radius et d'un serveur mandataire central. Chaque serveur local (site A) délègue les interrogations concernant des profils « extérieurs » (associé au site B) à ce serveur mandataire, lequel les réachemine vers le serveur d'origine de l'utilisateur concerné (site B).

*Question* : La détection des émetteurs ad-hoc est-elle possible ?

*Réponse* : La détection est possible, mais pas le blocage de ces émetteurs.

*Question* : Quel effort doit être fait pour la création d'un SSID « temporaire » (par exemple pour un congrès se tenant dans un ou deux amphithéâtres) ?

*Réponse* : L'effort est très réduit, de l'ordre de quelques minutes. Seules les bornes concernées diffuseront le SSID approprié (en plus des autres), grâce aux éléments de localisation des bornes : l'emplacement des bornes (bâtiment, étage, numéro de la borne) est stocké dans la base de l'outil.

*Question* : Comment l'INPT gère-t-il les visiteurs souhaitant se connecter au réseau ?

*Réponse* : Si le service est prévenu à l'avance, il n'y a aucune difficulté à mettre en place une configuration spécifique. Sinon (demande urgente), l'INPT a pré-défini des profils de visiteurs afin d'anticiper cette situation.