

Dans le cadre de *SECURIDAY 2009*

SECURINETS



*Présente*

**Atelier : Sécurisation d'un serveur mail face  
aux spams**

**Formateurs:** AKKARI Mohamed Amine

CHEBBI Imene

HAMMAMI Maroua

MKACHER Atef

WERTANI Amira

### **Introduction :**

Une machine zombie est une machine contrôlée par un pirate informatique dans le but de l'utiliser pour attaquer d'autres machines en dissimulant sa véritable machine.

Beaucoup de machines zombies sont liées les unes aux autres pour former ce qu'on appelle un réseau de machines zombies ou Bot Net. Grâce à cette union, ces machines deviennent dotées d'une capacité de destruction et un impact importants.

Ce réseau de bots est utilisé dans des attaques de type déni de service ou pour l'envoi en masse de courriers indésirables (les spams)...

Dans le présent atelier nous allons traiter le cas des bots d'envoi de spams.

### **Présentation générale de l'atelier :**

Dans le cadre de cet atelier, on se propose d'installer sur une machine un serveur mail POSTFIX auquel on lie deux clients de messagerie.

Le but de cet atelier est surtout de montrer la nécessité de protéger le serveur mail par des antispams puissants.

### **Les Techniques antispams :**

Afin de faire face au flot de spams envoyés par les bots, il s'avère utile voire même nécessaire d'utiliser des logiciels capables de détecter ces courriers indésirables et les détruire.

Ces logiciels sont connus sous le nom d'anti spam ou anti- pourriel.

Les méthodes de lutte contre les pourriels sont diverses et diffèrent d'un anti spam à un autre.

Parmi ces méthodes, on distingue :

#### **1) Analyse heuristique :**

Cette méthode consiste à rechercher des mails dont le corps ou l'entête a des caractéristiques connues pour avoir une forte probabilité d'être un spam.

#### **2) Listes noires :**

Cette méthode consiste à utiliser des listes qui contiennent des serveurs ou des réseaux connus pour produire et transmettre des spams ou fournir un service pouvant être utilisé pour l'envoi de spams.

#### **3) Bases collaboratives de spams :**

Ces bases de signatures de spams sont utilisées de la même manière que les bases de signatures de virus. Ces bases sont mises à jour par les utilisateurs et les antispams.

#### 4) Enregistrement DNS :

Généralement, les serveurs de messageries utilisent des adresses IP fixes et bijectives avec leurs noms de domaine associés. Cette méthode repose sur ce principe et consiste à vérifier la corrélation entre l'adresse IP du serveur source et son nom via une requête DNS inverse.

#### 5) Filtres bayésiens :

Cette méthode se base sur la détection de mots clés qui rend le mail suspect d'être spam. Cet algorithme utilise souvent des spams connus

#### 6) Liste blanche :

Cette méthode consiste à mettre dans une liste les noms et les adresse des serveurs mails connus et surs.

#### 7) Historique des transactions :

Cette méthode permet de vérifier si deux machines ont l'habitude d'échanger des mails légitimes entre elles.

#### 8) Adresses URL :

Cette analyse est basée sur la détection de sites suspects et des url suspects.

#### 9) SPF et DKIM :

Les techniques anti-spam appelées SPF (Sender Policy Framework) et DKIM (Domain Keys Identified Mail) ont pour but d'authentifier les serveurs de messagerie autorisés à expédier des emails pour un domaine donné.

#### 10) OS fingerprint :

Cette méthode permet de reconnaître le système d'exploitation utilisé par le serveur émetteur, par suite cette méthode nous permet de reconnaître les spams émis par des botnets.

#### 11) Greylisting :

Le greylisting est une technique antispam très récente qui consiste à rejeter temporairement un message, par émission d'un code de refus temporaire au serveur émetteur. Le serveur émetteur réexpédie le mail après quelques minutes tandis que la plupart des serveurs de spams ne prennent pas cette peine.

## 12) Test de Turing

Cette technique, également nommée challenge/réponse, consiste à renvoyer un email de demande d'authentification à l'expéditeur du message afin de s'assurer de son existence physique réelle.

### les outils utilisés :

- **POSTFIX** : serveur de messagerie libre.
- **SPAMASSASSIN** : le but de ce logiciel est de filtrer le trafic des courriels pour éradiquer les courriels reconnus comme pourriels ou courriels non sollicités. SpamAssassin est un programme qui fait passer un certain nombre de tests au message. En fonction du résultat de ces tests, il attribue un score au message. Si le score dépasse un certain seuil, le mail est alors considéré comme du Spam. Tous les messages doivent donc passer par SpamAssassin pour être traités, avant d'arriver dans leur dossier définitif.
- **Razor** : C'est une base de données des spam en cours de propagation. L'objectif est de détecter le lancement d'une vague de Spam le plus rapidement possible. A chaque message contrôlé par SpamAssassin, le serveur Razor externe est interrogé et une réponse est renvoyé permettant de déterminer si c'est le contenu est enregistré comme Spam ou non.
- **Pyzor** : C'est un filtre supplémentaire qui se greffe dans Spamassassin pour améliorer le filtrage des spam.
- **ClamAv** : C'est un logiciel antivirus très utilisé sous UNIX. Il est généralement utilisé avec les serveurs de courriels pour filtrer les courriers comportant des virus. Les virus ciblés sont très majoritairement des virus s'attaquant au système d'exploitation Microsoft Windows et non pas aux systèmes sur lesquels ClamAV s'installe, qui sont peu menacés par les virus.

## Partie Pratique

### 1) Installations et configurations du serveur mail:

#### ❖ *PostFix*

```
apt-get install postfix postfix-mysql postfix-doc mysql-client mysql-server courier-authdaemon  
courier-authlib-mysql courier-pop courier-pop-ssl courier-imap courier-imap-ssl postfix-tls  
libsasl2-2 libsasl2-modules libsasl2-modules-sql sasl2-bin libpam-mysql openssl phpmyadmin  
apache2 libapache2-mod-php5 php5 php5-mysql libpam-smbpass
```

Il faudrait les fichiers de configurations du POSTFIX après son installation. Ces fichiers sont :

- /etc/postfix/mysql-virtual\_domains.cf
- /etc/postfix/mysql-virtual\_forwardings.cf
- /etc/postfix/mysql-virtual\_mailboxes.cf
- /etc/postfix/mysql-virtual\_email2email.cf
- /etc/postfix/mysql-virtual\_transports.cf
- /etc/postfix/mysql-virtual\_mailbox\_limit\_maps.

❖ **Installation des outils antiSpam: Amavisd-new, SpamAssassin et ClamAV**

Il s'agit d'installer ces anti-spam et les configurer.

*apt-get install amavisd-new spamassassin clamav clamav-daemon zoo unzip bzip2 libnet-perl libnet-snpp-perl libnet-telnet-perl nomarch lzop pax*

Les fichiers concernés par la configuration sont :

- /etc/amavis/conf.d/15-content\_filter\_mode
- /etc/amavis/conf.d/20-debian\_defaults
- /etc/amavis/conf.d/50-user
- /etc/spamassassin/local.cf
- /etc/spamassassin/v310.pre
- /etc/postfix/master.cf

❖ **Mise en place d'autres outils de sécurisation du serveur mail : Razor, Pyzor et DCC**

*apt-get install razor pyzor*

**2) Remplissage et test de la BDD du serveur mail**

Il s'agit d'exécuter quelques requêtes permettant l'ajout :

- Des Domaines : INSERT INTO `domains` (`domain`) VALUES ('KING.com');
- Des Utilisateurs : INSERT INTO `users` (`email`, `password`, `quota`) VALUES ('atef@KING.com', ENCRYPT('secret'), 10485760);
- Des « forwardings » : INSERT INTO `forwardings` (`source`, `destination`) VALUES ('amine@KING.com', 'atef@KING.com');

- Des transports : INSERT INTO `transport` (`domain`, `transport`) VALUES ('KING.com', 'smtp:mail.KING.com');

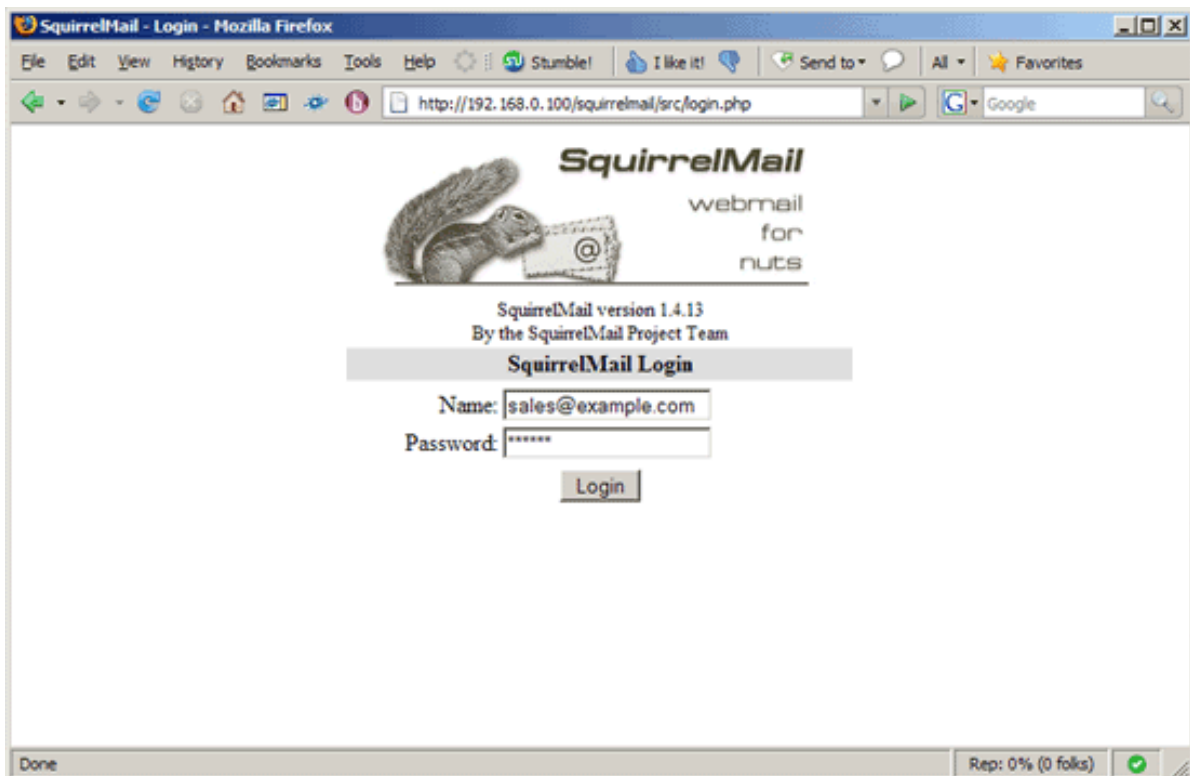
### 3) Autres outils à installer et à configurer:

- ✓ Mailx : Outil permettant aux utilisateurs d'envoyer des mails.

Pour envoyer un mail à un utilisateur « atef », on tape :  
« mailx atef@KING.com ». Puis on doit saisir le sujet du mail et le corps.

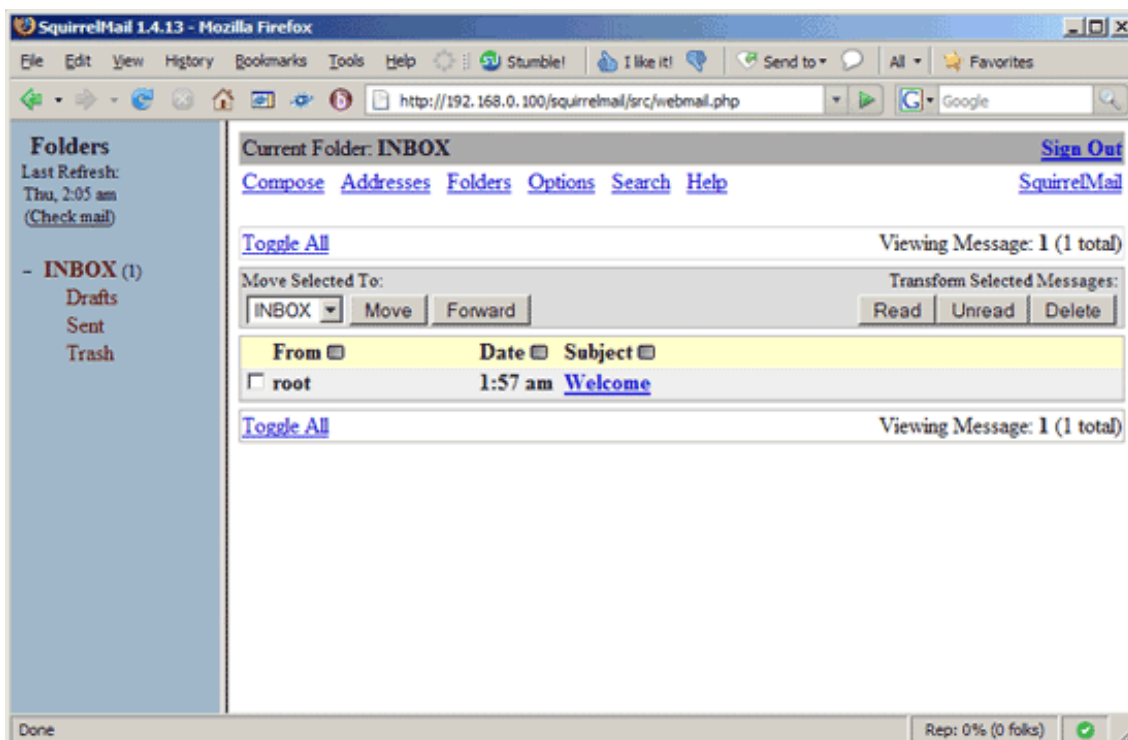
- ✓ SquirrelMail : Outils de consultation des boites e-mails des utilisateurs.

*apt-get install squirrelmail php-pear*



# S E C U R I N E T S

Club de la sécurité informatique  
I N S A T



## Conclusion :

Certes, il est important de connaître le principe de l'attaque d'un serveur mails par un flot de spam mais il est encore plus important de le sécuriser face à ces attaques. Pour cette raison, nous avons mis l'accent dans ce tutoriel sur la notion de protection du serveur par des antispams ainsi que les différentes techniques utilisées.