

SECURINETS



**CLUB DE LA SECURITE INFORMATIQUE
INSAT**

SECURILIGHT 2011

Mail Spoofing

Chef Atelier : Mohamed BOUMAIZA (RT5)

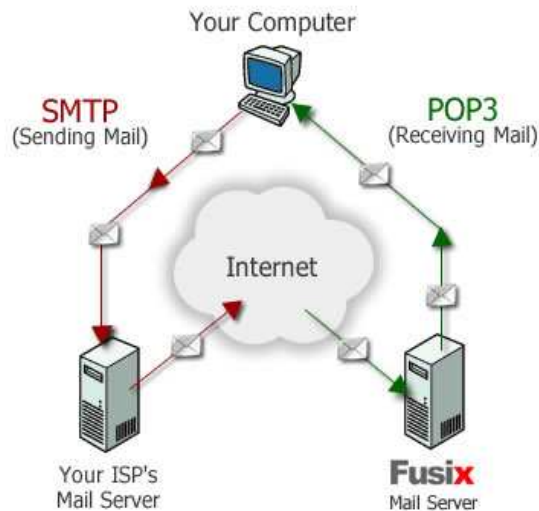
Taher BEN SALEM (RT3)

Mouna FALEH (RT3)

Aymen BEN TANFOUS (MPI)

30/11/2011

1- Fonctionnement du service Mail :



SMTP: (Le Simple Mail Transfer Protocol), utilisé depuis 1980, est un protocole de communication qui sert à transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique, il est affecté au port 25 .

POP3: (Post Office Protocol), est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique. Le port utilisé est le 110.

IMAP: (Internet Message Access Protocol) est un protocole qui permet de récupérer les courriers électroniques sur des serveurs de messagerie. Son but est donc similaire à POP3. Mais contrairement à ce dernier, il a été conçu pour permettre de laisser les messages sur le serveur.

2- Connaissez -vous le mail spoofing ?

L'Email- Spoofing est une technique **d'usurpation d'identité** : son utilisation ne nécessite aucune connaissance particulière, même si elle est un peu complexe pour un novice.

Elle consiste à modifier les champs présents dans le **Header Du mail** (« From », « Reply to », etc.) pour cacher l'origine réelle du mail.

Cette faille provient d'une trop grande liberté dans l'implémentation du protocole **SMTP**. Les spammeurs utilisent cette astuce pour envoyer des mails non sollicités en utilisant des adresses de personnes tierces.

Pour quoi spoofer un mail ?

Il existe quatre raisons majeurs pour l'usurpation de mails :

- envoi de SPAM
- envoi de virus
- commettre des fraudes
- Trouble makers « causer des ennuis à quelqu'un »

SPAM

De nombreuses sociétés publicitaire utilise le spoofing pour diffuser leurs SPAM

Cette méthode donne l'impression que le mail « spam » est envoyé par une personne réelle et non une machine, ce qui va accentuer un peu son importance, de plus elle leur permet de se cacher leur véritable identité.

VIRUS

Presque tous les programmes de virus les plus récentes utilisent le courrier électronique spoofing.

Les raisons sont simples: beaucoup de gens sont encore prêts à l'aveuglette de cliquer sur une pièce jointe envoyée par quelqu'un qu'ils connaissent.

Une fois activé, le virus va se transmettre à tout le monde dans carnet d'adresse de l'ordinateur infecté.

FRAUDE

C'est envoyer des e-mail spoofer usurpons l'adresse d'organisation légitime « banque, poste ... » demandant des mots de passe ou des informations de carte de crédit. Ces e-mails demandent souvent la victime à visiter une page web et de remplir un formulaire en ligne. Bien sûr, cette page web est fausse « c'est le principe du fishing ».

TROUBLES MAKERS

Le but de ces personnes est :

- La désinformation
- Générer des rumeurs ceci pour causer des ennuis, conduire à des conflits et des malentendus.

3- Passons a la Pratique :

Etapes à suivre :

1/ Se connecter avec le protocole telnet sur un serveur SMTP (serveur mail)

```
root# telnet serveur_smtp 25
```

Sachant que 25 est le numéro du port du protocole smtp

2/ Une fois connecté sur le serveur, il suffit d'introduire les champs du mail un par un et taper a chaque fois la touche «Entrée» .

On commence par l'enveloppe du mail qui se compose des champs <MAIL FROM> et <RCPT TO> puis DATA.

Le protocole SMTP ne dispose d'aucun mécanisme de vérification des adresses source et destination

```
220 mx.google.com ESMTP f10si15263139anh.109
HELO
250 mx.google.com at your service
MAIL FROM: <V1RUZWASHERE@YOUBEENHACKED.COM>
250 2.1.0 OK f10si15263139anh.109
RCPT TO: <mynameisblablablablabla@gmail.com>
250 2.1.5 OK f10si15263139anh.109
DATA
354 Please start mail input.
Date: 9/19/2010
To: mynameisblablablablabla@gmail.com
From: V1RUZWASHERE@YOUBEENHACKED.COM
Subject: junior biscuits
they r good i here
.
250 Mail queued for delivery.
quit
```

=>De ces faits, on peut donc introduire n'importe quelle adresse mail comme adresse source et le mail sera tout simplement spoofé .

Il suffit juste d'introduire ce qu'on veut dans le champ <MAIL FROM>

La sécurité dans tout ça ?

Sécurité :

- Il n'y a pas de méthodes fiables a 100% pour s'en protéger de l'attaque mail spoofing.
- En effet vu l'implémentation basique du protocole smtp, on ne peut pas connaitre si l'adresse source est spoofée ou pas.

- Mais on peut envoyer par exemple un mail a l'adresse source pour voir si c'est bien lui l'expéditeur du mail.

⇒ D'où la création de SPF et DKIM

SPF (Sender Policy Framework) :

SPF vise à réduire les possibilités d'usurpation en publiant, dans le DNS, un enregistrement (de type SPF ou, autrefois, de type TXT) indiquant quelles adresses IP sont autorisées ou interdites à envoyer du courrier pour le domaine considéré.

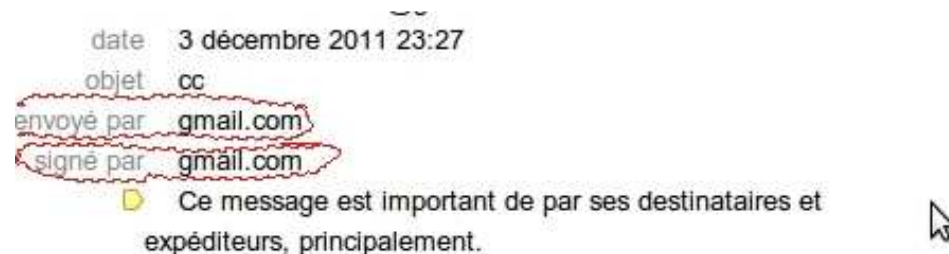
Exemple SPF

```
ietf.org. IN SPF "v=spf1 ip4:64.170.98.0/26 ip4:64.170.98.64/28 ip4:64.170.98.80/28 ip4:64.170.98.96/29 ip4:208.66.40.224/27 ip6:2001:1890:1112:1::0/64 -all"
```

DKIM (DomainKeys Identified Mail) :

Créée en 2004, DKIM fonctionne par signature cryptographique du corps du message et d'une partie de ses en-têtes. Une signature DKIM vérifie donc l'authenticité du domaine expéditeur et garantit l'intégrité du message.

Si un serveur mail applique la norme SPF et DKIM, le mail reçu sera signé et de source sûre.



Sinon, le mail ne sera pas signé et on ne pourra pas être sûr de son expéditeur et il se peut que le mail soit spoofé.

