

2013/2014

M2-Informatique SSI

GULDNER Geoffrey

HURIER Médéric

LACAVE Valentin

SOIHILI Mouchtali



[Rapport d'Attaque n°A008]

SOMMAIRE

I. DESCRIPTION DE L'ATTAQUE.....	3
II. RESULTAT DE L'ATTAQUE.....	4

I. Description de l'attaque

Groupe ciblé

Pour le groupe ciblé on a : le groupe 2

Propriétaires du serveur (les 4 noms)

- DEBRA
- DEBUFF
- KAISER
- JANATI

Nom de l'attaque

Le mail spoofing de la mort qui tue :p

Date de l'attaque

18/03/2014

Catégorie d'attaque

Spoofing

Technique utilisée

Connexion au serveur SMTP de l'université via Telnet (vue dans le TP de madame HERRMANN). Puis usurpation de l'adresse mail de Mr LANUEL afin de récupérer des informations confidentielles (demande de la procédure pour effectuer une attaque sur leur faille laissé volontairement).

```
Ubuntu 13.10 - SR CIRCLEAN - 32bits [En fonction] - Oracle VM VirtualBox
Machine  Écran  Périphériques  Aide
ubuntu@ubuntu-VirtualBox: ~
DATA
354 Enter mail, end with "." on a line by itself
TO: mIm-m2-inf-sssr@etu.univ-lorraine.fr
CC: francine.herrmann@univ-lorraine.fr

Bonjour,

La fin des projets de synthèse approchant à grand pas (le jeudi 27 mars), nous souhaiterions un rapport récapitulatif contenant :
- un bref résumé sur la première partie du projet de synthèse
- une partie récapitulatif des defenses mise en place
- un résumé sur les attaques effectuées et subies

Dans un second temps, nous voudrions avoir avant la fin de la semaine un rapport détaillé sur la manière d'exploiter votre faille par une person
ne exterieure au projet de synthèse par exemple des étudiants de M1 Informatique qui voudraient intégrer le M2-SSI.

Cordialement
YL

*
* Yann LANUEL
*
* Université de Lorraine |L.C.O.M.S.
* UFR MIM |UFR MIM
* Département INFORMATIQUE |Ile du Saulcy
* Ile du Saulcy |57045 METZ CEDEX 1
* 57045 METZ CEDEX 1 |FRANCE
* FRANCE
*
* Tel : (33) (0)3 87 54 71 26
* e-mail: yann.lanuel@univ-lorraine.fr
*
*****
250 2.0.0 s2IFM0En019433 Message accepted for delivery
quit
```

CID

100% : la confidentialité

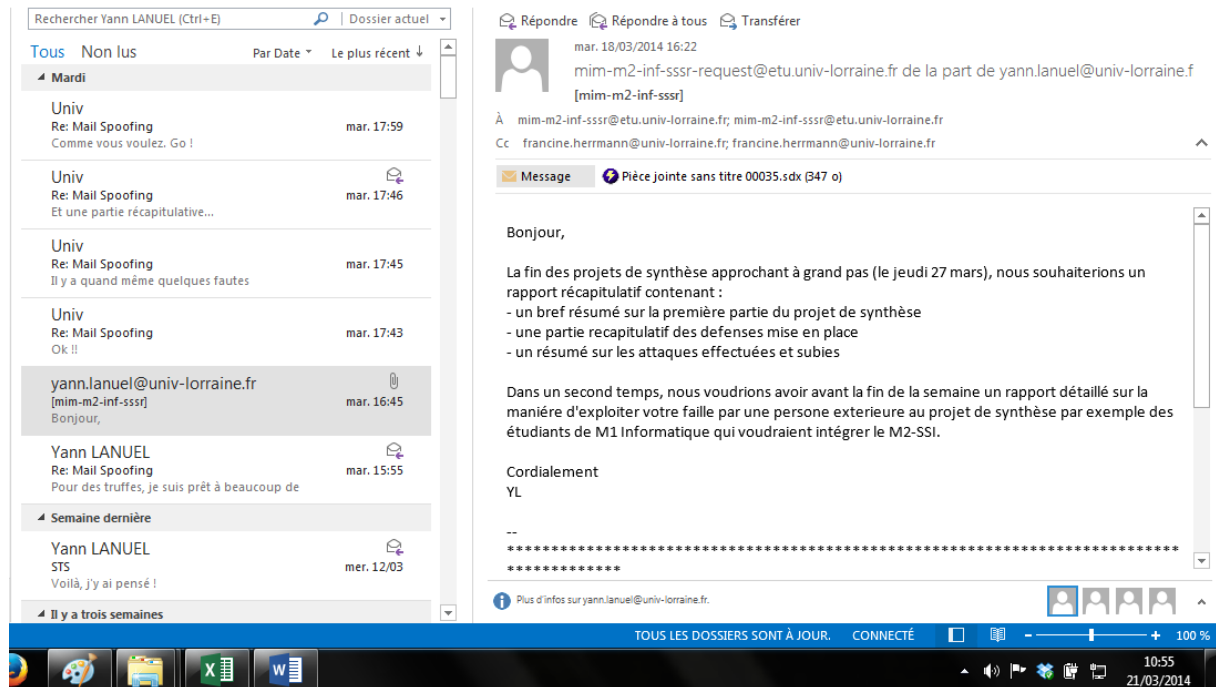
II. Résultat de l'attaque

Description du résultat

Le mail a bien été reçu par l'ensemble de la promo et tous on dut faire un rapport sur leur faille qu'ils doivent envoyer vendredi avant 12h.

Preuve de l'attaque

Comme on peut le voir ci-dessous le mail a été envoyé correctement et bien sous le nom de Yann LANUEL.



Information récupérée et/ou modifiées

Les Informations sont dans votre boîte mail :p théoriquement vous allez recevoir des rapports type mode d'emploi sur l'exploitation de leur faille.

Comment s'en protéger?

Signature et cryptage de mail avec clé privée – public.