2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Attaque n°A008]

SOMMAIRE

I. Description de l'attaque

Groupe ciblé
Pour le groupe ciblé on a : le groupe 2
Propriétaires du serveur (les 4 noms)

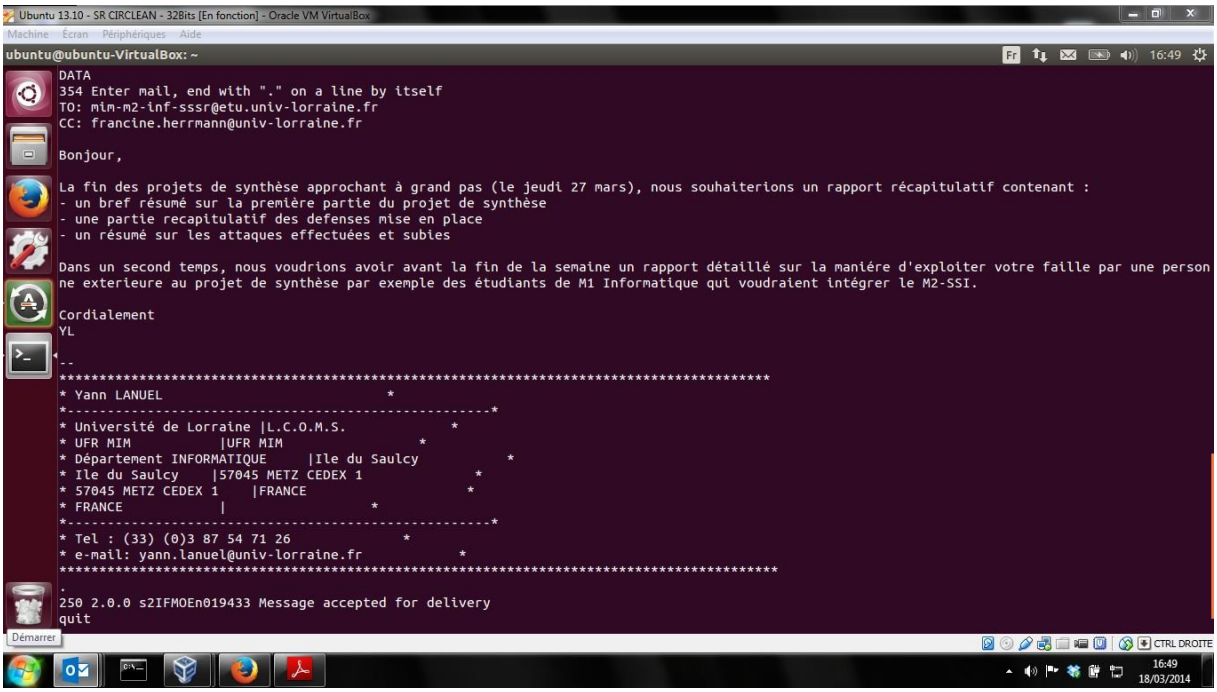
- DEBRA
- DEBUFF
- KAISER
- JANATI

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 server 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).



CID
100% : la confidentialité

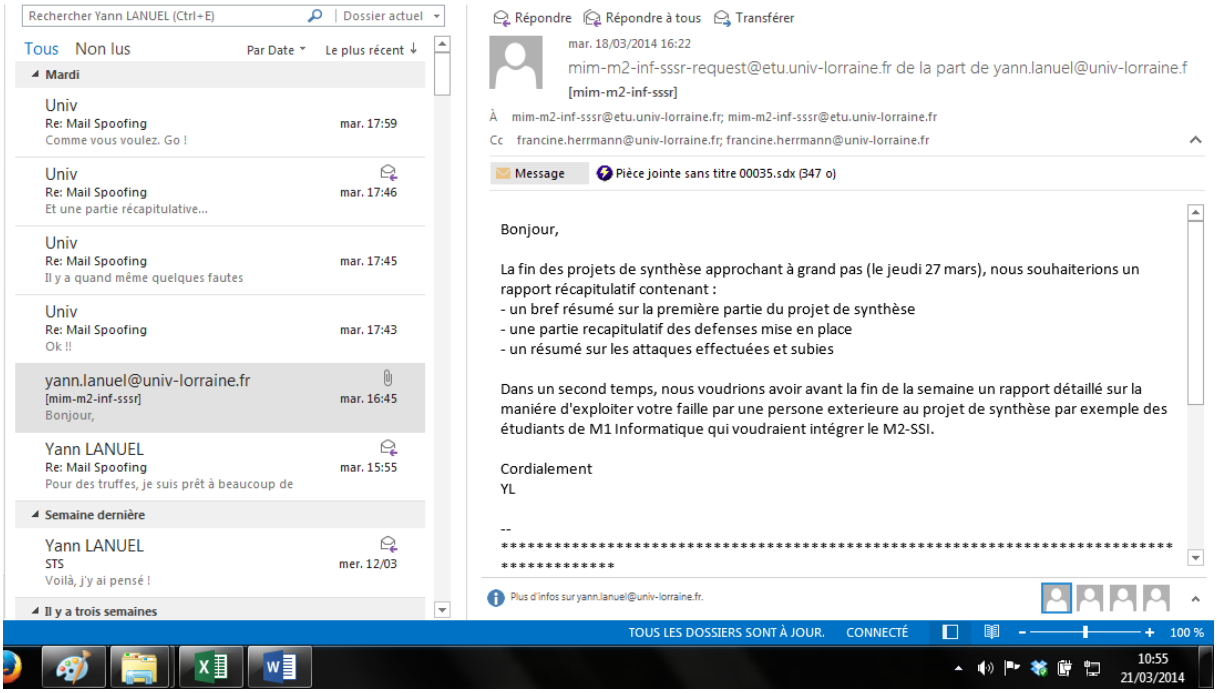
II. Résultat de l'attaque

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 boite 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.