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 testée 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 -->sekejujumimmim Array ([login] ⇒ Array ([result] ⇒ NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki [sessionid] => a4ypti5kpryul9chs1ybifeu44)) Array ([login] => Array ([result] => WrongPass)) 4/2/3/4/0/0 -->sekeiuse20132013 Array ([login] => Array ([result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44)) Array ([login] => Array ([result] => WrongPass)) 4/2/3/4/0/1 -->sekejuse2013mim $Array ([login] \Rightarrow Array ([result] \Rightarrow NeedToken [token] \Rightarrow 31acac877376d554541f2a3374525f8c [cookieprefix] \Rightarrow mediawiki_mediawiki [sessionid] \Rightarrow a4vpti5kprvul9chs1vbifeu44)) Array ([login] \Rightarrow Array ([result] \Rightarrow WrongPass))$ 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 -->sekejusemimmim $Array ([logim] \Rightarrow Array ([result] \Rightarrow NeedToken [token] \Rightarrow 31acac877376d554541f2a3374525f8c [cookieprefix] \Rightarrow mediawiki_mediawiki [sessionid] \Rightarrow a4vpti5kprvul9chs1vbifeu44)) Array ([logim] \Rightarrow Array ([result] \Rightarrow WrongPass))$ 4/2/3/5/0/0 -->sekejumo20132013 Array ([login] => Array ([result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki mediawiki [sessionid] => a4vpti5kpryul9chs1vbifeu44)) Array ([login] => Array ([result] => WrongPass)) 4/2/3/5/0/1 -->sekeiumo2013mim Array ([login] => Array ([result] => NeedToken [token] => 31acac877376d554541f2a3374525f8c [cookieprefix] => mediawiki_mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44)) Array ([login] => Array ([result] => Success [lguserid] => 1 [[gusername] => Roxoradmin [lgtoken] => cb71465464acc7fddab435121ba74bf4 [cookieprefix] => mediawiki mediawiki [sessionid] => a4vpti5kprvul9chs1vbifeu44)) GG go test: sekejumo2013mim ↑ Phrase non trouvée Tout surligner Respecter la casse × Firefox 🕶 🕤 http://localho...sedoff_ext.php × 💪 Partagés avec moi - Google ... × 📴 Rapport final - Google Drive 🗆 🗂 12. Tableaux Utilisateur:Roxoradmin - Wik... × + () @ 172.24.141.124/index.php/Utilisateur:Roxoradmir **₽** □ • ↓ 🔣 Google 🚥 Wawa-Mania 📕 Orange 📳 Facebook 🛅 Linkedin 🍠 Twitter 💭 Twitter 🖟 Twich 🦷 Ogame 🕒 Ogame Tools 🤼 Kongregate 🔂 Call of Duty 🖖 Trophées 🕭 Playstation 🛇 PSN 🔒 Master 🔒 Serveur Web page utilisateur discussion modifier historique supprimer renommer protéger Utilisateur:Roxoradmin hhjjjjjjjjjjjjjjjjjjjjj

Information récupérée et/ou modifiées

Compte administrateur du media wiki

Comment s'en protéger?

Mètre un mot de passe fort et difficilement crackable.