2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Attaque n°A005]

SOMMAIRE

I. Description de l'attaque

Groupe ciblé
Pour le groupe ciblé on a : le groupe 3
Adresse(s) IP cible : 172.24.141.125
Propriétaires du serveur (les 4 noms)

- CONTAL
- GORLT
- KONE
- HEYD

Nom de l'attaque
DOS du wiki

Date de l'attaque
29/01/2014 jusqu'à découverte de l'attaque

Catégorie d'attaque
Attaque par bot python

Technique utilisée
Bot python intelligent threadé utilisant l'API écrite pour le projet de synthèse (Je vais finir par lui donner un nom… : D)

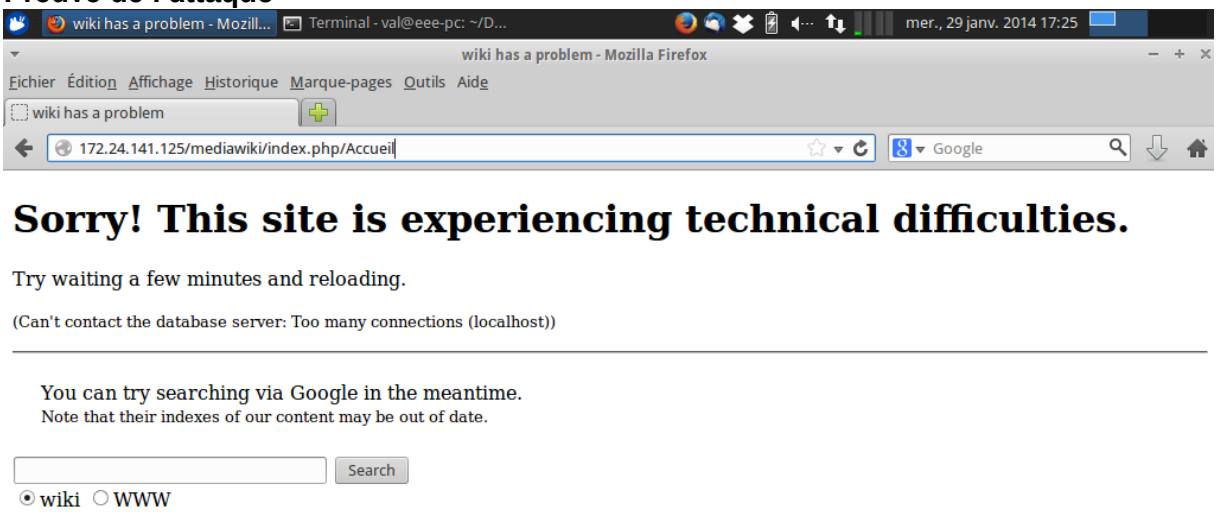
Le bot utilisé est le même que les autres attaques (N°A002- N°A003- N°A004)

Le but de l'attaque est la même que sur le serveur du groupe 2 (N°A004): remplir le disque dur et planter leur machine **MAIS** l'attaque c'est transformée en DOS du wiki : en effet, j'ai lancé 200 threads du robot ciblant le serveur du groupe 3 (j'ai réduit la taille des articles créés mais augmenté le nombre de thread car j'ai remarqué le souci de performance du serveur du groupe 3 et je pensais réussir la même attaque plus rapidement). Le résultat ne s'est pas fait attendre et ce n'étais pas attendu sous cette forme !

CID
L'attaque résulte donc en une indisponibilité du wiki.

II. Résultat de l'attaque

Description du résultat
Déni de service du wiki

Preuve de l'attaque


Information récupérée et/ou modifiées
/

Comment s'en protéger?
Améliorer grandement les performances du serveur.
Bloquer les requêtes trop fréquentes (ban ip par exemple)