# 2013/2014

## M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali


# [Rapport de défense n°D001]

# SOMMAIRE

# I. Description

**N° d'attaque subie**
Attaque n°1 sur notre serveur

**Groupe ayant réalisé l'attaque**
Groupe 2

- DEBUF-KAISER-JANATI-DEBRA (identifié grâce à l'adresse IP: 172.24.141.102)

**Date de l'attaque**
18/01/2014 entre 8h57 et 8h59

**Catégorie d'attaque**
Attaque de type Déni de Service (DoS) sur notre application Web (WikiWikiWeb)

**Technique utilisée**
L'attaquant a envoyé un grand nombre de requête HTTP sur une courte période (3341 requêtes en 2 minutes). Les requêtes n'ont rien de particulier, c'est leur quantité qui a posé problème.

**CID**
L'application WikiWikiWeb était rendue complétement indisponible (disponibilité).

# II. Dégâts subit

### Description des dégâts

L'attaque a porté atteinte à la disponibilité de notre application. Celle-ci n'était plus capable de répondre aux requêtes légitimes des autres utilisateurs (temps d'expiration dépassé).

### Traces / Preuves laissées

Les requêtes ont bien été enregistrées par les logs de notre serveur. Elles sont toutes disponibles dans le fichier que nous avons joins à ce rapport.

# III. Contre(s) mesure(s) mise(s) en place

Cette attaque nous a permis d'identifier plusieurs faiblesses sur notre système:

- mod_evasive (blocage des attaques de types DoS) n'a pas été capable de bloquer ce type d'attaque. Nous allons chercher la cause de cette défaillance.
- nous manquons d'outils de supervision pour surveiller le traffic et les performances de notre système. Nous comptons installer un logiciel capable d'assurer cette fonction: Munin.
- les logs ne sont pas facilement exploitables. Il faudrait mettre en place des outils pour gérer cette fonction, mais ce n'est pas prévu à court terme.

Plus globalement, nous devons revoir les performances globales de nos applications et de notre serveur web. C'est une partie très longue et fastidieuse, nous devrons la répartir dans le temps.
Nous avions prévu d'utiliser un serveur web plus performant dans le cahier des charges. Malheureusement, ce dernier s'est révélé incompatible avec Mediawiki. Cette attaque était prévisible, mais difficilement évitable sans des efforts conséquents.