2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Attaque n°A001]

SOMMAIRE

I. Description de l'attaque

Groupe ciblé
Pour le groupe ciblé on a : le groupe 2
Adresse(s) IP cible : 172.24.141.119
Propriétaires du serveur (les 4 noms)

- DEBUF
- KAISER
- DEBRA
- JANATI

Nom de l'attaque
Aspiration de site Web

Date de l'attaque
16/01/2014 pendant la présentation de leur projet…

Catégorie d'attaque
Vol d'informations

Technique utilisée
Script Python alimenté par un fichier index Git.

CID
Atteinte à la confidentialité du code source et de la base de données.

II. Résultat de l'attaque

Description du résultat

Notre script est disponible en pièce-jointe. Il lit un fichier index de Git pour extraire des chemins de fichier. Puis, il crée des requêtes HTTP pour télécharger le contenu. Le script index de Git a été récupéré par navigation manuelle sur le dossier 172.24.141.119/.git/. Il était impossible de lister le répertoire, mais la structure d'un dossier git étant identique d'un répertoire à l'autre, il est facile d'identifier les fichiers sensibles. Cette faiblesse a été identifiée suite à un scan NMAP le 16/01/2014.

Preuve de l'attaque

Vous pourrez trouver en pièce-jointe le code source de leur application et le script SQL.

Information récupérée et/ou modifiées

Nous avons récupéré tout le code source et toute la base de données du groupe 2 (structure et contenu).