2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Attaque n°A006]

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
slowloris: envoie de requête en simulant une faible bande-passante.

Date de l'attaque
29/01/2014

Catégorie d'attaque
Déni de Service

Technique utilisée
En envoyant des requêtes octet par octet, on peut simuler un client web très lent (c'est le cas par exemple pour un téléphone mobile sur bande GSM).
Ces requêtes sont très lourdes à gérer pour le serveur, car les délais de transferts occupent les processus dédiés à traiter les autres demandes. Si on envoie suffisamment ce type de requête, on peut saturer le serveur en quelques secondes.

Pour utiliser cette attaque, nous avons utilisé le script slowhttptest:

- slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u http://172.24.141.211 -x 24 -p 3

Plus d'informations à cette adresse:

- https://code.google.com/p/slowhttptest/

CID
Site indisponible à 95% (selon le délai de rejet par expiration de la requête).

II. Résultat de l'attaque

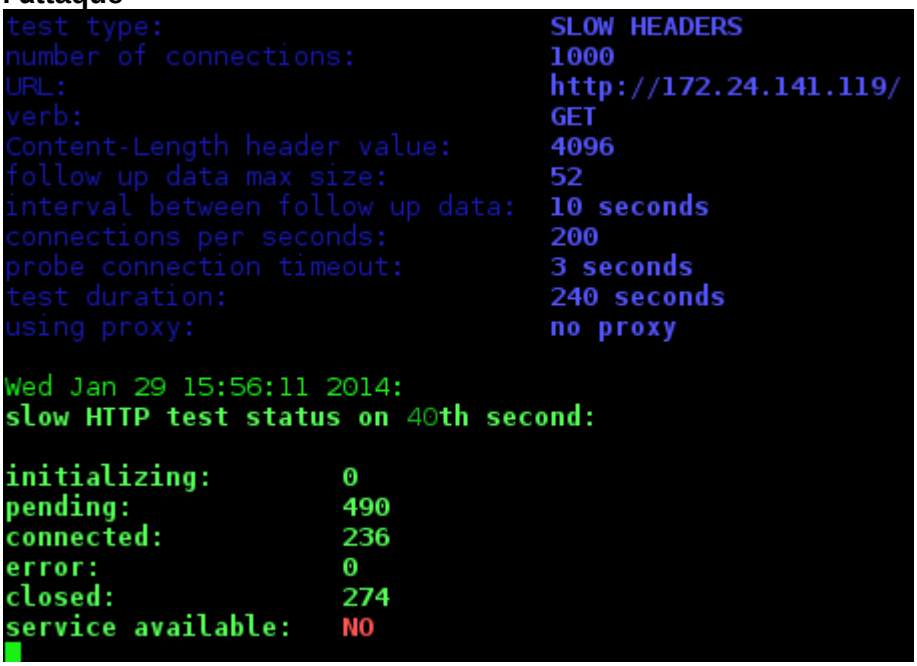
Description du résultat

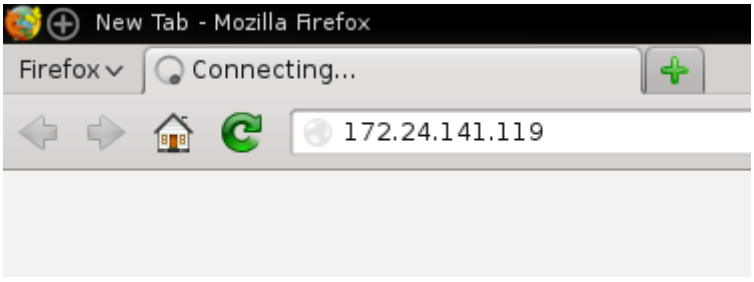
Les captures suivantes montrent le script d'attaque en cours de fonctionnement et le résultat sur le navigateur. Les requêtes restent en cours de chargement, sans jamais aboutir.

Notre site est également sensible à ce type d'attaque. Nous comptions nous en prémunir en installant un serveur web basé sur un modèle asynchrone (Cherokee, Nginx).

Il est possible de s'en prémunir, mais les règles sont très complexes et peuvent nuire au fonctionnement normal (ex: priver d'accès les clients mobiles).

Preuve de l'attaque





Information récupérée et/ou modifiées

/

Comment s'en protéger?

/