2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Attaque n°A004]

SOMMAIRE

I. Description de l'attaque

Groupe ciblé
Pour le groupe ciblé on a : le groupe 2
Adresse(s) IP cible : 172.24.141.124
Propriétaires du serveur (les 4 noms)
- DEBUF
- KAISER
- DEBRA
- JANATI

Nom de l'attaque
Flood du wiki

Date de l'attaque
23/01/2014 - 24/01/2014

Catégorie d'attaque
Attaque par bot python

Technique utilisée
Bot python intelligent threadé utilisant l'API écrite pour le projet de synthèse

Le bot fonctionne de cette manière:
1. Il créé des articles de manière aléatoire sur le wiki cible, les articles sont de taille conséquente

Le bot prend plusieurs options:
- --host => la cible du bot
- -l => le login pour le wiki
- -p => le password du login pour le wiki
- -alfu => le bot vas "Flush" tous les articles (les effacer)
- -alfo => le bot vas flooder le wiki avec plein d'articles aléatoires
  - (sois --aflu sois --aflo, pas les deux en même temps)
- --silent => le bot affiche le minimum de texte
- -nt => le nombre de thread à lancer (défaut:1)
- -s => le temps de mise en veille (défaut:60)
- -la => taille de l'article à créer pour flooder (nombres de caractères de l'article)

Le bot est intelligent car:
1. Il peut se connecter en utilisant un login et un MDP de passe fournit en paramètre
2. Il "flood" le wiki et adapte sa rapidité aux systèmes de défense mis en place: si il est repéré, il va continuer son travail mais de façon plus discrète:
   - il va augmenter le temps entre chaque création d'article jusqu'à ce qu'il ne soit plus repéré.

Le bot a été lancé le 23/01/2014 vers 15h30 sur 3 machines (au fond de la salle) et l'attaque a été concluante le 24/01/2014 vers 11h50.

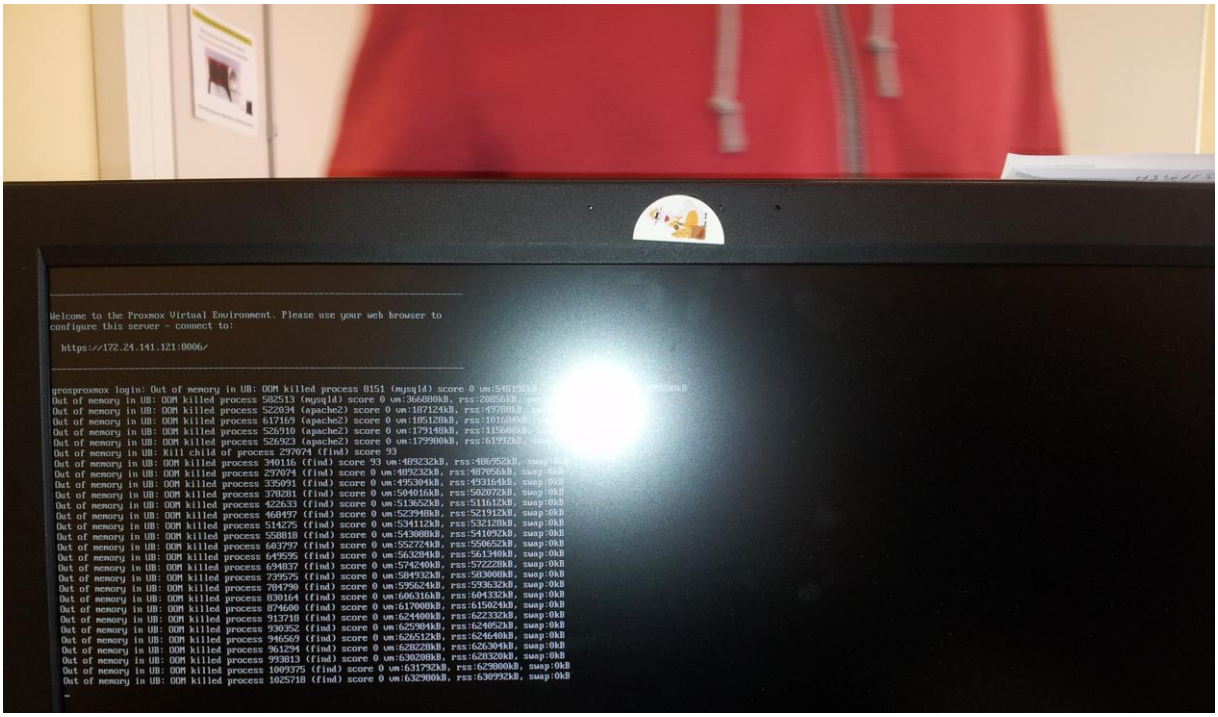
CID
Le bot va toucher la disponibilité du wiki voire du serveur en remplissant la base de donnée d'articles. On ne pourra plus créer d'articles et le serveur risque de planter.

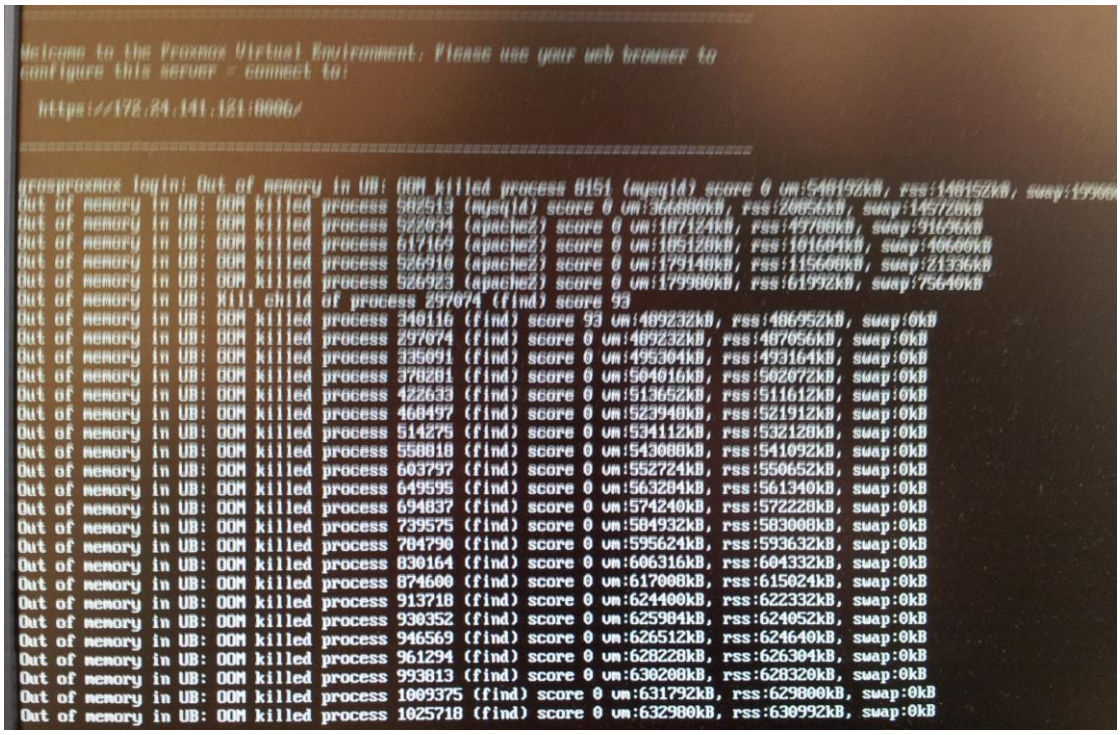
II. Résultat de l'attaque

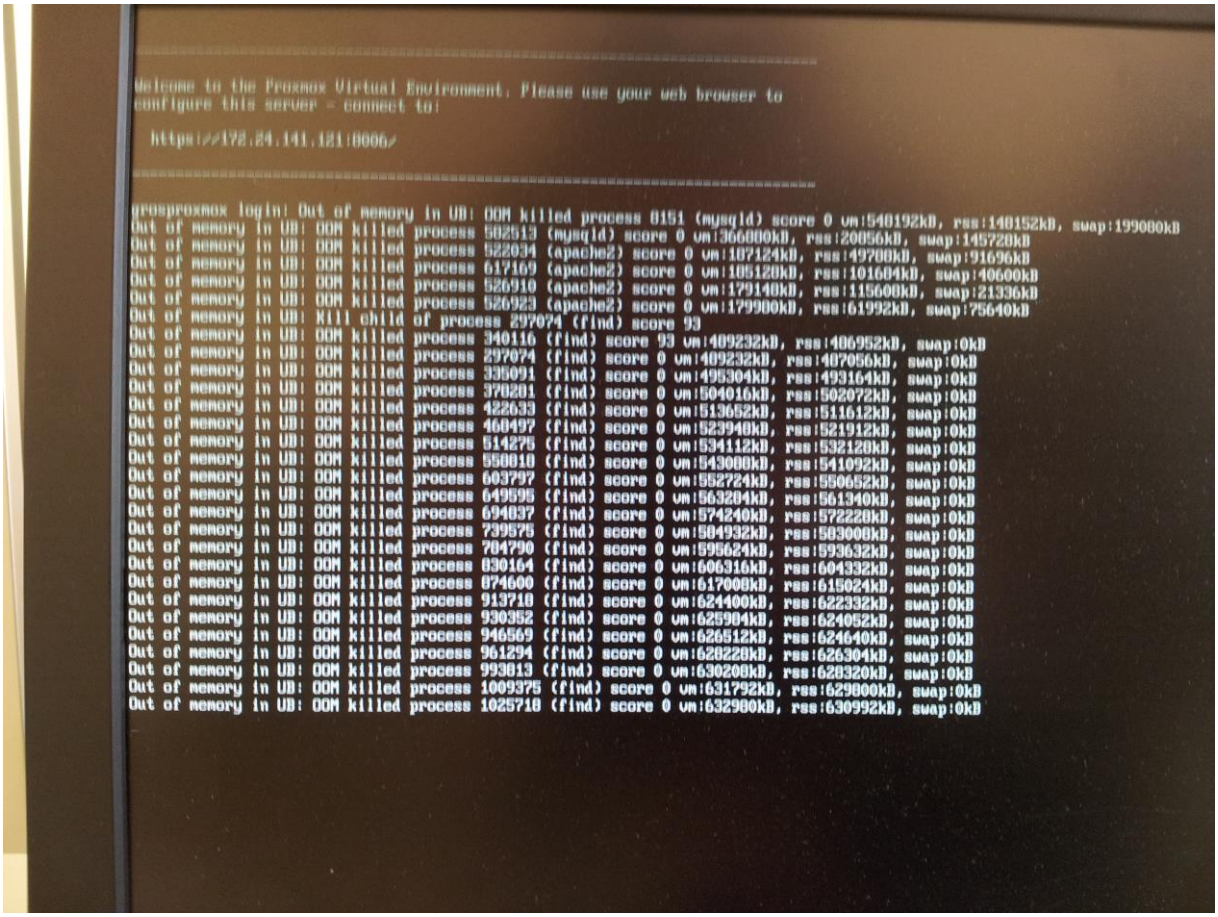
Description du résultat

Déni de service

Preuve de l'attaque







Information récupérée et/ou modifiées

/

Comment s'en protéger?

- Désactiver l'API publique et la mettre en localhost, interdis pour le projet.
- Avoir un IPS qui bloque le robot: il est intelligent donc inutile.
- Bloquer l'API pour les gens non connectés: le bot peut se connecter donc inutile (il est facile d'automatiser la création d'un compte et de s'y connecter ensuite)
- Bloquer les IP qui font trop de demandes: oui mais il est possible de ralentir manuellement le robot