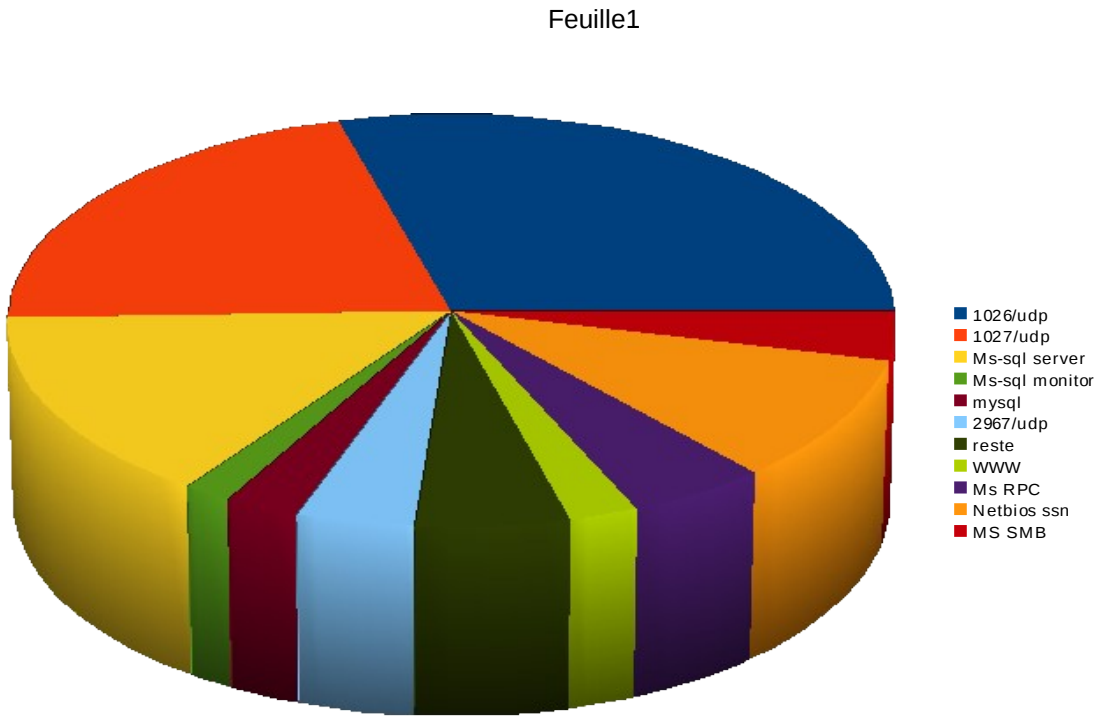
RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 27 Novembre 2007

Statistiques des scans



Statistiques

- Les scans
  - Les scans microsoft sont majoritaires (137,139,445 mais aussi 1434)
  - Constance des tests VNC et SSH
- en applicatif
  - les connexions MSSQL en grande proportion
  - persistance des brute force SSH et surtout des serveurs FTP
  - apparition de plus en plus massive de tests web

Statistiques

Les tests web sont faits sans aucune intelligence, uniquement par "brute force". Sur quarante jours :

- 1731 phpshell
- 37450 winnt
- 54473 w00tw00t.at.ISC.SANS.DFind
- 65914 phpmyadmin
- 64647 explorations d'un spampoison
- 114673 tentatives d'include à l'aveugle
- 134510 GET /unauthenticated/..%01/..%01/..%01/..%01/
- ...

Freewvs : un micro nessus web

- http ://source.schokokeks.org/freewvs/
- recherche en local les versions des applications
- compare avec une base
- recherche, souvent, dans les fichiers versions
- indique la version à installer

Freewvs : avantages

- rapide
- pas compliqué
- facilement évolutif
- utile pour ne pas oublier une vieille application dans un coin

Freewvs : inconvénients

- très jeune
- de nombreux logiciels manquent à l'appel
- il manque une structure d'accueil pour les contributeurs

flashsec : La sécurité du flash

- https ://www.flashsec.org
- les intrusions se basent désormais sur le client
- les clients web se sécurisent de plus en plus
- quid des modules et extensions ?
- quid de flash ?
- qu'en est-il des mécanismes de protections (javascript, DNS pinning, etc.)
  - sont-ils appliqués par les modules ?
- le site pour savoir comment nous allons nous faire piéger.

Les actualités

- Tor : Dan egerstad capture du trafic et des comptes d'ambassades.
- Les Anti-virus sont-ils dangereux ?
- 0,5 million de serveurs SQL vulnérables
- Snort 3.0 : bientôt multithread ?

- Retour d'expérience sur un déploiement VMWare à grande échelle

  Eric Spesotto, CLS

- Jouons avec les clés USB

  Pierre-Yves Bonnetain, B & A Consultants.