MEETUP TECHNOLOGIES WEB & LOGICIELS LIBRES À MONTRÉAL

MONTRÉAL, MARDI 23 JANVIER 2018

À PROPOS DE CE MEETUP

- Technologies Web à base de Logiciels Libres
- Partage ouvert de savoir-faire et d'expertise
- Rencontres pour la communauté LL de Montréal

Technologies **Web**
&& Logiciel **Libre**

evolix

Hébergement et Infogérance en Logiciels Libres

- Impartition TI
- Serveurs Linux/BSD
- Support technique 24h/24 7j/7
- Hébergement géré (Dédié/Cloud)
- Architecture/Conseil/Formation

INITIATION À LA (CYBER-)SÉCURITÉ

SOMMAIRE

- Théorie sur la sécurité
- Pistes pour sécuriser son serveur
- Questions/discussions

QU'EST CE QUE LA SÉCURITÉ

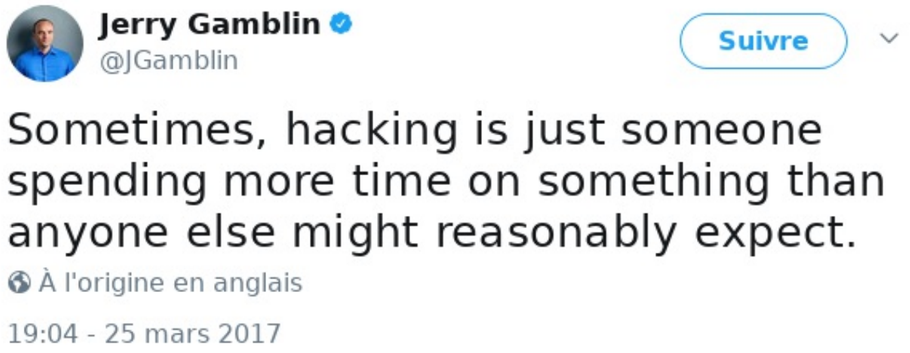
- « la sécurité est l'état d'une situation présentant le minimum de risque » © Wikipedia
- Il n'y a pas de solution magique

JE N'INTÉRESSE PERSONNE

- Pas forcément directement (proxy, envoi de spam etc)
- Mais directement aussi (ransomware/cryptovirus etc)

COMMENT AMÉLIORER SA SÉCURITÉ

- autrement dit, baisser les risques
- en baissant l'intérêt pour un attaquant
- en augmentant le coût de l'attaque
- Le risque 0 n'existe pas



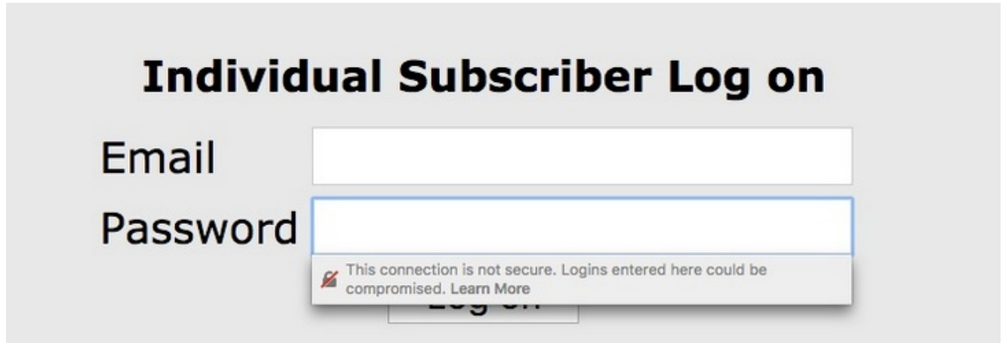
DRESSER SON MODÈLE DE MENACE

- Que protéger ? (données des clients ? sa réputation ?)
- De qui ? (volontairement ciblé ? *drive-by attack* VS concurrent / client mécontent)
- Quelle probabilité ?
- Quelle conséquence en cas d'échec ?
- À quel prix le protéger ?

CONSEILS DE BASE POUR AUGMENTER LE COÛT

- Limiter sa surface d'attaque
- Utiliser un gestionnaire de mot de passe
- Utiliser de la double authentification (2FA)
- Utiliser du chiffrement fort de bout-en-bout (*E2EE*) et au repos
- Appliquer **rapidement** les mises à jour de sécurité

CONSEILS DE BASE POUR RÉDUIRE L'INTÉRÊT

- Stocker le minimum de données
- Rester humble
- 

HOPE FOR THE BEST - PREPARE FOR THE WORST

- Plannifier comment réagir en cas de problèmes pour ne pas être pris au dépourvu
- Avoir des sauvegardes (des **vraies** sauvegardes)

PISTES POUR SÉCURISER SON SERVEUR

LA BASE : GARDER SON SYSTÈME À JOUR

80 % des attaques en moins

- sous Debian, unattended-upgrades + suivi par mail
- Pour les libs, CMS, frameworks et autres outils installés à la main : suivre régulièrement les mises à jour… ou préférez les paquets de votre distribution!
- Attention aux anciennes version des libs chargées en mémoire (paquet needrestart sous Debian)
- Pour Docker, votre image est-elle mise à jour si libXYZ est mise à jour? Sinon reconstruisez-là vous-même

PROTECTION DEPUIS L'EXTÉRIEUR

- Qui a accès physiquement à votre serveur?
- Qui a accès virtuellement à la machine hôte de votre VPS?
- Quels logiciels sont exposés sur le réseau :
  # netstat -utpln |grep -v 127.0.0.1
- Changez l'URL du backoffice, évitez « admin » comme login et mettez un mot de passe fort
- Une authentification HTTP (htpasswd) est toujours plus fiable que l'authentification du CMS
- Pare-feu applicatif : mod-security pour Apache, Naxsi pour Nginx, fail2ban pour le reste

ISOLATION SUR LE SERVEUR

- Isolation des comptes (permissions Unix, Apache ITK), base de données…
- Limiter l'accès à l'extérieur (récupération de code malicieux) : proxy/pare-feu en sortie
- Limiter l'accès en écriture aux répertoires d'upload/cache des applications web

MENACE INTERNE

- Contrôle des accès sur le serveur : un compte par admin + sudo
- Gestionnaire de mots de passe partagé, avec ACL
- Au delà du serveur : accès au centre de données, à l'interface de gestion de l'hébergeur, vos DNS…
- Tenir une liste de qui à accès à quoi

EXEMPLE POUR RETRACER UNE INJECTION DE CODE

Indices : mailq pleine de spam, contenu illégitime sur le site, trafic réseau anormal…

- Lister les fichiers modifiés récemment :

```
# find -mtime -3 -ls
```

- Fichiers .php dans un répertoire d'upload :

```
# find wp-content/uploads/ -name "*.php"
```

- Fichiers avec de très longues lignes (base64) :

```
# find -name "*.php" -exec wc -L {} \; |sort -n |tail
```

EXEMPLE POUR RETRACER UNE INJECTION DE CODE

Trouver la faille :

- Trouver les premiers appels au fichier :

```
# zgrep wp.conf.php /var/log/apache2/access.log*
192.0.2.223 - - [30/Nov/2017:09:55:46 -0400] "GET /wp.conf.php HTTP/1.0" 200
255 […]
…
```

- Rechercher les POST avant cette heure là :

```
# zgrep POST /var/log/apache2/access.log.18.gz |grep -v " 404 " |less
192.0.2.223 - - [30/Nov/2017:09:52:18 -0400] "POST /wp-
content/themes/sketch/functions.php HTTP/1.1" 200 186 […]
…
```

QUESTIONS ET DISCUSSIONS

POUR EN SAVOIR PLUS...

- Site : web-libre.ca
- Wiki Evolix : wiki.evolix.org
- Articles : blog.evolix.ca
- Twitter : @EvolixCanada
- Courriel : hello@evolix.ca