Sécurité élémentaire

Voici des conseils que n'importe quel utilisateur pourra appliquer pour améliorer la sécurité de son système. Les sujets pointus ne seront pas abordés, vous ne trouverez que les informations élémentaires permettant à chacun de mettre en place un niveau de sécurité décent.

Utiliser des mots de passe forts

La robustesse de votre mot de passe dépend de trois paramètres :

1. longueur : un mot de passe long est un mot de passe fort. Diverses recommandations suggèrent au moins 8 caractères.
2. complexité : plus les caractères sont variés, plus le mot de passe est fort.
3. déductibilité : la difficulté pour un attaquant de dériver votre mot de passe à partir d'une autre information (tel que votre nom)

Assurez-vous de changer votre mot de passe régulièrement de manière à ce que si quelqu'un réussi à le forcer, il devra recommencer par la suite.

Consultez également The ultimate guide for creating strong passwords (*Le guide ultime pour créer des mots de passe forts* - en anglais).

Désactiver les services inutiles

Avec Slackware, il suffit de rendre non-exécutable n'importe quel fichier rc dans `/etc/rc.d` servant à démarrer un service que vous n'utilisez pas. Par exemple :

```
chmod a-x /etc/rc.d/rc.gpm-sample
```

Avec moins de services actifs, vous encourrez moins de risques qu'un bug puisse être exploité à distance par un attaquant.

Mettre en place un pare-feu

Avec Slackware, la façon la plus simple pour cela est d'utiliser Easy Firewall Generator (*Générateur facile de pare-feu*) adapté par Alien Bob. Vous n'avez qu'à générer des règles de pare-feu, copier le résultat dans un fichier `/etc/rc.d/rc.firewall`, et le rendre exécutable.

```
chmod a+x /etc/rc.d/rc.firewall
```

D'autres possibilités existent tels que des programmes de génération avec interface graphique, tel que Firewall Builder.

X -nolisten tcp

Par défaut le serveur Xorg écoute sur le port 6000 pour les connexions distantes. Dans certains cas vous pouvez utiliser cette possibilité, mais si ce n'est pas le cas alors la désactiver est une bonne idée.

Le moyen le plus simple est de créer un fichier `~/.xserverrc` **OU** `/etc/X11/xinit/xserverrc`.

xserverrc

```
#!/bin/sh

exec /usr/bin/X -nolisten tcp
```

Vous pouvez indiquer d'autres options pour X dans ce même fichier si nécessaire.

Avec Slackware, l'écoute pour les requêtes XDMCP est désactivée par défaut dans xdm et kdm, ce qui est donc sécurisé par défaut. Certains dirons alors : “pourquoi désactiver Xorg dans ce cas ?” Il est toujours bon de ne pas faire confiance aveuglément aux fichiers de configuration, comme cela se voit dans un ancien rapport de bug lorsque xdm ignorait son fichier de configuration.

Lister les ports ouverts

Quelques commandes pour vérifier quels ports sont ouverts :

```
nmap localhost
nmap VOTRE_ADDRESSE_IP_PUBLIQUE
netstat -luntp
```

Votre adresse IP externe peut être connue via des sites tel que http://whatismyipaddress.com/.

Si vous ne savez pas à quoi correspond tel ou tel port, consultez la liste des ports logiciels sur Wikipédia.

Rechercher les malwares sur votre système

Les programmes suivants sont utiles pour rechercher les rootkits et virus :

- rkhunter
- ClamAV

Bien qu'il existe fort peu de malwares sous Linux, cela reste une bonne idée de faire une recherche de temps à autre.

Sources

- Version originale par htexmexh
- Traduction par Ellendhel

- The ultimate guide for creating strong passwords
- http://slackwiki.com/Basic_Security_Fixes
- http://slackwiki.com/Security_Assessment_using_Nmap

security, software, author htexmexh