Principes généraux de la sécurité

Objectifs de cette section

Pourquoi Linux est-il un OS relativement sécurisé ?

Qu'est-ce que l'utilisateur root sur les distributions Linux ?

En quoi l'utilisateur root diffère des autres utilisateurs ?

Pourquoi les systèmes d'exploitation Linux sont souvent évités par les attaquants ?

Quelles sont les implications au niveau sécurité de l'utilisation d'un système OpenSource ?

La gestion des logiciels sur Linux.

Le rôle et les responsabilités de l'administrateur du système.

Linux est-il sécurisé ?

La sécurisation d'un système Linux

Il n'existe pas de système d'exploitation 100% sécurisé.

La sécurité correspond à une série de compromis à accepter et faire accepter.

- Confort et Sécurité sont-ils opposés ?

Evaluation des risques

Quelle est la sévérité, l'impact du risque ?

Quelle est la probabilité que la faille soit utilisée ?

Quel est le coût associé à l'atténuation de ce risque ?

Quelle est l'efficacité des contre-mesures possibles ?

Linux est sécurisé ?

Linux est seulement aussi sécurisé que vous le décidez.

- Linux peut être configuré de manière non sécurisée.

L'utilisateur peut utiliser des autorisations « laxistes » sur des fichiers qu'il utilise (permettant ainsi à un autre utilisateur de pouvoir les consulter).

Des erreurs de configuration et d'administration peuvent rendre le système moins sécurisé.

Les mots de passe des utilisateurs peuvent être faciles à deviner ou à cracker.

Les données peuvent être transmises en clair sur le réseau.

Des logiciels vérolés peuvent être installés sur le système.

Manque de formation ou de sensibilisation à la sécurité.

Le piège !

Attention, ce n’est pas parce que vous utilisez Linux que votre système est forcément entièrement sécurisé.

Des failles existent même sur les systèmes Linux.

Beaucoup de serveurs web sont hébergés sur des machines Linux et sont pourtant parfois remplis de failles de sécurité.

La sécurisation de votre système est une action de tous les jours, ne restez jamais sur vos acquis…

Qu’est-ce qui fait la sécurité de Linux ?

Système Multiuser

Linux est un système Multiuser : plusieurs utilisateurs peuvent se connecter sur l'équipement et peuvent l'utiliser en même temps.

L'utilisateur « root » est le superutilisateur.

- Il peut effectuer toutes les tâches sur le système.
- Nécessaire pour l'installation de logiciels, la configuration du réseau, la gestion des autres utilisateurs.
- Même si des fichiers ont été créés et « cachés » par d'autres utilisateurs, root y a quand même accès.
- Attention donc si un attaquant réussi à obtenir l'accès de l'utilisateur root.

Les autres comptes sont dits « normaux » :

- Peuvent être utilisés par exemple par les autres personnes ou par des applications et des services.

Avantages d’un système multiuser

Utilisation des permissions sur les fichiers.

Tous les fichiers d’un système Linux possède un propriétaire.

Des permissions spécifiques peuvent être accordées aux autres comptes et utilisateurs si nécessaire.

Obtenir l’accès à un des comptes ne va donc pas compromettre nécessairement tout le système.

Avantages d’un système multiuser (2)

Chaque processus est lancé par un compte spécifique qui devient son propriétaire.

Chaque compte peut administrer les processus qui lui appartiennent (dont il est le propriétaire).

- Possibilité de killer les processus par le compte propriétaire.
- L’utilisateur root peut effectuer n’importe quelle action sur les processus.

Les attaquants sont paresseux !

Il y a bien plus d'ordinateurs sous Windows que sur Linux.

Linux est souvent utilisé par des professionnels de l'informatique, ou des passionnés qui font plus attention à la sécurisation du système.

Les concepteurs de virus conçoivent leur programme pour fonctionner sur des machines windows la plupart du temps.

Linux est Open Source

Le code source est disponible.

Vous n’avez pas besoin de faire confiance à une société particulière (comme Microsoft ou Apple).

Très difficile de faire fonctionner du code malveillant pour compromettre entièrement un système Linux.

L’utilisation de l’OpenSource augmente la possibilité que des utilisateurs découvrent des failles et partagent leur découverte pour créer des patchs.

Les failles de sécurité de Windows ne peuvent être patchées que par Microsoft, qui mettent parfois des années avant de sortir de bons patches de sécurité.

Gestion centralisée des logiciels

Sur Linux, les paquets sont gérés par des « package managers »

Les paquets correspondent à un ensemble de fichiers qui permettent à une application de fonctionner correctement.

Les « package managers » comme aptitude permettent de supprimer et d'installer de nouveaux paquets en allant chercher les informations dans les repositories (dépôts).

- Les paquets sont signés par la clé publique du dépôt officiel, ce qui permet d'être sur qu'ils sont « de confiance ».
- En utilisant des dépôts officiels, vous pouvez être surs que les logiciels sont libres de virus, ou de malware.

Installation de logiciels

Sur Linux :

- Recherche sur le dépôt et installation du paquet grâce au « package manager ».

Sur Windows :

- Recherche sur Internet et installer le logiciel depuis un tiers.
- Les logiciels ne sont pas tous testés en amont.
- Le code source n’est pas disponible (la plupart du temps) => patchs de sécurité publiés uniquement par le développeur.
- Vous n’êtes pas vraiment sur de ce que vous installez.

Règles de bonnes pratiques

Minimiser les logiciels et services

Si vous n’avez pas besoin d’une partie du logiciel, alors ne l’installez pas.

Si vous n’avez pas besoin d’un service, alors ne le démarrez pas.

Si vous n’avez plus besoin d’un logiciel ou d’un service, alors arrêtez-le et procédez à sa désinstallation.

Lancer des services sur des systèmes séparés

Permet de minimiser le risque que si un service est compromis, alors l'attaquant ne puisse pas compromettre d'autres services en se basant sur le premier.

Chiffrer les transmissions de données

Protège contre l'écoute du trafic par un attaquant, ou la capture d'informations grâce aux attaques Man-In-The-Middle.

Exemples :

- Utiliser SFTP plutôt que FTP.
- Utiliser SSH plutôt que telnet.
- Utiliser SNMPv3 plutôt que SNMPv1 et SNMPv2.
- Utiliser HTTPs plutôt qu'HTTP.

Ne partagez pas de comptes

Chaque personne doit posséder son propre compte utilisateur.

Chaque application ou service doit également posséder son propre compte utilisateur.

Le partage de comptes rend difficile les audits de sécurité.

Désactiver l'identification directe en root

Il faut toujours désactiver la capacité de se loguer directement sur la machine avec l'utilisateur root.

On peut cependant laisser les utilisateurs s'identifier avec leur compte personnel, puis leur permettre de switcher vers le compte root.

- Un log est inscrit sur le système, permettant aux audits de sécurité d'être plus efficace par la suite.

Privilégier l'utilisation du « sudo » pour permettre aux utilisateurs d'effectuer des actions root de manière temporaire.

- Un log est inscrit sur le système avec l'utilisateur qui a effectué une commande avec le « sudo »

Utiliser l’authentification avec plusieurs facteurs

Quelque chose que vous connaissez + quelque chose que vous avez.

Par exemple :

- Mot de passe du compte, puis un SMS qui vous délivre un mot de passe temporaire.
- Mot de passe du compte et empreinte digitale.

Le « Least Privilege »

Aussi connu sous le mot de « Principle of Least Authority ».

Exemple :

- N’utiliser les privilèges Root, uniquement pour effectuer les tâches qui les nécessitent.
- Eviter au maximum de lancer des services en tant qu’utilisateur root.
- Utiliser des permissions restrictives pour n’autoriser les personnes et services à n’effectuer que les tâches qu’ils ont besoin de faire.

Vérifier l’activité du système

Regarder régulièrement les logs du système, peut permettre de détecter un comportement anormal.

Envoyer si possible les logs sur un équipement dédié à leur centralisation.

Utiliser un pare-feu

Linux possède déjà par défaut un système de pare-feu grâce à « Netfilters » et « Iptables ».

Utiliser la notion de « Least Privilege » pour n’autoriser que les connexions réseaux nécessaires.

Chiffrement des données

Procéder au chiffrement des données sensibles sur votre disque dur.