Sécurité des systèmes Linux

Karim Sayadi

Institut Supérieur d'Informatique
et de Mathématiques de Monastir

23 octobre 2010

Sécurité des systèmes informatiques

La sécurité des systèmes informatiques est une activité du management du système elle est égale à celle de son maillon le plus faible, et peut s'évaluer suivant plusieurs critères

- Disponibilité.
- Intégrité.
- Confidentialité.

Sécurité des systèmes informatiques

La sécurité des systèmes informatiques est une activité du management du système elle est égale à celle de son maillon le plus faible, et peut s'évaluer suivant plusieurs critères

- Disponibilité.
- Intégrité.
- Confidentialité.

Sécurité des systèmes informatiques

La sécurité des systèmes informatiques est une activité du management du système elle est égale à celle de son maillon le plus faible, et peut s'évaluer suivant plusieurs critères

- Disponibilité.
- Intégrité.
- Confidentialité.

Particuliers et Entreprises

Pour les particuliers

- Tranquillité ;
- stabilité du système : Éviter les intrusions.

Pour les entreprises

- La sécurité est un enjeu majeur d'une politique économique ;
- Existence des boites d'espionnage qui peuvent récupérer un nombre colossales d'informations,y compris vitales ;
- Destruction de matériel..

Particuliers et Entreprises

Pour les particuliers

- Tranquillité ;
- stabilité du système : Éviter les intrusions.

Pour les entreprises

- La sécurité est un enjeu majeur d'une politique économique ;
- Existence des boites d'espionnage qui peuvent récupérer un nombre colossales d'informations,y compris vitales ;
- Destruction de matériel..

Particuliers et Entreprises

Pour les particuliers

- Tranquillité ;
- stabilité du système : Éviter les intrusions.

Pour les entreprises

- La sécurité est un enjeu majeur d'une politique économique ;
- Existence des boites d'espionnage qui peuvent récupérer un nombre colossales d'informations,y compris vitales ;
- Destruction de matériel..

Principales Menaces

Les principales menaces effectives auxquelles un système d'intrusion peut être confronté sont :

- Un utilisateur du système : insouciance, ou mauvaise manipulation ;
- Une personne malveillante : utilisant des failles connues et non corrigées par les systèmes ;
- Un programme malveillant : ouvrant la porte a des intrusions ou modifiant les données.

Une fois les risques énoncés passant aux méthodes de protections.

Principales Menaces

Les principales menaces effectives auxquelles un système d'intrusion peut être confronté sont :

- Un utilisateur du système : insouciance, ou mauvaise manipulation ;
- Une personne malveillante : utilisant des failles connues et non corrigées par les systèmes ;
- Un programme malveillant : ouvrant la porte a des intrusions ou modifiant les données.

Une fois les risques énoncés passant aux méthodes de protections.

Principales Menaces

Les principales menaces effectives auxquelles un système d'intrusion peut être confronté sont :

- Un utilisateur du système : insouciance, ou mauvaise manipulation ;
- Une personne malveillante : utilisant des failles connues et non corrigées par les systèmes ;
- Un programme malveillant : ouvrant la porte a des intrusions ou modifiant les données.

Une fois les risques énoncés passant aux méthodes de protections.

Utiliser un par-feu

- Le par-feu joue le rôle de contrôleur, il filtre les connexions qui entrent et qui sortent de votre ordinateur
- Bloque ce qui lui semble indésirables selon ce que vous lui avez paramétré comme politique de sécurité
- chaque ordinateur, possède plusieurs portes d'entrés possibles (Les portes d'entrée et les portes de sorties ne sont pas les mêmes)
  Objectif : Bloquer par défaut toutes les portes, et autoriser seulement celles dont vous avez besoin, celles que vous concèderez comme sures. Le port 80 utilisé par le WEB est un port sûr que vous pouvez activer

Utiliser un par-feu

- Le par-feu joue le rôle de contrôleur, il filtre les connexions qui entrent et qui sortent de votre ordinateur
- Bloque ce qui lui semble indésirables selon ce que vous lui avez paramétré comme politique de sécurité
- chaque ordinateur, possède plusieurs portes d'entrés possibles (Les portes d'entrée et les portes de sorties ne sont pas les mêmes)
  Objectif : Bloquer par défaut toutes les portes, et autoriser seulement celles dont vous avez besoin, celles que vous concèderez comme sures. Le port 80 utilisé par le WEB est un port sûr que vous pouvez activer

Utiliser un par-feu

- Le par-feu joue le rôle de contrôleur, il filtre les connexions qui entrent et qui sortent de votre ordinateur
- Bloque ce qui lui semble indésirables selon ce que vous lui avez paramétré comme politique de sécurité
- chaque ordinateur, possède plusieurs portes d'entrés possibles (Les portes d'entrée et les portes de sorties ne sont pas les mêmes)
  Objectif : Bloquer par défaut toutes les portes, et autoriser seulement celles dont vous avez besoin, celles que vous concèderez comme sures. Le port 80 utilisé par le WEB est un port sûr que vous pouvez activer

Uncomplicated Firewall (UFW)

Par défaut ubuntu inclus un logiciel de pare-feu, nommé uncomplicated Firewall (UFW) c'est un logiciel en ligne de commande.Mais il existe une version graphique Graphical UFW, **celle ci doit être installer**

- Avantages : facilités d'utilisation ;
- inconvénient : certain pourraient se sentir limités par les capacités de ce logiciel de par-feu

Uncomplicated Firewall (UFW)

Par défaut ubuntu inclus un logiciel de pare-feu, nommé uncomplicated Firewall (UFW) c'est un logiciel en ligne de commande.Mais il existe une version graphique Graphical UFW, **celle ci doit être installer**

- Avantages : facilités d'utilisation ;
- inconvénient : certain pourraient se sentir limités par les capacités de ce logiciel de par-feu

iptables un par-feu compliqué mais complet

nous allons voir ensemble comment cofigurer rapidement iptables

```
iptables -A (chain) -p (protocole) --dport (port) -j (décision)
```

Fig.: La syntaxe de l'Ajout

```
# iptables -A INPUT -p icmp -j ACCEPT
```

Fig.: Ajout du Port Ping

```
# iptables -A INPUT -p tcp --dport www -j ACCEPT
```

Fig.: Ajout du Port 80

```
# iptables -P INPUT DROP
```

Fig.: Refuser tout les autres connexions par défaut

- Créer le fichier myiptables sous /etc/init.d et y'ajouter les commandes que nous avons testé ;
- Rajouter /etc/init.d/myiptables dans /etc/rc.local

```
# iptables -A INPUT -p tcp --dport www -j ACCEPT
```

Fig.: Ajout du Port 80

```
# iptables -P INPUT DROP
```

Fig.: Refuser tout les autres connexions par défaut

- Créer le fichier myiptables sous /etc/init.d et y'ajouter les commandes que nous avons testé ;
- Rajouter /etc/init.d/myiptables dans /etc/rc.local

stabilité et sécurité

Ubuntu, et généralement tout les systèmes Linux, bénéficient d'une strict séparation des privilèges.
Cela fournit :

- Une meilleure stabilité du système : Les priviléges étant limités, les possibilités qu'une application puisse ralentir ou provoquer un crash systéme sont aussi limitées ;
- Une meilleure sécurité du système :
  - l'exploitation d'une faille dans un logiciel pour prendre le contrôle de la machine est rendu plus difficile pour un attaquant ;
  - Un virus ne peut accéder qu'à une partie des ressources et fonctionnalités d'un système Linux, mais ni aux données importantes du systéme ni aux données éventuelles d'autres utilisateurs.

stabilité et sécurité

Ubuntu, et généralement tout les systèmes Linux, bénéficient d'une strict séparation des privilèges.
Cela fournit :

- Une meilleure stabilité du système : Les priviléges étant limités, les possibilités qu'une application puisse ralentir ou provoquer un crash systéme sont aussi limitées ;
- Une meilleure sécurité du système :
  - l'exploitation d'une faille dans un logiciel pour prendre le contrôle de la machine est rendu plus difficile pour un attaquant ;
  - Un virus ne peut accéder qu'à une partie des ressources et fonctionnalités d'un système Linux, mais ni aux données importantes du systéme ni aux données éventuelles d'autres utilisateurs.

Faut-il utiliser un antivirus ?

Je dirais .... oui :) Ce qu'il faut savoir ce que ubuntu est un système relativement sûr, mais cela ne doit pas vous empêcher d'être vigilant.
Le nombre de programmes malicieux (incluant les virus, Trojans et autres types) sous Linux a augmenté ces dernières années, et plus particulièrement doublé en 2005, passant de 422 à 863.
Les antivirus (prioritaires) qui existent et qui sont gratuits ; Avast, AVG et Avira...

clamav un Antivirus Open Source

- En quelques années, le projet clamAV est devenu une référence en matiére de logiciel libre antivirus.
- La réactivité de l'équipe de développement est excellente :
  - Vitesse de publication des signatures de nouveaux virus ;
  - Publication de correctifs de sécurité du logiciel lui-même.
- Installation
  - Il faut installer les paquets suivant : clamav, clamav-base, clamav-daemon,clamav-freshclam(la base de données de l'antivirus),libclamav2 ;
  - Les paquets de clamav se trouvent dans les dépôts d'ubuntu.

clamav un Antivirus Open Source

- En quelques années, le projet clamAV est devenu une référence en matiére de logiciel libre antivirus.
- La réactivité de l'équipe de développement est excellente :
  - Vitesse de publication des signatures de nouveaux virus ;
  - Publication de correctifs de sécurité du logiciel lui-même.
- Installation
  - Il faut installer les paquets suivant : clamav, clamav-base, clamav-daemon,clamav-freshclam(la base de données de l'antivirus),libclamav2 ;
  - Les paquets de clamav se trouvent dans les dépôts d'ubuntu.

clamav un Antivirus Open Source

- En quelques années, le projet clamAV est devenu une référence en matiére de logiciel libre antivirus.
- La réactivité de l'équipe de développement est excellente :
  - Vitesse de publication des signatures de nouveaux virus ;
  - Publication de correctifs de sécurité du logiciel lui-même.
- Installation
  - Il faut installer les paquets suivant : clamav, clamav-base, clamav-daemon,clamav-freshclam(la base de données de l'antivirus),libclamav2 ;
  - Les paquets de clamav se trouvent dans les dépôts d'ubuntu.

Merci pour votre Attention
Présentation écrite en LaTeX.
e-mail : sayadi.karim@gmail.com

Fig.: Logo du club ISIMUX