Première année Master en Informatique

***Option* :**

Systèmes Distribues et Intelligence Artificielle

Module :

Sécurité des Systèmes

Rapport de recherche bibliographique

Rapport n° : 10m1-SS03

Sécurité des Systèmes d'exploitation

Etudiants :

TOURQUI Wafa.

Enseignant responsable : Saci MEDILEH

Résumé

Il est plus important de protéger les informations que le matériel

- *3 types d'attaques : accidents (matériel ou humain), criminalité (accès non autorisés jusqu'au hackers), catastrophes (incendie, tremblement de terre…)*
- *La sécurité absolue n'existe pas (que ce soit le domaine informatique ou tous les autres domaines de la vie).*
- *Pour que la sécurité fonctionne, il faut que toutes les personnes ayant un accès à une ressource soient conscient du degré de sécurité associé à la ressource.*
- *La sécurité informatique , consiste à assurer que les ressources matérielles ou logicielles sont uniquement utilisées dans le cadre prévu.*

Mots-clés : Système d'exploitation - Attaques - Pare feu - sécurité – Internet- Protection, répertoires, fichiers, Mots de passes,

Plan d'exposée

Introduction

Etudier la sécurité et la protection des systèmes d'exploitation revient à étudier les concepts et les mécanismes de sécurité et de protection des systèmes d'exploitation.

Pour que la sécurité fonctionne, il faut que toutes les personnes ayant un accès à une ressource soient conscient du degré de sécurité associé à la ressource.

I. Généralités sur la protection :

Il est difficile de définir ce que l'on entend par protection d'un système d'exploitation (et d'information en général), tant que les facteurs qui peuvent influer sur cette notion (humains, sociaux et économiques) sont nombreux.

Cependant, on peut dire, que la protection se rapporte à tout ce que par quoi l'information peut être modifiée, divulguée et détruite.

Dans certain cas elle peut être la garantie des performances du système

- La protection désigne l'ensemble des mécanismes qui protègent les objets du système contre l'environnement à priori "hostile".
- Un processus utilisateur ne peut être exécuté en mode système.
- La protection exige enfin la correction des processus système
- Pérennité du système
- Confidentialité des données (système, utilisateur…)
- Correction du système
- Le degré de protection du système dépend de deux facteurs
- Degré des informations qu'il manipule
- Degré de confiance en ses logiciels, en particulier le système d'exploitation

Evaluer si des applications critiques fonctionnent sur les stations.

Un système doit être assez sécurisé sans pour autant empêcher les utilisateurs de se servir de leurs applications.

Sécuriser un système c'est protéger ce système contre un fonctionnement imprévu ou défectueux.

Il peut s'agir :

- D'erreurs de programmation (d'un utilisateur ou du système lui-même) qui se propagent au système (du fait de contrôles insuffisants ou mal effectués).
- D'un mauvais fonctionnement du matériel
- D'un opérateur, concepteur ou réalisateur malveillant ou peu scrupuleux (quand il s'agit d'informations financières).

Plusieurs systèmes de protections dans un système :

- pour les fichiers sur les disques
- pour la mémoire principale
- pour les autres ressources du système (catalogue, taches (entre elles), segments mémoires (écriture ou lecture - écriture), les canaux d'E/S, certains sous-programmes du système, certaines instructions CPU…)
- Droits d'accès (permis / interdit)
- Quotas d'utilisation (Pas utiliser plus de N blocs d'espaces disque, pas lancer plus de N E/S, pas dépasser une certaine place mémoire…)
- Arguments d'appel des sous programmes utilisés par les taches, dans les requêtes aux services du système, doivent être vérifiés afin d'empêcher qu 'un programme accède à des données interdites en fournissant des arguments hors limites (zones tampons)

Les risques

- Ils correspondent aux coûts matériels et financiers si une attaque ou une menace se réalisait. Dans tous systèmes informatiques, les risques existent et ne doivent pas être minimisés afin d'assurer une politique de sécurité correcte.
- Les risques qui doivent être pris en compte sont l'intégrité, la disponibilité des services, la sécurité du système et les coûts engendrés en cas d'indisponibilité de la ressource informatique.

Aspects Financiers :

- La Sécurité passe par un compromis coût/ efficacité.
- Le coût des ressources étant resté stationnaire, les systèmes et les machines actuelles plus rapides ont rendu ce coût moins prohibitif.
- L'idée d'un système de protection est de traiter les différents types de problème de manière générale et unitaire.
- Implantés seuls les dispositifs de protection coûtent chers.
- Si ces dispositifs permettent d'augmenter les performances du logiciel, dans des domaines comme celui de la fiabilité ou de la résistance aux erreurs, leur coût relatif diminue.
- Si c'est de plus ces dispositifs permettent une gestion des ressources partagées plus facile et plus sûre, ils peuvent devenir compétitifs d'un point de vue commercial.

Objectifs de la sécurité :

Classiquement la sécurité s'appuie sur cinq concepts de base.

- L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information ;
- La non répudiation, permettant de garantir qu'une transaction ne peut être niée ;
- L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

II. Les types d'attaque :

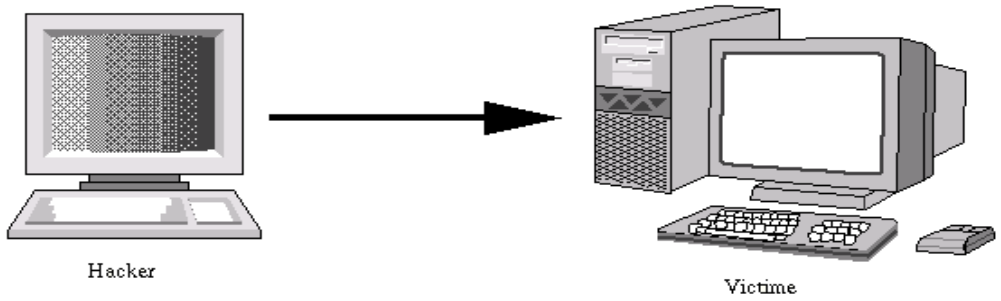
Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes :

- Les attaques directes.
- Les attaques indirectes par rebond.
- Les attaques indirectes par réponses.

Nous allons voir en détail ces trois familles.

1-Les attaques directes

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. La plupart des "script kiddies" utilisent cette technique.

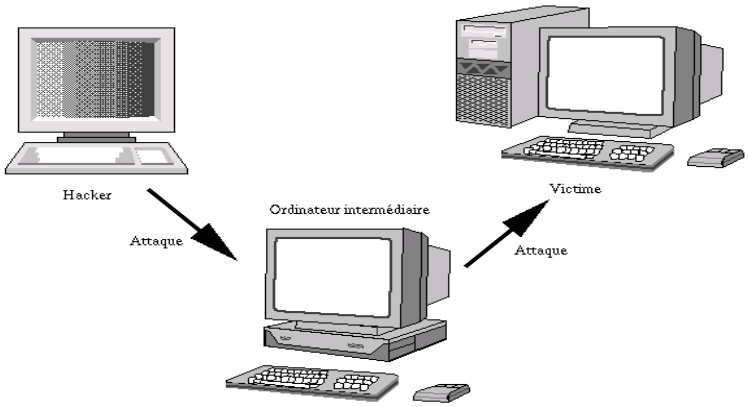


Attaque directe

2-Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

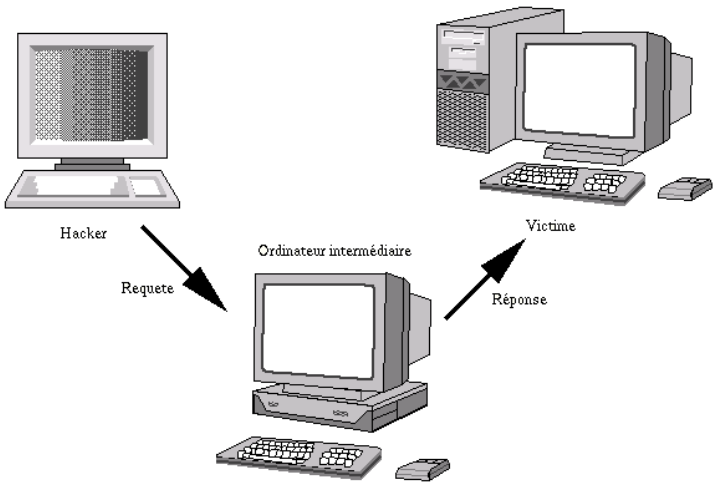
- Masquer l'identité (l'adresse IP) du hacker.
- Eventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer.



Attaque indirecte par rebond

3-Les attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les même avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.



Attaque indirecte par réponse

❖ Profils et capacités des attaquants

Les attaquants peuvent être classés non-seulement par leurs connaissances (newbies, experts, etc...) mais également suivant leurs capacités d'attaques dans une situation bien définie. Ainsi, on dénombrera les capacités suivantes :

- transmission de messages sans capacité d'écoute (IP spoofing...)
- écoute et transmission de messages
- écoute et perturbation des communications (blocage de paquets, DoS et DDoS...)
- écoute, perturbation et transmissions de messages
- écoute et relai de messages (attaques type man-in-the-middle)

Une autre caractéristique des attaquants va être leur emprise uni-directionnelle ou bi-directionnelle sur les communications, du fait de la nature asymétrique de celles-ci. En effet, la plupart des canaux de transmissions sur Internet ou sur tout autre réseau hétérogène sont uni-directionnels et empruntent des chemins différents suivant les règles de routage. Ainsi, de nombreux protocoles de sécurité sont également unidirectionnels et il faut établir plusieurs canaux pour permettre un échange en "duplex". Ces canaux qui sont au nombre de 2 minimum, sont la plupart du temps gérés de façon totalement indépendante par les protocole de sécurité. C'est le cas pour SSL/TLS mais également pour IPSec dont les associations de sécurité (SA) sont unidirectionnelles et indépendantes, chacune définissant son propre jeu de clés, algorithmes, etc...

❖ Quels risques pour les données informatiques ?

Il existe différents types de risques pour les données d'une entreprise, les principaux sont :

- les virus et programmes malveillants,
- les emails frauduleux,
- le piratage,
- l'espionnage industriel,
- la malversation,
- la perte d'information confidentielles,
- l'erreur de manipulation.

III. Mots de passes d'administration:

La gestion insuffisante des noms d'utilisateur et des mots de passe est un problème typique.

- Les quatre règles de base à respecter pour les noms d'utilisateur et les mots de passe sont les suivantes :

1. Utiliser des mots de passe plus longs comprenant des nbrs ou des symboles.
2. Changer régulièrement les mots de passe**.**
3. Ne pas utiliser de mots de passe évidents.
4. Ne JAMAIS laisser les informations par défaut sur les équipements de réseau.

IV. Protection des répertoires et fichiers :

Trois classes d'utilisateurs peuvent accéder aux fichiers et aux répertoires : propriétaire, groupe et autres utilisateurs. Pour chacune de ces classes d'utilisateurs, il existe trois types de **droits d'accès** : lecture, écriture et exécution. **Utilisateurs et droits d'accès**

Les trois classes d'utilisateurs sont :

• **Propriétaire** - en règle générale, la personne qui a créé le fichier.

• **Groupe** - les utilisateurs qui ont été regroupés par l'administrateur système. Par exemple, les membres d'un service peuvent appartenir au même groupe.

• **Autres** - Tous les autres utilisateurs du système.

V. *Enjeux et choix de support de sauvegarde*.

Que vous soyez un particulier ou une entreprise, une sauvegarde peut vous tirer d'affaire dans bien des cas.

Que vous soyez victime d'une attaque, d'un crash système, d'une défaillance matérielle, etc. seule une sauvegarde vous permettra de restaurer entièrement le système dans son état originel. Encore faut-il qu'elles soient bien faîtes !

❖ *La politique de sauvegarde*

1. **a sauvegarde totale :** l'ensemble des fichiers, répertoires, systèmes de fichiers ou disques sélectionnés est sauvegardé sans restriction**.**
2. **la sauvegarde incrémentale :** tous les fichiers modifiés depuis la dernière sauvegarde totale sont sauvegardés.

3. **la sauvegarde différentielle** : tous les fichiers modifiés depuis la dernière sauvegarde différentielle sont sauvegardés.

❖ Les différents supports de stockage :

Les ressources générées au cours du projet de numérisation sont, en général, stockées sur les disques durs d'un ou plusieurs serveurs de fichiers, ainsi que sur des supports de stockage portables (bande magnétique et supports optiques tels que CD-R et DVD).

Les supports de stockage numérique ont des spécificités logicielles et matérielles différentes. Leurs caractéristiques de stockage et de gestion diffèrent également. De nouveaux supports sont testés régulièrement. Il en va ainsi, par exemple, des systèmes de stockage holographique.

Les supports numériques de stockage couramment utilisés se répartissent en trois catégories :

1. **les disques magnétiques fixes**, magnétiques amovibles, magnéto-optiques (à lecture unique, à lecture-écriture), optiques (à lecture seule, à écriture unique, inscriptibles, à lecture-écriture : CD, DVD, Blue-Ray,…)
2. **les bandes magnétiques :** AIT/SAIT (Advanced Intelligent Tape et Super Advanced Intelligent Tape), LTO (Linear Tape Open), SDLT, …
3. **les semi-conducteurs ou mémoires nomades :** cartes mémoire CompactFlash, modules de mémoire MemoryStick, modules de mémoire SmartMedia (mémoire d'appareil photographique numérique) ; clés ou modules de mémoire USB ; lecteurs Flash.

❖ Les types de supports les plus connus :

Disquette, ZIP, JAZZ, Disque Dur, QIC : Quarter Inch Cartridge, DAT : Digital Audio Tape, DDS : Digital Data Storage, DLT : Data Linear Tape , SDLT : Super Data Linear Tape nouvelle technologie , CD-ROM , Disque Magnéto-Optiques , DVD : Digital Versatile Disk

❖ Les critères de choix des supports de stockage :

De nombreux facteurs interviennent dans le choix de supports numériques de stockage à long terme.

Les Archives nationales britanniques68 proposent une méthode de pondération de 6 critères pour 6 supports de stockage :

- **longévité** : avoir un horizon de 10 ans ; viser une longévité plus grande n'est pas nécessaire au vu de l'obsolescence des techniques ;
- **capacité** : ajuster la capacité de stockage au volume des données et à la dimension physique des équipements de stockage ;
- **viabilité** : les médias et les « drives » devraient supporter des modes de détection d'erreurs convenables. Prévoir de tester l'intégrité du média après écriture est un plus. Prévoir des mécanismes de protection pour éviter « d'écraser » accidentellement des données et maintenir l'intégrité de celles-ci ;
- **obsolescence** : préférer des technologies matures, largement disponibles et utilisées sur le marché aux technologies « à la pointe ». Choisir des standards ouverts pour les médias et les « drives » est préférable ;
- **coût** : deux éléments sont à prendre en considération, à savoir le coût du média luimêmeet le coût total. L'élément pertinent de comparaison pour le média est le coût par Gigabyte. Le coût total doit inclure les coûts d'achat et de maintenance des matériels et logiciels et celui des équipements de stockage. Si le coût du stockage en lui-même diminue, celui du management du stockage augmente fortement ;
- **vulnérabilité** : le média doit être peu vulnérable aux dommages physiques et supporter des environnements divers sans perte de données.

Chaque support reçoit pour chaque critère une note de 1 (ne répond pas au critère) à 3 (répond tout à fait au critère). Un support de stockage doit avoir une note totale d'au moins 10 pour être considéré comme une bonne solution de stockage.

VI. Aspects techniques de la sécurité

Les problèmes techniques actuels de sécurité informatique peuvent, au moins provisoirement, être classés en deux grandes catégories :

• ceux qui concernent la sécurité de l'ordinateur proprement dit, serveur ou poste de travail, de son système d'exploitation et des données qu'il abrite ;

• ceux qui découlent directement ou indirectement de l'essor des réseaux, qui multiplie la quantité et la gravité des menaces.

Si les problèmes de la première catégorie citée ici existent depuis la naissance de l'informatique, il est clair que l'essor des réseaux, puis de l'Internet, en a démultiplié l'impact potentiel en permettant leur combinaison avec ceux de la seconde catégorie.

Conclusion

En conclusion il est absolument impératif de rappeler que la sécurité absolue n'existe pas, sécuriser son système est obligatoire. Il faut être capable d'évaluer à quel est le degré de sécurisation à mettre en place, quels sont les points sensibles, quelles ressources matériels, humaines, financières dont on dispose, appliquer une politique de prévention auprès des utilisateurs. (90% des problèmes de sécurité sous UNIX dus aux utilisateurs).

Référence bibliographique

✓ *Document éléctronique:*

- *SECURITE et PROTECTION des SYSTEMES d'EXPLOITATIO.*
- *Sécurité des Systèmes d'Exploitation : cours 1, Frédéric Gava*
  Master SSI, Université de Paris-Est Créteil
  Cours SESE du M2 SSI, d'après le cours de Franck.
- *Sécurité des Systèmes d'exploitation*
  Didier Verna,didier@lrde.epita.fr
  http://www.lrde.epita.fr/˜didier,Version EPITA du 28 septembre 2009
- *PDF : LES SUPPORTS DE STOCKAGE.*
  PEP's – Normes et lignes directrices techniques et organisationnelles – 2009

✓ *Sites Internet:*

- *www.commentcamarche.net .*
- www.SecuriteInfo.com..
- *www.wikipedia.org.*