La sécurité des systèmes informatiques (Théorie)

Table des matières

Objectifs

Ce module de formation théorique a pour objectifs de :

- Permettre aux étudiants d'avoir une idée sur les enjeux et l'importance de la sécurité dans les systèmes d'information
- Permettre aux étudiants de s'auto former sur les attaques et les grands principes de la sécurité informatique
- Fournir aux étudiants, un ensemble d'outils de sécurité permettant de tester ou de sécuriser les réseaux et les systèmes
- Consolider un ensemble de ressources liées à la sécurité informatique

La partie pratique (études de cas) de ce module est développée dans un autre module.

Introduction

Le progrès remarquable des technologies de l'information et de la communication au cours des dix dernières années a fait naître un grand nombre de systèmes d'information dans les organisations et administrations. Ces systèmes d'information, moteurs de croissance et de développement des métiers et services sont assez importants, voire même indispensables pour le bon fonctionnement de tout entreprise. Cependant, avec les menaces actuelles et les ouvertures des systèmes d'information sur l'Internet et d'autres réseaux non maîtrisés, Il devient nécessaire de garantir la sécurité de l'ensemble des biens constituant tout système d'information.

Assurer la sécurité d'un système d'information n'est plus un sujet tabou. Les statistiques des attaques et des menaces font qu'aujourd'hui, les responsables en sont conscients des risques pesant sur un système d'information, même si les moyens ne suivent pas toujours pour assurer effectivement et efficacement la sécurité.

Ce document, destiné particulièrement aux étudiants de Licence de Technologie de l'Institut Universitaire Fotso Victor de Bandjoun au Cameroun, aborde des sujets liés à la sécurité des systèmes d'information en général, et celle des systèmes informatiques en particulier. Élaboré dans le cadre d'un séminaire de formation et de sensibilisation sur la sécurité des systèmes d'information, il vise avant tout à donner une impulsion à ceux qui aspirent les métiers liés à la sécurité informatique.

Le document globale comprend deux parties : une partie théorique (ce document) et une partie pratique (document séparé).

Qu'est ce que la sécurité d'un système ?

I

Avant d'apporter un élément de réponse à cette question, il est important de définir les termes "système informatique" et "système d'information" afin de permettre aux étudiants de mieux cerner la différence entre ces deux expressions qui font souvent l'objet de confusion.

A. Définition d'un système informatique et d'un système d'information

Définition : Système informatique

Un système informatique est un ensemble de dispositifs (matériels et logiciels) associés, sur lesquels repose un système d'information. Il est constitué généralement des serveurs, routeurs, pare-feu, commutateurs, imprimantes, médias (câbles, air, etc.), points d'accès, stations de travail, systèmes d'exploitation, applications, bases de données, etc.

Définition : Système d'information

Un système d'information est un ensemble de moyens (humains, matériels, logiciels, etc.) organisés permettant d'élaborer, de traiter, de stocker et/ou de diffuser de l'information grâce aux processus ou services. Un système d'information est généralement délimité par un périmètre pouvant comprendre des sites, des locaux, des acteurs (partenaires, clients, employés, etc.), des équipements, des processus, des services, des applications et des bases de données.

Et c'est quoi alors la sécurité d'un système ?

La sécurité d'un système (informatique ou d'information) est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un système d'information englobe celle du système informatique sur lequel il s'appuie.

Complément

Faire de la sécurité sur un réseau consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire

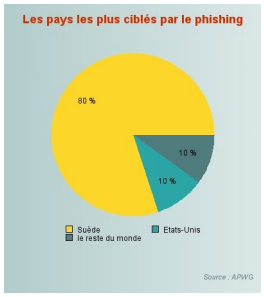
correctement car le service est disponible.

Rappel

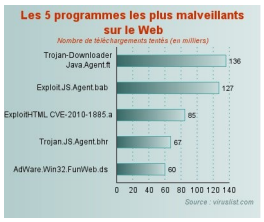
Dans la suite de ce support, nous parlerons beaucoup plus de la sécurité des systèmes informatiques (ensemble des éléments matériels et logiciels utilisés dans un système d'information pour acquérir, traiter et produire de l'information).

B. Quelques chiffres sur la sécurité informatique en images

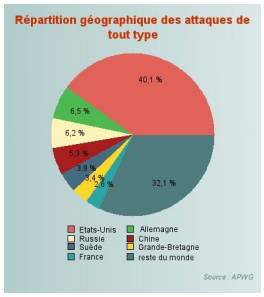
Les images suivantes donnent une idée sur les menaces et attaques du mois d'août 2010. Les statistiques illustrées par ces images sont actualisées chaque mois sur le site *www.journaldunet.com*[1]. Pour en savoir plus sur l'évolution mensuelle des menaces et attaques, consultez la rubrique "Solutions => Sécurité => Baromètre des menaces" du même site.



Les pays les plus ciblés par les attaques de type phishing



Les 5 programmes les plus malveillants sur le web



La répartition géographique des attaques de tout type

Rappel

Le site le "journaldunet" n'est pas le seul site produisant des statistiques sur les menaces et vulnérabilités informatiques.

1 - http://www.journaldunet.com/

C. Comment Évalue t-on la sécurité d'un système informatique

La sécurité d'un système informatique peut s'évaluer sur la base d'un certain nombre de critères de sécurité. On distingue généralement trois principaux critères de sécurité :

- Disponibilité : Elle consiste à garantir l'accès à un service ou à une ressource.
- Intégrité : Elle consiste à s'assurer que les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- Confidentialité : Elle consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs concernés.

Complément

En plus des ces trois critères, on peut ajouter les critères suivants:

- Authentification : Elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
- Non répudiation : Elle consiste à garantie qu'aucun des correspondants ne pourra nier la transaction.

L'évaluation de la sécurité d'un système informatique est un processus très complexe basé en général sur une méthodologie (standard ou non). Cette évaluation passe par une analyse de risques. L'analyse des risques pesant sur un système informatique elle même s'appuie sur un ensemble de métriques définies au préalable.

Exemple

Par exemple pour le critère "disponibilité", le choix des métriques d'évaluation peut être : Très haute, Haute, Moyenne, Basse.

L'analyse des risques fait partie du processus global de gestion de risques dans un système d'information.

II

Pourquoi sécuriser les systèmes informatiques ?

A. Les enjeux

1. Enjeux économiques

Les organismes ou entreprises à but lucratif ont presque toujours la même finalité : c'est de réaliser des bénéfices sur l'ensemble de leurs activités. Cette réalisation est rendue possible grâce à son système d'information considéré comme moteur de développement de l'entreprise. D'où la nécessité de garantir la sécurité de ce dernier.

La concurrence fait que des entreprises s'investissent de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fournit aux clients.

2. Enjeux politiques

La plupart des entreprises ou organisations se réfèrent aux documents officiels de sécurité élaborés et recommandés par l'État . Ces documents contiennent généralement des directives qui doivent être appliquées par toute structure engagée dans un processus de sécurisation du système d'information. Dans le cadre du chiffrement des données par exemple, chaque État définit des cadres et mesures d'utilisation des algorithmes de chiffrement et les recommande aux entreprises exerçant sur son territoire. Le non respect de ces mesures et recommandations peut avoir des conséquences grave sur l'entreprise. A ce niveau, l'enjeu est plus politique parce que chaque État souhaite être capable de décrypter toutes les informations circulant dans son espace.

3. Enjeux juridiques

Dans tout système d'information, on retrouve de l'information multiforme (numérique, papier, etc.). Le traitement de celle ci doit se faire dans un cadre bien définit et dans le strict respect des lois en vigueur. En matière de juridiction, le non respect des lois et exigences relatives à la manipulation des informations dans un

système d'information peut avoir des conséquences graves sur l'entreprise.

Exemple

En France par exemple, tout traitement de données à caractère personnel doit au préalable faire l'objet d'une déclaration auprès de la CNIL (Commission Nationale pour l'Informatique et les Libertés).

B. Les vulnérabilités

Tous les systèmes informatiques sont vulnérables. Peu importe le niveau de vulnérabilité de ceux ci. Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire.

Les vulnérabilités des systèmes peuvent être classés en catégorie (humaine, technologique, organisationnelle, mise en oeuvre).

1. Vulnérabilités humaines

L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car ne dit t-on pas souvent que l'erreur est humaine ? Un système d'information étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI.

Un exemple courant de vulnérabilité chez l'humain, c'est la sur-exploitation. Généralement, on a tendance à faire travailler un employer au delà de la limite de ses capacités normales. Ce qui peut l'amener à commettre des erreurs pouvant avoir des conséquences désastreuses pour l'entreprise.

Exemple

Par exemple le fait d'oublier une carte d'accès SerureID dans un taxi au retour de travail, ou alors de lire un document confidentiel de l'entreprise dans un train lors d'un voyage, sans s'assurer qu'on est pas filé.

2. Vulnérabilités technologiques

Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des vulnérabilités technologiques découvertes, il suffit de s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT(Computer Emergency Readiness ou Response Team). Exemple : *US-CERT*[2]

Exemple

Des exemples de vulnérabilités technologiques enregistrées peuvent être consultées sur le site suivant : *http://www.us-cert.gov/cas/bulletins/SB10-249.html*

3. Vulnérabilités organisationnelles

Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même

2 - http://www.us-cert.gov/

ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées.

Exemple

Un exemple de vulnérabilité organisationnelle peut être le manque de définition des responsabilités dans un système d'information.

4. Vulnérabilités mise en oeuvre

Les vulnérabilités au niveau mise en oeuvre peuvent être dues à la non prise en compte des certains aspects lors de la réalisation d'un projet.

Exemple

Par exemple la non prise en compte des procédures de maintenance dans un projet d'acquisition et de mise en en production d'un serveur de données.

C. Les menaces

Les systèmes informatiques sont confrontés aux menaces. Une menace est un événement pouvant se produire à tout moment et que l'on craint. Selon leurs origines, les menaces peuvent être classifiées en deux catégories:

- Menaces d'origine naturelle (incendie, inondation, séismes, etc.)
- Menaces d'origine humaine (fuite, malveillance, espionnage, vol, etc.).

Elles peuvent, en s'appuyant sur la puissance de l'informatique, causer des dommages d'une ampleur inédite.

La plupart des grandes entreprises ou organisations sont la cible de plusieurs d'attaques quotidiennes. Certaines attaques peuvent être bloquées automatiquement par des dispositifs (matériels et/ou logiciels) de sécurité, alors que d'autres attaques utilisant des procédés nouveaux auxquels ces dispositifs ne savent pas répondre, représentent un réel danger.

D. Les risques

Face aux différentes vulnérabilités susceptibles d'être exploitées pour attaquer les systèmes d'information et aux menaces multiformes existantes, il est clair que tout système d'information peut être impacté par des risques. Un risque est un événement susceptible de se produire.

Selon la nature physique, on peut classer les risques en plusieurs catégories dont voici quelques unes : Accident, perte de services, vols, fuites d'information.

1. Risque "accident"

Cette catégorie regroupe tous les sinistres comme les incendies, dégâts des eaux, explosions, catastrophes naturelles, etc. Certains de ces risques ne peuvent être raisonnablement pris en compte (par exemple, un effondrement causé par la présence d'une ancienne carrière souterraine), d'autres peuvent être prévenus ou combattus (par exemple, un incendie), l'informatique n'étant alors qu'un des aspects du problème.

Enfin, des mesures simples permettent de limiter les conséquences de certains

accidents (par exemple, si la salle informatique est située au premier étage, on évitera la perte du matériel en cas d'inondation, même si celle-ci ne peut être combattue).

2. Risque "perte de services"

On range dans cette catégorie les coupures de courant, de télécommunications, les ruptures de stocks de fournitures essentielles, etc. Il existe des moyens permettant de palier à ces problèmes, notamment la redondance, les techniques statistiques et les alarmes. Quelques exemples concrets :

- Onduleur et éventuellement groupe électrogène doublant le réseau EDF
- Liaison satellite doublant la ligne spécialisée
- Choix de fournitures disponibles auprès de multiples sources (et pas seulement de multiples fournisseurs d'une seule source)
- Programmation d'interventions ou de remplacements préventifs

Ces mesures ont évidemment un coût, mais lorsqu'il s'agit d'un service vital, ce coût est de très loin préférable aux conséquences d'une perte de service.

Remarquez que les pannes matérielles peuvent entrer dans cette catégorie : c'est évident pour les serveurs, mais les imprimantes d'une société d'affacturage peuvent également mériter certains égards.

Par contre une panne affectant un poste de travail banalisé n'a aucune importance : le remplacement d'un PC ne pose aucun problème et la panne n'affecte pas sérieusement la productivité de l'entreprise.

3. Risque "vol"

Ces problèmes sont la plupart du temps marginaux, sauf dans les grandes entreprises, l'administration et les établissements d'enseignement où les vols ou dégradations sont généralement commis par les personnes fréquentant habituellement les lieux (personnel, étudiants).

Ces problèmes sont loin d'être propres à l'informatique et les solutions existantes sont simples :

- Installation d'alarmes et de dispositifs de télésurveillance
- Fixation du matériel au mobilier et verrouillage des boîtiers
- Utilisation de cartes internes pour les clés électroniques
- Utilisation de matériel spécifique anti-vandalisme

4. Risque "fuite d'informations"

La fuite d'information est un phénomène difficile à éradiquer. Mais on peut en fonction des moyens dont on dispose, le rendre difficile à réaliser.

III

Comment et avec quoi les systèmes sont-ils attaqués ?

A. Les méthodes et types d'attaques

Définition

Une « attaque » est une activité malveillante qui consiste à exploiter une faille d'un système informatique (serveurs, routeurs, système d'exploitation, logiciel, etc.) à des fins non connues par les responsables du système et généralement préjudiciables pour le système d'information en général.

Les attaques sont souvent menées suite aux motivations diverses :

- Perturbation du bon fonctionnement d'un système ou d'un service
- Vol des informations sensibles (données bancaires par exemple)
- Utilisation des ressources du système à d'autres fins
- Etc.

Parmi les types d'attaques, nous pouvons citer : les attaques par intrusion, les attaques par déni de service, les attaques par interception (homme du milieu), les attaques par dictionnaire et par force brute, les attaques par ingénierie sociale.

1. Attaque par intrusion

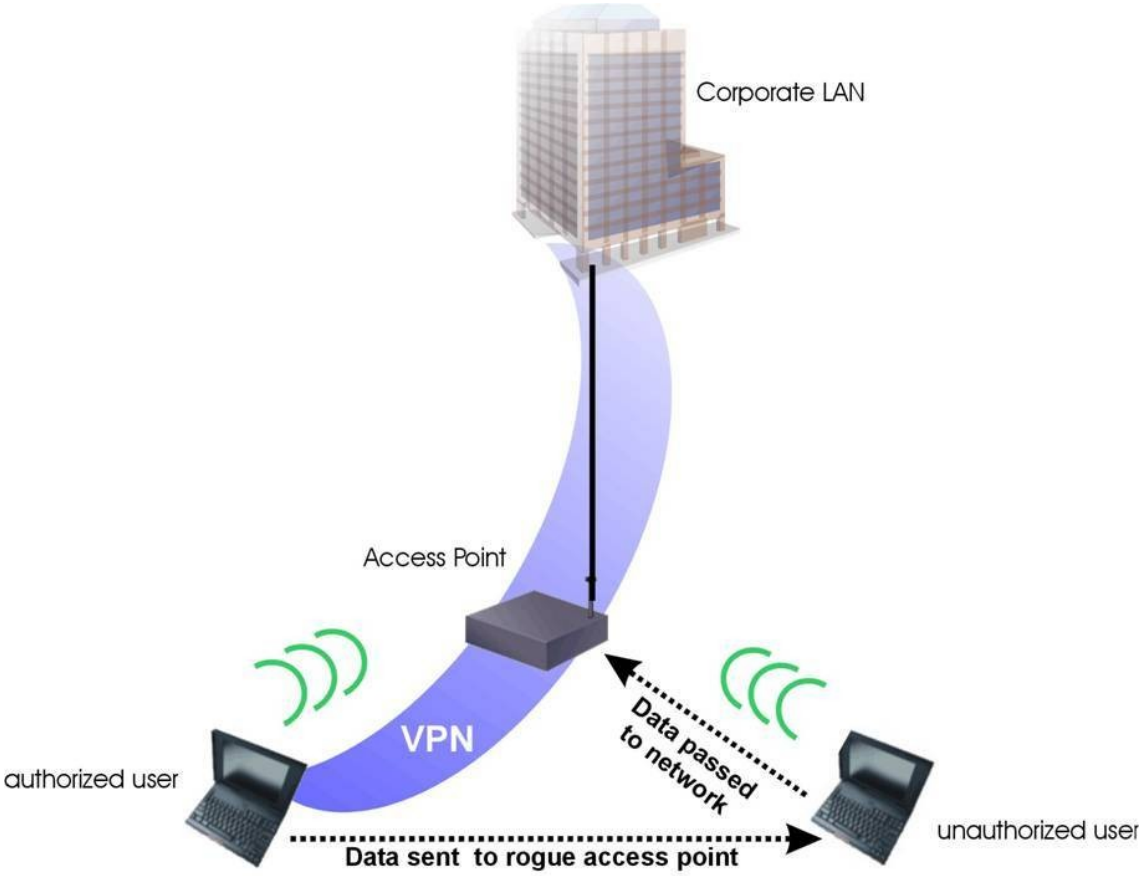
Ce type d'attaque vise à s'infiltrer physiquement ou logiquement dans un système informatique en vue de récupérer des informations exploitables à d'autres fins.

Exemple

Pas exemple, installer un écouteur (sniffer) sur un réseau informatique constitue une attaque de type intrusion sur le réseau.

2. Attaque de l'homme du milieu (Man-In-The-Middle)

Ce type d'attaque vise à intercepter les communications entre deux parties (personne, ordinateur) sans que ni l'une, ni l'autre ne puisse s'en apercevoir. Il s'agit ici d'une attaque par interception. Le schéma ci-après illustre ce type d'attaque entre un ordinateur client et un ordinateur serveur.



Man-in-the-Middle Attack

3. Attaque par déni de service

Ce type d'attaque très fréquente, vise à perturber le bon fonctionnement d'un service. Elle exploite généralement les faiblesses de la pile de protocole TCP/IP et les vulnérabilités logicielles existantes et non traitées.

Exemple

Par exemple, envoyer 1.000.000 de requêtes en moins de 5 secondes à un serveur web avec des adresses IP sources fictives, constitue une attaque de type déni de service sur le serveur Web.

4. Attaque par hameçonnage (phishing)

Le phishing est une technique dans laquelle des bandes organisées de cybercriminels se font passer pour des organismes financiers ou grandes sociétés en envoyant des emails ou des pages web frauduleux pour récupèrer des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds. Le phénomène existe depuis 1996 et a connu une accélération significative début 2003.

Complément

Pour en savoir d'avantage sur ce type d'attaque et comment se protéger, nous vous recommandons ce site : *http://www.phishing.fr/*

5. Attaque par dictionnaire et par force brute (mot de passe)

Attaque par dictionnaire

L'attaque par dictionnaire vise à retrouver un mot de passe à partir d'un dictionnaire élaboré au préalable. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire.

Attaque par force brute

L'attaque par force brute a le même objectif que l'attaque par dictionnaire, sauf que la technique change. Elle consiste à tester une à une, toutes les combinaisons possibles. Cette attaque est difficile d'aboutir lorsque le mot de passe contient plus de caractères variés (majuscules, minuscules, chiffres, caractère spéciaux).

6. Attaque par ingénierie sociale

Ce type d'attaque très fréquente également, vise à récupérer des informations sensibles des utilisateurs en s'appuyant sur leur naïveté. Elle exploite l'abus de confiance faite par les utilisateurs du système d'information.

Exemple

Par exemple un hacker qui se fait passer pour un technicien du support en appelant une secrétaire pour lui demander le mot de passe d'ouverture de session sur son poste. Il s'agit là d'une usurpation d'identité.

B. Les outils d'attaque

Pour mener à bien les attaques sur les systèmes informatiques, les pirates utilisent des outils informatiques bien connus du domaine. Ces outils sont également utilisés par les administrateurs et spécialistes de la sécurité pour tester la robustesse de leurs systèmes d'information, généralement dans le cadre d'un audit de sécurité.

Parmi ces outils, nous pouvons citer :

- Les programmes malveillants (virus, ver, cheval de troie, logiciel espion [spyware])
- Les scanners et sniffers
- Les backdors (portes dérobées)
- Les spams (courriers indésirables)

1. Les programmes malveillants

Définition : Virus

Un virus informatique est un programme malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les CD/DVD, les clefs USB, etc.

Définition : Ver

Un ver informatique est un programme malveillant qui se reproduit sur plusieurs

ordinateurs en utilisant un réseau informatique comme Internet.

Contrairement à un virus informatique, un ver n'a pas besoin d'un programme pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

Exemple

Comme exemple de ver, nous avons le ver "I LOVE YOU" découvert pour la première fois le 4 mai 2000, le ver "MORRIS" découvert en 1988. Ce ver a été à l'origine de la création du CERT (Computer Emergency Response Team).

Définition : Cheval de troie

Un cheval de Troie est un programme d'apparence légitime conçu pour exécuter de façon cachée des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

Définition : Logiciel espion (spyware, mouchard ou espiogiciel)

Un logiciel espion est un programme malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.

Un logiciel espion est généralement composé de trois mécanismes distincts: Infection, collecte et transmission

Définition : Rootkit

Un rootkit ("jeu de démarrage" en français) est un programme malveillant dont la principale fonctionnalité est de dissimuler la présence de son activité et celle des autres programmes néfastes aux yeux de l'utilisateur du système et des logiciels de sécurité (antivirus, pare-feu, IDS).

Certains rootkit peuvent en plus de cette fonctionnalité principale, installer des backdors (porte dérobée).

Les rootkits ont deux caractéristiques principales :

- Ils modifient profondément le fonctionnement du système d'exploitation
- Ils se rendent invisibles (difficile à les détecter)

Conseil : Détection et suppression des rootkits

Vous trouvez plusieurs méthodes de détection et de suppression des rootkits via ce lien : *http://www.commentcamarche.net/faq/14963-supprimer-les-rootkits*

2. Les sniffers

Un sniffer est un outil matériel ou logiciel, permettant de lire les données qui circulent dans un réseau. Si les données sont non chiffrées, on peut obtenir des informations sensibles comme les mots de passe. Ce genre d'outil peut également aider à résoudre des problèmes réseaux en visualisant ce qui passe à travers l'interface réseau.

Exemple

Un exemple d'outil sniffer : *Wireshark*[3]

3 - http://www.wireshark.org/

3. Les backdors (portes dérobées)

Une porte dérobée n'est pas un programme, mais une fonctionnalité d'un programme permettant de donner un accès secret au système. Ce genre de fonctionnalité est souvent ajoutée à un logiciel par l'éditeur, afin de lui permettre de surveiller l'activité du logiciel, ou de prendre le contrôle en cas de sollicitation.

Généralement, les pirates informatiques une fois entrés dans le système, créent une porte dérobée afin de pourvoir y avoir accès à n'importe quel moment.

Comment se protéger contre ces attaques ?

IV

A. Sur le plan organisationnel

1. Application des grands principes de la sécurité informatique

a) Amélioration continue de la sécurité (PDCA)

La roue de Deming

La roue de Deming est une illustration de la méthode qualité PDCA (Plan Do Check Act), son nom vient du statisticien américain William Edwards Deming (1900-1993).

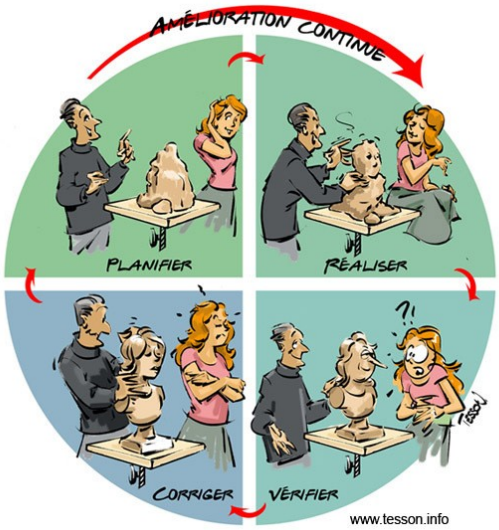
La méthode comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux. Sa mise en place doit permettre d'améliorer sans cesse la qualité d'un produit, d'une œuvre, d'un service...

Plan : ce que l'on va faire

Do : production

Check : mesure, vérification

Act : décision améliorative, corrective



b) Élaboration d'une Politique de Sécurité du Système d'Information (PSSI)

La politique de sécurité d'un système d'informatique est un document formel comprenant des directives, recommandations et principes de sécurité applicables à un système d'information pour garantir sa sécurité. Il s'agit d'un document stratégique généralement validé par la hiérarchie de l'organisme ou de l'entreprise. Ce document vise à démontrer le soutien de la direction en ce qui concerne la gestion de la sécurité.

Une politique de sécurité s'accompagne souvent des exigences de sécurité et des guides de bonnes pratiques visant à mettre en application cette politique de sécurité. De même, une PSSI est appelé à être maintenue. Elle doit évoluer en fonction des changements survenus ou observés dans le Système d'Information.

La révision régulière de la politique de sécurité permet d'assurer sa continuité et son efficacité.

Rappel

L'élaboration d'une PSSI passe par une méthodologie et doit faire intervenir plusieurs acteurs du Système d'Information (RSSI, administrateurs, utilisateurs, partenaires, etc.). Certaines méthodes d'analyse de risques peuvent être utilisées pour élaborer une PSSI. C'est le cas par exemple de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité).

c) Mise en place d'une gestion des risques

En matière de sécurité des systèmes d'information, la gestion des risques est un processus visant à :

- apprécier les risques qui pèsent sur les actifs de l'entreprise, ses valeurs et parfois son personnel
- traiter les risques appréciés

Un risque se défini comme un événement potentiel prévisible ou non.

Le processus de gestion des risques comprend plusieurs activités illustrées par le schéma ci après :

Schéma d'illustration des activités du processus de gestion des risques.

Méthodes de gestion des risques

Tout comme l'élaboration d'une PSSI, la gestion des risques s'appuie sur une méthodologie. Plusieurs méthodes de gestion des risques existent. Nous pouvons citer : *EBIOS*[4], *OCTAVE*[5], *MEHARI*[6], *CRAMM*[7], etc..

2. Application des grands principes de défense

Les grands principes de défense d'un système d'information peuvent être classés en quatre grandes catégories : Prévention, Protection, Détection et Réaction.

a) Principe de prévention

Le principe de prévention consiste à mettre en place des moyens ou dispositifs en vue de prévoir des éventuelles attaques qui pourraient avoir lieu sur le système.

Exemple

Par exemple, le fait de cloisonner un réseau en domaine de sécurité afin d'éviter qu'une attaque sur une partie du réseau n'affecte les autres parties du réseau, fait partie des principes de prévention.

b) Principe de protection

Le principe de protection consiste à mettre en place des moyens ou dispositifs permettant de protéger un bien ou un ensemble de biens (essentiel ou support) du système d'information

Exemple

Par exemple, installer un pare-feu à l'entrée du réseau local d'une entreprise pour assurer le filtrage des paquets entrant et/ou sortant, fait partie des principes de protection contre les attaques.

c) Principe de détection

Le principe de détection consiste à mettre en place des dispositifs matériels et/ou logiciels permettant identifier les intrusions dans un système ou dans une application. Sur le plan logiciel, ce principe s'appuie sur des outils tels que des bases de données, des algorithmes pour détecter les attaques.

Généralement, la procédure de détection est couplée à la procédure d'alerte, ce qui est tout a fait logique, car une détection sans alerte n'apporte pas de valeur ajoutée à la sécurisation d'un système.

Exemple

Par exemple, le fait de mettre en place une camera vidéo couplée à un déclencheur automatique d'alarme dans un bâtiment en vue de détecter les intrusions physiques, fait partie des principes de détection.

d) Principe de réaction

Le principe de réaction consiste à mettre en place un ensemble de moyens, procédures ou dispositifs (matériels ou logiciels) visant à réagir vis à vis des dysfonctionnements identifiés sur le système. Des procédures de réaction doivent

4 - http://www.securite-informatique.gouv.fr/gp_article82.html
5 - http://www.cert.org/octave/
6 - http://www.clusif.asso.fr/fr/production/mehari/
7 - http://www.cramm.com/

être rédigées de manière non ambiguë, et mises à la disposition non seulement des spécialistes en charge de la sécurité, mais aussi des utilisateurs.

Exemple

Par exemple, réviser les règles de filtrage au niveau d'un pare-feu suite à une attaque sur le réseau depuis l'extérieur, fait partie des principes de réaction.

B. Sur le plan technique

1. Application des mécanismes de sécurité

Un mécanisme de sécurité peu être vu au sens large comme une combinaison d'éléments destinés à fonctionner ensemble pour produire un résultat. Dans le carde d'un système d'information, il s'agit d'un groupe de fonctions ou de moyens ayant un objectif commun.

Mécanisme d'authentification

Ce mécanisme permet de vérifier la véracité des utilisateurs, du réseau et des documents. Il est utilisé dans le cadre du contrôle d'accès (physique ou logique).

Mécanisme de chiffrement

Ce mécanisme permet de rendre inintelligible des informations à ceux qui n'ont pas l'autorisation. Il est utilisé pour assurer la confidentialité des données et la signature numérique.

Mécanisme de contrôle d'accès

Ce mécanisme permet d'identifier tous les accès au système. Ces accès peuvent être physiques ou logiques.

Mécanisme de filtrage

Ce mécanisme permet de filtrer les paquets ou requêtes provenant d'une source (hôte, réseau), ou alors à destination d'un hôte ou d'un réseau. Il est utilisé par des équipements de filtrage tels que les parefeu, proxy, etc.

Mécanisme de détection

Ce mécanisme permet de détecter des anomalies dans un réseau, un système ou une application. Par exemple la détection des injections de code SQL dans une application.

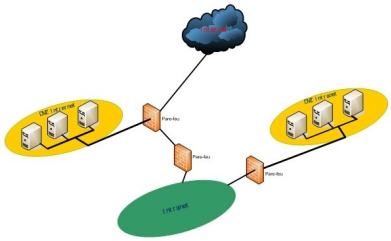
2. Application du mécanisme de cloisonnement et du principe de l'architecture n-tiers

Le cloisonnement fait partie des principes fondamentaux de la sécurité des systèmes d'information. Lorsqu'il est appliqué à un réseau, il consiste à segmenter physiquement ou logiquement le réseau en domaines de sécurité (intranet, Wifi, DMZ, etc..). Les équipements de sécurité tels que les pare-feu, les commutateurs peuvent être utilisés à cet effet.

Lorsqu'il est appliqué à une application, on parle plutôt d'architecture applicative n-tiers. Il s'agit d'une architecture en couches. Ainsi, dans une architecture 3-tiers, on distinguera trois couches :

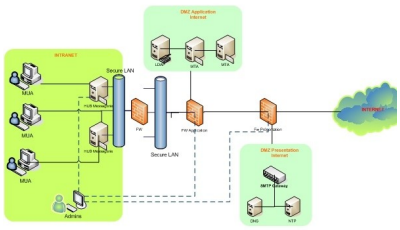
- une couche "présentation" qui est chargée de présenter les résultats traités par la couche application. Exemple : un portail web
- une couche "application" qui est chargée de traiter des données et de les mettre à la disposition de la couche présentation.
- une couche "donnée" qui est chargée de stocker des données brutes ou traitées.

Le schéma suivantt illustre un cloisonnement dans un réseau



cloisonnement-reseau

Le schéma suivant illustre une architecture applicative 3-tiers



cloisonnement-appli

3. Mise en place des dispositifs de sécurité

Sur le plan technique, la protection d'un système informatique passe par :

- la mise en place des dispositifs (matériel ou logiciel) de sécurité tels que les firewalls, IDS, HIPS, alarme, etc.
- l'installation et la configuration des logiciels de sécurité tels que les antivirus, anti-spam, etc.
- le durcissement (hardering) des dispositifs de sécurité, des serveurs et des stations de travail.
- l'installation et la configuration des dispositifs de contrôle (monitoring) afin de voir ce qui se passe aussi bien sur le réseau que sur les équipements du réseau.

Attention

Les équipements de sécurité doivent eux même être protégés et contrôlés afin de s'assurer qu'ils fonctionnent parfaitement. Quant aux logiciels de sécurité, ils doivent être mis à jour régulièrement.

4. Application des correctifs de sécurité

Les logiciels étant développés par des humains, ils sont susceptibles de contenir des erreurs. Lorsque des erreurs (failles) sont découvertes dans un logiciel, des actions sont entreprises par l'éditeur ou le responsable afin de les corriger. Ces corrections sont généralement fournies sous forme de modules appelés "patches" ou correctifs.

Il est recommandé de toujours appliquer les correctifs de sécurité aux logiciels, afin d'éviter que les failles ne soient exploitées.

C. Sur le plan mise en oeuvre opérationnelle

Assurer la sécurité d'un système informatique sur le plan mise en oeuvre opérationnelle consiste à prendre en compte tous les aspects en rapport avec la sécurité, avant, pendant et après la mise en production d'un service, d'une application ou d'un équipement.

Ces aspects peuvent porter sur :

- la définition et le suivi des contrats de maintenance avec les fournisseurs
- l'élaboration des procédures d'acquisition, de mise en place et de maintenance
- l'élaboration des manuels de procédures et le test de ces procédures. Par exemple, les procédures de gestion des incidents de sécurité.
- la sensibilisation et la formation des acteurs du système (responsable, administrateurs, utilisateurs, etc.)
- la réalisation des audits sécurité afin de s'assurer que le niveau de sécurité en place est satisfaisant
- l'élaboration d'un plan de continuité d'activités
- etc.

Les outils de sécurité des systèmes et réseaux

V

Il existe une multitude d'outils logiciels en sécurité informatique. La plupart de ces outils sont libres et gratuits. Cette partie présente quelques outils libres et gratuits, fréquemment utilisés dans le monde de la sécurité des systèmes d'information. Nous avons classé ces outils en trois catégories : réseaux, systèmes et mixtes, c'est à dire pouvant être utilisés à la fois pour les réseaux et les systèmes.

A. Les outils réseaux

1. OpenVAS (Open Vulnerability Assessment System)

OpenVAS est une excellente boîte à outils et services offrant une solution complète pour scanner les vulnérabilités réseaux. Cet outil open source remplace "NESSUS", un autre scanner de vulnérabilité qui n'est plus maintenu.

Pour plus de détails sur "OpenVAS", consultez son site officiel : *http://www.openvas.org*

2. NMAP

"NMAP" est un outil permettant de scanner un réseau afin d'identifier les services opérationnels. Cet outil est généralement utilisé par les administrateurs sécurité pour l'audit sécurité, mais aussi pas les hackers pour attaquer les systèmes. C'est un outil multi-plateforme (Unix/Linux, Windows, Mac) disposant plus d'une centaines d'options lorsqu'il est utilisé en ligne de commande.

3. Wireshark

Wireshark est un outil permettant de visualiser ce qui se passe dans un réseau. A travers la bibliothèque "libpcap", il capture les paquets qui circulent dans le réseau et fournit des informations sur ceux ci. Par exemple, à partir de Wireshark, on peut

avoir des informations sur le contenu d'un paquet (IP source et destination, protocole, etc.).

Il s'agit d'un logiciel open source placé sous la licence GPL (General Public Licence), pouvant s'exécuter sur plusieurs plates formes (UNIX/Linux, Windows, Mac)

Pour plus d'information sur cet outil, consultez son site officiel : *http://www.wireshark.org*

B. Les outils systèmes

1. AIDE (Advanced Intrusion Detection System)

AIDE est un système de détection d'intrusion basé sur les hôtes (hosts). Il s'agit d'un outil open source pouvant être installé sur des systèmes Unix/Linux. Il peut être considéré comme une clone avancée du célèbre outil de contrôle d'intégrité système "Tripwire".

Complément : Principe de fonctionnement

Une fois installé, AIDE construit une base de données de signatures de l'ensemble des fichiers (systèmes, configurations, bases de données, etc.) se trouvant sur la machine dont il est installé. Cette base de signatures est créée grâce à des algorithmes d'empreinte cryptographique des fichiers. AIDE va ensuite calculer régulièrement ces empreintes afin de garder la base toujours à jour.

Au niveau des vérifications, AIDE va comparer l'ensemble des fichiers présents sur le système aux signatures présentes dans la base de données. Si les empreintes (noms des fichiers, dates de dernière modification, etc.) sont différentes, AIDE détectera une modification de fichiers et en informera l'administrateur système soit par mail, soit par un fichier journal.

Mise en oeuvre de AIDE

La partie pratique (études de cas) de ce support contient un volet sur la mise en oeuvre de AIDE.

2. Cassage et test des mots de passe avec Medusa

Medusa est un logiciel open source de type brute-forceur d'authentification rapide. Il permet ainsi de tester la robustesse des mots de passe des services d'un système. Le mot de passe étant un élément essentiel dans la sécurité d'un système informatique, cet outil peut être utilisé aussi bien par des hackers que par des administrateurs des systèmes et réseaux.

Au moment de la rédaction de ce contenu, "Medusa" est disponible uniquement sous Unix/Linux. Les tests peuvent se faire en parallèle.

Les services pour lesquels "Medusa" peut tester les mots de passe sont nombreux : AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NCP (NetWare), NNTP, PcAnywhere, POP3, PostgreSQL, rexec, rlogin, rsh, SMB, SMTP (AUTH/VRFY), SNMP, SSHv2, SVN, Telnet, VmAuthd, VNC.

Rappel : Les caractéristiques d'un mauvais mot de passe

- Il peut facilement être deviné
- Il s'apparente à une liste de mots (dictionnaire)
- Il peut être cassé en un temps raisonnable

Remarque : Les mauvais mots de passe les plus populaires

Rang	Mot de passe	Nombre d'instances
1	123456	290,731
2	12345	79,078
3	123456789	76,790
4	Password	61,958
5	iloveyou	51,622
6	princess	35,231
7	rockyou	22,588
8	1234567	21,726
9	12345678	20,553
10	abc123	17,542

Source : *http://www.serverwatch.com*

Complément : Les mots de passe par défaut

Site de la base de données des mots de passe par défaut utilisés par les constructeurs et les éditeurs: *http://www.cirt.net/passwords*

Complément : Outils similaires à Medusa

- "Hydra" : c'est un outil proof of concept permettant de casser ou de tester les mots de passe. Il support également plusieurs protocoles.
- "John-the-ripper" : c'est un outil de cassage de mots de passe par dictionnaire. Il est disponible pour Windows, Unix/Linux et Mac. Pour en savoir plus sur John-the-ripper (Installation, configuration, utilisation), visitez ce lien : *http://www.openwall.com/john/*

Site de comparaison entre "Medusa" et "Hydra" : *http://www.foofus.net/~jmk/medusa/medusa-compare.html*

3. Autres outils systèmes

a) Nikto

"Nikto" est un outil permettant de détecter les vulnérabilités des serveurs Web. Pour plus d'information, consultez le site officiel *http://www.nikto.org*

b) SATAN

"SATAN" est un outil de test de vulnérabilités et de détection des erreurs de configuration. Pour plus d'information sur cet outil, consultez le site suivant : *http://www.satan.org*

C. Les outils mixtes (systèmes et réseaux)

1. I- BackTrack

a) Définition et description

BackTrack est une distribution Linux dédiée à l'analyse du réseau, aux tests d'intrusions et à l'audit de la sécurité des systèmes d'information. Avec plus d'une centaine d'outils de sécurité, BackTrack constitue une plate forme idéal pour les spécialistes de la sécurité.

Au moment de la rédaction de ce contenu, BackTrack est à sa version 4 avec un noyau 2.6.29.4. Cette distribution utilise le système de fichiers "squashfs" qui est un système de fichiers compressés et accessibles en lecture seule.

Entre BackTrack 4 et les versions antérieures, de nombreux changements ont eu lieu. Afin de découvrir ces changements, nous vous invitons à cliquer sur ce lien : *http://www.offensive - security.com/videos/backtrack - security - training - video/up - and - running - backtrack.html*

b) Les catégories d'outils de BackTrack

Les outils dans BackTrack sont classés par catégories. Voici quelques unes :

- BackTrack - Brutforce
- BackTrack - Discovery
- BackTrack - Passwords
- BackTrack - Spoofing
- BackTrack - Sniffers
- BackTrack - Cisco
- BackTrack - Wireless
- BackTrack - Databases
- BackTrack - Penetration

Remarque

Avec le système de catégorisation des outils, BackTrack 4 comprend également des "méta paquetages". Il s'agit d'un modèle de paquetages qui comprend plusieurs autres paquetages. Par exemple, le méta paquetages "BackTrack-web" comprend tous les outils de test de pénétration offerts par BackTrack pour les applications web.

Les méta paquetages sont regroupés en deux grandes groupes :

- "BackTrack-World" comprenant tous les méta paquetages
- "BackTrack-Desktop" contenant : "BackTrack-World", "BackTrack-Networking" et "BackTrack-multimédia"

Complément

Pour en savoir plus sur "BackTrack", consultez le site suivant : *http://www.backtrack-linux.org/*

Études des cas (document séparé)

VI

A. Case study 1 : Détection d'une intrusion dans un système Linux avec AIDE

Cette étude de cas est développée dans un document séparé. Voir module pratique.

B. Case study 2 : Utilisation de OpenVAS pour identifier les vulnérabilités d'un système

Cette étude de cas est développée dans un document séparé. Voir module pratique.

C. Case study 3 : Cassage d'un mot de passe grâce à une attaque par force brute avec MEDUSA

Cette étude de cas est développée dans un document séparé. Voir module pratique.

D. Case study 4 : Utilisation des outils de BackTrack pour attaquer le site web de la société "ELSI"

Cette étude de cas est développée dans un document séparé. Voir module pratique.

Glossaire, Webographie

VII

A. Glossaire

AFNOR : Association Française de NORmalisation
ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information (ancien DCSSI)
BP : Bonnes Pratiques
CERT : Computer Emergency Response Team
CLUSIF : CLUb de la Sécurité des systèmes d'Information Français
CNIL : Commission Nationale d'Informatique et des Libertés
DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information (devenue ANSSI)
EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité
FEROS : Fiche d'Expressions Rationnelles des Objectifs de Sécurité
HIPS : Host based Intrusion Prevention System
IDS : Intrusion Detection System
ISO : International Standardization Organization
NIDS : Network Intrusion Detection System
NSA : National Security Agency
OCTAVE : Operationally Critical Threat, Asset, and Vulnerability Evaluation
PSSI : Politique de sécurité des systèmes d'information
SI : Système d'Information
SSIC : Sécurité des Systèmes de l'Information et de la communication

B. Webographie

- Portail web de l'ANSSI : *http://www.ssi.gouv.fr/*
- Site dédié au phishing : *http://www.phishing.fr/*
- Site NBS sur la sécurité informatique : *http://www.nbs-system.com/securite-informatique/*
- Haching, IT security magazine : *http://hakin9.org/*
- MISC, le magazine français spécialisé dans la sécurité informatique :

http://www.miscmag.com/ ou *http://www.ed-diamond.com*

- SecurityFocus, site web anglophone de référence, consacré à la sécurité informatique : *http://www.securityfocus.com/*
- SANS Institute (SysAdmin, Audit, Network, Security) est une organisation regroupant près de 165 000 professionnels de la sécurité : *http://www.sans.org/*
- L'universite du SANS Institute : *http://www.sans.edu/*

Conclusion

Ce document théorique portant sur la sécurité des systèmes d'information en général et des systèmes informatiques en particulier, présente les notions, principes, méthodes et mécanismes de sécurité. Il a été élaboré dans le but de sensibiliser les étudiants de Licence de Technologie de l'Institut Universitaire de Technologie Fotso Victor de Banjoun, aux problématiques de sécurité dans les systèmes d'information.

Loin d'être une référence en la matière, il constitue tout de même un bon guide pour ceux qui aspirent aux métiers liés à la sécurité informatique. Bien que destiné aux étudiants, il peut être utilisé par des administrateurs et consultant sécurité dans le cadre de l'exercice de leurs activités.

Le document étant appelé à évoluer, nous restons très sensibles à vos retours. Cela nous permettra de l'améliorer.