République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira Bejaia
Faculté des Sciences Exactes
Département d'Informatique

Support de cours

Module : Sécurité des Réseaux

Niveau : 2ème année Master Réseaux et Systèmes Distribués

Etabli par Dr. HAMZA Lamia

2021/2022

Table des matières

Introduction générale 5
Chapitre 1 : Introduction à la sécurité des réseaux informatiques 6
Introduction 6
Cours 1 : Généralité, vulnérabilités, évaluation des risques 6
1. Principe de la sécurité 6
2. Vulnérabilité 6
3. Etude des risques 7
3.1 Types de risques 7
3.2 Précautions à prendre 8
Cours 2 : Menaces et Attaques 9
1. Menaces 9
2. Logiciel malveillant (malware) 9
3. Attaques 10
3.1. Types d'attaques 10
3.2. Quelques attaques 11
Cours 3 : L'authentification 14
1. Principe de l'authentification 14
2. Protocole d'authentification pour PPP : PAP, CHAP 14
2.1. Présentation du protocole PAP 14
2.2. Présentation du protocole CHAP 15
3. RADIUS (Remote Authentication Dial-In User Service) 16
3.1. Fonctionnement de RADIUS 16
4. Kerberos 16
4.1. Les principales composantes de Kerberos 16
4.2. Les différents types de tickets 17
4.3. Principales étapes du protocole Kerberos 17
5. Exercices 18
6. Corrigé des exercices 21
Conclusion 24
Chapitre 2 : Politiques et modèles de sécurité 25
Introduction 25
1. Notion d'objet, de sujet et de droit d'accès 25

2. Modèles de sécurité 26
2.1. Politiques et modèles d'autorisation discrétionnaires (DAC) 26
2.2. Politiques et modèles d'autorisation obligatoires (MAC) 27
2.3. Politique et modèle de sécurité par rôles (RBAC) 30
3. Exercice 30
4. Corrigé de l'exercice 30
Conclusion 31
Chapitre 3 : Sécurité des réseaux 32
Introduction 32
Cours 1 : Système de détection d'intrusions 32
1. Définition 32
2. Méthode de détection 33
3. Description d'un système de détection d'intrusions 33
Cours 2 : Firewall 36
1. Définition 36
2. Fonctionnement d'un système pare-feu 36
3. Filtrage simple de paquets 37
4. Filtrage dynamique 37
5. Filtrage applicatif 38
6. Notion de pare-feu personnel 38
Cours 3 : VPN 39
1. Définition 39
2. Fonctionnement d'un VPN 39
3. Architectures VPN 40
3.1. VPN d'accès 40
3.2. VPN Intranet 40
3.3. VPN Extranet 40
4. Protocoles sécurisés pour VPN 41
4.1. PPTP 41
4.2. L2TP 41
4.3. IPSec 42
5. Exercices 43
6. Corrigé des exercices 44
Conclusion 46

Chapitre 4 : Les applications sécurisées 47
Introduction 47
1. PGP (Pretty Good Privacy) 47
1.1. Principe de PGP 47
2. S/MIME (Secure / Multipurpose Internet Mail Extensions) 48
3. SSH (Secure Shell) 48
4. SSL (Secure Socket Layer) 49
5. SET (Secure Electronic Transaction) 50
6. Exercice 50
7. Corrigé de l'exercice 50
Conclusion 51
Chapitre 5 : Sécurité des bases de données 52
Introduction 52
1. Sécurité discrétionnaire 52
2. Sécurité obligatoire 53
2.1. Granularité de la classification 53
2.2. Gestion des leurres 54
Conclusion 55
Sujet d'examen en ligne (2020/2021) 56
Conclusion générale 62
Bibliographie 63

Introduction générale

Avec le besoin grandissant d'ouverture des systèmes à Internet, la sécurisation des systèmes est devenue un souci majeur. De ce fait, il est primordial pour un étudiant en informatique d'étudier la sécurité des réseaux informatiques.

Ce support de cours, dédiés aux étudiants ayant déjà des prérequis sur les réseaux et la cryptographie, présente les concepts de base liés à la sécurité des réseaux informatique. Il comprend cinq chapitres. Le premier chapitre s'intitule «**Introduction à la sécurité des réseaux informatiques**», il a pour objectifs d'initier l'étudiant aux fondements de la sécurité des réseaux informatiques. Le deuxième chapitre, intitulé «**Politiques et modèles de sécurité**», présente des modèles importants de politiques de sécurité. Comme les politiques discrétionnaires (ou DAC pour Discretionary Access Control) et les politiques obligatoires (ou MAC pour Mandatory Access Control). Le troisième chapitre, nommé «**Sécurité des réseaux**», présente les mécanismes les plus importants de la sécurité des réseaux informatiques. À savoir, les systèmes de détection d'intrusions, les par-feux (ou firewalls) et les réseaux privés virtuels (ou les VPNs pour Virtual Private Network). Le quatrième chapitre, intitulé «**Les applications sécurisées PGP, S/MIME, SSH, SSL, SET** », porte sur les applications de messagerie (PGP, S/MIME), les protocoles du commerce électronique (SSL et SET) et la transmission sécurisée via SSH. Le cinquième chapitre, intitulé «**Sécurité des bases de données**», étudie l'applicabilité des modèles DAC et MAC pour sécuriser les bases données.

Afin de rendre le document encore plus utile, pour les quatre premiers chapitres, il y a une série d'exercices ainsi que leurs corrigés. Ces exercices peuvent donner l'occasion à l'étudiant de tester ses connaissances acquises et de vérifier sa compréhension.

Chapitre 1 : Introduction à la sécurité des réseaux informatiques

Introduction

Ce chapitre a pour objectifs d'initier l'étudiant aux concepts de base de la sécurité des réseaux informatiques. Il contient trois cours ; le premier cours présente les concepts de vulnérabilité et d'analyse des risques, le deuxième cours présente quelques attaques réseaux et le troisième cours présente les protocoles d'authentification (PAP, CHAP, RADIUS et Kerberos).

Cours 1 : Généralité, vulnérabilités, évaluation des risques

1. Principe de la sécurité

La sécurité informatique : c'est l'ensemble des moyens mises en œuvre pour réduire la vulnérabilité d'un système contre les menaces afin d'assurer :

- **La confidentialité** : assure que l'information n'est lue que par les personnes autorisées.
- **L'intégrité** : l'information ne peut être modifiée que par les personnes autorisées.
- **La disponibilité** : l'information soit disponible pour les personnes autorisées.

2. Vulnérabilité

Une vulnérabilité est une faille dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité du système, c'est-à-dire à son fonctionnement normal, ou à la confidentialité ou l'intégrité des données qu'il contient.

<u>Remarque</u> : le meilleur moyen d'assurer la sécurité c'est d'évaluer d'abord les risques.

3. Etude des risques

Il s'agit d'identifier les problèmes potentiels avec les solutions et les coûts associés. L'ensemble des solutions doit être organisé sous forme d'une politique de sécurité cohérente.

∗ ***L'importance de mesurer les risques :***

- Identifier des failles,
- Evaluer les valeurs des éléments informatiques,
- Donner des priorités de correction,
- Elaborer des expertises,
- Définir une politique de sécurité adaptée.

3.1 Types de risques

3.1.1. Risques humains

Ce sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

1) la **maladresse** (commettre des erreurs) : exécuter un traitement non souhaité, effacer involontairement des données ou des programmes, etc.
2) **l'inconscience** et **l'ignorance** : introduire des programmes malveillants sans le savoir (par exemple lors de la réception de courrier).
3) la **malveillance** : impossible d'ignorer les différents problèmes de virus et de vers ces dernières années.
4) **l'ingénierie sociale** (social engineering) : est une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins.

   Elle consiste à :

   ∗ se faire passer pour quelqu'un que l'on n'est pas (en général un administrateur).

   ∗ demander des informations personnelles (nom de connexion, mot de passe, données confidentielles, etc.). En inventant un quelconque prétexte (problème dans le réseau, modification de celui-ci, etc.).

   L'ingénierie sociale peut se faire soit au moyen d'une simple communication téléphonique, soit par mail, soit en se déplaçant directement sur place.

5) **l'espionnage** (surtout industriel) : permet d'obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, etc.

3.1.2. Risques matériels

Ils sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels.

1) **Incidents liés** au **matériel** : les composants électroniques, produits en grandes séries, peuvent comporter des défauts et tomber en panne.
2) **Incidents liés** au **logiciel** : les programmeurs peuvent faire des erreurs de manière individuelle ou collective que les meilleurs outils de test ne peuvent pas éliminer en totalité.
3) **Incidents liés** à **l'environnement** : les machines électroniques et les réseaux de communication sont sensibles aux variations de température ou d'humidité (cas d'incendie ou d'inondation) ainsi qu'aux champs électriques et magnétiques.

3.2 Précautions à prendre

Dans le cas des risques matériels il est possible d'assurer :

- **redondance des matériels** : En doublant ou en triplant un équipement, on divise le risque total par la probabilité de pannes simultanées.
- **dispersion des sites** : un accident (incendie, tempête, tremblement de terre, etc.) a très peu de chances de se produire simultanément en plusieurs endroits dispersés.
- **procédures de contrôles indépendants** : te que les audits de sécurité qui permettent de découvrir les anomalies avant qu'elles ne produisent des effets indésirables.

Cours 2 : Menaces et Attaques

1. Menaces

Une menace est une violation potentielle de la sécurité, c'est-à-dire un signe qui laisse prévoir un danger. Elle peut être accidentelle ou intentionnelle, cette dernières peut être passive et active :

a) **Menace accidentelle :** ces menaces sont dues aux accidents (inondation, panne d'équipements et toute catastrophe naturelle, etc.).

b) **Menace intentionnelle** :

1) **Menace passive :** consiste à écouter ou copier des informations de manière illicite.
2) **Menace active :** consiste à altérer (modifier) des informations ou à altérer le bon fonctionnement d'un service.

2. Logiciel malveillant (malware)

Nous présentons dans cette Section un type de menace active qui est le malware :

Un malware est un terme anglais signifiant nuisible (malveillant). Un "malware" est donc un logiciel pouvant être un virus, vers, chevaux de Troie, backdoors, spywares, etc. :

- **Virus** : un virus est un fragment de code qui se propage à l'aide d'autres programmes.
- **Les vers :** un ver est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.) pour se propager.
- **Les chevaux de Troie ou Trojans :** le trojan est un logiciel de très petite taille (quelques lignes de code seulement) qui est dissimulé au sein d'un autre programme utile pour son destinataire. Il se présente comme un programme, son installation sur la machine repose principalement sur l'ingénierie sociale : abuser la victime pour qu'elle installe elle-même le cheval de Troie. Du code malicieux peut être caché dans un logiciel connu (la victime croit, à tort, installer un logiciel "sain") ou dans un logiciel conçu spécialement pour transporter le programme malicieux (jeux, utilitaire gratuit diffusé sur Internet, etc.).

- **Backdoor :** un programme backdoor (littéralement porte arrière mais traduit par porte dérobée) est un petit bout de code introduit en général par un pirate informatique pour pouvoir ouvrir un accès dérobé sur un système informatique et ainsi prendre le contrôle de celui-ci quand il le désire. La porte dérobée peut être installée directement par le pirate alors qu'il a eu accès à la machine de manière ponctuelle (par exemple l'administrateur s'est absenté quelques instants sans bloquer sa session). Il peut aussi avoir recours à un exploit, un virus ou encore un cheval de Troie.
- **Spyware :** logiciel qui transmet des informations privées.
- **etc.**

3. Attaques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une attaque est une **concrétisation** d'une menace. Autrement dit, une **attaque** est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système et généralement dommageables.

3.1. Types d'attaques

a. Attaque directe : c'est la plus simple des attaques, l'intrus attaque directement la victime à partir de son ordinateur.

Figure 1 : Attaque directe

Du point de vue de l'administrateur l'avantage de ces attaques est qu'on peut remonter facilement à l'origine.

b. Attaque indirecte par rebond : l'intrus attaque la victime par un ordinateur intermédiaire.

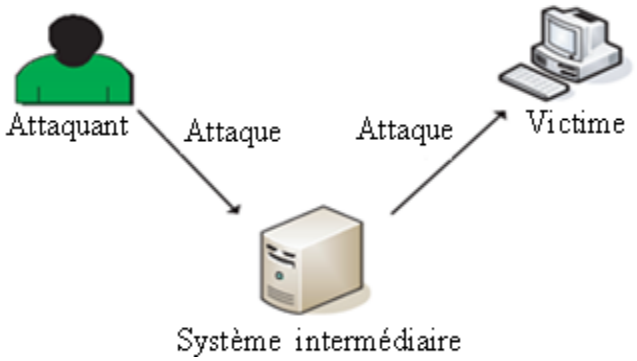

Figure 2 : Attaque indirecte par rebond

Du point de vue de l'intrus l'avantage du rebond est de masquer son identité et d'utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante, etc.) pour attaquer.

c. **Attaque indirecte par réponse :** Cette attaque est une variante de l'attaque par Rebon. Elle offre les mêmes avantages (du point de vue de l'intrus). Mais au lieu qu'il envoie une attaque à l'ordinateur, il lui envoie une requête et la réponse à cette requête sera envoyée à la victime.

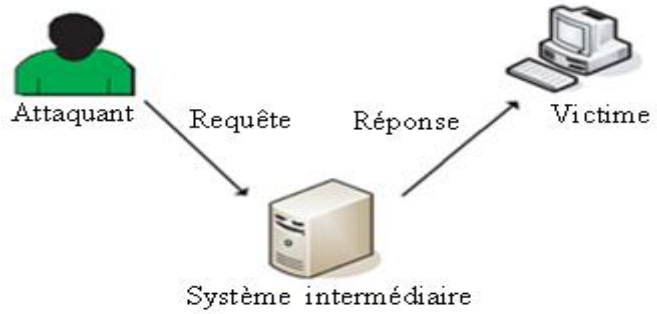

Figure 3 : Attaque indirecte par réponse

3.2. Quelques attaques

Le déni de service (DoS, Denial of Service)

Dans cette partie nous allons citer deux types d'attaques DoS, Smurf et TCP-SYN/Flooding

3.2.1 Smurf

La technique du "smurf" est basée sur l'utilisation de serveurs broadcasts pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

Le scénario d'une attaque est le suivant :

1) La machine attaquante envoie un ping[1] à un ou plusieurs serveurs broadcasts en falsifiant l'adresse IP source (adresse à laquelle le serveur devrait théoriquement répondre) et en fournissant l'adresse IP d'une machine cible.
2) Le serveur broadcast répercute la requête sur l'ensemble du réseau.
3) Toutes les machines du réseau envoient une réponse au serveur broadcast.
4) Le serveur broadcast redirige les réponses vers la machine cible.

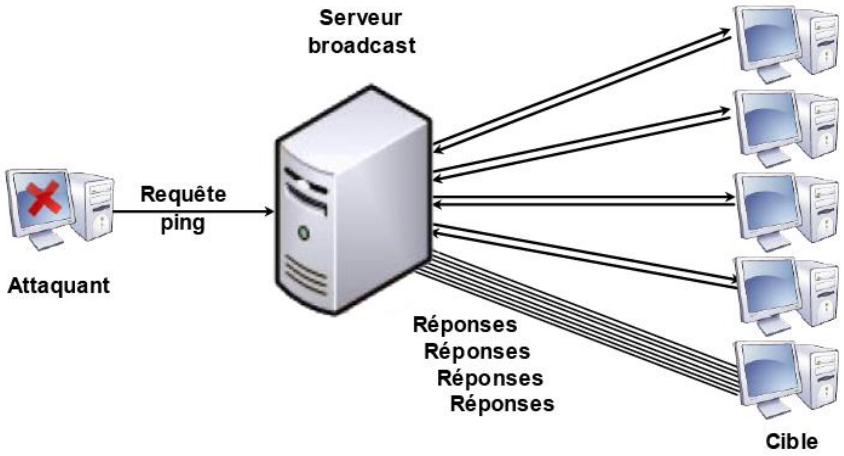

Figure 4 : Attaque smurf

3.2.2 TCP-SYN/Flooding

Quand un système client essaie d'établir une connexion TCP au près d'un serveur, le client et le serveur échangent une séquence de messages comme illustrés dans la Figure 5 :

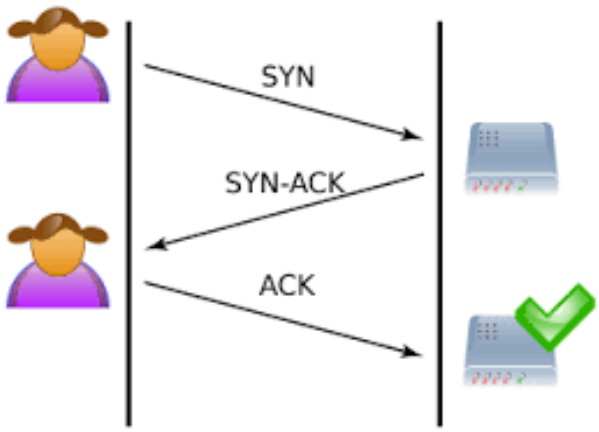

Figure 5 : Une connexion TCP

[1] le ping est un outil exploitant le protocole ICMP, permettant de tester les connexions sur un réseau en envoyant un paquet et en attendant la réponse.

Les excès viennent au moment où le serveur a renvoyé un SYN-ACK mais n'a pas reçu le ACK du client. C'est alors une connexion partiellement ouverte. En créant excessivement de connexions partiellement ouvertes un dépassement de capacité peut se créer.

La figure 6 montre que le message ACK de confirmation finale ne sera jamais renvoyé au serveur victime.

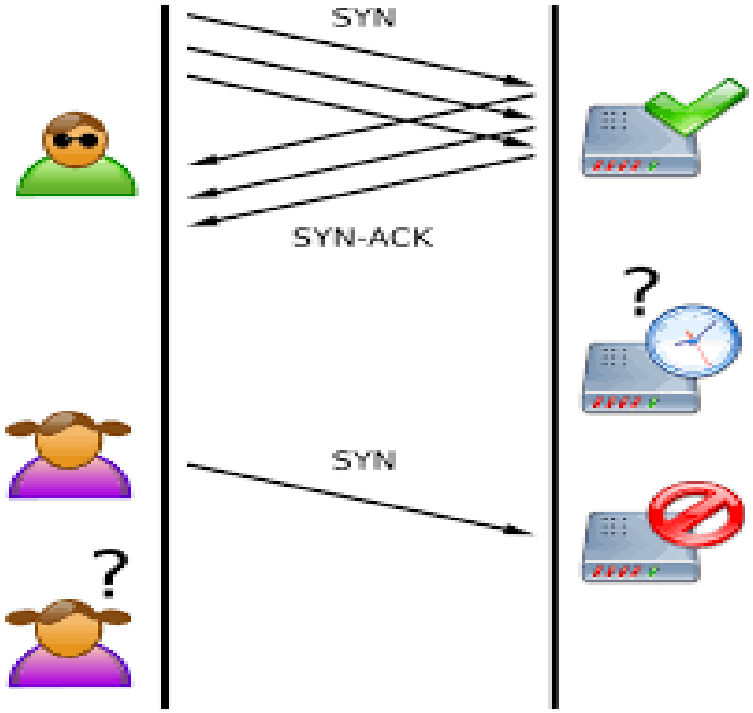

Figure 6 : Attaque TCP-SYN/Flooding

Cours 3 : L'authentification

1. Principe de l'authentification

Un service d'authentification repose sur deux composantes :

1) L'identification dont le rôle est de définir les identités des utilisateurs ;
2) L'authentification permettant de vérifier les identités présumées des utilisateurs.

Le processus d'authentification s'effectue en vérifiant la correspondance des informations fournies par l'utilisateur avec celles contenues dans la base de données. Si elles concordent alors, l'utilisateur se voit accorder l'accès au système de sécurité.

Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle d'authentification simple. Lorsque l'authentification nécessite plusieurs facteurs, on parle alors d'authentification forte.

L'authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

- Un élément d'information que l'utilisateur connaît (mot de passe, etc.)
- Un élément que l'utilisateur possède (carte à puce, etc.)
- Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (empreinte digitale, ADN, etc.)

2. Protocole d'authentification pour PPP : PAP, CHAP

Le protocole de réseau WAN, PPP (Point to Point Protocol), permet une connexion entre routeurs ou un hôte et un routeur. Par rapport à d'autres protocoles, PPP permet de prendre en charge plusieurs modes d'authentification tels que PAP et CHAP.

2.1. Présentation du protocole PAP

Le protocole PAP (Password Authentication Protocol) est un protocole d'authentification qui permet d'identifier un utilisateur lors de sa connexion à un serveur Internet. Lors de cette

authentification, le mot de passe est transmis en clair. Le protocole PAP est utilisé avec le protocole PPP. Il s'agit d'un protocole d'autorisation d'accès pour l'ouverture d'une session sur le réseau.

2.1.1. Fonctionnement du protocole PAP

Le principe du protocole PAP est le suivant : Une table de noms d'utilisateurs et de mots de passe est stockée sur un serveur. Lorsqu'un utilisateur s'identifie, son nom et son mot de passe sont transmis au serveur pour une vérification.

- **Une authentification au protocole PAP se fait en 4 étapes :**

1) Le processus serveur PPP envoie une requête d'authentification spécifiant l'utilisation du protocole PAP ;
2) Le client accepte de s'authentifier, il répond alors avec son nom PAP qui est très souvent correspondant au nom d'utilisateur ainsi qu'avec son mot de passe ;
3) Le serveur valide ou rejette la connexion avec un acquittement positif ou négatif ;
4) Cette requête d'acquittement peut contenir du texte visant à informer l'utilisateur de l'état de la connexion.

2.2. Présentation du protocole CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol) est un protocole d'authentification basé sur la résolution d'un défi (en anglais challenge).

- **Les étapes du défi sont les suivantes :**

1) Un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoie ;
2) La machine distante « hache » ce nombre, le compteur ainsi que sa clé secrète (le mot de passe) avec l'algorithme de hachage MD5 et le renvoie sur le réseau ;
3) Le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur ;
4) Si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue.

Remarque : Le protocole CHAP améliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau.

3. RADIUS (Remote Authentication Dial-In User Service)

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé **NAS** (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré et authentifié grâce à un secret partagé.

3.1. Fonctionnement de RADIUS

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

1) Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
2) Le NAS achemine la demande au serveur RADIUS ;
3) Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
   - **ACCEPT** : l'identification a réussi ;
   - **REJECT** : l'identification a échoué ;
   - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » ;
   - **GHANGE PASSWORD** : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

4. Kerberos

Kerberos est l'un des systèmes d'authentification les plus répandus dans les systèmes distribués. C'est un système client-serveur basé sur la cryptographie symétrique.

4.1. Les principales composantes de Kerberos

- Les principals représentant les divers usagers, applications et services voulant s'authentifier les uns aux autres.
- Le Key Distribution Center (KDC) est la composante principale de l'architecture. Cette composante offre les deux principaux services :
  - Authentication Service (AS) : Serveur de clés authentifiant un principal.

- Ticket Granting Service (TGS) : Serveur de tickets offrant à un principal un ticket permettant d'être authentifié par un autre principal. Ce ticket peut contenir aussi les droits d'accès du principal.

Donc, le KDC se doit de conserver tous les secrets et les clés cryptographiques permettant d'effectuer les diverses opérations.

4.2. Les différents types de tickets

Le protocole Kerberos nécessite la mise en place de deux types de tickets différents : les tickets TGT et les tickets TGS.

a) Les TGT: Ticket Granting Ticket

Les TGT ("ticket d'octroi de ticket") sont des tickets délivrés par le serveur Kerberos (AS) lors de la première authentification du client (lorsque celui-ci ouvre sa session). Il permet au client d'accéder au service de délivrement de tickets TGS. Ce ticket a une durée de vie relativement longue afin de permettre au client de s'authentifier pour plusieurs services différents sans avoir à fournir de nouveau ses paramètres d'authentification.

b) Les TGS: Ticket Granting Service

Les TGS ("ticket d'accès au service") sont fournis au client par le service de délivrement de tickets TGS lorsqu'un TGT valide lui a été présenté. Ce ticket est garant de l'identité de la personne qui le transporte, il permet donc au client d'accéder au service demandé. La durée de vie de ce ticket est relativement courte afin d'empêcher un utilisateur étranger qui aurait subtilisé le ticket d'accéder aux ressources du serveur d'application.

4.3. Principales étapes du protocole Kerberos

Le procédé d'authentification Kerberos est composé de quatre entités (voir Figure 1) : le client (C), le serveur de clés (AS), le serveur de tickets (TGS) et le Serveur qui offre le service désiré. Le client s'adresse successivement à chacun de ces serveurs.

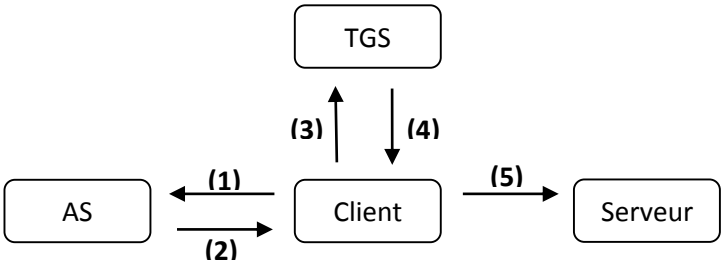

Figure 1 : Schéma d'authentification Kerberos.

(1) : un client C envoie à AS une requête contenant son identité et l'identité du TGS qu'il souhaite contacter afin d'obtenir un TGT

(2) $[\{K_{C,TGS}\}K_C , \{TGT\}K_{TGS}]$: AS envoie la clef de session $K_{C,TGS}$ chiffrée avec K_C qui sera utilisée par C et TGS, ainsi que le ticket TGT chiffré par le clef K_{TGS} de TGS. Le ticket TGT contient l'identité du client, une copie de la clé de session $K_{C,TGS}$ ainsi qu'une période de validité du ticket.

(3) $[\{A_C\}K_{C,TGS}, \{TGT\}K_{TGS}, S]$: C envoie TGT à TGS accompagné d'un authentificateur A_C contenant l'identité du client et l'horodatage. L'authentificateur est chiffré avec la clef de session $K_{C,TGS}$.

(4) $[\{K_{C,S}\}K_{C,TGS} , \{TS\}K_S]$: TGS envoie au client la clef de session $K_{C,S}$ chiffrée avec $K_{C,TGS}$ qui sera utilisée par le client et le serveur, ainsi que le ticket de service (TS) chiffré avec la clef K_S du serveur. Le ticket TS contient l'identité du client, une copie de la clé de session $K_{C,S}$ ainsi qu'une période de validité du ticket.

(5) $[\{A_C\}K_{C,S}, \{TS\}K_S]$: Le client envoie TS au serveur accompagné d'un authentificateur A_C contenant l'identité du client et l'horodatage. L'authentificateur est chiffré avec la clef de session $K_{C,S}$.

5. Exercices

Exercice 1

1. Quels sont les objectifs de la sécurité informatique ?
2. Quelles sont les différences entre une attaque passive et une attaque active ?
3. Quelles sont les conditions de succès d'une attaque ?
4. Quelle est la différence entre un virus et un ver ?
5. Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
6. Qu'est-ce qu'une "porte dérobée" ?

7. Qu'est-ce qu'un "cheval de Troie" ?

Exercice 2

L'organisme spatial Fusépartair possède un ordinateur stockant des informations sensibles, relatives au satellite géostationnaire Givouapa-Granschoze. L'accès aux données de cette machine (qui n'est reliée à aucun réseau) nécessite d'effectuer les trois contrôles suivants :

(1) authentification par *carte à puce* pour l'accès au bâtiment ;
(2) authentification par *système biométrique* pour l'accès à la salle sécurisée ;
(3) authentification par *mot de passe* pour l'accès à l'ordinateur.

Nous nous intéressons uniquement aux deux premiers contrôles d'accès. Pour chacun de ces contrôles, l'utilisateur doit saisir un identifiant (*Username*) ; on suppose que les identifiants des utilisateurs sont publiques. La Figure 2 représente le plan du bâtiment contenant la machine convoitée, en faisant apparaître l'emplacement des systèmes de contrôle d'accès et du serveur d'authentification, ainsi que les connexions entre ces entités. Aucun de ces dispositifs n'est relié à un autre réseau. On s'intéresse dans la suite de cet exercice à un espion, Jean Bond, dont l'objectif est d'accéder aux données relatives à Givouapa-Granschoze.

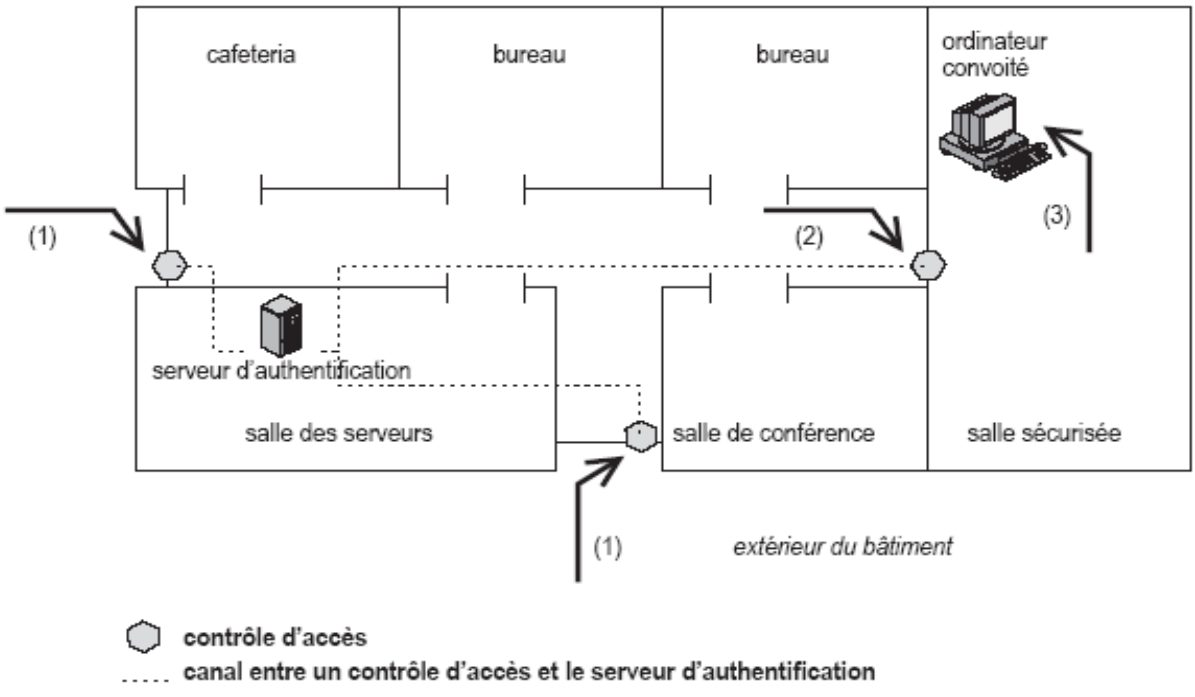

Figure 2 : *Contrôles d'accès biométrique, par carte et par mot de passe de la société Fusipartair.*

Accès au bâtiment par carte à puce

Afin d'accéder au bâtiment, chaque employé autorisé possède une carte à puce contenant son identifiant et une clé privée qui lui est associée. Pour s'authentifier, l'employé insère sa carte dans un lecteur relié à un serveur d'authentification, puis les deux étapes suivantes sont effectuées. L'utilisateur saisit son numéro d'identification personnel (NIP ou en anglais PIN : *Personal Identification Number*) à 4 chiffres sur le clavier du lecteur. La carte vérifie le NIP. Si celui-ci est correct, elle accepte de passer à la seconde étape. Dans le cas contraire, l'utilisateur peut effectuer de nouvelles tentatives, mais la carte se bloque définitivement après trois tentatives infructueuses consécutives. Elle doit ensuite s'authentifier auprès du serveur d'authentification car l'authentification n'est pas réalisée par les lecteurs de cartes eux-mêmes. Pour cela, un protocole par question-réponse est utilisé comme suit : le serveur envoie une valeur aléatoire à la carte ; la carte signe cette valeur avec sa clé privée et renvoie cette signature avec son identifiant au serveur ; le serveur vérifie que la signature est correcte en utilisant la clé publique correspondant à la carte. Le cas échéant, le serveur déclenche une procédure permettant d'ouvrir la porte du bâtiment (on ne s'intéresse pas dans cet exercice à la sécurité de la procédure d'ouverture de la porte).

1. Pourquoi considère-t-on que 4 chiffres sont suffisants pour le NIP de la carte alors que l'on estime qu'un mot de passe doit contenir au moins 8 caractères dans un alphabet suffisamment grand ?
2. Quel est l'intérêt de fonder le protocole d'authentification sur un système asymétrique plutôt que sur un système symétrique ?

Accès à la salle sécurisée par authentification biométrique

Le contrôle d'accès à la salle sécurisée se fait par authentification biométrique fondée sur l'empreinte digitale. L'utilisateur saisit son identifiant sur le clavier du lecteur et pose un doigt bien défini sur le boitier. L'empreinte est numérisée et envoyée au serveur d'authentification (le même que dans la question précédente) qui accepte ou refuse l'accès à la salle (comme auparavant, on ne s'intéresse pas au mécanisme d'ouverture de la porte de la salle). Le serveur d'authentification possède un certificat qui lie l'identifiant de la personne à son empreinte digitale. Des analyses statistiques ont montré que le taux de fausses acceptations du système biométrique de Fusépatair est de 0,01% et le taux de faux rejets est de 15%. Comme avec le système d'authentification par carte à puce, l'utilisateur dispose de

plusieurs essais : après cinq tentatives infructueuses consécutives, le service de sécurité est alerté et l'utilisateur interpellé.

3. Expliquer ce qu'est une fausse acceptation et un faux rejet. Les taux proposés sont-ils adaptés à une telle application ?
4. Si Jean est en mesure de trafiquer le lecteur à sa guise, quelle information intéressante peut-il obtenir ? Comment l'exploiter ?

Exercice 3

On considère un pirate qui écoute le réseau et voit passer le ticket que le TGS envoie au client. Le pirate connaît aussi l'identité du client à qui est destiné le ticket. Qu'est-ce qui empêche le pirate d'utiliser le ticket pour obtenir un service à la place du client légitime ?

6. Corrigé des exercices

Exercice 1

1) Quels sont les objectifs de la sécurité informatique ?

Les principaux objectifs de sécurité informatique sont de réaliser la confidentialité, l'intégrité, la disponibilité des données et des services des systèmes. Diverses mesures de sécurité permettent de les atteindre. Parmi elle nous pouvons citer : le contrôle d'accès, le chiffrement des données, la gestion : des incidents, des erreurs des dysfonctionnements, des intrusions, etc.

2) Quelles sont les différences entre une attaque passive et une attaque active ?

Les attaques passives n'altèrent pas la cible de l'attaque (écoute non autorisées, interception de flux sans modification, collecte d'information à l'insu du propriétaire par exemple), tandis que les attaques actives portent atteintes à l'environnement ciblé (perte d'intégrité, de disponibilité, vol, destruction, déni de service, etc.)

3) Quelles sont les conditions de succès d'une attaque ?

Les principaux facteurs de succès de réalisation d'une attaque sont liés essentiellement à la connaissance de la cible et de ses vulnérabilités (récolte d'information sur la cible, scan des ports de communication, détection des failles, etc.), à la capacité de rendre l'attaque non détectable, à la capacité de ne pas laisser de traces et à la célérité de réalisation de l'attaque.

4) *Quelle est la différence entre un virus et un ver ?*

Un virus est un fragment de code qui se propage à l'aide d'autres programmes alors qu'un ver est un programme autonome.

5) *Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?*

Même s'ils ne provoquent aucun dommage sur les machines, ces vers utilisent les ressources du réseau pour se propager, au détriment des communications utiles.

6) *Qu'est-ce qu'une "porte dérobée" ?*

Une porte dérobée est un programme qui permet à un pirate de contourner les contrôles de sécurité d'un système informatique. Un tel programme peut lui permettre par exemple d'avoir accès à une machine, physiquement ou à distance, sans avoir besoin de mot de passe.

7) *Qu'est-ce qu'un "cheval de Troie" ?*

Un cheval de Troie est un programme qui cache des fonctionnalités malicieuses. Typiquement, un cheval de Troie est utilisé pour permettre à un pirate de prendre le contrôle à distance d'une machine, c'est-à-dire pour installer une porte dérobée.

Exercice 2

1. *Pourquoi considère-t-on que 4 chiffres sont suffisants pour le NIP de la carte alors que l'on estime qu'un mot de passe doit contenir au moins 8 caractères dans un alphabet suffisamment grand ?*

   Contrairement aux mots de passe, où 8 caractères alphanumériques choisis aléatoirement dans un alphabet suffisamment grand sont considérés comme nécessaires, les systèmes utilisant des cartes à puce ne requièrent généralement que 4 chiffres.

   Deux grandes différences entre ces systèmes justifient ce fait :

   - Il est avant tout nécessaire de voler la carte avant de pouvoir mener une attaque pour retrouver le NIP.
   - La carte se bloque d'elle-même après trois tentatives infructueuses successives.

2. *Quel est l'intérêt de fonder le protocole d'authentification sur un système asymétrique plutôt que sur un système symétrique.*

   Dans l'authentification fondée sur la cryptographie symétrique (secret partagé), le serveur devient un point sensible dont la confidentialité des données est primordiale. La confidentialité des données stockées n'est évidemment pas nécessaire lorsque le système d'authentification repose sur la cryptographie asymétrique : l'utilisateur conserve sa clé privée alors que le serveur ne stocke que des clés publiques.

3. *Expliquer ce qu'est une fausse acceptation et un faux rejet. Les taux proposés sont-ils adaptés à une telle application ?*

   On dit que le système d'authentification a généré une fausse acceptation lorsque l'empreinte d'une personne non autorisée à pénétrer dans le système, a passé le contrôle d'accès biométrique avec succès. On parle de faux rejet lorsque l'empreinte d'une personne autorisée a été rejetée. Sachant que dans les technologies existantes le taux de fausses acceptations (TFA) et le taux de faux rejets (TFR) sont liés (augmenter l'un revient à diminuer l'autre et vice-versa), il est primordial, dans l'application présente, que le TFA soit très inférieur au TFR. Le fait que l'utilisateur dispose de 5 tentatives pour s'authentifier relativise le TFR qui est relativement élevé. (100 tentatives correctes ---> 15 rejetées alors 5 tentatives correctes ---> 0,75 rejetée)

4. *Si Jean est en mesure de trafiquer le lecteur à sa guise, quelle information intéressante peut-il obtenir ? Comment l'exploiter ?*

   Si Jean est en mesure de trafiquer le lecteur d'empreintes digitales à sa guise, il pourra recueillir sans difficulté les empreintes numériques des utilisateurs venant s'authentifier. Il pourra alors les réutiliser en les envoyant directement au serveur.

Exercice 3

Un pirate qui voit passer un ticket en écoutant l'échange (4), ne pourrait pas pour autant s'en servir auprès du serveur pour les deux raisons suivantes :

1) Ne connaissant pas la clé de session entre le client et le serveur, le pirate ne peut pas créer d'authentificateur valide, c.à.d. qui serait accepté par le serveur.

2) Le pirate ne peut pas réutiliser un authentificateur qui aurait déjà été accepté une première fois par le serveur car l'authentificateur contient un horodatage indiquant la date et l'heure de sa création.

Conclusion

À l'issue de ce chapitre l'étudiant comprend mieux les notions de menaces, vulnérabilités et attaques. Il conclut qu'il faut d'abord passer par l'analyse des risques avant de penser à élaborer une politique de sécurité. De plus, il aura la maitrise d'un mécanisme de sécurité qui est l'authentification.

Chapitre 2 : Politiques et modèles de sécurité

Introduction

Après l'authentification et avant l'accès de l'utilisateur à la ressource désirée, il est primordial de vérifier si l'utilisateur est autorisé à accéder à cette ressource. Ce chapitre permettra à l'apprenant de connaitre les principaux modèles de contrôle d'accès. Il commence par présenter le contrôle d'accès discrétionnaire, notamment le modèle de Lampson et le modèle de Harrison Ruzzo Ullmann. Par la suite, il expose les modèles de contrôle d'accès obligatoire comme les modèles Bell LaPadula et Biba. Enfin, le contrôle d'accès basé sur les rôles est présenté brièvement.

1. Notion d'objet, de sujet et de droit d'accès

La plupart des politiques de sécurité reposent sur les notions de sujets, d'objets et de droits d'accès.
Un **sujet** est une entité active, correspondant à un processus qui s'exécute pour le compte d'un utilisateur.
Un **objet** est une entité considérée comme passive qui contient ou reçoit des informations (fichiers, relations dans une base de données relationnelle, etc.).

Les actions (ou Opérations) permettent aux sujets de manipuler les objets (lecture d'un fichier, requête dans une base de données).

À un instant donné, un sujet à un **droit d'accès** sur un objet si et seulement si le processus correspondant au sujet est autorisé à exécuter l'opération correspondant à ce type d'accès sur cet objet.

2. Modèles de sécurité

Les politiques de sécurité se classent en deux grandes catégories : les politiques discrétionnaires (ou DAC pour Discretionary Access Control) et les politiques obligatoires (ou MAC pour Mandatory Access Control). Il existe également des variantes de ces politiques qui peuvent mieux s'adapter à des organisations particulières, comme les politiques basées sur la notion de rôles (ou RBAC pour Role-Based Access Control).

2.1. Politiques et modèles d'autorisation discrétionnaires (DAC)

Dans le cas d'une politique discrétionnaire, les droits d'accès à chaque information sont manipulés librement par le responsable de l'information (le propriétaire), à sa discrétion. Les droits peuvent être accordés par ce responsable à chaque utilisateur, à des groupes d'utilisateurs, ou bien aux deux. Ceci peut parfois amener le système dans un état d'insécurité. Une politique discrétionnaire n'est donc applicable que dans la mesure où il est possible de faire totalement confiance aux utilisateurs et aux sujets qui s'exécutent pour leur compte.

Dans le modèle d'autorisation discrétionnaire un utilisateur peut transmettre plus de droits que nécessaires à un autre utilisateur.

Exemple :

Un droit d'accès peut être transmis sans que son propriétaire soit informé : A donne un droit en lecture à B sur un de ses fichiers, B copie ce fichier, B étant propriétaire de la copie, transmet son droit de lecture à C.

2.1.1. Quelques modèles associés aux DAC

a) Modèle de Lampson

La notion de matrice de contrôle d'accès, dédiée à la représentation des droits d'accès, a été introduite par Lampson dès 1971. Les droits d'accès peuvent être symboliquement représentés dans une matrice de droits d'accès dont les lignes représentent les sujets et les colonnes représentent les objets. Une cellule de la matrice contient donc les droits d'accès d'un sujet sur un objet. La matrice est gérée conformément aux règles définies dans la politique de sécurité. Les droits correspondent généralement à des actions élémentaires telles que " lire " ou " écrire ".

Exemple :

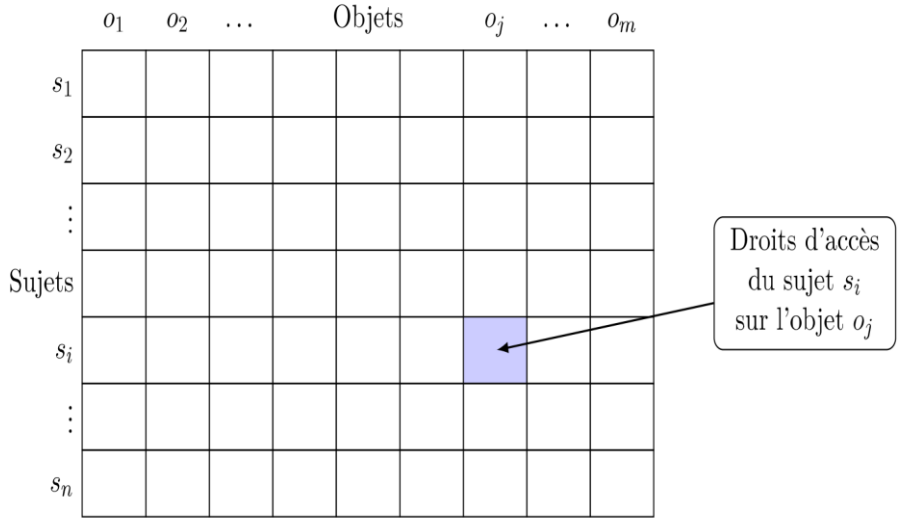

Figure 1 : Matrice de contrôle d'accès

b) Modèle HRU

Le modèle HRU a été introduit par M.A. Harrison, W.L. Ruzzo et J.D. Ullman en 1976. Comme dans le modèle de Lampson, HRU utilise une matrice d'accès classique, la différence réside en ce que HRU précise les commandes qui peuvent lui être appliquées. Les seules opérations possibles sont données dans le tableau 1 :

`Enter a into M(s,o)`	`delete a from M(s,o)`
`Create subject s`	`destroy subject s`
`Create object o`	`destroy object o`

Tableau 1 : Les commandes HRU

où a est un droit.

2.2. Politiques et modèles d'autorisation obligatoires (MAC)

Une politique de sécurité d'autorisation obligatoire impose des règles d'autorisation incontournables qui s'ajoutent aux règles discrétionnaires. Une politique obligatoire suppose que les utilisateurs et les objets aient été étiquetés. Classiquement, les objets se voient attribuer une classification, tandis que les utilisateurs possèdent une habilitation. Les règles qui gèrent les autorisations d'accès sont basées sur une comparaison de l'habilitation de l'utilisateur et de la classification de l'objet.

2.2.1. Quelques modèles associés aux MAC

a) Modèle de Bell-La Padula

Le modèle de Bell-La Padula (BLP) a été développé par David Elliott Bell et Leonard J. La Padula en 1973 pour formaliser la politique de sécurité multi-niveau du Département de la Défense des États-Unis. BLP est un modèle de transition d'états de la politique de sécurité informatique qui décrit des règles de contrôle d'accès qui utilisent des mentions de sécurité sur les objets et les habilitations. Les mentions de sécurité sont relatives aux niveaux de classification des informations.

Pour éviter la divulgation de l'information, deux caractéristiques doivent être maintenues :
No-read-up : Un sujet ne doit pas lire des informations appartenant à un niveau supérieur car il peut connaître des informations qui ne lui sont pas autorisées.

No-write-down : Un sujet ne doit pas écrire dans des informations de niveau inférieur car il peut révéler des secrets.

***Remarque* : La politique de Bell-La Padula vise à assurer la confidentialité.**

Exemple :
Considérons les éléments *S, O, L* tels que :

- *S* = {Bob, Sonia}
- *O* = {fichiers personnels, fichiers du courriel, fichiers du log, fichiers des coordonnées}
- *L* = {Top Secret, Secret, Confidentiel, Non classé}

Les niveaux de sécurité *L* attribués à l'ensemble de sujets *S* et à l'ensemble d'objets O sont :

Niveau de sécurité	Sujet	Objet
Top Secret	Bob	fichiers personnels
Secret		fichiers du courriel
Confidentiel		fichiers du log
Non classé	Sonia	fichiers des coordonnées

L’application du modèle Bell-La Padula donne les règles incontournables suivantes :

- Bob a le droit d’accéder en lecture à tous les fichiers parce qu’il a la classification Top Secret qui est supérieure aux classifications de tous les fichiers.
- Bob a le droit d’accéder en écriture aux fichiers personnels parce que son habilitation Top Secret est égale à la classification des fichiers personnels, mais il n’a pas le droit d’écrire dans les autres fichiers parce que leurs classifications sont inférieures à son habilitation.
- Sonia a le droit d’accéder en écriture à tous les fichiers parce qu’elle a la classification Non classé qui est inférieure aux classifications de tous les fichiers.
- Sonia a le droit d’accéder en lecture aux fichiers des coordonnées parce que son habilitation Non classé est égale à la classification des fichiers des coordonnées, mais elle n’a pas le droit d’accéder en lecture aux autres fichiers parce que leurs classifications sont supérieures à son habilitation.

b) Politique d’intégrité de Biba

Le modèle de Biba ou modèle d'intégrité de Biba, développé par Kenneth J. Biba en 1977 vise à assurer l'intégrité au travers d'une règle simple : « pas d'écriture dans un niveau supérieur, pas de lecture d'un niveau inférieur ». Il s'agit d'une autre approche que le modèle de Bell-La Padula qui se caractérise par « pas d'écriture dans un niveau inférieur, pas de lecture d'un niveau supérieur ».

Exemple :

Considérons les mêmes éléments S, O, L de Bell-La Padula, l’application du modèle Biba donne les règles incontournables suivantes :

- Bob a le droit d’accéder en écriture à tous les fichiers parce qu’il a la classification Top Secret qui est supérieure aux classifications de tous les fichiers.
- Bob a le droit d’accéder en lecture aux fichiers personnels parce que son habilitation Top Secret est égale à la classification des fichiers personnels, mais il n’a pas le droit d’accéder en lecture aux autres fichiers parce que leurs classifications sont inférieures à son habilitation.
- Sonia a le droit d’accéder en lecture à tous les fichiers parce qu’elle a la classification Non classé qui est inférieure aux classifications de tous les fichiers.

- Sonia a le droit d'accéder en écriture aux fichiers des coordonnées parce que son habilitation Non classé est égale à la classification de ces fichiers, mais elle n'a pas le droit d'accéder en écriture aux autres fichiers parce que leurs classifications sont supérieures à son habilitation.

2.3. Politique et modèle de sécurité par rôles (RBAC)

Un rôle représente de façon abstraite une fonction identifiée dans l'organisation (par exemple, chef de service, ingénieur d'études, etc.). À chaque rôle, on associe des permissions (ou privilèges), ensemble de droits correspondant aux tâches qui peuvent être réalisées par chaque rôle. Enfin, et contrairement aux modèles qui ont précédé RBAC (Lampson, par exemple), les permissions ne sont plus associées d'une façon directe aux sujets, mais à travers des rôles (exemple sa fonction dans l'entreprise).

Exemple :

Si le docteur Dupont est à la fois chirurgien et directeur de l'hôpital, en tant que chirurgien, il aura le droit d'accès aux dossiers médicaux, alors qu'en tant que directeur, il pourra accéder aux informations administratives.

3. Exercice

1. Quels sont les inconvénients des politiques discrétionnaires ?
2. Donner un exemple du modèle Biba.
3. Où utilise-t-on les politiques obligatoires ?

4. Corrigé de l'exercice

1. Inconvénients des politiques discrétionnaires

- Elles sont trop laxistes ;
- Il faut constamment redéfinir les règles, chaque fois qu'un nouvel utilisateur ou un nouvel objet est introduit dans le système ;
- Les fuites d'informations (si un utilisateur a le droit de lire une information, il a le droit de la transmettre à n'importe qui.)
- La vulnérabilité aux chevaux de Troie (s'il est possible à un utilisateur d'accéder à certains objets ou d'en modifier les droits d'accès, il est possible qu'un cheval de Troie s'exécutant pour le compte de cet utilisateur (à son insu) en fasse de même).

2. Donner un exemple du modèle Biba

Les intervenants dans le modèle de Biba peuvent uniquement créer/modifier du contenu dans leur propre niveau ou dans un niveau inférieur (par exemple, un cadre peut écrire une liste de directives pour ses employés, mais pas pour son directeur situé à un niveau d'intégrité supérieur). De même, les utilisateurs ne peuvent que voir le contenu qui se trouve à leur niveau d'intégrité ou au-dessus (le cadre peut lire les directives du directeur, mais pas celles en provenance des employés). En effet, si la règle n'était pas respectée, cela signifierait que le directeur pourrait lire une fausse directive émanant d'un employé et qui mettrait en péril l'intégrité de données sensibles (par exemple, "multiplier tous les salaires par deux").

3. Où utilise-t-on les politiques obligatoires ?

Le haut niveau de confidentialité et d'intégrité des politiques MAC a imposé son utilisation dans les secteurs utilisant des données sensibles. Comme l'armée, des autorités gouvernementales, du secteur de la politique, du domaine de la santé, etc.

Conclusion

Après avoir étudié ce chapitre l'étudiant comprend que le contrôle d'accès consiste à vérifier si un sujet possède les droits nécessaires pour accéder à un objet. Il aura aussi des prérequis sur quelques modèles de contrôle d'accès tels que Bell La Padula, Biba, etc.

Chapitre 3 : Sécurité des réseaux

Introduction

Ce chapitre a pour objectifs d'initier les étudiants aux mécanismes de sécurité des réseaux informatiques. Il contient trois cours ; Le premier cours présente un outil de détection, l'IDS (Intrusion Detection Système). Le deuxième cours présente un outil préventif, le firewall (pare-feu), le troisième cours présente un mécanisme restrictif, le VPN (Virtual Private Network).

Cours 1 : Système de détection d'intrusions

1. Définition

Un système de détection d'intrusions (souvent abrégé IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée. Il permet ainsi d'avoir une action de prévention sur les risques d'intrusion.
Il existe deux grandes familles distinctes d'IDS :

- Les N-IDS (Network-based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.
- Les H-IDS (Host-based Intrusion Detection System), ils assurent la sécurité au niveau des hôtes.

2. Méthode de détection

Les techniques de détection d'intrusions se répartissent en deux grandes classes : détection d'anomalies, aussi appelée approche comportementale, et détection d'attaques, dite également approche par scénarios.

a) Approche comportementale

L'approche comportementale (« anomaly detection » en anglais) consiste à comparer les comportements observés à une référence de comportement normal. Toute déviation entre les deux comportements déclenche une alerte.

b) Approche par scénarios

L'approche par scénarios («misuse detection» en anglais) est fondée sur la comparaison du comportement observé avec une référence correspondant à des scénarios d'attaques connus. Le principe consiste à considérer que tout ce qui est décrit dans la base d'attaques est reconnu comme intrusif, le reste est considéré comme normal.

3. Description d'un système de détection d'intrusions

Plusieurs schémas ont été proposés pour décrire les composants d'un système de détection d'intrusions, les plus connus sont : CIDF (the Common Intrusion Detection Framework) de DARPA (Defense Advanced Research Projects Agency) et IDWG (Intrusion Detection Working Group) de l'IETF (l'Internet Engineering Task Force).

Dans ce cours, on se base sur les travaux de l'IDWG, car ils résultent d'un large consensus parmi les intervenants du domaine. L'objectif des travaux du groupe IDWG est la définition d'un standard de communication entre certains composants d'un système de détection d'intrusions. La Figure 1 reproduit ce modèle et permet d'introduire un certain nombre de concepts :

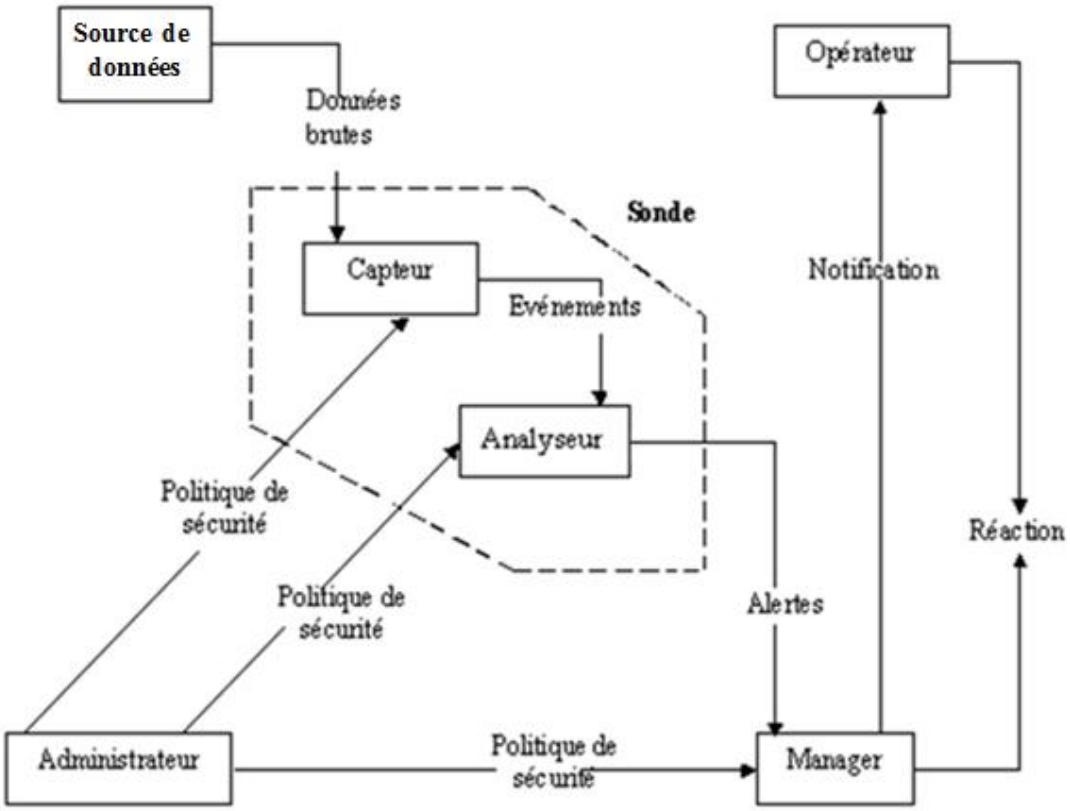

Figure 1 : Modèle générique de la détection d'intrusions proposé par l'IDWG

Les définitions ci-dessous sont largement inspirées de celles proposées par l'IDWG.

Administrateur : personne chargée de mettre en place la politique de sécurité, et par conséquent, de déployer et configurer les IDS.

Politique de sécurité : spécification des règles à respecter afin de garantir la confidentialité, l'intégrité et la disponibilité des ressources sensibles. Elle définit quelles activités sont autorisées et lesquelles sont interdites.

Source de données : dispositif générant de l'information sur les activités des entités du système d'information.

Capteur : logiciel générant des événements en filtrant et formatant les données brutes provenant d'une source de données.

Evénement : message formaté renvoyé par un capteur. C'est l'unité élémentaire utilisée pour représenter une étape d'un scénario d'attaques connu.

Analyseur : c'est un outil logiciel qui met en œuvre l'approche choisie pour la détection (comportementale ou par scénarios), il génère des alertes lorsqu'il détecte une intrusion.

Sonde : un ou des capteurs couplés avec un analyseur.

Alerte : message formaté émis par un analyseur s'il trouve des activités intrusives dans une source de données.

Manager : composant d'un IDS permettant à l'opérateur de configurer les différents éléments d'une sonde et de gérer les alertes reçues et éventuellement la réaction.

Notification : la méthode par laquelle le manager d'IDS met au courant l'opérateur de l'occurrence d'alerte.

Opérateur : personne chargée de l'utilisation du manager associé à l'IDS. Elle propose ou décide de la réaction à apporter en cas d'alerte. C'est, parfois, la même personne que l'administrateur.

Réaction : mesures passives ou actives prises en réponse à la détection d'une attaque, pour la stopper ou pour corriger ses effets.

Dans ce modèle, on peut voir le processus complet de la détection ainsi que le cheminement des données au sein d'un IDS. L'administrateur configure les différents composants (capteur(s), analyseur(s), manager(s)) selon une politique de sécurité bien définie. Les capteurs accèdent aux données brutes, les filtrent et les formatent pour ne renvoyer que les événements intéressants à un analyseur. Les analyseurs utilisent ces événements pour décider de la présence ou non d'une intrusion et envoient dans le cas échéant une alerte au manager, qui notifie l'opérateur humain, une réaction éventuelle peut être menée automatiquement par le manager ou manuellement par l'opérateur.

Cours 2 : Firewall

1. Définition

Un pare-feu (connu sous le nom de firewall), est un système permettant de protéger un ordinateur, ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivantes :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.

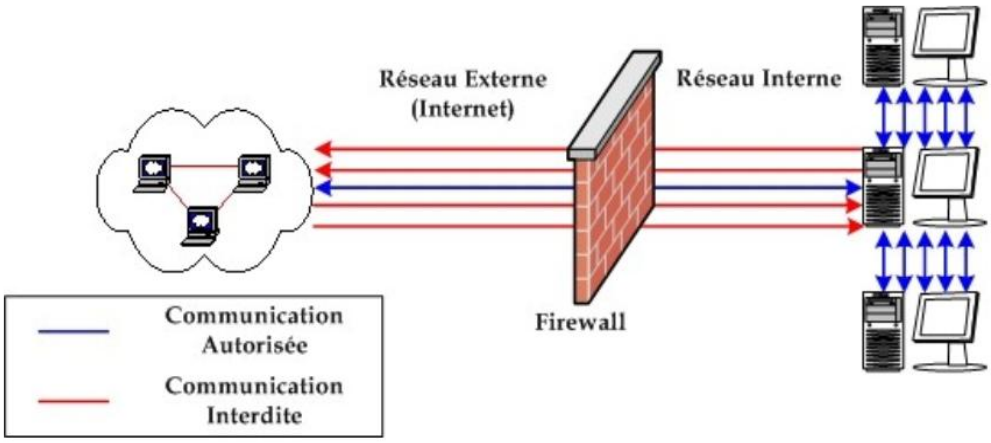

Figure 1 : Pare-feu (Firewall)

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes.

2. Fonctionnement d'un système pare-feu

Le filtrage de paquets peut se faire sur de multiples critères :

- @IP de la machine émettrice ;
- @IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;

- numéro de port ;
- flags et options : SYN, ACK, etc.
- etc.

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow) ;
- De bloquer la connexion (deny) ;
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité :

1) **Politique permissive** : tout permettre, excepté ce qui est explicitement interdit.
2) **Politique stricte** : interdire tout ce qui n'est pas explicitement permis.

Dans le premier cas, une erreur pourrait rendre une attaque possible, tandis que dans le second cas, cette erreur interdirait simplement une utilisation légitime.

3. Filtrage simple de paquets

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « stateless packet filtering »). Il analyse les en-têtes de chaque paquet de données échangé entre une machine du réseau interne et une machine extérieure. Il opère au niveau 3 du modèle OSI (niveau réseau).
Remarque : Ce type de pare-feu ne se rappelle pas des paquets qu'il a déjà vus.

4. Filtrage dynamique

Le terme anglo-saxon est « stateful packet filtering », traduisez « filtrage de paquets avec état ». Ce type de pare-feu opère aux niveaux 3 et 4 du modèle OSI (niveau réseau, niveau transport). IL est capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage.

5. Filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI. Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application. Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou « proxy »).

6. Notion de pare-feu personnel

Un pare-feu personnel est un logiciel, installé sur un ordinateur personnel d'un utilisateur, qui contrôle les communications entrantes et sortantes, autorisant ou refusant celles-ci suivant la politique de sécurité mise en œuvre sur le système.

Cours 3 : VPN

1. Définition

Un réseau privé virtuel (VPN : Virtual Private Network) est constitué de liaisons virtuelles sur Internet entre des sites distants appartenant à une même société ou à un même organisme. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût en chiffrant les données.

2. Fonctionnement d'un VPN

Le principe du VPN est basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel. Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunnelling encapsule les données en rajoutant un entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

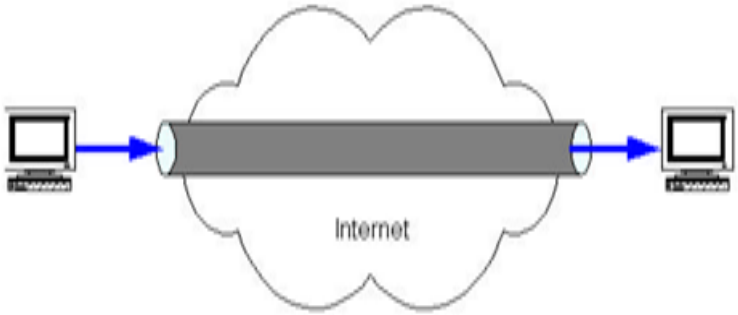

Figure 1 : Le tunnelling

3. Architectures VPN

3.1. VPN d'accès

L'exemple type est une connexion VPN entre un télétravailleur et l'intranet de son entreprise. L'utilisateur doit disposer d'une ligne d'accès à Internet. Sur son ordinateur, il configure une connexion VPN à l'aide d'un « client » fourni par son entreprise.

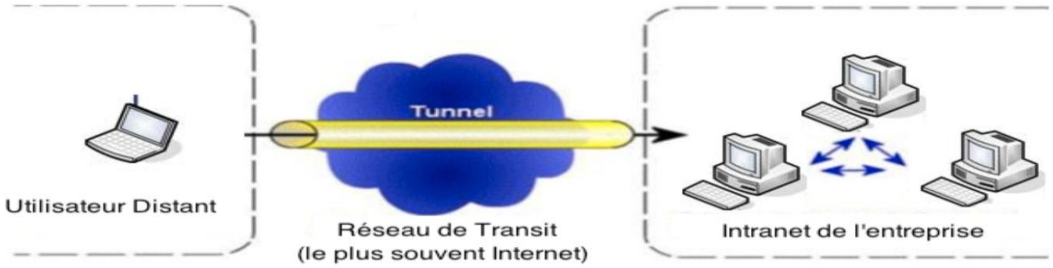

Figure 2 : VPN d'accès

3.2. VPN Intranet

La connexion VPN routeur à routeur reliant deux portions de réseau privé éloignées mais appartenant à la même entreprise.

L'exemple type est une connexion VPN entre le siège d'une société et une de ses agences.

Figure 3 : VPN Intranet

3.3. VPN Extranet

Le VPN Extranet ouvre le réseau local à des partenaires et des clients. Les sites e-commerces et banques s'en servent pour permettre aux utilisateurs d'accéder à leurs comptes.

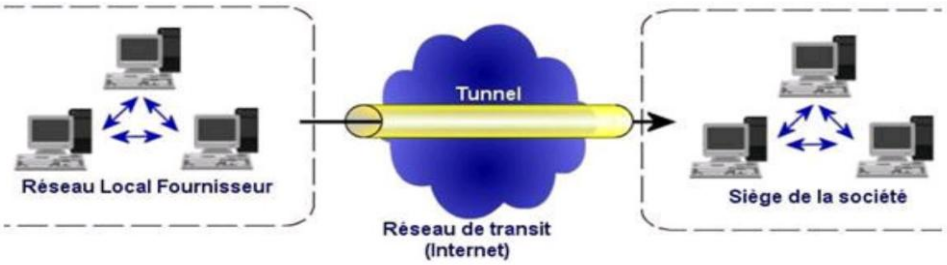

Figure 4 : VPN Extranet

4. Protocoles sécurisés pour VPN

Les principaux protocoles permettant l'établissement d'un VPN :

- le protocole PPTP (Point to Point Tunnelling Protocol) mis au point par la société Microsoft ;
- le protocole L2TP (Layer Two Tunnelling Protocol) proposé par l'IETF;
- le protocole IPSec (Internet Protocol Security) proposé par l'IETF.

4.1. PPTP

La Figure 5 illustre que PPTP encapsule les paquets dans PPP, lui-même encapsulé dans GRE (Generic Routing Encapsulation).

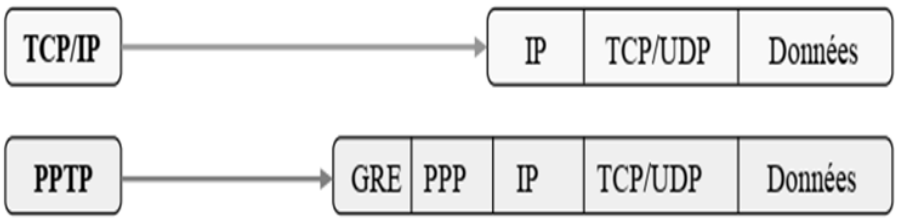

Figure 5 : Encapsultaion PPTP

Remarque : Ce protocole permet à PPP d'être transporté dans un tunnel au travers d'un réseau IP mais n'apporte aucun changement au protocole PPP.

4.2. L2TP

L2TP transporte des trames PPP dans des paquets IP. Il se sert d'une série de messages L2TP pour assurer la maintenance du tunnel et d'UDP pour envoyer les trames PPP dans L2TP.

La mise en place d'un VPN L2TP nécessite deux serveurs d'accès :

Les concentrateurs d'accès L2TP, signifiant L2TP Access Concentrator (LAC). Le rôle du concentrateur d'accès LAC se limite à fournir un support qui sera utilisé par L2TP pour transférer le trafic vers un ou plusieurs serveurs réseau L2TP (LNS signifiant L2tp Network Server).

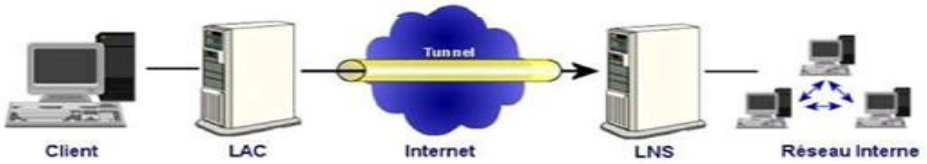

Figure 6 : Serveurs d'accès L2TP

4.3. IPSec

IPSec est compatible avec IPv6 et IPv4. IPSec offre plusieurs services : le chiffrement, le contrôle d'intégrité et l'authentification. IPSec fonctionne selon deux modes différents : mode transport et mode tunnel.

Mode transport

Dans le mode transport, ce sont uniquement les données transférées (la partie payload du paquet IP) qui sont chiffrées et/ou authentifiées. Le reste du paquet IP est inchangé.

Mode tunnel

En mode tunnel, c'est la totalité du paquet IP qui est chiffré et/ou authentifié. Le paquet est ensuite encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP.

IPV4	En-tête IP	En-tête TCP	Données utilisateur	
IPSec en mode transport	En-tête IP	En-tête IPSec	En-tête TCP	Données utilisateur
IPSec en mode tunnel	En-tête IP	En-tête IPSec	En-tête IP	En-tête TCP	Données utilisateur

Figure 7 : IPSec en mode transport et en mode tunnel

IPSec autorise deux formats d'en-tête : AH et ESP.

• **AH (Authentication Header)**

Le protocole AH garantit l'authentification de l'origine des données, le contrôle d'intégrité de l'ensemble du paquet (données + en-têtes IP) et des services anti-rejeu. AH ne garantit pas la confidentialité.

• **ESP (Encapsulating Security Payload)**

Le protocole ESP est un en-tête de protocole inséré dans un datagramme IP pour garantir la confidentialité, l'authentification de l'origine des données, l'anti-rejeu et les services d'intégrité des données.

5. Exercices

Exercice 1 :

1. Comparer les systèmes de détection d'intrusions dont la collecte d'informations est basée sur les machines hôtes et sur le réseau.
2. Quels sont les avantages et les inconvénients d'un système de détection d'intrusions utilisant l'approche par scénarios ?

Exercice 2 :

Les logs d'un serveur web contiennent une série d'entrées du type suivant [adresse source, date, requête, résultat, octets transférés] :

128.178.146.216 - - [24/Sep/2003:16:50:42 +0200] "GET /default.ida?

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a %HTTP/1.0" 404 209

1. De quoi peut-il bien s'agir ?

2. Comment faudrait-il configurer un système de détection d'intrusions pour détecter et réagir à ces attaques ?

Exercice 3 :

1. Qu'est-ce qu'un firewall (pare-feu) ?
2. Quel est l'avantage principal de placer l'IDS entre l'Internet et le pare-feu ? Quels sont les désavantages (nommez-en deux) ?

Exercice 4 :

Permettre aux employés d'une entreprise d'accéder à distance à la messagerie interne peut se faire de plusieurs façons. Donner les avantages et les inconvénients de la solution suivante :

- Utilisation d'un client IPSec pour établir une connexion VPN avec le réseau interne.

6. Corrigé des exercices

Exercice 1 :

1. *Comparer les systèmes de détection d'intrusions dont la collecte d'informations est basée sur les machines hôtes et sur le réseau.*

La collecte d'informations directement sur les machines s'opère via le système d'exploitation, ce qui permet d'observer le comportement et les événements d'un système particulier et peut être efficace même si les données sont chiffrées. Cette solution de collecte d'informations est difficile à déployer surtout pour des grands environnements informatiques. De plus, les performances des machines hôtes sont affectées par ce traitement additionnel. La collecte d'informations au niveau du réseau, consiste à récupérer les données lors de leur transit. Cela permet de détecter certaines attaques impossibles à déceler par la collecte d'information au niveau des machines hôtes (attaques basées sur les paquets malformés et certains dénis de service par exemple). La maintenance d'une telle solution ainsi que le cout de déploiement sont relativement bas comparés à ceux des IDS basés sur la collecte d'informations au niveau des machines hôtes. Néanmoins, cette solution reste inefficace si les données transitant sont chiffrées ou s'il s'agit d'un réseau commuté ou fortement segmenté.

2. *Quels sont les avantages et les inconvénients d'un système de détection d'intrusions utilisant l'approche par scénarios ?*

Les systèmes de détection d'intrusions basée sur la méthode d'analyse par signature (approche par scénarios) permettent d'identifier des attaques et des événements d'une manière rapide voire en temps réel. Cette méthode autorise un nombre de fausses alarmes relativement faible et ce type d'IDS est relativement facile à déployer.

Les inconvénients de cette méthode d'analyse par signature sont identiques à ceux des logiciels antivirus. Comme eux, ils ne détectent que les événements dont la signature est préenregistrée. Les nouveaux scénarios d'attaques, les nouvelles formes d'intrusions, les nouveaux virus ne sont pas repérés. De ce fait, des mises à jour de la base de données de signature doivent être effectuées fréquemment afin d'augmenter le degré d'efficacité des IDS, qui de toute manière seront impuissants pour détecter une attaque de signature inconnue.

Exercice 2 :

1. Le fait qu'il y ait une longue suite de lettres sans signification, suivie de caractères en Unicode, laisse fortement présager qu'il s'agisse d'une tentative d'attaque par débordement de tampon.
2. Le principal moyen permettant de détecter ces attaques est de déceler la signature d'une attaque connue ; un moyen heuristique consisterait à contrôler la longueur de la requête : si celle-ci est anormalement longue, alors on peut considérer que l'on doit faire face à une attaque de type débordement de tampon. L'IDS peut alors prévenir le pare-feu afin que celui-ci bloque l'adresse IP de l'attaquant.

Exercice 3 :

1. Qu'est-ce qu'un pare-feu ?

   Entité matérielle ou logicielle qui permet de filtrer les entrées indésirables et de protéger les environnements informatiques en les masquant, séparant, créant un périmètre de sécurité.

2. Quel est l'avantage principal de placer l'IDS entre l'Internet et le pare-feu ? Quels sont les désavantages (nommez-en deux) ?

   Avantages :

Permet de voir toutes les attaques, incluant celles visant le pare-feu lui-même, et donc on obtient plus d'informations sur la menace.

Désavantages:

- Si l'IDS n'est pas bien protégé il peut être attaqué,
- La grosseur des logs peut être énorme, étant donné qu'il n'y a aucun filtrage.

Exercice 4

Avantage :

- Le serveur de messagerie n'est accessible qu'après une authentification réussie au niveau IPSec. Ceci protège le serveur contre des attaques par des utilisateurs externes à l'entreprise.

Inconvénients :

- IPSec permet un accès complet au réseau interne, ce qui est bien plus que ce qui était recherché ; des moyens additionnels sont nécessaires pour n'autoriser l'accès qu'au service de courrier électronique.
- C'est une solution lourde à mettre en œuvre pour n'utiliser que la messagerie.

Conclusion

À l'issue de ce chapitre, l'étudiant apprend qu'il existe plusieurs mécanismes de sécurité permettant d'appliquer une politique de sécurité, à savoir : les IDSs qui permettent la détection des intrusions en temps réel, les firewalls qui assurent le filtrage des paquets selon les règles de la politique de sécurité et les VPNs qui offre la possibilité d'avoir des réseaux privés virtuels.

Chapitre 4 : Les applications sécurisées

Introduction

Ce chapitre présente brièvement les applications PGP, S/MIME, SSH, SSL et SET. Le but de ce chapitre est d'inculquer à l'étudiant d'autres solutions de sécurité.

1. PGP (Pretty Good Privacy)

PGP est la solution la plus connue des usagers pour rendre confidentielle la transmission de messages et authentifier l'émetteur. Elle fut développée et mise à disposition sur Internet dés 1991 par son auteur Philip Zimmermann.

1.1. Principe de PGP

PGP est un système de cryptographie *hybride*, utilisant une combinaison des fonctionnalités de la cryptographie à clé publique et de la cryptographie symétrique. PGP se base sur l'algorithme IDEA pour le chiffrement de messages, sur MD5 pour le hash du résumé, sur RSA pour le chiffrement du résumé et pour l'échange de la clé privée nécessaire à IDEA. Cette dernière est générée de façon aléatoire au moment du chiffrement et utilisée une seul fois. PGP utilise optionnellement la compression d'un message avant son chiffrement.

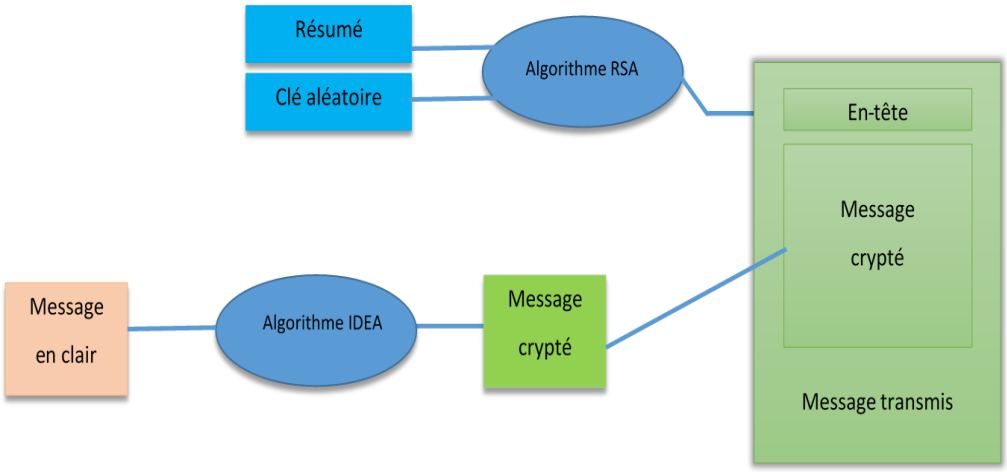

Figure 1 : Les étapes de chiffrement générées par PGP

2. S/MIME (Secure / Multipurpose Internet Mail Extensions)

S/MIME (pour *Secure MIME*, que l'on pourrait traduire par *extensions du courrier électronique à but multiples et sécurisées*). S/MIME est une extension sécurisée qui propose, comme PGP des services d'authentification et de confidentialité. Ainsi, S/MIME permet de chiffrer tout type de contenu ainsi que les clés de chiffrement à destination de un ou de divers destinataires.

La signature du message est réalisé par chiffrement via la clé privée de l'émetteur (RSA, par exemple), d'un résumé du message (*message digest*) crée par SHA-1 ou MD5. Les clés de session sont générées via l'algorithme Diffie-Hellman. Les algorithmes de chiffrement RSA, DES sont supportés par S/MIME.

3. SSH (Secure Shell)

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité. Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

Pour toutes ces raisons, le protocole **SSH** permet de remplacer efficacement le protocole telnet ainsi que d'autres protocoles vulnérable, tels que rsh et rlogin.

4. SSL (Secure Socket Layer)

SSL est un protocole de sécurisation mis en œuvre initialement par la société Netscape Communications mais qui a depuis été repris par l'IETF sous le nom TLS (Transport Layer Security)

Le protocole SSL a été conçu pour assurer une communication confidentielle et fiable entre deux applications (un client et un serveur), pour identifier le serveur et parfois le client. SSL nécessite un protocole de transport sûr pour la transmission et la réception de données.

Le protocole est composé de deux couches. Au niveau le plus bas, juste au-dessus d'un protocole de transport sûr, se trouve le SSL Record Protocol. Celui-ci est utilisé pour encapsuler d'autres protocoles de plus haut niveau tel le SSL Handshake Protocol qui permet au serveur et au client de s'authentifier et de négocier un algorithme de chiffrement et des clés cryptographiques avant que le protocole d'application ne reçoive son premier octet d'information.

Un serveur sécurisé par SSL possède une URL commençant par https : //, où le "s" signifie sécurisé.

Bien que SSL soit largement utilisé dans l'environnement web, SSL peut être invoqué indépendamment de celui-ci. SSL peut sécuriser la transmission du numéro de carte de crédit entre client et vendeur. L'authentification du numéro de la carte de crédit reste à faire hors Internet.

5. SET (Secure Electronic Transaction)

SET est basé sur l'utilisation d'une signature électronique au niveau de l'acheteur et une transaction mettant en jeu non seulement l'acheteur et le vendeur, mais aussi leurs banques respectives.

Lors d'une transaction sécurisée avec SET, les données sont envoyées par le client au serveur du vendeur, mais ce dernier ne récupère que la commande. En effet, le numéro de carte de crédit est envoyé directement à la banque du commerçant, qui va être en mesure de lire les coordonnées bancaires de l'acheteur, et donc de les vérifier en temps réel.

6. Exercice

1. IPSec et PGP sont des moyens de sécuriser des échanges de données. Pour chacune de ces techniques, indiquer comment elle se positionne par rapport au modèle en couches TCP/IP.
2. Comment sécuriser une transaction de commerce électronique ?

7. Corrigé de l'exercice

1. *IPSec et PGP sont des moyens de sécuriser des échanges de données. Pour chacune de ces techniques, indiquer comment elle se positionne par rapport au modèle en couches TCP/IP.*
   - Couche Réseau : IPSEC
   - Couche Application : PGP

2. *Comment sécuriser une transaction de commerce électronique ?*

La sécurité du commerce électronique passe par deux étapes primordiales :
-la sécurisation de la connexion entre l'acheteur et le vendeur en ligne ;
-la sécurisation du (des) serveur(s) du vendeur.
La connexion Internet entre le client et le vendeur doit être établie d'une manière sécurisée. Cette sécurité est réalisée par la mise en œuvre d'une connexion logique SSL via des mécanismes de chiffrement SSL. C'est la solution la plus largement adoptée par les acteurs du e-commerce. Le navigateur communique avec le serveur distant en utilisant SSL afin de

garantir la confidentialité et l'intégrité des données sensibles (information privées, numéro de carte de crédit, numéro du compte bancaire, etc.).
Le stockage temporaire et le traitement des informations client fait par le serveur distant font partie de la transaction et donc doivent être sécurisés et l'accès à ses ressources doit être restreint au minimum de personne ou point intermédiaires.
D'autres méthodes visant la sécurité des transactions commerciales en ligne existent. Le protocole SET élaboré par les principaux opérateurs de cartes de crédit est le concurrent de SSL. Il se base sur les certificats numériques et donc trouve les mêmes obstacles et limites des solutions de sécurité basées sur l'usage de certificats numériques.

Conclusion

À la fin de ce chapitre, l'étudiant applique ses prérequis de cryptographie sur quelques solutions de sécurité comme PGP. Il découvre aussi d'autres applications de sécurité telles que : SSL, SET, etc.

Chapitre 5 : Sécurité des bases de données

Introduction

Sécuriser une base de données consiste à mettre en œuvre une politique de sécurité dans un Système de Gestion de Base de Données (SGBD) conformément à un modèle de sécurité (les modèles présentés dans ce cours sont discrétionnaire et obligatoire).

1. Sécurité discrétionnaire

La norme SQL gère les contrôles d'accès discrétionnaires. Deux éléments de SQL plus ou moins indépendants interviennent : le mécanisme de vues qui est utilisé pour cacher des données sensibles à des utilisateurs non autorisés et le sous-système d'autorisation qui permet aux utilisateurs ayant des privilèges particuliers d'attribuer sélectivement et dynamiquement ces privilèges à d'autres utilisateurs, et de révoquer ensuite ces privilèges, s'ils le souhaitent.

Pour illustrer l'utilisation des vues pour des besoins de sécurité, considérons une relation Employe qui indique, pour un individu donné, s'il s'agit d'un homme ou d'une femme et quel est son âge, son salaire et sa profession. Nous définissons la vue suivante sur la relation Employe :

```
CREATE VIEW Emp_Programmeur AS
SELECT Nom, H/F, Profession
FROM Employe
WHERE Employe.Profession = "Programmeur" ;
```

Cette vue ne contient que les employés dont la profession est programmeur et pour ces employés, on donne uniquement le nom, la profession et s'il s'agit d'un homme ou d'une femme.

Le mécanisme de vues permet donc de diviser conceptuellement la base de données en plusieurs parties de sorte que des informations sensibles peuvent être cachées aux utilisateurs non autorisés. Cependant, il ne permet pas de spécifier les opérations que certains utilisateurs sont autorisés à exécuter sur ces parties de la base. Cette fonction est réalisée par l'instruction

GRANT. Par exemple, l'instruction suivante définit des autorisations sur la vue Emp_Programmeur :

GRANT SELECT, DELETE

ON Emp_Programmeur

TO Jean, Paul, Marie;

Cette instruction donne l'autorisation aux utilisateurs Jean, Paul et Marie de sélectionner et de supprimer n'importe quel n-uplet de la vue Emp_Programmeur.

Voici la syntaxe complète de l'instruction GRANT :

GRANT <liste privileges>

ON <objet>

TO <liste ID utilisateur>

[WITH GRANT OPTION];

2. Sécurité obligatoire

Dans cette section, nous nous intéressons plus particulièrement à la politique de sécurité multi-niveaux. Dans une politique de sécurité multi-niveaux, les utilisateurs reçoivent un niveau d'habilitation et les informations un niveau de classification. Les niveaux d'habilitation et de classification sont en général pris dans un ensemble partiellement ordonné de niveaux, par exemple Très Secret > Secret > Confidentiel > Public. Nous allons examiner quelques problèmes que pose la mise en œuvre d'une politique de sécurité multi-niveaux dans un SGBD : choix et interprétation d'une granularité de classification et gestion des leurres par exemple.

2.1. Granularité de la classification

Un premier problème à considérer lorsque l'on développe une application multi-niveaux est celui de la granularité de la classification, c'est-à-dire le grain d'information qui recevra une classification. Dans le cas des bases de données relationnelles, plusieurs granularités ont été proposées dans la littérature, les granularités les plus courantes étant le n-uplet et l'attribut de n-uplet. L'interprétation de la granularité « n-uplet » est simple. Si l'on attribue un niveau de classification n à un n-uplet, cela signifie que l'information représentée par le n-uplet est

elle-même classée au niveau n. Par exemple, considérons la relation Employe introduite dans la section précédente.

Alors, si l'on attribue le niveau de classification Secret au n-uplet

Employe(Dupont,H,30,200E,Programmeur), cela signifie que l'information

«Dupont est un employé masculin ayant 30 ans, gagnant 200E et travaillant comme programmeur » est classée au niveau Secret.

2.2. Gestion des leurres

Intuitivement, un leurre est une information fausse introduite dans une base de données multiniveaux, en général, pour protéger l'existence d'une information sensible. Par exemple, supposons que la base de données contienne l'information Salaire(Dupont,200E), c'est-à-dire « le salaire de Dupont est 200E ». Supposons que cette information soit classée au niveau Secret :

- [Secret]Salaire(Dupont,200E) où [Secret]p signifie que l'information représentée par la formule p a été classée au niveau Secret.

Supposons également que le salaire de Dupont soit unique et que la base de données contienne l'information Salaire(Dupont,150E) et que cette information soit classée au niveau Public :

- [Public]Salaire(Dupont,150E)

Comme Dupont ne peut pas avoir deux salaires dans la réalité, cette dernière information est en général interprétée comme un leurre. Les leurres sont nécessaires dans une base de données multi-niveaux dans des situations bien particulières. Ainsi, dans notre exemple, supposons qu'un utilisateur u de niveau Public pose la requête : quel est le salaire de Dupont ? La base de données ne peut naturellement pas répondre « le salaire de Dupont est 200E » puisque cette information est secrète. Supposons que la base de données réponde « vous n'avez pas le droit de connaître cette information ». L'utilisateur u peut alors déduire de cette réponse que le salaire de Dupont est classé secret ce qui est représenté par l'expression suivante :

- $\exists x$, [Secret]Salaire(Dupont,x)

On peut, dans certains cas, considérer que cette dernière information est elle-même secrète, ce qui est représenté par l'expression suivante :

- [Secret](∃x, [Secret]Salaire(Dupont,x))

Dans ce cas, la base de données ne peut plus répondre à u « vous n'avez pas le droit de connaître cette information ». L'utilisation d'un leurre est alors nécessaire et la base de données multi-niveaux va alors répondre, par exemple, que le salaire de Dupont est 150E.

Conclusion

À travers ce chapitre l'étudiant découvre le lien entre les modèles de politique de sécurité, vu dans le chapitre 2, et les bases de données étudiées en Licence et Master 1.

Sujet d'examen en ligne (2020/2021)

Corrigé type de l'examen Sécurité des réseaux

Le barème est: 1 point pour une réponse 100% correcte, 0,25 ou 0,5 point pont une réponse incomplète (selon la question) et 0 point lorsque des réponses fausses a été choisie.

Question 1

Correct

Note de 1,00 sur 1,00

Comment savoir si on se trouve sur une page Web sécurisée ?

Veuillez choisir au moins une réponse :

- [ ] On ne peut pas le savoir
- [ ] On a dû obligatoirement entrer un mot de passe pour y accéder
- [ ] La couleur de fond de la page est modifiée
- [x] L'URL commence par https://
- [x] Le navigateur affiche une icône de cadenas près de la barre d'adresse

Votre réponse est correcte.

Les réponses correctes sont : Le navigateur affiche une icône de cadenas près de la barre d'adresse, L'URL commence par https://

Question 2

Correct

Note de 1,00 sur 1,00

RBAC fournit un bon compromis entre DAC et MAC.

Sélectionnez une réponse :

- (•) Vrai
- ( ) Faux

La réponse correcte est « Vrai ».

Question 3

Correct

Note de 1,00 sur 1,00

Les éléments à entreprendre pour bien gérer la sécurité incluent :

(1) Quels sont les risques ?

(2) Comment protéger l'entreprise ?

(3) Que protéger et pourquoi ?

(4) De quoi protéger les biens ?

Dans quel ordre doit-on traiter ces questions ?

Veuillez choisir une réponse :

- ( ) 2, 3, 4, 1
- ( ) 4, 2, 3, 1
- ( ) 1, 2, 3, 4
- (•) 3, 4, 1, 2

Votre réponse est correcte.

La réponse correcte est : 3, 4, 1, 2

Question 4

Correct

Note de 1,00 sur 1,00

Peut-on avoir confiance en un système de détection d'intrusions ?

Veuillez choisir une réponse :

- Non
- Oui

Votre réponse est correcte.

La réponse correcte est : Non

Question 5

Correct

Note de 1,00 sur 1,00

Quels sont les algorithmes cryptographiques utilisables par PGP ?

Veuillez choisir une réponse :

- RSA et DES
- DES et Diffie-Hellman
- RSA et IDEA

Votre réponse est correcte.

La réponse correcte est : RSA et IDEA

Question 6

Correct

Note de 1,00 sur 1,00

IPSec est un protocole qui :

Veuillez choisir une réponse :

- chiffre et authentifie les paquets
- chiffre et authentifie les trames
- chiffre les trames
- chiffre les paquets
- sécurise un terminal

Votre réponse est correcte.

La réponse correcte est : chiffre et authentifie les paquets

Question 7

Correct

Note de 1,00 sur 1,00

Le domaine de la sécurité informatique comprend la protection contre les catastrophes naturelles de force majeure.

Sélectionnez une réponse :

- Vrai
- Faux

La réponse correcte est « Vrai ».

Question 8

Correct

Note de 1,00 sur 1,00

L'IDS basé signature :

Veuillez choisir au moins une réponse :

- [x] identifie les attaques plus rapidement
- [ ] détecte les attaques zero-day
- [x] ne détecte que les attaques dont la signature est préenregistrée

Votre réponse est correcte.

Les réponses correctes sont : identifie les attaques plus rapidement, ne détecte que les attaques dont la signature est préenregistrée

Question 9

Correct

Note de 1,00 sur 1,00

Parmi les termes suivants, lesquels désignent des logiciels malveillants ?

Veuillez choisir au moins une réponse :

- [ ] Un bug
- [x] Un cheval de Troie
- [x] Un ver
- [x] Un virus
- [x] Un logiciel espion

Votre réponse est correcte.

Les réponses correctes sont : Un cheval de Troie, Un ver, Un virus, Un logiciel espion

Question 10

Correct

Note de 1,00 sur 1,00

L'ingénierie sociale est

Veuillez choisir une réponse :

- ( ) un logiciel malveillant qui se propage par l'intermédiaire des réseaux sociaux
- (•) l'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité
- ( ) un logiciel malveillant nommé d'après ses inventeurs qui sont d'anciens ingénieurs

Votre réponse est correcte.

La réponse correcte est : l'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité

Question 11

Correct

Note de 1,00 sur 1,00

Concernant un VPN, quelles affirmations sont exactes ?

Veuillez choisir au moins une réponse :

- [x] Un tunnel sécurisé est créé entre deux sites distants
- [x] Les paquets qui circulent sur Internet sont chiffrés
- [x] Tout se passe comme si la connexion se faisait en dehors d'infrastructure d'accès partagé comme Internet.
- [ ] Les utilisateurs doivent chiffrer les messages qu'ils envoient
- [x] Seuls les utilisateurs ou les groupes qui sont enregistrés dans le VPN peuvent y accéder.

Votre réponse est correcte.

Les réponses correctes sont : Seuls les utilisateurs ou les groupes qui sont enregistrés dans le VPN peuvent y accéder., Les paquets qui circulent sur Internet sont chiffrés, Tout se passe comme si la connexion se faisait en dehors d'infrastructure d'accès partagé comme Internet., Un tunnel sécurisé est créé entre deux sites distants

Question 12

Correct

Note de 1,00 sur 1,00

Concernant les pare-feux, quelles affirmations sont fausses ?

Veuillez choisir au moins une réponse :

- [x] Les pare-feux apportent sécurité et confidentialité des transmissions
- [x] Les pare-feux assurent la sécurité des connexions entrantes par authentification forte des utilisateurs
- [x] Les pare-feux peuvent réaliser l'ensemble des fonctions de sécurité identifiées dans une politique de sécurité
- [ ] Les pare-feux servent à filtrer les connexions selon des règles établies par l'administrateur
- [x] Les pare-feux assurent la cryptographie et la vérification d'intégrité

Votre réponse est correcte.

Les réponses correctes sont : Les pare-feux apportent sécurité et confidentialité des transmissions, Les pare-feux assurent la sécurité des connexions entrantes par authentification forte des utilisateurs, Les pare-feux peuvent réaliser l'ensemble des fonctions de sécurité identifiées dans une politique de sécurité, Les pare-feux assurent la cryptographie et la vérification d'intégrité

Question 13

Correct

Note de 1,00 sur 1,00

Les tickets d'accès KERBEROS

Veuillez choisir une réponse :

- ( ) n'inclut pas de notion de durée de vie
- (•) ont une durée de vie limitée
- ( ) ont une durée de vie illimitée

Votre réponse est correcte.

La réponse correcte est : ont une durée de vie limitée

Question 14
Correct
Note de 1,00 sur 1,00

Un employé qui n'a pas obéi à la politique de sécurité d'une entreprise, dont il a reçu une copie lors de son engagement, pourrait être renvoyé s'il a enfreint une des règles de cette politique.

Sélectionnez une réponse :

- (●) Vrai
- ( ) Faux

La réponse correcte est « Vrai ».

Question 15
Correct
Note de 1,00 sur 1,00

Concernant un virus, quelles affirmations sont vraies ?

Veuillez choisir au moins une réponse :

- [ ] Il ne s'attrape que par la messagerie électronique
- [x] Il peut prendre le contrôle de l'ordinateur
- [ ] Il ne pourra jamais s'installer si l'ordinateur possède un anti-virus
- [ ] Il détruit systématiquement tous les fichiers du disque dur
- [x] Il peut utiliser le réseau pour se propager

Votre réponse est correcte.
Les réponses correctes sont : Il peut utiliser le réseau pour se propager, Il peut prendre le contrôle de l'ordinateur

Question 16
Correct
Note de 1,00 sur 1,00

L'authentification d'un utilisateur consiste à :

Veuillez choisir une réponse :

- ( ) demander d'entrer une deuxième fois son mot de passe à l'utilisateur qui souhaite en changer
- ( ) demander à l'utilisateur d'entrer son mot de passe à intervalles périodiques au cours de sa session.
- ( ) établir une correspondance entre le pseudonyme entré par l'utilisateur et son vrai nom
- ( ) garder l'historique de la visite de l'utilisateur sur le système (identifiant, dates et heures de connexion et de déconnexion, etc.)
- (●) Aucune réponse juste

Votre réponse est correcte.
La réponse correcte est : Aucune réponse juste

Question 17
Correct
Note de 1,00 sur 1,00

On peut saturer, par des requêtes, un serveur même s'il est protégé par un pare-feu.

Sélectionnez une réponse :

- (●) Vrai
- ( ) Faux

La réponse correcte est « Vrai ».

Question 18

Correct

Note de 1,00 sur 1,00

Dans quel ordre doit-on mettre en œuvre les principaux objectifs de sécurité ?

Veuillez choisir une réponse :

- confidentialité, disponibilité, intégrité
- confidentialité, intégrité, disponibilité
- intégrité, confidentialité, disponibilité
- intégrité, disponibilité, confidentialité
- disponibilité, intégrité, confidentialité
- disponibilité, confidentialité, intégrité

Votre réponse est correcte.

La réponse correcte est : confidentialité, intégrité, disponibilité

Question 19

Correct

Note de 1,00 sur 1,00

La confidentialité des données assure :

Veuillez choisir au moins une réponse :

- [x] qu'aucune copie illicite des données ne puisse être faite
- [ ] que les données ne puissent pas être modifiées suite à une intrusion
- [ ] que les données ne contiennent aucune information incorrecte
- [x] que les données ne puissent être consultées que par ceux qui sont éligibles à le faire

Votre réponse est correcte.

Les réponses correctes sont : que les données ne puissent être consultées que par ceux qui sont éligibles à le faire, qu'aucune copie illicite des données ne puisse être faite

Question 20

Correct

Note de 1,00 sur 1,00

Le Smurf est une attaque :

Veuillez choisir une réponse :

- indirecte par réponse
- directe
- indirecte par rebond

Votre réponse est correcte.

La réponse correcte est : indirecte par réponse

Conclusion générale

À travers ce support de cours, on a présenté l'ensemble de connaissances de base qu'un étudiant informaticien doit connaitre sur le domaine de la sécurité des réseaux informatiques, à savoir, l'analyse des risques, les attaques, les protocoles d'authentification (PAP, CHAP, RADUIS, Kerbers) et modèles de gestion des autorisations (DAC, MAC, etc.). Pour sécuriser un réseau l'étudiant apprend que les techniques et outils disponibles aujourd'hui pour faire appliquer une politique de sécurité peuvent être classés en trois catégories : les outils de prévention (exemple : les pare-feu, les mécanismes de contrôle d'accès, les mécanismes d'authentification, etc.), les outils de détection (exemple : les IDSs) et les outils restrictifs (exemple : les VPN). Le premier but des outils de prévention est la mise en œuvre d'une politique de sécurité, les outils de détection quant à eux sont destinés à signaler les cas de violation de celle-ci. Les outils restrictifs assurent la prévention et la détection mais sur des zones bien déterminées. Ce support permet également à l'étudiant d'exercer ses prérequis de cryptographie sur quelques solutions de sécurité comme PGP et de découvrir le lien entre les modèles de politique de sécurité et les bases de données.

Bibliographie :

[1] Jean-François Pillou, Jean-Philippe Bay, *Tout sur la sécurité informatique* – 3ème édition, Dunod, 2013.

[2] Solange Ghernaouti-Hélie, *Sécurité informatique et réseaux (Cours avec plus de 100 exercices corrigés)*, 3ème édition, Dunod, 2011.

[3] Gildas Avoine, Pascal Junod, Philippe Oechslin, *Sécurité informatique (exercices corrigés)*, Edition Vuibert, 2006.

[4] Jean-Marie Flaus, *Cybersécurité des systèmes industriels*, Editions ISTE, 2019.

[5] Franck Huet, Christian Verhille , *GNU-Linux Fedora : sécurité du système, sécurité des données, pare-feu, chiffrement, authentification...*, Edition ENI, 2007.

[6] Laurent Bloch, Christophe Wolfhugel, Nat Makarévitch, Christian Queinnec, Hervé Schauer, *Sécurité informatique: Principes et méthode à l'usage des DSI, RSSI et administrateurs*, Eyrolles, 2011

[7] Lamia HAMZA, *Génération automatique de scénario d'attaques pour les systèmes de détection d'intrusions*, mémoire Magistère, Université de Bejaia, 2005.

[8] Sofiene Boulares, *Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès*, Maitrise en informatique, Université du Québec en Outaouais, Canada, 2010.

[9] Anas Abou El Kalam.. *Modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales* (Doctoral dissertation, Institut National Polytechnique de Toulouse-INPT). 2003.

[10] Cuppens, F. *Modélisation formelle de la sécurité des systèmes d'informations.* Habilitation à Diriger les Recherches, Université Paul Sabatier. 2000.

[11] https://www.bestcours.com/documents/0241-formation-securite-informatique.pdf