Université de khenchela
Département MI

Sécurité informatique

Dr. Hichem Rahab

L3 ISIL

2021 - 2022

Chapitre 1: Introduction à la sécurité informatique

Overview

Introduction (1)

- La sécurité informatique constitue l'ensemble de moyennes mises en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. L'objectif de la sécurité informatique est d'assurer que les ressources matérielles et/ou logicielles d'un parc informatique sont uniquement utilisées dans le cadre prévu et par des personnes autorisées.

Introduction (2)

- La sécurité d'un système est modélisée par une chaine où on mesure la sécurité de cette chaine entière à la sécurité de son maillon le plus faible. Ainsi, si tout un système est sécurisé techniquement mais que le facteur humain, souvent mis en cause, est défaillant, c'est toute la sécurité du système qui est remise en cause.

Figure: Chaine de sécurité

Le risque en informatique

Le risque en sécurité informatique est souvent donné par la formule suivante :

$$Risque = \frac{Menace \times Vulnerabilie}{Contremesures}$$

- **Risque:** C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
- **Vulnérabilité :** C'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille ou brèche, elle représente le niveau d'exposition face à la menace dans un contexte particulier.
- **Menace :** c'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.
- **Contre-mesure :** c'est l'ensemble de moyens mises en place pour faire face aux risques dans une organisation.

Conséquences de la formule:

- Plus on augmente les contre-mesures; plus on réduise les risques possibles.
- Le plus sont les vulnérabilités et les menaces contre le système ; le plus le risque est important.

Objectifs de la sécurité

Il convient d'identifier les exigences fondamentales en sécurité informatique, qui caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques au regard de la sécurité :

1. L'authentification
2. Le contrôle d'accès
3. La confidentialité
4. L'intégrité
5. La disponibilité
6. La non-répudiation

1. L'authentification

- L'authentification permet de limiter l'accès aux personnes autorisées.
- Elle exige d'assurer de l'identité des utilisateurs avant l'échange de données.
- Le service d'authentification est chargé d'assurer qu'une communication est authentique.
- Dans le cas d'un seul message, tel qu'un signal d'avertissement ou d'alarme, la fonction du service d'authentification est d'assurer au destinataire que le message provient de la source qu'il prétend être.

Figure: Authentification

1. L'authentification (2)

- Dans le cas d'une interaction continue, comme la connexion d'un terminal à un hôte, deux aspects sont impliqués:
  1. Tout d'abord, au moment de l'initiation de la connexion, le service garantit que les deux entités sont authentiques, c'est-à-dire que chacune est l'entité qu'elle prétend être.
  2. Deuxièmement, le service doit s'assurer que la connexion n'est pas entravée de telle sorte qu'un tiers peut se faire passer comme l'une des deux parties légitimes aux fins d'une transmission ou d'une réception non autorisée.

Figure: Authentification

2. Le contrôle d'accès

- Le contrôle d'accès constitue une précaution prise contre l'utilisation non autorisée d'une ressource;
- cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.
- Dans le contexte de la sécurité du réseau, le contrôle d'accès permet de limiter et de contrôler l'accès aux systèmes et aux applications via les liaisons de communication.
- Pour ce faire, chaque entité qui tente d'accéder doit d'abord être identifiée ou authentifiée, de sorte que les droits d'accès peuvent être adaptés à l'individu.

3. La confidentialité

- Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.
- Seules les personnes habilitées doivent avoir accès aux données.
- Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- La confidentialité doit assurée que l'information est inintelligible à d'autres personnes que les seuls acteurs de la transaction.

3. La confidentialité (2)

- La confidentialité est également un principe éthique associé à plusieurs professions, notamment dans les domaines de la médecine, du droit, de la vente, de l'informatique, de la religion, du journalisme, etc.
- En éthique et en droit, certains types de communication entre une personne et un de ces professionnels sont dites " privilégiées ", et ne peuvent être discutées avec, ou divulguées à des tierces parties.
- Dans certaines juridictions où la loi assure une telle confidentialité, des sanctions sont habituellement prévues dans les cas d'infraction.

4. L'intégrité

- Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.
- Il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication.
- L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- Un service d'intégrité axé sur la connexion, qui traite d'un flux de messages, assure que les messages sont reçus comme envoyés, sans: duplication, insertion, modification, réorganisation ou répétition.

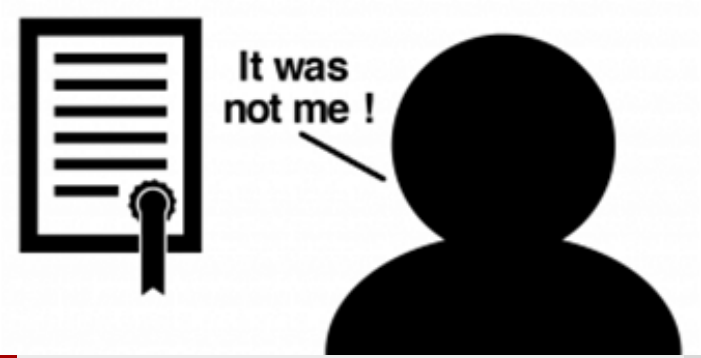
5. La disponibilité

- C'est la propriété d'être accessible et utilisable sur demande par une entité autorisée.
- Il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment.
- La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.
- Ce service répond aux problèmes de sécurité soulevés par les attaques de déni de service.

$$Disponibilite = \frac{duree\_durantlaquellecetequipementestoperationnel}{Dureedurantlaquelleilauraitduetreoperationnel}$$

6. La non-répudiation

- Une transaction ne peut être niée par aucun des correspondants.
- La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues.
- La non répudiation empêche l'émetteur ou le récepteur de refuser un message transmis.
- Ainsi, lorsqu'un message est envoyé, le destinataire peut prouver que l'expéditeur présumé a en effet envoyé le message.
- De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le récepteur a effectivement reçu le message.
- Cela se fait par le biais de certificats numériques grâce à une clé privée.



Les attaques informatiques

- Une attaque en informatique est une tentative d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé à l'information.
- Le gouvernement des États-Unis, selon l'instruction CNSS n°4009 du 26 avril 2010 par le Comité des systèmes de sécurité nationale des États-Unis d'Amérique définit une attaque comme suit : " Toute activité malveillante qui tente de collecter, perturber, nier, dégrader ou détruire les ressources du système d'information ou l'information elle-même. ".

Classification des attaques

Une attaque peut être classée par son comportement ou par la position de l'attaquant. Une attaque peut être active ou passive.

- Une **"attaque active"** tente de modifier les ressources du système ou d'affecter leur fonctionnement.
- Une **"attaque passive"** tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système. (P. Ex., Écoutes téléphoniques).

Une attaque peut être perpétrée de l'intérieur ou de l'extérieur de l'organisation:

- Une **"attaque interne"** est une attaque initiée par une entité dans le périmètre de sécurité, c'est-à-dire une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui ont accordé l'autorisation.
- Une **"attaque externe"** est initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système.

Ingénierie sociale

- Généralement l'utilisateur constitue le maillon le plus faible dans toute politique de sécurité.
- 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 :
  1. Se faire passer pour quelqu'un que l'on n'est pas (en général un administrateur réseau) ;
  2. Demander des informations personnelles (nom de connexion, mot de passe, données confidentielles, etc.) en intervenant un quelconque prétexte (problème dans le réseau, modification de celui-ci, etc.) ;

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

Cheval de Troie

- Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance).
- Les chevaux de Troie lisent les mots de passe, enregistrent les frappes ou ouvrent la voie à d'autres programmes malveillants qui peuvent même prendre en otage l'ordinateur tout entier. Ces actions peuvent être les suivantes :
  - Suppression de données
  - Blocage de données
  - Modification de données
  - Copie de données
  - Perturbation des performances des ordinateurs ou des réseaux informatiques

  Contrairement aux virus et aux vers informatiques, les chevaux de Troie ne s'auto-répliquent pas.

Reniflage (sniffing)

- Cette technique consiste à écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée.
- Cette technique peut être utilisée à l'interne pour le débogage ou de manière abusive par un pirate cherchant, par exemple, à se procurer un mot de passe.
- Vise surtout à intercepter les données non chiffrées. Dans certains réseaux (non commutés, reliés par "hub, l'ensemble des messages est transmis à tous. L'adversaire peut intercepter toutes les communications pour les analyser).

Mystification (Spoofing)

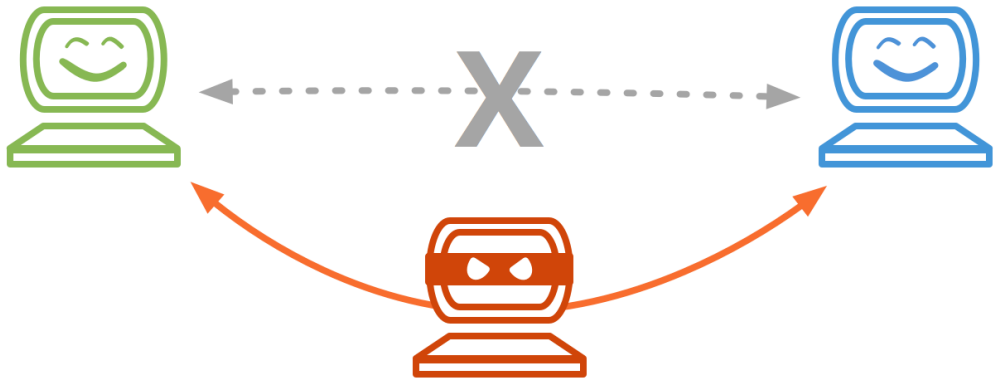
- Technique d'intrusion consistant à envoyer à un serveur des paquets qui semblent provenir d'une adresse IP connue par le coupe-feu. La machine est rendue inatteignable par le pirate pour pouvoir intercepter les codes de communication et établir la liaison pirate.

Attaque par rebond (bounce attack)

- Menée via un autre ordinateur qui se retrouve complice involontaire. Cet ordinateur expédie des messages d'attaque à la victime, masquant l'identité du pirate.

Attaque de l'homme du milieu

- Le pirate se place entre deux ordinateurs et se fait passer pour un afin d'obtenir le mot de passe de l'autre.
- Il peut alors se retourner contre le premier avec un mot de passe valide pour l'attaquer.
- L'attaquant intercepte toutes les messages échangés entre les deux victimes et peut aussi injecter d'autres.
- Exemple, un attaquant peut cibler une connexion Wi-Fi non chiffrée et s'insérer en tant que homme de milieu.



Déni de service (denial of service DoS) :

- Selon la norme ISO x.800 l'attaque de déni de service est: Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.
- Une attaque cherchant à rendre un ordinateur hors service en le submergeant de trafic inutile. Par exemple, un serveur entièrement occupé à répondre à de fausses requêtes de connexion.
- Des machines peuvent être à l'origine de l'attaque généralement à l'insu de leur propriétaire.
- Le but d'une telle attaque n'est pas de dérober (voler) des informations sur une machine distante, mais de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources.

Attaque physique

- C'est une attaque au niveau des infrastructures matérielles :
  - Salles sécurisées,
  - lieux ouverts au public,
  - espaces communs de l'entreprise,
  - postes de travail des personnels,
  - etc.
- Le but peut être de voler du matériel, comme il peut aller plus loin à la perturbation du bon fonctionnement des services de l'organisation.

Méthodes de défense

- La défense contre les attaques informatiques comporte un ensemble d'opérations de gérer et de diriger les différentes incidences liées à la manipulation de l'outil informatique.
- La gestion des risques consiste en trois actions majeures :
  1. Étudier les risques potentiels (identifier/mettre au jour ces risques) ;
  2. Imposer une politique de sécurité adéquates pour réduire ces risques ;
  3. Formation des utilisateurs à tous les niveaux.

a. Étudier les risques potentiels

- Cette phase consiste à faire un examen intégral de la méthodologie de l'étude des risques informatique en vigueur. Cela se matérialise aux moyens :
- **Définition de l'environnement:** Définition des acteurs et leurs intérêts ; il s'agit de préciser l'importance de la sécurité dans la stratégie de l'entreprise ; Type de données impliquées ; Visibilité extérieure de la sécurité (importance pour la clientèle, le public).
- **Étude des menaces:** Identifier la nature de la menace; accidentelles (désastre, bugs...) ou intentionnelles (attaques, vols...); S'enquérir des sources de la menace: personnel non autorisé, intrus, logiciel ; Localiser la menace : Procédures manuelles, informatique (software, réseau, stockage, hardware), infrastructure (concrète et abstraite).
  - Etude des vulnérabilités - Etudes des faiblesses engendrées par l'exécution d'une menace.
  - Etude des risques - Probabilité d'occurrence de ces menaces conduisant à une vulnérabilité.

a. Étudier les risques potentiels (2)

- **Estimation du risque et du plan stratégique :** Le Risque (Coût des pertes à court, moyen et long terme engendrées, Coût de la mise en place de la contremesure tant au niveau logique que logistique, Comparer la perte potentielle au coût de la contre-mesure) ; Plan stratégique (Planning de l'implémentation avec prise en compte des besoins futurs en termes de sécurité ou non, Planning du suivi de l'implémentation).
- **Audit de sécurité:** L'audit de sécurité consiste à s'appuyer sur un tiers de confiance (de préférence une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité. En fait, l'objectif de l'audit est ainsi de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent.

b. Mise en place d'une politique de sécurité

Les mécanismes de sécurité mis en place peuvent gêner les utilisateurs et les consignes et règles y définies peuvent devenir de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. Il est nécessaire de définir dans un premier temps une politique de sécurité dont la mise en œuvre s'effectue en quatre phases:

- Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- Élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

c. Formation des utilisateurs

- Il est de plus en plus admis que la sécurité est essentielle.
- Les coûts engendrés par les pertes de données dues aux attaques réseaux et autres malwares diminuent sensiblement d'années en années.
- Il est beaucoup plus simple de corrompre l'utilisateur et ce qui l'entoure que l'algorithme de chiffrement utilisé comme par exemple :
  - L'utilisateur ne connait pas les risques engendrés par la conservation de la liste des mots de passe utilisés à coté de l'ordinateur;
  - Il est souvent plus simple de s'introduire dans l'ordinateur de l'utilisateur afin de retrouver le texte en clair (hacking, vol, . . .) ;
  - Il est possible de l'espionner, le pousser à la délation, pratiquer tout autre technique dite de "social engineering", ...
- Il ne s'agira donc pas ici d'expliquer aux employés comment fonctionnent les algorithmes qu'ils utiliseront, mais plutôt comment et dans quelles conditions ils devront les utiliser en définissant des règles qui ne devront pas être transgressées.

Éléments d'une politique de sécurité informatique

- L"élément de politique de sécurité est l'ensemble des orientations suivies par une organisation en termes de sécurité.
- Elle est élaborée au niveau de système de pilotage (Direction), car elle concerne tous les utilisateurs du système.
- La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs,
- elle doit aussi aller au-delà de cela tout en couvrant les champs ci-après:
  - Mise en place des correctifs ;
  - Une stratégie de sauvegarde correctement planifiée ;
  - Description de la sécurité (de l'infrastructure physique, des données informatiques, des applications, du réseau) ;
  - Plan en cas de sinistre (Un plan de reprise après incident) ;
  - Sensibilisation du personnel aux nouvelles procédures,
  - Sanctions en cas de manquements.
  - Objectifs, Portée, Responsables ;

Éléments d'une politique de sécurité informatique (2)

La politique de sécurité fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptables. Voici quelques éléments pouvant aider à définir une politique :

- Quels furent les coûts des incidents informatiques passés ?
- Quel degré de confiance pouvez-vous avoir envers vos utilisateurs internes ?
- Quel sera l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte qu'elle devient contraignante ?
- Y a-t-il des informations importantes sur des ordinateurs en réseaux ? Sont-ils accessible de l'externe ?
- Quelle est la configuration du réseau et y a-t-il des services accessibles de l'extérieur ?
- Les règles juridiques applicables à l'entreprise concernant la sécurité et la confidentialité des informations (ex: loi " informatique et liberté", ...)

Parties d'une politique de sécurité

la politique de sécurité peut être découpée en plusieurs parties :

- **Défaillance matérielle:** Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut...) ; L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.
- **Défaillance logicielle:** Tout programme informatique contient des bugs. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problèmes peuvent contribuer à en diminuer la fréquence.
- **Accidents:** (pannes, incendies, inondations...) Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes; Disques RAID pour maintenir la disponibilité des serveurs ; Copie de sécurité via le réseau (quotidienne) ; Copie de sécurité dans un autre bâtiment (hebdomadaire).

Parties d'une politique de sécurité (Suite...)

la politique de sécurité peut être découpée en plusieurs parties :

- **Erreur humaine :** Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème.
- **Vol via des dispositifs physique (disques et bandes) :** Contrôler l'accès à ces équipements; ne mettre des disques amovibles, bandes... que sur les ordinateurs où c'est essentiel. Mettre en place des dispositifs de surveillances.
- **Virus provenant de supports amovibles :** Ce risque peut-être réduit en limitant le nombre de pots USB et lecteur mémoires en service. L'installation de programmes antivirus peut s'avérer une protection efficace mais elle est coûteuse, diminue la productivité, et nécessite de fréquentes mises à jour.
- **Piratage et virus réseau :** Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière.

Défauts de sécurité informatique

Les défauts de sécurité peuvent être considérés comme des modifications accidentelles ou inconscientes du fonctionnement normal des équipements informatiques. Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

- Installation des logiciels et matériels par défaut ;
- Mises à jour non effectuées ;
- Mots de passe inexistants ou par défaut ;
- Procédures de sécurité obsolètes ;
- Authentification faible ;
- Télémaintenance sans contrôle fort.

Les Anti-virus

Les antivirus

- Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie).
- Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).
- Il est intéressant de noter qu'une fois un fichier infecté, il ne l'est jamais deux fois.
- En effet, un virus est programmé de telle sorte qu'il signe le fichier dès qu'il est contaminé. On parle ainsi de signature de virus. Cette signature consiste en une suite de bits apposée au fichier. Cette suite, une fois décelée, permettra de reconnaitre le virus.

- Lorsque le virus est détecté par l'antivirus, plusieurs possibilités sont offertes pour l'éradiquer :
  1. Supprimer le fichier infecté ;
  2. Supprimer le code malicieux du fichier infecté ;
  3. Placer le ou les fichiers infectés en "quarantaine" pour un traitement futur.

Fonctionnement de l'Anti-virus

- Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteurs de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet) . Différentes méthodes sont possibles :
  - *la signature virale:* Les principaux antivirus du marché se concentrent sur des fichiers et comparent alors la signature virale du virus aux codes à vérifier ;
  - *La méthode heuristique* est la méthode la plus puissante, tendant à découvrir un code malveillant par son comportement. Elle essaie de le détecter en analysant le code d'un programme inconnu. Parfois de fausses alertes peuvent être provoquées ;
  - *L'analyse de forme:* repose sur du filtrage basé entre des règles rege-xp oubautres, mises dans un fichier junk. Cette dernière méthode peut être très efficace pour les serveurs de messagerie électronique supportant les rege-xp type postfix puisqu'elle ne repose pas sur un fichier de signatures.

Techniques de détection des Anti-virus (1)

Pour détecter les virus, les antivirus doivent user de plusieurs techniques spécialement :

- **Le scanning des signatures (Dictionnaire):** La détection des virus consiste à la recherche de ces signatures à partir d'une base de données de signatures (on parle également de définitions de virus). Le principal avantage de cette technique est qu'il est possible de détecter le virus avant qu'il ne soit en action. Cependant, il est nécessaire que sa signature soit présente dans la base de données afin qu'il soit détecté. De plus, il est nécessaire de tenir la base régulièrement à jour afin de pouvoir détecter les nouveaux virus.
- **Le moniteur de comportement :** Il s'agit ici de contrôler en continu toute activité suspecte telles que les lectures et écritures dans des fichiers exécutables, les tentatives d'écriture dans les secteurs de partitions et de boot du disque.

Techniques de détection des Anti-virus (2)

Pour détecter les virus, les antivirus doivent user de plusieurs techniques spécialement :

- **Liste autorisée:** est une technique de plus en plus utilisée pour lutter contre les logiciels malveillants. Au lieu de rechercher les logiciels connus comme malveillants, on empêche l'exécution de tout logiciel à l'exception de ceux qui sont considérés comme fiables par l'administrateur système (dans la liste autorisée). En adoptant cette méthode de blocage par défaut, on évite les problèmes inhérents à la mise à jour du fichier de signatures virales. De plus, elle permet d'empêcher l'exécution de logiciels indésirables. Étant donné que les entreprises modernes possèdent de nombreuses applications considérées comme fiables, l'efficacité de cette technique dépend de la capacité de l'administrateur à établir et mettre à jour la liste d'autorisation. Cette tâche peut être facilitée par l'utilisation d'outils d'automatisation des processus d'inventaire et de maintenance.

Techniques de détection des Anti-virus (3)

Pour détecter les virus, les antivirus doivent user de plusieurs techniques spécialement :

- **Le contrôleur d'intégrité :** Le principe est que l'antivirus maintienne une liste des fichiers exécutables associés à leur taille, leur date de création, de modification, voire un CRC (Contrôleur Redondance Cyclique). L'utilisation du CRC permet de vérifier qu'un exécutable n'a pas été modifié en comparant sa somme de contrôle avant et après son exécution. En effet, en dehors d'une mise à jour explicite du fichier, un fichier exécutable n'est pas sensé être modifié. Le même type de vérifications peut être instauré avec la date et l'heure de modification. Cependant, il suffira aux virus de mémoriser ces valeurs afin de pouvoir les restaurer par la suite.

Techniques de détection des Anti-virus (4)

Pour détecter les virus, les antivirus doivent user de plusieurs techniques spécialement :

- **L'analyse heuristique :** A la différence du moniteur de comportement qui détecte les modifications causées par les virus, l'analyse heuristique tente de détecter les virus avant leur exécution, en cherchant des portions de code suspectes. Il pourrait par exemple chercher des séquences de lecture suivies de séquences d'écriture sur un même fichier exécutable. Cette technique permet donc de détecter des virus même s'ils ne sont pas présents dans la base de données, puisque l'analyseur teste des séquences d'instructions communes à de nombreux virus.

Les systèmes de détection d'intrusion (IDS)

Les systèmes de détection d'intrusion (IDS)

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.
Les IDS, les plus connus selon leurs différentes catégories sont :

- Les IDS réseau (NIDS) - Snort ; Bro ; Suricata ; Enterasys ; Check Point ; Tipping point ; etc.
- Les IDS système (HIDS) - AIDE ; Chkrootkit ; DarkSpy ; Fail2ban ; IceSword ; OSSEC ; Rkhunter ; Rootkit Unhooker; Tripwire ; etc.
- Les IDS hybride - Prelude; OSSIM ; etc.

Typologie des systèmes de détection d'intrusion

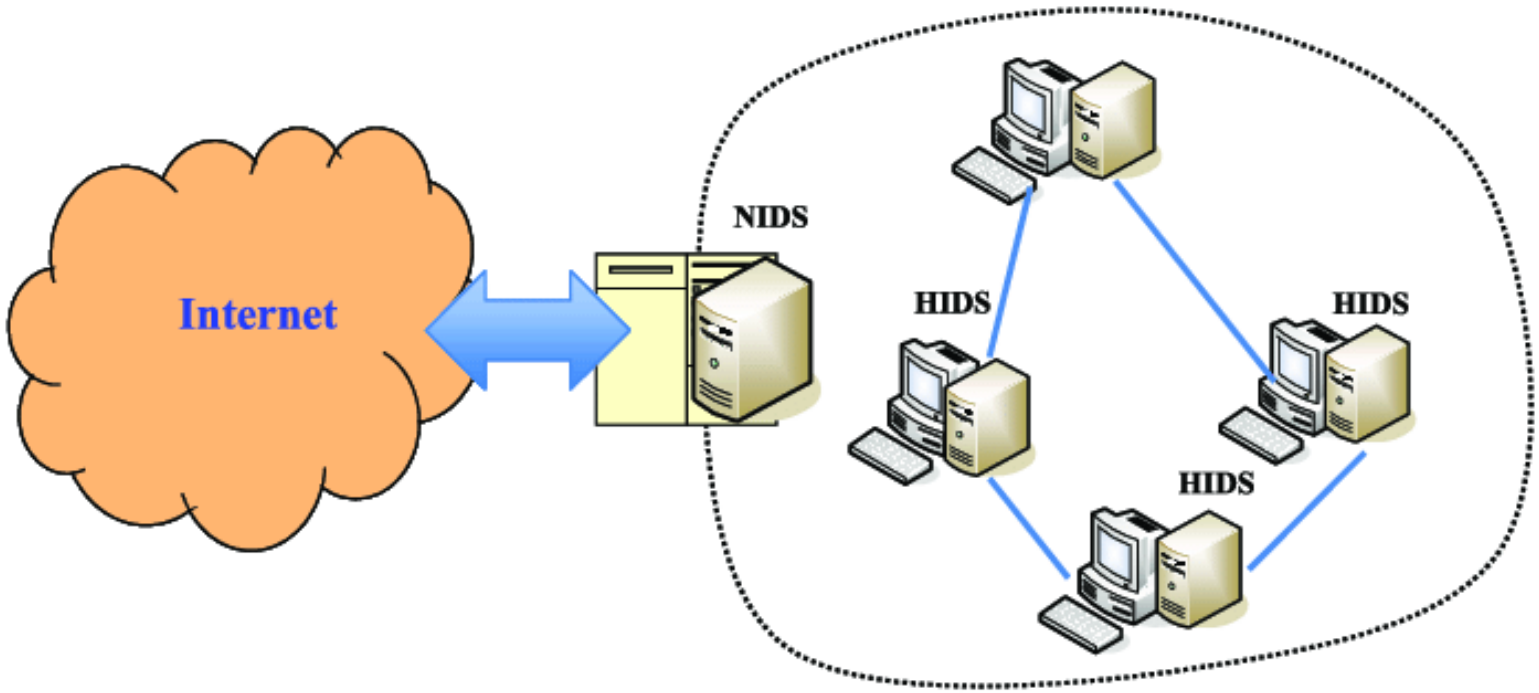
Il existe trois grandes familles distinctes d'IDS :

- les NIDS (Network Based Intrusion Detection System), qui surveillent l'état de la sécurité au niveau du réseau ;
- les HIDS (HostBased Intrusion Detection System), qui surveillent l'état de la sécurité au niveau des hôtes. Les HIDS sont particulièrement efficaces pour déterminer si un hôte est contaminé et les NIDS permettent de surveiller l'ensemble d'un réseau contrairement à un HIDS qui est restreint à un hôte.
- les IDS hybrides, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes.

Les NIDS (IDS réseau)

Un NIDS se découpe en trois grandes parties :

- la capture,
- les signatures et,
- les alertes.



Les NIDS (IDS réseau) (2)

1. **La Capture :**
   - La capture sert à la récupération de trafic réseau. En général cela se fait en temps réel, bien que certains NIDS permettent l'analyse de trafic capturé précédemment.
   - La plupart des NIDS utilisent la bibliothèque standard de capture de paquets libpcap.
   - La bibliothèque de capture de paquets (Packet Capture Library) est portée sur quasiment toutes les plates-formes, ce qui permet en général aux IDS réseau de suivre.
   - Le fonctionnement de la capture d'un NIDS est donc en général fortement lié à cette libpcap. Son mode de fonctionnement est de copier tout paquet arrivant au niveau de la couche liaison de données du système d'exploitation. Une fois ce paquet copié, il lui est appliqué un filtre BPF (Berkeley Packet Filter), correspondant à l'affinage de ce que l'IDS cherche à récupérer comme information.

Les NIDS (IDS réseau) (3)

1. **La Capture :**
   - Il se peut que certains paquets soient ignorés car sous une forte charge, le système d'exploitation ne les copiera pas.
   - Le comportement de la libpcap est différent dans le monde BSD, puisqu'il lui attache le fichier périphérique "/dev/bpf", permettant ainsi aux NIDS de ne pas avoir besoin des droits super utilisateur pour capturer le trafic mais simplement de pouvoir lire sur ce fichier sur lequel les filtres sont directement compilés.
   - Aussi, le trafic analysé n'est pas forcément égal à celui du trafic entrant, étant donné que la libpcap agit à une couche en dessous du pare-feu (qui agit au niveau réseau).

Les NIDS (IDS réseau) (3)

2. Les Signatures:

- Les bibliothèques de signatures (approche par scénario) rendent la démarche d'analyse similaire à celle des anti-virus quand ceux-ci s'appuient sur des signatures d'attaques.
- Ainsi, le NIDS est efficace s'il connaît l'attaque, mais inefficace dans le cas contraire.
- Les outils commerciaux ou libres ont évolué pour proposer une personnalisation de la signature afin de faire face à des attaques dont on ne connaît qu'une partie des éléments.
- Les outils à base de signatures requièrent des mises à jour très régulières.

Les NIDS (IDS réseau) (4)

3. Les alertes:

- Les alertes sont généralement stockées dans les journaux du système.
- Cependant il existe une norme qui permet d'en formaliser le contenu, afin de permettre à différents éléments de sécurité d'inter-opérer.
- Ce format s'appelle IDMEF (pour Intrusion Detection Message Exchange Format) décrit dans la RFC 4765.
- Le format IDMEF est popularisé par le projet Prelude, qui offre une infrastructure permettant aux IDS de ne pas avoir à s'occuper de l'envoi des alertes.
- Cela permet aux IDS de n'avoir qu'à décrire les informations qu'ils connaissent et "Prelude" se charge de les stocker pour permettre une visualisation humaine ultérieure.

Les HIDS (IDS machine)

- Les HIDS, (pour Host based IDS), signifiant "Système de détection d'intrusion machine" sont des IDS dédiés à un matériel ou système d'exploitation.
- Généralement, contrairement à un NIDS, le HIDS récupère les informations qui lui sont données par le matériel ou le système d'exploitation.
- Il y a pour cela plusieurs approches :
  1. Signatures,
  2. Comportement (statistiques) ou
  3. Délimitation du périmètre avec un système d'ACL (Access Control List).
- Un HIDS se comporte comme un daemon ou un service de fond standard sur un système hôte qui détecte une activité suspecte en s'appuyant sur une norme.

Les HIDS (IDS machine) (2)

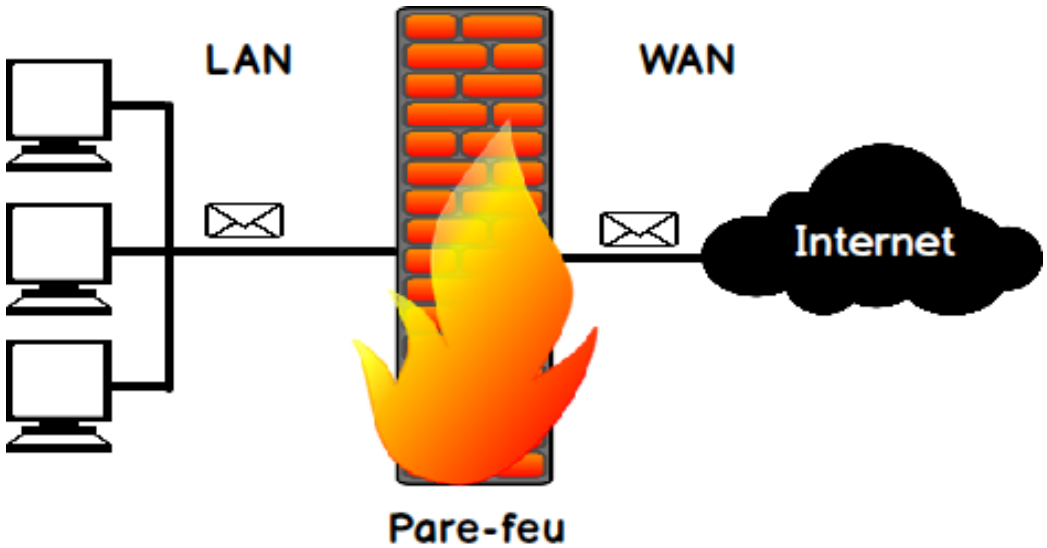
Si les activités s'éloignent de la norme, une alerte est générée. La machine peut être surveillée sur plusieurs points :

- **Activité de la machine** : nombre et listes de processus ainsi que d'utilisateurs, ressources consommées, ...
- **Activité de l'utilisateur :** horaires et durée des connexions, commandes utilisées, messages envoyés, programmes activés, dépassement du périmètre défini...
- **Activité malicieuse :** d'un ver, virus ou cheval de Troie.

Les pare-feu (Firewall)

Le pare-feu

- .Un pare-feu (parfois appelé coupe-feu, garde-barrière, barrière de sécurité, ou encore firewall.
- Est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique.
- Le pare-feu a pour objectif principal de surveiller et contrôler les applications et les flux de données (paquets), en empêchant les connexions non-autorisées sur un réseau informatique ou autres.



Niveaux d'action

En fait, un firewall peut être configuré à de nombreux niveaux :

- **Niveau des adresses IP :** on peut lui faire accepter les flux de données provenant d'une plage d'adresses, ou même d'une adresse uniquement.
- **Niveau des noms de domaine :** il est également possible d'empêcher l'accès à certaines adresses Internet.
- **Niveau des protocoles :** pour empêcher tout transfert FTP, tout accès Telnet, ou encore pour éviter le surf sur Internet (HTTP).
- **Niveau des ports :** pour supprimer le FTP, on peut refuser les connexions sur le port 21.
- **Niveau des mots ou phrases :** semblable aux expressions régulières, il est possible de refuser les paquets dont le contenu renferme des séquences de lettres données.

Principes de fonctionnement

- Le pare-feu est jusqu'à ces dernières années est considéré comme une des pierres angulaires de la sécurité d'un réseau informatique ,
- Il permet d'appliquer une politique d'accès aux ressources réseau (serveurs).
- Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.
- Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).
- Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège. On peut alors distinguer 3 types de principes de fonctionnement des pare-feux :
  1. Le filtrage de paquets (Packet Filtering)
  2. Le filtrage du flux (Circuit Filtering)
  3. La passerelle applicative (Application Gateway)

Catégories de pare-feu

Il existe 3 modèles de firewalls. Chacun possède des avantages et désagréments. Il faudra donc préalablement analyser les besoins réels en termes de sécurité, ainsi que les coûts engendrés avant toute utilisation :

- **Les firewalls Bridge :** Ce format de mur de feu a l'apparence d'un simple câble réseau, sans machine spécifique. Il est invisible et indétectable pour un pirate, son adresse MAC ne circulant jamais sur le réseau. Placé sur le réseau, le pirate devra donc automatiquement passer par lui pour transmettre des requêtes. On trouvera notamment ce type de firewalls dans des Switch. Ces formats de pare-feu ont pour avantages : Ils sont relativement peu coûteux et transparent lors de leurs mises en place. Ils présentent comme Inconvénients : Pour les contourner, il suffit d'adapter l'attaque ; et ses fonctionnalités sont souvent restreintes.

Catégories de pare-feu

Il existe 3 modèles de firewalls. Chacun possède des avantages et désagréments. Il faudra donc préalablement analyser les besoins réels en termes de sécurité, ainsi que les coûts engendrés avant toute utilisation :

- Les firewalls hardware - Ils sont souvent assimilés à des boites noires, l'accès à leur code étant difficile. Ce type de matériel propriétaire renferme d'ailleurs souvent un système de protection permettant d'authentifier le logiciel associé (par signature RSA par exemple), et ainsi rendre toute modification pratiquement impossible. Ils ont pour avantages : Ils sont facilement intégrables au réseau ; leur administration est souvent simplifiée et leur niveau de sécurité est assez élevé. Ils présentent comme Inconvénients : Ce type de firewall étant propriétaire, les mises à jour dépendent entièrement du constructeur et en raison de l'architecture hardware, peu de modifications sont autorisées.

Catégories de pare-feu

Il existe 3 modèles de firewalls. Chacun possède des avantages et désagréments. Il faudra donc préalablement analyser les besoins réels en termes de sécurité, ainsi que les coûts engendrés avant toute utilisation :

- Les firewalls logiciels - Ces pare-feu existent autant sous forme commerciales que sous forme gratuites. Quelque soit leur origine, la sécurité pourra fortement varier. Un logiciel commercial pourra parfois mettre en avant sa facilité de mise en place et de configuration, mais ce sera souvent aux dépends de la sécurité. Au niveau des logiciels gratuits et/ou libres, ils seront souvent plus flexibles (c'està- dire plus fournis en options), mais nécessiteront la plupart du temps de bonnes connaissances en réseau afin de les configurer finement sans abaisser le niveau de sécurité.

The end