CHAPITRE 4 :

VULNÉRABILITÉS ET SYSTÈMES DE DÉTECTION D'INTRUSION

I.VULNÉRABILITÉS

I.1 DÉFINITION

- Faiblesse au niveau **d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).

- Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire

I.VULNÉRABILITÉS

I.2 TYPES

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

- **Vulnérabilités humaines**

L'être humain par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (**négligence, manque de compétences, surexploitation**, etc.),

Un système d'information étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI.

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

I.VULNÉRABILITÉS

I.2 TYPES

- **Vulnérabilités technologiques**

Les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine lors de **la conception et la réalisation**.

- **Vulnérabilités organisationnelles**

  Les vulnérabilités d'ordre organisationnel sont dues **à l'absence des documents cadres** et formels, **des procédures (de travail, de validation) suffisamment détaillées** pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées.

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

- **Vulnérabilités mise en œuvre**

  Les vulnérabilités au niveau mise en œuvre peuvent être dues à la non prise en compte des certains aspects lors de la réalisation d'un projet. Par exemple, **la non prise en compte des procédures de maintenance** dans un projet d'acquisition et de mise en en production d'un serveur de données.

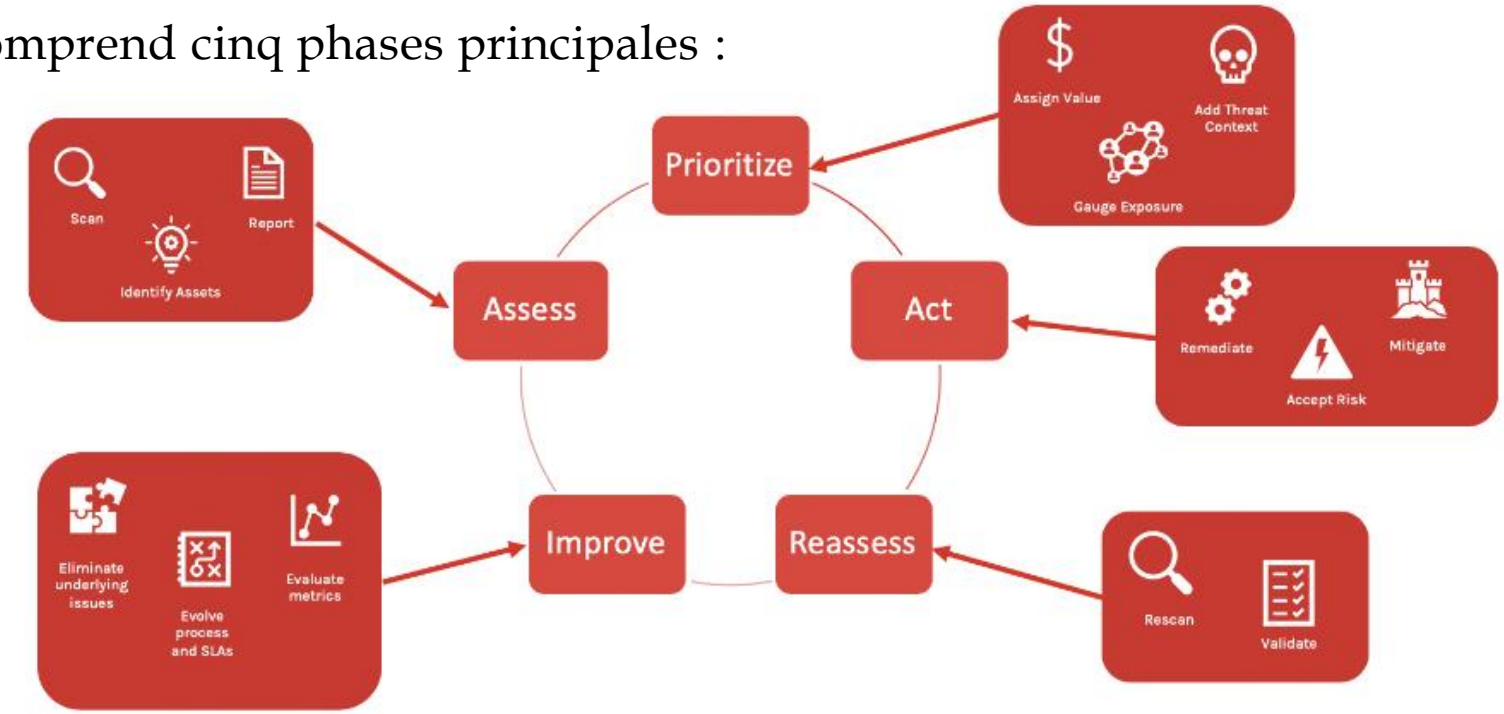
I. VULNÉRABILITÉS

I.3 CYCLE DE VIE DE GESTION DES VULNÉRABILITÉS

Les cinq phases du cycle de vie de la gestion des vulnérabilités

Le cycle de gestion des vulnérabilités comprend cinq phases principales :

- Phase 1. Évaluer
- Phase 2. Prioriser
- Phase 3. Agir
- Phase 4. Réévaluer
- Phase 5. Améliorer



I. VULNÉRABILITÉS

I.3 CYCLE DE VIE DE GESTION DES VULNÉRABILITÉS

Phase 1. Évaluer

L'évaluation constitue la première étape du cycle. Durant celle-ci, les analystes en sécurité trient et **identifient** les ressources à évaluer en vue d'identifier les vulnérabilités. L'étape suivante consiste à évaluer les vulnérabilités de chaque ressource, puis à générer un rapport identifiant les ressources à risque qui nécessitent un correctif ou qui doivent faire l'objet d'une investigation et d'une correction approfondies.

L'évaluation des vulnérabilités est généralement effectuée de deux manières : **à l'aide d'une solution déployée sur le réseau ou au moyen d'un capteur, ou agent, installé sur chaque ressource.**

Phase 2. Prioriser les vulnérabilités

Au cours de cette phase, l'équipe en charge de la gestion des vulnérabilités suit trois étapes afin de déterminer les mesures qui devront être prises lors de la phase suivante.

1. **Détermination de la valeur :** classer chaque ressource par ordre de priorité aux fins de l'investigation.
2. **Évaluation de l'exposition aux menaces de chaque ressource en fonction de son degré de priorité.** La détermination du niveau de risque de chaque ressource nécessite des investigations et des recherches.
3. **Ajout du contexte des menaces au rapport**

I. VULNÉRABILITÉS

I.3 CYCLE DE VIE DE GESTION DES VULNÉRABILITÉS

Phase 3. Agir

Que faire des informations recueillies lors de la phase de priorisation ? Trois possibilités s'offrent:

- **accepter le risque** que présente la ressource vulnérable pour le système. Cette option est envisageable dans le cas de ressources et systèmes non critiques, lorsque le risque d'exposition est très faible.
- **atténuer la vulnérabilité** ou élaborer une stratégie ou une technique qui compliquera, voire empêchera, l'exploitation de la vulnérabilité par un cyber-attaquant. La vulnérabilité n'est pas éliminée, mais les règles ou les protections mises en place préservent la sécurité de vos systèmes.
- **corriger la vulnérabilité.** Cette option doit être privilégiée si la vulnérabilité présente un risque élevé et/ou concerne un système ou une ressource critique de l'entreprise. Appliquez un correctif ou mettez la ressource à niveau avant qu'elle ne serve de point d'entrée à une attaque.

Phase 4. Réévaluer

Une fois les vulnérabilités classées par priorité et les mesures attribuées en fonction du niveau d'exposition, il faut bien réévaluer et vérifier le travail. Cette opération indiquera si les mesures prises ont été efficaces et si de nouveaux problèmes sont apparus au niveau des ressources concernées. Vous pourrez ainsi valider votre travail, supprimer les problèmes corrigés de votre liste et ajouter les éventuels nouveaux problèmes. La phase de réévaluation permet également de communiquer aux dirigeants de l'entreprise la mesure des efforts déployés par votre équipe.
menacer votre entreprise.

I. VULNÉRABILITÉS

I.3 CYCLE DE VIE DE GESTION DES VULNÉRABILITÉS

Phase 5. Améliorer

Il s'agit de la phase finale du processus de gestion des vulnérabilités. Les programmes de gestion des vulnérabilités les plus performants visent à améliorer constamment la sécurité, en renforçant les défenses déficientes, en éliminant les problèmes sous-jacents, en réévaluant la phase de travail préparatoire et en réexaminant les questions préparatoires. L'examen régulier de l'ensemble du cycle de vie de la gestion des vulnérabilités, ainsi que la recherche de possibilités d'évolution et d'amélioration vous permettent de vous protéger de manière proactive contre les vulnérabilités susceptibles d'être exploitées par un cyberattaquant pour menacer votre entreprise.

I. VULNÉRABILITÉS
I.4 EXEMPLES

Mécanisme d'authentification	Échec à authentifier adéquatement les utilisateurs.
Gestion de la session	Échec à créer, stocker, transmettre et protéger adéquatement l'information sensible de sessions telle que les mots de passe.
Permissions, privilèges et contrôle d'accès	Échec à appliquer les permissions et autres restrictions d'accès aux ressources, ou problème de gestion de privilèges.
Tampon	Dépassement de tampon, causé par une mauvaise gestion de celui-ci, permettant d'insérer plus d'information que la limite possible et créant ainsi une potentielle injection de code en mémoire.
Cross-Site Request Forgery (CSRF)	Échec à vérifier qu'une requête Web effectuée par un utilisateur provient de lui-même.
Cross-Site Scripting (XSS)	Échec d'un site à valider, filtrer ou encoder adéquatement l'information envoyée par un utilisateur avant de la lui retourner.
Cryptographie	Utilisation d'un algorithme de chiffrement non sécuritaire ou mauvaise utilisation d'un algorithme.
Parcours de chemin d'accès	Échec à valider adéquatement les chemins d'accès, permettant d'accéder à des fichiers en dehors du ou des répertoires prévus.

I. VULNÉRABILITÉS
I.4 EXEMPLES

Injection	Échec à valider les données d'utilisateurs ou les téléchargements de fichiers, permettant l'exécution de code arbitraire sur le système[20].
Configuration	Mauvaise configuration d'un système de l'organisation, permettant une utilisation non sécuritaire de celui-ci.
Fuite d'information	Exposition d'information système, sensible ou privée.
Situation de compétition (*Race Conditions*)	Défaut d'un système, caractérisé par un résultat différent selon l'ordre dans lequel agissent les composants et clients du système.
Architecture	Défaut de conception qui n'est pas causé par un problème d'implantation ou de configuration.

I.VULNÉRABILITÉS
I.5 IDENTIFICATION

Les techniques utilisées pour déceler des vulnérabilités sont nombreuses. Celles-ci dépendent notamment du contexte de l'organisation, des systèmes, de l'expertise disponible et de la stratégie de tests, y compris le niveau d'information disponible, le niveau d'accès utilisateur et le niveau d'accès réseau. En outre, ces techniques se catégorisent en deux grandes familles, **l'approche automatisée et l'approche manuelle**.

I.VULNÉRABILITÉS
I.5 IDENTIFICATION

- **Approche automatisée**

L'approche automatisée consiste à utiliser des outils, souvent appelés **balayeurs de vulnérabilités (scanners),** qui ont la capacité d'effectuer un nombre élevé de tests en peu de temps.

Cette technique, également appelée « balayage », permet d'analyser un certain nombre de problèmes dans le but de découvrir des vulnérabilités.

Par exemple, pour tester un site Web, un balayeur de vulnérabilités de sites Web pourrait être utilisé afin d'effectuer un balayage rapide du serveur Web.

Ce type d'outils permet de découvrir des problèmes de configuration majeurs et facilement identifiables. Par contre, ce type d'outils ne serait pas en mesure de déceler des vulnérabilités applicatives ou des vulnérabilités propres au produit utilisé.

Par ailleurs, les tests ne doivent pas s'arrêter aux outils automatisés, puisque ceux-ci ne tiennent pas suffisamment compte du contexte du système, identifient des faux positifs, ne contiennent pas l'ensemble des tests ou sont incapables de détecter certaines vulnérabilités.

De plus, les filtres de sécurité tels que les pare-feu applicatifs peuvent également influencer le fonctionnement des outils.

I.VULNÉRABILITÉS
I.5 IDENTIFICATION

- **Approche manuelle**

L'approche manuelle consiste à analyser, au moyen d'outils spécialisés, chaque composant en profondeur et, surtout, dans le contexte de leur environnement.
Exemple, dans le but de tester une page d'authentification, il est possible, entre autres, d'utiliser un serveur mandataire (proxy), outil permettant d'intercepter des requêtes et réponses afin de les lire ou de les modifier avant leur envoi. Il est également possible d'effectuer des injections directement dans les champs d'une page Web, simplement en utilisant un navigateur Web
Il est important de mentionner que l'approche manuelle requiert des connaissances avancées en Web, en programmation et en base de données, en plus des compétences en sécurité de l'information

bien que l'approche manuelle soit plus complexe, c'est l'approche qui est la plus efficiente. De manière générale, lorsque des tests sont envisagés par un organisme public, celui-ci devrait s'attendre à ce que 20 % du temps soit consacré à l'approche automatisée et que 80 % du temps soit dédié à l'approche manuelle.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.1 QU'EST CE QU'UNE INTRUSION?

- **Une intrusion** dans le système d'information correspond à l'accès **non autorisé** à une ressource logique.
- Par exemple, pénétrer dans un réseau d'entreprise ou un réseau wifi, parcourir et accéder aux données d'un ordinateur, d'un serveur.
- Les intrusions ont des objectifs multiples pour leur auteur : **Utiliser le SI pour des attaques** (utilisation d'un SI tiers piraté pour attaquer la cible voulue), Défiguration de site Web, Altérations ou vols de données (en forte croissance).
- Tous les systèmes sont concernés : Ordinateurs, téléphones portables, consoles de jeux, éléments réseaux
- Les intrusion touchent aussi bien les couches matérielles que Réseau, Systèmes ou Application.

II. SYSTÈMES DE DÉTECTION D'INTRUSION

II.2 DÉFINITION D'UN SYSTÈME DE DÉTECTION D'INTRUSION

- Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir **un logiciel spécialisé** dont le rôle serait **de surveiller** les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes.

- IDS (Intrusion Detection Systems), les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche.

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. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Ensemble de **composants logiciels et matériels** dont la fonction principale est de détecter et analyser toute tentative d'effraction (volontaire ou non).

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.2 DÉFINITION D'UN SYSTÈME DE DÉTECTION D'INTRUSION

- Les IDS protègent un système contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du système et du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus. Selon les méthodes de détection que vous choisissez de déployer, il existe plusieurs avantages directs et secondaires au fait d'utiliser un IDS.

- Les systèmes de détection d'intrusions (IDS pour Intrusion Detection System) ont pour objectif de révéler, généralement via des alertes, toute activité pouvant être considérée comme intrusive, depuis ou vers un système d'information, par analyse de données. Les sources de ces données correspondent à des événements générés par différents services ou utilisateurs.

- Aujourd'hui, il existe plus de 140 systèmes de détection d'intrusions différents

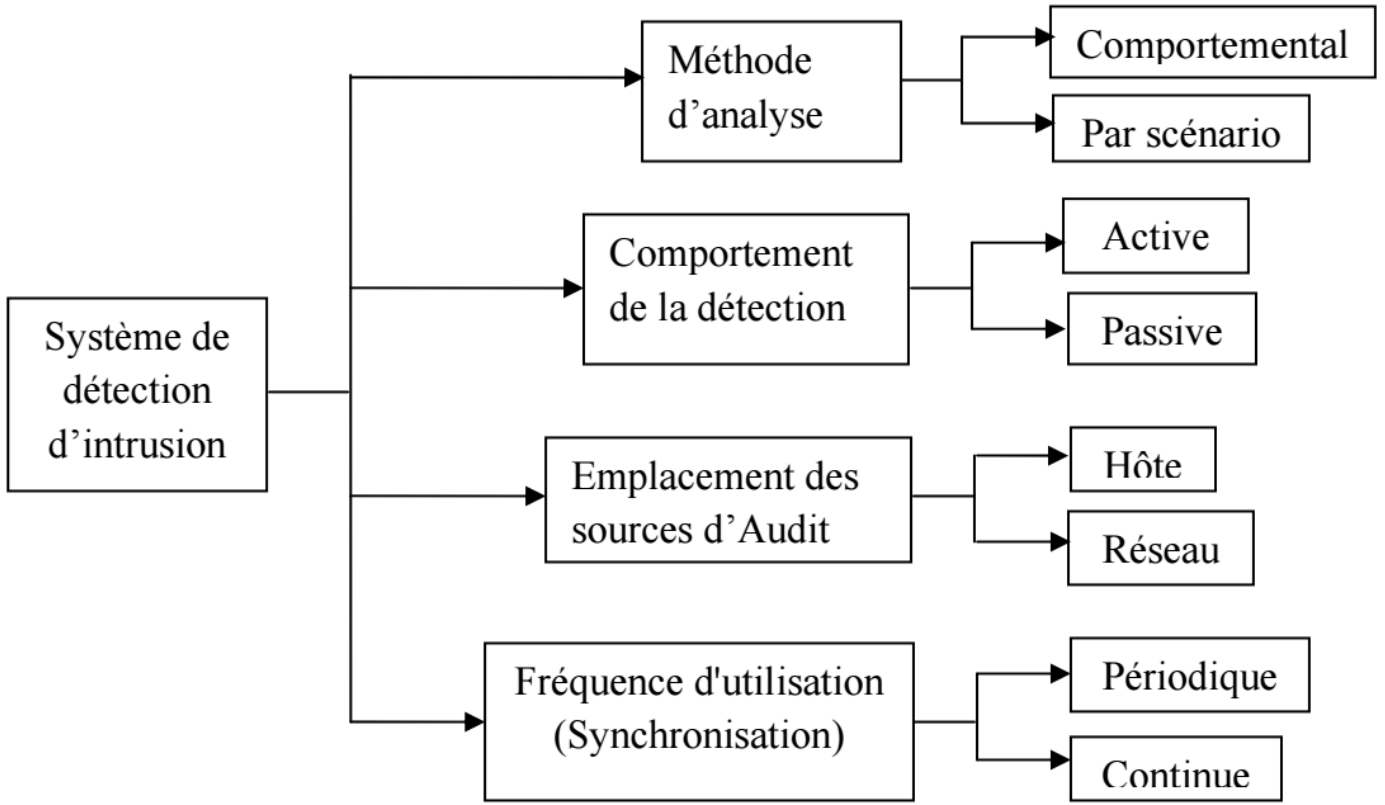
II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.3 OBJECTIFS

Les systèmes de détection d'intrusion sont considérés comme un élément nécessaire dans l'infrastructure de la sécurité informatique de chaque organisation. En effet, il y a plusieurs raisons pour acquérir et utiliser les systèmes de détection d'intrusion:

- Pour détecter les attaques et autres violations de sécurité qui ne sont pas empêchées par d'autres outils de sécurité.
- Pour documenter les menaces existantes dans une organisation, c'est-à-dire découvrir les vulnérabilités avant qu'elles ne soient exploitées par un attaquant.
- Pour agir en tant que contrôle de qualité pour la conception de sécurité, particulièrement dans les grandes et complexes entreprises.
- Pour fournir des informations utiles au sujet des intrusions qui ont eu lieu, et faire des diagnostics, recouvrement, et corrections des facteurs causatifs
- Pour arrêter les intrusions afin de limiter les dégâts. Malheureusement cela n'est pas toujours possible à cause de la complexité et la diversité des intrusions, et la naissance de nouveaux types d'intrusions liées au développement des nouvelles technologies d'information.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.4 CLASSIFICATION DES IDS

Il existe plusieurs critères qu'on peut utiliser pour classifier les différents systèmes de détection d'intrusion, dont les principaux sont résumés dans cette figure:



II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.4 CLASSIFICATION DES IDS

II.4.1 La méthode d'analyse

La méthode d'analyse définit **l'ensemble des techniques utilisées par les systèmes de détection d'intrusion dans le processus de la détection**.

- L'approche est dite **par scénario** si le détecteur analyse les informations relatives aux attaques,
- L'approche est dite **comportementale** si le détecteur analyse les informations relatives au comportement normal du système.

- la détection par scénario se base sur les caractéristiques d'une attaque connue pour la détecter.
- la détection comportementale se base sur la définition d'un modèle d'utilisation normal pour détecter tout ce qui est anormal.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II. 4 CLASSIFICATION DES IDS

II. 4. 1 . 1 L'approche par scénario:

La détection par scénario (mauvaise utilisation) considère comme normal tout ce qui n'est pas hostile, et elle adopte la politique suivante: " si ce n'est pas dangereux, alors c'est normal ". Donc, il est impératif de bien connaître les attaques possibles, la détection par scénarios (ou misuse detection) permet de détecter une attaque connue via la définition d'un scénario.

Cette approche utilise une base de connaissances, appelée base de signatures d'attaques (= **ensemble de caractéristiques permettant d'identifier une activité intrusive : une chaîne alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte**, …) d'attaques et une méthode de recherche de motifs permettant de reconnaître les signatures définies.

Un détecteur d'intrusions par scénario est alors composé de:

- Un ensemble de sondes produisant un flux d'évènements.
- Une base de signatures d'attaques.
- Un algorithme de recherche de motifs, comparant le flux d'événements aux signatures contenues dans la base.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II. 4 CLASSIFICATION DES IDS

- Recherche de motifs (pattern matching)
La méthode la plus connue et la plus à facile à comprendre. Elle se base sur la recherche de motifs (chaînes de caractères ou suite d'octets) au sein du flux de données. L'IDS comporte une base de signatures où chaque signature contient les protocole et port utilisés par l'attaque ainsi que le motif qui permettra de reconnaître les paquets suspects.

- Recherche de motifs dynamiques
Le principe de cette méthode est le même que précédemment mais les signatures des attaques évoluent dynamiquement. L'IDS est de ce fait doté de fonctionnalités d'adaptation et d'apprentissage.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II. 4 CLASSIFICATION DES IDS

La détection par scénario

Avantages

- Très efficace pour détecter des attaques sans produire un grand nombre de fausses alertes.
- Fiabilité pour les attaques connues.
- Peut rapidement et sûrement diagnostiquer l'utilisation d'un outil spécifique ou une technique d'attaque. Ceci peut aider les responsables de sécurité à donner la priorité aux mesures correctives.

Inconvénients

- Peut seulement détecter les attaques connues, dont les signatures sont introduites dans le système, donc le système de détection doit être constamment mis à jour avec les signatures des nouvelles attaques.
- Beaucoup de systèmes adoptant cette approche sont conçus pour employer un nombre limité de signatures qui peuvent être définis, ce qui les empêchent de détecter des variantes de ces attaques.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.4 CLASSIFICATION DES IDS

II. 4. 1 . 2 La détection d'anomalie (comportementale)

Cette technique consiste à détecter une intrusion en fonction du comportement passé de l'utilisateur. Pour cela, il faut préalablement dresser un profil utilisateur à partir de ses habitudes et déclencher une alerte lorsque des événements hors profil se produisent. Cette technique peut être appliquée non seulement à des utilisateurs mais aussi à des applications et services. Plusieurs métriques sont possibles : la charge CPU, le volume de données échangées, le temps de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés, les heures de connexion, …

Plusieurs approches peuvent être utilisées pour la méthode de détection comportementale :

- **Approche probabiliste**: Des probabilités sont établies permettant de représenter une utilisation courante d'une application ou d'un protocole. Toute activité ne respectant pas le modèle probabiliste provoquera la génération d'une alerte.

- Approche statistique: Le but est de quantifier les paramètres liés à l'utilisateur : taux d'occupation de la mémoire, utilisation des processeurs, valeur de la charge réseau, nombre d'accès à l'Intranet par jour, vitesse de frappe au clavier, sites les plus visités, …

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II. 4 CLASSIFICATION DES IDS

La détection d'anomalie (comportementale)

Avantages

- Les systèmes de détection d'intrusion basés sur la détection d'anomalie détectent le comportement peu commun, et ils ont ainsi la capacité de détecter des symptômes des attaques connues et inconnues sans la connaissance spécifique des détails.
- Cette approche permet de produire l'information utile pour la définition des signatures pour les systèmes de détection d'intrusion à base de signatures.

Inconvénients

- Le point noir de cette approche est le grand nombre de faux positif dues aux comportements imprévisibles des utilisateurs du réseau.
- Elle exige souvent l'historique à long terme des évènements enregistrés afin de caractériser les modèles normaux de comportement. Les systèmes basés sur cette approche doivent être dotés d'une certaine intelligence pour raison d'apprentissage automatique en utilisant par exemple les réseaux de neurones.
- Risque d'attaque lors de la construction des profils.
- Evolution des profils au cours du temps peut être vue comme une faille.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.4 CLASSIFICATION DES IDS

II. 4. 2 Le comportement de la détection (la réponse)

Le comportement de la détection décrit la réponse du système de détection d'intrusion à une attaque.

Elle est qualifiée d'active, si le détecteur réagit activement par des actions correctives, ou proactives (changer les règles de filtrage de Firewall, arrêter des connexions TCP, ou encore attaquer l'attaquant, etc.).

Si le système de détection d'intrusion génère simplement des alertes (afficher un message sur l'écran, générer un son spécifique, envoi d'un email, archivage dans un fichier ou dans une base de données, etc.), la réponse est qualifiée de passive.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.4 CLASSIFICATION DES IDS

II. 4. 2 . 1 Les réponses actives

Les réponses actives des IDSs sont des actions automatisées prises quand certains types d'intrusions sont détectés. Il y a trois catégories de réponses actives:

- **Rassembler des informations additionnelles :** Il est très important de rassembler des informations additionnelles sur une attaque afin de l'identifier avec précision. Dans le cas des IDSs, cela se traduira par l'exigence d'analyse des informations additionnelles, faire des corrélations, ou bien communiquer avec d'autres types d'IDSs installés sur le réseau.
- **Changer l'environnement:** Une autre réponse active doit stopper une attaque en progression et puis bloquer l'accès de l'attaquant. Typiquement, les IDSs n'ont pas les capacités de bloquer l'accès d'une personne spécifique, mais ils peuvent uniquement rompre des connexions ou bloquer certains paquets spécifiques en s'appuyant sur les mécanismes des protocoles Internet, cela est dû à la capacité du hacker expert de construire des paquets falsifiés .
- **Agir contre l'intrus:** la forme la plus agressive de cette réponse implique le lancement des contre-attaques ou d'essayer d'obtenir activement les informations sur le hôte ou l'emplacement de l'attaquant

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II. 4CLASSIFICATION DES IDS

II.4. 2. 2 Les réponses passives

Les réponses passives des IDSs fournissent l'information nécessaire aux administrateurs réseau et aux responsables de la sécurité pour les aider à prendre des mesures basées sur cette information. Beaucoup d'IDSs se fondent seulement sur des réponses passives dont les principales sont:

- **L'alerte:** Les alertes sont produites par les IDSs pour informer les administrateurs réseau quand des attaques sont détectées. La forme la plus commune est d'afficher un message d'alerte contenant des informations détaillées de l'intrusion détectée sur la console du responsable de la sécurité réseau. Une autre option très utile consiste à envoyer ces alertes au téléphone du responsable, on peut aussi envoyer des e-mails, ou générer des alertes sonores.

- **SNMP Trap:** Certains IDSs sont conçus pour produire des alertes et envoyer les rapports au système de gestion de réseau (network management system). Ils utilisent le protocole SNMP (Sample Network Management Protocol), qui est un protocole dédié à la gestion du réseau.

- **L'archivage**: L'archivage (logging) permet aux analystes de faire des analyses approfondies, et de faire des corrélations avec l'historique dont ils disposent concernant les évènements qui se sont produits auparavant.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.4 CLASSIFICATION DES IDS

II.4. 3 L'emplacement des sources d'audits

La manière la plus connue pour classifier les IDSs est de les grouper par sources d'informations (sondes). Certains IDSs analysent des paquets capturés à partir du réseau, en plaçant des sniffers sur les différents segments du réseau local. D'autres IDSs analysent des informations produites par le système d'exploitation ou par des applications pour la recherche des signes d'intrusions.

II. 4.3 .1 NIDS (Network-Based IDS)

Ces outils analysent **le trafic réseau**, ils comportent généralement une sonde qui "écoute" sur le segment de réseau à surveiller et un moteur qui réalise l'analyse du trafic afin de détecter les signatures d'attaques.

La plupart des NIDS sont aussi dits IDS on-line car ils analysent le flux en temps réel. Pour cette raison, la question des performances est très importante. De tels IDSs doivent être de plus en plus performants afin d'analyser les volumes de données de plus en plus importants pouvant transiter sur les réseaux.

II. 4.3 . 2 HIDS (Host-Based IDS)

Les IDSs de ce type analysent le fonctionnement et l'état des machines sur lesquelles ils sont installés afin de détecter les attaques. Pour cela ils ont pour mission l'analyse des journaux système (logs), le contrôle d'accès aux appels systèmes, la vérification d'intégrité des systèmes de fichiers, etc. Ils sont très dépendants de système sur lequel ils sont installés. Il faut donc employer des outils spécifiques en fonction des systèmes déployés. Ces IDSs peuvent s'appuyer sur des fonctionnalités d'audit propres ou non au système d'exploitation, pour en vérifier l'intégrité, et générer des alertes. Il faut cependant noter qu'ils sont incapables

II. 4.3 .3 IDS d'application

Similaires aux HIDSs, ils sont installés sur un serveur ou une machine pour détecter les attaques relatives à une application donnée. Par exemple un IDS installé sur un serveur Oracle pour détecter les intrusions relatives à Oracle.

II. 4. 3 .4 IDS hybrides

Les IDS hybrides rassemblent les caractéristiques de plusieurs IDS différents. En pratique, on ne retrouve que la combinaison de NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et l'hôte. Les sondes sont placées dans des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser, agréger, et lier les informations d'origines multiples.

II. 4. 4 La fréquence d'utilisation (la synchronisation)

La synchronisation se rapporte au temps écoulé entre les évènements qui sont surveillés et l'analyse de ces évènements. Elle est réalisée en: temps réel ou différé:

II.4.4.1 En temps différé (périodique)

Dans cette classe, le flux d'informations émanant des points de surveillance vers les détecteurs n'est pas continu. En effet, l'information est traitée dans un mode semblable au principe "emmagasiner et expédier". Cette approche est employée surtout dans les Host-IDSs qui scrutent les logs du système d'exploitation dans des intervalles de temps réguliers.

II.4.4.2 En temps réel (continu)

Les IDSs en temps réel traitent des flux continus d'informations à partir des différentes sources d'informations. C'est la technique prédominante de synchronisation pour les IDSs réseau, qui recueillent l'information du trafic réseau. Par conséquent Les IDSs peuvent prendre des actions pour affecter la progression d'une attaque détectée.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.5 PRINCIPES GÉNÉRAUX ET INSTALLATION TECHNIQUE

Lors de la mise en place d'un système de détection d'intrusions au sein d'un réseau, il est important de le déployer correctement d'une part, mais aussi de comprendre son fonctionnement interne pour pouvoir le configurer efficacement. Toute erreur lors de l'installation d'un IDS pourra le rendre inefficace ou inutilisable

Configurer correctement l'IDS afin qu'il n'inonde pas les rapports d'alertes avec des faux positifs. La présence de faux positifs semble inoffensive. Or, s'ils sont trop nombreux, les rapports d'alertes seront longs à analyser. Par conséquent, les administrateurs passeront beaucoup de temps à distinguer un faux positif d'une véritable intrusion. Et de plus, en voyant toutes ces fausses alertes, ils auront tendance à minimiser le risque d'attaque.

Un NIDS ne fera qu'analyser le trafic réseau. Mais complété par un HIDS, des intrusions non détectées sur le réseau pourront l'être lorsqu'elles atteindront la machine cible. En général, un seul NIDS par réseau est suffisant. Mais il est possible de placer des sondes à différents endroits du réseau afin de répartir la charge. L'idéal pour les HIDS serait d'en déployer sur toutes les machines du parc informatique mais cela n'est rarement fait pour des raisons de coût et d'exploitation.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.6 TECHNIQUES ANTI-IDS

Comme tout système informatique, ou presque, il existe des failles dans les IDS, ou plutôt des techniques qui permettent d'outrepasser ces systèmes sans se faire repérer. Si un pirate détecte la présence d'un IDS, il peut le désactiver, ou mieux encore, générer de fausses attaques pendant qu'il commettra son forfait tranquillement.
Il existe trois catégories d'attaques contre les IDS :

- Attaque par déni de service : rendre l'IDS inopérant en le saturant.
- Attaque par insertion : le pirate, pour éviter d'être repéré, injecte des paquets de leurre qui seront ignorés par le système d'exploitation de la cible mais pris en compte par l'IDS : l'IDS ne détecte rien d'anormal, alors que sur le système cible, l'attaque a bien lieu puisque les paquets superflus sont ignorés.
- Attaque par évasion : il s'agit de la technique inverse à l'attaque par insertion. Ici, des données superflues sont ignorées par l'IDS mais prises en compte par le système d'exploitation.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II.7 CRITÈRES D'EFFICACITÉ DES IDS

Lors de la mise en place d'un IDS, il est nécessaire de prendre en considération plusieurs critères qui permettront de choisir au mieux l'IDS.

Tester un IDS avec des scanners de vulnérabilité est une mesure nécessaire pour évaluer un IDS, mais est loin d'être suffisante. D'autres critères doivent être pris en compte :

- Méthodes et capacités de détection : estimer le taux de faux positifs et la qualité d'information fournie par l'IDS.
- Rapidité : tester l'IDS en condition de charge élevée. Il est important de tester cela de manière réaliste, et non pas en utilisant des générateurs de paquets.
- Ouverture : il faut que l'IDS permette de modifier les signatures afin d'éviter certains faux positifs, mais aussi d'ajouter de nouvelles signatures spécifiques à l'environnement.
- Architecture logicielle : pour les grandes entreprises, il est intéressant de pouvoir séparer les fonctions d'administration.
- Exploitabilité des données : il faut disposer d'outils permettant de retrouver et analyser facilement les événements suspects car le volume généré par les IDS est important.
- Ergonomie : on retrouve différents types d'interfaces dans les IDS.

II. SYSTÈMES DE DÉTECTION D'INTRUSION

II. 7 EFFICACITÉ DES IDS

- **L'exactitude** (accuracy): on parle de l'exactitude quand le système de détection d'intrusion déclare comme malicieux une activité légale.
- **La performance** (performance): la performance de système de détection d'intrusion est la vitesse de traitement des évènements. Si cette vitesse est faible, la détection en temps réel est donc impossible.
- **La complétude** (completeness): on parle de la complétude quand le système de détection d'intrusion rate la détection d'une attaque. Ce critère est le plus difficile parce qu'il est impossible d'avoir une connaissance globale sur les attaques.
- **La tolérance aux fautes** (Fault tolerance): le système de détection d'intrusion doit lui- même résister aux attaques, particulièrement au déni de service. Ceci est important, parce que plusieurs systèmes de détection d'intrusion s'exécutent sur des matériels ou logiciels connus comme vulnérables aux attaques.
- **La réaction à temps** (Timeliness): le système de détection d'intrusion doit s'exécuter et propager les résultats de l'analyse le plus tôt possible, pour permettre à l'autorité de réagir avant que des graves dommages n'aient lieu. Ceci implique plus qu'un calcul de performance, parce qu'il ne s'agit pas seulement de temps de traitement des évènements, mais aussi du temps nécessaire pour la propagation et la réaction à cet évènement.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II. 8 L'ÉVALUATION DES IDS

La performance d'un système de détection d'intrusions, et notamment de sa méthode d'analyse, est liée à deux notions importantes qui permettent d'évaluer ces performances :

- Faux négatif
Idéalement, toute intrusion doit donner lieu à une alerte. **Une intrusion non détectée, c'est-à-dire n'ayant pas généré d'alerte**, constitue alors un faux négatif. La fiabilité (ou couverture) d'un Analyseur est liée à son taux de faux négatifs qui représente alors le pourcentage d'intrusions non détectées, ce taux devant être le plus bas possible.

- Faux positif
Toute alerte doit correspondre à une intrusion effective. Lorsqu'un système **de détection d'intrusions génère une alerte qui n'a pas lieu d'être, cette alerte est qualifiée de faux positif.** La pertinence (ou crédibilité) d'un Analyseur est liée à son taux de faux positifs qui représente alors le pourcentage de fausses alertes.

II. SYSTÈMES DE DÉTECTION D'INTRUSION
II. 9 LES LIMITATIONS DES IDS

Les systèmes de détection d'intrusion, souffrent généralement de limitations communes, on peut citer les points suivants :

- Le nombre important de faux positifs et faux négatifs.
- L'identification faible et imprécise: même lorsque l'IDS détecte des attaques, il les identifie parfois mal.
- La corrélation des alertes.
- Les nouvelles attaques: sont les attaques qui jamais n'ont été observées avant ou précédemment. Ces attaques essayent d'exploiter des vulnérabilités.
- Variation d'attaque.

CONCLUSION

Ces dernières années, les systèmes de détection d'intrusion ont gagné une place importante dans la conception de la sécurité des systèmes d'information. Ils sont largement déployés dans les entreprises pour diverses raisons telles que: la documentation des attaques, l'évaluation de la sécurité, et plus généralement la surveillance des systèmes d'information pour arrêter, voir empêcher les attaques afin de limiter les dégâts. Les systèmes de détection d'intrusion se caractérisent principalement par:

- La méthode de détection, on distingue deux principales méthodes: détection par scénario et détection d'anomalie. Ces deux méthodes présentent des avantages et des inconvénients;
- Les sources d'information, qui peuvent être: le réseau, le hôte et les applications;
- Le comportement de la détection, qui peut être passif ou actif;
- La synchronisation entre les sources et le détecteur, qui peut être périodique ou continue pour les IDS temps réel.

Enfin, notons que le système de détection d'intrusion n'est pas une solution complète, il possède beaucoup de limites et problèmes liés à plusieurs facteurs tels que:

- l'observation des évènements, le facteur humain et les attaques par déni de service. Mais le problème majeur de ce mécanisme de sécurité est le taux très important de faux positifs