Chapitre 1 - Détection d'Intrusion : Concepts et Classification

Dr. ZAMOUCHE Djamila

Université A. MIRA - Bejaia

Faculté des Science Exactes

Département d'Informatique

Email : djamila.zamouche@univ-bejaia.dz

2024 / 2025

Table des matières

Objectifs **4**

I - Pré-requis **5**

II - Organisation du module **6**

III - Introduction **7**

IV - Attaques réseau **8**

1. Types d'attaques réseau....8

2. Les étapes d'une attaque réseau....10

V - Détection d'intrusion **12**

VI - Systèmes de détection d'intrusion **13**

1. Définition....13

2. Classification....14

2.1. Approches d'analyse....14
2.2. Sources d'information....16
2.3. Réponse à l'intrusion....20
2.4. Avantages d'IDS....20
2.5. Limites d'IDS....20

3. Similitudes et différences entre IDS et IPS....20

4. Critères d'évaluation....21

4.1. Erreurs de classification....21
4.2. Exactitude....22
4.3. Précision....22
4.4. Rappel....22
4.5. F1 score....22

5. Exemples d'IDS....23

5.1. SNORT....23

VII - Exercices **26**

1. Exercice....26

2. Exercice....26

3. Exercice....26

4. Exercice....26

5. Exercice....27

6. Exercice....27

7. Exercice....27

8. Exercice 27

Solutions des exercices **28**

Objectifs

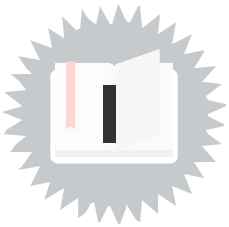
Le module "*Intelligence Artificielle et Sécurité des Réseaux*" a pour but d'aider l'étudiant à :

- Connaître des définitions pertinentes sur les Systèmes de Détection d'Intrusion ;
- Comprendre le lien qui relie inévitablement deux concepts omniprésents : *Intelligence Artificielle (IA)*, *Sécurité des Réseaux* ;
- Identifier la façon dont les techniques de l'IA, notamment celles du Machine Learning (ML) peuvent être appliquées à des problèmes de sécurité ;
- Connaître les différents concepts du Deep Learning (DL) ;
- Découvrir des principaux ensembles de données (datasets) utilisés pour le test et l'évaluation des IDS.

Le cours "*Détection d'Intrusion : Concepts et Classification*" vise à :

- Rappeler les différentes attaques réseau les plus courantes ;
- Introduire les définitions pertinentes sur les Systèmes de Détection d'Intrusion (IDS) ;
- Établir une classification des IDS ;
- Décrire certaines métriques qui peuvent être utilisées pour évaluer ces systèmes ;
- Présenter certains des IDS actuels.

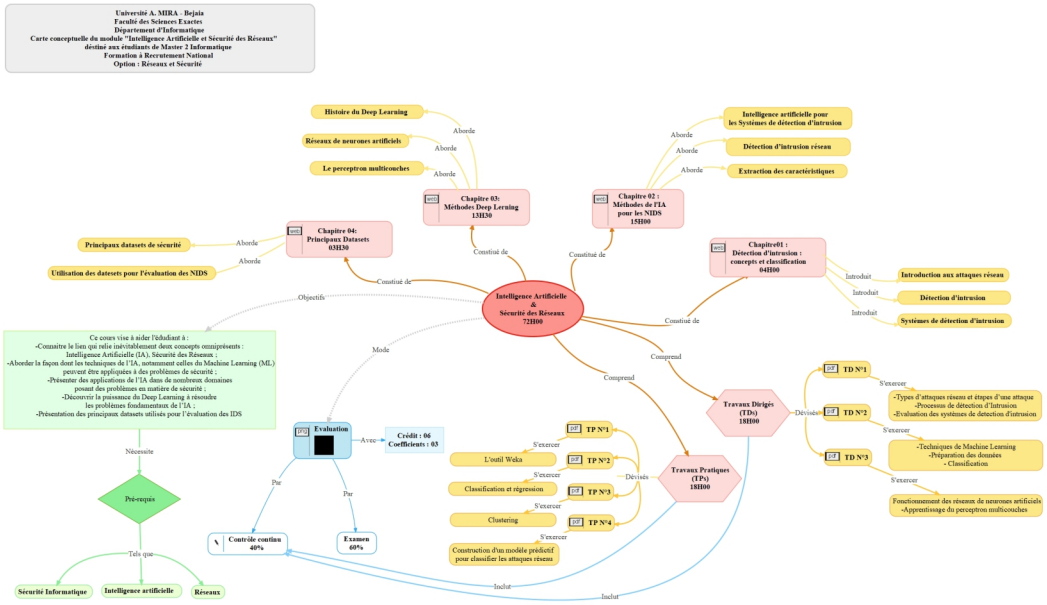
Pré-requis



Des connaissances préalables sont nécessaires pour une compréhension adéquate du cours "*Intelligence Artificielle et Sécurité des Réseaux*" . Ces connaissances sont logiquement déjà acquises par les étudiants au cours de leur formation à travers le module Sécurité et le module réseaux en troisième année de Licence et le module Intelligence Artificielle en première année de Master. Donc, il est recommandé aux étudiants de connaître :

- Des connaissances en sécurité Informatique, notamment sur les menaces et malveillances informatique ;
- Des notions relatives à l'intelligence artificielle et à l'apprentissage automatique (Machine Learning) ;
- Réseaux (leur rôle ainsi que les différents équipements qui les composent).

Organisation du module



Carte conceptuelle du cours

Introduction

De nombreuses techniques de sécurité informatique ont été développées au cours de la dernière décennie. Une contrainte fondamentale dans la conception des systèmes de sécurité est de protéger la confidentialité, l'intégrité et la disponibilité des ressources. La protection des systèmes/réseaux d'information est généralement assurée par la restriction des accès aux ressources du système au moyen d'un antivirus, d'un pare-feu, de la cryptographie, de protocoles de réseau sécurisés, d'un mécanisme de protection par mot de passe, etc. Cependant, en raison de la nature dynamique des données sur les réseaux informatiques, aussi vu l'évolution des techniques utilisées par les attaquants, les mécanismes ci-dessus de protection des informations ne sont pas suffisants. Une suite naturelle à cette exigence est de concevoir des systèmes de détection d'intrusion (IDS pour Intrusion Detection Systems en anglais), qui sont l'un des composants les plus courants de toute infrastructure de sécurité de réseau, y compris les réseaux sans fil afin d'identifier les intrusions qui ne peuvent pas être détectées par les méthodes classique.

Dans ce chapitre, nous abordons d'abord les différentes attaques réseau les plus courantes. Nous présentons brièvement par la suite toutes les définitions pertinentes sur les IDS, suivi d'une classification des IDS, basée sur leur emplacement et l'approche adoptée. Nous expliquons également et fournissons un certain nombre de métriques qui peuvent être utilisées pour évaluer ces systèmes. Finalement, une brève introduction à certains des IDS actuels est donnée.

Attaques réseau

Attaque *Définition*

C'est n'importe quelle action malveillante visant à menacer la sécurité des informations et de nuire au moins à l'une des propriétés de la sécurité informatique (disponibilité, Confidentialité, Intégrité, l'authentification).

Attaque réseaux *Définition*

Une attaque réseau est une action ciblant les composants d'un réseau informatique dans le but de compromettre la sécurité des données ou des services qui transitent sur ce réseau. Elle peuvent prendre diverses formes, cependant, la plupart d'entre elles ne sont que des variantes des autres.

1. Types d'attaques réseau

Il existe un nombre énorme d'attaques qui menacent les systèmes et les réseaux informatiques. Dans ce qui suit, nous présentons les attaques réseau les plus courantes que nous exploiterons dans ce module.

- **Dénie de Service** : les attaques par déni de service (Denial of Service (DoS)) visent à perturber le fonctionnement normal des services du réseau en inondant, épuisant et submergeant les ressources du réseau ou de l'hôte visé. Ces ressources peuvent être la bande passante du réseau, la capacité de transfert de paquets du routeur, la mémoire/la puissance de calcul des serveurs ou les structures de données des systèmes d'exploitation. Au cours des attaques DoS, les attaquants génèrent généralement de grandes quantités de trafic absurde, comme des connexions TCP incomplètes, des paquets IP mal-formés, des demandes de pages Web générées par des bots et d'autres méthodes soigneusement élaborées, ce qui entraîne l'arrêt du fonctionnement du service ou du programme ou empêche d'autres personnes de l'utiliser.
- **Dénie de Service Distribué :** les attaques par déni de service distribué (Distributed Denial of Service (DDoS)) se développent de manière distribuée. Dans les réseaux réels, les victimes visées par les attaques DoS sont généralement des serveurs puissants disposant de connexions réseau rapides. Dans la plupart des cas, l'attaquant ne dispose que de ressources limitées en matière de calcul. Par conséquent, pour mener à bien une telle attaque contre un serveur victime puissant, l'attaquant distribue et propage le scénario de l'attaque sur plusieurs hôtes intermédiaires. Ces hôtes intermédiaires sont appelés "zombies" ou "bots" dans la communauté des pirates.
- **Attaque par sondage :** les attaques par sondage du réseau (appelée network probe attack) sont généralement des attaques qui examinent les réseaux informatiques pour recueillir des informations ou trouver des vulnérabilités connues, qui sont exploitées pour des attaques ultérieures ou futures. Ces informations comprennent l'adresse IP, l'adresse électronique, le nom de l'hôte, le nom du service, l'adresse du pays, l'application du système d'exploitation, etc., qui sont nécessaires à l'attaquant. L'objectif de cette collecte d'informations est de découvrir les ordinateurs et les services présents sur un réseau et de détecter la possibilité d'une attaque basée sur des vulnérabilités connues.

- **Attaque de l'homme au milieu (Man-in-the-Middle) :** Dans ces attaques, un attaquant s'insère entre les communications de deux parties pour intercepter ou manipuler les données échangées. Exemple : Attaque ARP poisoning.
- **Attaque de Scan de Port :** Les attaques de scan de port consistent à explorer les ports ouverts sur un système ou un réseau pour trouver des vulnérabilités. Exemple : Scan de ports SYN.
- **Attaque par Usurpation d'Identité (Spoofing) :** L'usurpation d'identité consiste à falsifier l'adresse IP, MAC ou d'autres informations pour se faire passer pour une source légitime. Cela peut être utilisé pour tromper les systèmes de sécurité ou les utilisateurs. Exemple : Spoofing ARP.
- **Attaque de routage :** les attaques de routage (Routing attacks) exploitent les failles et les vulnérabilités dans la conception et la mise en œuvre des routeurs. Une attaque de routage est une intrusion spécifique à un protocole qui cible les opérations d'échange d'informations de routage. La plupart des attaques sophistiquées ou des attaques DoS substantielles sont à l'origine basées sur les attaques de routage contre l'infrastructure de routage IP.
- **Logiciels malveillants :** les malwares peuvent être utilisés comme composants d'une attaque réseau plus large. Par exemple, un attaquant peut utiliser un malware pour infecter un ordinateur sur un réseau, puis utiliser ce malware pour exfiltrer des données ou prendre le contrôle du système à distance. Dans ce cas, le malware est un vecteur d'attaque qui contribue à l'attaque réseau globale.

  Un logiciel malveillant (malware) est un programme ou un fichier qui endommage intentionnellement un système informatique. Certains des principaux types de malwares sont les suivants :

  - **Botnets :** les bots sont un malware dont l'objectif est de tenter de se propager à un plus grand nombre possible d'hôtes d'un réseau, afin de mettre leur capacité de calcul au service de l'attaquant. Ils compromettent les hôtes, établit une communication avec un serveur de commande et de contrôle et commence à exécuter des actions automatisées sous le contrôle de l'attaquant. À l'aide du malware bot, les attaquants rassemblent les appareils dans un botnet, un vaste réseau d'appareils compromis sous leur contrôle. Les botnets sont fréquemment utilisés dans les attaques DDoS.
  - **zero-day :** une attaque de type "zero-day" (ou 0-day) est une vulnérabilité logicielle exploitée par des attaquants avant que le fournisseur n'en ait pris connaissance. À ce stade, aucun correctif n'existe, de sorte que les attaquants peuvent facilement exploiter la vulnérabilité en sachant qu'aucune défense n'est en place. Les vulnérabilités de type "zero day" constituent donc une grave menace pour la sécurité.

    Une fois que les attaquants ont identifié une vulnérabilité de type "zero day", ils ont besoin d'un mécanisme de diffusion pour atteindre le système vulnérable. Dans de nombreux cas, le mécanisme de livraison est un courrier électronique d'ingénierie sociale, un courrier électronique ou un autre message censé provenir d'un correspondant connu ou légitime, mais qui est en fait celui d'un attaquant. Le message tente de convaincre un utilisateur d'effectuer une action telle que l'ouverture d'un fichier ou la visite d'un site web malveillant, activant ainsi involontairement l'exploit.
  - **Les chevaux de Troie :** les chevaux de Troie sont des logiciels malveillants que les utilisateurs installent sciemment et considèrent comme des logiciels légitimes. Les chevaux de Troie s'appuient sur des techniques d'ingénierie sociale pour s'infiltrer dans l'appareil d'une victime. Une fois déployé sur un appareil, un cheval de Troie déploie sa charge utile - un logiciel malveillant conçu pour faciliter l'exploitation de l'appareil. Les chevaux de Troie permettent aux attaquants d'accéder par une porte dérobée aux appareils, d'exécuter des enregistreurs de frappe, d'installer des virus ou des vers et de voler des données.

    - **Rootkit :** est un logiciel qui permet à un attaquant de prendre le contrôle à distance de l'ordinateur d'une victime avec des privilèges d'administrateur complets. Les rootkit se propagent par le biais du phishing, de pièces jointes malveillantes, de téléchargements malveillants et de lecteurs partagés corrompus. Ils peuvent également être utilisés pour cacher d'autres logiciels malveillants tels que les enregistreurs de frappe.
- **Spams :** les spams peuvent être considérés comme une forme d'attaque réseau, bien que leur objectif principal ne soit généralement pas de compromettre la sécurité du réseau, mais plutôt de diffuser du contenu non sollicité à un grand nombre de destinataires. Les spams peuvent prendre différentes formes, notamment des courriers électroniques indésirables, des messages texte non sollicités, des commentaires publics non désirés sur les réseaux sociaux, etc. Donc, bien que les spams ne soient pas nécessairement aussi nuisibles que certaines attaques réseau plus graves, ils peuvent toujours être considérés comme une forme de perturbation non autorisée du réseau.

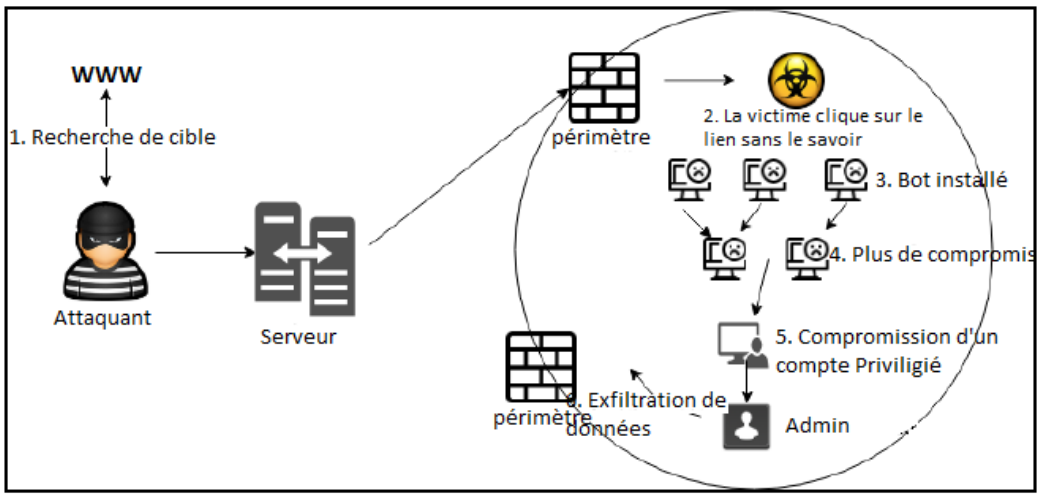
2. Les étapes d'une attaque réseau

Pour comprendre les détails de l'anomalie réseau, nous allons aborder les six (06) étapes des cyberattaques.

1. **Phase 1 – Reconnaissance :** il s'agit de la toute première étape d'une attaque réseau, au cours de laquelle les vulnérabilités et les cibles potentielles sont identifiées. Une fois l'évaluation des vulnérabilités et la mesure des défenses effectuées, une arme est choisie, qui peut être une attaque par hameçonnage, une attaque de type "zero-day" ou une autre forme d'attaque par logiciel malveillant.
2. **Phase 2 – Compromission initiale :** c'est au cours de cette phase de l'attaque que se produit la première compromission, par exemple le dépôt d'un courriel de harponnage ou le contournement des pare-feu du réseau.
3. **Phase 3 – Commande et contrôle :** une fois la compromission initiale effectuée, une connexion est établie avec le dispositif d'origine, également appelé serveur de commande et de contrôle. En général, cette étape nécessite que l'utilisateur installe un cheval de Troie d'accès à distance, qui établit une connexion à distance avec le serveur de commande et de contrôle ou le botnet.
4. **Phase 4 – Mouvement latéral :** cette étape de l'attaque réseau intervient lorsqu'une connexion solide avec le serveur de commande et de contrôle est déjà établie depuis un certain temps sans être remarquée. Le serveur de commande et de contrôle donne des ordres sous la forme de codes cachés pour se propager latéralement sur plusieurs appareils du même réseau.
5. **Phase 5 – Atteinte de l'objectif :** lorsque le logiciel malveillant a établi une connexion latérale avec plusieurs dispositifs du réseau, il transporte plusieurs commandes d'autorisation non sollicitée, d'élévation de privilèges et de compromission de comptes.
6. **Phase 6 – Exfiltration, corruption et perturbation :** dans cette dernière phase de l'attaque, les autorisations escaladées sont utilisées pour transférer des données hors du réseau, ce que l'on appelle également l'ex-filtration. Ils volent les données sensibles de l'organisation et corrompent les ressources critiques.

   Souvent, la perturbation peut également inclure la suppression de fichiers systèmes.

La Figure *(cf. p.11)* montre la façon la plus courante dont une intrusion dans un réseau se propage au sein d'une organisation :



Propagation d'une intrusions dans un réseau.

Détection d'intrusion

Intrusion ***Définition***

Le terme "*intrusion*" désigne l'accès d'un utilisateur non autorisé au système informatique, qui a réussi à en prendre le contrôle et qui tente de mener des activités inappropriées, incorrectes ou anormales visant à compromettre le système. En termes simples, une intrusion fait référence à un événement anormal résultant d'une attaque qui a réussi à exploiter une vulnérabilité.

Une intrusion signifie aussi les tentatives des employés ou administrateurs d'utiliser de plus hauts privilèges que ce qui leur a été attribués.

Détection d'intrusion ***Définition***

La *détection d'intrusion* désigne tout type de mécanisme permettant de détecter un comportement intrusif. Le principe de base de la détection des intrusions repose sur l'hypothèse que les activités intrusives sont sensiblement différentes des activités normales et sont donc détectables.

Complément

La notion de détection d'intrusion est née lorsque Anderson a publié un article intitulé "*Computer Security Threat Monitoring and Surveillance*", au début de l'année

1980. Dans cet article fondateur, rédigé pour une organisation gouvernementale, Anderson proposait d'utiliser des *pistes d'audit*[1] pour suivre les utilisations abusives des ordinateurs et comprendre le comportement des utilisateurs. Avec la publication de cet article, le concept de détection des abus et des activités des utilisateurs a émergé. Depuis lors, de nombreuses recherches qui ont été menées sur la détection d'intrusion et les *systèmes de détection des intrusions* ont été considérablement améliorés.

[1] Une piste d'audit consiste à mettre en place des contrôles permanents, étape par étape, qui établissent un enregistrement séquentiel détaillant l'historique et les événements liés à une tâche.

Systèmes de détection d'intrusion

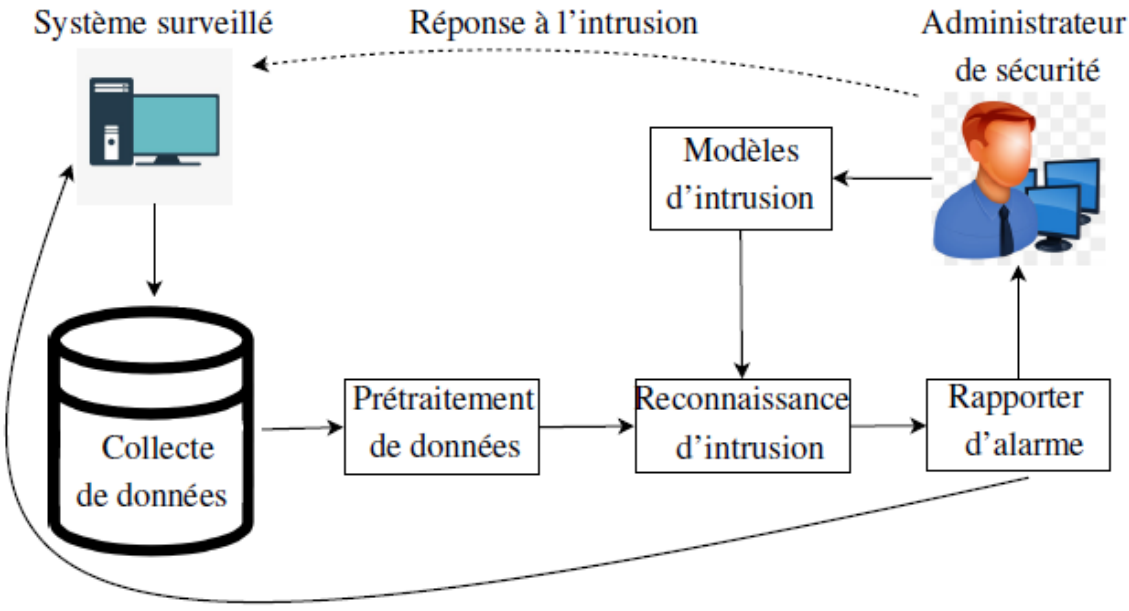
1. Définition

Les *Systèmes de Détection d'Intrusion* (IDS pour Intrusion Detection System) sont des composants importants de l'infrastructure de sécurité des réseaux, qui se positionnent au sein d'un système Informatique. Ils examinent l'activité du système ou du réseau pour détecter d'éventuelles intrusions et déclenchent des alertes de sécurité en cas d'activités malveillantes. les IDS surveillent l'ensemble ou une partie des réseaux, et visent un taux élevé de détection des attaques et un faible taux de fausses alarmes.

Un IDS est basé sur trois aspects fonctionnels, à savoir :

1. Un moteur d'analyse qui trouve des signes d'intrusion ;
2. Une source d'information qui fournit un flux d'enregistrements d'événements ;
3. Un composant de réponse qui génère des réactions basées sur les résultats du moteur d'analyse.

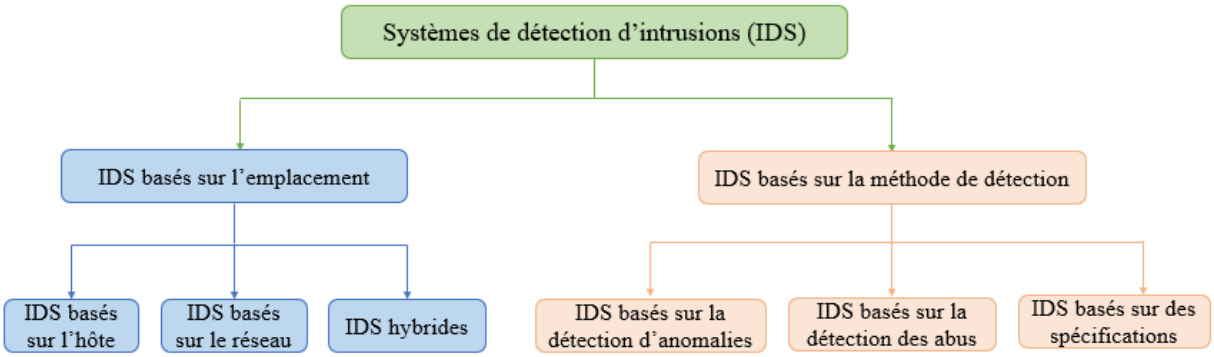
La Figure *(cf. p.13)* représente le processus de détection d'intrusion. Pour identifier une intrusion, un IDS effectue les tâches suivantes : (a) collecte des données, (b) prétraitement des données, (c) reconnaissance de l'intrusion, et (d) mise en œuvre de mesures correctives. Les données sont collectées à partir d'une ou plusieurs sources de données, y compris les pistes d'audit, le trafic réseau, la trace des appels système, etc. Un prétraitement est effectué sur les données collectées et seront transférées dans un format compréhensible par le composant de détection. Ce dernier est utilisé pour caractériser le comportement intrusif en utilisant plusieurs techniques et algorithmes. Enfin, le composant de réponse signale l'intrusion et éventuellement les informations temporelles correspondantes.



Processus de détection d'intrusions.

2. Classification

Les IDS peuvent être classés en fonction de l'emplacement de déploiement et de la méthode de détection (cf., Figure *(cf. p.14) (cf. p.14)*). En fonction de l'emplacement du module IDS dans le réseau, nous pouvons distinguer les IDS en trois classes : les IDS basés sur l'hôte, les IDS basés sur le réseau, et les IDS hybrides. En fonction de la méthode de détection, les IDS sont classés en trois grandes catégories : les IDS basés sur la détection des abus, les IDS basés la détection d'anomalie, et les IDS basés des spécifications.



Classification des IDS.

2.1. Approches d'analyse

Dans le domaine de la détection d'intrusions dans les réseaux en particulier, les IDS sont basés sur nombreuses méthodes d'analyse des attaques. Ces méthodes sont classées en trois catégories : la détection d'utilisation abusive, la détection d'anomalie et la détection basée sur des spécifications. Les IDS basés sur la détection des utilisations abusives (connu sous le nom de IDS basé sur la signature) visent à encoder, sous forme de signatures spécifiques, des connaissances sur les schémas du flux de données qui sont connus pour correspondre à des procédures intrusives. En revanche, les IDS basés sur la détection d'anomalie sont dédiés à l'établissement d'un modèle du flux de données qui est surveillé dans des conditions normales sans la présence de procédures intrusives. Dans les IDS basés sur des spécifications, les experts en sécurité prédéfinissent les comportements autorisés du système et les événements qui ne correspondent pas aux spécifications sont étiquetés comme des attaques.

Dans ce qui suit, nous discutons en détail de ces différentes approches et soulignons les points forts et les limites de chaque catégorie.

1. **Détection des abus :** les intrusions sont détectées en partant de l'analyse des attaques déjà connues, en construisant une base de connaissances des signatures des attaques qui ont été détectées précédemment. Par conséquent, les intrusions sont connues à priori et facilement identifiées avec un taux d'échec minimal.

   Cette base est combinée à un système d'alerte à lancer dès qu'une correspondance avec les signatures archivées est détectée dans le trafic du réseau. Cette approche convient à la détection des attaques connues, mais elle est inutile lorsqu'on est confronté à des formes d'attaques inconnues ou nouvelles. Ainsi, la mise à jour régulière de la base de connaissances des signatures pourrait être la solution, mais elle est laborieuse et coûteuse en temps.

   - **Avantages de détection des abus**
     - Les IDS basées sur détection des abus peuvent détecter les intrusions avec un certain degré de certitude. Les détecteurs de mauvaise utilisation sont très efficaces pour détecter les attaques sans donner un taux élevé de fausses alarmes.
     - Ils peuvent détecter toutes les intrusions dont les signatures sont connues.
     - Ils sont faciles à mettre en oeuvre (machine d'état, analyse de signature) et à déployer (pas besoin de former un profil du système).

- **Limites de détection des abus**
  - La capacité de détection des détecteurs est limitée aux signatures qu'ils possèdent. Une nouvelle intrusion ou même une variation d'une intrusion connue peut ne pas être détectée. la méthode de détection des abus nécessite donc des mises à jour régulières des signatures afin de rester à jour.
  - Le processus de développement d'une nouvelle signature d'attaque prend du temps.

2. **Détection basée sur des spécifications :** les IDS basés sur les spécifications ne sont ni basés sur les abus, ni basés sur les anomalies, car ils utilisent les spécifications comportementales du système pour détecter les attaques et partent du principe que toute exécution correcte du système doit se conformer à la spécification de son comportement prévu. Au lieu d'apprendre les comportements du système, dans les systèmes basés sur les spécifications, les connaissances des experts déterminent les limites de fonctionnement (seuil) d'un système. Une fois que le comportement correct (ou autorisé) du système est spécifié, les événements qui s'écartent de la spécification génèrent une alerte. En théorie, cette approche permet de détecter des attaques invisibles qui pourraient être exploitées à l'avenir. Cependant, la spécification du comportement d'un grand nombre de programmes privilégiés s'exécutant dans des environnements d'exploitation réels est une tâche ardue et difficile. La validation rigoureuse des spécifications d'un si grand nombre de programmes reste un problème ouvert. Par conséquent, malgré ses principes séduisants, la détection basée sur les spécifications n'en est encore qu'à ses débuts.
   - **Avantages de détection des spécifications**
     - Ils sont utiles pour détecter les attaques sans un taux élevé de fausses alarmes.
     - Ils permettent de détecter des attaques invisibles qui pourraient être exploitées à l'avenir.
   - **Limites de détection des spécifications**
     - La spécification du comportement d'un grand nombre de programmes privilégiés s'exécutant dans des environnements d'exploitation réels est une tâche ardue et difficile.
     - La spécification des règles est limitée aux connaissances des experts.
3. **Détection d'anomalie :** différente de la détection d'abus, la détection des anomalies est dédiée à l'établissement de profils d'activité normale pour le système. Elle repose sur l'identification du comportement du trafic réseau qui peut être défini comme normal, afin de détecter les différences de comportement qui s'écartent de la normalité comme des anomalies. Cette approche permet donc de détecter les nouveaux types d'attaques en analysant les caractéristiques du trafic réseau ; en tant que telle, elle répond à la plus grande limite de la détection des utilisations abusives.
   - **Avantages de détection d'anomalie**
     - Comme toute déviation significative par rapport au profil normal sera signalée comme anormale, les détecteurs d'anomalies peuvent détecter des attaques inconnues.
     - Les détecteurs d'anomalie ne nécessitent pas une mise à jour constante des règles ou des signatures des nouvelles intrusions.
     - Les détecteurs d'anomalie peuvent produire des informations qui peuvent à leur tour être utilisées pour définir des signatures pour les détecteurs des abus.

- **Limites de détection d'anomalie**
  - Le taux élevé de faux positifs est le principal inconvénient des IDS basés sur la détection d'anomalie. Cela est dû au fait que le profil normal d'un système ne peut pas être entièrement appris et/ou que le comportement des utilisateurs ou des programmes peut changer avec le temps.
  - Afin de construire le profil normal d'un système, le système en question doit être surveillé et des informations doivent être collectées, qui à leur tour seront utilisées pour déterminer le comportement normal du système. Mais si les informations collectées contiennent des attaques, le comportement intrusif fera partie du profil normal, et à l'avenir ces attaques ne seront pas détectées.
  - Les approches de détection d'anomalies nécessitent des jeux de données étendus pour établir le profil du système.

Le tableau *(cf. p.16)* illustre une comparaison des types d'IDS en fonction de la méthodologie de détection.

	IDS basé sur les abus	IDS basé sur les anomalies	IDS basé sur les spécifications
Méthode	Identifier les attaques dont les signatures sont déjà établies	Identifier les d'activité inhabituels	Identifier la violation des règles prédéfinies
Taux de détection	Faible	Élevé	Élevé
Taux de fausse alarmes	faible	Élevé	Faible
Détection des attaques inconnus	Incapable	Capable	Incapable
Avantage	Capable de détecter toutes les intrusions dont les signatures sont connues	Capables d'identifier des intrusions inconnues	Il détecte les attaques sans un taux élevé de fausses alarmes
Inconvénient	La mise à jour des signatures est laborieuse et coûteuse	Nécessité des jeux de données étendus pour établir le profil du système.	S'appuyer sur les connaissances des experts pour définir les règles

Comparaison des types d'IDS en fonction de la méthodologie de détection

Remarque

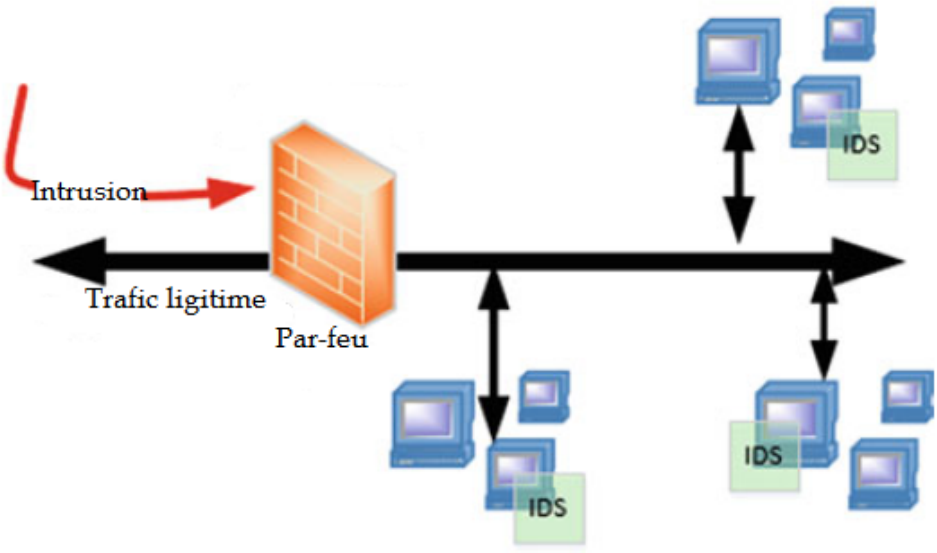
L'importance de la détection des anomalies ne se limite pas au contexte de la sécurité. Dans un schéma plus général, la détection d'anomalies concerne toute méthode permettant de trouver des événements qui ne sont pas conformes à une attente. Dans les cas où la fiabilité du système est d'une importance critique, vous pouvez utiliser la détection d'anomalie pour identifier les premiers signes de défaillance du système, et déclencher le lancement d'enquêtes précoces ou préventives. Une autre application importante de la détection d'anomalie est le domaine des fraudes. Une fraude dans le secteur financier peut souvent être pêchée au milieu d'un vaste bassin de transactions légitimes en étudiant les tendances des événements "normaux" et en détectant les écarts par rapport à cette normale.

2.2. Sources d'information

La collecte de données est l'une des étapes les plus importantes de la conception d'IDS. Elle influence l'ensemble du processus de conception et de mise en œuvre, ainsi que le résultat final de la détection. En général, les attaques ne visent pas seulement un ordinateur individuel mais aussi un groupe d'ordinateurs. Par conséquent, certaines intrusions peuvent présenter un comportement anormal au niveau du réseau, tandis que d'autres peuvent présenter des comportements anormaux au niveau de l'hôte. Afin de couvrir les différentes intrusions, nous devons surveiller chaque endroit. Les

informations d'entrée peuvent être des journaux d'audit, des appels système ou des paquets réseau. Par conséquent, en fonction de cet aspect et du positionnement du module IDS, nous pouvons distinguer trois classes d'IDS : les IDS basés sur l'hôte, les IDS basés sur le réseau et les IDS hybrides.

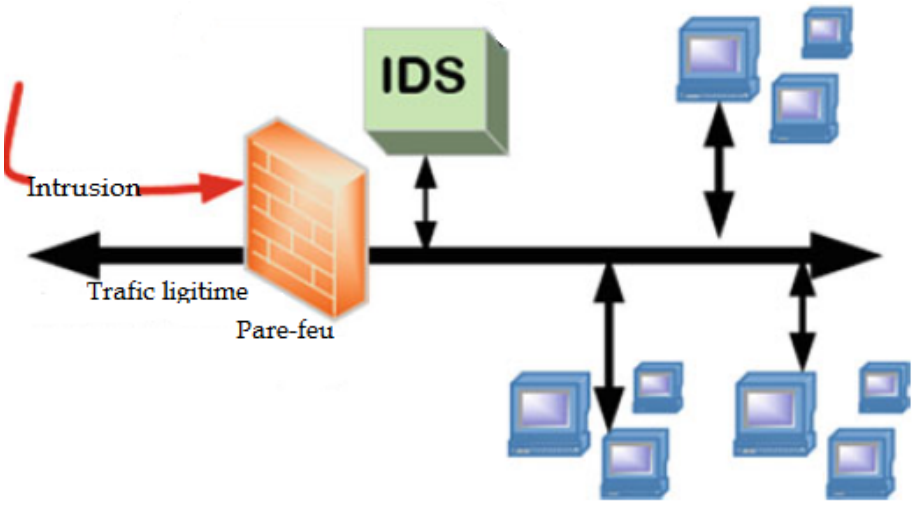
1. **IDS basés sur l'hôte :** les systèmes de détection d'intrusion basés sur l'hôte (HIDS) analysent les activités sur un hôte protégé en surveillant différentes sources de données qui résident sur cet hôte, comme un fichier journal, les appels système, les accès aux fichiers ou le contenu de la mémoire. Un HIDS est généralement un logiciel s'exécutant sur l'hôte protégé, et donc, la protection d'un HIDS est limitée à une seule machine. Par conséquent, pour protéger l'ensemble du réseau, un HIDS doit être installé sur chaque machine du réseau interne, comme illustré sur la Figure 1.4. Il existe deux sources de données principales qui peuvent être utilisées pour la détection basée sur l'hôte, à savoir les journaux d'audit et les appels système. Les journaux d'audit représentent un ensemble d'événements créés par le système d'exploitation pour effectuer certaines tâches, et les appels système représentent le comportement de chaque application critique pour l'utilisateur exécutée sur le système d'exploitation.
    - **Avantages des IDS basés sur l'hôte**
        - Comme les HIDS surveillent les activités locales, ils peuvent détecter attaques qui ne peuvent pas être détectées par les IDS basés sur le réseau.
        - Les sources d'information des IDS basés sur l'hôte sont généralement générées sur des données en clair, ils peuvent donc fonctionner avec succès dans un environnement où le trafic réseau est crypté.
        - Les performances des HIDS ne sont pas affectées par la topologie du réseau dans lequel ils fonctionnent.
    - **Inconvénients des IDS basés sur l'hôte**
        - Un HIDS n'est pas bon pour la surveillance qui s'adresse au réseau entier, parce que le HIDS ne voit que les paquets du réseau reçus sur l'host.
        - Comme les HIDS ne peuvent voir que les paquets réseau reçus par leur hôte, les performances de détection des HIDS sont faibles dans le cas où les attaques visent l'ensemble du réseau.
        - La quantité d'informations utilisées par les IDS basés sur l'hôte peut être énorme ; par conséquent, ils peuvent nécessiter un stockage supplémentaire sur le système en cours d'exécution.
        - Les HIDS partagent les ressources informatiques (par exemple, l'unité centrale, la mémoire principale) avec l'hôte surveillé. Par conséquent, ils peuvent affecter les performances de l'ordinateur.



IDS basé sur l'hôte.

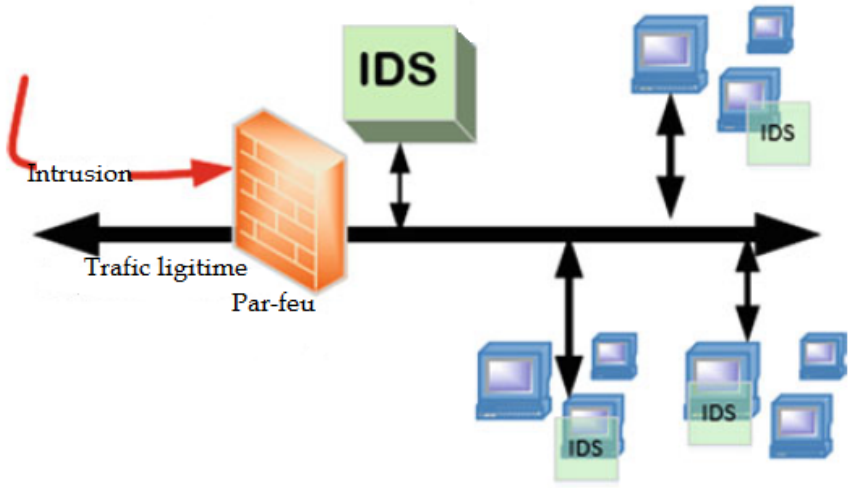
2. **IDS basés sur le réseau :** lorsque les environnements informatiques sont passés des ordinateurs centraux aux réseaux de stations de travail, les études sur la détection des intrusions ont commencé à se concentrer sur les attaques visant le réseau. Les attaques réseau ne peuvent pas être détectées en examinant les traces du système d'exploitation. Par conséquent, des IDS basés sur le réseau ont été développés, qui place le module IDS à l'intérieur du réseau où il peut être surveillé dans son ensemble. Les systèmes de détection d'intrusion basés sur le réseau (NIDS) collectent et analysent les données capturées directement à partir du réseau. Ils fonctionnent généralement en capturant et en examinant les types et le contenu des paquets ou des flux lorsqu'ils traversent le réseau pour identifier les schémas d'attaque possibles. La Figure 1.5 montre un IDS basé sur le réseau.

- **Avantages des IDS basés sur le réseau**
  - Il est possible de surveiller facilement un grand réseau en utilisant un petit nombre de capteurs, si ceux-ci sont placés aux endroits critiques du réseau (par exemple, aux concentrateurs, aux routeurs ou aux sondes).
  - Les NIDS sont généralement des dispositifs passifs qui fonctionnent en mode discret et n'affectent donc pas le fonctionnement normal du réseau.
  - Les capteurs placés sur le réseau sont placés en mode furtif (ou stealth mode), de façon à être invisibles aux autres machines. Du fait de leur invisibilité sur le réseau, il est beaucoup plus difficile de les attaquer et de savoir qu'un NIDS est utilisé.
- **Inconvénients des IDS basés sur le réseau**
  - Si le réseau surveillé est vaste ou si le trafic réseau est élevé, il peut être difficile de traiter tous les paquets réseau.
  - Des problèmes surviennent lorsque les NIDS sont placés sur un réseau commuté. La plupart des commutateurs ne fournissent pas de ports de surveillance universels, ce qui limite la capacité de surveillance des des NIDS.
  - Les IDS basés sur le réseau ne peuvent pas analyser le trafic crypté. Cela est dû au fait que les capteurs analysent les en-têtes des paquets pour déterminer les adresses de source et de destination et le type de données transmises, et analysent la charge utile des paquets pour découvrir des informations dans les données transmises.
  - Les paquets réseau mal-formés peuvent provoquer la panne d'un IDS basé sur le réseau.



IDS basé sur le réseau.

3. **IDS hybrides :** ces deux types d'IDS présentent des inconvénients spécifiques : l'IDS basé sur le réseau risque d'alourdir la charge de travail et de passer à côté de certaines activités malveillantes, tandis que l'IDS basé sur l'hôte ne surveille pas tous les trafics réseau et a une charge de travail moindre que l'IDS basé sur le réseau. Par conséquent, l'IDS hybride, comme le montre la Figure 1.6, est placé dans le réseau ainsi que sur les hôtes afin de surveiller simultanément les activités des clients spécifiques et du réseau.



IDS hybride.

Types d'architecture de NIDS ***Complément***

Dans cette partie, nous allons voir les différents emplacements qu'un NIDS peut prendre au sein d'un réseau. C'est une étape importante car toute erreur d'installation pourrait rendre votre système de détection/prévention inefficace. L'installation consiste à non seulement correctement déployer votre IDS mais aussi savoir le configurer.

1. **IDS entre le pare-feu et le réseau externe :** Dans cette architecture, le NIDS est placé avant le pare-feu, ce qui signifie que le NIDS recevra tout le trafic entre le réseau externe et le réseau interne et va pouvoir réceptionner tout types d'attaques provenant du réseau public. Les inconvénients avec cette architecture sont:
    - Exposer le NIDS à des attaques externes.
    - Les attaques internes ne sont pas détectées.
    - Beaucoup d'alerte vu que tout le trafic passe par le NIDS.
2. **NIDS entre le pare-feu et le réseau interne :** Dans cette architecture, le NIDS est placé après le pare-feu, ce qui signifie que le NIDS recevra et analysera uniquement les flux acceptés par le pare-feu. Cette architecture permet de réduire fortement la charge du NIDS et de détecter les attaques internes. Outre, le NIDS/NIPS n'est pas exposé à l'externe ce qu'il le rend moins vulnérable. Il est souvent préférable d'utiliser cette architecture plutôt que la première.
3. **NIDS dans la zone démilitarisée (DMZ) :** Dans cette architecture, le NIDS est placé au niveau de la zone démilitarisée (DMZ). Le trafic entre le réseau externe et le réseau DMZ est analysé par le NIDS. Ce type d'architecture permet d'identifier les attaques qui ciblent les serveurs publics (messagerie, FTP, Web, etc.).

Remarque

A noter que:

- Un NIDS seul avec une seule architecture n'est pas suffisant pour assurer un bon niveau de sécurité.
- Les différentes architectures peuvent être combinées au sein d'un même réseau.
- Une configuration correcte est nécessaire pour assurer le bon fonctionnement de votre système NIDS/NIPS. Par exemple: des règles destinées à un réseau Windows peuvent ne pas fonctionner pour un réseau Unix.
- D'autres technologies sont à ajouter dans votre réseau d'entreprise afin d'accroître la sécurité. Par exemple: les pare-feux, Les AV, les HIDS, etc.

2.3. Réponse à l'intrusion

Une autre façon de classer les IDS est de les classer en fonction de leur mécanisme de réponse.

- *Les IDS passifs* fonctionnent généralement hors ligne pour analyser les fichiers journaux du système et les traces du trafic réseau. Dans certains cas, ils fonctionnent également en ligne pour surveiller passivement les données d'audit des hôtes et le trafic réseau. Les IDS passifs signalent les alarmes d'intrusion à l'administrateur du système/réseau après avoir détecté d'éventuelles attaques qui prend les mesures nécessaires en fonction de ces informations.
- En revanche, les IDS sont dites *actifs* s'il réagit activement à l'attaque en prenant des mesures pour stopper une attaque au moment de sa détection sans attendre l'intervention humaine . Pour cela, deux techniques sont utilisées : la reconfiguration du firewall et l'interruption d'une connexion, ce qui permet de bloquer le trafic malveillant au niveau du firewall, en fermant le port utilisé ou en interdisant l'adresse de l'attaquant ; un IDS peut également interrompre une session établie entre un attaquant et sa machine cible, de façon à empêcher le transfert de données ou la modification du système attaqué.

2.4. Avantages d'IDS

- Fournir des informations sur les intrusions et les tentatives qui ont eu place ;
- Agir et contrôler la qualité de la sécurité et l'administration, en particulier dans les grandes entreprises ;
- Détecter les attaques et les violations de sécurité qui ne sont pas prévus par d'autres mesures de sécurité ;
- Il peut prendre des réponses actives, comme le blocage des adresses IP, l'arrêt des connexions ;
- Plus important encore, IDS fournit des lignes directrices qui aident dans le développement de la politique de sécurité de l'organisation.

2.5. Limites d'IDS

- Il ne peut pas résister à des volumes élevés et des vitesses élevées de trafic Internet.
- Il ne peut pas protéger contre tous les types d'attaques: ils sont incapables de détecter certains types d'attaques, ils sont eux-mêmes attaquables.
- Il n'est pas automatisé, il a besoin d'importantes ressources humaines pour leur gestion.
- Les systèmes de détection d'intrusions génèrent trop de faux positifs.

3. Similitudes et différences entre IDS et IPS

1. **Les similitudes entre IDS/IPS :** ci-après leurs points communs :
    - **Surveiller :** une fois installées, les solutions IDS et IPS (Intrusion Prevention System) surveillent un réseau ou un système en fonction des paramètres spécifiés. Vous pouvez définir ces paramètres en fonction de vos besoins de sécurité et de votre infrastructure réseau et les laisser inspecter tout le trafic entrant et sortant de votre réseau.
    - **Détection des menaces :** les deux lisent tous les paquets de données circulant dans votre réseau et comparent ces paquets à une bibliothèque contenant des menaces connues. Lorsqu'ils trouvent une correspondance, ils signalent ce paquet de données comme malveillant.
    - **Apprendre :** ces deux technologies utilisent des technologies modernes telles que l'apprentissage automatique pour s'entraîner pendant une période et comprendre les menaces et les modèles d'attaque émergents. De cette façon, ils peuvent mieux répondre aux menaces modernes.

- **Journal :** lorsqu'ils détectent une activité suspecte, ils l'enregistrent avec la réponse. Il vous aide à comprendre votre mécanisme de protection, à détecter les vulnérabilités de votre système et à former vos systèmes de sécurité en conséquence.
- **Alerte :** dès qu'ils détectent une menace, l'IDS et l'IPS envoient des alertes au personnel de sécurité. Cela les aide à se préparer à toutes les circonstances et à prendre des mesures rapides.

2. **Les différences entre IDS/IPS :** la différence principale entre l'IDS et l'IPS est que l'IDS fonctionne comme un système de surveillance et de détection tandis que l'IPS fonctionne comme un système de prévention en dehors de la surveillance et de la détection. Certaines différences sont :
   - **Réponse :** les solutions IDS sont des systèmes de sécurité passifs qui surveillent et détectent uniquement les réseaux pour les activités malveillantes. Ils peuvent vous alerter mais ne prennent aucune mesure par eux-mêmes pour empêcher l'attaque. L'administrateur du réseau ou le personnel de sécurité affecté doit prendre des mesures immédiatement pour atténuer l'attaque. D'autre part, les solutions IPS sont des systèmes de sécurité actifs qui surveillent et détectent votre réseau pour les activités malveillantes, alertent et empêchent automatiquement l'attaque de se produire.
   - **Protection :** si vous êtes menacé, l'IDS pourrait être moins utile car votre personnel de sécurité doit trouver comment sécuriser votre réseau et nettoyer le système ou le réseau immédiatement. l'IPS peut effectuer une prévention automatique par lui-même.
   - **Faux positifs :** si l'IDS donne un faux positif, vous pouvez trouver une certaine commodité. Mais si l'IPS le fait, l'ensemble du réseau en souffrira car vous devrez bloquer tout le trafic entrant et sortant du réseau.
   - **Les performances du réseau :** comme l'IDS n'est pas déployé en ligne, il ne réduit pas les performances du réseau. Cependant, les performances du réseau peuvent être réduites en raison du traitement IPS, qui est en phase avec le trafic.

4. Critères d'évaluation

Dans cette section, nous présentons les critères les plus importants qui ont été utilisés pour une évaluation plus réaliste des systèmes de détection d'intrusion.

4.1. Erreurs de classification

Lorsqu'un IDS effectue une classification des données, sa décision peut être soit vraie, soit fausse. Il existe plusieurs types d'erreurs venant d'un détecteur, influençant plus ou moins sa puissance.

- **Vrais positifs (True Positive (TP)) :** se produient lorsqu'un IDS classifie correctement une intrusion.
- **Vrais négatifs (True Negative (TN)) :** se produisent lorsqu'un événement normal est correctement classé comme une action légitime.
- **Faux positifs (False Positive (FP)) :** se produisent lorsque le système reconnaît à tort que des actions légitimes sont une intrusion.
- **Faux négatifs (False Negative (FN)) :** se produisent lorsque un IDS classifie à tort des intrusions comme des actions légitimes.

	Événement actuel	Prédiction d'IDS
Vrais positifs (TP)	Intrusion	Intrusion
Faux positifs (FP)	Ligitime	Intrusion
Vrais négatifs (TN)	Ligitime	Ligitime
Faux négatifs (FN)	Intrusion	Ligitime

Types d'erreurs provenant d'un IDS.

Par conséquent, l'objectif d'un IDS est de produire autant de TP et TN que possible, tout en essayant de réduire le nombre de FP et FN.

a) Matrice de confusion

La matrice de confusion est une méthode de classement appliquée à tout type de problème de classification. La taille de la matrice est déterminée par le nombre de classes distinctes qui doivent être détectées. L'objectif ici est de comparer les étiquettes réelles des événements aux étiquettes prédites. Par conséquent, la diagonale représentera toutes les classifications correctes. Le tableau *(cf. p.22)* illustre la représentation dans la matrice de confusion.

		Résultat de prédiction	
		Ligitime	Intrusion
Evénement actuel	Ligitime	TN	FP
	Intrusion	FN	TP

La matrice de confusion.

La grande majorité des critères d'évaluation utilise les quatre variables précédentes (TP, FP, TN, FN) et les relations entre elles pour analyser l'efficacité des IDS.

4.2. Exactitude

L'exactitude (Accuracy) est une déclaration de l'exactitude du fonctionnement d'un IDS, mesurant le pourcentage de détection et d'échec ainsi que le nombre de fausses alarmes que le système produit. Un système qui a une accuracy de 80% est un système qui classe correctement 80 instances sur 100 dans leur classe réelle. L'exactitude est calculée comme suit :

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} * 100$$

4.3. Précision

Précision (Precision) s'agit d'une métrique indiquant combien d'événements, quin sont prédits par un IDS comme étant intrusifs, sont des intrusions réelles. L'objectif d'un IDS est d'obtenir une précision élevée, ce qui signifie que le nombre de fausses alarmes est minimisé. La précision est calculée comme suit :

$$Precesion = \frac{TP}{TP + FP} * 100$$

4.4. Rappel

Rappel (Recall) mesure la partie manquante de la précision, c'est-à-dire là partir de toutes les événements normaux, combien sont correctement classées par le système. Par conséquent, il est souhaitable qu'un système ait une valeur de rappel élevée. Le rappel est calculé comme suit :

$$Recall = \frac{TP}{TP + FN} * 100$$

4.5. F1 score

Étant donné que les deux métriques discutées précédemment (c'est-à-dire la précision et le rappel) ne définissent pas complètement l'exactitude d'un IDS, il serait plus approprié d'utiliser une combinaison de celles-ci. Le F1 score est calculé comme suit :

$$F1 - score = \frac{Precision * Recall}{Precision + Reccal} * 2$$

5. Exemples d'IDS

Dans cette section, nous décrivons quelques exemples d'IDS existants, à savoir Bro, Prelude, Snort, OSSEC et Multi Router Traffic Grapher (MRTG). Nous résumons brièvement ces produits en termes de leurs sources d'information, de leur approche de détection, et de leur type de réponse.

IDS	Caractéristiques
Bro	– Rebaptisé Zeek fin 2018 et est parfois appelé Bro-IDS ou maintenant Zeek-IDS, il s'agit d'un système de détection des intrusions dans le **réseau** fonctionnant sur Unix. – Bro mélange des signatures d'attaques connues et des comportements normaux pour détecter une intrusion. – Il entre donc dans la catégorie des NIDS basés sur des signatures et les anomalies.
Prelude	– Prelude est un système hybride de détection d'intrusion, principalement développé sous Linux. – Il analyse les activités de l'utilisateur, du système et du réseau, il cible les intrusions basées sur **l'hôte** et **le réseau**. – Les capteurs envoient des messages à une unité centrale (le gestionnaire) qui les traites et est responsable de l'enregistrement des événements. Outre le gestionnaire, Prelude comprend également un module responsable du retour d'information graphique à l'utilisateur.
Snort	– Snort est un système de détection des intrusions capable de collecter les paquets, d'analyser le trafic et de détecter les intrusions à l'aide de signatures. – Outre l'analyse des protocoles, Snort effectue diverses correspondances de contenu sur les paquets réseau à la recherche de modèles d'attaques connues. – Snort fonctionne sur une variété de plateformes : Linux, MacOS, Win32, etc.
OSSEC	– Il s'agit d'un système de détection des intrusions dans **l'hôte**. – OSSEC fonctionne sur presque tous les principaux systèmes d'exploitation (tels que Windows, Linux et MacOs.) – Snort comprend une architecture de gestion basée sur le client/serveur, ce qui est très important dans un système HIDS. Il transmette les informations de sécurité à un serveur centralisé où l'analyse et la notification peuvent avoir lieu même si le système hôte est mis hors ligne ou compromis.
MRTG	– Multi Router Traffic Grapher (MRTG) est un IDS pour surveiller le trafic réseau. Il génère des pages HTML contenant des images graphiques au format PNG. – Sa principale application est de fournir une représentation visuelle en direct du trafic sur les liens du réseau. MRTG crée les représentations visuelles du trafic vu pendant les dernières 24 heures, les sept derniers jours, les cinq dernières semaines, et les douze derniers mois. – MRTG a été utilisé pour surveiller des variables telles que les sessions de connexion, la disponibilité du modem, etc.

58

Exemples d'IDS.

5.1. SNORT

A l'origine SNORT était simplement un outil de capture réseau. Actuellement, c'est aussi un système de détection/prévention d'intrusion réseau (NIDS/NIPS) open source, son code source est accessible et modifiable sur le site: "http://www.snort.org".

Il est très populaire et très utilisé au sein des entreprises vu sa capacité d'effectuer l'analyse du trafic réseau en temps réel.

Ce dernier a prouvé son efficacité en détectant plusieurs types d'attaques (tentative de fingerprinting, la vulnérabilité log4shell, l'attaque buffer overflow, botnets, l'utilisation du P2P, etc.) SNORT a trois mode de fonctionnement:

- **Le mode sniffer (reniflage de paquets) :** dans ce mode, SNORT lit les paquets transitant le réseau et les affiche d'une façon continue sur l'écran.
- **Le mode « packet logger » :** dans ce mode SNORT journalise (log) le trafic réseau dans des répertoires sur le disque.
- **Le mode détection/prévention d'intrusion réseau (NIDS/NIPS) :** dans ce mode, SNORT analyse le trafic du réseau, et le traite. Ce qui signifie qu'il le compare à des règles prédéfinies par l'administrateur réseau ou l'équipe de sécurité et établit des actions à exécuter (exemple: accepter le trafic, alerter, bloquer le trafic, journaliser, etc.).

a) Architecture de SNORT

L'architecture de SNORT est composée de :

- **Un noyau de base :** au démarrage, ce noyau charge un ensemble de règles, les compile, les optimise et les classe. Durant l'exécution, le rôle principal du noyau est la capture de paquets.
- **Une série de pré-processeurs :** se charge d'analyser et de recomposer le trafic capturé. Ils reçoivent les paquets directement capturées, éventuellement les retravaillent puis les fournissent au moteur de recherche de signatures.
- **Analyse** : Une série d'analyses est ensuite appliquée aux paquets. Ces analyses se composent principalement de comparaisons de différents champs des headers des protocoles (IP, ICMP, TCP et UDP) par rapport à des valeurs précises.
- **Après la détection** d'intrusion, une série de « output plugins » permet de traiter cette intrusion de plusieurs manières : envoie vers un fichier log, envoie d'un message d'alerte, stocker cette intrusion dans une base de données.

b) Les règles SNORT

Syntaxe d'une règle SNORT

Action protocole IP-source port-source -> IP-destination port-destination (flags :"TCP-flag" ; content : "trafic contient"; msg: "votre-message"; sid: >1000000; rev: 1; classtype: "protocole-event")

Les règles de SNORT sont composées de deux parties distinctes : le header et les options.

1. **Le header :** permet de spécifier le type d'alerte à générer (alert, log et pass) et d'indiquer les champs de base nécessaires au filtrage : le protocole ainsi que les adresses IP et ports sources et destinations.

   Les règles headers :

   - **Action :** action de la règle. exemple action = alert signifie que Snort va générer une alerte quand l'ensemble des conditions est rempli.
   - **Protocole :** protocole de la couche transport (TCP/UDP) utilisé ou de la couche réseau (ICMP).
   - **IP-source :** La source du trafic.
   - **port-source :** le port source du trafic.
   - **-> :** La Direction du trafic (de la source vers la destination).
   - **IP-destination :** La destination du trafic.
   - **port-destination :** le port destination du trafic.
2. **Les options :** spécifiées entre parenthèses, permettent d'affiner l'analyse, en décomposant la signature en différentes valeurs à observer parmi certains champs du header ou parmi les données. Nous avons plusieurs options, nous citons:
   - **flags** : flag du header TCP est activé.
   - **content** : le trafic contient la chaine de caractère "trafic contient".
   - **msg** : Snort va affichier le message "votre-message" quand il envoie l'alerte.
   - **sid:1000001** : Snort rule ID (identifiant de la règle snort). Pour information, les identifiants inférieurs ou égal à 1,000,000 sont réservés. Raison à laquelle nous commençons par 1000001 (vous pouvez utiliser n'importe quel numéro tant que c'est supérieur à 1000000).
   - **rev:1** : Revision number (numéro de révision). cette option permet une maintenance simplifiée de règle.

- **classtype** : Permet de catégoriser la règle comme par exemple “icmp-event” (l'une des catégories snort prédéfinie). Permet aussi l'organisation des règles.
- etc.

Exemple de règles ***Exemple***

- Alert tcp any any -> 192.168.0.0/16 80 (flags :A ; content : “passwd”; msg: “detection de ` passwd' “ ;)

Cette règle permet de générer un message d'alerte “detection de passwd” lorsque le trafic à destination d'une machine du réseau local 192.168.0.0/16 vers le port 80, contient la chaîne « passwd » (spécifié par l'utilisation du mot-clé « content »), et que le flag ACK du header TCP est activé (flags : A).

- Alert tcp any any -> any any (content: “www.youtube.com” ; msg: ''visite youtube actuellement''; sid:1000002;)

Cette règle permet de générer un message d'alerte ''visite youtube actuellement'' à chaque fois qu'un utilisateur visite youtube.

Exercices

1. Exercice

[solution n°1 p. 28]

Une souhaite se protéger contre les attaques de type smurf, vous lui proposez d'installer :

- O Un WAF (Web Application FW).
- O Un pare-feu de la couche réseau.
- O Un IDS/IPS
- O Un antivirus.

2. Exercice

[solution n°2 p. 28]

Trouvez les mots manquants.

les bots sont un dont l'objectif est de tenter de à un plus grand nombre possible d'hôtes d'un réseau, afin de mettre leur capacité de calcul au service de l'attaquant. Ils compromettent les hôtes, établit une communication avec et commence à exécuter des actions automatisées sous le contrôle de l'attaquant. À l'aide du malware bot, les attaquants rassemblent les appareils dans , un vaste réseau d'appareils compromis sous leur contrôle. Les botnets sont fréquemment utilisés dans les attaques .

3. Exercice

[solution n°3 p. 28]

Une entreprise souhaite installer un système permettant de détecter et de prévenir les attaques sur son réseau, vous lui proposez:

- O NIDS.
- O NIPS.
- O HIDS.
- O HIPS.

4. Exercice

[solution n°4 p. 28]

Un IDS vous permet de détecter les intrusions et les prévenir.

- O Vrai
- O Faux

5. Exercice

[solution n°5 p. 29]

A quoi correspond un "faux positif"

- ☐ Un message d'alerte qui ne devrait pas déclencher une alerte (émis à tort).
- ☐ Un message d'alerte qui devrait déclencher une alerte.
- ☐ Un message d'alerte pour un événement légitime.
- ☐ Aucune réponse n'est correcte.

6. Exercice

[solution n°6 p. 29]

MRTG OSSEC Bro Prelude Snort

NIDS	NIDS & HIDS	HIDS

7. Exercice

[solution n°7 p. 29]

Quelle est la différence entre un système de réponse active et un IPS ?

8. Exercice

[solution n°8 p. 29]

Quels sont les avantages d'un IDS qui inspecte les données au niveau de la couche Application ?

Solutions des exercices

Solution n°1

[exercice p. 26]

Une souhaite se protéger contre les attaques de type smurf, vous lui proposez d'installer :

- ○ Un WAF (Web Application FW).
- ◉ Un pare-feu de la couche réseau.
- ○ Un IDS/IPS
- ○ Un antivirus.

Solution n°2

[exercice p. 26]

Trouvez les mots manquants.

les bots sont un `malware` dont l'objectif est de tenter de `se propager` à un plus grand nombre possible d'hôtes d'un réseau, afin de mettre leur capacité de calcul au service de l'attaquant. Ils compromettent les hôtes, établit une communication avec `un serveur de commande et de contrôle` et commence à exécuter des actions automatisées sous le contrôle de l'attaquant. À l'aide du malware bot, les attaquants rassemblent les appareils dans `un botnet`, un vaste réseau d'appareils compromis sous leur contrôle. Les botnets sont fréquemment utilisés dans les attaques `DDoS`.

Solution n°3

[exercice p. 26]

Une entreprise souhaite installer un système permettant de détecter et de prévenir les attaques sur son réseau, vous lui proposez:

- ○ NIDS.
- ◉ NIPS.
- ○ HIDS.
- ○ HIPS.

Solution n°4

[exercice p. 26]

Un IDS vous permet de détecter les intrusions et les prévenir.

- ○ Vrai
- ◉ Faux

Solution n°5

[exercice p. 27]

A quoi correspond un "faux positif"

- ☑ Un message d'alerte qui ne devrait pas déclencher une alerte (émis à tort).
- ☐ Un message d'alerte qui devrait déclencher une alerte.
- ☑ Un message d'alerte pour un événement légitime.
- ☐ Aucune réponse n'est correcte.

Solution n°6

[exercice p. 27]

NIDS	NIDS & HIDS	HIDS
Snort	Prelude	OSSEC
Bro		
MRTG		

Solution n°7

[exercice p. 27]

Quelle est la différence entre un système de réponse active et un IPS ?

La principale différence est qu'un système de réponse active a souvent une architecture qui ne peut pas fondamentalement empêcher une attaque de compromettre un système, mais peut seulement atténuer les effets d'une attaque. Un IPS, en revanche, peut non seulement répondre à une attaque par des contre-mesures appropriées, mais aussi empêcher une attaque de compromettre un système grâce à son architecture. En termes de réponse active au réseau par rapport à la prévention des intrusions, l'IPS doit être en ligne avec le flux de paquets.

Solution n°8

[exercice p. 27]

Quels sont les avantages d'un IDS qui inspecte les données au niveau de la couche Application ?

1- Un IDS de couche Application peut avoir une meilleure compréhension du contexte dans lequel une communication se déroule. 2- Il peut inspecter le contenu chiffré. 3- Il permet une protection ciblée. etc.