

Systeme de détection d'intrusion

➤ Pour les articles homonymes, voir IDS.

Un **système de détection d'intrusion** (ou **IDS** : Intrusion detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance

sur les tentatives réussies comme échouées des intrusions.

Il existe deux grandes catégories d'IDS, les plus connues sont les détections par signatures (reconnaissance de programme malveillant) et les détections par anomalies (détecter les écarts par rapport à un modèle représentant les bons comportements, cela est souvent associé à de l'apprentissage automatique). Il est aussi possible de classer les IDS selon la cible qu'ils vont surveiller, les plus communs sont les systèmes de détection d'intrusion réseau et les systèmes de détection d'intrusion hôte.

Certains IDS ont la possibilité de répondre aux menaces qu'ils ont détectées, ces IDS avec capacité de réponse sont des systèmes de prévention d'intrusion.

Description générale

Les systèmes de détection d'intrusion sont des outils ayant pour objectifs de détecter des activités malicieuses sur la cible qu'ils surveillent^[1]. Une alerte sera déclenchée dès lors qu'un comportement malicieux est détecté. Les systèmes de détection d'intrusion sont utilisés en plus des solutions traditionnelles telles que les pare-feux,

pour détecter différents types d'utilisation malicieuse de leur cible qui ne peuvent être détectée par ces dernières^[2]. Pour cela, de nombreux paramètres doivent être pris en compte selon ce que l'on cherche à surveiller. En effet, le système de détection d'intrusion ne se placera pas au même endroit dans l'architecture réseau. Celui-ci peut être placé en coupure du réseau, ou sur un hôte^[3]. De plus, la temporalité de l'analyse est un paramètre important, celui-ci peut produire son analyse en temps réel ou à posteriori.

Les systèmes de détection d'intrusion vont se baser sur l'écriture de règles de

filtrage écrites par les utilisateurs pour effectuer leurs analyses^[4]. Par exemple, pour le système de détection d'intrusion Snort, les règles de filtrages seront composées des éléments suivants^[5] :

- l'action (alert, log, pass, activate, dynamic) déterminant le comportement à adopter en cas de détection d'intrusion ;
- le protocole à filtrer ;
- les adresses IP source et destination ;
- les numéros de ports ;
- la direction du trafic (->, <- ou <>), s'il est entrant, sortant ou bidirectionnelle ;

- les options (motifs dans le paquet, drapeaux, taille, etc.).

Voici un exemple d'une règle Snort qui déclenche une alerte dès qu'un paquet TCP est reçu par l'adresse 10.1.1.0/24 sur le port 80 s'écrit comme suit^[5] :

```
alert tcp any any ->  
10.1.1.0/24 80
```

Méthodologie de détection

Les systèmes de détection d'intrusion sont généralement classifiés en deux catégories, les systèmes de détection d'intrusion par signatures et les

systèmes de détection d'intrusion par anomalies^[1].

Systèmes de détection d'intrusion par signatures

...

Les systèmes de détection d'intrusion par signature (ou SIDS : Signature-based Intrusion Detection System), reposent sur des bibliothèques de description des attaques (appelées signatures)^[6]. Au cours de l'analyse du flux réseau, le système de détection d'intrusion analysera chaque événement et une alerte sera émise dès lors qu'une signature sera détectée^[7]. Cette signature peut référencer un seul paquet,

ou un ensemble (dans le cas d'une attaque par déni de service par exemple). Cette méthodologie de détection se révèle être efficace uniquement si la base de signatures est maintenue à jour de manière régulière^{[7],[8]}. Dans ce cas, la détection par signatures produit peu de faux-positifs^{[7],[8],[9]}. Cependant, une bonne connaissance des différentes attaques est nécessaire pour les décrire dans la base de signature^[8]. Dans le cas d'attaques inconnues de la base, ce modèle de détection s'avérera inefficace et ne générera donc pas d'alertes^[6]. La base de signature est donc très dépendante de l'environnement (système

d'exploitation, version, applications déployées, ...)^[8].

Plusieurs implémentations existent pour effectuer une détection par signature, parmi celles-ci, nous pouvons trouver :

- Les arbres de décision, les règles de filtrage sont représentées sous forme d'arbre de décisions où chaque feuille de l'arbre correspondra à une règle^[10].
- Les système de transition d'états, les intrusions sont décrites comme des scénarios, représentés eux-mêmes comme une séquence de transitions qui caractérisent l'évolution des états du système^{[11],[12]}.

Systèmes de détection d'intrusion ... par anomalies

Contrairement aux SIDS, les systèmes de détection d'intrusion par anomalies (ou AIDS : Anomaly-based Intrusion

Detection System) ne se reposent pas sur des bibliothèques de description des attaques. Ils vont se charger de détecter des comportements anormaux lors de l'analyse du flux réseau^[13]. Pour cela, le système va reposer sur deux phases:

- Une phase d'apprentissage, au cours de laquelle ce dernier va étudier des comportements normaux de flux réseau.

- Une phase de détection, le système analyse le trafic et va chercher à identifier les événements anormaux en se basant sur ses connaissances.

Cette méthode de détection repose sur de nombreuses techniques d'apprentissage supervisé, telles que :

- Les réseaux de neurones artificiels^[14]
- Le modèle de Markov caché^[15]
- Les machines à vecteurs de support^{[16],[17]}

En 2019, la détection d'intrusion par anomalies est reconnue par la communauté comme étant très efficace. En effet, selon les méthodes

d'apprentissage implémentées,
l'exactitude des résultats peut
rapidement atteindre plus de 90% de
détection^{[18],[19],[20]}.

Hybride

...

Cette méthodologie de détection
consiste à reposer à la fois sur un
système de détection par signatures et
sur un système de détection par
anomalies. Pour cela, les deux modules
de détection, en plus de déclencher des
alertes si une intrusion est détectée,
peuvent communiquer leurs résultats
d'analyse à un système de décision qui
pourra lui-même déclencher des alertes

grâce à la corrélation des résultats remontés par les deux modules^[21].

L'avantage de cette méthodologie de détection est la combinaison du faible taux de faux-positifs générés par les systèmes de détection d'intrusion par signature, tout en possédant la capacité de détecter des attaques inconnues dans la base de signature grâce à la détection par anomalie^[22].

L'analyse des protocoles

...

Les systèmes de détection d'intrusion peuvent également reposer sur l'analyse des protocoles. Cette analyse (appelée

en anglais SPA : Stateful Protocol Analysis) a pour objectif de s'assurer du fonctionnement normal d'un protocole (par exemple de transport ou d'application)^{[23],[24]}. Celle-ci repose sur des modèles définis, par exemple par des normes RFC. Ces normes n'étant pas exhaustives, cela peut entraîner des variations dans les implémentations. De plus, les éditeurs de logiciels peuvent ajouter des fonctionnalités propriétaires, ce qui a pour conséquence que les modèles pour ces analyse doivent être régulièrement mis à jour afin de refléter ces variations d'implémentation^[25].

Cette méthode d'analyse a pour principal inconvénient que les attaques ne violant pas les caractéristiques du protocole, comme une attaque par déni de service, ne seront pas détectées^[24].

Temporalité de détection

...

Il existe deux types de temporalité dans les systèmes de détection d'intrusion. La détection en temps réel (système temps réel), et la détection post-mortem (analyse forensique). Le plus souvent, l'objectif est de remonter les alertes d'intrusion le plus rapidement possible à l'administrateur système. La détection en temps réel sera donc privilégiée. Cette

temporalité de détection présente des défis de conception pour s'assurer que le système puisse analyser le flux de données aussi rapidement qu'il est généré^[26]. Cependant, il est aussi envisageable d'utiliser un système de détection d'intrusion dans le cadre d'analyse post-mortem. Dans ce cas, ce dernier permettra de comprendre le mécanisme d'attaque pour aider à réparer les dommages subis et réduire le risque qu'une attaque du même genre se reproduise^[27].

Corrélation des alertes

...

La corrélation des alertes a pour objectif de produire un rapport de sécurité de la cible surveillée (un réseau par exemple). Ce rapport sera basé sur l'ensemble des alertes produites par les différentes sondes de détection d'intrusion disséminées sur l'infrastructure^[28]. Pour cela, il est nécessaire de différencier deux composants^[29] :

- les sondes : chargées de récupérer les données depuis les sources concernant leurs cibles (fichiers de logs, paquets réseaux ,...) et de générer, si nécessaire, des alertes ;
- les composants d'agrégation et de corrélation : chargés de récolter les

données des sondes et des autres composants d'agrégation et de corrélation afin de les corréler et produire le rapport de sécurité transmis à l'administrateur.

Les corrélations peuvent être décrites en deux types^[30] :

- les corrélations explicites : ces corrélations sont utilisées lorsque l'administrateur peut exprimer une connexion entre des événements connus ;
- les corrélations implicites : celles-ci sont utilisées lorsque les données ont des relations entre elles et que des

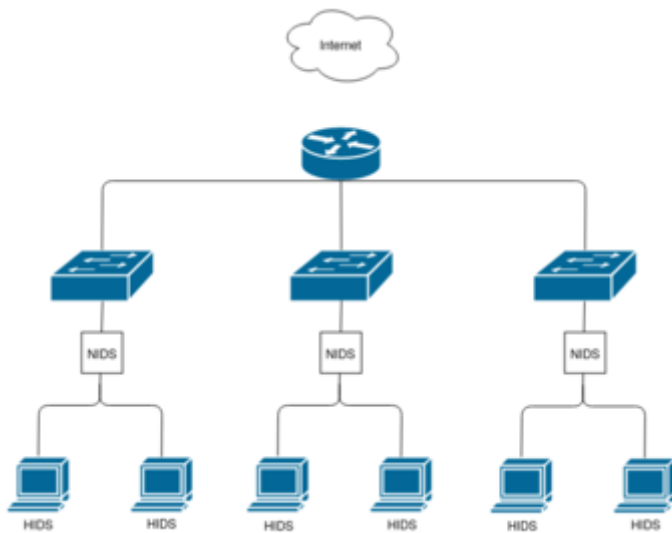
opérations sont nécessaires pour mettre en valeur certains événements.

Pour rendre la corrélation plus efficace, le format de données IDMEF définit un format et une procédure de partage des données spécifique aux systèmes de détection d'intrusion^[31].

Familles de systèmes de détection d'intrusion

En fonction des données qu'ils traiteront, les systèmes de détection d'intrusion peuvent être considérés comme ou étant des systèmes de détection d'intrusion hôtes (analysant les événements au niveau du système d'exploitation), ou

réseaux (analysant les événements propres au trafic réseau)^[9].



Positionnement d'un IDS selon sa famille (NIDS pour Network Intrusion Detection System, ou HIDS pour Host-based Intrusion Detection System).

Systèmes de détection d'intrusion réseaux

...

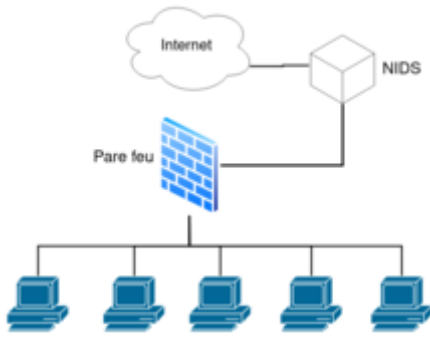


Fig 1 : Placement d'un NIDS en amont d'un pare-feu.



Fig 2 : Placement d'un NIDS en aval d'un pare-feu.

Les systèmes de détection d'intrusion réseaux (ou NIDS : Network Intrusion Detection System) sont les IDS les plus répandus^[32]. Ce sont des outils très utiles pour l'administrateur réseaux qui

va pouvoir, en temps réel, comprendre ce qui se passe sur son réseau et prendre des décisions en ayant toutes les informations^[33].

Ils peuvent être placés à divers endroits sur le réseau, en amont ou en aval d'un pare feu ou encore sur chaque hôte, comme un anti virus. Ces IDS vont analyser tout le trafic entrant et sortant du réseau afin d'y déceler des attaques. Cependant, un NIDS placé sur chaque hôte ne saura pas détecter toutes les attaques possibles comme les attaques par déni de service (DDoS) car il ne verra pas tout le trafic réseau, mais que celui qui arrive à l'hôte final^[34].

Quand un NIDS est positionné en amont d'un pare feu (Fig 1), il pourra alors générer des alertes pour le pare feu qui va pouvoir filtrer le réseau^[35]. Placé en aval du pare feu (Fig 2), le NIDS produira moins de faux positifs, car le trafic réseau qu'il analysera aura déjà été filtré par le pare feu^[35].

Avec l'arrivée du Cloud computing, le positionnement des sondes dans le réseau devient stratégique. En effet, n'importe qui peut louer une machine chez un hébergeur et attaquer une autre machine louée par quelqu'un d'autre chez le même hébergeur. On parlera alors d'attaque interne. Dans ce type d'attaque,

les solutions disposées en bordure du réseau ne détecteront pas ces attaques, il est donc nécessaire de disséminer plusieurs NIDS au sein de l'infrastructure Cloud afin de les détecter^[36].

Dès qu'une attaque est détectée, que ce soit par signature (SIDS) ou anomalies (AIDS), une alerte est remontée afin de pouvoir prendre une décision sur l'action à effectuer, soit par un IPS (Système de prévention d'intrusion), soit par l'administrateur.

Les NIDS peuvent être complétés par d'autres technologies comme l'apprentissage automatique, qui va venir se greffer à un NIDS qui procède par

AIDS, appelé ADNIDS (Anomaly Detection base NIDS). Différentes techniques d'apprentissage profond ont déjà été appliquées aux problèmes des ADNIDS, comme les réseaux de neurones artificiels ou encore les machines à vecteurs de support par exemple. L'ajout de ces techniques aux IDS réseaux permettent de détecter plus d'attaques inconnues, contre lesquelles un NIDS classique fonctionnant avec un SIDS ne pourrait pas détecter. Il est envisagé que le deep learning va participer à surmonter les défis liés au développement d'un NIDS efficace^{[37],[38]}.

Systèmes de détection d'intrusion ...

hôtes

Les systèmes de détection d'intrusion hôte (ou HIDS : Host-based Intrusion Detection System) sont des IDS mis en place directement sur les hôtes à surveiller. Ils vont directement analyser les fichiers de l'hôte, les différents appels système et aussi les événements réseaux^{[39],[40]}. Par conséquent ces analyses sont strictement limitées à l'hôte sur laquelle l'HIDS est installé et n'ont aucune vue sur le réseau^[41].

Les HIDS agissent comme des antivirus mais en plus poussé, car les antivirus ne sont intéressés que par les activités malveillantes du poste alors qu'un HIDS

va pouvoir intervenir s'il détecte des attaques par dépassement de tampon et concernant les processus système par exemple^[39].

La fonction de base d'un HIDS est l'inspection des fichiers de configuration du système d'exploitation afin d'y déceler des anomalies^[42] contre les rootkit notamment. Les HIDS utilisent des sommes de contrôle (MD5, SHA-1...) des programmes exécutables pour s'assurer qu'ils n'ont pas été modifiés.

Étant donné que les HIDS sont installés directement sur les machines, quelqu'un de malveillant qui aurait réussi à prendre

le contrôle de la machine pourrait sans mal désactiver l'HIDS^[43].

Systemes de détection d'intrusion collaboratifs

...



Approche centralisée d'un CIDS.



Approche hiérarchique d'un CIDS.



Approche distribuée d'un CIDS.

Les systèmes de détection d'intrusion collaboratif (ou CIDS : Collaborative Intrusion Detection System) sont des systèmes reposant sur d'autres IDS, de ce fait le CIDS peut opérer sur des systèmes hétérogènes. Il existe trois façons de mettre en place un CIDS, l'approche centralisée, l'approche hiérarchique et l'approche distribuée.

L'approche centralisée

Elle se compose de deux éléments, le système expert et les IDS (HIDS ou

NIDS). Les IDS vont pouvoir détecter, sur leur réseau local ou sur leur hôte, des anomalies qu'ils enverront au système expert. Il va permettre de déterminer s'il s'agit d'une attaque globale contre les différents systèmes ou plus locale, s'il n'a reçu qu'une seule alerte par exemple. Les CIDS déployés sur cette approche ont un très bon taux de détection.

Mais ils ont deux désavantages majeurs, le premier est que si le système expert tombe en panne, tout le système est inutilisable, il s'agit d'un point de défaillance unique (single-point of failure en anglais, ou SPOF)^{[44],[45]}. Le deuxième

inconvénient de cette approche est qu'en cas de grosse attaque, il est possible que certaines des alertes reçues soient ignorées en raison de la quantité reçue par le système expert, ou que ces alertes soient traitées plus tard et donc, possiblement, après l'attaque^{[46],[45]}.

Cette approche a été mise en place pour DIDS (Distributed Intrusion Detection System) par Snapp^[47].

L'approche hiérarchique

Cette approche va permettre d'éviter le point de défaillance unique, mis en lumière par l'approche centralisée. En effet, dans cette solution, plusieurs nœuds (Système expert) sont chargés

de la corrélation des alertes. Un nœud est désigné dans chaque groupe afin qu'il agisse en tant que nœud de corrélation et d'alerte, il va donc analyser les alertes qui viennent de son groupe, les corréler et transmettre une alerte, si besoin, au nœud supérieur. Cette fois-ci si un nœud intermédiaire vient à être désactivé, toute la sous-branche sera inutilisable^{[48],[49]}.

L'approche distribuée

La dernière approche, permet d'éviter d'avoir des points de défaillance, qui pourrait mettre à mal tout le système de détection. Pour cela, chaque nœud est collecteur d'information ainsi

qu'analyseur. Ces nœuds détectent localement les attaques et sont capables de corréler les informations des nœuds voisins pour détecter les attaques globales^{[50],[51]}.

Autres

...

Il existe également d'autres familles de systèmes de détection d'intrusion. Parmi celles-ci, nous pouvons retrouver les familles suivantes :

WIDS (Wireless Intrusion Detection System)

Ce type de système de détection d'intrusion permet de détecter et d'avertir sur les attaques spécifiques

aux réseaux sans-fil (découverte de réseau, attaque de l'homme du milieu, attaque par déni de service, ...) [52].

APHIDS (Agent-Based Programmable Hybrid Intrusion Detection System)

Ce type de système de détection d'intrusion se base sur des agents autonomes réactifs, capables de communiquer avec d'autres systèmes [53], ou de se déplacer d'hôte en hôte (on parle alors d'agents mobiles), permettant ainsi de réduire l'impact réseau du système de détection d'intrusion pour sa collecte de données [54].

HAMA-IDS (Hybrid Approach-based Mobile Agent Intrusion Detection

System)

Cette méthode de détection basée sur des agents mobiles, possédant à la fois une base de signature d'intrusion (SIDS), et une base contenant des informations sur le système recueilli à l'aide de statistiques (peut être assimilé à un AIDS)^[55].

Exemples de systèmes de détection d'intrusion

Systèmes de détection d'intrusion réseaux

...

- Snort
- Bro
- Suricata

- Enterasys
- Check Point
- Tipping Point

Systèmes de détection d'intrusion hôtes

...

- AIDE
- Chkrootkit
- DarkSpy
- Fail2ban
- IceSword (fr)
- OSSEC
- Rkhunter
- Rootkit Unhooker
- Tripwire

Hybrides

...

- Prelude
- OSSIM

Domaines d'application

Systemes distribués

...

Article principal : Systemes de detection et de prevention d'intrusions dans les systemes distribués.

Les systemes de detection et de prevention d'intrusions dans les systemes distribués permettent de repérer et d'empêcher l'intrusion d'un utilisateur malveillant dans un systeme

distribué comme une grille informatique ou un réseau en nuage^[56].

Internet des objets

...

Article principal : Systèmes de détection et prévention d'intrusion pour les réseaux de capteurs sans fil.

Avec la constante augmentation des réseaux de capteurs, leur nombre devrait approcher les 26 milliards en 2020^[57], l'internet des objets représente de nombreux enjeux de sécurité, notamment dus à leur faible puissance de calcul, leur hétérogénéité, le nombre de capteurs dans le réseau ainsi que la topologie du réseau^{[58],[59]}. De ce fait, les

systèmes de détection d'intrusion traditionnels ne peuvent pas directement être appliqués aux réseaux de capteurs^[60]. Néanmoins, de nombreuses avancées ont été présentées au cours des années 2000-2010 pour pallier cette problématique^[61].

Systemes de prévention d'intrusion

Article détaillé : Systeme de prevention d'intrusion.

Principe

...

Contrairement aux systèmes de détection d'intrusion qui se contentent

d'analyser des données pour émettre des alertes, les systèmes de prévention d'intrusions sont des outils permettant de détecter une attaque sur le système monitoré et de mettre en place des mécanismes de défense permettant de mitiger l'attaque^[62]. Pour cela, différentes contre-mesures peuvent être mises en place telles que :

- Re-configurer des équipements réseaux (routeurs, pare-feux, ...) pour bloquer les futures attaques^[63]
- Filtrer le trafic réseau en supprimant les paquets malicieux^[63]

Les familles de systèmes de prévention d'intrusion

Tout comme les systèmes de détection d'intrusion, il existe deux grandes familles de systèmes de prévention d'intrusion^{[64],[65]} :

- Les IPS réseau (ou NIPS : Network-based Intrusion Prevention Systems), capables de stopper certaines attaques rapidement et de se protéger des dommages critiques sur un réseau^[66]
- Les IPS hôtes (ou HIPS : Host-based Intrusion Prevention Systems), capables de bloquer l'accès aux ressources systèmes selon des règles définies par l'administrateur ou par des réponses apprises automatiquement

par le système de prévention d'intrusion^[67]. Ce type de système de prévention d'intrusion permet de protéger des serveurs de différentes vulnérabilités^[65].

Histoire des IDS

Avant l'invention des IDS, la détection d'intrusion se faisait à la main, car toutes les traces devaient être imprimées afin que les administrateurs puissent y déceler des anomalies. C'est une activité très chronophage et pas très efficace, car utilisée après les attaques afin de déterminer les dommages et de retrouver comment les assaillants s'y sont pris pour entrer dans le système.

À la fin des années 70, débuts des années 80, le stockage de données en ligne est de moins en moins coûteux, les traces sont migrées sur des serveurs et en parallèle de cette migration de données, du format papier au format numérique, des chercheurs développent les premiers programmes d'analyse de traces^[68], mais cela reste inefficace car ces programmes sont lents et fonctionnent la nuit lorsque la charge sur le système est faible^[69], donc les attaques sont le plus souvent détectées après coup.

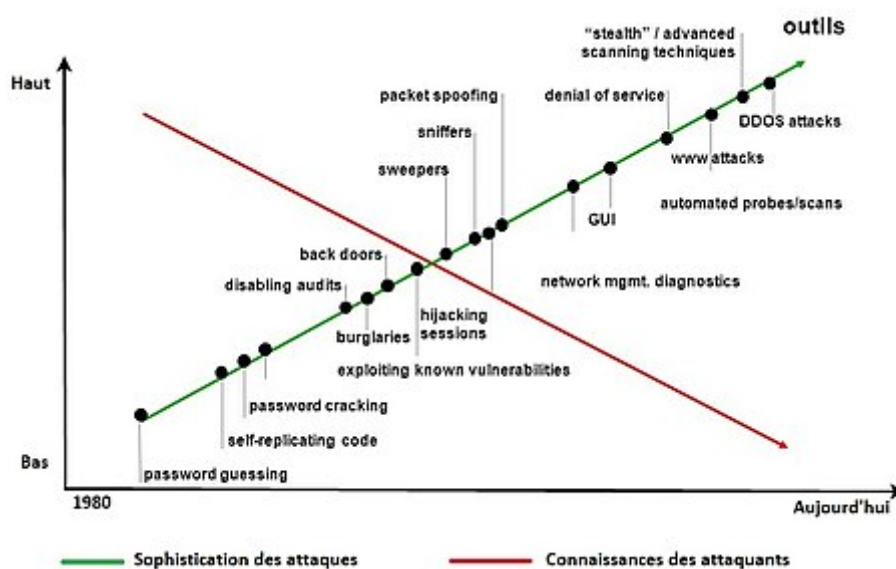
En 1980, James Anderson, chercheur à la NSA, introduit le concept d'IDS^{[53],[70]}, mais c'est en 1987 quand Dorothy.

Denning publie les premiers modèles de détection^[71] que les IDS vont réellement se développer.

Au début des années 90, apparaissent les premiers programmes d'analyse en temps réel, qui permettent d'analyser les traces dès qu'elles sont produites. Cela a permis de détecter les attaques plus efficacement et cela a rendu possible dans certains cas la réalisation de prévention d'attaque.

Avant l'apparition d'outils de piratage, les attaques perpétrées envers des sites web, étaient menées par des personnes expérimentées^[72]. La figure suivante représente les connaissances des

attaquants en fonction du temps, on constate donc qu'aujourd'hui, n'importe qui peut attaquer des sites Web sans connaissances préalables^[72], notamment grâce à ces outils, qui ont été développés dans ce but.



Évolution des connaissances des attaquants en fonction du temps.

Entre 2006 et 2010, le nombre d'attaques est passé d'environ 5000 à plus de 35000^[73], d'où le besoin d'avoir des IDS performants.

Depuis quelques années, les avancées produites en matière d'IDS sont de permettre à l'utilisateur de déployer celui-ci dans un large réseau tout en garantissant une sécurité effective, à l'heure du changement perpétuel de l'environnement informatique et des innombrables nouvelles attaques dévoilées chaque jour.

Références

1. *Kruegel 2003, p. 173*

2. *Khraisat 2019, p. 3*
3. *Depren 2005, p. 713*
4. *Kumar 2012, p. 36*
5. *Roesch 1999, p. 232*
6. *Kemmerer 2002, p. 28*
7. *Yeo 2017, p. 3*
8. *Kumar 2012, p. 35*
9. *Kruegel 2003, p. 174*
10. *Kruegel 2003, p. 178*
11. *Ilgun 1993, p. 18*
12. *Vigna 2000, p. 2*
13. *Yeo, p. 3*
14. *Debar 1992, p. 244*
15. *Wang 2011, p. 277*

16. *Wang 2004, p. 358*
17. *Zhang 2015, p. 103*
18. *Wang 2011, p. 279*
19. *Wang 2004, p. 363*
20. *Zhang 2015, p. 106*
21. *Depren 2005, p. 714*
22. *Kim 2014, p. 1693*
23. *Mudzingwa 2012, p. 3*
24. *Sakri 2004, p. 21*
25. *Pérez 2014, p. 223*
26. *Ghosh 2000, p. 106*
27. *Lippmann 2000, p. 579*
28. *Valeur 2004, p. 147*
29. *Debar 2001, p. 86-87*

30. *Cuppens 2002, p. 6*
31. *Cuppens 2002, p. 2*
32. *Kumar 2007, p. 1*
33. *Niyaz 2016, p. 1*
34. *Kumar 2007, p. 5*
35. *Kumar 2007, p. 4*
36. *Riquet 2015, p. 40*
37. *Djemaa 2011, p. 303*
38. *Fiore 2013, p. 22*
39. *Das 2014, p. 2266*
40. *Riquet 2015, p. 13*
41. *Bace 1998, p. 1*
42. *Bace 1998, p. 12*
43. *Glass-Vanderlan 2018, p. 3*

44. *Riquet 2015, p. 18*
45. *Zhou 2010, p. 129*
46. *Riquet 2015, p. 19*
47. *Snapp 1991, p. 1*
48. *Riquet 2015, p. 21*
49. *Zhou 2010, p. 130*
50. *Riquet 2015, p. 22*
51. *Zhou 2010, p. 131*
52. *Haddadi 2010, p. 85*
53. *Djemaa 2012, p. 1*
54. *Onashoga 2009, p. 670*
55. *Djemaa 2012, p. 3*
56. *Patel 2013, p. 33*
57. *Zarpelao 2017, p. 25*

58. *Chen 2009, p. 52*
59. *Fu 2011, p. 315*
60. *Sicari 2015, p. 146*
61. *Zarpelao 2017, p. 27*
62. *Beigh 2012, p. 667*
63. *Patel 2010, p. 279*
64. *Zhang 2004, p. 387*
65. *Stiennon 2002, p. 1*
66. *Shin 2009, p. 5*
67. *Stiennon 2002, p. 4*
68. *Saltzer 1975, p. 1279*
69. *Kemmerer 2002, p. 27*
70. *Innella 2001, p. 1*
71. *Denning 1987, p. 222*

72. *McHugh 2000, p. 43*



73. *Ashoor 2011, p. 4*

Bibliographie




✍️ : document utilisé comme source pour la rédaction de cet article.

- ✍️_(en) Martin Roesch, « Snort – Lightweight Intrusion Detection for Networks », *Proceedings of LISA '99: 13th Systems Administration Conference*, 1999, p. 229-238
- _(en) Dong Seong Kim, Ha-Nam Nguyen et Jong Sou Park, « Genetic Algorithm to Improve SVM Based Network Intrusion Detection System », *Proceedings of the 19th International Conference on*

Advanced Information Networking and Applications (AINA'05), 2005, p. 155-158 (ISBN 0-7695-2249-1,
DOI 10.1109/AINA.2005.4)

-  _(en) Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid et Mansoor Alam, « A Deep Learning Approach for Network Intrusion Detection System », *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2016, p. 41 - 50 (ISSN 2471-285X,
DOI 10.1109/TETCI.2017.2772792)
-  _(en) David Mudzingwa et Rajeev Agrawal, « A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS) », 2012 *Proceedings of IEEE Southeastcon*,



2012, p. 1 - 6 (ISBN 978-1-4673-1375-9,
ISSN 1558-058X,
DOI 10.1109/SECon.2012.6197080)



- _(en) Sapiah Sakri, « Intrusion detection and prevention », *acadox*, 2004, p. 1 - 25
- _(en) Saidat Adebukola Onashoga, Adebayo D. Akinde et Adesina Simon Sodiya, « A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems », *Issue s in Informing Science and Information Technology*, 2009, p. 669 - 682 (ISSN 1547-5867)
- _(en) Christopher Kruegel et Thomas Toth, « Using Decision Trees to Improve Signature-Based Intrusion

Detection », *6th International Symposium, RAID 2003*, 2003, p. 173–191 (ISBN 3-540-40878-9)


-  _(en) Vinod Kumar et Om Prakash Sangwan, « Signature Based Intrusion Detection System Using SNORT », *International Journal of Computer Applications & Information Technology*, 2012, p. 35-41 (ISSN 2278-7720)
-  _(en) André Pérez, *Network Security*, ISTE Ltd., 2014, 256 p.
(ISBN 978-1-84821-758-4, lire en ligne)
-  _(en) John McHugh, Alan Christie et Allen, « Defending yourself: The Role of

Intrusion Detection System », *IEEE Software*, Volume: 17 , Issue: 5, 2000, p. 42-51 ([ISSN 1937-4194](#), [DOI 10.1109/52.877859](#))

-  (en) Ahmed Patel, Mona Taghavi, Bakhtiyari et Celestino Júnior, « An intrusion detection and prevention system in cloud computing: A systematic review », *Journal of Network and Computer Applications*, Volume 36, Issue 1, 2013, p. 25-41 ([DOI 10.1016/j.jnca.2012.08.007](#))
-  (en) Asmaa Shaker Ashoor et Sharad Gore, « Importance of Intrusion Detection System (IDS) », *International Journal of Scientific and Engineering Research*, 2011, vol. 2, no 1, 2011, p. 1-7



- ^(en) Christina Warrender, Stephanie Forrest et Barak Pearlmutter, « Detecting Intrusions Using System Calls: Alternative Data Models », *International Journal of Computer Applications & Information Technology*, 1999, p. 133-145 (ISBN 0-7695-0176-1, ISSN 1081-6011, DOI 10.1109/SECPRI.1999.766910)
-  ^(en) Richard A. Kemmerer et Giovanni Vigna, « Intrusion Detection: A Brief History and Overview », *Computer*, 2002, suppl27 - suppl30 (ISSN 1558-0814, DOI 10.1109/MC.2002.1012428)
-  ^(en) R. Stiennon et M. Easley, « Intrusion Prevention Will Replace Intrusion


Detection », *Technology*, T17-0115,
2002, p. 1-5

-  _(en) Hervé Debar, Monique Becker et Didier Siboni, « A Neural Network Component for an Intrusion Detection System », *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, 1992, p. 240-250 ([ISBN 0-8186-2825-1](#), [DOI 10.1109/RISP.1992.213257](#))
- _(en) David Wagner et Paolo Soto, « Mimicry Attacks on Host-Based Intrusion Detection Systems », *CCS '02 Proceedings of the 9th ACM conference on Computer and communications security*, 2002, p. 255-264



(ISBN 1-58113-612-9,

DOI 10.1145/586110.586145)


-  (en) Chenfeng Vincent Zhou, Lecki et Karunasekera, « A survey of coordinated attacks and collaborative intrusion detection », *Computers & Security, Volume 29, Issue 1*, 2010, p. 129-140
(DOI 10.1016/j.cose.2009.06.008)
-  (en) Ozgur Depren, Murat Topallar, Emin Anarim et M. Kemal Ciliz, « An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks », *Expert Systems with Applications*, 2005, p. 713-722 (ISSN 0957-4174,
DOI 10.1016/j.eswa.2005.05.002)

- ^(en) Ken Deeter, Kapil Singh, Steve Wilson, Luca Filipozzi et Son Vuong, « APHIDS: A Mobile Agent-Based Programmable Hybrid Intrusion Detection System », *Mobility Aware Technologies and Applications*, 2004, p. 244-253 (ISBN 3-540-23423-3, ISSN 0302-9743)
- ^(en) Guoning Hu, Deepak Venugopal et Shantanu Bhardwaj, « Wireless intrusion prevention system and method », *United States Patent*, 2011, p. 1-10
-  ^(en) Seung Won Shin, Jintaz Oh, Ki young Kim, Jong Soo Jang et Sung Won Sohn, « Network intrusion detection and prevention system and



method thereof », *United States Patent*, 2009, p. 1-10

-  ^(en) Boukhoulouf Djemaa et Kazar Okba, « Intrusion Detection System: Hybrid Approach based Mobile Agent », *International Conference on Education and e-Learning Innovations*, 2012 ([ISBN 978-1-4673-2226-3](#), [DOI 10.1109/ICEELI.2012.6360647](#))
- ^(en) Gary Manuel Jackson, « Intrusion prevention system », *United States Patent*, 2008
-  ^(en) Xinyou Zhang, Chengzhong Li et Wenbin Zheng, « Intrusion Prevention System Design », *The Fourth International Conference on Computer and Information Technology*, 2004,

p. 386-390 (ISBN 0-7695-2216-5,
DOI 10.1109/CIT.2004.1357226)

-  _(en) Steven R Snapp, James Brentano, Gihan V Dias, Goan, Heberlein, Ho, Levitt, Mukherjee, Smaha, Grance, Teal et Mansur, « DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype », *In Proceedings of the 14th National Computer Security Conference*, 1991, p. 167-176
- _(en) Ismail Butun, Salvatore D Morgera et Ravi Sankar, « A Survey of Intrusion Detection Systems in Wireless Sensor Networks », *IEEE Communications Surveys & Tutorials*, 2014, p. 266-282



([DOI 10.1109/SURV.2013.050113.00191](#)
)

- ^(en) Stefan Axelsson, « Intrusion Detection Systems : A Survey and Taxonomy », *Technical report*, 2000
-  ^(en) Ansam Khraisat, Iqbal Gondal, Peter Vamplew et Kamruzzaman, « Survey of intrusion detection systems: techniques, datasets and challenges », *Cybersecurity*, 2019 ([DOI 10.1186/s42400-019-0038-7](#))
-  ^(en) Ahmed Patel, Qais Qassim et Christopher Wills, « A survey of intrusion detection and prevention systems », *Information Management & Computer Security*, Vol. 18 No. 4, 2010,

p. 277-290

([DOI 10.1108/09685221011079199](https://doi.org/10.1108/09685221011079199))

- ^(en) Farzad Sabahi, Ali Movaghar et Christopher Wills, « Intrusion Detection: A Survey », *Third International Conference on Systems and Networks Communications*, 2008, p. 23-26 ([ISBN 978-0-7695-3371-1, DOI 10.1109/ICSNC.2008.44](https://doi.org/10.1109/ICSNC.2008.44))
- ^(en) Aleksandar Milenkoski, Marco Vieira, Samuel Kounev, Avritzer et Payne, « Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices », *ACM Computing Surveys (CSUR) Volume 48 Issue 1, Article No. 12*, 2015 ([DOI 10.1145/2808691](https://doi.org/10.1145/2808691))

-  _(en) Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin et Kuang-Yuan Tunga, « Intrusion detection system: A comprehensive review », *Journal of Network and Computer Applications*, 2012, p. 16-24
([DOI 10.1016/j.jnca.2012.09.004](https://doi.org/10.1016/j.jnca.2012.09.004))
-  _(en) Liu Hua Yeo, Xiangdong Che et Shalini Lakkaraju, « Understanding Modern Intrusion Detection Systems: A Survey », *arXiv:1708.07174*, 2017
- _(en) Aumreesh Ku Saxena, Dr. Sitesh Sinha et Dr. Piyush Shukla, « General Study of Intrusion Detection System and Survey of Agent Based Intrusion Detection System », *International Conference on Computing*,




Communication and Automation, 2017,
p. 417-421

([DOI 10.1109/CCAA.2017.8229866](https://doi.org/10.1109/CCAA.2017.8229866))

- 📄 Damien Riquet, « Discus: Une architecture de détection d'intrusions réseau distribuée basée sur un langage dédié », *these.fr*, 2015
- Jonathan Roux, « Détection d'Intrusion dans l'Internet des Objets : Problématiques de sécurité au sein des domiciles », *Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI)*, 2017
- ^(en) Amol Borkar, Akshay Donode et Anjali Kumari, « A Survey on Intrusion Detection System (IDS) and Internal



Intrusion Detection and Protection System (IIDPS) », *Proceedings of the International Conference on Inventive Computing and Informatics*, 2017, p. 949-953

([DOI 10.1109/ICICI.2017.8365277](https://doi.org/10.1109/ICICI.2017.8365277))

-  _(en) Jerry H Saltzer, « The Protection of Information in Computer Systems », *Proc. IEEE*, vol. 63, no. 9, 1975, p. 1278–1308
([DOI 10.1109/PROC.1975.9939](https://doi.org/10.1109/PROC.1975.9939))
-  _(en) Paul Innella, « The Evolution of Intrusion Detection Systems », *LLC. SecurityFocus*, 2001
-  _(en) Dorothy E Denning, « An intrusion detection model », *IEEE Transactions on Software Engineering*, Volume: SE-13



, Issue: 2, 1987, p. 222-232

(ISBN 0-8186-0716-5, ISSN 1540-7993,
DOI 10.1109/TSE.1987.232894)





-  _(en) Fei Wang, Hongliang Zhu, Bin Tian, Yang Xin, Xinxin Niu et Yu Yang, « A HMM-Based Method For Anomaly Detection », *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*, 2011, p. 276-280 (ISBN 978-1-61284-159-5,
DOI 10.1109/ICBNMT.2011.6155940)
-  _(en) Yanxin Wang, Johnny Wong et Andrew Miner, « Anomaly intrusion detection using one class SVM », *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop*, 2004, 2004, p. 358-364

(ISBN 0-7803-8572-1,



DOI 10.1109/IAW.2004.1437839)

-  _(en) Ming Zhang, Boyi Xu et Jie Gong,
« An Anomaly Detection Model based
on One-class SVM to Detect Network
Intrusions », *11th International
Conference on Mobile Ad-hoc and
Sensor Networks*, 2015, p. 102-107
(ISBN 978-1-5090-0329-7,
DOI 10.1109/MSN.2015.40)
-  _(en) Bilal Maqbool Beigh et M.A Peer,
« Intrusion Detection and Prevention
System: Classification and Quick
Review », *ARPJ Journal of Science and
Technology*, 2012, p. 661-675
(ISSN 2225-7217)




-  _(en) Sailesh Kumar, « Survey of Current Network Intrusion Detection Techniques », *CSE571S: Network Security*, 2007, p. 102-107
- _(en) Mostafa A Salama, Heba F Eid, Rabie A Ramadan, Darwish et Ella Hassanien, « Hybrid Intelligent Intrusion Detection Scheme », *Springer, Berlin, Heidelberg*, 2011, p. 293-303 ([ISBN 978-3-642-20505-7](#))
-  _(en) Ugo Fiore, Francesco Palmieri, Aniello Castiglione et De Santis, « Network Anomaly Detection with the Restricted Boltzmann Machine », *Neurocomputing, volume 122*, 2013, p. 13-23 ([DOI 10.1016/j.neucom.2012.11.050](#))

-  _(en) Niva Das et Tanmoy Sarkar,
« Survey on Host and Network Based
Intrusion Detection System », *Int. J.
Advanced Networking and Applications
Volume: 6 Issue: 2*, 2014, p. 2266-2269
-  _(en) Rebecca Bace, « An Introduction to
Intrusion Detection & Assessment »,
*ICSA intrusion detection systems
consortium white paper*, 1998, p. 1-38
-  _(en) Tarrah R Glass-Vanderlan, Michael
D Iannacone, Maria S Vincent, Chen et
Bridges, « A Survey of Intrusion
Detection Systems Leveraging Host
Data », *arXiv preprint arXiv:1805.06070*,
2018, p. 1-40
-  _(en) Koral Ilgun, « USTAT: a real-time
intrusion detection system for UNIX »,



Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy, 1993, p. 16-28
(ISBN 0-8186-3370-0,
DOI 10.1109/RISP.1993.287646)

-  (en) Giovanni Vigna, Steve T. Eckmann et Richard A. Kemmerer, « The STAT Tool Suite », *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, 2000
(ISBN 0-7695-0490-6,
DOI 10.1109/DISCEX.2000.821508)
-  (en) Anup K. Ghosh, Christoph Michael et Michael Schatz, « A Real-Time Intrusion Detection System Based on Learning Program Behavior », *Recent*

Advances in Intrusion Detection, 2000,
p. 93-109 (ISBN 978-3-540-41085-0)



-  _(en) Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba et Kumar Das, « The 1999 DARPA off-line intrusion detection evaluation », *Computer Networks*, 2000, p. 579-595 (ISBN 978-3-540-41085-0)
-  _(en) Xiangqian Chen, Kia Makki, Kang Yen et Niki Pissinou, « Sensor Network Security: A Survey », *IEEE Communications surveys & tutorials*, 2009, p. 52-73 (ISSN 1553-877X, DOI 10.1109/SURV.2009.090205)
-  _(en) Rongrong Fu, Kangleng Zheng, Dongmei Zhang et Yixian Yang, « An Intrusion Detection Scheme Based on




Anomaly Mining in Internet of Things », *4th IET International Conference on Wireless, Mobile & Multimedia Networks (ICWMMN 2011)*, 2011, p. 315-320 ([ISBN 978-1-84919-507-2](#), [DOI 10.1049/cp.2011.1014](#))

-  _(en) Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Claudio Toshio Kawakani et Sean Carlisto De Alvarenga, « A survey of intrusion detection in Internet of Things », *Journal of Network and Computer Applications*, 2017, p. 25-37 ([DOI 10.1016/j.jnca.2017.02.009](#))
-  _(en) S. Sicari, A. Rizzardi, L.A. Grieco et A. Coen-Porisini, « Security, privacy and trust in Internet of Things: The road

ahead », *Computer Networks*, 2015,
p. 146-164

([DOI 10.1016/j.comnet.2014.11.008](#))

-  _(en) Fariba Haddadi et Mehdi A. Sarram,
« Wireless Intrusion Detection System
Using a Lightweight Agent », *Second
International Conference on Computer
and Network Technology*, 2010, p. 84-
87 ([ISBN 978-0-7695-4042-9](#),
[DOI 10.1109/ICCNT.2010.26](#))
-  _(en) Gisung Kim, Seungmin Lee et
Sehun Kim, « A novel hybrid intrusion
detection method integrating
anomalydetection with misuse
detection », *Expert Systems with
Applications*, 2014, p. 1690-1700
([DOI 10.1016/j.eswa.2013.08.066](#))

-  (en) Hervé Debar et Andreas Wespi, « Aggregation and Correlation of Intrusion-Detection Alerts », *Recent Advances in Intrusion Detection*, 2001, p. 85-103 ([ISBN 978-3-540-42702-5](#))
-  (en) Frédéric Cuppens et Alexandre Miège, « Alert Correlation in a Cooperative Intrusion Detection Framework », *IEEE Symposium on Security and Privacy*, 2002, p. 1-14 ([ISBN 0-7695-1543-6](#), [ISSN 1081-6011](#), [DOI 10.1109/SECPRI.2002.1004372](#))
-  (en) Fredrik Valeur, Giovanni Vigna, Christopher Kruegel et Richard A. Kemmerer, « A Comprehensive Approach to Intrusion Detection Alert Correlation », *IEEE Transactions on*

dependable and secure computing,
vol. 1, 2004, p. 146-169 (ISSN 1545-5971)



Portail de la sécurité informatique

Ce document provient de

« https://fr.wikipedia.org/w/index.php?title=Systeme_de_d%C3%A9tection_d%27intrusion&oldid=178604709 ».

Dernière modification il y a 5 jours par CodexBot

Le contenu est disponible sous licence CC BY-SA 3.0 sauf mention contraire.