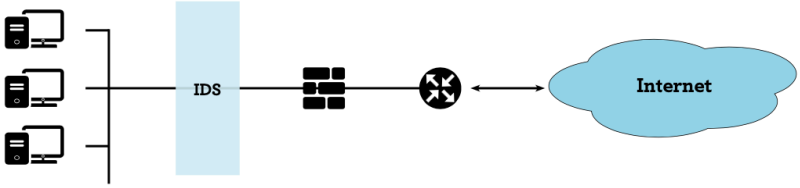
S4L1
Systèmes de détection et prévention d'intrusions IDS/IPS
Rida KHATOUN

Contenu de la leçon :

- Définition IDS / IPS
- Différentes méthodologies de détection
- Typologie IDS / IPS
- Évaluation d'un système IDS

Bonjour.

- Understand the key functions performed by intrusion detection and prevention systems and the detection methodologies that they use.
- Understand how to evaluate an IDS.



Après avoir suivi la vidéo, vous serez capables de décrire le fonctionnement des systèmes de détection d'intrusions, leurs différents types, et comment évaluer leur performance. Nous présenterons tout d'abord la définition d'un système de détection d'intrusion et la différence par rapport à un système de prévention d'intrusion, puis les différentes méthodologies de détection et le principe d'évaluation de tels systèmes. Enfin, nous allons voir la liste des systèmes de détection d'intrusion les plus utilisés.

Définition des IDS/IPS

- Intrusion detection
  - Intrusion detection is the act of detecting unwanted traffic on a network or a device;
  - Example of an intrusion: XMAS scan through nmap tool
- Intrusion Detection System (IDS)
  - Set of software or hardware components;
  - Main function is to **monitor** in order to **detect** any intentional or unintentional intrusion into an information system and any possible alteration of data.
  - Example: `alert tcp any any -> home-net 80 (msg:"XMAS Scan"; flags:FPU; sid:1000001; rev:1;)`
- Intrusion Prevention System (IPS)
  - Set of software or hardware components;
  - Main function is to **prevent** suspicious activity detected within a system.
  - Example: `drop tcp any any -> web-serveur 80 (classtype:attempted-user; msg:"I have blocked the traffic in destination to the web-server!";)`

Par définition, une intrusion est une action non-conforme à la politique de sécurité d'un système ou réseau. La détection d'intrusion s'applique à toutes les phases d'une attaque :

- La reconnaissance comme par exemple la récupération d'informations sur le système - L'attaque sur les points vulnérables
- Les traitements post attaque comme par exemple la dissimulation des traces.

Un IDS (ou système de détection d'intrusion) est un ensemble de composants logiciels ou matériels dont la fonction principale est de détecter et analyser toute tentative d'effraction volontaire ou non dans un SI ainsi que toute altération éventuelle de ces données. Comme nous le savons, la communication TCP (se connecter sur un serveur web, par exemple) se fait tout d'abord par une connexion TCP à trois étapes (SYN, SYN/ACK et ACK) avec la machine cible. Mais parfois, au lieu d'utiliser ces drapeaux TCP, l'attaquant réalise ce qu'on appelle un scan en envoyant différents drapeaux TCP au serveur pour voir sa réaction et par conséquent savoir si un port est ouvert ou fermé. XMAS est l'une de ces méthodes qui consiste à envoyer au serveur les drapeaux Fin, PSH et URG pour connaitre l'État d'un port donné. Un IDS peut détecter cette intrusion en analysant tout simplement la combinaison de ces drapeaux dans une connexion entrante comme montré dans la règle « *alert tcp any any --> home-net 80* ».

Un IPS (système de prévention d'intrusion) est un ensemble de composants logiciels ou matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système. Par exemple la règle :

drop tcp any any --> web-serveur 80

permet de bloquer tout le trafic à destination d'un serveur web.

Les méthodes de détection

▸ Signature-based IDS

- Principle
  - Common attacks can be characterized with a signature;
  - An IDS has a database of signatures and compare the current traffic with these signatures and detect a classic attack.
- Example of a signature
  - Find the "`/win7/system32/cmd.exe Pattern`" in an http request;
  - Find the "`failed su for root`" pattern in a system log;
  - Find this content in a packet: : "`|00 01|W|00 00 00 18|`".
- Advantages:
  - Quick detection of all known attacks;
  - Easy to implement;
  - Precision (according to the rules).
- *Disadvantages:*
  - Detects only known attacks;
  - Frequently update the signature database.

Il existe plusieurs méthodes de détection d'intrusions : la détection à base de signature, la détection à base d'anomalie ou comportementale et la détection par vérification d'intégrité. La détection par scénarios ou signature consiste à comparer l'activité du réseau aux représentations d'intrusion ou signatures préétablies comme la présence de certains motifs dans une requête au niveau applicatif ou même dans un paquet IP. Ce type de détection permet de détecter toutes les attaques ou intrusions dont les motifs sont connus et référencés. Par ailleurs, la détection est très rapide. Par contre, une attaque ou intrusion nouvelles ou non référencée ne sera pas détectée. Ce type de détection, nécessite donc de souvent mettre à jour la base de signatures.

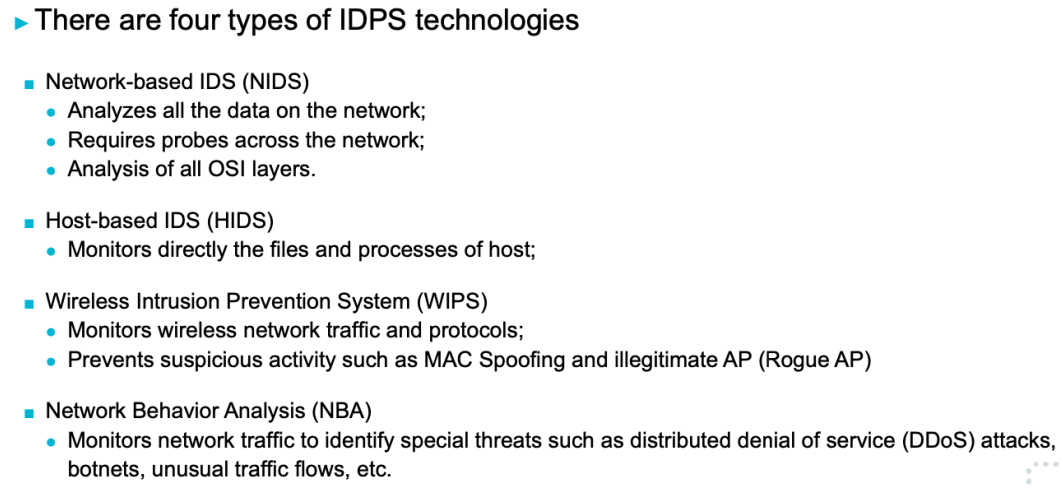
Anomaly-based IDS

- Principle
  - Based on the «normal» behavior of the system;
  - A deviation from this behavior is considered suspicious;
  - A behavior must be modeled by a profile which relies on tools of various complexity: thresholds, distances, probabilities, etc.
- Example of a signature
  - Volumes of network exchanges over a day;
  - System calls from an application;
  - Usual commands of a user;
  - Usual requests and used ports on server;
- Advantages:
  - Detection of unknown attacks;
  - Hard to deceive.
- *Disadvantages:*
  - Complexity of implementation and deployment;
  - High number of false alert;
  - Duration of the learning phase.

La détection comportementale, appelée aussi détection par apprentissage, consiste à comparer l'activité d'un utilisateur à un référentiel prédéfini ce qui permet de détecter des attaques non connues comme l'accès à une ressource à des heures non habituelles ou l'envoi d'une requête inhabituelle à un serveur web sur un port fermé par exemple.

L'IDS établit un modèle de trafic normal en se basant sur certains paramètres comme la moyenne de connexions et le type de trafic à des heures précises et ensuite compare le trafic actuel au modèle ou référence. Si les deux trafics sont trop différents, alors il se pourrait qu'une attaque soit en cours. Ce type de détection permet de détecter des nouvelles intrusions si les profils ont été bien définis ce qui n'est pas facile parce que les méthodes de détection comportementale se basent sur des outils de complexité diverses comme les seuils, l'intelligence artificielle, les méthodes probabilistes ou même la Big Data ce qui rend forcément le système très gourmand en temps de calcul, sans garantir pour autant qu'il ne génère pas de fausses alertes. En outre, s'il y a un grand besoin de sécurité cela signifie que l'IDS devra analyser plus de flux d'une manière plus détaillée nécessitant de bien meilleures performances matérielles et logicielles pour l'IDS.

Les technologies IDS/IPS

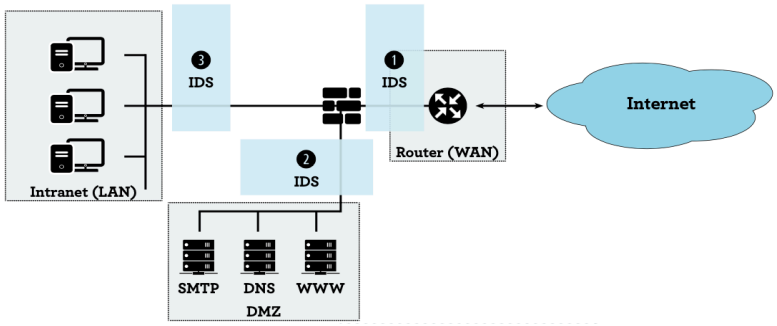


Il existe plusieurs technologies d'IDS : NIDS, HIDS, WIPS et NBA. Un NIDS est un matériel dédié, capable de contrôler les paquets concernant divers équipements du réseau et ceci pour en détecter les intrusions. Il est généralement placé dans une zone clé du réseau et il est possible de déployer plusieurs IDS sur les différentes parties du réseau.

- Un NIDS a souvent plusieurs carte réseau configurées en mode promiscuité ou la carte accepte tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés. Il est donc difficile pour un attaquant d'effacer les traces d'intrusion.
- Dans un HIDS (Host Detection System), les sources de données sont les logs systèmes ou applicatifs, messages d'erreurs, droits de service ou même les métadonnées d'un fichier. Son but est donc de surveiller directement les fichiers et les processus de la machine.
- Le Wireless Intrusion Prevention System (WIPS) permet de monitorer et analyser le spectre du signal WiFi et peut détecter des équipements non autorisés et peu sécurisés, ou encore des attaques comme le déni de service ou les attaques de l'homme du milieu.
- Le Network Behavior Analysis (NBA) consiste en une solution utilisant des algorithmes sophistiqués et un apprentissage automatique pour identifier des anomalies qui contournent les pare-feux, les IDS ou les antivirus. Il fournit aussi une vision complète de la performance du réseau et l'analyse de flux.

Où placer un IDS dans un réseau ?

- An IDS can have three positions in a LAN:



Un IDS réseau (ou NIDS) peut être positionné à 3 endroits du réseau :

1. Dans la première position, l'IDS va pouvoir détecter l'ensemble des attaques frontales provenant de l'extérieur, en amont du firewall mais il déclenchera trop d'alertes et les logs sont difficilement consultables.
2. Dans la position (2), il détectera les attaques qui n'ont pas été filtrées par le firewall et les logs seront plus clairs à consulter puisque les attaques bénignes ne seront pas recensées.
3. Dans la position (3), l'IDS peut détecter des attaques internes, provenant du réseau local de l'entreprise.

Evaluation des performances des IDS

- How to evaluate an IDS ?
  - The performance of an IDS is usually assessed using its sensitivity and specificity
  - Using ROC (Receiver Operating Characteristic) curves make it possible to study the variations in the sensitivity and specificity of a test for different threshold values of a test
- Sensitivity
  - Ability to correctly identify an attack that exists
- Specificity
  - Ability to correctly detect that there is no attack

Les performances des IDS sont généralement évaluées à l'aide de leur sensibilité, spécificité et valeurs prédictives positives et négatives. Les courbes comme ROC (Receiver Operating Characteristic) qui permettent d'étudier les variations de la sensibilité et de la spécificité pour différentes valeurs seuil d'un test sont utilisées pour évaluer les IDS.

La sensibilité est la capacité d'un test à détecter les cas d'une attaque, il s'agit de la capacité d'identifier correctement une attaque qui existe alors que la spécificité est la capacité d'un test à détecter correctement qu'il n'y a pas eu d'attaque.

- How to calculate the Sensitivity and Specificity?
- There are 4 types of alerts:
  - True Positive (TP): Bad traffic triggering an alert;
  - False Positive (FP): Good traffic triggering an alert;
  - False Negative (FN): Bad traffic without alert;
  - True Negative (TN) :Good traffic without alert.

	Attack	No attack
Detection	TP	FP
No detection	FN	TN

- If an IDS has a sensitivity of 100%
  - all attacks are correctly detected, there is no FN
- If an IDS has a specificity of 100%
  - all normal cases are correctly identified, there is no FP

Sensitivity=TP/(TP+FN)

Specificity=TN/(TN+FP)

Pour calculer la sensibilité et la spécificité, on se base sur certains paramètres comme : le nombre de vrais positifs, le nombre de vrais négatifs, le nombre de faux positifs et le nombre de faux négatifs.

- Un vrai positif est une détection d'attaque qui a réellement eu lieu.
- Un faux positif est une détection d'attaque alors qu'elle n'a pas eu lieu.
- Un vrai négatif est une non détection d'attaque lorsqu'en effet il n'y a pas eu d'attaque.
- Un faux négatif est une non détection d'attaque alors qu'une attaque est en cours.

La sensibilité est calculée de la manière suivante : VP/(VP+FN).

Et la spécificité est calculée de la manière suivante : VN/(VN+FP).

Si un test a une sensibilité de 100%, alors toutes les attaques sont correctement détectées. Si un test a une spécificité de 100%, alors tous les cas normaux sont correctement identifiés.

Les outils

- Open Source NIDS
  - Snort
  - Bro
  - Suricata
- Open Source HIDS
  - OSSEC
  - Tripwire
  - AIDE
- Commercial IDS/IPS
  - McAfee
  - Huawei
  - Cisco NGIPS
- NBA tools
  - Arbor SP platform
  - NetFlow


Pour terminer, nous citons, à titre d'exemple, quelques IDS/IPS que nous trouvons sur le marché. Parmi ces IDS/IPS, Snort est une solution très répandue, ayant une bonne réputation et utilisée parfois dans les entreprises conjointement à un IDS commercial. A cela s'ajoute Suricata qui est aussi un IDS/IPS open source supportant le même langage de signatures que Snort et qui dispose de nombreuses fonctionnalités. Quant à Bro, c'est un IDS à base de signatures développé par la communauté de recherche pour la détection d'intrusions et l'analyse de trafic réseau. Néanmoins, il est moins répondu que Snort et Suricata.

Comme HIDS open source, citons OSSEC, Tripwire et AIDE. Les deux derniers font un contrôle d'intégrité sur certains fichiers sensibles contenant, par exemple, la clé privée, les mots de passe, etc. Quant à OSSEC, il s'agit d'un HIDS qui a plus de fonctionnalités qu'AIDE et Suricata. Il analyse, par exemple, les logs, les registres de Windows et il détecte même certaines intrusions comme les rootkit.

Comme IDS/IPS commerciaux, il existe McAfee Network Security Platform, Huawei Next-Generation IPS et NGIPS de Cisco. A titre d'exemple, les systèmes NGIPS de Cisco sont des systèmes de prévention d'intrusions nouvelle génération (comme la série Firepower) qui reçoivent régulièrement de nouvelles signatures et règles développées par une équipe dédiée de Cisco, ceci pour garantir une protection la plus à jour possible.

Enfin, nous pouvons citer des IDS aux fonctionnalités avancées. Ce sont des analyseurs du comportement réseau et des détecteurs d'anomalies, aussi répertoriés sous l'appellation NBA pour Network Behavior Analysis. Ces outils qui se basent, par exemple, sur Arbor SP platform et NetFlow, permettent d'analyser les flux réseaux et détecter les comportements malveillants qui ne sont pas référencés par des signatures dans les dispositifs de sécurité traditionnels. Ces outils permettent de détecter des flux de trafic inhabituels, tels que des attaques par déni de service distribuées (DDoS) ou certaines formes de programmes malveillants.