

**Installation de OSSEC**

Mise en place de OSSEC et étude comparative des outils

**JEANNE d’Arc Sagna**

**PROFESSEUR CHERIF DIALLO**

**Présentation de ossec**

OSSEC est un HIDS (Host Intrusion Detection System). Il a pour objectif de détecter un comportement anormal sur une machine. Il collecte les informations qui lui sont envoyées par les équipements, il utilise les signatures ou le comportement pour détecter une anomalie.

OSSEC est un système de détection d’intrusion (HIDS) gratuit et open-source basé sur l’hôte. Il effectue l’analyse des slogs, la vérification de l’intégrité, la surveillance du registre Windows, la détection du kit racine, les alertes basées sur le temps et la réponse active.

Il fournit une détection d’intrusion pour la plupart des systèmes d’exploitation, y compris Linux, OpenBSD, FreeBSD, OS X, Solaris et Windows. OSSEC dispose d’une architecture centralisée multiplateforme permettant à plusieurs systèmes d’être facilement surveillés et gérés.

On va d’abord redémarrer le serveur en tapant la commande suivante



2.- Installez certains packages requis

Il est maintenant nécessaire d'installer certains packages nécessaires pour poursuivre l'installation d'OSSEC. Par exemple, wgetpour le télécharger et build-essentialpour compiler le programme.



Ensuite, vous pouvez continuer.

# 3. Installez le serveur Web Apache

OSSEC nécessite un serveur Web pour exécuter son agent Web. Il existe de nombreuses alternatives, mais j'utiliserai [Apache](https://www.osradar.com/how-to-install-apache-gui-on-debian-9/)



Ensuite, activez et démarrez le service.



# 4. Installez PHP et d'autres packages

L'étape suivante consiste à installer PHP. [PHP](https://www.osradar.com/how-to-install-php-7-on-centos-7-in-an-easy-way/) est un langage de programmation pour le web. J'utiliserai cette section pour installer d'autres packages utiles et nécessaires pour OSSEC.

# 

# 5. Téléchargez et installez OSSEC

Il est maintenant temps d'installer OSSEC dans Ubuntu, mais vous devez d'abord le télécharger

# 

# On passe à la décomréssion

# 

# Ensuite, entrez dans le dossier décompressé et lancez le script d'installation. Regardez les images pour répondre correctement aux questions. Tout d'abord, choisissez la langue d'installation.

# 

# 

Une fois le script lancé, entrez « fr » au premier choix pour lancer l’installation en français.

Complétez les questions comme ci-dessous, vous pouvez modifier certaines réponses afin d’adapter à votre infrastructure:

# 

# Suite des questions

# 

# On continu jusqu’à présent à répondre les questions suivantes

# 

# Après avoir appuyer sur entrer on passe à l’installation du système

# 

# La fin de l’installation de notre serveur ossec

# 

# On redémarre notre système

# 

# L’installation du serveur est terminée.

# 

# Enfin, l'installation se terminera. Vous verrez cela.

# 

# Alors, démarrez le service OSSEC

# 

# L’interface graphique de ossec

# 

# Installation de l’agent sur une autre machine ubuntu

# 

# On dézipe avec la commande suivante

# 

# On va aller dans le répertoire hids

# 

# Après on install agent en tapant la commande *sh install.sh*

# 

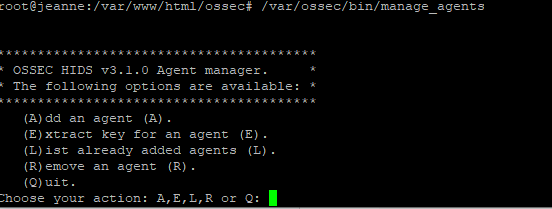
# Suite des réponses

# 

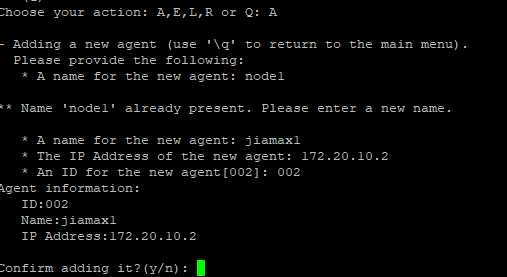
# Suite

# 

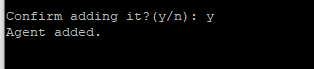
# Après l’installation notre agent, on passe à l’ajout d’un nœud sur le serveur ossec an tapant la commande suivante que j’ai appelé *jiamax1*



Et on fait entrer l’option A pour ajouter un agent

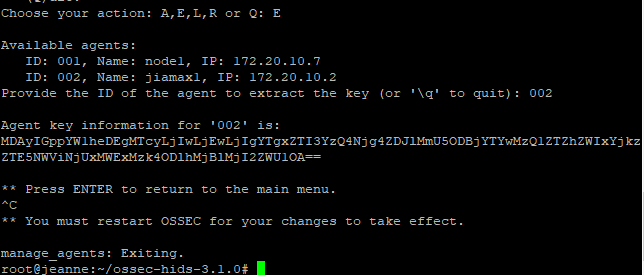


# Après faire tout cela on fait entrer ‘y’ pour ajouter l’agent au serveur



# Si on appuie sur l’option on aura à configurer un nœud pour l’agent avec comme nom jiamax1, l’adresse ip de l’agent et comme ID 002,après

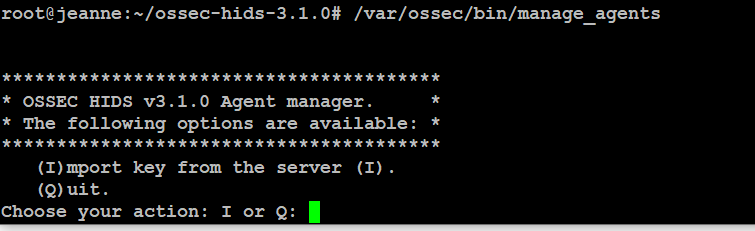
On appuie sur E pour avoir la clé de l’agent sur le serveur ossec



Après avoir générer la clé de l’agent , on le copie quelque part pour l’importer sur l’agent afin les deux puissent se voir

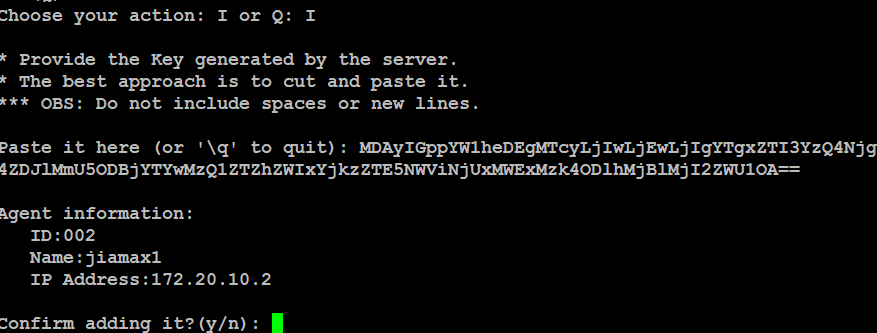
### Importer la clé du serveur OSSEC

Ensuite, vous devrez importer la clé de l'agent extraite sur le serveur vers la machine de l'agent OSSEC. Tout d'abord, connectez-vous à l'instance de l'agent OSSEC et exécutez la commande suivante :en tapant la commande suivante

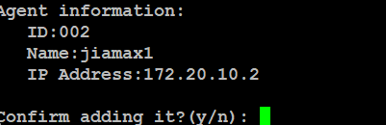


# Sélectionnez I pour importer la clé depuis le serveur. Vous verrez la sortie suivante

# Collez la clé générée sur le serveur et appuyez sur Entrée. La sortie suivante s'affiche :



# Collez la clé générée sur le serveur et appuyez sur Entrée. La sortie suivante s'affiche :



# Sur l'instance du serveur OSSEC, vous pouvez lister les agents actifs en exécutant la commande suivante :

# 

# Appuyez sur y et appuyez sur Entrée pour confirmer la clé. Après cela, votre serveur et votre agent OSSEC sont maintenant configurés pour communiquer entre eux. Ensuite, redémarrez le service OSSEC sur les deux instances pour appliquer les modifications :

# Sur le serveur ossec

# 

# Sur l’agent ossec

# 

# Maintenant, on va ouvrir notre navigateur Web et tapez l'URL http://172.20.10.4/ossec. Vous serez redirigé vers l'interface web OSSEC à la page suivante :

# Après on ajoute l’agent au serveur ossec

# 

# On voit que le serveur ossec a deux agents pour le premier c’est celui du localhost et pour le deuxième c’est l’agent que j’ai appelé jiamax

# Installation de l’ossec agent windows

# 

# On appuie next

# 

# On passe à l’installation

# 

# Après on crait un agent sur le serveur appelé nodeWind

# 

# On génére la clé de l’agent nodeAgent

# 

# On confirme l’adresse ip du serveur et la clé de l’agent

# 

# Après le client peut voir le serveur

# 

# Etudes comparative des outils Ossec et snort

|  |  |  |
| --- | --- | --- |
| Point de différence | SNORT | OSSEC |
| Définition | Snort est un système gratuit et open source de prévention des intrusions sur le réseau et un système de détection des intrusions sur le réseau. | Ossec est l'un des HIDS le plus utilisés. Il est très facile d'accès tant pour l'installation que pour l'utilisation. |
| Travail | Renifle les données en temps réel | Vérifier les fichiers journaux pour les détections des menaces |
| Prix | Plage entre 29,99Dollard et 399Dollar | Ses frais d’intallation sont 80,16Dollard |
| Alert | Alerte avec six modes comme le mode rapide, complet, consol, | Via syslog, email et Json |
| Caractéristique | Evolutivité, moteur de détection modulaire et déploiement flexible | Log bases,rootkit et malware avec audit de conformité |
| Avantages | -- Surveillance sans agent des périphériques de réseau – Outils de réduction du bruit configurables et système d’alerte – Filtrage et suppression – Seuils d’alerte configurables | effectue l’analyse des slogs, la vérification de l’intégrité, la surveillance du registre Windows, la détection du kit racine, les alertes basées sur le temps et la réponse active |
| Outil payant ou gratuit | Gratuit | Gratuit |

|  |  |  |  |
| --- | --- | --- | --- |
| Points de  différence  outils | Payant | Non payant | Définition |
| Nmap | Non | oui | Nmap est un scanner de ports open source créé par Fyodor et distribué par Insecure.org. |
| Metasploit | Non | oui | **Metsploit est un outil pour le développement et l'exécution d'exploits contre une machine distante.** |
| Nessus | non | Il est gratuit et propose un essay gratuit | **Nessus** est le scanner de vulnérabilité réseaux de Tenable Network Security. |