ELOIFI BADR
BIRABAKARAN SUBISAN

TP – MISE EN PLACE DE OSSEC

SÉCURITÉ – PROMO224

INTRODUCTION :

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. Un agent est installé sur chacune des machines.

Le serveur OSSEC est le centre de l'architecture. C'est lui qui va stocker les bases de données de vérification, les journaux ou encore l'intégrité des fichiers. L'ensemble des règles sont centralisées sur le serveur, ce qui offre une facilité d'administration.

L'agent OSSEC est le programme qui va être installé sur les systèmes à surveiller, celui-ci va utiliser le port 1514 (udp) pour se connecter au serveur. Il va collecter des informations sur ces systèmes et les transmettra au serveur pour analyse. Certaines informations sont collectées en temps réel, d'autres périodiquement.

Et nous avons une machine linux nous permettant d'attaquer le serveur web avec Nmap.

I. INSTALLATION ET CONFIGURATION DU SERVEUR OSSEC

Tout d'abord nous commençons par mettre à jour notre serveur avec les commandes suivante :

```
#apt-get update
#apt-get upgrade
```

Nous installons ensuite les prérequis :

```
#apt-get install build-essential inotify-tools ntp
```

Nous téléchargeons ensuite le fichier d'installation à l'aide de la commande « wget ». Le lien peut changer, nous vous invitons donc à aller sur le site d'OSSEC pour obtenir le nouveau :

```
#Wget https://github.com/ossec/ossec-hids/archive/3.1.0.tar.gz
```

Une fois l'archive téléchargée, nous la décompressons à l'aide de la commande « tar » :

```
#tar xf 3.1.0.tar.gz
```

En allant ensuite dans le dossier « ossec-hids-3.1.0 » grâce à la commande « cd », on lance l'installation d'OSSEC :

```
#cd ossec-hids-3.1.0
#./install.sh
```

```
1- Quel type d'installation voulez-vous (serveur, agent, local ou aide) ? serveur

  - Installation du serveur choisie.

2- Définition de l'environnement d'installation.

 - Choisissez votre répertoire d'installation de OSSEC HIDS [/var/ossec]:

    - L'installation sera faite sur  /var/ossec .

3- Configuration de OSSEC HIDS.

 3.1- Voulez-vous une alerte par email ? (o/n) [o]: n

  --- Alerte par email désactivée.

 3.2- Voulez-vous démarrer le démon de vérification d'intégrité ? (o/n) [o]: o

  - Lancement de syscheck (démon de vérification d'intégrité).

 3.3- Voulez-vous démarrer le moteur de détection de rootkit ? (o/n) [o]: o

  - Lancement de rootcheck (détection de rootkit).

 3.4- La réponse active vous permet d'éxécuter des commandes
      spécifiques en fonction d'évènement. Par exemple,
      vous pouvez bloquer une adresse IP ou interdire
      l'accès à un utilisateur spécifique.
      Plus d'information sur :
      http://www.ossec.net/en/manual.html#active-response

  - voulez-vous démarrer la réponse active ? (o/n) [o]: o

    - Réponse active activée.

  - Par défaut, nous pouvons activer le contrôle d'hôte
    et le pare-feu (firewall-drop). Le premier ajoute
    un hôte dans /etc/hosts.deny et le second bloquera
    l'hôte dans iptables (sous linux) ou dans ipfilter
    (sous Solaris, FreeBSD ou NetSBD).
  - Ils peuvent aussi être utilisés pour arrêter les scans
    en force brute de SSHD, les scans de ports ou d'autres
    formes d'attaques. Vous pouvez aussi les bloquer par
    rapport à des évènements snort, par exemple.

  - Voulez-vous activer la réponse pare-feu (firewall-drop) ? (o/n) [o]: o

    - pare-feu (firewall-drop) activé (local) pour les levels >= 6

  - liste blanche (white list) par défaut pour la réponse active :
     - 127.0.0.1

  - Voulez-vous d'autres adresses IP dans votre liste (white list) ? (o/n)? [n]: n


 3.5- Voulez-vous activer fonctionnalité syslog (port udp 514) ? (o/n) [o]: n

  --- Fonctionnalité syslog désactivé.

 3.6- Mise en place de la configuration pour analyser les logs suivants :
   -- /var/log/auth.log
   -- /var/log/syslog
   -- /var/log/dpkg.log
```

Une fois le chargement terminé, nous utilisons la commande suivante pour lancer OSSEC :

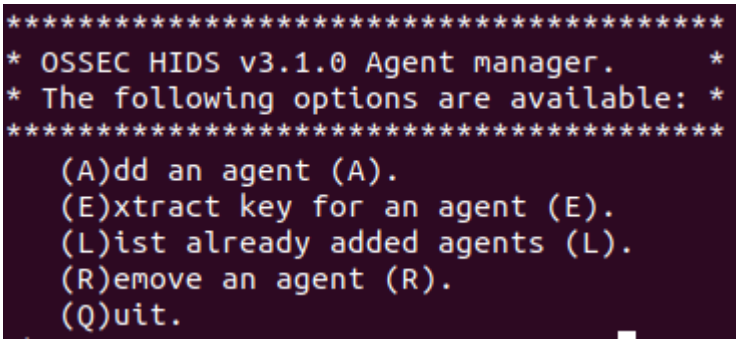
```
# /var/ossec/bin/ossec-control start
```

II. INSTALLATION ET CONFIGURATION DE L'AGENT OSSEC

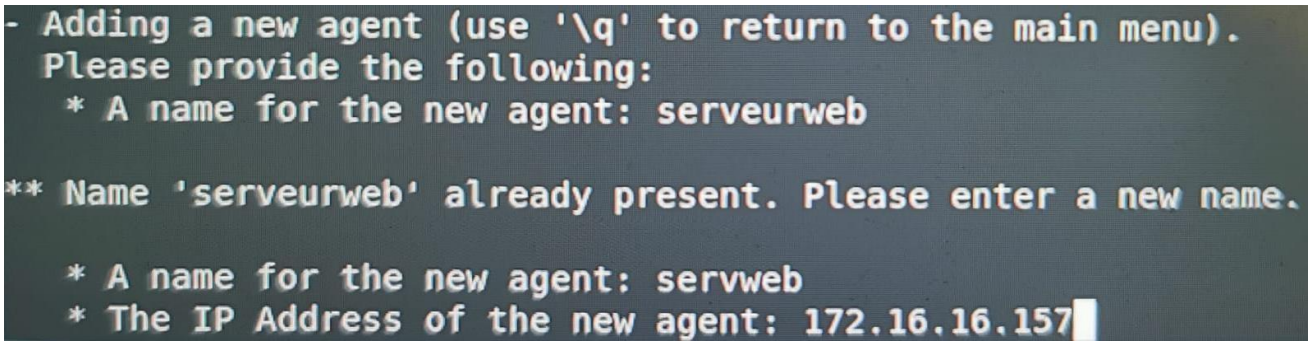
Nous commençons par configurer les agents coté serveur avec la commande suivante pour lancer le manager d'agents :

```
#/var/ossec/bin/manage_agents
```

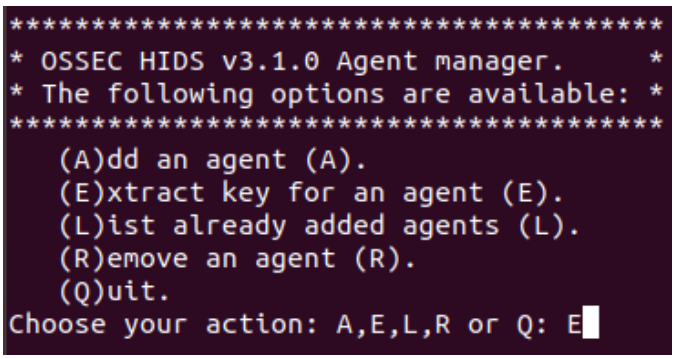
On entre « A » pour ajouter l'agent du client Linux :



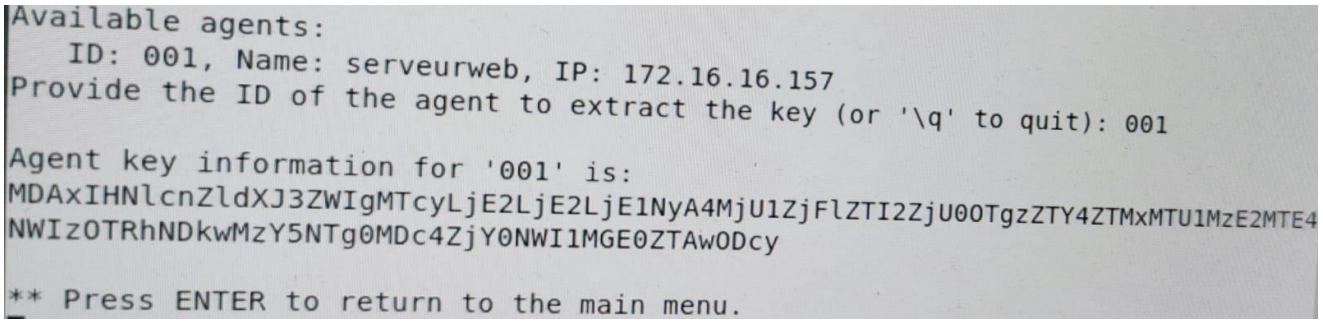
Nous définissons le nom de l'agent et l'adresse IP correspondant à l'adresse IP du client :



Pour récupérer la clé associée, nous saisissons « E » dans le menu :



Nous renseignons ensuite le numéro d'agent associé au client Linux pour obtenir la clé :



Nous passons ensuite sur le client pour le mettre à jour avec les commandes suivantes :

```
#apt-get update
#apt-get upgrade
```

Comme sur le serveur nous installons ensuite les prérequis :

```
#apt-get build-essential inotify-tools ntp
```

Nous téléchargeons ensuite le fichier d'installation et décompressons l'archive avec la commande « tar » :

```
#Wget https://github.com/ossec/ossec-hids/archive/3.1.0.tar.gz
#tar xf 3.1.0.tar.gz
```

En allant ensuite dans le dossier « ossec-hids-3.1.0 » grâce à la commande « cd », on lance l'installation d'OSSEC :

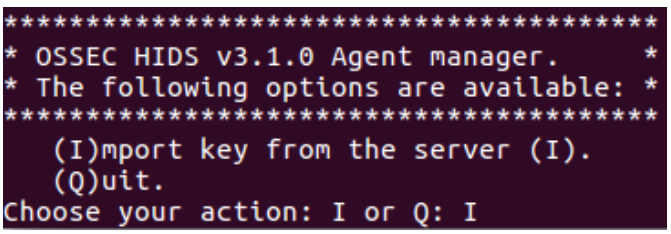
```
#cd ossec-hids-3.1.0
#./install.sh
```

Au contraire de tout à l'heure nous choisissons « agent » et nous complétons les informations.

Une fois l'agent installé, nous allons devoir ajouter la clé présente sur le serveur :

```
# /var/ossec/bin/manage-agents
```

On entre « I » pour importer la clé :



Après avoir collé la clé mise de côté auparavant et confirmez l'ajout et une fois le chargement terminé, on utilise la commande suivante pour démarrer ***OSSEC*** sur le client :

```
#  /var/ossec/bin/ossec-control start
```

Et on redémarre le service sur le serveur aussi :

```
#  /var/ossec/bin/ossec-control restart
```

Pour vérifier que l'agent est bien connecté au serveur, on utilise la commande suivante :

```
# /var/ossec/bin/agent_control -lc
```

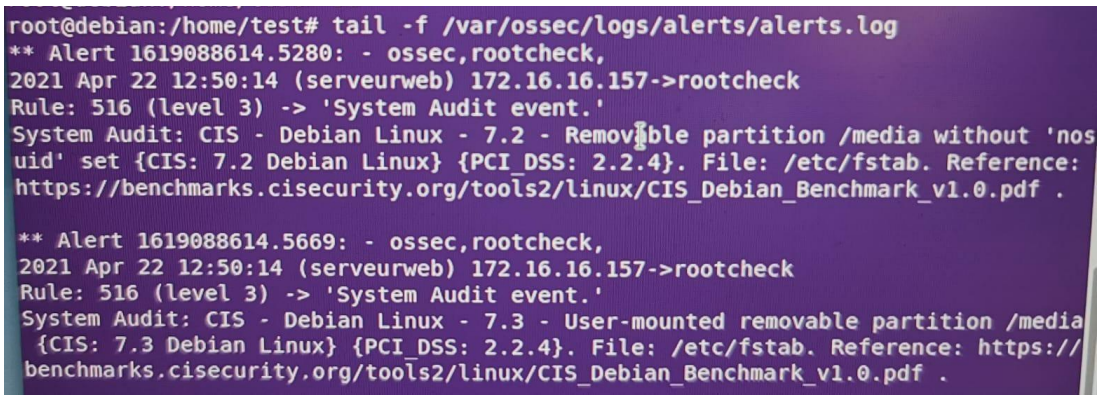
III. PARTIE ATTAQUE AVEC NMAP

A l'aide de la machine attaque et la commande Nmap nous attaquons le serveur web pour voir s'il arrive à la détecter :

```
# Nmap -sV 172.16.16.157
```

Puis sur le serveur nous vérifions le fichier de consultations des alertes avec la commande suivante :

```
# tail -f /var/ossec/logs/alerts/alerts.log
```



ANNEXE :

A. ANATOMIE D'UNE ATTAQUE :

Fréquemment appelés « les 5P » dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique : Probe, Penetrate, Persist, Propagate, Paralyze.

Probe : consiste en la collecte d'informations par le biais d'outils comme whois, Arin, DNS lookup. La collecte d'informations sur le système cible peut s'effectuer de plusieurs manières, par exemple un scan de ports grâce au programme Nmap pour déterminer la version des logiciels utilisés, ou encore un scan de vulnérabilités à l'aide du programme Nessus.

Penetrate : utilisation des informations récoltées pour pénétrer un réseau. Des techniques comme le brute force ou les attaques par dictionnaires peuvent être utilisées pour outrepasser les protections par mot de passe. Une autre possibilité pour s'infiltrer dans un système est d'utiliser des failles applicatives que nous verrons ci-après.

Persist : création d'un compte avec des droits de super utilisateur pour pouvoir se réinfiltrer ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot (ex. : un cheval de Troie).

Propagate : cette étape consiste à observer ce qui est accessible et disponible sur le réseau local.

Paralyze : cette étape peut consister en plusieurs actions. Le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur.

B. LOGICIEL POSSIBLE POUR MIEUX SECURISER UN SERVEUR WEB :

Pour les serveurs web, il existe un outil nommé Nikto qui permet de rechercher les failles connues ou les problèmes de sécurité. C'est un scanner de vulnérabilités web écrit en perl et sous licence GPL. Il va permettre de tester la sécurité de la configuration de votre serveur web (les options HTTP, les index, les failles XSS potentielles, injections SQL etc…)

Il y a aussi des outils comme firewalk, hping ou SNMP Walk permettent quant à eux de découvrir la nature d'un réseau.

WEBOGRAPHIE

https://doc.ubuntu-fr.org/ossec
https://www.mytinydc.com/blog/ossec-installation/
https://all-it-network.com/ossec/
https://dbprog.developpez.com/securite/ids/