INSTALACION Y CONFIGURACION

SIEM

En el presente ejercicio se ha instalado la OVA de Wazuh 4.8.1, la cual una vez actualizada ha pasado a su versión 4.9.0, procediendo a su configuración para poder ser observada en su entorno GUI, en el navegador de mi Kali, configurando como agentes (NXlog) a la mencionada maquina y a la metaesploitable3, con la finalidad de recopilar y analizar los registros de datos de estos dispositivos, generándose alertas configuradas. Se ha seguido los siguientes pasos:

1. Se realiza las descarga, importación y actualización de la ova de Wazuh:

2. Se configuran ambas maquinas en la mismas RED NAT para que exista comunicación entre ellas, siendo la termina en 5 la metaesploitable3 y la terminada en 15 el servidor de Wazuh:

3. Se conecta por ssh con la maquina Wazuh desde la Kali, para una mayor comodidad, conectando con el archivo principal de configuración de Wazuh, al cual se accede a través de ”sudo *nano /var/ossec/etc/ossef.conf*” , agregándole *l*a IP del servidor de Wazuh.

4. Se procede a comprobar los permisos de los certificados necesarios para la conexión SSL/TLS, ejecutando *“ls -ltr /etc/wazuh-indexer/certs” y* “*ls -ltr /etc/wazuh-dashboard/certs”* (certs, son las carpetas donde se guardan los certificados tanto del *módulo indexer y dashboard*), confirmando que no tienen los permisos necesarios, modificando los mismos *“chmod 644 /etc/wazuh-indexer/certs/*.pem”:*

```
[root@wazuh-server ~]# sudo chmod 600 /etc/wazuh-indexer/certs/*.pem
[root@wazuh-server ~]# ls -ltr /etc/wazuh-indexer/certs
total 20
-rw------- 1 wazuh-indexer wazuh-indexer 1229 Jun  6 17:53 wazuh-indexer.pem
-rw------- 1 wazuh-indexer wazuh-indexer 1708 Jun  6 17:53 wazuh-indexer-key.pem
-rw------- 1 wazuh-indexer wazuh-indexer 1184 Jun  6 17:53 root-ca.pem
-rw------- 1 wazuh-indexer wazuh-indexer 1107 Jun  6 17:53 admin.pem
-rw------- 1 wazuh-indexer wazuh-indexer 1704 Jun  6 17:53 admin-key.pem
```

```
[root@wazuh-server ~]# sudo chmod 644 /etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem
[root@wazuh-server ~]# sudo chmod 644 /etc/wazuh-dashboard/certs/root-ca.pem
[root@wazuh-server ~]# sudo chmod 644 /etc/wazuh-dashboard/certs/wazuh-dashboard.pem
[root@wazuh-server ~]# ls -ltr /etc/wazuh-dashboard/certs
total 12
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard 1184 Jun  6 17:53 root-ca.pem
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard 1233 Jun  6 17:53 wazuh-dashboard.pem
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard 1704 Jun  6 17:53 wazuh-dashboard-key.pem
[root@wazuh-server ~]#
```

5. Se accede al archivo de configuración del módulo Wazuh-Indexer, el cual se encuentra en *“etc/wazuh-indexer/opensearch.yml”,* donde se modifica el *“network.root” con la dirección IPV4:* 0.0.0.0, es decir para el que servidor pueda escuchar todas las interfaces, el *“http.port: 9200”,* así como el host y el puerto de transporte

   El puerto 9200 es usado por Wazuh-indexer (similar al opensearch) para consultas externas, siendo un puerto fundamental para las comunicaciones de las aplicaciones externas (dashboard, API, etc…) con su motor de búsqueda, donde se alama cenan los logs y eventos de seguridad, es decir, es el puerto a través del que se realizan las consultas de datos con los datos almacenados en Wazuh-Indexer.

```
#escucha todos las interfaces
network.host: 0.0.0.0
#puerto predeterminado
http.port: 9200
#Ip del servidor de WAZUH
transport.host: 10.0.2.15
#Puertos para el trasnport
transport.port: 9300-9400
```

   Por otro lado, el host y puerto de transporte de Wazuh-Indexer, son necesarios para configurar la comunicación interna entre los diferentes nodos de Wazuh-Indexer, siendo éste, el componente básico de Wazuh que ejecuta tareas de almacenamiento. Además, garantizan la correcta operación del/los clústeres/s, los cuales esta formados por un conjunto de nodos que trabajan juntos en la gestión de grandes volúmenes de datos dentro de Wazuh.

6. Se accede al archive de configuración de Wazuh-dashboard, accediendo a través de las ruta “*etc/wazuh-dashboard/opensearch_dashboards.yml”,* estableciendo el server.host para que el dashboard pueda escuchar cualquier IP y el puerto que utilizará para la conexión la interfaz GUI del dashboard a través del navegador (se puede establecer otro puerto).

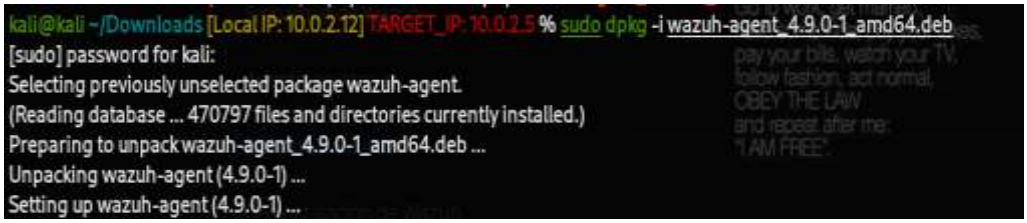
También se establece el hosts para la comunicación interna entre Wazuh-dashboard y Wazuh-indexer, como se explicó anteriormente.

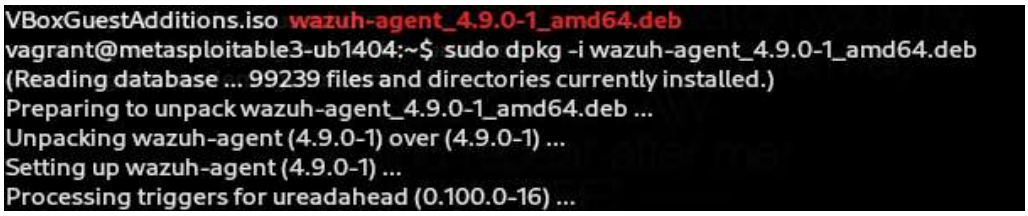
7. Una vez acabada la configuración se restauran los tres módulos de Wazuh y se comprueba sus estados, estando todos en perfecto funcionamiento.

8. Se procede a comprobar la interfaz GUI a través del navegador de la Kali, a través de la URL:https://10.0.2.15:5601, siendo resultado positivo, pero aun no habiendo ningún agente instalado.

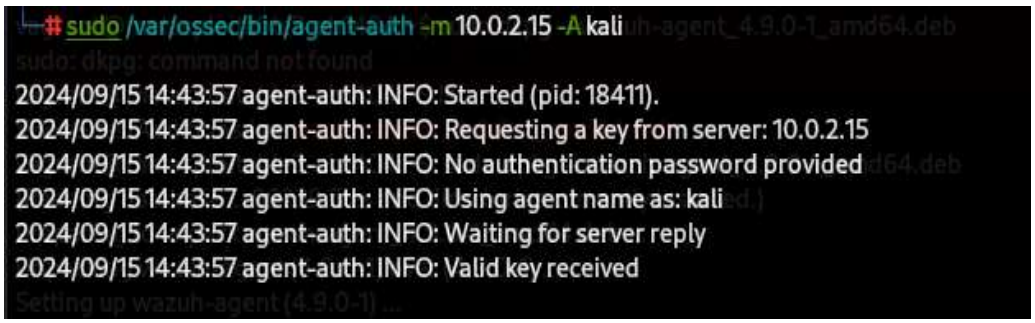
9. Una vez acabado con el servidor de Wazuh, ahora se van a configurar los *"Wazuh-agents"* para la Kali y para la Metasploitable 3, llevando a cabo las siguientes acciones en cada una de las maquinas:

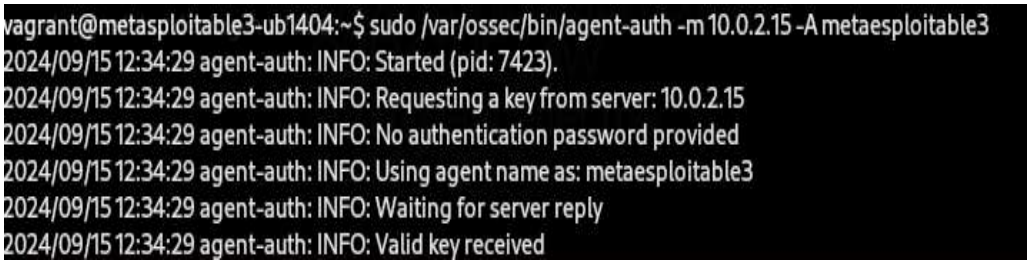
    - Descarga e Instalación:





    - Activación de la Key para cada agente, siendo una credencial única que genera la API de Wazuh para la autenticación de nuevos dispositivos (Kali y metaexploitable3):





Con el comando *"sudo /etc/ossec/bin/agent-auth -m xxx -A xxx"*, es la manera de agregar manualmente a un nuevo agente en el Wazuh-manager, usando la ruta completa para ejecutar el comando *"agent-auth"* (no incluida en el PATH del sistema), el cual se encarga de autenticar al nuevo agente, y las opciones -m y -A, es usan para déficit la IP del servidor Wazuh-manager y dar el nombre al nuevo agente, respectivamente.

- Configuración de los Wazuh-agents en sus archivos sitos en "*/var/ossec/etc/ossef.conf* ", cambiando el campo "MANAGER_IP" por la IP de nuestro servidor :10.0.2.15, dentro de los tags *"address":*

- Restauración y comprobación:

10. Resultado final de todas las operaciones, es la correcta instalación y configuración predeterminada con dos agentes Wazuh (Kali y metaeexploitable3):