GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DEL HIDS WAZUH

1. Instalamos *VirtualBox*: https://www.virtualbox.org/

2. Importamos la OVA proporcionada en el archivo *.zip* de la entrega. **Fijamos la memoria base del sistema en un valor dentro de la franja verde**. Para ello vamos a: **Sistema** en el menú de la izquierda. Si ejecutamos la máquina una vez importada y obtenemos un error del adaptador de red, simplemente accede al apartado **Red** en la izquierda y selecciona el adaptador correspondiente a tu host.

3. Conexión de agentes servidor/cliente. Para ello descargamos el agente cliente para el sistema operativo que tengamos, en nuestro caso *Windows 10*. En el siguiente enlace puede encontrar dicho agente, y además, para otros sistemas operativos anfitriones distintos:

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html

4. Iniciamos OVA de Wazuh e introducimos credenciales de acceso, **usuario: *wazuh-user*, contraseña: *wazuh***. Una vez dentro del sistema nos hacemos *super user* con: **sudo su**, ya que sin ser *super use*r no podremos acceder a los archivos binarios del HIDS.

5. Accedemos a la ruta de los binarios del HIDS: ***cd /var/ossec/bin***. Una vez en la ruta ***bin,*** haciendo un ***ls*** podremos comprobar todos los comandos que podemos ejecutar para el monitoreo.

6. Lo primero es hacer la conexión cliente-servidor a través del comando: ***./manage_agents*** el cual lanzará una consola interactiva que nos permitirá: **(A)ñadir un agente nuevo y (E)xtraer clave para un agente** aportando el ID correspondiente entre otras opciones. Para añadir la IP del agente introducimos la ip del sistema anfitrión, que si es Windows usaremos el comando: ***ipconfig*** para verla**.** La clave extraída la tendremos que copiar a mano o en su defecto emplear alguna aplicación como google Lens desde el teléfono y asegurarnos que está bien escrita.

7. Ejecutamos con ***permisos de administrador*** el archivo ***win32ui.exe*** de la ruta: **C:*\ossec-agent\win32ui.exe** previamente descargado en el paso 3.

8. Con el comando: ***ip a*** en el agente servidor obtenemos la ip. Dicha ip será ingresada en el campo *Manager ip* en el agente cliente lanzado en el paso anterior.

9. La clave de autenticación que se solicita en el siguiente campo del agente cliente se obtiene siguiendo el paso 6 en el agente servidor. Una vez los dos campos rellenados hacemos click en ***save*** y nuestros agentes estarán correctamente enlazados. Para comprobarlo podemos hacer click en ***View*****>view Config** y veremos que aparece en la sección ***<server>*** del archivo de configuración ***ossec.conf***. Será necesario reiniciar *Wazuh* mediante el comando: ***./wazuh-control restart*** disponible en la ruta: ***/var/ossec/bin***. Después hacemos click en ***Manage>Restart*** y comprobamos que aparece ***Status: Running***. Finalmente reiniciamos el servicio de *Wazuh* desde el agente servidor mediante el comando: ***systemctl restart wazuh-manager.service***

10. Si se han seguido todos los pasos correctamente deberíamos poder introducir en la URL de nuestro navegador lo siguiente: ***https://IP AGENTE SERVIDOR*** , dicha ip obtenida en el paso 8, y nos aparecerá el ***dashboard*** de *Wazuh* el cual nos pedirá los siguientes credenciales: ***usuario: admin, contraseña: admin*****.**

11. Una vez dentro del dashboard tendremos los agentes enlazados, disponibles y activos que hayamos creado disponibles para ser monitoreados.

12. Para indicar el directorio con los ficheros que queremos monitorear tendremos que añadir una entrada en el archivo ***ossec.conf*** del agente cliente dentro de las etiquetas ***<syscheck>*** tal que:

<syscheck>

<directories check_sha256sum="yes" report_changes="yes" realtime="yes" recursion_level="5">Ruta del directorio a monitorear del agente cliente</directories>

<directories>...</directories> <!-- Resto de directorios que siguen en el archivo - ->
<syscheck>

y por otro lado tendremos que añadir otra entrada al final del archivo ***ossec.conf*** en la ruta ***/var/ossec/etc*** del agente servidor entre las etiquetas ***<localfile>*** con la ruta del directorio del agente cliente para indicarle qué tiene que monitorear, entre las etiquetas ***<location>***. Quedaría algo así:

<localfile>

<log_format>syslog</log_format>

<location>Ruta del directorio a monitorear del agente cliente</location>

</localfile>

13.- Finalmente para que recibamos notificaciones en un correo determinado cuando se produzcan cambios en la integración se lo indicaremos en el archivo ossec.conf del agente servidor al comienzo de dicho archivo. Este paso y todos los relacionados con los archivos de configuración pueden verse en la siguiente imagen de ejemplo para ver como quedaría.