Procedimiento de instalación y configuración de servidor Wazuh sobre Ubuntu 22.04

Necesidad:

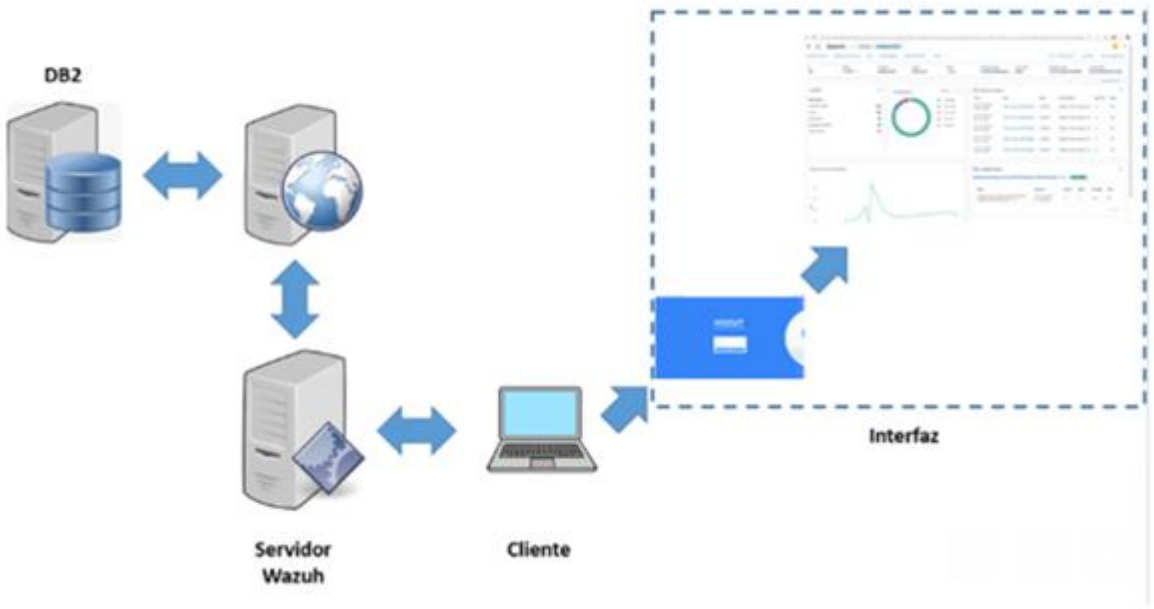
Monitorear a los usuarios privilegiados.

Propuesta:

Detectar cambios en el servidor principal, mediante el monitoreo de los accesos y el monitoreo de la integridad de los archivos (creación, eliminación, modificación).

Para lo anterior se propone la instalación de un servidor de monitoreo (identificado como "Servidor Wazuh" en el diagrama), el cual tendrá la herramienta de monitoreo.

La herramienta se denomina "Wazuh", herramienta Open Source que implementa un EDR mediante la instalación de agentes ligeros en los servidores a monitorear.



Se realizó un "laboratorio" mediante máquinas virtuales (en VMWare Workstation) mediante un servidor Wazuh sobre Ubuntu 22.04 "monitoreando" un servidor Windows 2016

Instalación del Servidor Wazuh

Partiendo de una instalación de un servidor Ubuntu 22.04 se realiza:

```
apt-get install inet-tools

apt-get update

apt-get upgrade
```

```
apt-get install apache2

systemctl restart apache2

apt install openssl
```

Posteriormente se hace la instalación de Wazuh

```
apt install vim curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg2

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh

bash ./wazuh-install.sh –a
```

Si termina satisfactoriamente nos indicará el usuario administrador y la contraseña generada, por ejemplo:

```
User: admin
Password: <contraseña que se genera>
```

Con esto se ha terminado la instalación del servidor.

Ahora, en el servidor a monitorear (Windows), en caso de tener salida a Internet se ejecuta desde una ventana de PowerShell (con privilegios de administrador) lo siguiente:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile ${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='<ip del servidor wazuh>' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='<nombre del servidor a monitorear>' WAZUH_REGISTRATION_SERVER='<ip del servidor wazuh>'
```

Si el servidor no tiene salida a Internet se debe descargar en otro equipo el ejecutable del agente desde el siguiente URL:

https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi

Una vez descargado, en el servidor a monitorear, se ejecuta desde una ventana de PowerShell (con privilegios de administrador) lo siguiente:

```
msiexec.exe /i wazuh-agent-4.7.5-1.msi /q WAZUH_MANAGER='<ip del servidor wazuh>' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='<nombre del servidor a monitorear>' WAZUH_REGISTRATION_SERVER='<ip del servidor wazuh>'
```

NOTA: Es necesario "validar" esta instalación, ya que en la prueba se realizó mediante salida a Internet.

Al terminar la instalación (en ambos casos de los indicados anteriormente) se debe iniciar el servicio mediante:

```
NET START WazuhSvc
```

Ahora para definir un directorio y/o archivo a monitorear iremos (en el servidor a monitorear) al directorio: C:\Program Files (x86)\ossec-agent y editando el archivo ossec.conf (con permisos de administrador) se debe localizar la sección <syscheck> realizando los siguientes cambios:

En la sección <frequency> se indica el tiempo (en segundos) en que se realizará el monitoreo de integridad, por default está configurado a 12 hrs:

```
<frequency>43200</frequency>
```

Ahora para agregar un directorio a monitorear (para este ejemplo será c:\privado) se inserta una línea con:

```
<directories check_all="yes">c:\privado</directories>
```

NOTA: Lo que se busca es que se monitoree el directorio donde está instalado el software a monitorear del servidor principal.

Al concluir, se ejecuta desde una ventana de PowerShell (con privilegios de administrador) lo siguiente:

```
Restart-Service -Name wazuh
```

Para lo relacionado al monitoreo de logon fallidos y exitosos es necesario configurar esto en el servidor a monitorear, para ello:

Win+R
gpedit.msc

Configuración de auditoría:

En el panel izquierdo -> Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Directiva de auditoría -> Auditar eventos de inicio de sesión.

Dar doble clic en esa política y en la ventana de propiedades, marcar las casillas Correcto y Erróneo.

Realizar los mismos para la opción de Auditar eventos de inicio de sesión de cuenta.

Aceptar para guardar los cambios.

Ahora en una ventana de MS-DOS (con permisos de administrador) escribir:

gpupdate /force

Podemos validar tecleando:

auditpol /get /category:*