Práctica Monitorización

PRÁCTICA REALIZADA POR
ALEX DOLS

Parte 1: Windows 8.1

Configurar Windows 8.1

Empezaremos la práctica teniendo una máquina virtual (VBox) con Windows 8.1 instalada.

Para empezar vamos a descargar el fichero “Configure-Win81.bat” del siguiente repositorio:

https://github.com/Xandler/Monitorizacion/blob/master/Configure-Win81.bat

Una vez descargado lo ejecutaremos como administrador.

SYSMON

Ahora descargaremos e instalaremos SYSMON. Lo podemos descargar del siguiente enlace:

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

También nos descargaremos el fichero de configuración XML del repositorio y lo guardaremos en la misma ruta que SYSMON:

https://github.com/Xandler/Monitorizacion/blob/master/SysmonConfig.xml

Ejecutaremos CMD en modo administrador y nos dirigiremos a la ruta donde lo hemos instalado.

Ejecutaremos el siguiente comando:

sysmon -accepteula -i

sysmon –c sysmonconfig.xml

Revisando que SYSMON funcione

Para revisar que esté bien configurado, deberemos acceder al visor de eventos de Windows (eventvwr.exe) y nos desplazaremos a la siguiente ruta:

"Applications and Services Logs/Microsoft/Windows/Sysmon/Operational"

Nxlog

Por último descargaremos y configuraremos nxlog.

Para descargarlo lo haremos desde el siguiente enlace:

https://nxlog.co/products/nxlog-community-edition/download

Nos descargaremos el fichero de configuración del repositorio:

https://github.com/Xandler/Monitorizacion/blob/master/nxlog.conf

Una vez descargado lo moveremos a la siguiente ruta:

C:\Program Files (x86)\nxlog\conf

Una vez movido deberemos editarlo indicando la ip que tenga nuestro equipo Ubuntu.

Debemos fijarnos que en mi caso lo he instalado en program files (x86). En caso de no ser así deberemos cambiar también la ruta para que apunte al sitio correcto.

Finalmente vamos a reiniciar el servicio nxlog con el siguiente comando (como administrador):

net start nxlog

Parte 2: Ubuntu 14

Configurar Ubuntu 14

Vamos a descargar los scripts de configuración de Ubuntu 14 y de la instalación de Splunk del repositorio:

https://github.com/Xandler/Monitorizacion/blob/master/Configure-Ubuntu14.sh

https://github.com/Xandler/Monitorizacion/blob/master/InstallSplunk.sh

Ejecutaremos los siguientes comandos desde el terminal:

cd "ruta donde se hayan descargado los scripts"

sudo chmod u+x Configure-Ubuntu-14.sh InstallSpunk.sh

sudo ./Configure-Ubuntu-14.sh

sudo ./InstallSpunk.sh

Una vez instalado vamos a configurar el rsyslog. Para ello iremos a: ***/etc/rsyslog.conf*** y des comentaremos las siguientes líneas:

$***ModLoad imudp***

$UDPServerRun 514

Ahora que hemos configurado rsyslog vamos a reiniciar el servicio para que aplique los cambios realizados. Para ello utilizaremos el siguiente comando:

Sudo service rsyslog restart

Revisando que rsyslog funcione

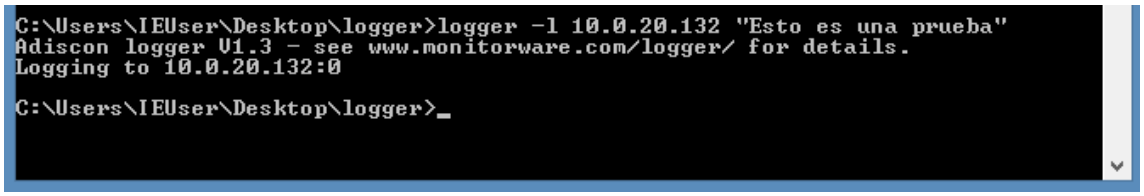
En Ubuntu ejecutamos lo siguiente:

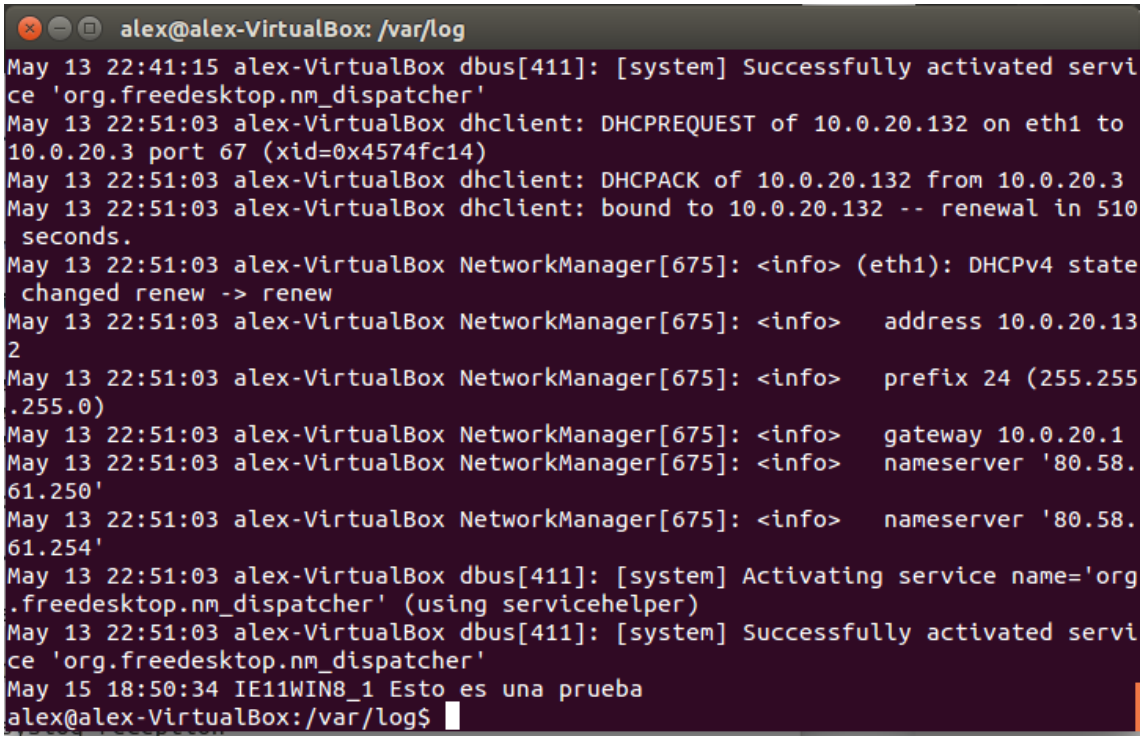
Tail –f /var/log/syslog

Minetras se está ejecutando, en Windows podoemos abrir una ventana de comandos en modo administrador y mandar un mensaje con Logger utilizando el siguiente comando:

Logger –l (ip de Ubuntu) "Esto es una prueba"

Automáticamente en Ubuntu deberíamos recibir dicha notificación. Quedaría algo como lo siguiente:





Parte 3: Splunk

Configurar Splunk

Ya tenemos configurado Windows (con SYSMON y nxlog), Ubuntu (con rsyslog) y ya hemos instalado Splunk así que nos falta configurarlo.

Para ello accederemos a: ***http://127.0.0.1:8000***

Deberemos seguir todas las instrucciones que nos indican. Al final de todo nos dejan elegir la versión de Splunk que queremos configurar. (En mi caso he elegido la gratuita).

Una vez configurado deberemos desplazarnos a ***Add Data / Moitor / Files & Directories***

Pulsaremos en ***Browse*** y seleccionaremos la ruta ***/var/log .*** Los siguientes campos los podemos dejar por defecto.

Al acabar esta configuración nos mostrará toda la información que vaya registrando Windows y que hemos configurado para que nos muestre.

SI queremos verlo de una manera más bonita y ordenada, podemos crear un ***dashboard***.

Para ello iremos a la parte de arriba de la web de Splunk y pulsaremos en "***dashboard"***.

Crearemos un dashboard nuevo. Le pondremos el nombre y una descripción que queramos.

Luego creraemos un panel. En mi caso utilizaré "Nuevo" y la categoría de "Eventos".

Deberemos poner un título de panel y qué queremos que se muestre.

Por ejemplo podríamos indicar que se muestre todo lo que pueda del ordenador Windows 8.1.

Host="IE11Win8_1"

Poniendo los comandos adecuados podremos crear paneles donde nos muestre las conexiones IP's realizadas desde el equipo Windows, o las aplicaciones que ejecute el usuario "IEUser".