LABORATORIO DE REDES Y SISTEMAS OPERATIVOS

TEMA:

“KALIBROWSER”

ALUMNOS:

PATRICIO OTEL,
RIPOLI FERNANDO,
LÓPEZ SUSANA MARIEL.

Fecha de entrega: 14/07/2016

KALIBROWSER

Introducción:

El uso de una máquina virtual es una ventaja para diferente tipo de actividades. Que sea de acceso remoto la vuelve una herramienta más versátil ya que se puede utilizar en cualquier otro equipo sin tener que recurrir a la instalación de los paquetes o de requerir al usuario a utilizar Linux/Windows/otros como sistema operativo principal.

El objetivo principal del equipo fue lograr instalar el programa docker y hacer que este levante una imagen de kali linux para docker, llamada KaliBrowser.

¿Qué es KaliBrowser?

KaliBrowser es una imagen de docker diseñada para ser ligera, solo tiene algunas herramientas de kali linux y no posee GUI. Esta imagen es necesaria para poder utilizar kali en docker, y se la hizo más pequeña para que sus requisitos sean menores.

Kali se utiliza para realizar auditorías de seguridad informática, el poder usarla a través de docker, nos permite utilizarla sin la necesidad de instalarla en una partición o requerir correrla en un live USB.

Desarrollo:

Para hacerla funcionar hay que tener en cuenta que corre los siguientes paquetes:

§ noVNC: cliente VNC (basado en HTML5) para conectarnos a cualquier servicio remotamente sin necesidad de instalar software adicional en el equipo, y a través de cualquier navegador.

§ OpenBox: gestor de ventanas libres de gran rapidez, ya que fue diseñado para consumir una mínima cantidad de recursos

§ docker.io: empaqueta una aplicación y sus dependencias en un contenedor virtual que se puede ejecutar en cualquier servidor Linux. Esto ayuda a permitir la flexibilidad y portabilidad en donde la aplicación se puede ejecutar, ya sea en las instalaciones físicas, la nube pública, nube privada, etc.

En la terminal escribimos para instalarlos:

```
>sudo apt-get install novnc
>sudo apt-get install openBox
>sudo apt-get install docker.io
```

Es importante recordar que además de instalar los paquetes requeridos, la versión del kernel de nuestra máquina debe ser el apropiado (mayor a la versión 3.10). Para revisar la versión utilizamos el siguiente comando en nuestra terminal:

```
>uname –r
```

De acuerdo a la documentación de docker para probar que este funcionando correctamente se suele hacer un container de hello world a través de la terminal, de esta manera:

```
>sudo docker run hello-world
```

Al tratar de correr este container de docker o intentar ver la versión del mismo (`>docker version`)nos topamos con un error que no era lo suficientemente claro para saber qué era lo que nos faltó. El error era:

> “CanNot connect to the docker daemon is the docker daemon running on this host”

Este mensaje de error, nos llevó a investigar sobre servicios en linux, como levantar el daemon de docker. El cual, según diferentes páginas webs y conocimientos previos nos condujo al siguiente comando de la terminal:

```
>service docker start
```

Al hacer esto notamos que el servicio ya estaba levantado. Hay fue cuando nos dimos cuenta que el mensaje de error no era certero.

En este punto, mediante la documentación de docker, logramos llegar a la conclusión que habíamos pasado por alto la creación de un grupo docker para agregarles nuestro usuario al mismo. Lo quisimos crear mediante:

```
>sudo groupadd docker
```

Nos figuró que el grupo ya existía por defecto. A lo que procedimos a la creación de nuestro usuario dentro del mismo.

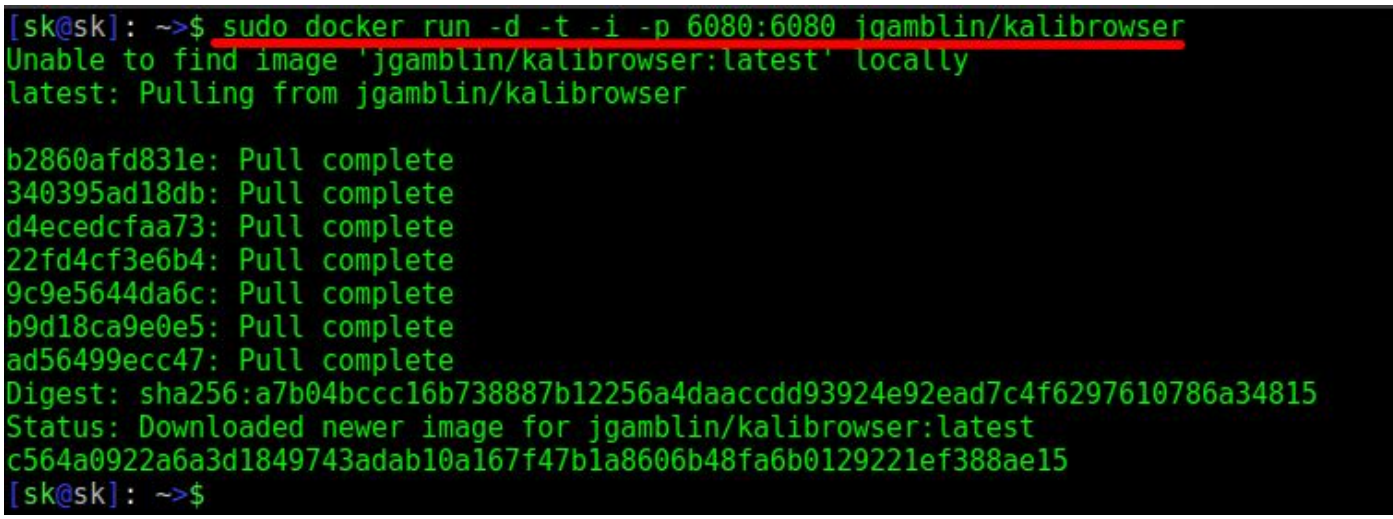
```
>sudo usermod –aG docker pato
```

En este caso “pato”, es el hostname y docker es el nombre del grupo al que queremos agregar nuestro usuario(si el grupo no existe debe ser creado previamente).

Procedimos a reiniciar el equipo(necesario para agregar al grupo). Luego de reiniciar la computadora el error había desapareció.

Finalmente corrimos la imagen de KaliBrowser , al ser esta la primera vez, se empezó a descargar la imagen.

```
>docker run –d –t –i –p 6080:6080 jgamblin/kalibrowser
```



En la imagen se puede ver el comando que se ejecutó, y además, como no se encontró localmente, docker descargo la imagen. Este comando es la combinación de otros dos(docker create y docker start), lo que hace es crear un container y luego lo inicia en el puerto 6080

Y ahora acceder desde un navegador a la máquina virtual nos dirigimos a la direccion **http://localhost:6080** o **0.0.0.0:6080** en nuestro caso.

Luego de comprobar que esto funcionó dentro de la máquina en la cual efectuamos toda la instalación y configuración, pasamos a probar entrar a la misma máquina virtual desde otro equipo, el cual contaba con un sistema operativo Windows. Para poder entrar nos fijamos la IP de la máquina en la que nos encontrábamos trabajando, la copiamos como dirección en el navegador y al final agregamos el puerto al que nos queríamos conectar (aprendimos que a esta combinación se la llama socket).

Cuando quisimos tener la máquina virtual abierta en los dos equipos notamos que no era posible, ya que habíamos dejado las configuraciones por defecto.

Y para finalizar repetimos el proceso para asegurarnos que no haya nuevos inconvenientes, como era de esperarse si los hubo.

Cada vez que en la terminal escribimos los comandos para iniciar el conteiner tanto el de kalibrowser como el de helloworld, que nosotros creíamos que siempre era él mismo, en realidad nos creaba uno nuevo en vez de continuar con el que habíamos trabajado la primera vez. Esto se observa al listar los containers con el comando:

```
>docker ps -a
```

Esto nos llevó a investigar cómo "nombrar" a nuestro docker para poder invocarlo en vez de crear uno nuevo.

```
>docker run –d –t –i –p 6080:6080 --name
nombreDeseado jgamblin/kalibrowser
```

de esta manera podemos hacer

```
>docker start nombreDeseado
```

y para detenerla

```
>docker stop nombreDeseado
```

lamentablemente siempre que iniciamos un container con su nombre, en vez de su identificador obtenido con el comando `ps` el servicio se cierra solo al cabo de unos segundos.

Conclusión:

El uso de docker con kalibrowser permite utilizar herramientas para auditorias que no estarían disponibles en otros sistemas operativos sin grandes complicaciones. Esto también se complementa al usarlo de manera remota ya que puede llegar a facilitar trabajos

grupales que necesiten acceso a estas herramientas, dando así un espacio de trabajo fácil de fácil acceso.