Módulo 0

Redes y Seguridad

Grado Inf. Informática

J.L. Vázquez Poletti

Objetivo

En este módulo aprenderemos a lanzar máquinas virtuales con **VirtualBox** de una forma sencilla, así como una serie de comandos que nos serán útiles en el resto de prácticas de la asignatura.

Punto de partida

Antes de enfrentarnos a los supuestos de la asignatura, necesitamos adquirir los conocimientos básicos de Linux o confirmar que disponemos de los mismos. Para ello, realizaremos esta práctica en el mainframe de la subdivisión Third Echelon.

Lanzamiento de máquinas virtuales

Debido a las restricciones de seguridad de la Facultad, las prácticas de la asignatura se realizarán en máquinas virtuales. Éstas ya están preparadas y están esperando a que se arranquen según la práctica que toque.

El hipervisor escogido es **VirtualBox** y las imágenes de las máquinas virtuales se encuentran en el directorio **RyS** en la partición especial que se notifica una vez se abre sesión (ubicado en **`/mnt/`**).

La aplicación de gestión de máquinas virtuales se abre con el icono de **VirtualBox** que hay en el escritorio. Como hasta el momento no se ha arrancado ninguna, tampoco hay ninguna registrada en el gestor.

1. Copiar al escritorio el directorio **RyS-ThirdEchelon**. Esta operación se deberá realizar para cada práctica con las máquinas virtuales indicadas.
2. Arrastrar el archivo **.vbox** a **VirtualBox**.

NOTA: el fichero **.vbox** es una descripción de las características de la máquina virtual (imagen, procesador, interfaces de red, …).

La máquina virtual ahora aparecerá registrada en **VirtualBox**. En la columna de la derecha se pueden desplegar las propiedades de la misma y haciendo doble click en ella, se procederá a su arranque.

IMPORTANTE: Antes de copiar los directorios de las máquinas virtuales con las que se trabajará en cada práctica, será necesario hacer espacio borrando las **máquinas de la asignatura previamente registradas** y que no se vayan a necesitar. El borrado se realizará desde el mismo **VirtualBox** (botón derecho encima de la máquina, **"Eliminar"** y **"Eliminar todos los archivos"**).

Máquinas Virtuales

- RyS-ThirdEchelon (ubuntu:reverse)

Obteniendo información de los comandos

Preguntar a los compañeros y buscar en Google son una buena idea, pero no siempre disponemos de conexión a Internet.

1. La mayoría de los comandos admiten el parámetro **--help** o **-h**. Obtener información de los comandos **ls**, **cat** y **tee**.
2. También la mayoría de los comandos disponen de una página de manual a la que se puede acceder ejecutando **man <COMANDO>**. Para salir del mismo hay que pulsar la tecla **q**. Obtener información de los comandos anteriores.

Gestión de procesos

El comando para visualizar los procesos es **ps**. Con el parámetro **-ef** podremos ver todos los procesos que se ejecutan en el sistema.

1. En una terminal ejecutaremos **sleep 500** (esperar 500 segundos) y en otra ejecutaremos **ps –ef | grep sleep** para localizarlo.
2. ¿Qué procesos está ejecutando nuestro usuario (**ubuntu**)?

Con **pgrep** obtenemos el PID (identificador) del proceso que le pasemos como argumento.

1. ¿Qué PID tiene el proceso asociado al **sleep**? Es posible que haya que volver a ejecutarlo.

El comando **kill** manda por defecto la señal de apagado (equivalente a pulsar **CTRL+C**) al proceso cuyo identificador de proceso (PID) le pasemos.

1. Apagar el proceso del **sleep**.
2. Al comando **pkill** sólo se le debe pasar el nombre del proceso y no su identificador. Volver a ejecutar **sleep 500** y matarlo con **pkill**.

Podemos ejecutar procesos en segundo plano al pasarle al completar el comando con el símbolo **&**.

1. Lanzar **sleep 500** en segundo plano. Ponerlo en primer plano ejecutando **fg**.
2. Lanzar **sleep 500** en primer plano. Parar el proceso con **CTRL+Z** y luego pasarlo a segundo plano con **bg**.

Sistema de ficheros

El comando **ls** nos permite visualizar el contenido del directorio que le pasemos como parámetro (por defecto, en el que estamos ubicados).

1. Listar el contenido del directorio raíz (`/`).
2. Averiguar qué parámetro se necesita para obtener la mayor información en el listado.
3. Averiguar qué parámetro permite mostrar los archivos ocultos (probar

en el directorio del usuario: **/home/ubuntu/**)

El comando **cd** nos desplaza por el árbol de directorios y **pwd** nos muestra en qué directorio estamos.

Las rutas absolutas son aquellas que parten del directorio raíz y por tanto comienzan por **/**. Las relativas lo son desde el directorio en el que nos encontramos y por tanto no empiezan por **/**.

Si ejecutamos **cd** sin suministrarle un parámetro, iremos al directorio del usuario.

1. Desplazarnos al directorio **/etc** dando su dirección absoluta y ejecutar **pwd**.
2. Desplazarnos al directorio raíz y de ahí, al **/etc** usando su dirección relativa. Ejecutar **pwd**.

El comando **mkdir** crea un directorio con el nombre que le facilitemos.

El comando **mv** mueve un archivo/directorio desde un origen a un destino que le pasemos como parámetro. Por otro lado, **cp** copia el archivo/directorio.

El comando **rm** borra archivos.

1. Crear dos directorios en el directorio del usuario llamados **nsa** y **3ech**.
2. Mover **3ech** dentro de **nsa**.
3. Ejecutar **touch** para colocar un archivo llamado **bug** dentro de **nsa**.
4. Ejecutaremos **rm *** (borrar todo) dentro de **nsa**. ¿Qué sucede?
5. Volveremos a colocar el archivo **bug** y esta vez borraremos con los parámetros **-Rf**.

IMPORTANTE: El comando **rm * -Rf** ejecutado en un lugar equivocado puede tener consecuencias catastróficas.

Redirección y encadenamiento de comandos

Con el símbolo **>** redirigimos la salida estándar de un comando a un archivo que indiquemos. Si usamos **2>**, se redirigirá la salida de error.

1. Redirigir la salida del listado de archivos que hay en el raíz a un archivo llamado **output** en el directorio del usuario.
2. Redirigir la salida de error de visualizar el archivo **/etc/shadow** con el comando **cat** a un archivo llamado **error** en el directorio del usuario.

Podemos encadenar la salida de un comando con la entrada de otro empleando el símbolo **|** (conocido también como pipe).

3. Redirigir la salida del listado de archivos que hay en el raíz a un archivo llamado **output** en el directorio del usuario.

Visualización y edición de archivos de texto

El comando **more** se emplea para visualizar archivos de texto largos (que ocupan más de una pantalla). Con **retorno** y **f** avanzamos páginas, con

espacio avanzamos líneas y con **b** retrocedemos páginas. Para salir, pulsaremos **q**.

1. Visualizar el fichero **/var/log/dmesg** y navegar por él.

Tenemos varios editores para elegir. Entre ellos están **nano** y **vim.tiny** (o **vim** según el sistema). Es fundamental hacernos a uno de estos para las prácticas.

2. Crear un archivo de texto en nuestro directorio de usuario.
3. Introducir nuestros datos personales (uno por línea), guardar los cambios y salir.
4. Volver a abrir el archivo y borrar la penúltima línea. Guardar y salir.
5. Añadir **(RyS)** a continuación del nombre (en la misma línea). Guardar y salir.