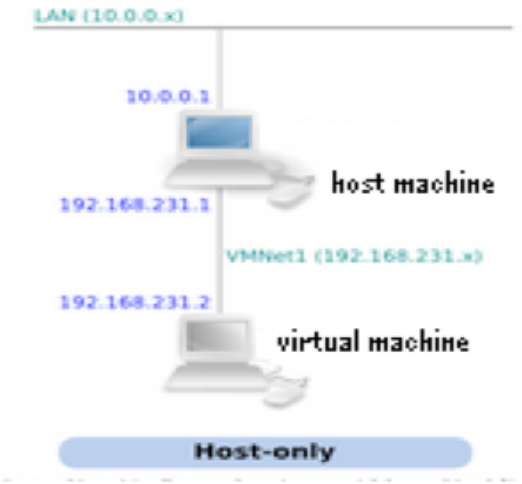
Seguridad de los Sistemas Informáticos

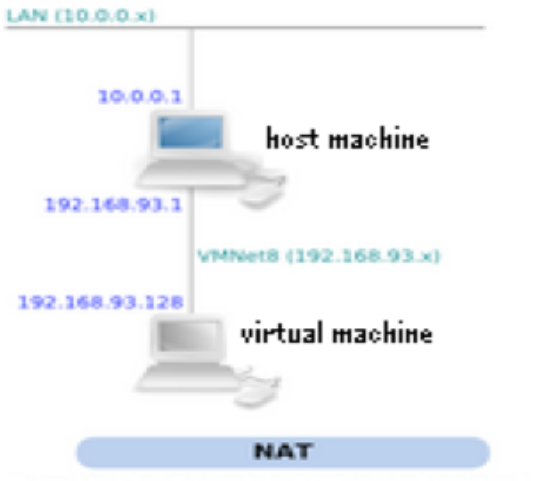
PARTE 2: Seguridad en Linux: Preparación del Entorno

Objetivos de aprendizaje

- Crear y configurar de manera adecuada una máquina virtual, incluyendo su interfaz de red.
- Instalar un sistema operativo Linux.
- Llevar a cabo las tareas post-instalación necesarias sobre un sistema Linux.
- Manejar las órdenes básicas del sistema Linux y trabajar con los distintos ficheros de configuración del mismo.

Infraestructura a utilizar





- **Bridged**: La máquina virtual está conectada directamente a la red real. **Será la que utilizaremos.**
- **NAT**: se conecta a una red virtual que sale al exterior a través de la máquina real utilizando NAT.
- **Host-only**: se conecta sólo con la máquina real.
- **LAN segment**: sólo útil para VPNs o grupos máquinas virtuales.

Trabajo post-instalación

- Tras la instalación básica es conveniente actualizar el sistema.

- Para todas estas tareas se necesitan privilegios administrativos (orden *sudo*).

- Toda distribución Linux suele tener algún mecanismo para facilitar la actualización e instalación de software *(gestor de paquetes*). En ubuntu es ***aptitude***.

Trabajo post-instalación: aptitude

Órdenes varias

Búsqueda de paquetes: `apt-cache search nombre`

Instalación de paquetes: `install paquete`

Desinstalación de paquetes: `apt-get remove paquete`

Actualizar base de datos de paquetes: `apt-get update`

Saber si un paquete está instalado: `aptitude show nombre`

Listado de paquetes instalados: `dpkg --get-selections`

Actualización de todos los paquetes instalados: `apt-get upgrade`

Actualización del sistema a una nueva distribución: `apt-get dist-upgrade`

Trabajo post-instalación: aptitude

Actualización del sistema

Siempre que queramos realizar una operación con aptitude, es aconsejable actualizar la base de datos de paquetes.

```
apt-get update
```

Una vez actualizada la base de datos, podemos actualizar todo el software instalado utilizando:

```
apt-get upgrade
```

Importante: esta operación sólo actualiza el software gestionado por *aptitude.* Si hemos instalado algo de forma manual, deberemos actualizarlo siguiendo el procedimiento indicado por el fabricante de ese software.

Instalación de software adicional

Para esta primera parte de las prácticas, trabajaremos en modo texto.

Sí es interesante instalar las herramientas de desarrollo de programas (nos harán falta para el paso siguiente). Para ello instalaremos el paquete *build-essential:*

```
apt-get install build-essential
```

Visión general de un sistema Linux

Para poder defender un sistema, el primer paso es conocerlo lo mejor posible:

- Las órdenes básicas de manejo del sistema.
- La estructura del sistema de ficheros.
- Los ficheros de configuración más importantes.

Linux: Órdenes básicas

`ls -lart:` muestra el contenido del directorio actual.

`pwd:` muestra el directorio actual

`touch fichero:` crea un fichero vacío o actualiza la fecha/hora de acceso del fichero.

`rm fichero:` borra el fichero.

`shred fichero:` sobreescribe el contenido del fichero.

`cd directorio:` cambia el directorio actual.

`hostname:` muestra el nombre del host.

`ifconfig -a:` muestra la configuración de los interfaces de red.

`cat fichero:` muestra el contenido del fichero.

`less fichero:` muestra, paginándolo, el contenido del fichero

`head/tail fichero:` muestra el principio/fin del fichero.

`history:` muestra las últimas órdenes introducidas.

`dmesg`: muestra los mensajes del arranque del sistema.

Linux: Órdenes básicas

`script` *`fichero:`* crea un fichero de log con la actividad realizada hasta introducir la orden `exit`.

`strings` *`fichero`*: muestra el fichero, eliminando los caracteres no imprimibles.

`date`: muestra la fecha y hora del sistema.

`man` *`orden`*: muestra información sobre esa orden.

`find` *`ruta expresión`*: busca ficheros a partir de la ruta indicada que cumplan la expresión.

`grep` *`patrón fichero:`* muestra las líneas del fichero que contienen el patrón.

`df` *`directorio:`* calcula lo que ocupa el directorio y todo su contenido.

`du:` muestra el uso del disco.

`mount:` lista los puntos de montaje.

`sudo` *`orden:`* ejecuta la orden con privilegios administrativos.

Linux: Órdenes básicas

`mkdir directorio:` crea el directorio indicado.

`chmod` ***`perm fichero:`*** cambia los permisos de acceso del fichero indicado.

`chown` ***`propietario.grupo fichero:`*** cambia el propietario y el grupo del fichero.

`pico, vi, mcedit, nano, …:` editores de texto

`halt`: para el sistema.

`reboot`: rearranca el sistema.

`shutdown`: rearranca el sistema (permite indicar una hora o un intervalo de tiempo).

Linux: File Hierarchy Standard (FHS)

FHS define la estructura y contenido de los directorios en las distribuciones LINUX:

`/dev`: ficheros de dispositivos.

`/bin`, **`/usr/bin`**, **`/usr/local/bin`**: mayoría de órdenes del sistema.

`/sbin`: órdenes de administración.

`/etc`: ficheros de configuración.

`/home`: ficheros propios de los usuarios.

`/mnt`: puntos de montaje.

`/lib`: bibliotecas compartidas.

`/tmp`: ficheros temporales.

`/opt`: software opcional.

`/var`: ficheros de log, de spool, …

`/boot`: ficheros necesarios durante el arranque.

`/proc`: "pseudoficheros" de procesos en ejecución.

Linux: ficheros interesantes

Los siguientes directorios suelen contener los ficheros que se indican:

`/etc/passwd`: usuarios del sistema.

`/etc/group`: grupos del sistema.

`/etc/shadow`: contraseñas de acceso al sistema.

`/etc/sudoers`: usuarios que pueden hacer sudo

`/etc/network/interfaces`: configuración de red.

`/var/log/*`: ficheros de log.

`/etc/init.d/*`: ficheros de control de servicios.

`/etc/hostname:` nombre de la máquina.

`/etc/host.allow, /etc/host.deny:` máquinas a las que se permite/se niega la conexión.

`/etc/hosts:` nombres de máquinas conocidas.

`/etc/fstab:` sistemas de ficheros que se montan al arrancar.

Particionado

- Protección contra errores físicos de disco. Aislar el daño.
- Protección contra escritura de ficheros críticos.
- Optimización y gestión del espacio en disco:
- Cuota de uso del espacio.
- Usar diferentes sistemas de ficheros.
- Cifrado de las particiones individuales.

Niveles de ejecución

- 0 Halt
- 1 Single-user mode
- 2 Multi-user mode
- 3 Multi-user mode with networking
- 4 Not used/user-definable
- 5 Start the system normally with appropriate display manager (with GUI)
- 6 Reboot Reboots the system.

Consejos de seguridad Linux

- Tener el sistema actualizado.
- No usar interfaces gráficas.
- Controlar los procesos que se están ejecutando y desinstalar aquellos que no se utilicen.
- Si utlizamos ssh no permitir el inicio de sesión con root.
- Deshabilitar la posibilidad de conectar unidades de disco usb.
- Deshabilitar el reinicio con Ctrl+Alt+Supr.
- Proteger con contraseñas seguras todos lo elementos posibles: BIOS,GRUB,…