maquina virtual

-es un software que permite emular el funcionamiento de un ordenador dentro de otro ordenador gracias a un proceso de encapsulamiento que aísla a ambos
-Las máquinas virtuales son ordenadores de software que proporcionan la misma funcionalidad que los ordenadores físicos. Como ocurre con los ordenadores físicos, ejecutan aplicaciones y un sistema operativo. Sin embargo, las máquinas virtuales son archivos informáticos que se ejecutan en un ordenador físico y se comportan como un ordenador físico. En otras palabras, las máquinas virtuales se comportan como sistemas informáticos independientes.

Configuracion de la maquina virtual (Debian sin interfaz grafica)
**Debian porque es mas sencillo de configurar y user-friendly que CentOS*
* aptitude -- apt apt (**Advanced Package Tool)** es una herramienta de instalacion/administracion de paquetes y aptitude parecido pero con interfaz en consola (interfaz opcional de curses) y mayor cantidad de herramientas, ejem recuerda dependencias de paquetes que fueron instalados automáticamente al instalar el paquete principal
* SELinux Las distribuciones Linux incorporan MAC mediante módulos de seguridad, como **SELinux** y **AppArmor**. Cada uno tiene sus peculiaridades.
* AppArmor Linux security system that provides Mandatory Access Control (MAC) security. Allows the system admin to restrict the actions that processes can perform. It is included by default with Debian. Run aa-status to check if it is running

-particiones LVM Logical Volume Manager – allows us to easily manipulate the partitions or logical volume on a storage device
`lsblk`

-SSH (solo en puerto 4242) terminal remota
ssh ccalvo-p@127.0.0.1 -p 4242
`systemctl status ssh`
`hostname -i` `en terminal (`virtualmachine`) para ver la ip` adress

-Firewall UFW (puerto abierto 4242)
sudo ufw status verbose (comprobamos estado)

-Hostname de la maquina virtual: ccalvo-p42
`uname -vm` (informacion del sistema)
>modificar el hostname durante evaluacion
hostnamectl (visualiza nombre actual hostname nombre de red de tu servidor)
hostnamectl set-hostname <nombre>
/etc/hosts
127.0.0.1 localhost
127.0.1.1 ccalvo-p42

-Politica de contraseñas fuerte (*)

-Usuarios: root y usuario ccalvo-p (debe pertener a grupos user42 y sudo)
>crear un usuario y asignarselo a un grupo en la evalucaion
sudo adduser <nombre> #Para añadir un usuario
sudo gpasswd -a <nombre> <grupo> `#Para añadir un usuario al grupo`
sudo gpasswd -d <nombre> <grupo> `#Para eliminar un usuario al grupo`

comprobacion: groups <nombre>
saber usuarios de un grupo: getent group <grupo>
en sudo visudo o /etc/sudoers `#Añadir <user_name> ALL=(ALL) ALL`
`Userdel <user name> -r #(eliminar usuario)`

#(*)POLITICA DE CONTRASEÑAS fuerte (para usuarios y root):

se ha modificado la politica de contraseñas:
/etc/login.defs
160 PASS_MAX_DAYS 99999 >30
160 PASS_MIN_DAYS 0 >2
161 PASS_WARN_DAYS 7 >7

-expirar 30 dias (160 PASS_MAX_DAYS 99999 >30)
-min numero dias modificacion contraseña (160 PASS_MIN_DAYS 0 >2)
-mensaje aviso usuario 7 dias (161 PASS_WARN_DAYS 7 >7)

Instalamos una herramienta para implementar dicha politica (**common-password**)

/etc/pam.d/common-password
retry=3 minlen=10 ucredit=-1 dcredit=-1 maxrepeat=3 reject_username enforce_for_root difok=7

-contraseña min 10 caracteress (minlen=10)

-contener mayus (ucredit) y un numero (dcredit) (ucredit=-1 dcredit=1)
-no contener +3 caracter consecuitivo (maxrepeat=3)
-no nombre usuario (reject_username)

-no root. 7 caracteres diferentes respecto a anterior contraseña (difok=7)

DESPUES DE HACER LA CONFIGURACION, SE DEBERAN CAMBIAR LAS CONTRASEÑAS DE TODAS LAS CUENTAS

#CONFIGURACION CONTRASEÑA fuerte para tu grupo sudo (super user do):
SUDO
para visualizar el archivo de configuracion sudo
sudo visudo
/etc/sudoers

-autentificacion con sudo limitado a 3 intentos (Defaults passwd_tries=3)
-mensaje personalizado contraseña incorrecta (Defaults badpass_message="<message>")
-comandos input output archivados en directorio /var/log/sudo/. (Defaults logfile="var/log/sudo/sudo.logs")
(Defaults log_input,log_output; Defaults iolog_dir="/var/log/sudo")
-modo TTY (solo se accede con sudo desde terminal) (Defaults requiretty) tty muestra (escribe a la salida estándar) el nombre de fichero de la terminal de la entrada estándar
-directorios utilizables por sudo restringidos
(Defaults secure_path="usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin")

TTY `requiretty` is set, `sudo` must be run from a logged-in terminal session (a tty). This prevents `sudo` from being used from daemons or other detached processes like cronjobs or webserver plugins. It also means you can't run it directly from an `ssh` call without setting up a terminal session.

ver los logs en /var/log/sudo/sudo.logs

#SCRIPT monitoring.sh
La arquitectura de tu sistema operativo y su versión de kernel.
El número de núcleos físicos.
El número de núcleos virtuales.
La memoria RAM disponible actualmente en tu servidor y su porcentaje de uso.
La memoria disponible actualmente en tu servidor y su utilización como un por- centaje.
El porcentaje actual de uso de tus núcleos.
La fecha y hora del último reinicio.
Si LVM está activo o no.
El número de conexiones activas.
El número de usuarios del servidor.
La dirección IPv4 de tu servidor y su MAC (Media Access Control)
El número de comandos ejecutados con sudo.

Crear script "monitoring.sh" en /usr/local/bin/ (chmod 777)

dar privilegios sudo: sudo visudo (sudoers file)
`ccalvo-p ALL=(root) NOPASSWD:` /usr/local/bin/monitoring.sh

SE EJECUTE CADA 10min (Crontab configuration) usamos crontap para programar tarea command line utility to schedule commands or scripts

#(Crontab configuration)
`sudo crontab -u root -e` to open the crontab and add the rule
`*/10 * * * * /usr/local/bin/monitoring.sh` this means that every 10 mins, this script will show

#COMANDOS a utilizar para comprobaciones
head -n 2 /etc/os-release
en home: /usr/sbin/aa-status (sudo) ->Apparmor status
en home: ss -tunlp
en home /usr/sbin/ufw status

- `sudo ufw status`
- `sudo systemctl status ssh`
- `getent group sudo`
- `getent group user42`
- `sudo adduser new username`
- `sudo groupadd groupname` – add new user group;
- `sudo usermod -aG group username` - add user to user group
- `sudo chage -l username` - check password expire rules
- `hostnamectl`
- `hostnamectl set-hostname new_hostname` - to change the current hostname
- `sudo nano /etc/hosts` - change current hostname to new hostname
- `lsblk` to display the partitions
- `dpkg -l | grep sudo` – to show that sudo is installed
- `sudo ufw status numbered`
- `sudo ufw allow port-id`
- `sudo ufw delete rule number`
- `ssh your user id@127.0.0.1 -p 4242` - do this in terminal to show that SSH to port 4242 is working