LSI P1

PARTE 1

a) Configure su máquina virtual de laboratorio con los datos proporcionados por el profesor. Analice los ficheros básicos de configuración (interfaces, hosts, resolv.conf, nsswitch.conf, sources.list, etc.)

/etc/network/interfaces	Interfaces de red (ens33, ens34, v4av6)
/etc/hosts	Hosts de la máquina
/etc/resolv.conf	Servidores y dominios
/etc/nsswitch.conf	
/etc/apt/sources.list	Fuentes de soporte del SO (Debian 11 Bullseye)

b) ¿Qué distro y versión tiene la máquina inicialmente entregada? Actualice su máquina a la última versión estable disponible.

lsb_release -d	Ver versión actual
cat /etc/*release	Ver versión actual (con detalle)

Última versión estable: Debian 11 Bullseye

c) Identifique la secuencia completa de arranque de una máquina basada en la distribución de referencia (desde la pulsación del botón de arranque hasta la pantalla de login). ¿Qué target por defecto tiene su máquina? ¿Cómo podría cambiar el target de arranque? ¿Qué targets tiene su sistema y en qué estado se encuentran? ¿Y los services?. Obtenga la relación de servicios de su sistema y su estado. ¿Qué otro tipo de unidades existen?

Secuencia de arranque:

1. Ecendido pasa el control de la BIOS, en mem de solo lectura
2. La BIOS hace comprobaciones y obtiene param de mem no volátil
3. La BIOS detecta discos duros y carga el MBR
4. La BIOS ejecuta el gestor de arranque (normalmente grub)
5. El gestor toma el control, busca el kernel , lo carga y ejecuta
6. Se inicia el kernel y monta la partición
7. Se ejecuta el init, que entrega el control al systemd para empezar el proceso de inicio estándar

Anteriormente teníamos graphical.target

Hemos cambiado a multi-user.target

dmesg	Ver secuencia de arranque
systemctl get-default	Ver target por defecto

systemctl set-default xxxxx.target	Establecer nuevo target por defecto
systemctl list-units --type=target	Ver los targets en memoria*
systemctl list-unit-files --type=target	Ver todos los targets instalados*
systemctl list-units --type=service	Ver los services en memoria*
systemctl list-unit-files -–type=service	Ver todos los services instalados*
systemctl list-units	Ver todos los tipos de unidades*

*se les puede añadir | grep enabled (p.ej.)

d) Determine los tiempos aproximados de botado de su kernel y del userspace. Obtenga la relación de los tiempos de ejecución de los services de su sistema.

systemd-analyze	Ver tiempos de arranque userspace + kernel
systemd-analyze blame	Ver relación de tiempos de ejecución de los services

e) Investigue si alguno de los servicios del sistema falla. Pruebe algunas de las opciones del sistema de registro journald. Obtenga toda la información journald referente al proceso de botado de la máquina. ¿Qué hace el systemd-timesyncd?

journalctl -b -p 4	Errores en el arranque actual (“-b” indica en el arranque actual, “-p” la prioridad que queremos, “4” es la prioridad de los errores)* *Podemos añadir | grep error o | grep failed
journalctl -b	Obtener toda la info del arranque actual
systemd-cgls	Esquema de grupos de control de los servicios, indicando los recursos que se asignan a cada uno

f) Identifique y cambie los principales parámetros de su segundo interface de red (ens34). Configure un segundo interface lógico. Al terminar, déjelo como estaba.

ifconfig	Muestra las interfaces activas
Ifconfig -a	Muestra las todas las interfaces
ifconfig ens33 up	Activar interfaz*
ifconfig ens33 down	Desactivar interfaz*
nano /etc/network/interfaces	Para configurar otro interfaz (NO añadir gateway)*

*Después debe hacerse systemctl restart networking

g) ¿Qué rutas (routing) están definidas en su sistema? Incluya una nueva ruta estática a una determinada red.

netstat –rn Ver rutas estáticas definidas en el sistema

Añadir una nueva ruta:*

route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.0.1

Eliminar una ruta:*

route del -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.0.1

*Para que se guarde físicamente hay que añadir al principio “up” o “down”

h) En el apartado d) se ha familiarizado con los services que corren en su sistema. ¿Son necesarios todos ellos? Si identifica servicios no necesarios, proceda adecuadamente. Una limpieza no le vendrá mal a su equipo, tanto desde el punto de vista de la seguridad, como del rendimiento.

systemctl stop/restart xxxxx.target

systemctl disable/enable xxxxx.target

systemctl mask/unmask xxxxx.target

systemctl list-unit-files --type=service Ver todos los servicios

i) Diseñe y configure un pequeño “script” y defina la correspondiente unidad de tipo service para que se ejecute en el proceso de botado de su máquina.

Ruta del script: /usr/bin/myscript.sh

Ruta del servicio: /etc/systemd/system/myservice.service

Fichero creado: /home/lsi/Escritorio/mytime.txt

chmod +x myscript.sh Dar permisos de ejecución

Chmod -

j) Identifique las conexiones de red abiertas a y desde su equipo.

netstat [-4, -6]	Muestra los sockets IPv4/IPv6
netstat -a	Muestra todos los sockets (por defecto los conectados)
netstat -c	Muestra información en tiempo real (listado continuo)
netstat -e	Muestra información extendida
netstat -n	Resuelve nombres
netstat [-t, -u]	Muestra conexiones TCP/UDP

netstat –neta	Las conexiones abiertas

k) Nuestro sistema es el encargado de gestionar la CPU, memoria, red, etc., como soporte a los datos y procesos. Monitorice en "tiempo real" la información relevante de los procesos del sistema y los recursos consumidos. Monitorice en "tiempo real" las conexiones de su sistema.

systemd-cgtop	Información en tiempo real de los procesos
netstat -netac	Información en tiempo real de las conexiones

l) Un primer nivel de filtrado de servicios los constituyen los tcp-wrappers. Configure el tcp-wrapper de su sistema (basado en los ficheros hosts.allow y hosts.deny) para permitir conexiones SSH a un determinado conjunto de IPs y denegar al resto. ¿Qué política general de filtrado ha aplicado? ¿Es lo mismo el tcp-wrapper que un firewall? Procure en este proceso no perder conectividad con su máquina. No se olvide que trabaja contra ella en remoto por ssh.

Un TCP-Wrapper es un sistema que nos permite filtrar el acceso a los servicios de un servidor con un SO Unix. Es como un firewall pero a nivel de aplicación, aunque no trabaja con UDP.

En etc/hosts.allow indicamos a quién permitimos entrar.

En etc/hosts.deny indicamos a quién no dejamos entrar.

m) Existen múltiples paquetes para la gestión de logs (syslog, syslog-ng, rsyslog). Utilizando el rsyslog pruebe su sistema de log local.

Los logs se encuentran en: /var/log

logger -p mail.err "mensaje"	Escribir mensaje en un log (ej. mail.err)
systemctl stop/restart syslog.socket syslog.service	Pausar/reanudar servicio de log

n) Configure IPv6 6to4 y pruebe ping6 y ssh sobre dicho protocolo. ¿Qué hace su tcp-wrapper en las conexiones ssh en IPv6? Modifique su tcp-wapper siguiendo el criterio del apartado h). ¿Necesita IPv6? ¿Cómo se deshabilita IPv6 en su equipo?

Configurado en /etc/network/interfaces y añadido a /etc/hosts.allow

Configuración para habilitar IPv6 en /etc/sysctl.conf

ifup/ifdown red	Levantar o tirar una red
ssh -6 lsi@IP(v6)	Entrar a través de IPv6
ping -6 IP(v6)	Ping a la dirección IPv6

PARTE 2

a) En colaboración con otro alumno de prácticas, configure un servidor y un cliente NTP.

SERVIDOR: JOAQUÍN - CLIENTE: ÁLVARO

(TRAS UN BOOTEADO, EL SERVIDOR TARDA DE 5 A 10 MINUTOS EN ESTABLECER CONEXION CON LOS CLIENTES Y TARDA AL MENOS 1-2 MINUTOS MÁS EN SINCRONIZARSE TOTALMENTE)

ntpdate –u IP	Establecer conexión con el servidor NTP (puede tardar de 5 a 10 minutos en funcionar si el server se ha booteado recientemente)
ntpq -pn -4	Muestra el estado de la sincronización con el cliente.
	Funcionamiento: *when* sube hasta igualar *poll*, entonces se envía la consulta y se actualizan los campos de fecha/hora, *reach* indica el éxito de la consulta.
ntpstat	Muestra el estado de la conexión, si no está aproximadamente sincronizado, muestra “unsynchronised”.

Ruta de configuración: /etc/ntp.conf

Comprobar funcionamiento en cliente:

1. Cambiar la hora de la maquina:

   sudo date --set "07 Dec 2020 13:15"

   date (comprobar hora)

2. Sincronizar con el servidor NTP:

   ntpdate –u 10.11.48.143

   date (comprobar hora)

b) Cruzando los dos equipos anteriores, configure con rsyslog un servidor y un cliente de logs.

SERVIDOR: JOAQUÍN - CLIENTE: ÁLVARO

Realizado por TCP

Puerto elegido para el servidor: 514

Ruta de configuración: /etc/rsyslog.conf

Ruta log del cliente en el servidor: /var/log/logAlvaro (Recomendado usar “tail”)

logger -p mail.err “msg” (CLIENTE) Enviar mensaje al log.

systemctl stop syslog.socket rsyslog.service (SERVIDOR) Parar servicio.

systemctl restart syslog.socket rsyslog.service (SERVIDOR) Reanudar servicio.

c) Haga todo tipo de propuestas sobre los siguientes aspectos.: ¿Qué problemas de seguridad identifica en los dos apartados anteriores? ¿Cómo podría solucionar los problemas identificados?

- NTP:

    1. Se puede hacer ip-spoofing para suplantar la identidad de un cliente. Si dicho cliente tiene privilegios, podrían realizarse consultas para obtener información relevante del sistema → Utilizar sistemas de autenticación en cada consulta aumentaría la desincronización.
    2. La información no está cifrada, por lo que podría interceptarse y reenviar tras un cierto delay, afectando a aplicaciones críticas que dependan del tiempo. Lo mismo si suplantas la identidad del servidor.

- Rsyslog:

    1. Igualmente, se podría spoofear la ip del cliente y saturar al servidor con logs, o bien la del servidor y obtener todo el log del cliente → Autenticación mediante intercambio de keys.
    2. La información no se cifra, por lo que si se intercepta comprometería la seguridad del cliente → Cifrar la información

d) En la plataforma de virtualización corren, entre otros equipos, más de 200 máquinas virtuales para LSI. Como los recursos son limitados, y el disco duro también, identifique todas aquellas acciones que pueda hacer para reducir el espacio de disco ocupado.

du -sh <path> Ver cuánto ocupa el fichero # 4.1G -> 3.8G

- Aplicaciones que no uses: apt-get remove <package>, apt-get autoremove --purge
- Cache apt (/var/cache/apt/archives/*.deb): apt-get clean
- Versiones viejas del kernel (/boot): apt-get autoremove --purge
- Logs (/var/log/): rm *[1-9].log, rm *.gz
- Agrupar logs (/etc/rsyslog.conf): mail.* /var/log/mail.log y comentar el resto
- Editar la rotación de logs (/etc/logrotate.conf): parámetros autodescriptivos.

  Comentar el include u otros parámetros pueden ser superpuestos.
- Eliminar man-db: apt-get autoremove --purge man-db
- Vaciar /tmp: reboot o para los server buscar los archivos que no se estén utilizando
- Vaciar papelera (~/local/share/Trash)
- Eliminar historial del bash (~/.bash_history) y cache (~/.cache)
- Eliminar las páginas en otros idiomas (/usr/share/help)