IP personal: 10.11.48.69 | 10.11.50.69 | 2002:a0b:3045::1

IP Brais: 10.11.48.70 | 10.11.48.70 | 2002:a0b:3046::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
auto lo ens33 ens34
iface lo inet loopback

iface ens33 inet static
address 10.11.48.50
netmask 255.255.254.0
broadcast 10.11.49.255
network 10.11.48.0
gateway 10.11.48.1

iface ens34 inet static
address 10.11.50.50
netmask 255.255.254.0
broadcast 10.11.51.255
network 10.11.50.0

/etc/hosts/ -> resolución de nombres a ips
/etc/resolv.conf -> Archivo para la configuración de los resolvers DNS
/etc/nsswitch.conf -> Fichero de configuración de las Bases de Datos del Sistema y del sistema de Conmutación de los Servicios de Nombre – name service switch
/etc/apt/sources.list -> repositorios/fuente del soporte/seguridad del sistema operativo

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

lsb_release -a: muestra la distro/sistema operativo

uname -r: muestra la version del kernel

uname –a: version del kernel detallada

Actualizamos:

```
# apt update -y && sudo apt upgrade -y
```

apt dist-upgrade (dist-upgrade instala nuevos o elimina)

Se modifica el archivo **/etc/apt/sources.list** con las sources de debian 11

```
# apt upgrade

# apt full-upgrade

# reboot
```

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?.

dmesg

```
0       runlevel0.target, poweroff.target   Shut down and power off
1       runlevel1.target, rescue.target     Set up a rescue shell
2,3,4   runlevel[234].target,               Set up a non-gfx multi-user shell
        multi-user.target
5       runlevel5.target, graphical.target  Set up a gfx multi-user shell
6       runlevel6.target, reboot.target     Shut down and reboot the system
```

```
# systemctl get-default
```

El target por defecto es el grapgical.target, para cambiarlo utilizamos:

```
# systemctl set-default multi-user.target
```

ver targets del sistema(instalados):

```
$ systemctl list-unit-files --type=target
```

ver services del sistema(instalados):

```
$ systemctl list-unit-files --type=service
```

Otro tipo de unidades: **systemctl list-units -t help**

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

systemd-analyze blame

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?.

Para comprobar servicios que han fallado:

systemctl list-unit-files --type=service –failed

 # journalctl -xe | grep fail

Error ntpd:

`/etc/ntp.conf`: añadir la linea:

interface ignore IPv6|all

Error udisks:

systemctl status udisks2
apt-get install libblockdev-crypto2
apt-get install libblockdev-mdraid2
systemctl restart udisks2
systemctl status udisks2

Para ver la informacion del boot actual:

```
# journalctl -b
```

systemd-timesyncd es un servicio del sistema que se usa para sincronizar el reloj local del sistema con un servidor NTP remoto

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 ens34 <ip> netmask <netmask>
ifconfig ens34 up
```

```
root@debian:/home/lsi# ifconfig ens34 down
root@debian:/home/lsi# ifconfig ens34 mtu 1200
root@debian:/home/lsi# ifconfig ens34 hw ether 00:1e:2e:b5:18:07
root@debian:/home/lsi# ifconfig ens34 10.11.50.51 netmask 255.255.254.0
root@debian:/home/lsi# ifconfig ens34 up

para ens34 no tenemos gateway, la red es solo interna
```

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

 # ip route show

```
default via 10.11.48.1 dev ens33 onlink
10.11.48.0/23 dev ens33 proto kernel scope link src 10.11.48.69
10.11.50.0/23 dev ens34 proto kernel scope link src 10.11.50.69
169.254.0.0/16 dev ens33 scope link metric 1000

$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.11.48.1      0.0.0.0         UG    0      0        0 ens33
10.11.48.0      0.0.0.0         255.255.254.0   U     0      0        0 ens33
10.11.50.0      0.0.0.0         255.255.254.0   U     0      0        0 ens34
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33

$ ip route add 10.11.52.0/24 via 10.11.48.1
$ traceroute 10.11.52.2 (para comprobar que el trafico se procesa
correctamente)
$ ip route del 10.11.52.0/24 via 10.11.48.1
```

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 list-unit-files -t service --state=enabled

disable avahi-daemon
disable accounts-daemon
disable NetworkMaganer
disable cups
disable ModemManager
disable bluetooth
switcheroo
wpa_supplicant
ModemManager
open vm tools

`/etc/default/bluetooth-> BLUETOOTH_ENABLED=0`
/etc/bluetooth/main.conf -> AutoEnable=false

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.

/etc/systemd/system/storage-check.service
[Unit]
Description=System storage check on boot
After=multi-user.target

[Service]
ExecStart=/usr/local/bin/storage-check.sh

[Install]
WantedBy=multi-user.target

/usr/local/bin/storage-check.sh

```
#!/bin/bash
date >> /home/disk-storage-status.txt
df -h /dev/sda1 >> /home/disk-storage-status.txt
LIMIT=30
USE=$(echo $(df /  | grep -v 'S.ficheros' | awk '{print $5}' | sed 's/&//g' | cut -d'%' -f1))

if [ $USE  -ge $LIMIT ]; then
                echo "running out of space bobi" >> file.txt
fi
```

systemctl daemon-reload
systemctl enable servicio
systemctl start servicio -> para probarlo sin reboot

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

netstat -netua -> conexiones de red abiertas a y desde su equipo.

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.

top –> procesos en tiempo real
netstat -netuac -> conexiones en tiempo real

l) Un primer nivel de filtrado de servicios los constituyen los tcp-wrappers. Configure el tcpwrapper 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

/etc/hosts.allow:

#loopback
sshd:127.0.0.1: spawn /bin/echo "($(date) - loopback) from %a service %d" >>
/var/log/SSHConnections.txt
#partner - Brais
sshd:10.11.48.70: spawn /bin/echo "($(date) - Brais) from %a service %d" >>
/var/log/SSHConnections.txt
#Eduroam
sshd:10.20.32.0/255.255.252.0: spawn /bin/echo "($(date) - Eduroam) from %a service %d" >>
/var/log/SSHConnections.txt
#VPN
sshd:10.30.8.0/255.255.248.0: spawn /bin/echo "($(date) - VPN) from %a service %d" >>
/var/log/SSHConnections.txt

en el host.deny se puede usar un twist en vez de spawn para reemplazar el servicio solicitado con el comando especificado
spawn lanza el comando

- `%a` — Suministra la dirección IP del cliente.
- `%A` — Suministra la dirección IP del servidor.

- **%c** — Proporciona información variada sobre el cliente, como el nombre de usuario y el de la máquina o el nombre del usuario y la dirección IP.
- **%d** — Proporciona el nombre del proceso demonio.
- **%h** — Suministra el nombre de la máquina del cliente (o la direccción IP, si el nombre de la máquina no está disponible).
- **%H** — Suministra el nombre de la máquina del servidor (o la dirección IP si el nombre de la máquina no está disponible).
- **%n** — Proporciona el nombre de la máquina del cliente. Si no está disponible aparecerá unknown. Si el nombre de la máquina y la dirección de la máquina no se corresponden, aparecerá paranoid.
- **%N** — Proporciona el nombre de la máquina del servidor. Si no está disponible aparecerá unknown. Si el nombre de la máquina y su dirección no coinciden, aparecerá paranoid.
- **%p** — Suministra el ID del proceso demonio.
- **%s** — Suministra información varia del servidor como el proceso demonio y la máquina o la dirección IP del servidor.
- **%u** — Proporciona el nombre de usuario del cliente. Si no está disponible aparecerá unknown.

TCP-Wrappers-> filtro de acceso a la red
Firewall -> trabaja a nivel so, deniega conexiones desde ip a determinados servicios o puertos

primero firewall y despues wrapper

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

logger prueba
logger “prueba2”
tail -2 /car/log/syslog
---------- debian lsi: prueba
---------- debian lsi: prueba2

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?

/etc/network/interfaces

```
auto lo ens33 ens34 6to4
iface 6to4 inet6 v4tunnel
        address 2002:a0b:3045::1
        netmask 16
        endpoint any
        local 10.11.48.69
```

ifup 6to4 -> activa la interfaz
ping6 2002:a0b:3045::1
ssh lsi@2002:a0b:3045::1

Para deshabilitar la ipv6 se añaden las siguientes lineas en **/etc/sysctl.conf**:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Para aplicar los cambios:

```
sysctl -p
```

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

Servidor:

`/etc/ntp.conf`

`# Server`
server 10.11.48.70 minpoll 4
fudge 127.127.1.0 stratum 9

`hosts.allow:`
ntpd: 10.11.48.69

`etc/ntp.conf`
`# Client`
server 10.11.48.69 minpoll 4
fudge 127.127.1.0 stratum 10

restrict source notrap nomodify noquery

noserve : ignorar los paquetes que no consultan o modifican el estado del servidor, esto es, consultas de sincronización de relojes.
nomodify : Ignorar todos los paquetes de esa dirección IP que intentenmodificar el servidor excepto las respuestas a las consultas realizadas, que obviamente modifican la hora del servidor.
noquery : Ignorar todos provenientes de esa dirección IP que soliciten consultas de información o configuración.
nopeer : Proporcionar servicio a esa IP solo si ya se estaba proporcionando servicio a la misma.

Para probar el servidor:
systemctl restart ntp
date +%T -s 1
ntpdate -u 10.11.48.70

ntpq -pn
-n: Output all host addresses in dotted-quad numeric format rather than converting to the canonical host names.

-p: List of the peers known to the server as well as a summary of their state.

-4: Force IPv4 name resolution.

Descripción del output:

remote – The remote peer or server being synced to. “LOCAL” is this local host (included in case there are no remote peers or servers available);
refid – Where or what the remote peer or server is itself synchronised to;
st (stratum) – The remote peer or server Stratum

t (type) – Type (u: unicast or manycast client, b: broadcast or multicast client, l: local reference clock, s: symmetric peer, A: manycast server, B: broadcast server, M: multicast server, see "Automatic Server Discovery");
when – When last polled (seconds ago, "h" hours ago, or "d" days ago);
poll – Polling frequency: rfc5905 suggests this ranges in NTPv4 from 4 (16s) to 17 (36h) (log2 seconds), however observation suggests the actual displayed value is seconds for a much smaller range of 64 (26) to 1024 (210) seconds;
reach – An 8-bit left-shift shift register value recording polls (bit set = successful, bit reset = fail) displayed in octal;
delay – Round trip communication delay to the remote peer or server (milliseconds);
offset – Mean offset (phase) in the times reported between this local host and the remote peer or server (RMS, milliseconds);
jitter – Mean deviation (jitter) in the time reported for that remote peer or server (RMS of difference of multiple time samples, milliseconds);

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

hosts.allow:

rsyslogd: 10.11.48.70

Cliente

```
*.* action(
       type="omfwd"
       target="10.11.48.50"
       port="514"
       protocol="tcp"
       action.resumeRetryCount="-1"
       queue.type="linkedlist"
       queue.filename="/var/log/rsyslog-queue"
       queue.saveOnShutdown="on"
)
```

Probamos el servidor:

```
# systemctl restart rsyslog
```

Cliente:

```
# logger "prueba1"
```

Servidor: `# cat /var/log/rsyslog-server/10.11.48.69/lsi.log`

```
2022-09-28T20:49:58+02:00 debian lsi: prueba1
```

Probamos la cola:

Servidor: se comenta la linea `# input(type="imtcp" port="514")` para que deje de escuchar

```
# systemctl restart rsyslog
```

Cliente:

```
# logger "prueba cola"
```

Se comprueba que no se guarda en el servidor, se descomenta la línea y se vuelve a probar

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?

- En rsyslog se pueden enviar logs hasta llenar el disco, al igual que enviar contenido no deseado ya que los logs no son cifrados.
- Como NTP trabaja sobre UDP, se puede atacar a partir de IP Spoofing

Se asegura la conexión a traves de firewalls y otros mecanismos

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.

Para limpiar el disco se lleva a cabo el siguiente proceso:

- apt autoclean
- apt clean
- apt --purge autoremove
- apt remove –purge man-db
- eliminación de otros paquetes innecesarios
- borrado de kernels antiguos
    - uname -r
    - dpkg --list | grep linux-imag (muestra los kernes actuales)
    - apt-get --purge remove <name> (elimina el kernel especificado)
    - se eliminan todos menos *linux-image-5.10.0-18-amd64* y linux-image-amd64