

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Actividad individual: Fortificación de un sistema

Linux

Objetivos

La actividad va a permitir al alumno poner en práctica los conceptos revisados durante el tema 2 relativos a sistemas Linux. Concretamente el alumno va a fortificar un sistema Ubuntu, restringiendo el acceso a usuarios privilegiados, gestionando de forma segura el acceso a través de SSH, restringiendo la navegación web con un proxy y creando usuarios con permisos determinados.

Descripción

La misma empresa de la actividad anterior nos ha contactado nuevamente para solicitarnos la instalación y configuración segura de una máquina virtual basada en VirtualBox y cuyo sistema operativo sea Ubuntu.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	17-02-2022
	Nombre: Amir Fernando Mamdouh	

Contenido

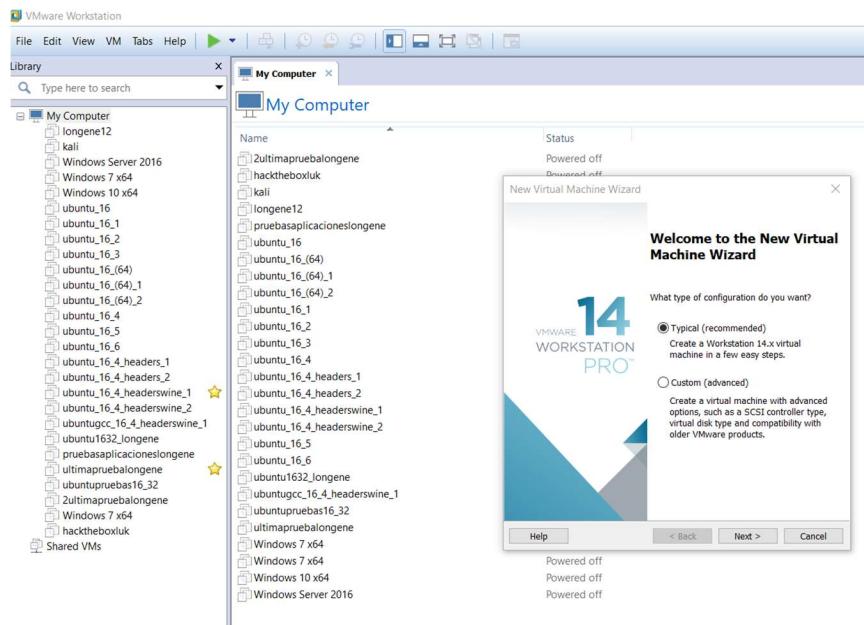
1.	Creación y configuración de la maquina virtual	3
I.	La máquina virtual debe tener 4GB de RAM, 10GB de disco duro y una interfaz de red en modo NAT.....	3
II.	El espacio de usuario, /home, debe estar en un volumen lógico separado.....	6
III.	El disco duro debe estar cifrado con la clave: <i>discoUnir</i>	8
IV.	El usuario creado durante la instalación será <i>unir</i> con una clave <i>SSSOoUnir</i>	10
2.	Instalación y configuración segura del grub	11
V.	El grub debe estar protegido.	11
VI.	Securizar los comandos su y sudo	13
3.	Configuración de IPTables	14
VII.	Se debe tener instalado OpenSSH server	14
VIII.	Configurar IPTables para que solamente acepte conexiones a OpenSSH a través del puerto 22.	16
4.	Script y creación de usuarios y grupos.....	18
IX.	Los usuarios que van a trabajar en la máquina son del área de dirección y de ingeniería. Crear un script que nos solicite el nombre de usuario, la contraseña, su grupo (que si no existe se añadirá) y si es usuario administrador para permitirnos crear usuarios en el sistema. Además, el script debe verificar si el usuario ya existe en el sistema antes de darle de alta.	18
X.	Usando el script anterior, crear el usuario <i>Ingenieriao1</i> no administrador con la contraseña <i>SSSOoIngo1</i> y otro <i>Direcciono1</i> con la contraseña <i>SSSOoDiro1</i> . Se debe contemplar que se puedan añadir nuevos usuarios en el futuro.....	19
XI.	Listar el fichero /etc/passwd para verificar que los usuarios existentes son los que se han definido.....	21
XII.	El usuario <i>Ingenieriao1</i> creará una carpeta que pertenezca a todos los usuarios del área ingeniería y en la que puedan leer y escribir. A su vez, los usuarios del área de dirección tendrán acceso de lectura al contenido ubicado en dicha carpeta.	21
5.	Configuración de Squid. Por último, se nos solicita montar un servidor proxy Squid con las siguientes características:.....	23
XIII.	Evitar que los usuarios naveguen por sus correos personales de gmail.com, hotmail.com, yahoo.com.....	24
XIV.	Restringir que no se pueda navegar ningún día de la semana entre las 8 y las 10 de la mañana.	24
XV.	Que los logs se almacenen en un fichero que se llame mensajes.log	25
XVI.	Instalar y configurar el navegador Firefox para usar el servidor Squid configurado y verificar que se aplican correctamente las restricciones.	26
	Bibliografia.....	30

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	17-02-2022
	Nombre: Amir Fernando Mamdouh	

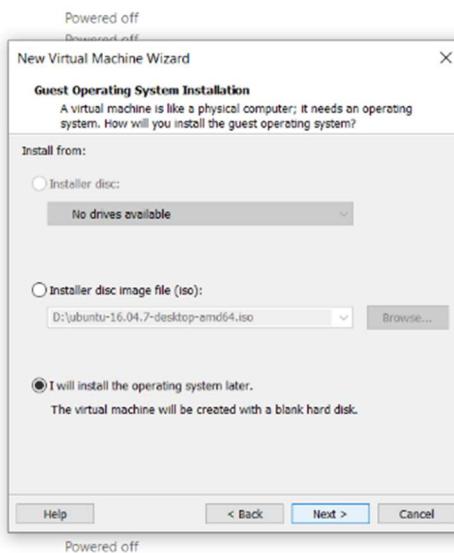
1. Creación y configuración de la maquina virtual.

I. La máquina virtual debe tener 4GB de RAM, 10GB de disco duro y una interfaz de red en modo NAT.

Para la creación use VMWare, este software permite crear máquinas virtuales, es el hipervisor de escritorio estándar del sector para ejecutar máquinas virtuales en PC con Linux o Windows. Lo primero es hacer click en File-> New virtual Machine.

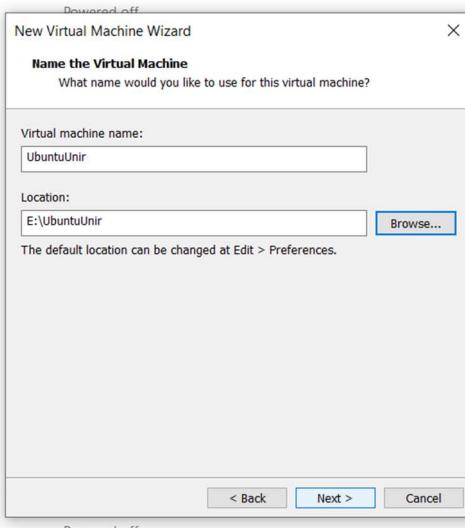


Para poder realizar las configuraciones solicitadas en la actividad se requieren hacer configuraciones previas a la instalación del sistema operativo en cuestión, en el caso de VMWare realiza estas configuraciones previas por su interfaz, por lo que la única opción es cargar el ISO de la instalación después de crear la máquina virtual por lo que elegiré la opción. Instalare el sistema operativo después.

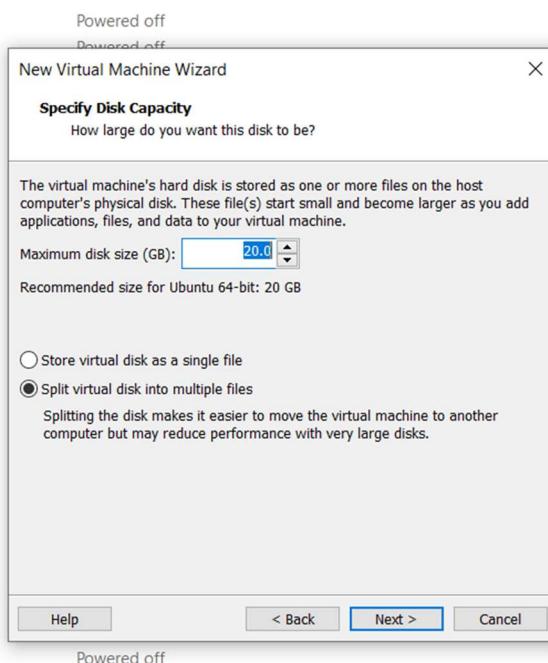


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Selecciono la ubicación donde instalare la maquina virtual.

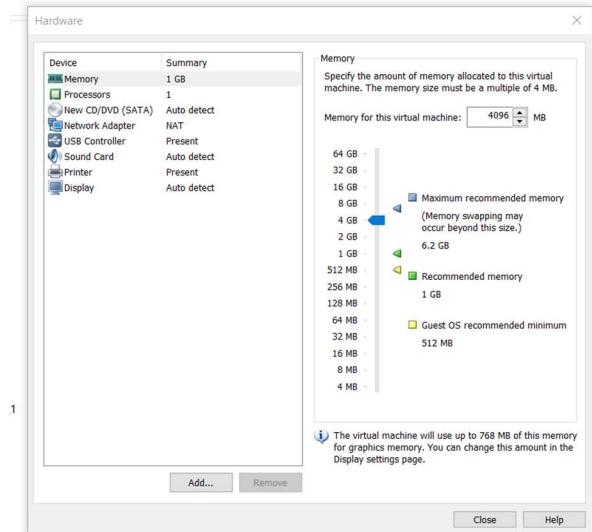


Por temas de facilidad al configurar elegí darle 20 GB al disco de la maquina.

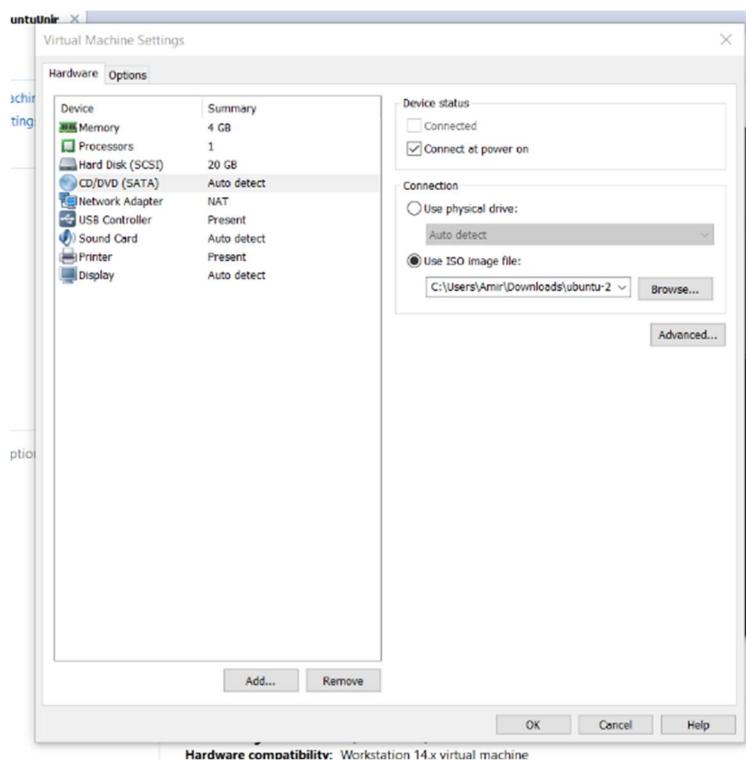


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Asigno 4 GB de memoria RAM a la maquina virtual.



Ahora bien puedo seleccionar el ISO del sistema operativo a instalar para cargarlo como un CD al arranque de la maquina virtual.

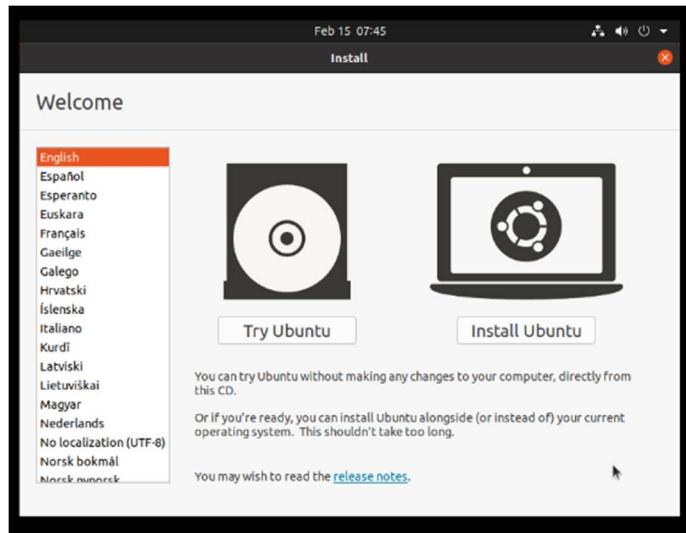


Lamentablemente VMWare si se instala normalmente pide el usuario y contraseña directamente, pero en este caso como se tenían que crear discos separados tuve que adicionar el iso después de la configuración de la maquina, para instalarlo por mi cuenta

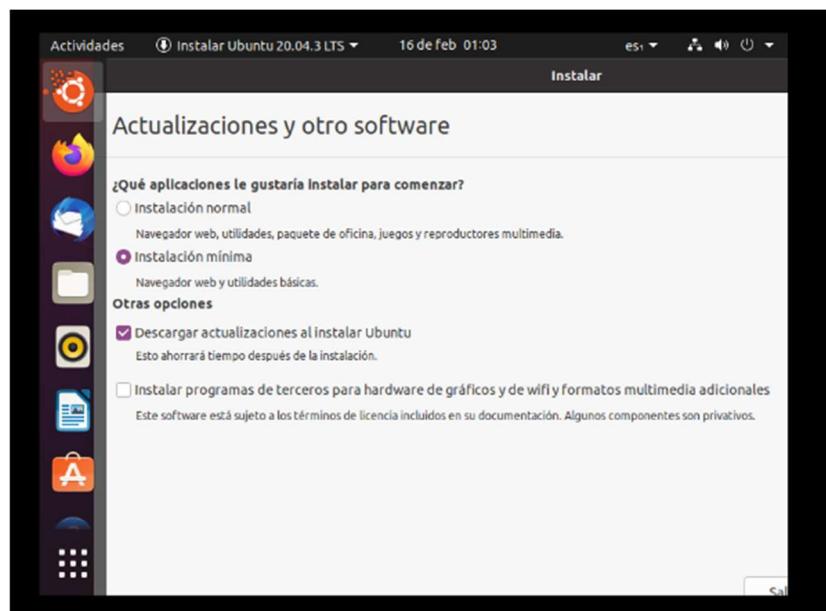
Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

II. El espacio de usuario, /home, debe estar en un volumen lógico separado.

Al cargar el ISO, selecciono la opción Try Ubuntu para realizar las configuraciones. Además, para poder revisar ciertas cuestiones con el programa gparted.

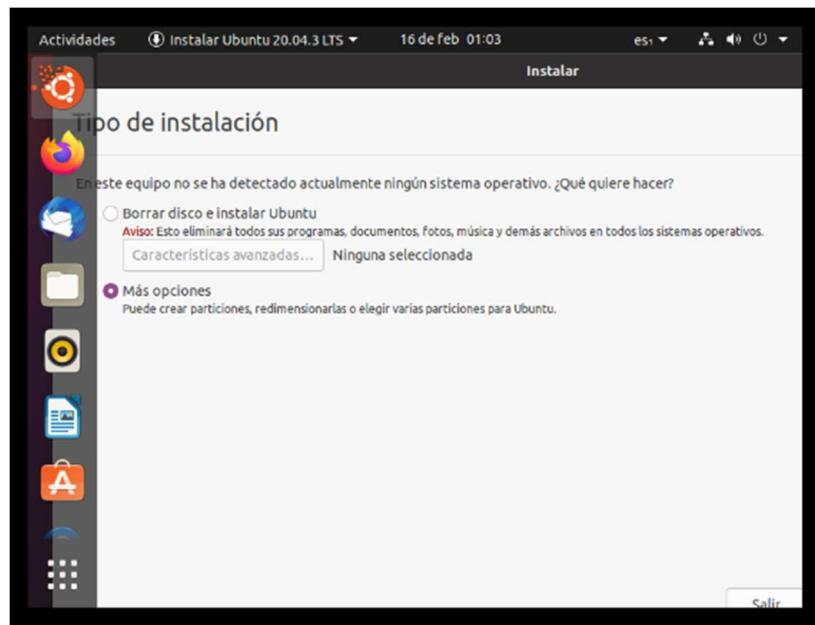


Después de unas cuantas pruebas y errores me di cuenta que podía cifrar el disco sin usar comandos, por lo que obvié el uso de comandos desde la terminal y seguí con el software de instalación habitual. (Esto lo explicare con la futura imagen, luego de esta). Selecciono la opción de instalación mínima.

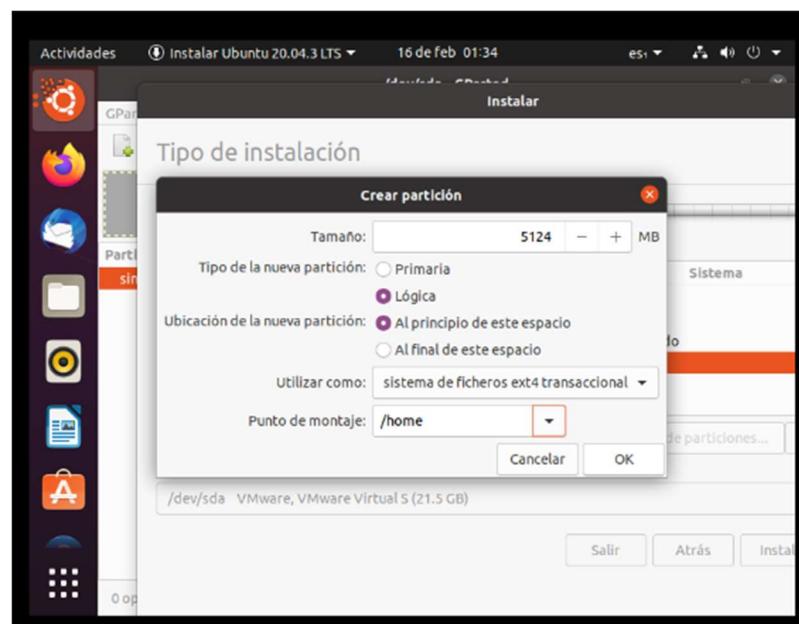


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Como mencione previamente probe muchas formas de configurar lo solicitado por la actividad, la forma más fácil era usar la opción de borrar disco, ya que esta permitía cifrar el disco dentro de las opciones de características avanzadas, pero esto iba en contra de una de las configuraciones que era la de crear home como una partición lógica, por lo que lo que tuve que hacer fue seleccionar en más opciones porque me permite configurar las tablas de partición, aunque no me permitía de cifrar al mismo tiempo a primera vista, y esto era algo que me preocupaba.

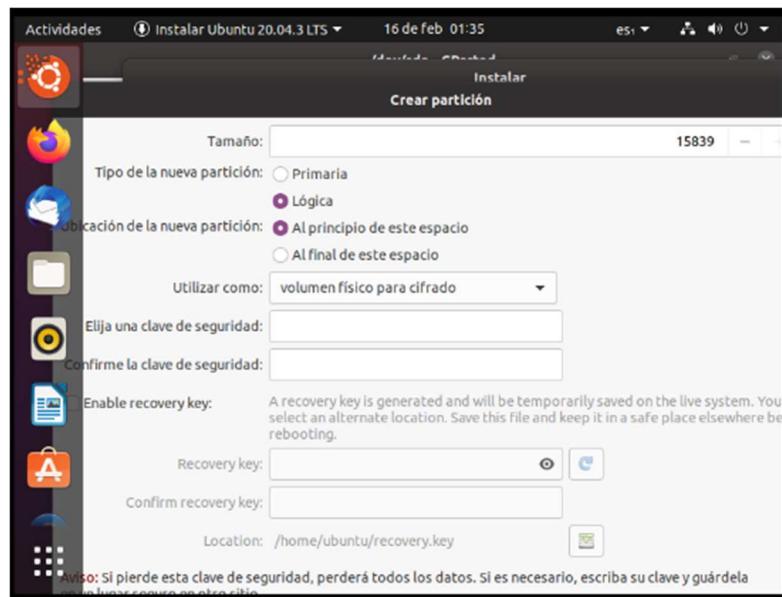


Al final descubrí que era viable cifrar el disco desde más opciones así que continue. Lo primero fue crear el disco lógico /home

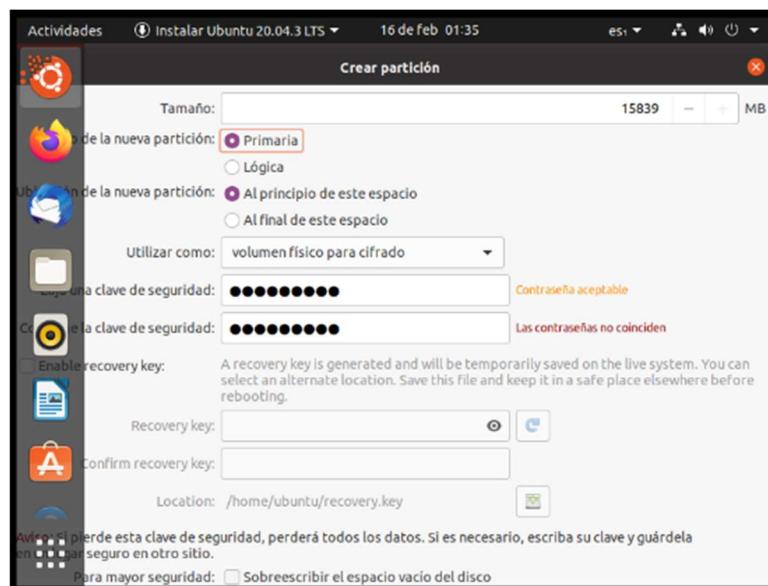


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

III. El disco duro debe estar cifrado con la clave: *discoUnir*
 Para el disco duro cifrado se tenía que seleccionar la opción “volumen físico para cifrado” para luego asignar la clave.

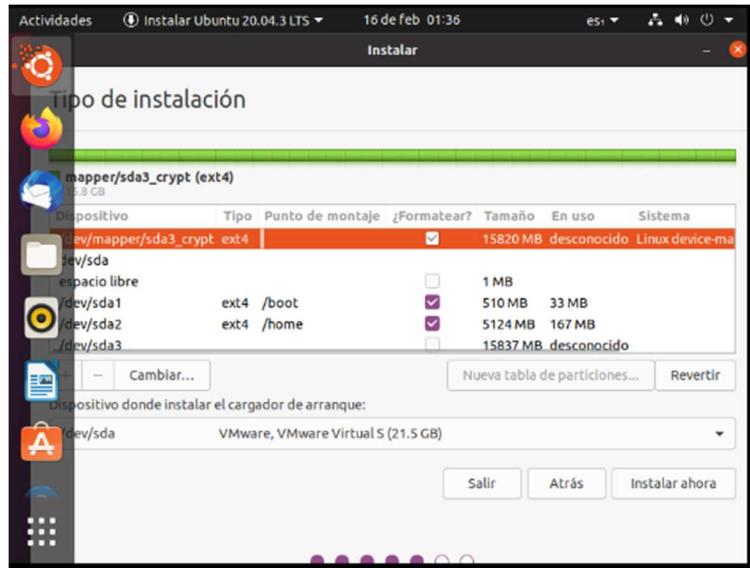


Introduzco la clave brindada por el documento la actividad y selecciono este disco como partición primaria para que sea asignada a la raíz.

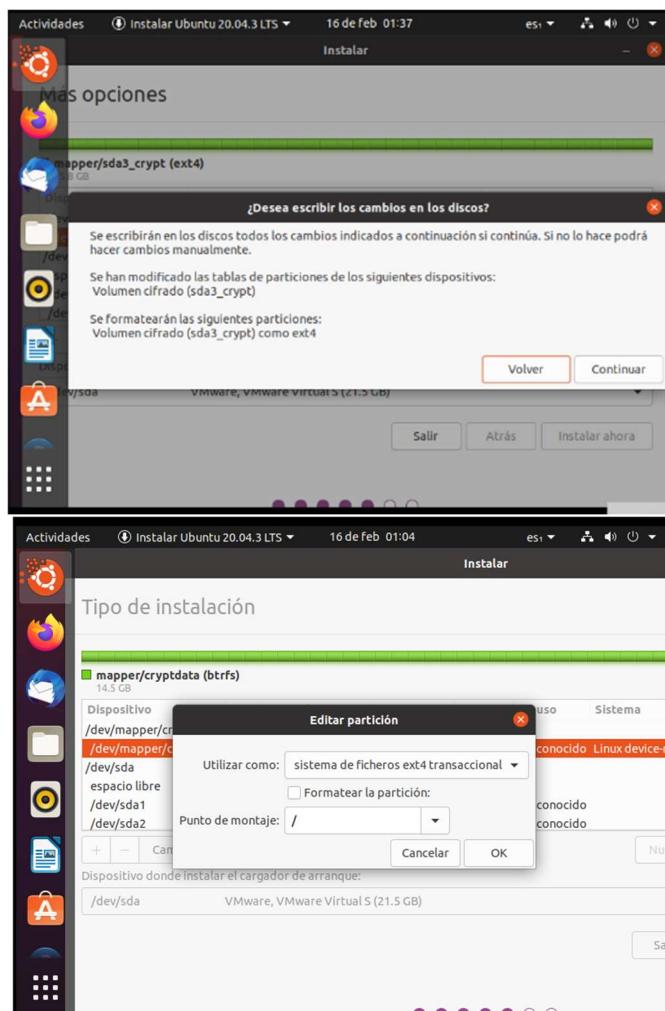


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	17-02-2022
	Nombre: Amir Fernando Mamdouh	

El resultado de como quedaron las particiones antes de asignar la raíz, fue como se muestra en la siguiente imagen.



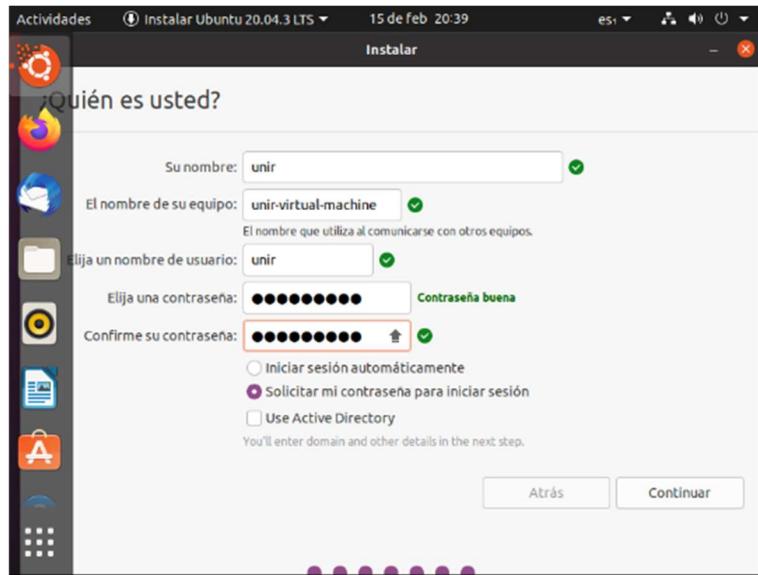
Después simplemente se tenía que montar de punto de acceso el directorio raíz “/” al disco “dev/mapper/sda3_crypt ext4”



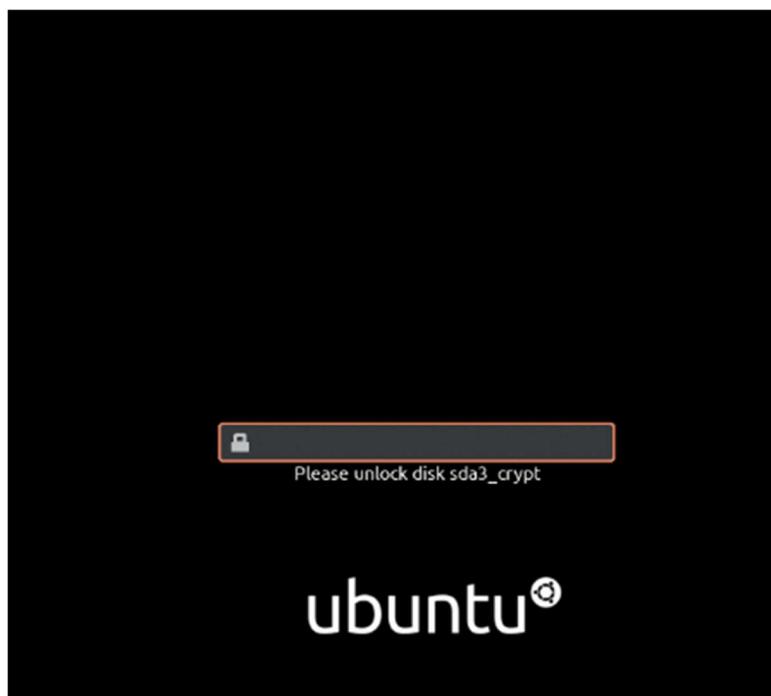
Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

IV. El usuario creado durante la instalación será *unir* con una clave *SSSOoUnir*

Siguiendo con la instalación lo que toca es asignar el usuario y contraseña solicitados por la actividad



Y cuando termine el proceso de instalación termino y se reinicio la maquina, me pedía una contraseña para acceder. Así que use la contraseña que nos fue indicada **discoUnir**, la misma contraseña con la que encripte el disco raíz

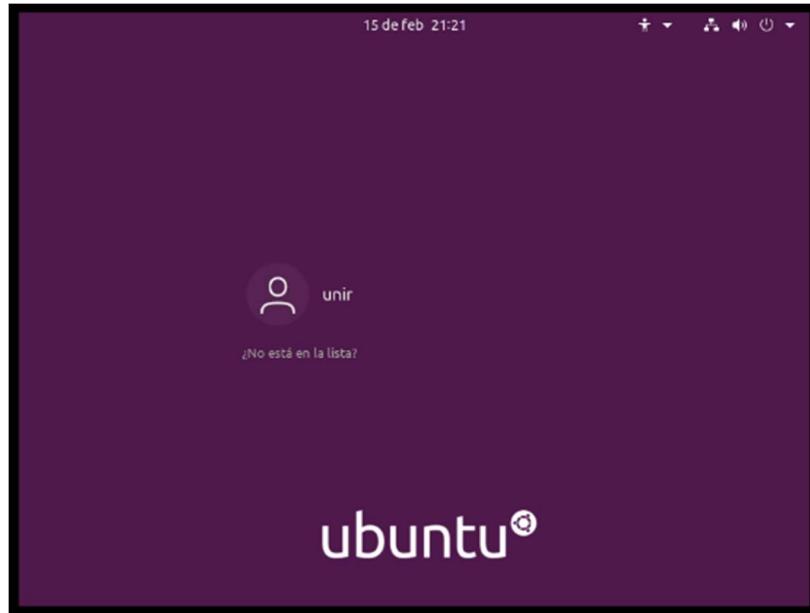


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

2. Instalación y configuración segura del grub

V. El grub debe estar protegido.

Accedo al usuario creado con la contraseña SSSOoUnir



Para securizar el grub, leí que debía acceder a grub.cfg y configurar los usuarios y contraseñas. Por ende primero hice una copia de las configuraciones. Para tenerlos por si acaso tengo algún fallo al momento de modificar este archivo.

```

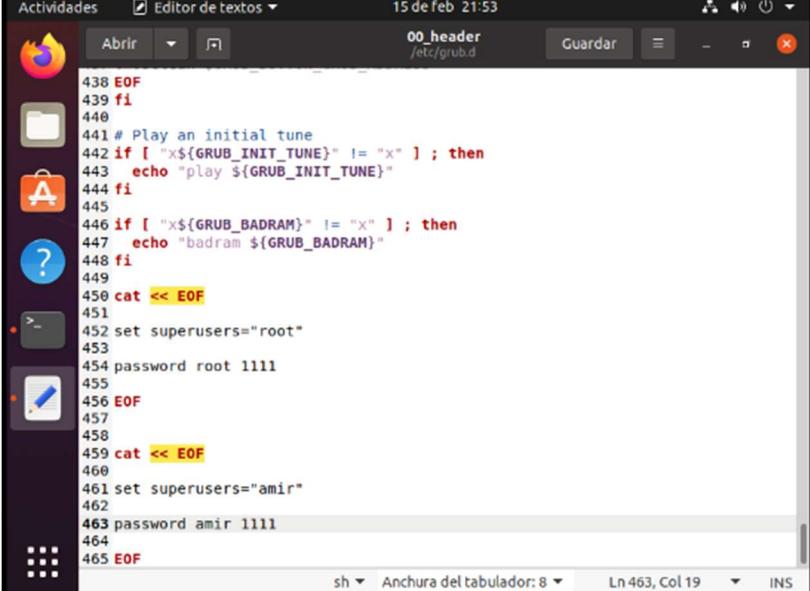
Actividades Terminal 15 feb 21:45
root@unir-virtual-machine: /boot/grub
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

unir@unir-virtual-machine:~$ sudo cp /boot/grub/grub.cfg /boot/grub/grub.cfg.old
[sudo] contraseña para unir:
Lo sentimos, vuelva a intentarlo.
[sudo] contraseña para unir:
unir@unir-virtual-machine:~$ sudo su
root@unir-virtual-machine:/home/unir# cd /boot/grub/
root@unir-virtual-machine:/boot/grub# ls
fonts gfxblacklist.txt grub.cfg grub.cfg.old grubenv i386-pc unicode.pf2
root@unir-virtual-machine:/boot/grub#

```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Luego en el archivo oo_header agregue un nuevo usuario amir y a ambos les puse la clave “1111”.

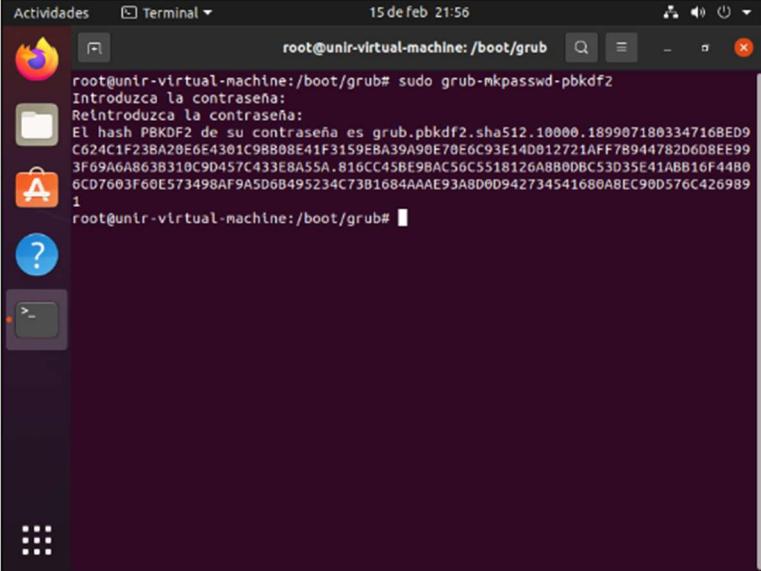


```

Actividades  Editor de textos  15 de feb 21:53
          Abrir  Guardar
          00_header  /etc/grub.d
          438 EOF
          439 fi
          440
          441 # Play an initial tune
          442 if [ "${GRUB_INIT_TUNE}" != "x" ] ; then
          443   echo "play ${GRUB_INIT_TUNE}"
          444 fi
          445
          446 if [ "${GRUB_BADRAM}" != "x" ] ; then
          447   echo "badram ${GRUB_BADRAM}"
          448 fi
          449
          450 cat << EOF
          451
          452 set superusers="root"
          453
          454 password root 1111
          455
          456 EOF
          457
          458
          459 cat << EOF
          460
          461 set superusers="amir"
          462
          463 password amir 1111
          464
          465 EOF

```

Pero al ser un archivo de configuración de tan fácil acceso y con texto en claro procedí a crear un password sha512 de la clave “1111” con el comando grub-mkpasswd-pbkdf2



```

Actividades  Terminal  15 de feb 21:56
          root@unir-virtual-machine:/boot/grub# sudo grub-mkpasswd-pbkdf2
          Introduzca la contraseña:
          Relintruduzca la contraseña:
          El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.189907180334716BED9
          C624C1F23BA20E6E4301C98B808E41F3159EBA39A90E70E6C93E14D012721AFF78944782D608EE99
          3F69A6A863B310C90457C433E8A55A.B16CC458E9BAC56C5518126A880DBC53D35E41ABB16F44B0
          6CD7603F60E573498AF9A5D6B495234C73B1684AAAE93A8D0D942734541680ABEC90D576C426989
          1
          root@unir-virtual-machine:/boot/grub#

```

Gracias a esto obtuve la clave hasheada de 1111 a
grub.pbkdf2.sha512.10000.6CE8773EA6EB70EC88ECF958524940417A982F7593DF1
7613160FF3E24C365E68A90F440C8CoFF12125014FE982DA992A7E2259128B4CDE
E8E1857E4B483D3A1.A9C6525DF5E4D65AD11800EF3443D3C103FDD395DBE9A5F
C1880CoF8E80ACCEAFDDoB75E10E4D3F8Co26B793250CB56A4B3239C66CA1CE1
7DA6FD96D2E77B16E. Y copie esta clave en el archivo oo_header

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

```

Actividades Editor de textos 15 de feb 22:12
Abrir Guardar
*00_header /etc/grub.d
439 fi
440
441 # Play an initial tune
442 if [ "${GRUB_INIT_TUNE}" != "x" ] ; then
443   echo "play ${GRUB_INIT_TUNE}"
444 fi
445
446 if [ "${GRUB_BADRAM}" != "x" ] ; then
447   echo "badram ${GRUB_BADRAM}"
448 fi
449
450 cat << EOF
451
452 set superusers="root"
453
454 password root
  grub.pbkdf2.sha512.10000.6CE8773EA6EB70EC88ECF958524940417A982F7593DF1761316
455
456 EOF
457
458
459 cat << EOF
460
461 set superusers="amir"
462
463 password amir
  grub.pbkdf2.sha512.10000.6CE8773EA6EB70EC88ECF958524940417A982F7593DF1761316
464
sh Anchura del tabulador: 8 Ln 463, Col 297 INS

```

VI. Securizar los comandos su y sudo

Lo que tocaba era securizar los comandos su y sudo, para este paso tenía que asegurarme que cuando se ingrese al computador si se quería acceder a sudo tenía que pedir la contraseña de inmediato, ya que sudo por defecto tiene un tiempo de 15 minutos antes de que comience a pedir la clave, por ende en la configuración de sudoers agregue **Defaults timestamp_timeout=0**

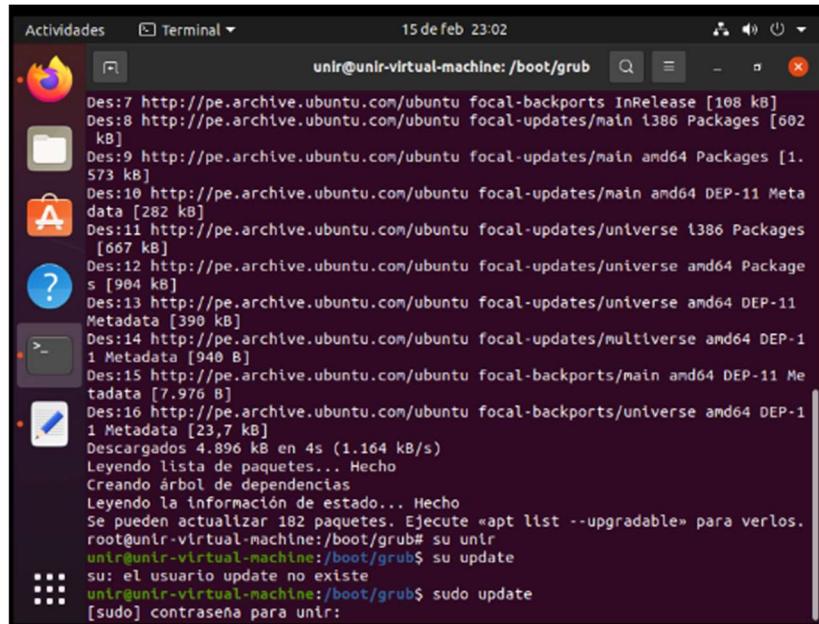
```

Actividades Editor de textos 15 de feb 23:01
Abrir Guardar
sudoers /etc
1 #
2 # This file MUST be edited with the 'visudo' command as root.
3 #
4 # Please consider adding local content in /etc/sudoers.d/ instead of
5 # directly modifying this file.
6 #
7 # See the man page for details on how to write a sudoers file.
8 #
9 Defaults      env_reset
10 Defaults     mail_badpass
11 Defaults     secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin:/sbin:/bin:/snap/bin"
12 Defaults     timestamp_timeout=0
13
14 # Host alias specification
15
16 # User alias specification
17
18 # Cmnd alias specification
19
20 # User privilege specification
21 root      ALL=(ALL:ALL) ALL
22
23 # Members of the admin group may gain root privileges
24 %admin  ALL=(ALL) ALL
25
26 # Allow members of group sudo to execute any command
27 %sudo    ALL=(ALL:ALL) ALL
sh Anchura del tabulador: 8 Ln 12, Col 1 INS

```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Para mostrar que esto estaba funcionando procedí a intentar actualizar la distro con sudo apt update, y como se muestra pedía la contraseña del usuario unir al instante.



```

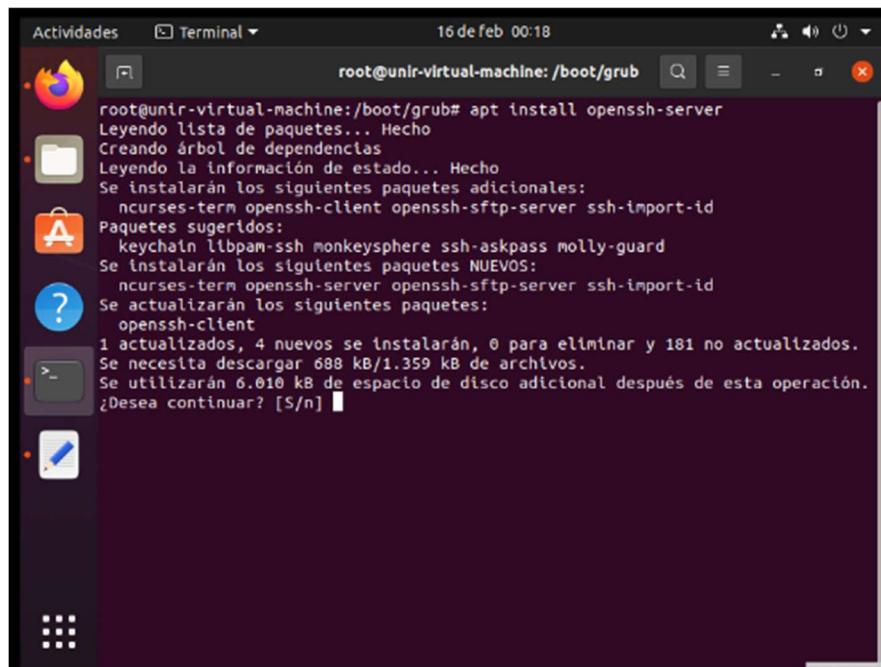
Actividades Terminal 15 de feb 23:02
unir@unir-virtual-machine:/boot/grub
Des:7 http://pe.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Des:8 http://pe.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [602 kB]
Des:9 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1.573 kB]
Des:10 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [282 kB]
Des:11 http://pe.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [667 kB]
Des:12 http://pe.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [904 kB]
Des:13 http://pe.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [390 kB]
Des:14 http://pe.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [940 kB]
Des:15 http://pe.archive.ubuntu.com/ubuntu focal-backports/main amd64 DEP-11 Metadata [7.976 kB]
Des:16 http://pe.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [23,7 kB]
Descargados 4.896 kB en 4s (1.164 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se pueden actualizar 182 paquetes. Ejecute «apt list --upgradable» para verlos.
root@unir-virtual-machine:/boot/grub# su unir
unir@unir-virtual-machine:/boot/grub$ su update
su: el usuario update no existe
unir@unir-virtual-machine:/boot/grub$ sudo update
[sudo] contrasena para unir:

```

3. Configuración de IPTables

VII. Se debe tener instalado OpenSSH server

Para instalar openssh server, la instrucción a utilizar es apt install openssh-server y luego presionar S



```

Actividades Terminal 16 de feb 00:18
root@unir-virtual-machine:/boot/grub#
root@unir-virtual-machine:/boot/grub# apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
Se actualizan los siguientes paquetes:
  openssh-client
1 actualizados, 4 nuevos se instalarán, 0 para eliminar y 181 no actualizados.
Se necesita descargar 688 kB/1.359 kB de archivos.
Se utilizarán 6.010 kB de espacio de disco adicional después de esta operación.
Desea continuar? [S/n]

```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Lo que toca es visualizar los servicios que se están ejecutando y por cuales puertos.
(Esto lo realice con la instrucción ps aux)

```

root@unir-virtual-machine:/boot/grub# netstat -an
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux      1/tcp          # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp          sink null
discard     9/udp          sink null
sysstat     11/tcp         users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd       17/tcp          quote
chargen    19/tcp          ttyst source
chargen    19/udp          ttyst source
ftp-data   20/tcp
ftp         21/tcp
fsp         21/udp          fspd
ssh         22/tcp          # SSH Remote Login Protocol
telnet     23/tcp
smtp        25/tcp          mail
time        37/tcp          timserver
time        37/udp          timserver
whois      43/tcp          nicname
:
```

Compruebo nuevamente con el comando lsof -i -P -n, aquí ssh server es mencionado como sshd,

```

root@unir-virtual-machine:/boot/grub# lsof -i -P -n
COMMAND  PID  USER   FD  TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 728 systemd-resolve  12u  IPv4  34138      0t0  UDP 127.0.0.53:53
systemd-r 728 systemd-resolve  13u  IPv4  34139      0t0  TCP 127.0.0.53:53 (LISTEN)
avahi-dae 762  avahi   12u  IPv4  37241      0t0  UDP *:5353
avahi-dae 762  avahi   13u  IPv6  37242      0t0  UDP *:5353
avahi-dae 762  avahi   14u  IPv4  37243      0t0  UDP *:39322
avahi-dae 762  avahi   15u  IPv6  37244      0t0  UDP *:36386
cupsd     765  root     6u  IPv6  37144      0t0  TCP [::1]:631 (LISTEN)
cupsd     765  root     7u  IPv4  37145      0t0  TCP 127.0.0.1:631 (LISTEN)
NetworkMa 767  root    23u  IPv4  112530     0t0  UDP 192.168.93.163:68->192.168.93.254:67
cups-brow 839  root     7u  IPv4  37270      0t0  UDP *:631
firefox   2847 untr    37u  IPv4  112786     0t0  TCP 192.168.93.163:34640->157.240.197.17:443 (ESTABLISHED)
firefox   2847 untr    38u  IPv4  112806     0t0  TCP 192.168.93.163:36196->157.240.197.10:443 (ESTABLISHED)
firefox   2847 untr    44u  IPv4  131861     0t0  TCP 192.168.93.163:38396->52.42.96.247:443 (ESTABLISHED)
sshd     6212  root     3u  IPv4  114582     0t0  TCP *:22 (LISTEN)
sshd     6212  root     4u  IPv6  114593     0t0  TCP *:22 (LISTEN)
root@unir-virtual-machine:/boot/grub#
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Después reviso el versionado de los ssh que tengo instalados con el comando ssh --version

```
root@unir-virtual-machine:/boot/grub# ssh --version
unknown option -- -
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
root@unir-virtual-machine:/boot/grub# dpkg --list openssh\*
Deseado=desconocido(U)/Instalar/eliminar/Purgar/retener(H)
| Estado=No/Inst/ficheros-Conf/desempaquetado/medio-conf/medio-inst(H)/espera-
| / Err?=(ninguno)/requiere-Reinst (Estado,Err: mayúsc.=malo)
||/ Nombre          Versión          Arquitectura Descripción
=====-=====
ii  openssh-client   1:8.2p1-4ubuntu0.4  amd64      secure shell (SSH) cli>
ii  openssh-server   1:8.2p1-4ubuntu0.4  amd64      secure shell (SSH) ser>
ii  openssh-sftp-server 1:8.2p1-4ubuntu0.4  amd64      secure shell (SSH) sft>
un  openssh-sk-helper <ninguna>        <ninguna>    (no hay ninguna descri>
lunes 1-9/9 (END)
```

VIII. Configurar IPTables para que solamente acepte conexiones a OpenSSH a través del puerto 22.

Una vez instalado el openssh y viendo que se esta ejecutando procedo a revisar las iptables con el comando iptables -L (Como era de esperar no se tiene registrada ninguna ip).

```
root@unir-virtual-machine:/boot/grub# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@unir-virtual-machine:/boot/grub#
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	17-02-2022
	Nombre: Amir Fernando Mamdouh	

Para este item teníamos que aceptar solo las conexiones por el puerto 22 así que (como se nos enseñó en el curso de seguridad en redes, usares los comandos) primero permitir las entradas a la maquina:

- iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT

Para las salidas:

- iptables -A OUTPUT -p tcp --dport 22 -j DROP

Finalmente, para los paquetes que son generados por equipos remotos y pasan por la computadora:

- iptables -A FORWARD -p tcp --dport 22 -j DROP.

Luego hago esta revisión con iptables -L

```

root@unir-virtual-machine:/boot/grub# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
          tcp   --  anywhere             anywhere            state NEW -j ACCEPT
root@unir-virtual-machine:/boot/grub# iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
root@unir-virtual-machine:/boot/grub# iptables -A OUTPUT -p tcp --dport 22 -j DROP
root@unir-virtual-machine:/boot/grub# iptables -A FORWARD -p tcp --dport 22 -j DROP
root@unir-virtual-machine:/boot/grub# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT    tcp  --  anywhere             anywhere            tcp dpt:ssh state NEW
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP      tcp  --  anywhere             anywhere            tcp dpt:ssh
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP      tcp  --  anywhere             anywhere            tcp dpt:ssh
root@unir-virtual-machine:/boot/grub#

```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	17-02-2022
	Nombre: Amir Fernando Mamdouh	

4. Script y creación de usuarios y grupos

IX. Los usuarios que van a trabajar en la máquina son del área de dirección y de ingeniería. Crear un script que nos solicite el nombre de usuario, la contraseña, su grupo (que si no existe se añadirá) y si es usuario administrador para permitirnos crear usuarios en el sistema. Además, el script debe verificar si el usuario ya existe en el sistema antes de darle de alta.

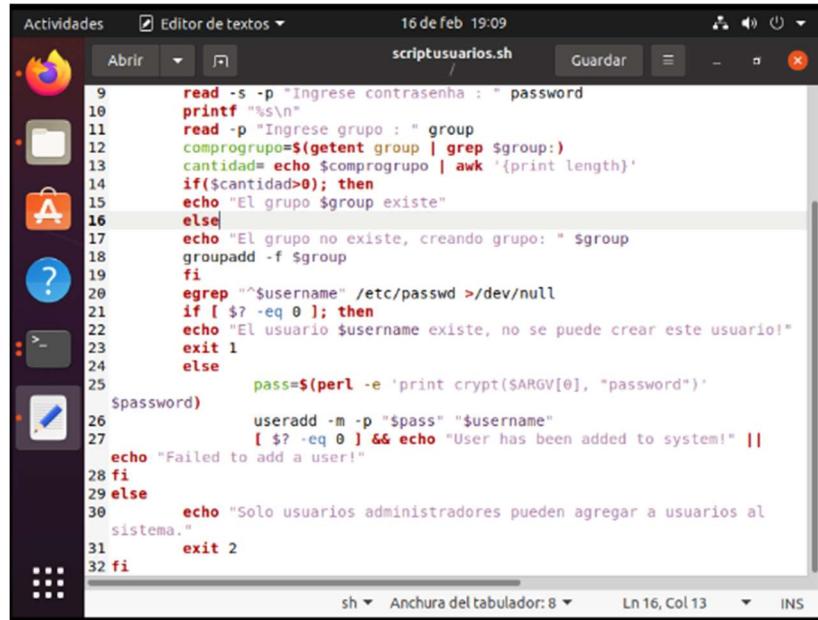
Primero reviso los grupos existentes con la denominación de unir con getent group | grep unir, grep permite filtrar las salidas de texto

```
unir@unir-virtual-machine:~$ getent group | grep unir
Unidad «gentet» no encontrada. Quizá quiso decir:
    La orden «gentest» del paquete deb «samba-testsuite (2:4.13.17-dfsg-0ubuntu0.21.04.1)»
Pruebe con: sudo apt install <nombre del paquete deb>
unir@unir-virtual-machine:~$ getent group | grep unir
adm:x:4:syslog,unir
cdrom:x:24:unir
sudo:x:27:unir
dip:x:30:unir
plugdev:x:46:unir
lpadmin:x:120:unir
lxd:x:132:unir
unir:x:1000:
sanbsahare:x:133:unir
admin:x:1002:unir
unir@unir-virtual-machine:~$ getent group | grep bka
unir@unir-virtual-machine:~$
```

Después de varios intentos logré crear mi script en lenguaje bash, este archivo con extensión .sh para poder crear usuarios de forma automática. Solicitando usuario, contraseña y grupo

```
#!/bin/bash
# Purpose - Script to add a m including password
# Author - Vivek Gite <www.cyberciti.biz> under GPL v2.0+
#
# Am I Root user?
if [ $(id -u) -eq 0 ]; then
    read -p "Ingrese usuario : " username
    read -s -p "Ingrese contraseña : " password
    printf "%s\n"
    read -p "Ingrese grupo : " group
    comprogrupo=$(getent group | grep $group)
    cantidad=echo $comprogrupo | awk '{print length}'
    if($cantidad>0); then
        echo "El grupo $group existe"
    else
        echo "El grupo no existe, creando grupo: " $group
        groupadd -f $group
    fi
    egrep "^$username" /etc/passwd >/dev/null
    if [ $? -eq 0 ]; then
        echo "El usuario $username existe, no se puede crear este usuario!"
        exit 1
    else
        pass=$(perl -e 'print crypt($ARGV[0], "password")'
        $password)
        useradd -m -p "$pass" "$username" -g "$group"
    fi
else
    echo "No es root"
fi
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022



```

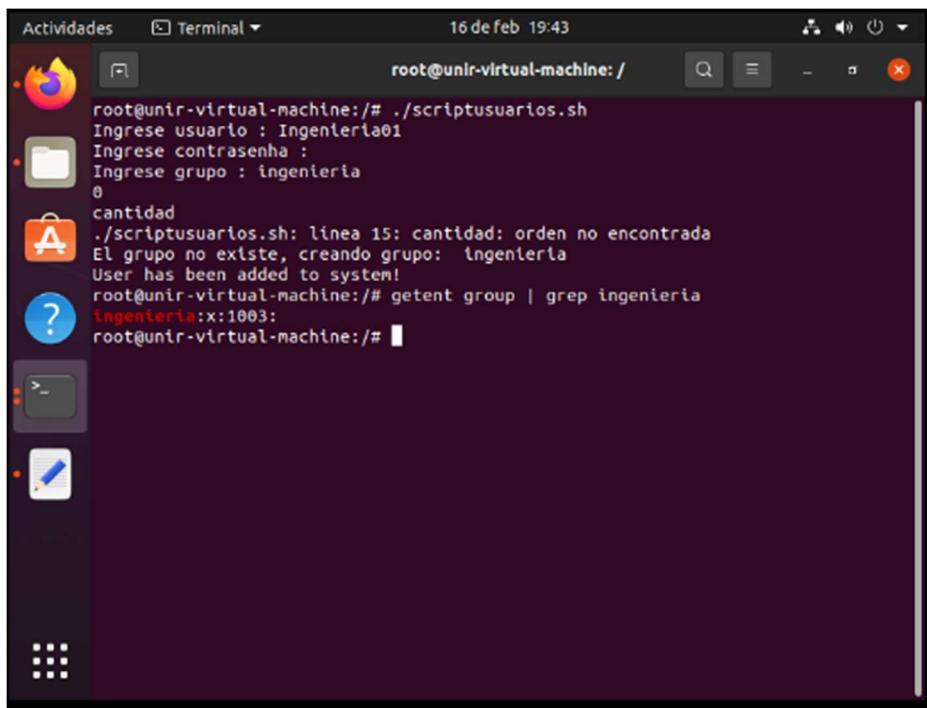
Actividades Editor de textos 16 de feb 19:09
scriptusuarios.sh
read -s -p "Ingrese contraseña : " password
printf "%s\n"
read -p "Ingrese grupo : " group
comprogru=$(getent group | grep $group:)
cantidad= echo $comprogru | awk '{print length}'
if($cantidad>0); then
echo "El grupo $group existe"
else
echo "El grupo no existe, creando grupo: " $group
groupadd -f $group
fi
egrep "^$username" /etc/passwd >/dev/null
if [ $? -eq 0 ]; then
echo "El usuario $username existe, no se puede crear este usuario!"
exit 1
else
pass=$(perl -e 'print crypt($ARGV[0], "password")'
$password)
useradd -m -p "$pass" "$username"
[ $? -eq 0 ] && echo "User has been added to system!" ||
echo "Failed to add a user!"
fi
else
echo "Solo usuarios administradores pueden agregar a usuarios al
sistema."
exit 2
fi

```

sh ▾ Anchura del tabulador: 8 ▾ Ln 16, Col 13 ▾ INS

- X. Usando el script anterior, crear el usuario *Ingenieria01* no administrador con la contraseña *SSSOoIngo1* y otro *Direccion01* con la contraseña *SSSOoDiro1*. Se debe contemplar que se puedan añadir nuevos usuarios en el futuro.

Procedí a hacer la prueba usando el comando de ejecución de mi script `./scriptusuarios.sh` y era un éxito, aunque todavía no estaba afinada porque no me agarraba la longitud del grep de los grupos correctamente, pero si le quitaba el \$ en el primer if de esta condición y no existía el grupo, los creaba correctamente.



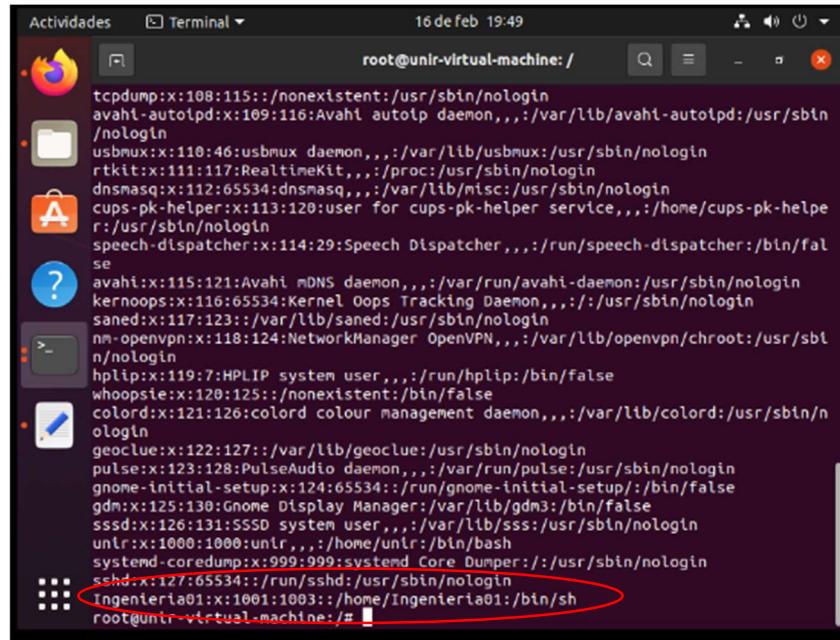
```

Actividades Terminal 16 de feb 19:43
root@unir-virtual-machine:~/scriptusuarios.sh
Ingrese usuario : Ingenieria01
Ingrese contraseña :
Ingrese grupo : ingenieria
0
cantidad
./scriptusuarios.sh: linea 15: cantidad: orden no encontrada
El grupo no existe, creando grupo: ingenieria
User has been added to system!
root@unir-virtual-machine:~/scriptusuarios.sh
Ingenieria01:x:1003:
root@unir-virtual-machine:~#

```

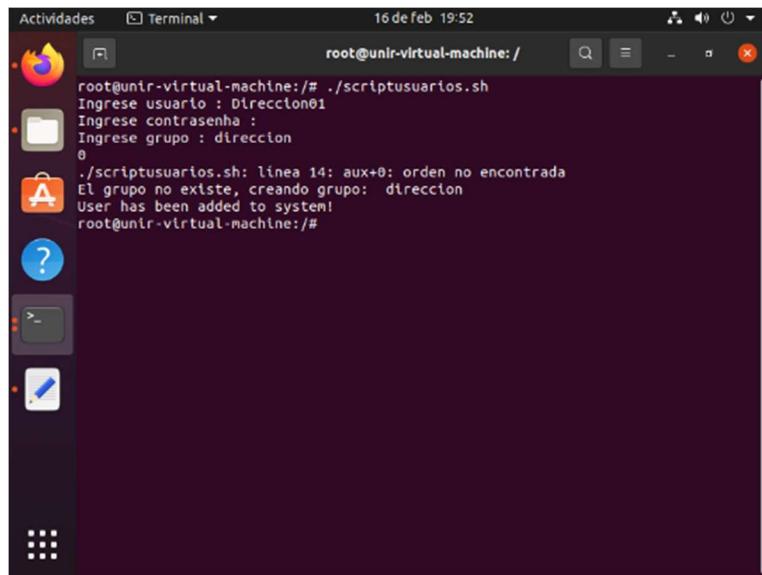
Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Si mandaba el comando **vi /etc/passwd**, también lo mostraba



```
root@unir-virtual-machine:~# vi /etc/passwd
...
Ingenieria01:x:1001:1003::/home/Ingenieria01:/bin/sh
root@unir-virtual-machine:~#
```

Para el área de dirección también hago lo mismo Direccion01 SSSOoDiro01 dirección



```
root@unir-virtual-machine:~# ./scriptusuarios.sh
Ingrese usuario : Direccion01
Ingrese contraseña :
Ingrese grupo : direccion
0
./scriptusuarios.sh: linea 14: aux+0: orden no encontrada
El grupo no existe, creando grupo: direccion
User has been added to system!
root@unir-virtual-machine:~#
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

- XI. Listar el fichero /etc/passwd para verificar que los usuarios existentes son los que se han definido.

Para esto uso nuevamente el comando vi /etc/passwd

```

Actividades Terminal 16 de feb 19:52
root@unir-virtual-machine: /
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Ooops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
sssd:x:126:131:SSSD system user,,,:/var/lib/sssd:/usr/sbin/nologin
unir:x:1000:1000:unir,,,:/home/unir:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:127:65534::/run/sshd:/usr/sbin/nologin
Ingenieria01:x:1001:1003::/home/Ingenieria01:/bin/sh
Direccion01:x:1002:1004::/home/Direccion01:/bin/sh
root@unir-virtual-machine: #

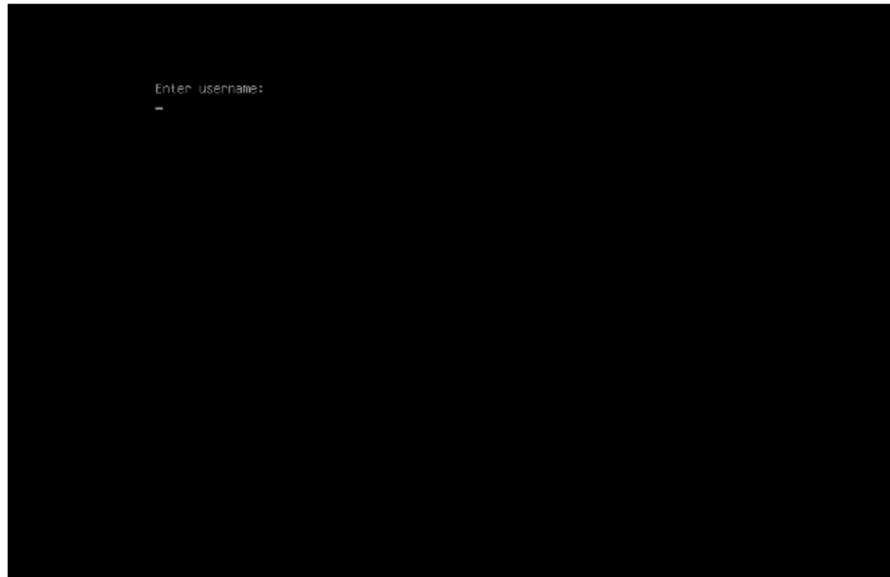
```

De esta forma, verifico que los usuarios solicitados fueron creados exitosamente.

- XII. El usuario *Ingenieria01* creará una carpeta que pertenezca a todos los usuarios del área ingeniería y en la que puedan leer y escribir. A su vez, los usuarios del área de dirección tendrán acceso de lectura al contenido ubicado en dicha carpeta.

Lastimosamente y aquí comienza mi excusa, mi computadora se apago y al momento de tratar de ingresar, no me fue posible por el bloqueo del grub, con ninguna de las claves que puse. Se que no es una excusa, pero realmente no pude. Y para acrecentar esto, mi ojo derecho esta inflamado desde hace 3 días, parece que por el uso excesivo del computador, por lo que me es imposible hacer todo esto otra vez para poder continuar, y lamento hacer este trabajo muy por debajo de mis actividades acostumbradas.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022



Para no entregar un trabajo incompleto, use otra de mis máquinas y proseguí con los comandos que tenía que hacer si normalmente esto no hubiera sucedido.

Previamente se debe usar el comando `install -g "nombregrupo" -d "nombrecarpeta"` en la misma carpeta.

Con el usuario ingeniería tenía que usar el comando `> mkdir "ingenieriacarpeta"`

Luego dar los permisos de lectura y escritura a la carpeta creada con `> chmod -R 765 "ingenieriacarpeta"`

En el caso de dirección `> mkdir "direccioncarpeta"`

Luego dar los permisos de lectura y escritura a la carpeta creada con `> chmod -R 740 "direccioncarpeta"`

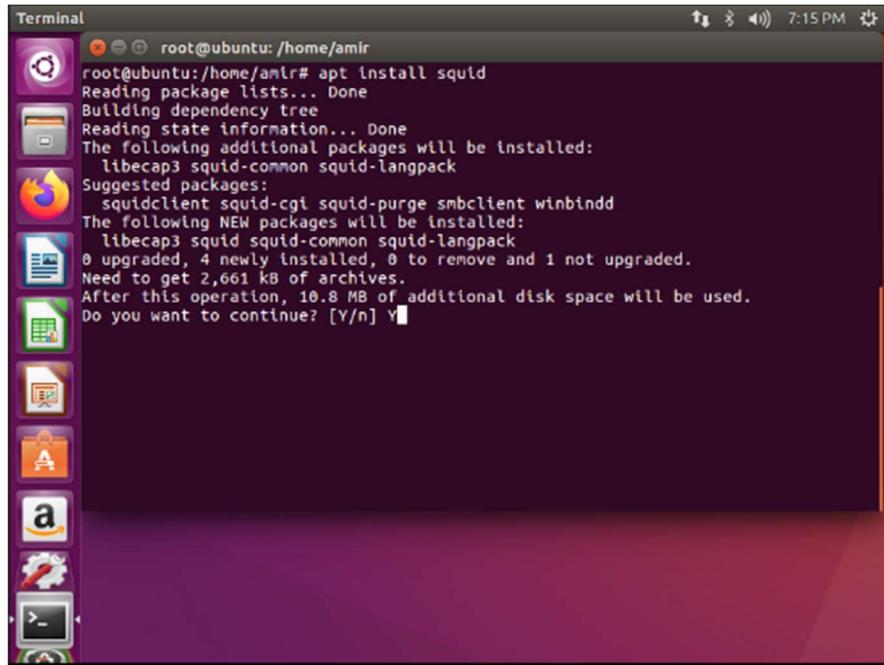
Chmod brinda permisos de lectura, escritura y ejecución los valores son 4,2 y 1 respectivamente; estos valores se asignan al propietario, grupo y otros usuarios

```
root@ubuntu:/home/amir# ls -la
total 124
drwxr-xr-x 19 amir amir 4096 Feb 16 19:12 .
drwxr-xr-x  3 root root 4096 Jan 18 19:11 ..
-rw-r--r--  1 amir amir  31 Jan 25 19:22 .bash_history
-rw-r--r--  1 amir amir 220 Jan 18 19:11 .bash_logout
-rw-r--r--  1 amir amir 3771 Jan 18 19:11 .bashrc
drwx----- 15 amir amir 4096 Jan 25 19:19 .cache
drwx-----  3 amir amir 4096 Jan 25 19:22 .compiz
drwx----- 14 amir amir 4096 Jan 18 19:16 .config
drwxr-xr-x  2 amir amir 4096 Jan 18 19:15 Desktop
drwxr-xr-x  2 root root 4096 Feb 16 19:12 direccioncarpeta
-rw-r--r--  1 amir amir  25 Jan 18 19:14 .dnrc
drwxr-xr-x  2 amir amir 4096 Jan 18 19:15 Documents
drwxr-xr-x  4 amir amir 4096 Jan 25 19:20 Downloads
-rw-r--r--  1 amir amir 8980 Jan 18 19:11 examples.desktop
drwx-----  2 amir amir 4096 Jan 20 14:34 .gconf
drwx-----  3 amir amir 4096 Feb 16 19:08 .gnupg
-rw-----  1 amir amir 1272 Feb 16 19:08 .ICEauthority
dr-----  2 root root 4096 Feb 16 19:11 ingenieriacarpeta
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

5. Configuración de Squid. Por último, se nos solicita montar un servidor proxy Squid con las siguientes características:

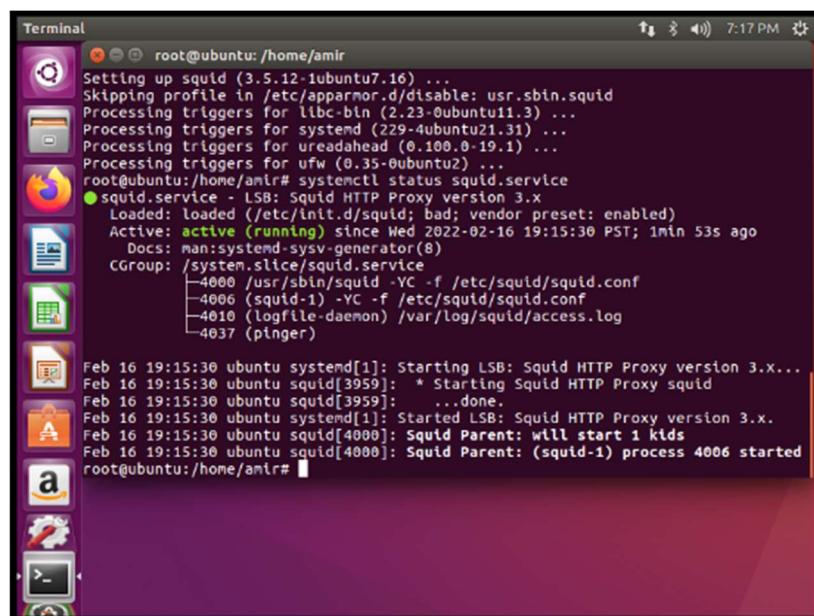
Para instalar squid se usa el comando apt install squid



```
Terminal
root@ubuntu:/home/amir
root@ubuntu:/home/amir# apt install squid
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcap3 squid-common squid-langpack
Suggested packages:
  squidclient squid-cgi squid-purge smbclient winbindd
The following NEW packages will be installed:
  libcap3 squid squid-common squid-langpack
0 upgraded, 4 newly installed, 0 to remove and 1 not upgraded.
Need to get 2,661 kB of archives.
After this operation, 10.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Se verifica que este activo el servicio de squid esta activo con el comando:

systemctl status squid.service

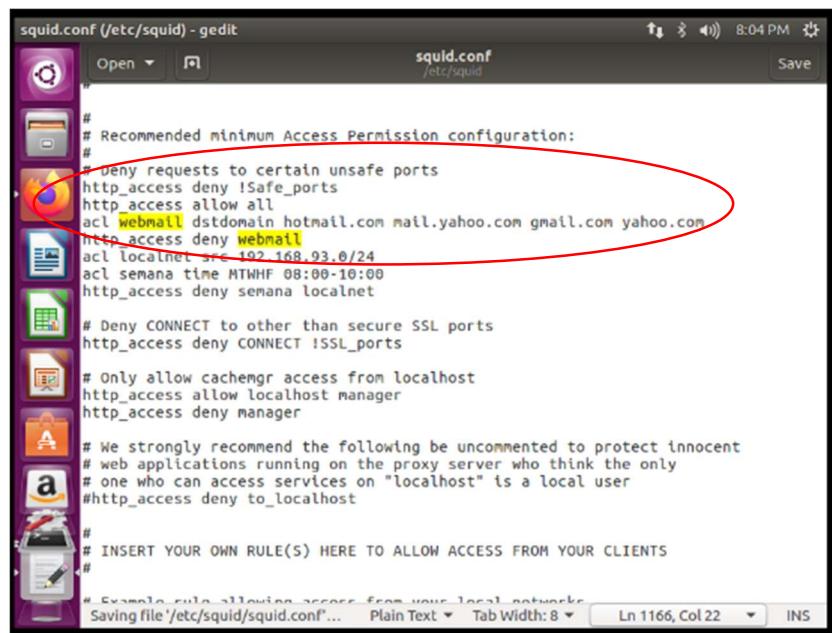


```
Terminal
root@ubuntu:/home/amir
root@ubuntu:/home/amir# Setting up squid (3.5.12-1ubuntu7.16) ...
root@ubuntu:/home/amir# Skipping profile in /etc/apparmor.d/disable: usr.sbin.squid
root@ubuntu:/home/amir# Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
root@ubuntu:/home/amir# Processing triggers for systemd (229-4ubuntu21.31) ...
root@ubuntu:/home/amir# Processing triggers for ureadahead (0.100.0-19.1) ...
root@ubuntu:/home/amir# Processing triggers for ufw (0.35-0ubuntu2) ...
root@ubuntu:/home/amir# squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
   Active: active (running) since Wed 2022-02-16 19:15:30 PST; 1min 53s ago
     Docs: man:systemd-sysv-generator(8)
     CGroup: /system.slice/squid.service
             └─4000 /usr/sbin/squid -YC -f /etc/squid/squid.conf
                 ├─4006 (squid-1) -YC -f /etc/squid/squid.conf
                 ├─4010 (logfile-daemon) /var/log/squid/access.log
                 ├─4037 (pinger)
                 ...
Feb 16 19:15:30 ubuntu systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Feb 16 19:15:30 ubuntu squid[3959]: * Starting Squid HTTP Proxy squid
Feb 16 19:15:30 ubuntu squid[3959]: ...done.
Feb 16 19:15:30 ubuntu systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
Feb 16 19:15:30 ubuntu squid[4000]: Squid Parent: will start 1 kids
Feb 16 19:15:30 ubuntu squid[4000]: Squid Parent: (squid-1) process 4006 started
root@ubuntu:/home/amir#
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

XIII. Evitar que los usuarios naveguen por sus correos personales de gmail.com, hotmail.com, yahoo.com.

Para denegar el acceso a los correos personales, debia configurar el archivo /etc/squid/squid.conf, primero permití todos los accesos a http con http_access allow all luego creo una lista de control de acceso (acl), con el nombre de webmail y los dominios dstdomain hotmail.com mail.yahoo.com gmail.com yahoo.com, luego se debe crear denegar el acceso con http_access deny webmail



```
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports
http_access allow all
acl webmail dstdomain hotmail.com mail.yahoo.com gmail.com yahoo.com
http_access deny webmail
acl localnet src 192.168.93.0/24
acl semana time MTWTF 08:00-10:00
http_access deny semana localnet

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

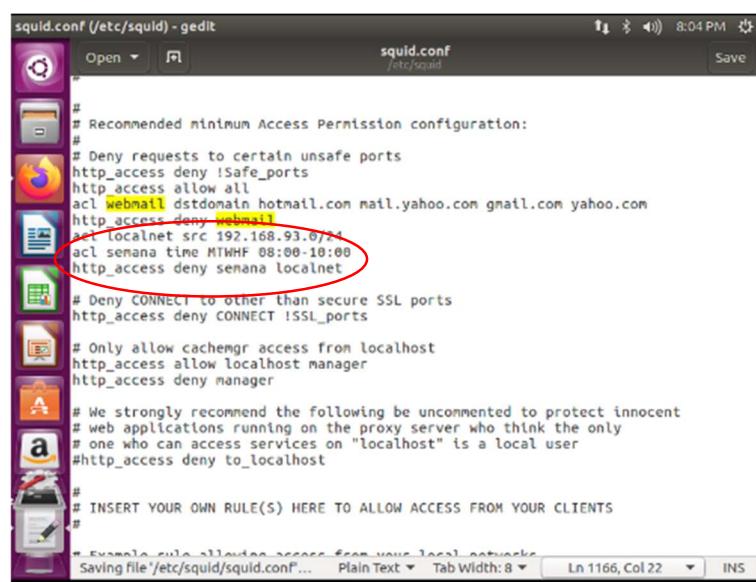
# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# Example rule allowing access from your local network
Saving file '/etc/squid/squid.conf'... Plain Text Tab Width: 8 Ln 1166, Col 22 INS
```

XIV. Restringir que no se pueda navegar ningún día de la semana entre las 8 y las 10 de la mañana.

Para restringir el acceso desde las 8 a las 10 am se establece la ip del área local con acl localnet src <ip>(en mi caso 192.168.93.0/24), después un acl semana time MTWHF 08:00-10:00. MTWHF cada sigla representa un dia de la semana en este caso de lunes a viernes. Luego http_access deny semana localnet (el acl de días y el de la ip)



```
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports
http_access allow all
acl webmail dstdomain hotmail.com mail.yahoo.com gmail.com yahoo.com
http_access deny webmail
acl localnet src 192.168.93.0/24
acl semana time MTWHF 08:00-10:00
http_access deny semana localnet

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

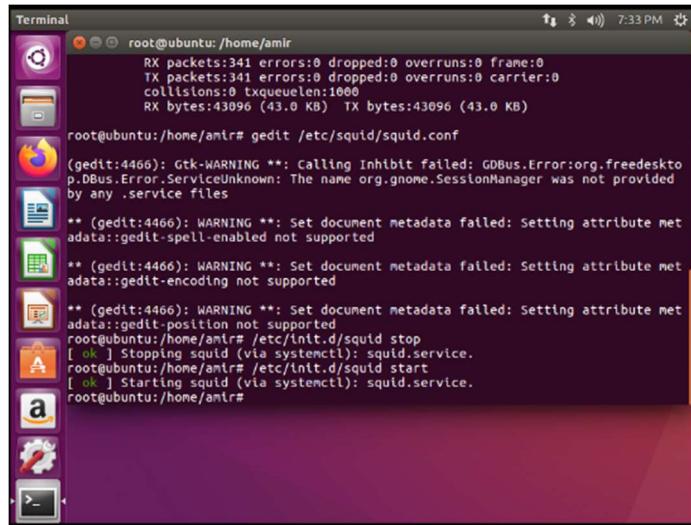
# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# Example rule allowing access from your local network
Saving file '/etc/squid/squid.conf'... Plain Text Tab Width: 8 Ln 1166, Col 22 INS
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	17-02-2022
	Nombre: Amir Fernando Mamdouh	

Después se reinicia el servicio de Squid, para ejecutar la nueva configuración.

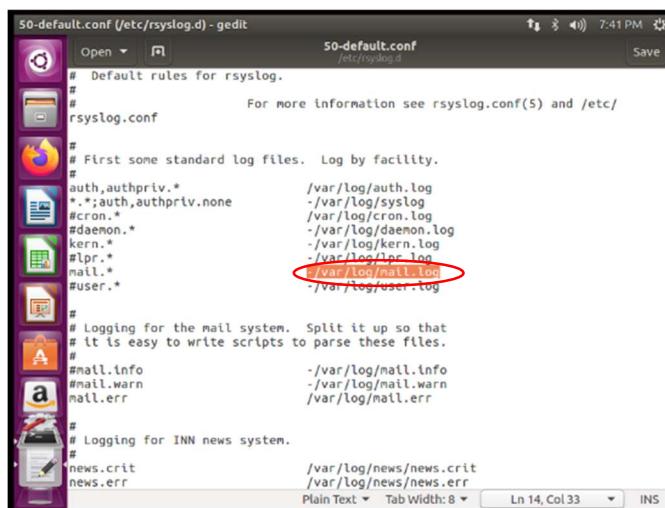


```

root@ubuntu:/home/amir# RX packets:341 errors:0 dropped:0 overruns:0 frame:0
root@ubuntu:/home/amir# TX packets:341 errors:0 dropped:0 overruns:0 carrier:0
root@ubuntu:/home/amir# collisions:0 txqueuelen:1000
root@ubuntu:/home/amir# RX bytes:43096 (43.0 KB) TX bytes:43096 (43.0 KB)
root@ubuntu:/home/amir# gedit /etc/squid/squid.conf
(gedit:4466): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:4466): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:4466): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:4466): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
root@ubuntu:/home/amir# /etc/init.d/squid stop
[ ok ] Stopping squid (via systemctl): squid.service.
root@ubuntu:/home/amir# /etc/init.d/squid start
[ ok ] Starting squid (via systemctl): squid.service.
root@ubuntu:/home/amir#

```

XV. Que los logs se almacenen en un fichero que se llame mensajes.log
Para configurar los logs debia acceder a /etc/syslog.conf pero este hace referencia a los archivos dentro de la carpeta /etc/rsyslog.d, por lo que dentro de este configure el archivo 50-default.conf referenciando logs de mail y mail error a /var/log/mensajes.log



```

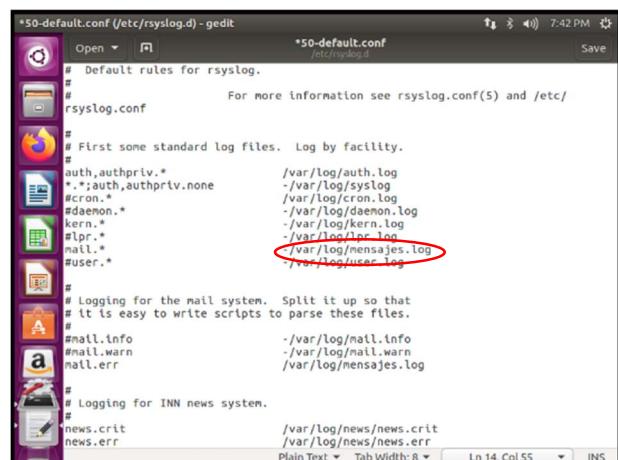
50-default.conf (/etc/rsyslog.d) - gedit
Open ▾ Save 50-default.conf
# Default rules for rsyslog.
# For more information see rsyslog.conf(5) and /etc/
rsyslog.conf

# First some standard log files. Log by facility.
auth,authpriv.*          /var/log/auth.log
.*;auth,authpriv.none     -/var/log/syslog
#cron.*                   /var/log/cron.log
#daemon.*                 /var/log/daemon.log
kern.*                    /var/log/kern.log
#lpr.*                     /var/log/lpr.log
mail.*                    /var/log/mail.* (Original path)
#user.*                   -/var/log/user.log

# Logging for the mail system. Split it up so that
# it is easy to write scripts to parse these files.
#mail.info                -/var/log/mail.info
#mail.warn                -/var/log/mail.warn
mail.err                  /var/log/mail.err

# Logging for INN news system.
news.crit                /var/log/news/news.crit
news.err                  /var/log/news/news.err

```



```

*50-default.conf (/etc/rsyslog.d) - gedit
*50-default.conf
Open ▾ Save *50-default.conf
# Default rules for rsyslog.
# For more information see rsyslog.conf(5) and /etc/
rsyslog.conf

# First some standard log files. Log by facility.
auth,authpriv.*          /var/log/auth.log
.*;auth,authpriv.none     -/var/log/syslog
#cron.*                   /var/log/cron.log
#daemon.*                 /var/log/daemon.log
kern.*                    /var/log/kern.log
#lpr.*                     /var/log/lpr.log
mail.*                    /var/log/mensajes.log (New path)
#user.*                   -/var/log/user.log

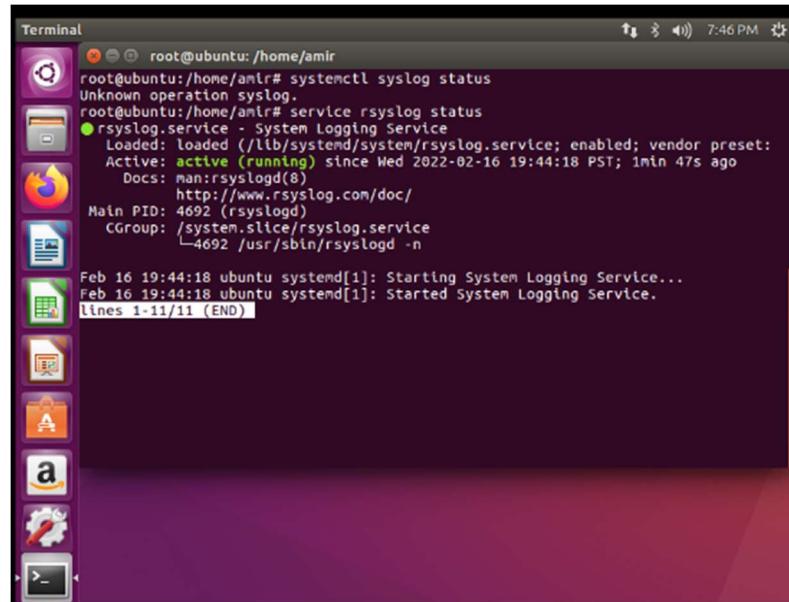
# Logging for the mail system. Split it up so that
# it is easy to write scripts to parse these files.
#mail.info                -/var/log/mail.info
#mail.warn                -/var/log/mail.warn
mail.err                  /var/log/mensajes.log

# Logging for INN news system.
news.crit                /var/log/news/news.crit
news.err                  /var/log/news/news.err

```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

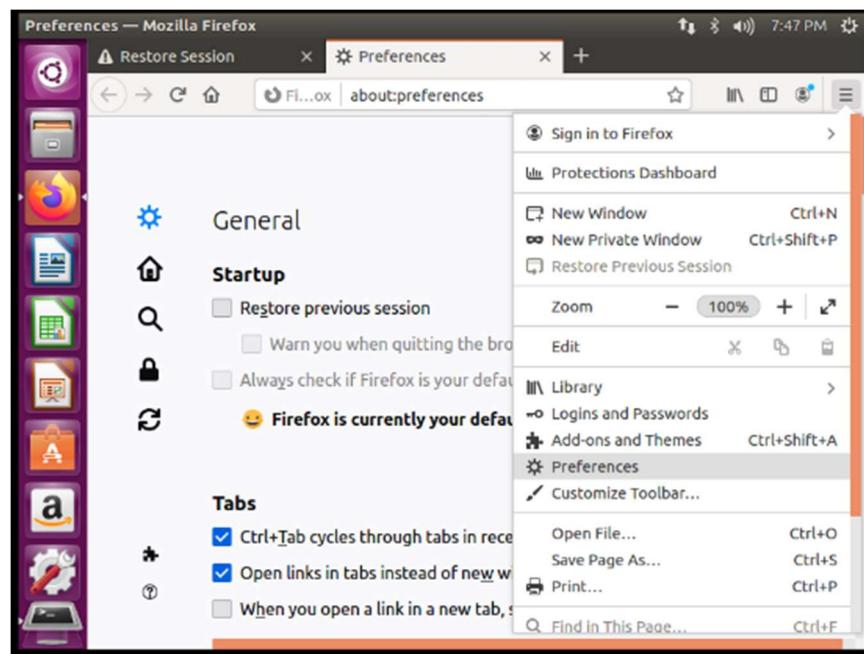
Después reinicio el servicio de syslog y luego compruebo que este activo.



```
Terminal
root@ubuntu:/home/amir
root@ubuntu:/home/amir# systemctl status syslog
Unknown operation syslog.
root@ubuntu:/home/amir# service rsyslog status
● rsyslog.service - System Logging Service
  Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: active
  Active: active (running) since Wed 2022-02-16 19:44:18 PST; 1min 47s ago
    Docs: man:rsyslogd(8)
          http://www.rsyslog.com/doc/
  Main PID: 4692 (rsyslogd)
  CGroup: /system.slice/rsyslog.service
          └─4692 /usr/sbin/rsyslogd -n

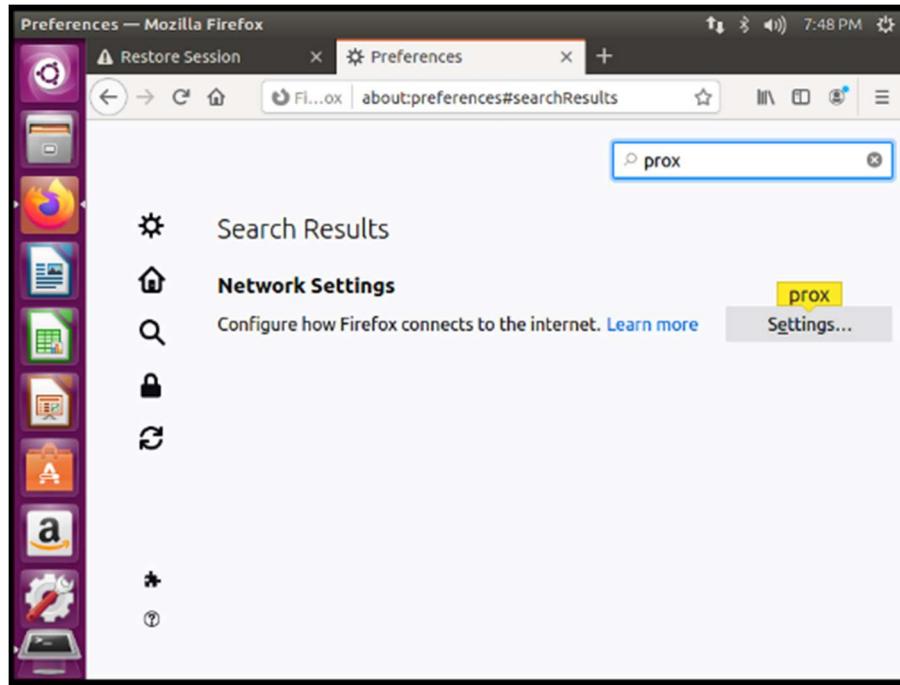
Feb 16 19:44:18 ubuntu systemd[1]: Starting System Logging Service...
Feb 16 19:44:18 ubuntu systemd[1]: Started System Logging Service.
lines 1-11/11 (END)
```

XVI. Instalar y configurar el navegador Firefox para usar el servidor Squid configurado y verificar que se aplican correctamente las restricciones.
Lo que toca es configurar Mozilla, por lo que primero se debe acceder a preferencias,



Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Busco proxy dentro del navegador y le doy click a la opción herramientas.



Squid tiene por defecto el puerto 3128 y es donde se ejecuta este servicio.

```
squid.conf (/etc/squid) - gedit
visible on the internal address.

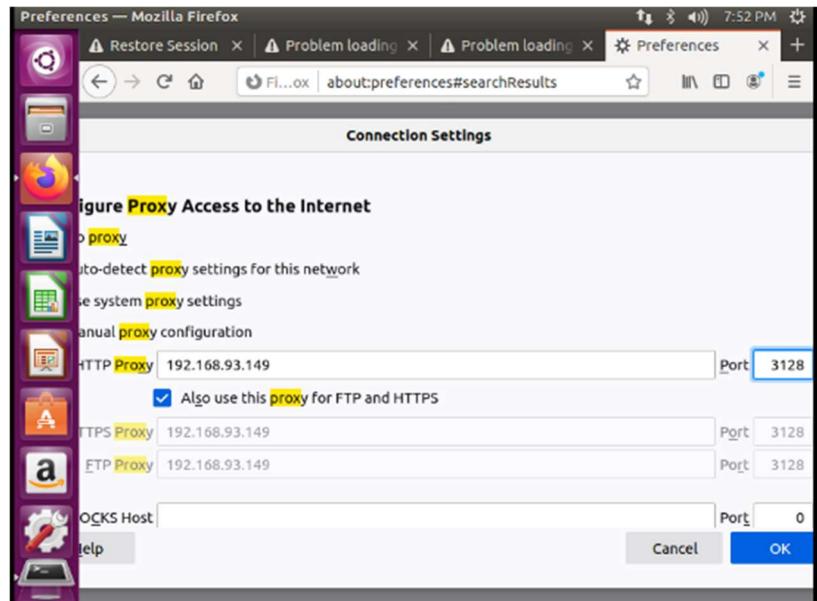
#
#
# Squid normally listens to port 3128
http_port 3128

# TAG: https_port
# Note: This option is only available if Squid is rebuilt with the
# --with-openssl
#
# Usage: [ip:]port cert=certificate.pem [key=key.pem] [mode] [options...]
#
# The socket address where Squid will listen for client requests made
# over TLS or SSL connections. Commonly referred to as HTTPS.
#
# This is most useful for situations where you are running squid in
# accelerator mode and you want to do the SSL work at the accelerator
# level.
#
# You may specify multiple socket addresses on multiple lines,
# each with their own SSL certificate and/or options.

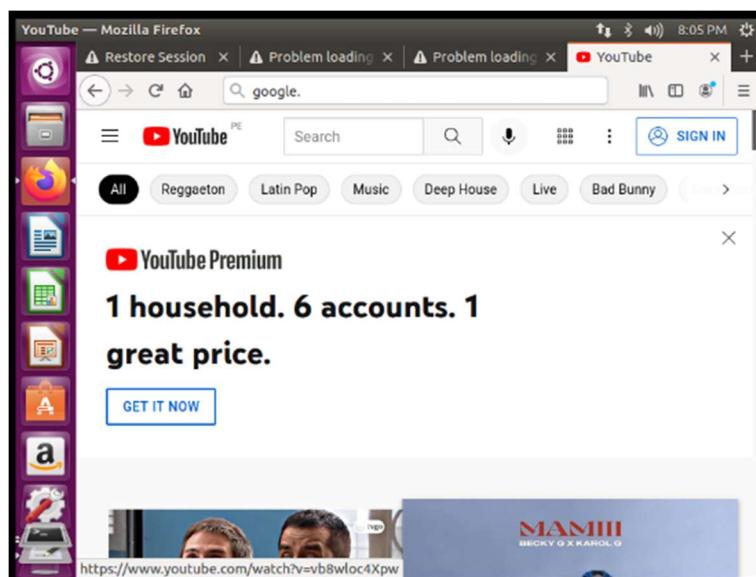
Modes:
    accel      Accelerator / reverse proxy mode
    intercept  Support for IP-Layer Interception of
               outgoing requests without browser settings.
               NP: disables authentication and IPv6 on the port.
Plain Text ▾ Tab Width: 8 ▾ Ln 1607, Col 31 ▾ INS
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Escribo mi propia ip de la maquina actual en HTTP Proxy y el puerto por defecto de squid, ya que no cambie esta configuración, además de seleccionar el usar esto también para ftp y https

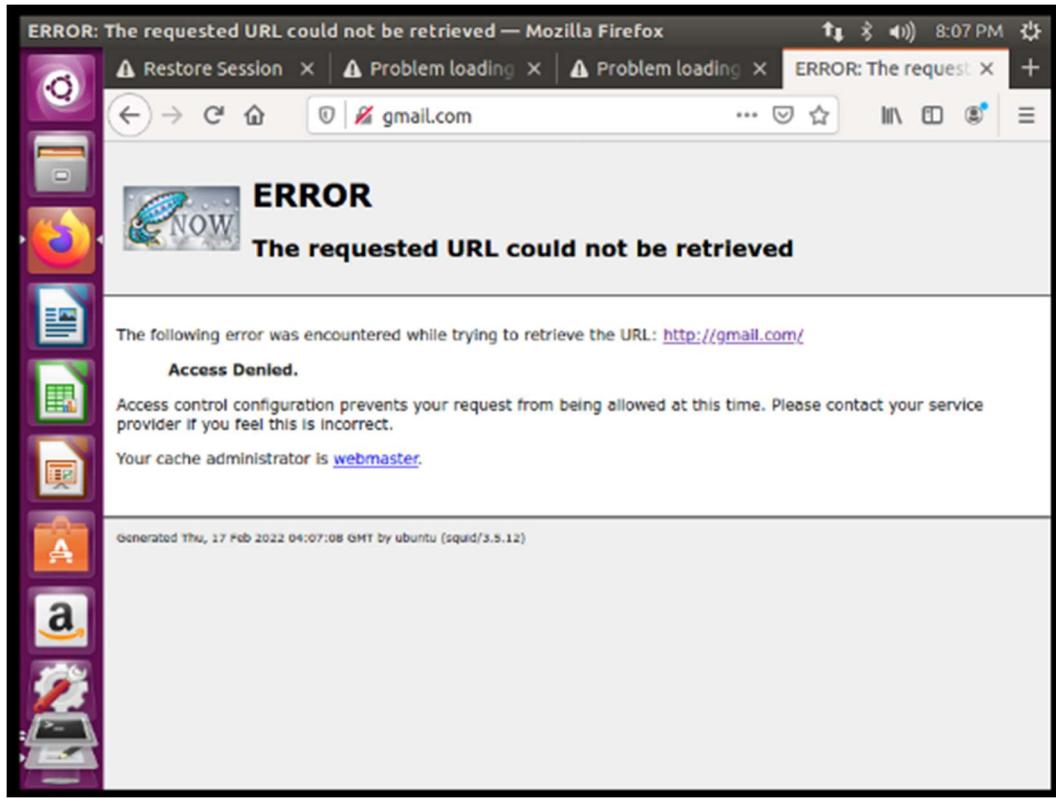


Comprobando de que estén funcionando las páginas las cuales no estén configuradas con squid. Para que esto funcione tuve que darle http_access allow all previamente, como mencione antes, sino no mostraría ninguna página.



Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

Y en el caso de intentar acceder a gmail.com muestra la pantalla de error de Squid



De esta forma, demuestro que el proxy esta funcionando correctamente.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	17-02-2022
	Nombre: Amir Fernando Mamdouh	

Bibliografia

- https://learning.lpi.org/es/learning-materials/101-500/102/102.1/102.1_01/
- <https://superuser.com/questions/1194229/why-cant-i-create-a-logical-partition-with-gparted>
- https://www.youtube.com/watch?v=yRSELRp7TQ&ab_channel=WilliMutschler
- <https://blog.desdelinux.net/proteger-las-entradas-de-windows-en-grub2-con-password/>
- <https://devconnected.com/how-to-add-user-to-sudoers-on-ubuntu-20-04/>
- <https://www.cyberciti.biz/tips/howto-write-shell-script-to-add-user.html>
- <https://superuser.com/questions/487312/how-to-add-a-user-to-wheel-group>
- <https://phoenixnap.com/kb/how-to-create-add-sudo-user-centos>
- <https://superuser.com/questions/67765/sudo-with-password-in-one-command-line>
- <https://acloudguru.com/hands-on-labs/enabling-su-sudo-access-with-wheel-group>
- <https://forums.opensuse.org/archive/index.php/t-500684.html>
- <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-wstation-privileges.html>
- <https://www.cyberciti.biz/faq/unix-linux-check-if-port-is-in-use-command/>
- <https://www.cyberciti.biz/faq/unix-linux-check-if-port-is-in-use-command/>
- <https://www.redeszone.net/tutoriales/servidores/servidor-openssh-linux- configuracion-maxima-seguridad/>
- <https://www.cyberciti.biz/tips/howto-write-shell-script-to-add-user.html>
- <https://www.howtogeek.com/50787/add-a-user-to-a-group-or-second-group-on-linux/>
- <https://linuxize.com/post/how-to-list-groups-in-linux/>
- <https://linuxize.com/post/how-to-create-groups-in-linux/#:~:text=defs%20file.-,Creating%20a%20Group%20in%20Linux,by%20the%20new%20group%20name.&text=The%20command%20adds%20an%20entry,adding%20users%20to%20the%20group%20.>
- <https://www.cyberciti.biz/faq/unix-linux-bsd-appleosx-bash-assign-variable- command-output/>
- https://linuxhint.com/length_of_string_bash/
- <https://unix.stackexchange.com/questions/493088/write-a-script-that-accepts-group-numbers-gids-as-parameters>
- <https://bash.cyberciti.biz/guide/If..else..fi>
- <https://www.cyberciti.biz/faq/systemctl-view-status-of-a-service-on-linux/>

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia Nombre: Amir Fernando Mamdouh	17-02-2022

<https://serverfault.com/questions/116505/squid-disallow-emailing>

<https://www.alcancelibre.org/staticpages/index.php/19-4-como-squid-tiempo>

<https://betterstack.com/community/guides/logging/linux/how-to-view-and-configure-linux-logs-on-ubuntu-20-04>

<https://rm-rf.es/installacion-basica-de-proxy-squid-y- configuracion-en-navegadores/>