UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Escuela de ciencias básicas tecnología e Ingeniería
Ingeniería de Sistemas
Sistemas operativos
301402_21
2014

INFORME DE LABORATORIO PRÁCTICA 2.

RUBÉN DARÍO CASTRO COLMENARES

CC 79623251

rubendcasro@gmail.com

ZONA CENTRO

CDAD JAG

Grupo 301402_21

TUTOR Y DIRECTOR DEL CURSO
JAIME JOSE VALDES

INTRODUCCIÓN

El presente informe pretende recopilar con evidencias las labores realizadas en el laboratorio en la práctica dos.

Utilizando sistemas operativos Windows y Linux se pretende mostrar las características, configuración, ventajas y desventajas del sistema de conexión cifrado SSH.

La actividad se desarrolló en dos equipos, uno con arquitectura ARM y sistema operativo Raspebian, el segundo un X86 con sistema operativo Fedora 17, virtual izando Windows y Ubuntu Linux para las pruebas de laboratorio.

El presente trabajo pretende mostrar las ventajas y recomendaciones en el uso de protocolo SSH, el protocolo SSH se ha extendido a diferentes plataformas, incluidas MS Windows a través de programas como Ciwin, entre otros.

También se muestran comandos básicos de usuario y de administración, se describe su funcionamiento y utilidad.

También se trabaja sobre una máquina virtual con Windows para mostrar un paralelo con el sistema operativo Linux.

El contenido evidencia la calidad de trabajo realizado en las practicas.

OBJETIVOS

Trabajar utilizando un plan basado en la teoría de sistemas operativos.

Identificar las ventajas y diferencias al utilizar el protocolo SSH.

Plasmar las actividades de laboratorio en un informe.

Facilitar las comunicaciones seguras entre sistemas, usando la arquitectura Cliente/Servidor.

Realizar configuración de seguridad en los recursos de los servidores.

Establecer conexiones tipo telnet con un servidor, pero de forma segura (la información va encriptado).

Administración de grupos, usuarios y permisos, para la gestión de recursos del sistema.

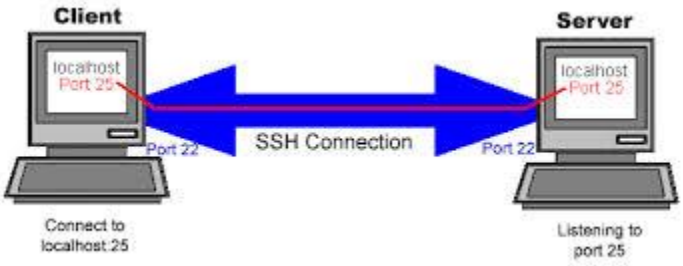
INTRODUCCIÓN O TEORÍA

SSH es uno de los protocolos más utilizados en entornos tipo Unix, es un intérprete de ordenes o shell que ejecuta las tareas de menara segura.

También es utilizado como FTP, opción a sistema de archivos como NFS, como túnel seguro que permite la conexión segura de otros servicios de red a través de SSH.

Permite gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de

cualquier otra aplicación por un canal seguro tunelizado mediante SSH.



También permite automatizar tareas entre servidores ya que al establecer una relación de confianza la cuenta en el equipo remoto no requiere contraseña para ingresar al servidor, y ejecuta las conexiones de manera cifrada.

Para conectar desde un servidor a otro se utiliza el llamado al protocolo, muy parecido a telnet o ftp, se utiliza el comando ssh, para conectar al puerto TCP 22 no se requiere opciones adicionales sólo el nombre de la cuenta, la dirección IP y la contraseña.

Por ejemplo: ssh btulia@servidor

Para realizar las conexiones por otros puertos se utiliza la opción -p, por ejemplo: ssh -p 2498 btulia@servidor.

Esto en el entorno texto de Linux o Unix, para conectar desde un servidor Windows, se utiliza la utilidad putty, la conexión con putty se describe más adelante.

El protocolo permite copiar archivos mediante el comando scp, por ejemplo si deseamos trasladar un archivo de un servidor A a un servidor B:

Ejemplo: scp -P 2498 btulia@servidor:/home/btulia/archivo .
El ejemplo anterior copia un archivo en el equipo remoto al directorio actual donde se encuentra la cuenta.

1. Instalar el protocolo SSH en su sistema operativo LINUX (yum -y install openssh-server para instalación en la distribución de Centos o derivados de RedHad o para sistemas Ubuntu o derivados de debian apt-get install openssh-server).

```
[root@fedora17 ~]#
[root@fedora17 ~]# yum -y install openssh-server
```

Instalación del servidor ssh en un equipo con fedora 17

```
[root@fedora17 ~]# rpm -qa|grep openssh
openssh-5.9p1-30.fc17.x86_64
openssh-server-5.9p1-30.fc17.x86_64
openssh-askpass-5.9p1-30.fc17.x86_64
openssh-clients-5.9p1-30.fc17.x86_64
[root@fedora17 ~]#
```

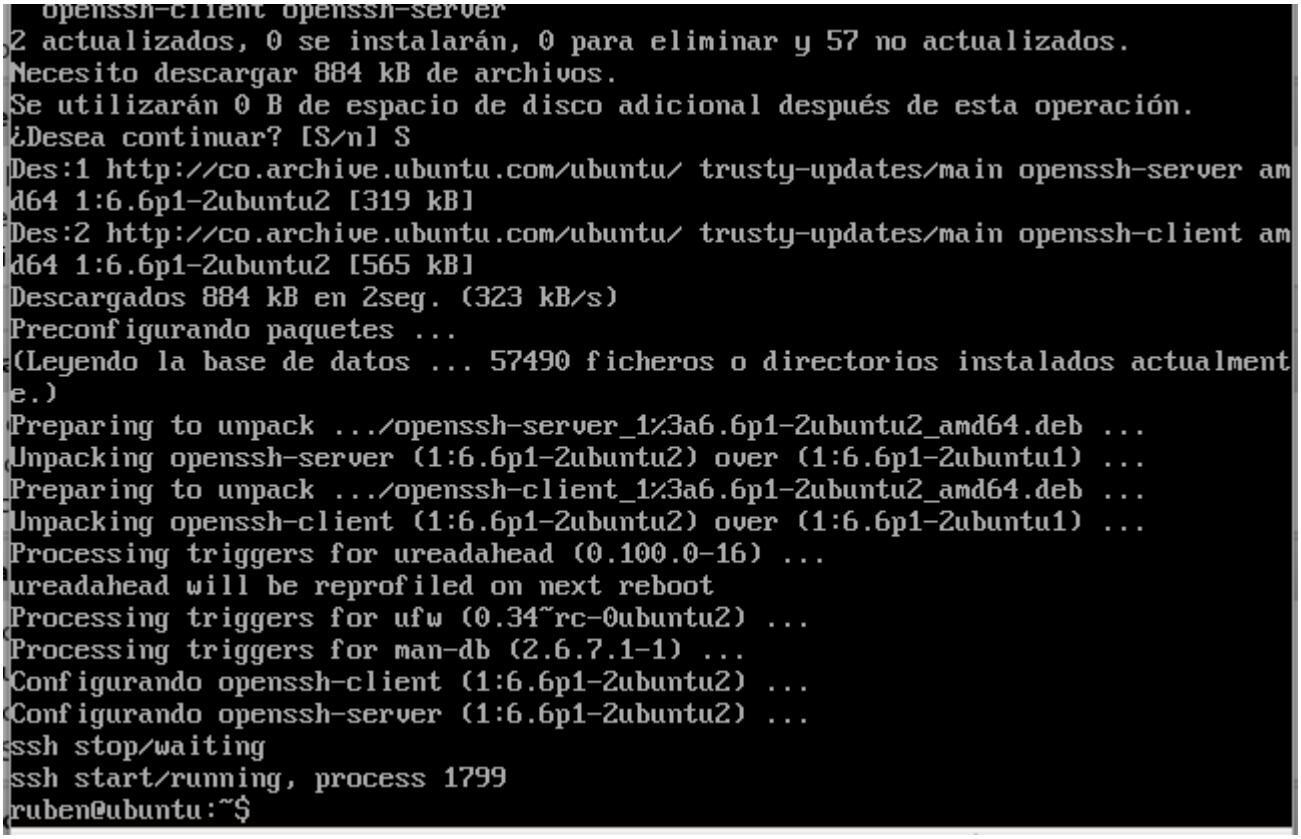
Validación post instalación.

```
ruben@ubuntu:~$ sudo apt-get install openssh-server
[sudo] password for ruben:
no talloc stackframe at ../source3/param/loadparm.c:4864, leaking memory
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  openssh-client
Paquetes sugeridos:
  ssh-askpass libpam-ssh keychain monkeysphere rssh molly-guard
Se actualizarán los siguientes paquetes:
  openssh-client openssh-server
2 actualizados, 0 se instalarán, 0 para eliminar y 57 no actualizados.
Necesito descargar 884 kB de archivos.
Se utilizarán 0 B de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Instalación del servidor ssh en una máquina virtual con UBUNTU server

```
ruben@ubuntu:~$ sudo apt-get install openssh-server
[sudo] password for ruben:
no talloc stackframe at ../source3/param/loadparm.c:4864, leaking memory
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  openssh-client
Paquetes sugeridos:
  ssh-askpass libpam-ssh keychain monkeysphere rssh molly-guard
Se actualizarán los siguientes paquetes:
  openssh-client openssh-server
2 actualizados, 0 se instalarán, 0 para eliminar y 57 no actualizados.
Necesito descargar 884 kB de archivos.
Se utilizarán 0 B de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://co.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-server am
d64 1:6.6p1-2ubuntu2 [319 kB]
Des:2 http://co.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-client am
d64 1:6.6p1-2ubuntu2 [565 kB]
Descargados 884 kB en 2seg. (323 kB/s)
Preconfigurando paquetes ...
(Leyendo la base de datos ... 57490 ficheros o directorios instalados actualment
e.)
Preparing to unpack .../openssh-server_1%3a6.6p1-2ubuntu2_amd64.deb ...
Unpacking openssh-server (1:6.6p1-2ubuntu2) over (1:6.6p1-2ubuntu1) ...
```

Proceso de instalación.



Instalación completa

2. Verifique los archivos de configuración identifique por lo menos 8 funciones de SSH e indique su función.

Archivo de configuración del Servidor sshd_conf
Archivo de configuración del Cliente ssh_conf

Archivo sshd_conf

```
[root@fedora17 ~]# cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.84 2011/05/23 03:30:07 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

```
# The default requires explicit activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile    .ssh/authorized_keys

#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
#GSSAPIAuthentication no
GSSAPIAuthentication yes
#GSSAPICleanupCredentials yes
GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in Fedora and may cause several
# problems.
#UsePAM no
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
```

```
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none

# no default banner path
#Banner none

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server

# Uncomment this if you want to use .local domain
#Host *.local
#       CheckHostIP no

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       ForceCommand cvs server
```

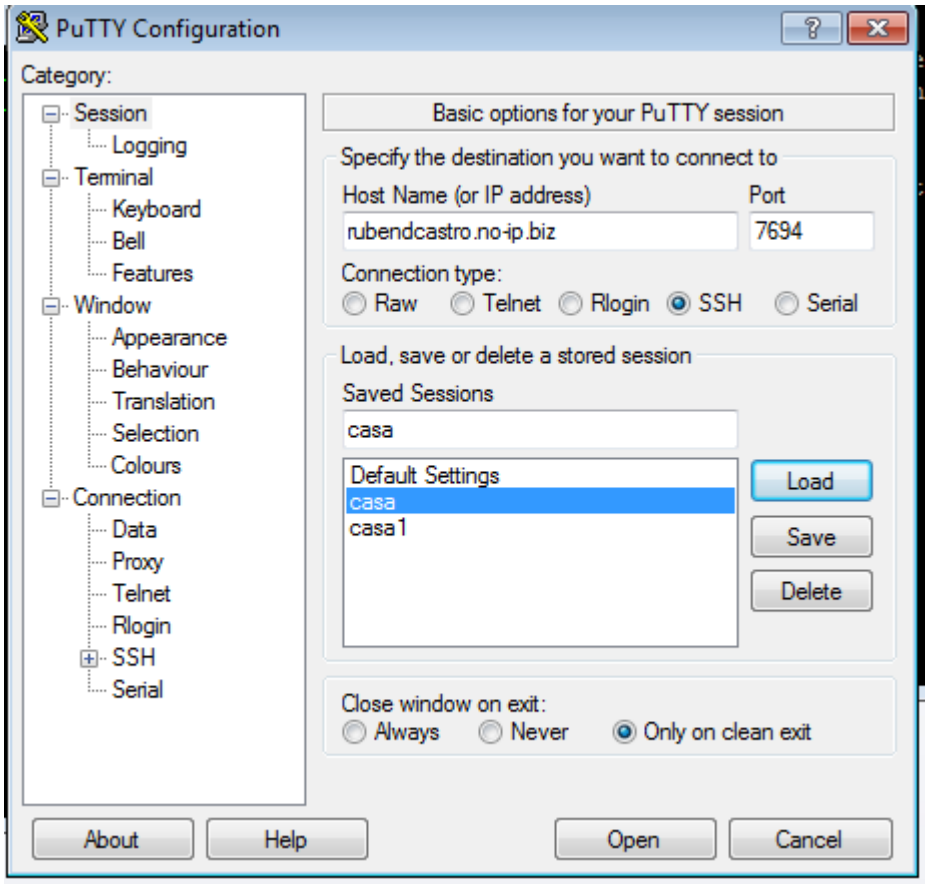
8 funciones de ssh:

1. Aunque no aparece en el archivo de configuración, existe una extraordinaria utilidad llamada SSHFS, sistema de archivos de ssh, la cual no interfiere con el buen funcionamiento de un servidor de archivos comparando SSHFS contra NFS, no requiere privilegios especiales para montar un SSHFS y se puede desde el directorio home, la unión de SSH con FUSE logra una gran solución segura y rápida para compartir archivos vía red.
2. Generar acceso al entorno gráfico por medio de la función X11Forwarding, con lo cual podemos iniciar programas de entorno gráfico de manera remota.
3. Se puede modificar el puerto de servicio de SSH, normalmente es el puerto 22, pero aún más seguro si se utiliza otro diferente al puerto TCP 22, por ejemplo un puerto 8799.
4. Colocando en el archivo la opción PermitRootLogin no, se puede restringir el acceso de la cuenta root directamente por ssh, esto mejora la seguridad del sistema.

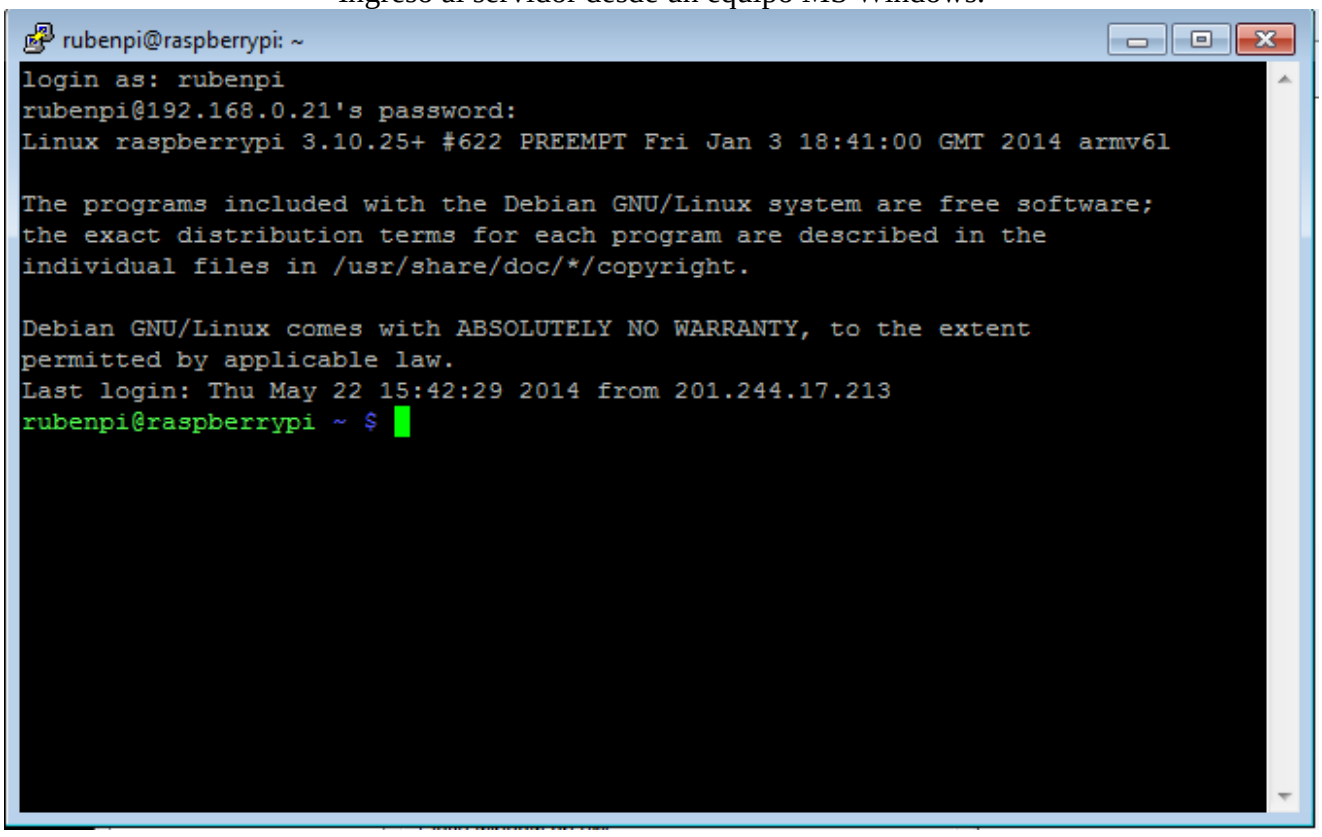
5. El servicio ssh se puede apoyar en el servicio de cifrado con Kerberos "Kerberos options" para mejorar aún más la seguridad
6. Refiriendo se a la parte de la configuración HostKey /etc/ssh/ssh_host_dsa_key. Se puede configurar un acceso remoto sin que pida contraseña desde otro servidor, esto con unos requisitos especiales en cuanto a permisos, se recomienda que la cuenta tenga configurada una contraseña, lo anterior se llama una relación de confianza por ssh, la relación de confianza permite automatizar procesos entre servidores sin que se requiere intervención del operador para dar una contraseña.
7. El servidor ssh se puede apoyar en dos tipos de sistema de cifrado, el cifrado DSA y el RSA, se puede ver en la configuración de HostKey, el cual maneja estos dos tipos.
8. En una configuración estricta, la cuenta que ingresa al servidor puede cambiar de directorio de destino al configurar la opción ChrootDirectory.
9. El servidor permite configurar un mensaje de bienvenida a través de la opción Banner.
10. En la sección de Authentication del archivo, se pueden configurar parámetros como máximo de intentos fallidos "MaxAuthTries", tiempo que el servidor le permite para ingresar datos de inicio de sesión "LoginGraceTime", máximo de sesiones permitidas " MaxSessions"

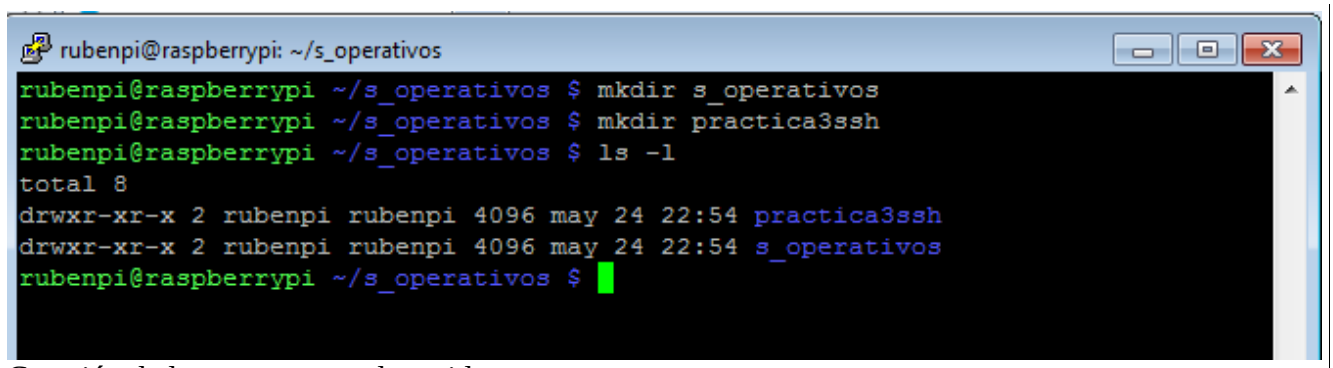
```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

3. Desde, el sistema operativo Windows realice la conexión remota a su servidor SSH con el programa fillezilla o con putty cree 2 carpetas con los siguientes nombres practica3ssh y s_operativos.



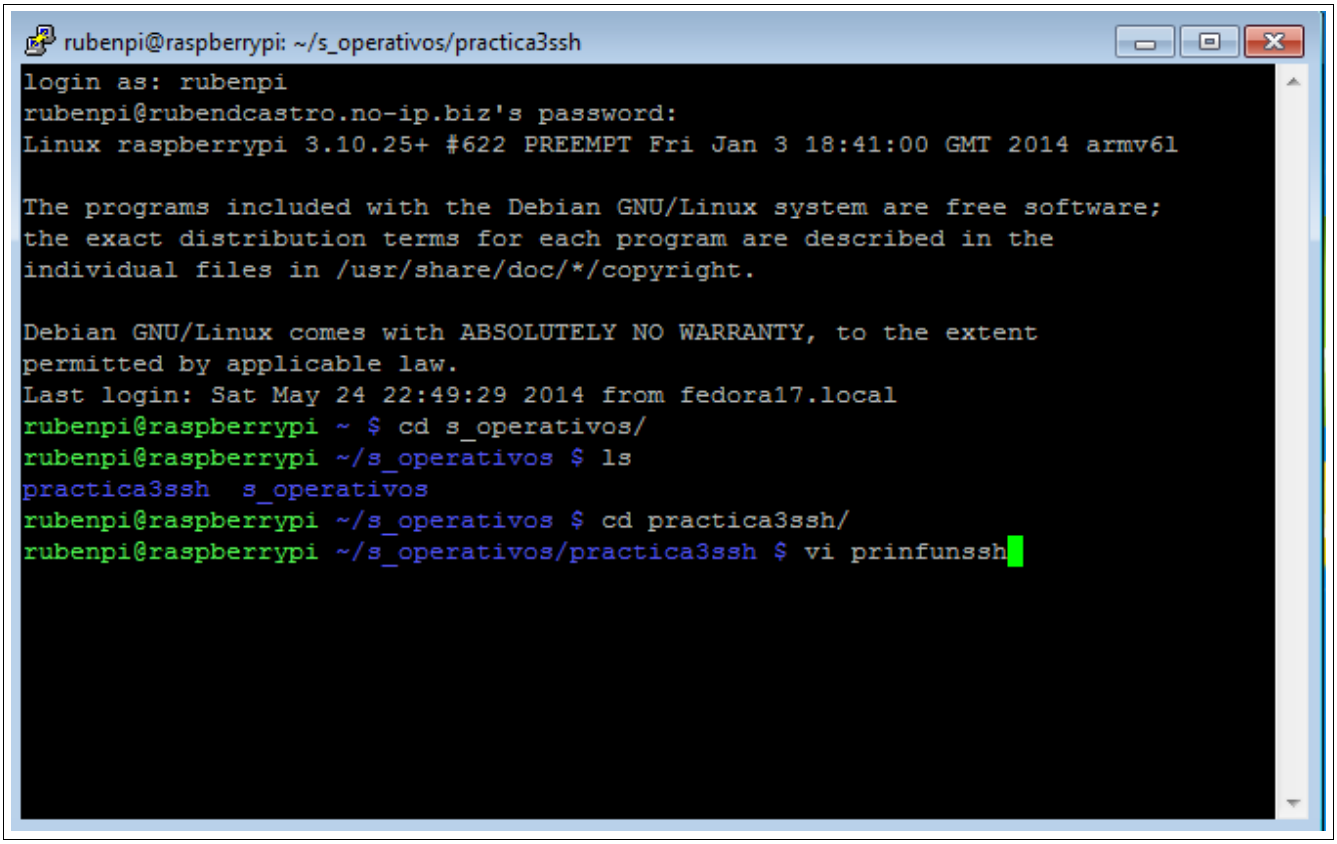
Ingreso al servidor desde un equipo MS Windows.

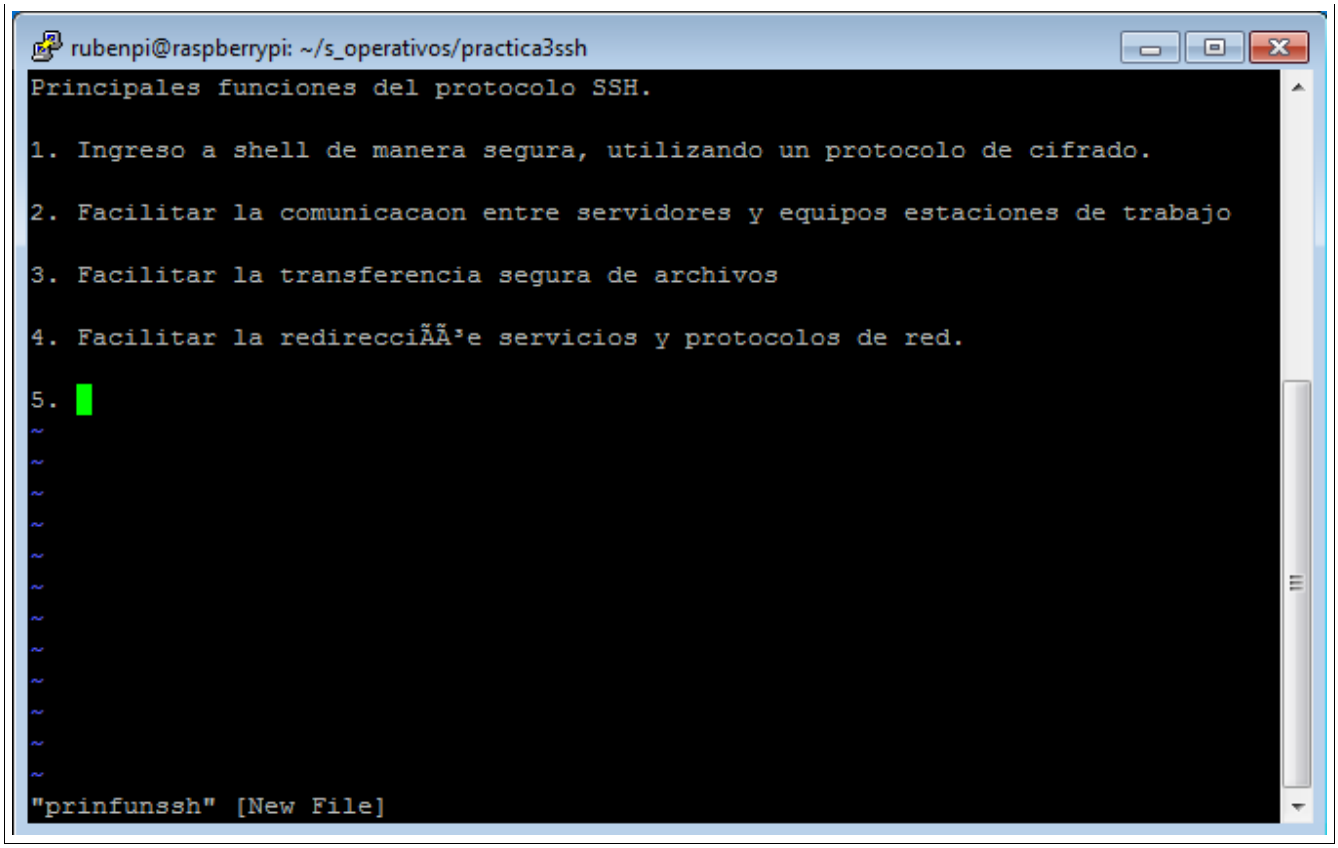




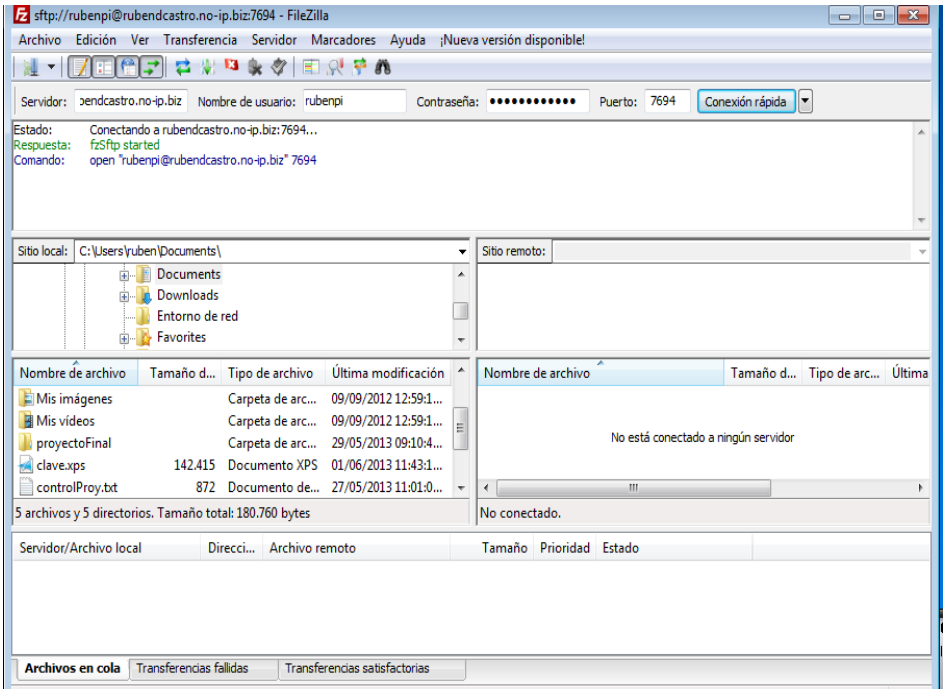
Creación de las carpetas en el servidor.

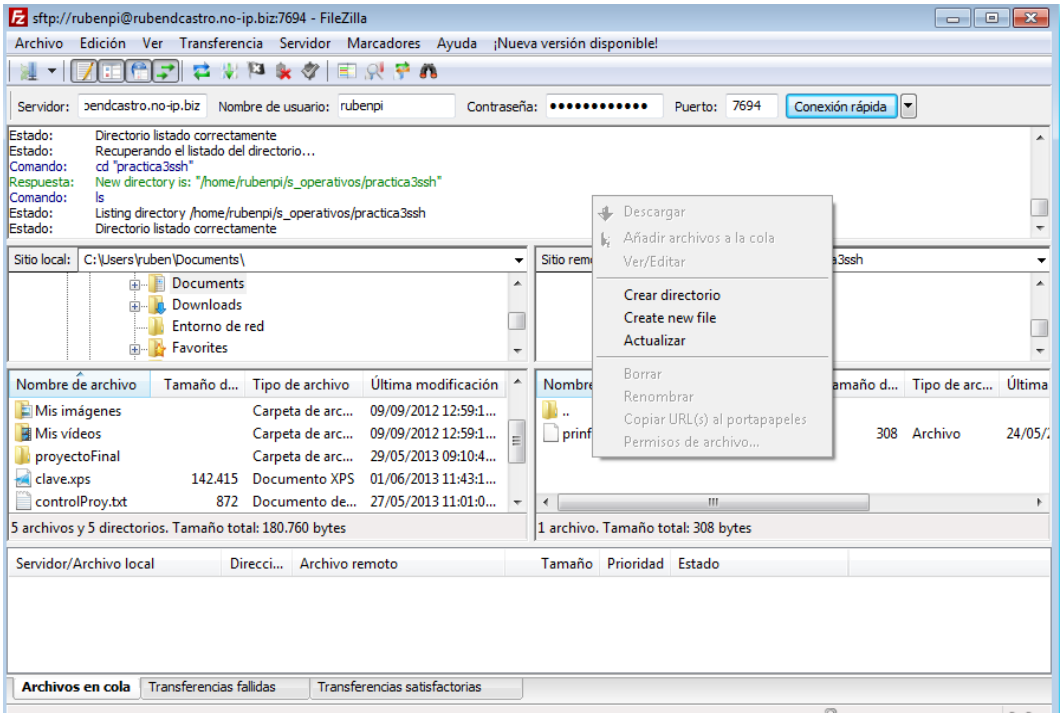
4. Cree un archivo dentro de la carpeta practica3ssh que contenga el nombre de las principales funciones del protocolo SSH.

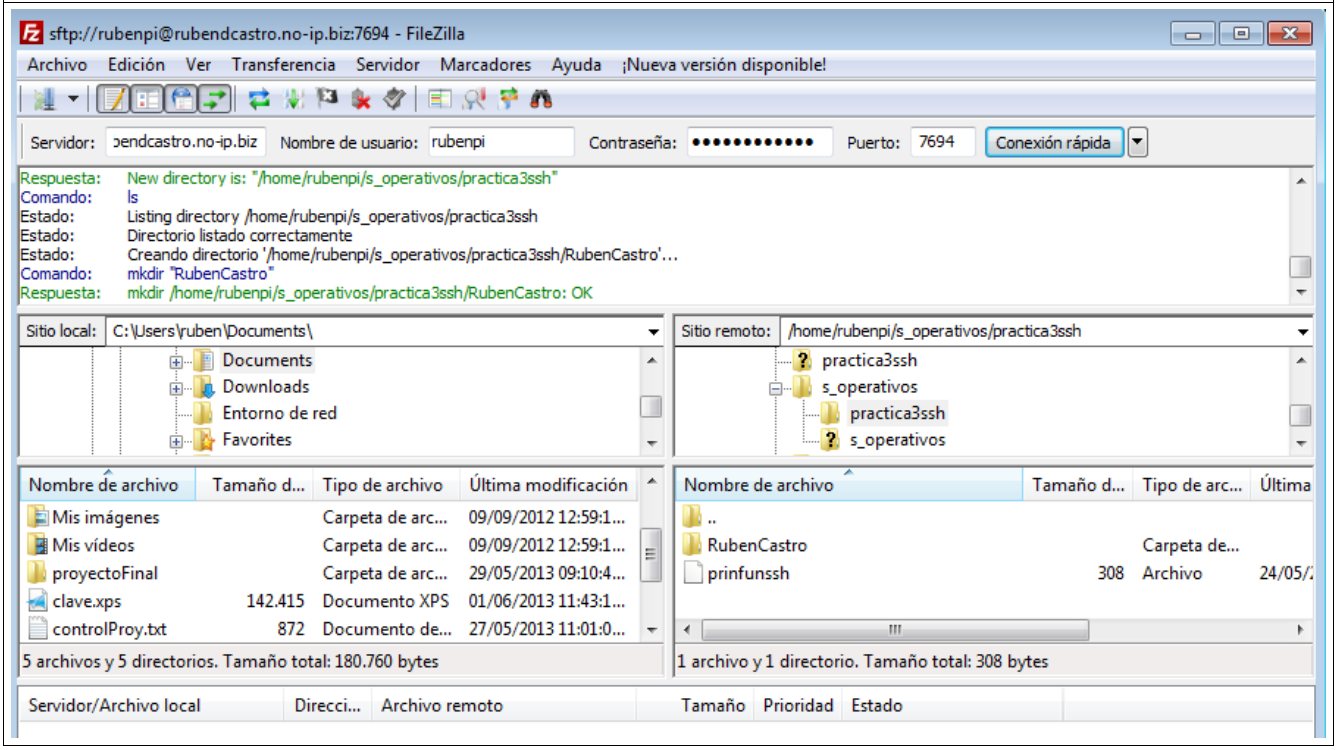


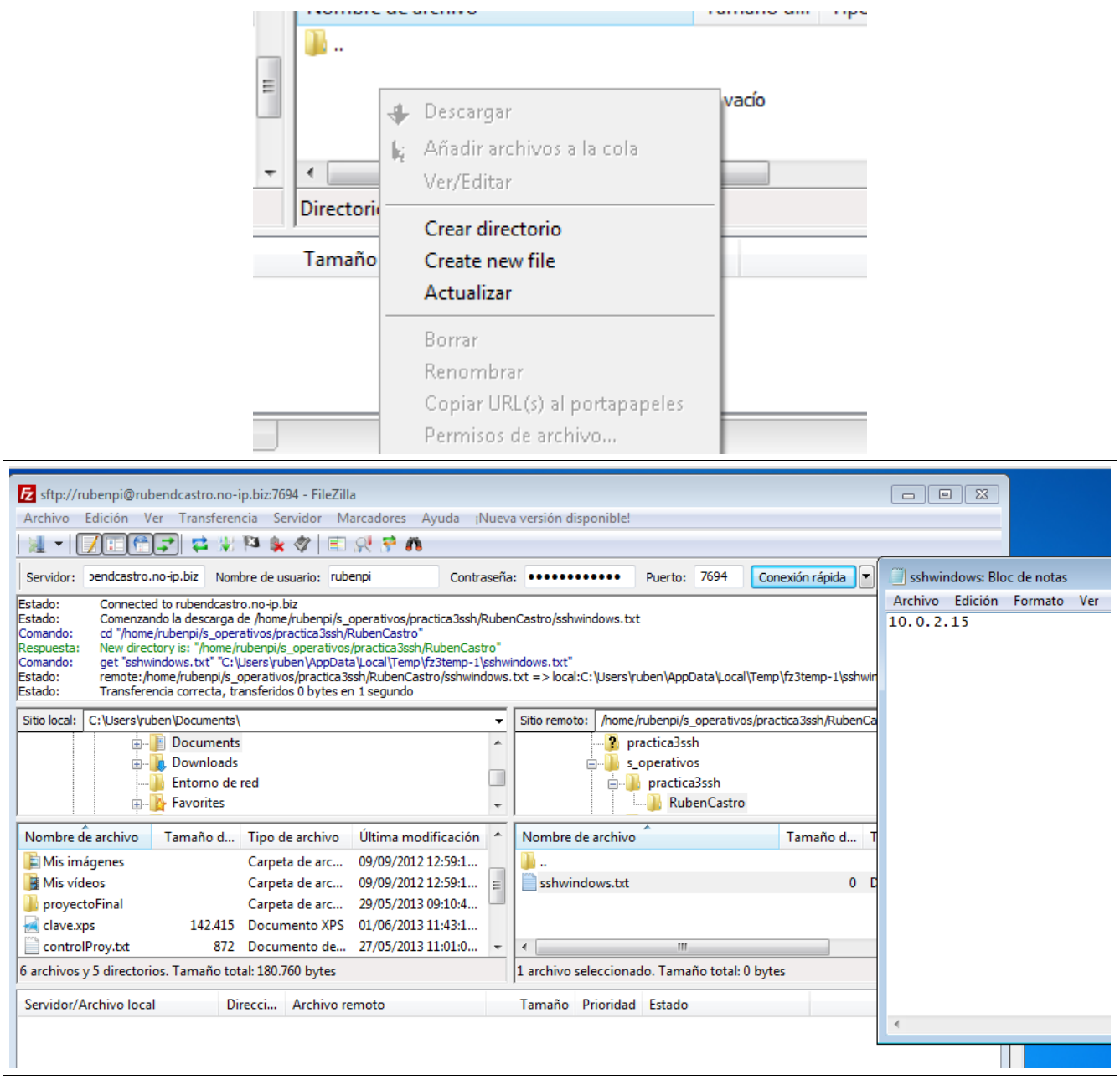


5. Conecte su servidor SSH desde el sistema operativo Windows lo puede realizar por medio del programa filezilla cliente cree dentro de la carpeta practica3ssh, una carpeta con su nombre y un archivo con el nombre de sshwindows.txt dentro de el escriba la dirección IP de su máquina Windows.




sftp://rubenpi@rubendcastro.no-ip.biz:7694 - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda ¡Nueva versión disponible!
Servidor: Nombre de usuario: rubenpi Contraseña: Puerto: 7694 Conexión rápida
Estado: Directorio listado correctamente
Estado: Recuperando el listado del directorio…
Comando: cd "practica3ssh"
Respuesta: New directory is: "/home/rubenpi/s_operativos/practica3ssh"
Comando: ls
Estado: Listing directory /home/rubenpi/s_operativos/practica3ssh
Estado: Directorio listado correctamente
Descargar
Añadir archivos a la cola
Ver/Editar
Crear directorio
Create new file
Actualizar
Borrar
Renombrar
Copiar URL(s) al portapapeles
Permisos de archivo...
Sitio local: C:\Users\ruben\Documents\
Documents
Downloads
Entorno de red
Favorites
Nombre de archivo Tamaño d... Tipo de archivo Última modificación
Mis imágenes Carpeta de arc... 09/09/2012 12:59:1...
Mis vídeos Carpeta de arc... 09/09/2012 12:59:1...
proyectoFinal Carpeta de arc... 29/05/2013 09:10:4...
clave.xps 142.415 Documento XPS 01/06/2013 11:43:1...
controlProy.txt 872 Documento de... 27/05/2013 11:01:0...
5 archivos y 5 directorios. Tamaño total: 180.760 bytes
308 Archivo
1 archivo. Tamaño total: 308 bytes
Servidor/Archivo local Direcci... Archivo remoto Tamaño Prioridad Estado
Archivos en cola Transferencias fallidas Transferencias satisfactorias

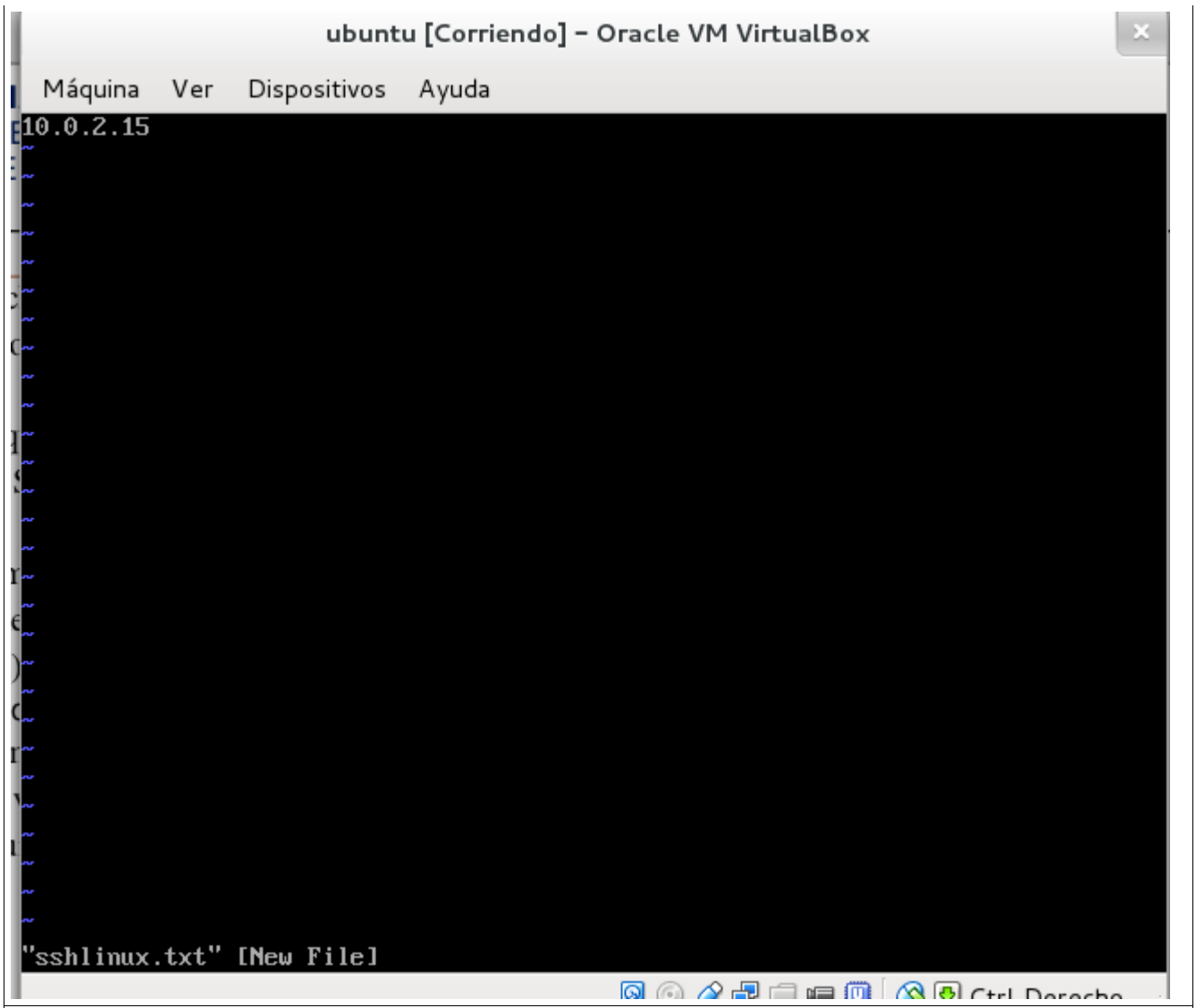

sftp://rubenpi@rubendcastro.no-ip.biz:7694 - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda ¡Nueva versión disponible!
Servidor: Nombre de usuario: rubenpi Contraseña: Puerto: 7694 Conexión rápida
Respuesta: New directory is: "/home/rubenpi/s_operativos/practica3ssh"
Comando: ls
Estado: Listing directory /home/rubenpi/s_operativos/practica3ssh
Estado: Directorio listado correctamente
Estado: Creando directorio '/home/rubenpi/s_operativos/practica3ssh/RubenCastro'…
Comando: mkdir "RubenCastro"
Respuesta: mkdir /home/rubenpi/s_operativos/practica3ssh/RubenCastro: OK
Sitio local: C:\Users\ruben\Documents\
Documents
Downloads
Entorno de red
Favorites
Sitio remoto: /home/rubenpi/s_operativos/practica3ssh
practica3ssh
s_operativos
practica3ssh
s_operativos
Nombre de archivo Tamaño d... Tipo de archivo Última modificación
Mis imágenes Carpeta de arc... 09/09/2012 12:59:1...
Mis vídeos Carpeta de arc... 09/09/2012 12:59:1...
proyectoFinal Carpeta de arc... 29/05/2013 09:10:4...
clave.xps 142.415 Documento XPS 01/06/2013 11:43:1...
controlProy.txt 872 Documento de... 27/05/2013 11:01:0...
5 archivos y 5 directorios. Tamaño total: 180.760 bytes
Nombre de archivo Tamaño d... Tipo de archivo Última
..
RubenCastro Carpeta de...
prinfunssh 308 Archivo 24/05/
1 archivo y 1 directorio. Tamaño total: 308 bytes
Servidor/Archivo local Direcci... Archivo remoto Tamaño Prioridad Estado



6. Conecten dos máquinas virtuales con otro compañero del grupo de LINUX a LINUX, haciendo conexión SSH dentro de la carpeta s_operativos de su compañero cree un carpeta con su nombre ejemplo Juan_Perez y un archivo con el nombre sshlinux.txt dentro de él escriba la dirección IP de su máquina, se deben conectar mediante un puerto diferente al 22 por lo cual se debe cambiar el puerto en los archivos de configuración (se recomienda hacer uso de un rango entre 1025 y 65535)

```
ruben@ubuntu:~$ ssh -p 7694 rubenpi@rubendcastro.no-ip.biz
The authenticity of host '[rubendcastro.no-ip.biz]:7694 ([186.84.129.88]:7694)'
can't be established.
ECDSA key fingerprint is 6b:48:42:fe:5e:81:79:b5:8f:62:99:7b:b6:11:0d:29.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[rubendcastro.no-ip.biz]:7694,[186.84.129.88]:7694'
(ECDSA) to the list of known hosts.
```

```
-h
ruben@ubuntu:~$ ping google.com
PING google.com (74.125.196.101) 56(84) bytes of data.
64 bytes from yk-in-f101.1e100.net (74.125.196.101): icmp_seq=1 ttl=63 time=115
ms
64 bytes from yk-in-f101.1e100.net (74.125.196.101): icmp_seq=2 ttl=63 time=116
ms
^C
--- google.com ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 2004ms
rtt min/avg/max/mdev = 115.797/115.950/116.103/0.153 ms
ruben@ubuntu:~$
ruben@ubuntu:~$ ssh -p 7694 rubenpi@rubendcastro.no-ip.biz
The authenticity of host '[rubendcastro.no-ip.biz]:7694 ([186.84.129.88]:7694)'
can't be established.
ECDSA key fingerprint is 6b:48:42:fe:5e:81:79:b5:8f:62:99:7b:b6:11:0d:29.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[rubendcastro.no-ip.biz]:7694,[186.84.129.88]:7694'
(ECDSA) to the list of known hosts.
rubenpi@rubendcastro.no-ip.biz's password:
Linux raspberrypi 3.10.25+ #622 PREEMPT Fri Jan 3 18:41:00 GMT 2014 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat May 24 22:59:34 2014 from 186.84.129.88
rubenpi@raspberrypi ~ $ cd s_operativos/
```



7. Con el comando chmod ejecute las 7 opciones de permisos de lectura, escritura y ejecución a la carpeta s_operativos intercale los niveles de permisos e intente realizar el ejercicio anterior de acuerdo a la siguiente tabla:

Octal Number	Permissions
0	No Permission
1	Execute
2	Write
3	Write, execute
4	Read
5	Read, Execute
6	Read, Write
7	Read, Write, Execute

```
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 000 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ ls -l
total 4
d--------- 2 rubenpi rubenpi 4096 may 24 23:22 RubenCastro
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
-bash: cd: RubenCastro/: Permiso denegado
rubenpi@raspberrypi ~/s_operativos/s_operativos $
```

```
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 111 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls
ls: no se puede abrir el directorio .: Permiso denegado
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls -l
ls: no se puede abrir el directorio .: Permiso denegado
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $
```

```
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 222 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
-bash: cd: RubenCastro/: Permiso denegado
rubenpi@raspberrypi ~/s_operativos/s_operativos $
```

```
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 333 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls
ls: no se puede abrir el directorio .: Permiso denegado
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ cd ..
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 444 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
-bash: cd: RubenCastro/: Permiso denegado
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 555 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls
sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ cd ..
rubenpi@raspberrypi ~/s_operativos/s_operativos $ ls -l
total 4
dr-xr-xr-x 2 rubenpi rubenpi 4096 may 24 23:22 RubenCastro
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 666 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
-bash: cd: RubenCastro/: Permiso denegado
rubenpi@raspberrypi ~/s_operativos/s_operativos $ chmod 777 RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos $ cd RubenCastro/
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ vi sshlinux.txt
```

8. Ejecute los siguientes comandos e indique que permisos son otorgados o restringidos:
chmod ug+x sshlinux.txt
chmod go-rx sshwindows.txt
chmod uo+wx sshlinux.txt
chmod u=rwx,g=rw,o= * sshwindows.txt

```
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ chmod ug+x sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls -l
total 4
-rwxr-xr-- 1 rubenpi rubenpi 10 may 24 23:22 sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ chmod go+rx sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls -l
total 4
-rwxr-xr-x 1 rubenpi rubenpi 10 may 24 23:22 sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ chmod uo+wx sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls -l
total 4
-rwxr-xrwx 1 rubenpi rubenpi 10 may 24 23:22 sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ chmod u+rwx,g=rw,o=* sshlinux.txt
chmod: modo invÃ¡lido: Â«u+rwx,g=rw,o=*Â»
Pruebe `chmod --help' para mÃ¡s informaciÃ³n.
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls -l
total 4
-rwxr-xrwx 1 rubenpi rubenpi 10 may 24 23:22 sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ chmod u+rwx,g=rw,o= * sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $ ls -l
total 4
-rwxrw---- 1 rubenpi rubenpi 10 may 24 23:22 sshlinux.txt
rubenpi@raspberrypi ~/s_operativos/s_operativos/RubenCastro $
```

chmod ug+x sshlinux.txt Los permisos otorgados son de lectura, escritura y ejecución para el propietario, lectura y ejecución para el grupo y de sólo lectura para los otros usuarios.
chmod go-rx sshwindows.txt Los permisos otorgados son de lectura, escritura y ejecución para el propietario, lectura y ejecución para el grupo y lectura y ejecución para otros.
chmod uo+wx sshlinux.txt Los permisos otorgados son de lectura, escritura y ejecución para el propietario, lectura y ejecución para el grupo y lectura, escritura y ejecución para otros.
chmod u=rwx,g=rw,o= * sshwindows.txt Los permisos otorgados son de lectura, escritura y ejecución para el propietario, lectura y escritura para el grupo y ningún permiso para otros.

9. Desde la línea de comandos cree los siguiente grupos y usuarios:

GRUPOS	USUARIOS
gruposistemas	Usuario1
	Usuario2
grupooperativos	Usuario3
	Usuario4

(y) y cuatro usuarios (usuario1, usuario2, usuario3 y usuario4).

```
root@raspberrypi:~# groupadd gruposistemas
root@raspberrypi:~# groupadd grupooperativos
root@raspberrypi:~# useradd usuario1
root@raspberrypi:~# useradd usuario2
root@raspberrypi:~# useradd usuario3
root@raspberrypi:~# useradd usuario4
root@raspberrypi:~#
```

10. Asignar a usuario1 y usuario2 al gruposistemas y el usuario3 y usuario4 al grupooperativos.

```
root@raspberrypi:~# usermod -g gruposistemas usuario1
root@raspberrypi:~# usermod -g gruposistemas usuario2
root@raspberrypi:~# id usuario1
uid=1007(usuario1) gid=1008(gruposistemas) grupos=1008(gruposistemas)
root@raspberrypi:~#  usermod -g grupooperativos usuario3
root@raspberrypi:~#  usermod -g grupooperativos usuario4
root@raspberrypi:~#
```

11. Verificar los archivos de configuración de grupos y usuarios de Linux (passwd, shadow, group) y explicarlos.

```
statd:x:103:65534::/var/lib/nfs:/bin/false
messagebus:x:104:106::/var/run/dbus:/bin/false
usbmux:x:105:46:usbmux daemon,,,:/home/usbmux:/bin/false
lightdm:x:106:109:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:107:110:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:108:112:RealtimeKit,,,:/proc:/bin/false
mysql:x:109:114:MySQL Server,,,:/nonexistent:/bin/false
juli:x:1001:1002::/home/juli:/bin/bash
fafi:x:1002:1002::/home/fafi:/bin/bash
rdcastro:x:1003:1003::/home/rdcastro:/bin/bash
colord:x:110:117:colord colour management daemon,,,:/var/lib/colord:/bin/false
avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
hplip:x:112:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:113:119::/home/saned:/bin/false
smmta:x:114:120:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:115:121:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
ilda:x:1004:1005::/home/ilda:/bin/bash
rubenpi:x:1006:1007::/home/rubenpi:/bin/bash
motion:x:116:124::/home/motion:/bin/false
usuario1:x:1007:1008::/home/usuario1:/bin/bash
usuario2:x:1008:1008::/home/usuario2:/bin/bash
usuario3:x:1009:1009::/home/usuario3:/bin/bash
usuario4:x:1010:1009::/home/usuario4:/bin/bash
root@raspberrypi:~#
```

Archivo /etc/passwd, en éste archivo se guarda la configuración de usuarios, se divide en columnas separadas por doble punto ":" en la primera columna aparece el nombre del usuario, en la segunda una "x" que representa el espacio de la contraseña, el siguiente el número ID del usuario, luego el número ID del grupo, un espacio donde se puede colocar la descripción de la cuenta en modo comentario, luego el directorio home de la cuenta y por último la shell que ejecuta en cada ingreso al sistema.

```
root@raspberrypi:~# cat /etc/shadow
root:$6$ZLnHGbfu$miFYYOc3LynjxDYyUsTVHr7w3Tmp8M2Y1BXWmUwhJMF7HX88rfP/.Zq7UlI9fkUmhipwhkqv4jI/HAXb1qId0/:16059:0:9
9999:7:::
daemon:*:15689:0:99999:7:::
bin:*:15689:0:99999:7:::
sys:*:15689:0:99999:7:::
sync:*:15689:0:99999:7:::
games:*:15689:0:99999:7:::
man:*:15689:0:99999:7:::
lp:*:15689:0:99999:7:::
mail:*:15689:0:99999:7:::
news:*:15689:0:99999:7:::
uucp:*:15689:0:99999:7:::
proxy:*:15689:0:99999:7:::
www-data:*:15689:0:99999:7:::
backup:*:15689:0:99999:7:::
list:*:15689:0:99999:7:::
irc:*:15689:0:99999:7:::
gnats:*:15689:0:99999:7:::
nobody:*:15689:0:99999:7:::
libuuid:!:15689:0:99999:7:::
pi:$6$6h.A5Wqf$vLegvblK98JTIjzZIzAvGzY7291P6bKph7aNjIW1p1B7tv0g8gVk3SA2xErqxyYskd5uuVexAKFPae.//5/40/:15966:0:999
99:7:::
```

```
ilda:$6$BM4OONfZ$pipPo79S1X2VJdve6.rwSKfvt5OCsm6co/KN3Rod5B/xZjQ9Xfg/WOg38lWztu6kK4jzCbDlWwkr5B9Qs6pwR0
9999:7:::
rubenpi:$6$5NkYWUey$AVCe8YJvJ8wCBtKQ1l75e6s5xPm0CS4Np22Rv6SRiCT8alY30t9gHbyaquZIayBPI.3/PSd7evpXT0RtJ94
0:99999:7:::
motion:*:16076:0:99999:7:::
usuario1:!:16215:0:99999:7:::
usuario2:!:16215:0:99999:7:::
usuario3:!:16215:0:99999:7:::
usuario4:!:16215:0:99999:7:::
root@raspberrypi:~#
```

El archivo /etc/shadow, en éste archivo se guardan las contraseñas cifradas, en la columna inicial aparece el nombre de la cuenta, luego unos símbolos si tiene contraseña en caso de no tenerla aparece el símbolo e admiración "!", luego la configuración de vencimiento de la cuenta y configuración de ingreso.

```
ssl-cert:x:113:
mysql:x:114:
i2c:x:115:
juli:x:1002:
rdcastro:x:1003:
scanner:x:116:saned
colord:x:117:
avahi:x:118:
saned:x:119:
smmta:x:120:
smmsp:x:121:
web:x:1004:pi,rubenpi
rdma:x:122:
utempter:x:123:
ilda:x:1005:
rubenpi:x:1007:
motion:x:124:
gruposistemas:x:1008:
grupooperativos:x:1009:
usuario1:x:1010:
usuario2:x:1011:
usuario3:x:1012:
usuario4:x:1013:
root@raspberrypi:~#
```

El archivo /etc/groups guarda la información de configuración de las cuentas respecto a los grupos creados, también aparece el ID de la cuenta o grupo.
Un grupo puede tener contraseña también.

12. Elimine un usuario4 del grupooperativos.

```
root@raspberrypi:~# deluser usuario4 grupooperativo
/usr/sbin/deluser: El grupo `grupooperativo' no existe.
root@raspberrypi:~# id usuario4
uid=1010(usuario4) gid=1009(grupooperativos) grupos=1009(grupooperativos)
root@raspberrypi:~# deluser usuario4 grupooperativos
/usr/sbin/deluser: No puede eliminar al usuario de su grupo primario.
root@raspberrypi:~# id usuario2
uid=1008(usuario2) gid=1008(gruposistemas) grupos=1008(gruposistemas)
root@raspberrypi:~# usermod -g gruposisitemas usuario4
usermod: el grupo Â«gruposisitemasÂ» no existe
root@raspberrypi:~# usermod -g gruposistemas usuario4
root@raspberrypi:~# deluser usuario4 grupooperativos
/usr/sbin/deluser: El usuario `usuario4' no es un miembro del grupo grupooperativos.
root@raspberrypi:~# id usuario4
uid=1010(usuario4) gid=1008(gruposistemas) grupos=1008(gruposistemas)
root@raspberrypi:~#
```

13. Cree desde la línea de comandos Linux password para alguno de los usuarios que tiene creados ya sea del gruposistemas o del grupooperativos.

```
root@raspberrypi:~# passwd usuario2
Introduzca la nueva contraseÃ±a de UNIX:
Vuelva a escribir la nueva contraseÃ±a de UNIX:
passwd: contraseÃ±a actualizada correctamente
root@raspberrypi:~#
```

14. Bloquear en SSH el acceso al usuario root e ingresar con uno de los usuarios creados.

```
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
```

Se edita el archivo sshd_config y se agrega la opción PermitRootLogin co el valor no. De esta manera le cuenta de root no ingresará al sistema directamente por ssh.

```
login as: root
root@rubendcastro.no-ip.biz's password:
Access denied
root@rubendcastro.no-ip.biz's password:
```

Se hacen pruebas con la cuenta root.

```
login as: usuario2
usuario2@rubendcastro.no-ip.biz's password:
Linux raspberrypi 3.10.25+ #622 PREEMPT Fri Jan 3 18:41:00 GMT 2014 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Could not chdir to home directory /home/usuario2: No such file or directory
usuario2@raspberrypi:/$
```

Se ingresa al sistema con la cuenta usuario2.

15. Nombre las características y ventajas que ofrece el protocolo SSH.

El protocolo SSH ofrece un acceso a la shell del servidor cómodo, rápido y seguro.
El protocolo SSH es flexible y altamente configurable, permite modificar las características del servidor en pocos pasos.
El protocolo SSH permite trasladar archivos con la función SCP o SFTP, de manera confiable.
El protocolo SSH permite hacer túneles IP para exportar servicios a través de SSH.
El protocolo SSH en conjunto con FUSE permite configurar el sistema SSHFS que permite montar sobre nuestra carpeta, sin tener muchos privilegios, un directorio exportado por ssh.

CONCLUSIONES

El protocolo SSH permite una conexión rápida y segura desde cualquier equipo dentro del segmento de la red donde se encuentra el servidor.
El protocolo SSH permite elevar la seguridad cifrando la conexión, también se puede transferir de manera segura archivos y hacer túnel IP para re direccionar servicios de red.

El protocolo SSH tiene muchos usos y características, poder hacer un sistema de archivos a partir del protocolo hace que sea más seguro la comparación de archivos con otros equipos.

La configuración flexible de la seguridad del protocolo SSH permite facilitar la seguridad, por ejemplo cambiando el puerto de conexión del puerto de red 22 a otro para así mejorar la seguridad.

REFERENCIA DOCUMENTAL

(http://www.ubuntu.com/getubuntu/download)

(https://www.virtualbox.org)

http://www.linuxtotal.com.mx/?cont=info_admon_002

http://support.microsoft.com/?ln=es-es

SISTEMAS OPERATIVOS por David Luiz La Red Martinez.

*sistop.gwolf.org/html/.../**Sistemas_Operativos**_-_Luis_La_Red_Martinez....*

http://www.mcgraw-hill.es/bcv/guide/capitulo/8448180321.pdf

http://www.informatica.us.es/~ramon/articulos/AdminAvanzadaLinux.pdf

http://www.pacorabadan.com/?p=191

*www.chiark.greenend.org.uk/.../**putty**/download.htm*

*www.**putty**.org/*

http://es.wikipedia.org/wiki/Secure_Shell

http://eldiabloenlosdetalles.net/2006/08/29/howtocomo-usar-sshfs-para-montar-directorios-con-ssh/

http://ubunturoot.wordpress.com/2007/11/06/comandos-basicos-para-linux/