



Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Ing. Magdalena Reyes Granados

Asignatura: Laboratorio de Redes de Datos

Grupo: 02

No de Práctica(s): 9

Integrante(s): Amado Fuentes Yerenia

Moreno Madrid Maria Guadalupe

No. de Equipo de cómputo empleado:

Semestre: 2021-1

Fecha de entrega: 2/12/2020

Observaciones:

CALIFICACIÓN: _____



**Manual de prácticas del
Laboratorio de Redes de Datos
Seguras**

Código:	MADO-31
Versión:	03
Página	127/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Práctica 9

SSH: Secure Shell

Capa 6 del Modelo OSI



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	128/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

1.- Objetivo de aprendizaje

- El alumno al finalizar la práctica, conocerá la importancia de utilizar el protocolo SSH (Secure Shell) y su herramienta OpenSSH.
- El alumno iniciará una sesión remota a través de SSH, utilizando autenticación por contraseña.
- El alumno iniciará una sesión remota con clave pública, generando las claves.
- El alumno podrá transferir claves públicas al servidor.

2.- Conceptos teóricos

SSH™ permite a los usuarios registrarse en sistemas de host remotamente. A diferencia de *FTP* o *Telnet*, SSH cifra la sesión de registro imposibilitando que alguien pueda obtener contraseñas no cifradas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través del shell de comando, tales como *telnet* o *rsh*. Un programa relacionado, el *scp*, reemplaza otros programas diseñados para copiar archivos entre hosts como *rcp*. Ya que estas aplicaciones antiguas no cifran contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas hará disminuir los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

Características de SSH

SSH (o Secure SHell) es un protocolo para crear conexiones seguras entre dos sistemas usando una arquitectura cliente/servidor.

El *protocolo SSH* proporciona los siguientes tipos de protección:

- Despues de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando un cifrado robusto de 128 bits.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de un cifrado de 128 bits, lo cual los hacen extremadamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de enviar aplicaciones X11 lanzadas desde el intérprete de comandos del shell. Esta técnica proporciona una interfaz gráfica segura (llamada *reenvío por X11*) que proporciona un medio seguro para usar aplicaciones gráficas sobre una red.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	129/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Ya que el protocolo *SSH* cifrado todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor *SSH* puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada *reenvío por puerto*, como por ejemplo *POP*, incrementando la seguridad del sistema en general y de los datos.

Linux contiene el paquete general de *OpenSSH (openssh)*, el servidor de *OpenSSH (openssh-server)* y los paquetes de clientes (*openssh-clients*). Los paquetes *OpenSSH* requieren el paquete *OpenSSL (openssl)*. *OpenSSL* instala varias librerías criptográficas importantes que ayudan a *OpenSSH* a proporcionar comunicaciones cifradas.

Una gran cantidad de programas de cliente y servidor pueden usar el protocolo *SSH*. Muchas aplicaciones *SSH* cliente están disponibles para casi todos los principales sistemas operativos en uso hoy día.

¿Por qué usar *SSH*?

Los usuarios maliciosos tienen a su disposición una variedad de herramientas para interceptar y dirigir el tráfico de la red para ganar acceso al sistema. En términos generales, estas amenazas se pueden catalogar del siguiente modo:

- *Intercepción de la comunicación entre dos sistemas:* En este escenario, existe un tercero en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. La parte interceptora puede interceptar y conservar la información o puede modificar la información y luego enviarla al receptor al cual estaba destinado. Este ataque se puede articular a través del uso de un paquete sniffer — una utilidad de red muy común.
- *Personificación de un determinado host:* Con esta estrategia, un sistema interceptor finge ser el receptor a quien está destinado un mensaje. Si funciona la estrategia, el cliente no se da cuenta del engaño y continúa la comunicación con el interceptor como si su mensaje hubiese llegado a su destino satisfactoriamente. Esto se produce con técnicas como el envenenamiento del DNS o spoofing de IP.

Ambas técnicas causan que se intercepte información, posiblemente con propósitos hostiles. El resultado puede ser catastrófico.

Si se utiliza *SSH* para inicios de sesión de shell remota y para copiar archivos, estas amenazas a la seguridad se pueden disminuir notablemente. Esto es porque el cliente *SSH* y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es cifrada. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una clave conocida sólo por el sistema local y el remoto.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	130/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Capa de Presentación

El papel principal de la capa de presentación es facilitar una comunicación segura entre los dos hosts en el momento y después de la autenticación. La capa de presentación lleva esto a cabo manejando la encriptación y decodificación de datos y proporcionando protección de integridad de los paquetes de datos mientras son enviados y recibidos. Además, la capa de presentación proporciona compresión de datos, lo que acelera la transmisión de información.

Al contactar un cliente a un servidor por medio del protocolo SSH, se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de presentación correctamente. Durante el intercambio se producen los siguientes pasos:

- Intercambio de claves.
- Se determina el algoritmo de cifrado de la clave pública.
- Se determina el algoritmo de cifrado simétrico.
- Se determina el algoritmo autenticación de mensajes.
- Se determina el algoritmo de hash que hay que usar.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- 1 Computadora con Sistema Operativo Linux

4.- Desarrollo

4.1 Sistema Operativo Linux Debian

Modo de trabajar

La realización de la práctica se hará por equipos de dos personas por computadora y se trabajará conjuntamente, un equipo hará la función de servidor y el otro de cliente.

4.2 Ejercicio

NOTA: Para ejemplificar el siguiente ejercicio se muestra la siguiente Figura No. 1.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 131/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 1 Computadoras trabajando conjuntamente

4.2.1 Abra la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 2).

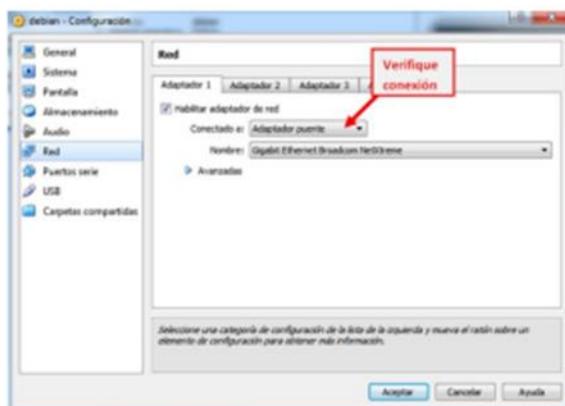


Figura No. 2. Conexión de red.

4.2.2 Encienda la máquina virtual

4.2.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 3), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	132/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

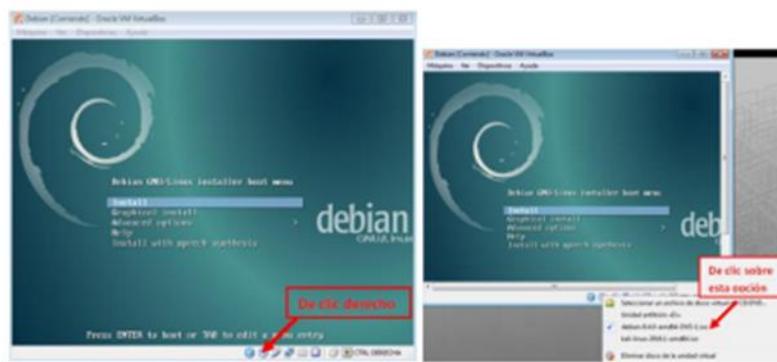


Figura No. 3. Inicio de Máquina Virtual.

- 4.2.4** Entre a sesión como usuario redes (cliente) o estudiante (servidor), según le indique su profesor. La cuenta y la contraseña serán proporcionadas por el profesor del laboratorio.
- 4.2.5** Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 4)

NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root
redes@debian:~\$ su



Figura No. 4. Terminal de comandos como root.

- 4.2.6** Teclee la contraseña de root. (Ver Figura No. 5)

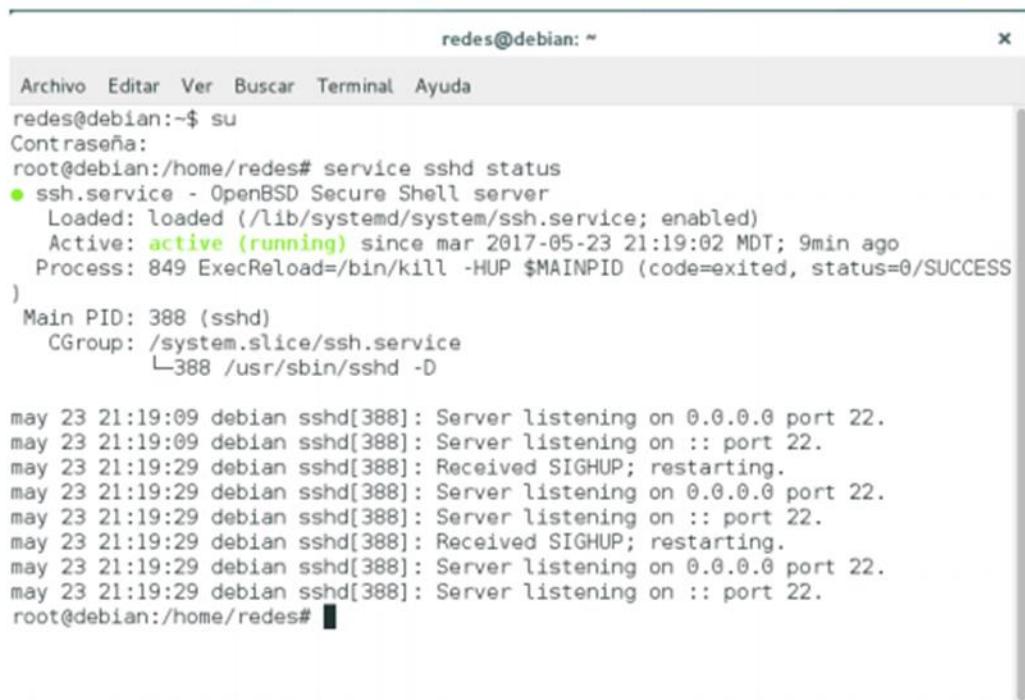


Figura No. 5. Cambio de sesión con privilegios

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 133/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.7** Verifique que la aplicación SSH se encuentre instalada (Active: active (running)) (Figura No. 6), para ello teclee:

```
root@debian:/home/redes# service sshd status
```



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes# service sshd status
● sshd.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled)
  Active: active (running) since mar 2017-05-23 21:19:02 MDT; 9min ago
    Process: 849 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
   Main PID: 388 (sshd)
     CGroup: /system.slice/sshd.service
             └─388 /usr/sbin/sshd -D

may 23 21:19:09 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:09 debian sshd[388]: Server listening on :: port 22.
may 23 21:19:29 debian sshd[388]: Received SIGHUP; restarting.
may 23 21:19:29 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:29 debian sshd[388]: Server listening on :: port 22.
may 23 21:19:29 debian sshd[388]: Received SIGHUP; restarting.
may 23 21:19:29 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:29 debian sshd[388]: Server listening on :: port 22.
root@debian:/home/redes#
```

Figura No. 6. Verificación de SSH

NOTA: En caso de que no se encuentre instalada, debe teclear el siguiente comando para instalarla (Figura No. 7)

```
root@debian:/home/redes# apt-get install ssh
```



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	134/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

```
redes@Pooh: ~
Archivo Editar Ver Terminal Solapas Ayuda
redes@Pooh:~$ su
Contraseña:
Pooh:/home/redes# apt-get install ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
ssh ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 3 no actualizados.
Pooh:/home/redes#
```

Figura No. 7. Descarga del paquete SSH

4.2.8 Visualice el archivo *sshd_config*. (Ver figura No. 8). Teclee lo siguiente:

root@debian:/home/redes# cat /etc/ssh/sshd_config

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# cat /etc/ssh/sshd_config
```

Figura No. 8. Archivo *sshd_config*

La salida del comando dará algo similar a lo siguiente (Ver figura No. 9). Comente la información obtenida en la pantalla.

Muestra la información de configuración del paquete SSHD

```
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::

#ListenAddress 0.0.0.0
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
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
```

 Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 135/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada	

Figura No. 9 Archivo sshd.config

4.2.9 Teclee el comando ifconfig y anote la dirección IP que tiene asignada su máquina

Dirección IP 192.168.2.32

4.2.10 Cierre la sesión de root, colocando *exit*.

4.3 Iniciando una sesión remota con contraseña

4.3.1 El primer ejemplo que se analizará será el inicio de una sesión remota a través de SSH, utilizando autenticación por contraseña. Para ello, ingrese como usuario “estudiante” en el servidor (su propia máquina).

Abra una segunda terminal en el cliente (cuenta de redes) e introduzca el siguiente comando (Ver figura No. 10):

redes@debian:~\$ ssh estudiante@192.168.2.x

NOTA: El valor X será de acuerdo con la máquina que esté utilizando como servidor.



Figura No. 10 Conexión con equipo remoto

Al ser la primera vez que se conecta al servidor, si previamente no ha agregado la clave pública del mismo en */home/redes/.ssh/known_hosts*, aparecerá un mensaje similar al siguiente: (Ver figura No. 11).



Figura No. 11 Confirmación de la sesión con equipo remoto

4.3.2 Debido a que se confía que ésa es la verdadera clave pública del servidor. Teclee yes. Luego el cliente informará algo similar a lo siguiente:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 136/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

Warning: Permanently added '192.168.2.x' (RSA) to the list of known hosts.

Lo que significa que se ha agregado la clave pública del servidor en `/home/redes/.ssh/known_hosts`. (Ver figura No. 12). Luego el cliente solicitará el ingreso de la contraseña:

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ ssh estudiante@192.168.2.48
The authenticity of host '192.168.2.48 (192.168.2.48)' can't be established.
ECDSA key fingerprint is c1:48:55:3e:f1:71:fd:5c:24:34:e3:5e:16:da:1a:61.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.48' (ECDSA) to the list of known hosts.
estudiante@192.168.2.48's password: ■
```

Figura No. 12 Acceso al equipo remoto

4.3.3 Teclee la contraseña de la cuenta estudiante, que será proporcionada por el profesor. Finalmente, si la contraseña ingresada es correcta, aparecerá algo similar a lo siguiente: (Ver figura No. 13).

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ ssh estudiante@192.168.2.48
The authenticity of host '192.168.2.48 (192.168.2.48)' can't be established.
ECDSA key fingerprint is c1:48:55:3e:f1:71:fd:5c:24:34:e3:5e:16:da:1a:61.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.48' (ECDSA) to the list of known hosts.
estudiante@192.168.2.48's password:
Connection closed by 192.168.2.48
redes@debian:~$ ssh estudiante@192.168.2.48
estudiante@192.168.2.48's password:

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.
estudiante@debian:~$ ■
```

Figura No. 13 Sesión iniciada en el equipo remoto

Con lo cual se ha iniciado una sesión en el servidor como el usuario estudiante.

4.3.4 Cierre la sesión remota. Teclee exit: (Ver figura No. 14).

estudiante@debian:~\$ exit

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	137/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```

estudiante@debian:~$ exit
logout
Connection to 192.168.2.48 closed.
redes@debian:~$ █

```

Figura No. 14 Sesión terminada en el equipo remoto

4.4 Iniciando una sesión remota con clave pública

- 4.4.1** El primer paso para utilizar la autenticación mediante clave pública es modificar el archivo de configuración de SSH en la computadora cliente (sesión redes). Debe estar en la cuenta root para poder modificar el archivo.

Para ello, edite el archivo *sshd_config* borrando el símbolo # de las siguientes líneas y verificando que estén escritas como se ve a continuación, si alguna falta inclúyala: (Ver Figura No. 15)

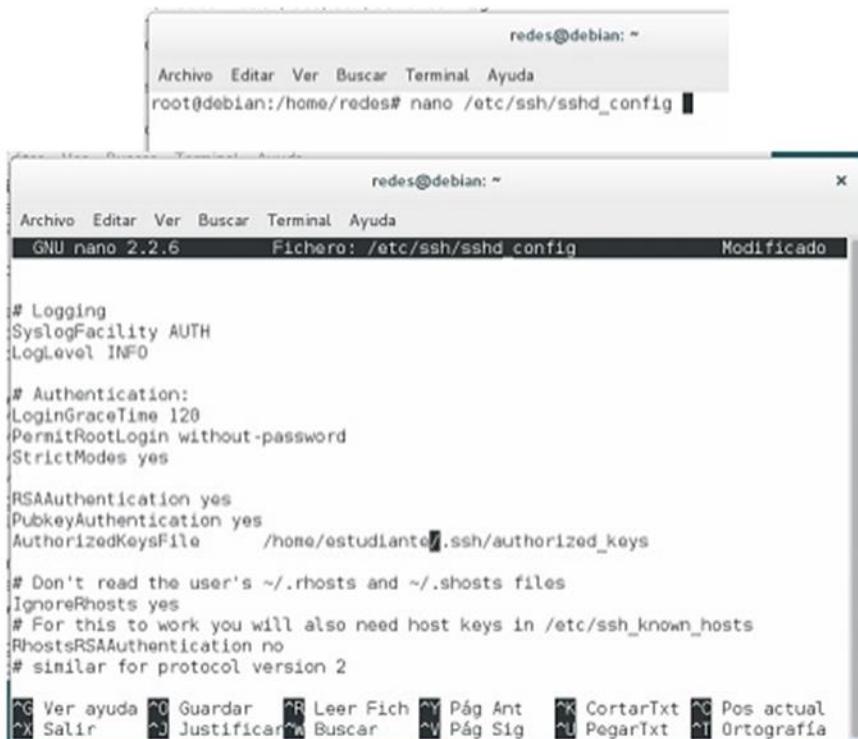
```
root@debian:/home/redes# nano /etc/ssh/sshd_config
```

```

RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile /home/estudiante/.ssh/authorized_keys

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 138/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile      /home/estudiante/.ssh/authorized_keys

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

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^X CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^W Pág Sig ^U PegarTxt ^I Ortografía

```

Figura No. 15 Archivo de configuración

Guarde los cambios (ctrl+o), salga del editor (ctrl+x) y reinicie el servicio (Ver Figura No. 16).

root@debian:/home/redes# /etc/init.d/ssh restart



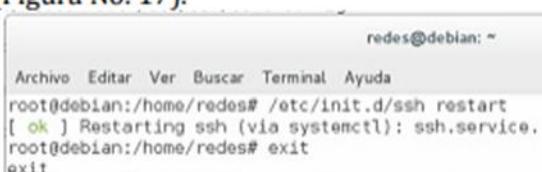
```

root@debian:/home/redes# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.

```

Figura No. 16 Reiniciando el servicio de SSH

Cierre la sesión de root (Figura No. 17).



```

root@debian:/home/redes# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.
root@debian:/home/redes# exit
exit

```

Figura No. 17. Cerrando sesión de root



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	139/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Generando las claves

4.4.2 Genere el par de claves de RSA que se utilizarán.

Para ello, ejecute el siguiente comando en el Shell de la cuenta de redes: (Ver figura No. 18).

```
redes@debian:~$ ssh-keygen -t rsa
```

```
|redes@debian:~$ ssh-keygen -t rsa
```

Figura No. 18 Comando para generar las claves

El programa responderá algo similar a lo siguiente: (Ver figura No. 19).

```
|redes@debian:~$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/redes/.ssh/id_rsa): |
```

Figura No. 19 Generando las claves

4.4.3 Solicita que se ingrese el nombre del archivo en donde se almacenará la clave privada, asegúrese que la ruta sea /home/redes/.ssh/id_rsa, de no ser así introduzca la ruta para que concuerde con la configuración del cliente SSH. Presione <Enter>. Luego solicitará una frase clave: (Ver figura No. 20).

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

```
redes@debian:~$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/redes/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again: |
```

Figura No. 20 Colocando la frase

4.4.4 Presione dos veces <Enter> para omitir el uso de una frase clave. Más adelante se realizará esto. Finalmente informa: (Ver figura No. 21).

Your identification has been saved in /home/redes/.ssh/id_rsa.

Your public key has been saved in /home/redes/.ssh/id_rsa.pub.

The key fingerprint is:

13:8b:23:74:53:e4:0f:b3:16:49:1b:79:64:60:7c:38 redes@cliente



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	140/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

```
redes@debian:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/redes/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/redes/.ssh/id_rsa.
Your public key has been saved in /home/redes/.ssh/id_rsa.pub.
The key fingerprint is:
bf:2a:0f:7d:6a:35:b5:86:fe:8d:0b:2a:3b:59:7f:ae  redes@debian
The key's randomart image is:
+---[RSA 2048]----+
|          .         |
|          .         |
|          .         |
|          .         |
|          S o .     |
|          ...+ 0     |
|          .o.++0     |
|          =..+oo.0    |
|          .B=.E==..   |
+-----+
redes@debian:~$
```

Figura No. 21 Claves generadas satisfactoriamente

4.5 Transfiriendo la clave pública al servidor

Luego, se debe transferir la clave pública del usuario *redes* (*/home/redes/.ssh/id_rsa.pub*) al directorio *home* del usuario estudiante en servidor y añadirla al final del archivo */home/estudiante/.ssh/authorized_keys*.

4.5.1 Desde la terminal teclee sin omitir la tilde: (Ver figura No. 22).

```
redes@debian:~$ scp /home/redes/.ssh/id_rsa.pub estudiante@192.168.2.x:~
```

NOTA: El valor X será de acuerdo con la máquina que esté utilizando como servidor.

Teclee la contraseña de la cuenta estudiante y la transferencia finalizará

```
Archivo Editar Ver Terminal Solapas Ayuda
redes@debian:~$ scp /home/redes/.ssh/id_rsa.pub estudiante@192.168.2.20:~
estudiante@192.168.2.20's password:
id_rsa.pub                                100%  392      0.4KB/s  00:00
```

Figura No. 22 Trasferencia de la clave

4.5.2 Para añadir la clave pública al archivo *authorized_keys* realice lo siguiente en el servidor

- Realice lo siguiente en el servidor (sesión estudiante):

Teclee:

```
estudiante@debian:~$su
```



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	141/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

NOTA: su significa super usuario, por lo que se emplea la misma contraseña de root

Ahora teclee (Figura No. 23)

```
root@debian:/home/estudiante# cat /home/estudiante/id_rsa.pub>  
/home/estudiante/.ssh/authorized_keys
```

```
root@debian:/home/estudiante# cat /home/estudiante/id_rsa.pub >/home/estudiante/  
.ssh/authorized_keys
```

Figura No. 23 Añadiendo la clave al archivo authorized_keys

b) Ahora diríjase al cliente (sesión redes) y agregue la clave (Figura No. 24)

```
root@debian:/home/redes# ssh-add /home/redes/.ssh/id_rsa
```

```
redes@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
redes@debian:~$ ssh-add /home/redes/.ssh/id_rsa  
Identity added: /home/redes/.ssh/id_rsa (rsa w/o comment)
```

Figura No. 24 Agregando la clave

Salga de la sesión de root

4.6 Iniciando la sesión

4.6.1 Ingrese el siguiente comando:

```
redes@debian:~$ ssh estudiante@192.168.2.x
```

NOTA: El valor X será de acuerdo con la máquina que esté utilizando como servidor.

El servidor nuevamente envía su clave pública de RSA, la cual es comparada con la almacenada en *known_hosts*, y si coincide, el proceso continúa.

El cliente de SSH, al encontrar el archivo */home/redes/.ssh/id_rsa*, primero intentará la autenticación con clave pública. El servidor le enviará el *challenge* cifrado con la clave pública encontrada en */home/estudiante/authorized_keys* (en el directorio *home* del usuario *estudiante*) y el cliente deberá devolverla descifrada (usando la clave */home/redes/.ssh/id_rsa* en el directorio *home* del usuario *redes*).

NOTA: Esto se realiza automáticamente, sin la intervención del usuario.

Si esto se realiza correctamente, se iniciará la sesión remota (Ver figura No. 25).



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	142/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

```
redes@debian:~$ ssh estudiante@192.168.2.48
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: Mon Jun 26 17:06:53 2017 from 192.168.2.34
estudiante@debian:~$
```

Figura No. 25 Sesión iniciada con el equipo remoto

- 4.6.2** Si la autenticación con clave pública hubiera fallado, el cliente intentará con la autenticación con contraseña. Después de conectarse al servidor, salga de este. (Ver figura No. 26).

```
estudiante@debian:~$ exit
logout
Connection to 192.168.2.48 closed.
redes@debian:~$
```

Figura No. 26 Cerrando la sesión remota

4.7 Asegurando la clave privada en el cliente

- 4.7.1** Cuando creó el par de claves usando ssh-keygen, se omitió especificar la frase clave que se usaría a tal efecto. Usando nuevamente ssh-keygen se asignará una nueva. Teclee lo siguiente:

```
redes@debian$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
```

Pedirá ingresar la nueva frase clave: (Ver figura No. 27).

Enter new passphrase (empty for no passphrase):

Enter same passphrase again:

```
redes@debian:~$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
Key has comment 'rsa w/o comment'
Enter new passphrase (empty for no passphrase):
```

Figura No. 27 Asegurando la clave privada

- 4.7.2** Ingrese la frase clave, usted seleccione una y escriba esta misma en ambas ocasiones.

Frase clave empleada: AmadoMoreno

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página: 143/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada		

4.7.3 Finalmente informa: (Ver figura No. 28).

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
Key has comment 'rsa w/o comment'
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.
redes@debian:~$
```

Figura No. 28 Ingresando clave, para la conexión remota

4.8 Usando ssh-agent en el shell

4.8.1 En la sesión redes, ejecute el ssh-agent de la siguiente forma: (Ver figura No. 29).

redes@debian:~\$ eval 'ssh-agent'

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ eval 'ssh-agent'
SSH_AUTH_SOCK=/tmp/ssh-1gcOTB6kogog/agent.3066; export SSH_AUTH_SOCK;
SSH_AGENT_PID=3067; export SSH_AGENT_PID;
echo Agent pid 3067;
redes@debian:~$
```

Figura No. 29 Utilizando el ssh-agent

4.8.2 Agregue la clave privada de RSA. (Ver figura No. 30). Para ello use el comando *ssh-add*:

redes@debian:~\$ ssh-add /home/redes/.ssh/id_rsa

```
redes@debian:~$ ssh-add /home/redes/.ssh/id_rsa
```

Figura No. 30 Agregando la clave privada de RSA

Este procedimiento puede repetirse si se tienen varias claves privadas. Luego, al ejecutar ssh éste le solicitará al ssh-agent la clave privada.

Reinicie la sesión del cliente (sesión redes) (cierra la sesión e ingrese nuevamente) (Figura No. 31).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 144/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 31 Cierre e inicio de sesión en redes

Una vez estando dentro de la sesión cliente y empleando una terminal, conéctese de manera remota al servidor (sesión estudiante) y comente lo que sucede, para ello teclee:

redes@debian\$ ssh estudiante@192.168.2.x

Pide la clave privada que se guardó y nos asocia la clave pública.

Cierre la sesión de estudiante.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	145/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

4.9 Restaurando la configuración de las máquinas

4.9.1 Eliminación de los archivos

Teclee lo siguiente para eliminar los archivos generados en el servidor (sesión estudiante), recuerde que debe estar como superusuario.

```
root@debian:/home/estudiante# rm /home/estudiante/id_rsa.pub
```

Teclee lo siguiente para eliminar los archivos generados en el cliente (sesión redes) recuerde que debe estar como superusuario.

```
root@debian:/home/redes# rm /home/redes/.ssh/id_rsa.pub
root@debian:/home/redes# rm /home/redes/.ssh/id_rsa
```

4.9.2 Desinstalación de ssh

En modo superusuario teclee lo siguiente:

```
root:/home/redes# apt-get autoremove -- purge ssh
```

4.9.3 Borrado del contenido de los archivos

Debe borrar el contenido de los archivos y dejarlos en blanco completamente, como estaban originalmente, recuerde que debe encontrarse en modo superusuario.

Teclee lo siguiente y borre el contenido de cada archivo, dentro del archivo puede oprimir ctrl+k para eliminar cada línea rápidamente, guarde el archivo en blanco:

```
root:/home/redes# nano /home/redes/.ssh/known_hosts
```

4.9.4 Cierre la sesión.

4.9.5 Cuestionario

1. ¿Qué sucedería si escribiera mal la contraseña al querer hacer una conexión remota con ssh?

—No nos permite el acceso, rechaza la conexión.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	146/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

2. Investigue las características de los algoritmos de cifrado RSA y 3DES

RSA. Los mensajes enviados se representan con números y usan el protocolo de dos números primos grandes. Se basa en la exponenciación modular de exponente fijo y módulos fijos.

Crea sus claves de la siguiente forma:

- Se buscan dos números primos grandes p y q.
- Se obtiene $n=p \cdot q$ y $\phi = (p-1) \cdot (q-1)$.
- Se busca un número e que no tenga múltiplos comunes con ϕ .
- Se calcula $d=e^{-1} \pmod{\phi}$, con mod = resto de la división con enteros.

Dónde n es la clave pública y d es la privada.

- p, q y ϕ se destruyen
- Se hace público el numero e para alimentar el algoritmo.

Los pasos son:

- Se genera la clave pública y privada.
- Se cifra el mensaje usando la clave pública.
- Se descifra el mensaje usando la clave privada.

RDES. Fraccionamiento del texto en bloques de 64 bits. Hace triple cifrado del DES.

Sus partes son:

- Fraccionamiento del texto en bloques de 64 bits.
- Permutación inicial de los bloques.
- Partición de los bloques L(izquierda) y D (derecha).
- Fases de permutación y de sustitución repetidas 16 veces (rondas).

Reconexión de la parte izquierda y derecha, seguida de la permutación inicial inversa.

Configuración de SSH en Switch y Router Cisco:

Configuración de PC Paso 1: Configuración de IP

IP Address:	192.168.0.100
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1

Habilitar SSH en Switch Cisco

Paso 1: Configuración de IP de administración

- Switch#conf t
- Switch(config)#interface vlan 1
- Switch(config-if)#ip address 192.168.0.10 255.255.255.0
- Switch(config-if)#no shutdown

Paso 2: Configuración de default Gateway apuntando al Router

- Switch(config)#ip default-gateway 192.168.0.1

Paso 3: Configuración de hostname y nombre de dominio

- Switch(config)#hostname eclassvirtual-sw
- eclassvirtual-sw(config)#ip domain-name eclassvirtual.com

Paso 4: Generación de llaves RSA

- eclassvirtual-sw(config)# crypto key generate rsa
- The name for the keys will be: eclassvirtual-sw.eclassvirtual.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: **2048** % Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

Paso 5: Cambiar SSH versión 1 a la 2 (la versión 2 es más segura)

- eclassvirtual-sw(config)#ip ssh version 2

Paso 6: Configuración de Line VTY

- eclassvirtual-sw(config)# line vty 0 15
- eclassvirtual-sw(config-line)# transport input ssh
- eclassvirtual-sw(config-line)# login local

Paso 7: Crear nombre de usuario y password

- eclassvirtual-sw(config)# username eclassvirtual privilege 15 secret cisco123

Paso 8: Habilitar enable secret

- eclassvirtual-sw(config)# enable secret cisco123

Paso 9: Realizar pruebas de SSH desde el PC

- C:\>ssh -l eclassvirtual 192.168.0.10 Open Password:

Paso 10: Revisión de conexión SSH en el Switch

- eclassvirtual-sw# show ssh

Habilitar SSH en Router Cisco:

- Router#conf t
- Router(config)#hostname eclassvirtual-router
- eclassvirtual-router(config)#interface g0/0
- eclassvirtual-router(config-if)#ip address 192.168.0.1 255.255.255.0
- eclassvirtual-router(config-if)#no shutdown
- eclassvirtual-router(config-if)#exit
- eclassvirtual-router (config)#ip domain-name cisco.com
- eclassvirtual-router(config)#username eclassvirtual privilege 15 secret cisco123
- eclassvirtual-router(config)#crypto key generate rsa
- The name for the keys will be: eclassvirtual-router.cisco.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 2048 % Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
- eclassvirtual-router(config)#ip ssh version 2
- eclassvirtual-router(config)#enable secret cisco123
- eclassvirtual-router(config)#line vty 0 15
- eclassvirtual-router(config-line)#transport input ssh
- eclassvirtual-router(config-line)#login local
- eclassvirtual-router#show ip ssh C:\>ssh -l eclassvirtual 192.168.0.1 Open Password:

SE ANEXA EL PROGRAMA EN CISCO PACKET TRICER

- USUARIO: eclassvirtual
- CONTRASEÑA: cisco123

Conclusiones:

Yerenia Amado: En esta práctica comprendimos el concepto y funcionamiento del protocolo SSH y observamos que podemos acezar remotamente de forma segura, ya que nos permite acceder de manera cifrada sin que puedan ver la contraseña, además vimos las diferencias entre clave pública y privada y como transferir claves públicas al servidor.

Guadalupe Moreno: SSH es un protocolo que nos permite acezar de forma segura a plataformas cliente – servidos de forma cifrada, por medio de una clave privada que asocia a la clave pública, evitando que terceras personas puedan descubrir el usuario y contraseña ni lo que se escribe durante toda la sesión.

Referencias:

- <https://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/rsa.html>
- <http://seguridad-en-redes-mimi.blogspot.com/2012/03/algoritmo-3des.html?m=1>
- <https://eclassvirtual.com/configuracion-ssh-switch-router-cisco/>
- <https://www.youtube.com/watch?v=ekOs1DSQixg>