



Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: ING. Edgar Martínez Meza

Asignatura: Laboratorio de Redes de datos seguras

Grupo: 6

No. de Práctica(s): #9

Integrante(s): Barrera Peña Víctor Miguel

Tapia Escobar José Alejandro

No. de Equipo de cómputo empleado: # 3

Semestre: 2024 - 2

Fecha de entrega: 09 - 04- 2024

Observaciones:

CALIFICACIÓN: _____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 139/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

La impresión de este documento es una copia no controlada

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 140/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

La impresión de este documento es una copia no controlada

1.- Objetivo de aprendizaje : *Sección 1*

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

- Después 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 *envío por X11*) que proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

► Ejercicios comenjos

Práctica 9

SSH: Secure Shell

Capa 6 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 141/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 142/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	Facultad de Ingeniería

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 *envío 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-client*). Los paquetes OpenSSH requieren el paquete OpenSSL (*openssl*). OpenSSL instala varias librerías criptográficas importantes que ayudan a OpenSSL 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 las 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 inicio 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: 06 Página: 141/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 142/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	Facultad de Ingeniería

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 de cifrado simétrico.
- 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 trabajo

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.

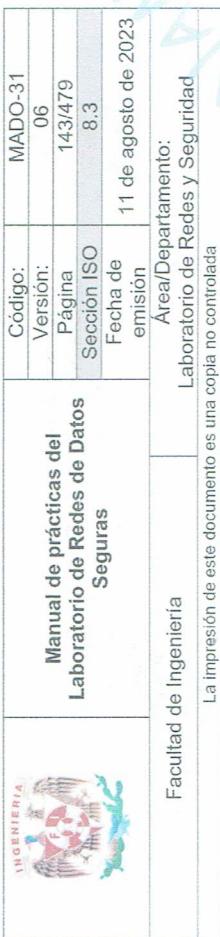
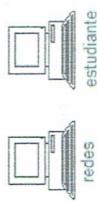


Figura No. 1 Compuadoras trabajando conjuntamente



redes
estudiante

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
Versión:	06	Página:	143/479
Página	143/479	Sección ISO	8.3
Sección ISO	8.3	Fecha de emisión	11 de agosto de 2023
Fecha de emisión	11 de agosto de 2023	Área/Departamento:	Área/Departamento: Laboratorio de Redes y Seguridad
Área/Departamento:	Laboratorio de Redes y Seguridad	Facultad de Ingeniería	La impresión de este documento es una copia no controlada

La impresión de este documento es una copia no controlada

4.2.2 Encienda la máquina virtual.

4.2.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: Para realizar la práctica exitosamente debe tener instalado los paquetes ifconfig y ssh.

4.2.4 Entre a sesión como usuario redes (cliente) o estudiante (servidor) según le indique su profesora o profesor. La cuenta y la contraseña serán proporcionadas por la profesora o 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. 3)

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

```
redest@DEBIAN2023:~$ su
redest@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:~/home/redest#
```

Figura No. 3.Término de comandos como root.

4.2.6 Teclee la contraseña de root. (Ver Figura No. 4)

```
redest@DEBIAN2023:~$ su
redest@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:~/home/redest#
```

Figura No. 4. Cambio de sesión con privilegios

4.2.7 Verifique que la aplicación SSH se encuentre instalada (Active: active (running)) (Figura No. 5), para ello teclee:

root@debian:/home/redest# service sshd status

 INGENIERÍA	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 06
		Versión: Página Sección ISO
		146/479 8.3
		Fecha de emisión
		11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad

```
redes@DEBIAN2023: ~
```

```
word:
```

```
@DEBIAN2023:/home/redes# service sshd status
  service= OpenBSD Secure Shell server
    Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-06-15 13:14:08 CST; 4min 48s ago
     Docs: man:sshd(8)
       Main PID: 393 (sshd)
          Tasks: 1 (limit: 2954)
         CPU: 24ms
        CGroup: /system.slice/sshd.service
                 └─ 393 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

15 13:14:07 DEBIAN2023 systemd[1]: Starting OpenBSD Secure Shell server...
15 13:14:08 DEBIAN2023 sshd[503]: Server listening on 0.0.0.0 port 22.
15 13:14:09 DEBIAN2023 sshd[503]: Server listening on :: port 22.
15 13:14:08 DEBIAN2023 systemd[1]: Started OpenBSD Secure Shell server.
```

La impresión de este documento es una copia no controlada

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

redes@DEBIAN2023: ~

root@DEBIAN2023:~/home/redes# cat /etc/ssh/sshd_config

Figura No. 7. Archivo sshd_config

Salida del comando dará algo similar a lo siguiente (Ver figura No. 8). Comente la información obtenida en la pantalla.

nte. donde se pone. Licencias la clave que envíamos tipo de llaves para la security shelf así como los permisos y privilegios.

NOTA: En caso de que no se encuentre instalada, debe teclear el siguiente comando para instalarla (figura No. 6)

www.edubion.com/bannedbooksandcensorshipbook

```
[@DEBIAN2023:~/home/redes# apt-get install ssh  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The package ssh is already the newest version (1:8.4p1-5+deb11u1).  
0 newly installed, 0 to remove and 4 not upgraded.  
[@DEBIAN2023:~/home/redes# ]
```

Figura No. 6. Descarga del paquete SSH

Figura No. 8 Archivo sshd config

```
# default value.

#Include /etc/ssh/sshd_config.d/*.conf

Port 22

ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying

#LogLevel INFO

# Logging
#syslogfacility AUTH
#LogLevel INFO

# Authentication:
```

La salida del comando dará algo similar a lo siguiente (Ver figura No. 8). Comente la información obtenida en la pantalla.

Bote donde se guarda el inventario la clave es la

generativa envíenmas tiros de su yelo para la

diferencia envíenlos RSA y security y Sheff y

comunicaciones confidenciales

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 147/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	redes@debian:~

La impresión de este documento es una copia no controlada

4.2.9 Teclee el comando liconfig y anote la dirección IP que tiene asignada su máquina Dirección IP 192.168.2.53

4.2.10 Cierra 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. 9):

`redes@debian:~$ ssh estudiante@192.168.2.53`

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

```
estudiante@DEBIAN2023:~$ ssh estudiante@192.168.2.53
redes@DEBIAN2023:~$ ssh estudiante@192.168.2.42
```

Figura No. 9 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. 10).

```
redes@debian:~$ ssh estudiante@192.168.2.53
redes@DEBIAN2023:~/practica/sock_1$ ssh -l redes 192.168.2.42
The authenticity of host '192.168.2.42' can't be established.
ECDSA key fingerprint is SHA256:RjEJB4dmRo/GTw1LTwFQ25mlwRbw0RIVwZhNQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: permanently added '192.168.2.42' (ECDSA) to the list of known hosts.
```

Figura No. 10 Confirmación de la sesión con equipo remoto

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

Warning: Permanently added '192.168.2.53' (RSA) to the list of known hosts.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 148/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	redes@debian:~

La impresión de este documento es una copia no controlada

Lo que significa que se ha agregado la clave pública del servidor en `/home/redes/.ssh/known_hosts`. (Ver figura No. 11). Luego el cliente solicitará el ingreso de la contraseña:

4.3.3 Teclee la contraseña de la cuenta estudiante, que seá proporcionada por la profesora o el profesor. Finalmente, si la contraseña ingresada es correcta, aparecerá algo similar a lo siguiente: (Ver figura No. 12).

4.3.4 Cierre la sesión remota. Teclee `exit`; (Ver figura No. 13).

```
estudiante@DEBIAN2023:~$ ssh estudiante@192.168.2.53
root@DEBIAN2023:~/home/redes# ssh estudiante@192.168.2.55
The authenticity of host '192.168.2.55' (192.168.2.55) can't be established.
ECDSA key fingerprint is SHA256:prJEB4dmRo/GTw1LTwFQ25mlwRbw0RIVwZhNQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: permanently added '192.168.2.55' (ECDSA) to the list of known hosts.
```

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. 10).

```
redes@debian:~$ ssh estudiante@192.168.2.53
redes@DEBIAN2023:~/practica/sock_1$ ssh -l redes 192.168.2.42
The authenticity of host '192.168.2.42' can't be established.
ECDSA key fingerprint is SHA256:RjEJB4dmRo/GTw1LTwFQ25mlwRbw0RIVwZhNQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Figura No. 11 Acceso al 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. 13).

estudiante@debian:~\$ exit

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 149/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada
		La impresión de este documento es una copia no controlada

estudiante@DEBIAN2023:~\$ exit

logout
Connection to 192.168.2.55 closed.

root@DEBIAN2023:/home/redes#

Figura No. 13 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 inclúyalas: (Ver Figura No. 14)

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

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

redes@DEBIAN2023:~

root@DEBIAN2023:/home/redes# nano /etc/ssh/sshd_config

redes@DEBIAN2023:~

root@DEBIAN2023:/home/redes# /etc/init.d/ssh restart

Figura No. 14 Archivo de configuración

Guarde los cambios (ctrl+o), salga del editor (ctrl+x) y reinicie el servicio (Ver Figura No. 15).

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

Figura No. 15 Reiniciando el servicio de SSH

Cierre la sesión de root (Figura No. 16).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 150/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada
		La impresión de este documento es una copia no controlada

redes@DEBIAN2023:~

redes@DEBIAN2023:~

/etc/ssh/sshd_config

GNU nano 5.4

Logging

SyslogFacility AUTH

LogLevel INFO

Authentication:

LoginGraceTime 2m

PermitRootLogin without-password

StrictModes yes

RSAAuthentication yes

PubkeyAuthentication yes

AuthorizedKeysFile

#AuthorizedPrincipalsFile none

#AuthorizedKeyCommand none

#AuthorizedKeyCommandUser nobody

For this to work you will also need host keys in /etc/ssh/ssh_known_hosts

HostbasedAuthentication no

Change to yes if you do not trust -> \$SSH/known_hosts for

HostbasedAuthentication

#IgnoreUserKnownHosts no

Don't read the user's \$HOME/.ssh/known_hosts and -> .ssh/hosts files

redes@DEBIAN2023:~

redes@DEBIAN2023:~

/etc/init.d/ssh

Restarting ssh (via systemctl): ssh.service.

root@DEBIAN2023:/home/redes#

[redes@DEBIAN2023:~]

Figura No. 15 Reiniciando el servicio de SSH

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 15/1479 Sección ISO 8.3
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	Fecha de emisión 11 de agosto de 2023 La impresión de este documento es una copia no controlada

Figura No. 16. Cerrando sesión de root

```
root@DEBIAN2023:/home/redes# /etc/init.d/ssh restart
Restarting ssh (via systemctl): ssh.service.
root@DEBIAN2023:/home/redes# exit
[...]
root@DEBIAN2023:/home/redes#
```

Figura No. 16. Cerrando sesión de root

Generando las claves

4.4.2 Generar 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. 17).

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

Figura No. 17 Comando para generar las claves

El programa responderá algo similar a lo siguiente: (Ver figura No. 18).

redes@DEBIAN2023:~\$ ssh-keygen -t rsa

Figura No. 18 Generando las claves

4.4.3 Solicitud 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. 19).

Enter passphrase (empty for no passphrase):
Enter same passphrase again:



Figura No. 19 Colocando la frase

```
redes@DEBIAN2023:~$ 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. 19 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. 20).

```
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
redes@DEBIAN2023:~
```

```
redes@DEBIAN2023:~$ 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
The key fingerprint is:
SHA256:UefczgbGUYtLhoyNDKxXjLCm63Rjgkh4H3ETU redes@DEBIAN2023
The key's randomart image is:
+---[RSA 3072]---+
|   . * + * . |
|   . o o X + |
|   . . S B = |
|   . o . B . |
|   . + . O . |
|   . . . . . |
|   . . . . . |
|   . . . . . |
|   . . . . . |
|   . . . . . |
redes@DEBIAN2023:~$
```

Figura No. 20 Claves generadas satisfactoriamente

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 153/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

4.5 Transferiendo 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. 21).

```
redes@debian:~$ scp /home/redes/.ssh/id_rsa.pub estudiante@192.168.2.8:~
```

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

Teclee la contraseña de la cuenta estudiante y la transferencia finalizará

```
redes@DEBIAN2023:~$ 
[redes@DEBIAN2023:~$ scp /home/redes/.ssh/id_rsa.pub estudiante@192.168.2.55:~ 
id_rsa.pub 100% 570 248.5KB/s 00:00
```

Figura No. 21 Trasferencia de la clave

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

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

Teclee:

estudiante@debian:~\$ su

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

A continuación teclee lo siguiente (Figura No. 22):

```
root@debian:~# cat /home/estudiante/.ssh/authorized_keys
```

Ahora teclee el siguiente comando para crear la carpeta .ssh en */home/estudiante*

```
root@debian:~# mkdir .ssh
```

A continuación teclee lo siguiente (Figura No. 22):

```
root@debian:~# cat /home/estudiante/.ssh/authorized_keys
```

Figura No. 22 Añadiendo la clave al archivo *authorized_keys*

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 154/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

- b) Ahora diríjase al cliente (sesión redes) y agregue la clave (Figura No. 23)

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

redes@DEBIAN2023:~

```
[redes@DEBIAN2023:~$ ssh-add /home/redes/.ssh/id_rsa
Identity added: /home/redes/.ssh/id_rsa (redes@DEBIAN2023)
redes@DEBIAN2023:~$
```

Figura No. 23 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 está 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. 24).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 155/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

```
estudiante@192.168.2.55:~$ ssh estudiante@192.168.2.55
estudiante@192.168.2.55's password:
Linux DEBIAN2023 5.10.0-23-and64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64

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: Thu Aug 3 11:05:38 2023 from 192.168.2.56
estudiante@DEBIAN2023:~$
```

Figura No. 24 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. 25).

```
estudiante@DEBIAN2023:~$ exit
logout
Connection to 192.168.2.55 closed.
redes@DEBIAN2023:~$
```

Figura No. 25 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. Técete lo siguiente:

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

Pedirá ingresar la nueva frase clave: (Ver figura No. 26).

*Enter new passphrase (empty for no passphrase):
Enter same passphrase again:*

```
redes@DEBIAN2023:~$
```

Figura No. 26 Asegurando la clave privada

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 156/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

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

Frases clave empleadas: **redes 123**

4.7.3 Finalmente informa: (Ver figura No. 27).

```
redes@DEBIAN2023:~$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
key has comment : redes@DEBIAN2023.
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.
redes@DEBIAN2023:~$
```

Figura No. 27 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. 28).

```
redes@DEBIAN2023:~$ eval `ssh-agent`
```

4.8.2 Utilizando el ssh-agent

```
redes@DEBIAN2023:~$ ssh-add /home/redes/.ssh/id_rsa
```

Figura No. 28 Utilizando el ssh-agent

4.9.2 Agregue la clave privada de RSA. (Ver figura No. 29). Para ello use el comando ssh-add:

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

Figura No. 29 Agregando la clave privada

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 157/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

```
redes@DEBIAN2023: ~$ ssh -add /home/redes/.ssh/id_rsa
Enter passphrase for /home/redes/.ssh/id_rsa:
Identity added: /home/redes/.ssh/id_rsa (redes@DEBIAN2023)
redes@DEBIAN2023: ~$
```

Figura No. 29 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. 30).



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 158/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad



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@192.168.2.10
Se conecta a estudiante de forma remota
en acceso remoto RSA publico ya no
solicita contraseña, pero su clave
se conectó como estudiante.
```

Cierre la sesión de estudiante.

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 de 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
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 159/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

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 optimizarlo 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

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

No nos va a怜dar al dev una contraseña incorrecta, ya se pague autentica con dicha contraseña y por ende la conexión no se podra llevar a cabo

- Investigue las características de los algoritmos de cifrado RSA Y 3DES.
La mayoría de los algoritmos RSA se basa en la complejidad de calcular que tiene que encontrar los dos factores primos de un número compuesto muy grande.
El algoritmo 3DES se basa en DES que aplica un servicio de operaciones básicas para conectar un texto en cifrado, empleando una clave criptográfica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 160/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	La impresión de este documento es una copia no controlada

- Anote sus Conclusiones u Observaciones, revisando los objetivos planteados al inicio de la práctica:

Tapias: Nos pudimos dar cuenta de como utilizar el protocolo ssh para tener conexión remota más segura a través de los que son las claves públicas y privadas que es lo que se utiliza para mantener seguridad en la información o cuentas.
Barreiro Peña Victoria Alvarado:
Cuando se hace una conexión a otra máquina se accede a través de las claves públicas y se accede correctamente mediante ssh. El uso de la clave pública es compleja

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
	Versión: 06	Página: 161/479
	Sección ISO: 8.3	Fecha de emisión: 11 de agosto de 2023
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

Cuestionario Previo

1. ¿Qué es el reenvío por X11?
2. ¿Qué es un sniffer?
3. Mencione cuáles son las versiones del protocolo SSH y explique sus características.
4. ¿Cuáles son las secuencias de eventos a llevar a cabo en una conexión SSH?
5. ¿A qué nos referimos con la Autenticación?
6. Explique detalladamente los pasos que se producen cuando un cliente contacta a un servidor a través del protocolo SSH.
7. ¿Qué algoritmo de cifrado emplea el protocolo SSH?
8. ¿En dónde es conveniente utilizar SSH?
9. ¿Cuáles son los objetivos principales de la capa 6 del modelo OSI?