[redacted]

Este tipo de problemáticas ha llevado al diseño de herramientas que permitan evitar estas situaciones, una de

[redacted]

los protocolos SSH1y SSH2. La última versión de OpenSSH cliente/servidorpara Unix es la 2.3.0P1 (Liberada el 6 de Noviembre del 2000).

Debido a que OpenSSH rompe la barrera de los protocolos, ha causado confusión entre diversos sectores, al ser muy usada en la comunidad, tal es el caso de distribuciones como Linux RedHat 7.0 que ya la incluye dentro de su sistema operativo.

Sin embargo OpenSSH ha demostrado en los últimos meses cierta inestabilidad, por lo que sí se instala dicha versión es altamente recomendable actualizar periódicamente el OpenSSH y estar al pendiente de vulnerabilidades presentadas.

¿Dónde obtener el Secure Shell?

5.1.Secure Shell cliente/servidor para sistemas Unix

Sitio FTP de Secure Shell
http://ftp.ssh.com/pub/ssh

Departamento de Seguridad en Cómputo
ftp://ftp.seguridad.unam.mx/Herramientas/Unix/Comunicacion

5.2 OpenSSH Cliente/Servidor para sistemas Unix

Sitio FTP de OpenSSH
http://www.openssh.com/ftp.html

Departamento de Seguridad en Cómputo
ftp://ftp.seguridad.unam.mx/Herramientas/Unix/Comunicacion

5.3 Secure Shell cliente para sistemas Windows

Sitio FTP de Secure Shell (Solo para clientes con protocolo SSH2)
http://ftp.ssh.com/pub/ssh

Departamento de Seguridad en Cómputo
ftp://ftp.seguridad.unam.mx/Herramientas/Windows/Comunicacion

5.4 Secure Shell cliente para sistemas Mac

Departamento de Seguridad en Cómputo
ftp://ftp.seguridad.unam.mx/Herramientas/Mac/Comunicacion/Ssh1

OpenSSL

OpenSSL se puede encontrar en:
http://www.openssl.org/

Departamento de Seguridad en Cómputo
ftp://ftp.seguridad.unam.mx/Herramientas/Une6asl.ompie4aci63mpn/enSSsshTj 0 -2652.8d(De7.2.1. Instalaci63mpne

% ./Configure solaris-sparc-gcc

c)Compilación de OpenSSL

Siguiente paso, realizar la compilación de las librerías de OpenSSL simplemente tecleando make

% make

d)Instalación de OpenSSL

Si no se presentó problema alguno, el paso consiguiente es como superusuario teclear la sentencia apropiada para la instalación de las librerías.

make install

Si todo funcionó perfecto se procede a instalar el software OpenSSH, descrito a continuación.

OpenSSH

Una vez realizados los pasos 7.1 y 7.2 y si la compilación no presentó problema alguno, es ahora necesario instalar OpenSSH.

La última versión disponible del OpenSSH es la Versión 2.3.0.P1 (Liberada en Noviembre del 2000).

OpenSSHse puede obtener de:
http://www.openssh.com

Después de haber obtenido el programa de Secure Shell (ssh32-014.zip) del sitio del Departamento de Seguridad en Cómputo se deben realizar los pasos siguientes.

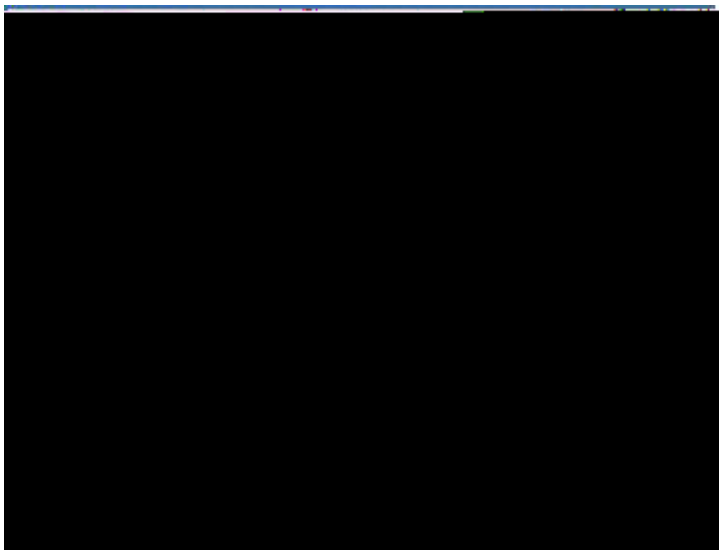
a)Descomprimir el programa usando WinZip o unzip en cualquier directorio temporal.

b)Copiar las librerías (*.dll) al directorio correspondiente en Windows. En Windows 95/98/MEcopiarlos al directorioC:\WINDOWS\SYSTEM". Sí usa Windows NT/2000deben de copiarse al directorio "C:\WINNT\SYSTEM32".

A partir de este momento ya se puede utilizar el cliente de Secure Shell y Secure Copy protocolo SSH1 en modo de comandos desde la Interfaz de Comandos(MS-DOS o Command Prompt).

Secure Shell Tera Term Pro v2.3 (Ambiente Gráfico, protocolo SSH1)

Después de haber obtenido el programa de Secure Shell(sshTeraterm.zip) del sitio del Departamento de



d)Finalmente, cree un acceso directo desde el Escritorioal programa Secure Shell Tera Term Pro (C:\ARCHIVOS DE PROGRAMA\TTERMPRO\ttssh.exe).

De esta manera ya puede utilizar el programa cliente de Secure Shell con una interfaz gráfica agradable.

Secure Shell y Secure File Transfer v2.4 (Ambiente Gráfico, protocolo SSH2)

Después de haber obtenido el programa deSecure Shell(SSHWin-2.4.0.exe) del sitio de Secure Shell o de sitio del Departamento de Seguridad en Cómputo realice los siguientes pasos.

a)Ejecutar el programa de instalación de Secure Shellcliente protocolo SSH2 (SSHWin-2.4.0.exe). Después de aceptar la licencia de uso, indicar el directorio donde será instalado, el fólder donde se almacenarán las herramientas y finalmente los componentes que desean instalarse.

Este cliente de Secure Shell le permitirá conectarse a sistemas remotos con Secure Shell protocolo SSH2 y también realizar transferencias de archivos de forma gráfica.

Usando SSH

Sesión entre máquinas en UNIX

SSH permite mantener sesiones interactivas con una máquina remota de la forma como lo hace el comando telnet.

ssh [-a] [-c idea|blowfish|des|3des|arcfour|none] [-e esc] [-i identity_file] [-l login_name] [-n] [-k] [-V] [-o] [-p

-a Habilita la estadística de transferencia de cada archivo que se transfiere.

-A

$ ssh -l cuenta maquina.cliente.de.shosts
Esto es para que la máquina a la que se entrará, utilice el mecanismo .shostsy obtenga la llave pública de la máquina cliente.

2.-En la máquina servidor cree sobre el homedel usuario el archivo .shostsconteniendo el nombre de la máquina o la IP cliente.

$ more .shots
maquina.cliente.de.shosts

3.-Desde la máquina cliente realizamos el enlace.

$ ssh -l cuenta maquina.con.shosts

NOTA:Este tipo de conexiónno solicitará el password.

Esta conexión presenta un riesgo, sin embargo, introduce mecanismos propios de SSH, mayores niveles de seguridad se pueden obtener utilizando el método de llave RSA.

9.4.1. Tips

Sí no se lleva a cabo la conexión verifique los permisos del archivo.

$ chmod 644tiidvcosts

Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_dsa.
Your public key has been saved in /home/usuario/.ssh/id_dsa.pub.
The key fingerprint is:
1a:84:34:9f:d1:97:76:03:c0:c7:be:12:b0:95:1e:37 usuario@Cliente

Se generan dos archivitos en el directorio ~/.ssh/.

id_dsa.pub(publica)
id_dsa (privada)

2.-Exportar id_dsa.pubal servidor, éste realizará la conexión, e incluirá su contenido en el archivo ~/.ssh/authorized_keys2.

Servidor>cat id_dsa.pub.Cliente >> ~/.ssh/authorized_keys2

Quedando algo así:

Servidor> cat ~/.ssh/authorized_keys2
ssh-rsa mslHXihCHvYNADHKvFPSESKHUpwF0TbpmvMesSGifqhQftn8BOU=usuario@Cliente

3.-Probar la conexión.

Cliente> ssh cuenta@Servidor
Servidor>

Referencias

UNAM-CERT Equipo de Respuesta a Incidentes UNAM
StREirección de Seguridad de la Información
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Naciónal Autónoma de México
E-Mail: seguridad@seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 43