Acceso remoto por SSH

(versión 2.0)

Índice

Resumo

No caso de que se dispoña de equipos que non teñen teclado ou pantalla, de servidores apilados nun rack ou ordenadores que non estan fisicamente presentes é moi importante contar con mecanismos que permitan administralos remotamente de forma cómoda, rápida e segura.

Os servizos de acceso e control remotos permiten a utilización de determinadas aplicacions de software para establecer conexions con equipos a distancia e administralos de xeito centralizado sen necesidade de acceder a eles.

Introdución

O acceso remoto é a capacidade de acceder a un ordenador ou a unha rede ando non se está fisicamente sentado nun dispositivo dos que forman parte desa rede. Pode ser empregado para traballar dende casa, para acceder a arquivos ou para controlar unha rede dende un lugar distante.

Os servizos de acceso e control remotos permiten establecer conexións con equipos a distancia e administralos de xeito centralizado sen necesidade de estar fisicamente diante deles. Loxicamente este uso pode ter consecuencias impredecibles se non se leva a cabo coas condicións de seguridade ben definidas. Calquera burato de seguridade pode permitir o acceso de terceiros non desexados a informacións confidenciais.

O acceso remoto pode ser feito de varias maneiras, dependendo do sistema operativo e do tipo de conexión que se desexe establecer. As conexións remotas permiten facer fundamentalmente dúas cousas: control remoto e transferencia de arquivos.

- **O control remoto** permite acceder a un equipo dende outro e manexalo coma se estiveramos diante del. Pódese facer en modo texto ou en modo gráfico. O control remoto en modo texto é máis seguro e rápido, xa que non require a transmisión de imaxes. O control remoto en modo gráfico é máis cómodo para o usuario xa que pode ver a pantalla do equipo ao que se conecta.
- **A transferencia de arquivos** permite copiar arquivos entre equipos. A transferencia de arquivos segura cifra a información que se transmite, mentres que a transferencia de arquivos non segura non o fai.

As ferramentas de administración remota máis utilizadas actualmente son:

modo texto: telnet, rlogin e Secure Shell (SSH)

modo gráfico: VNC e os servizos de Terminal Server en Windows.

1. Telnet

Telnet é un protocolo da capa de aplicación do modelo TCP/IP que permite conectarse a outra máquina e utilizar os seus recursos coma se estivéramos traballando dela. Vale tanto para conexións dentro dunha rede local como a traverso de internet. Hoxe en día practicamdnte só se usa para conectarse a dispositivos como switches e routers para configuralos ou para facer probas de conexión entre equipos.

A máquina á que se accede debe ter un programa especial que reciba e xestione as conexións. O porto que se utiliza xeralmente é o 23. Con *telnet* e a IP da máquina de destino áccedese en modo texto dende un terminal.

A súa maior eiva é a seguridade ao non estar a comunicación protexida; non vai cifrada. Todo o que se transmite pode ser visto por programas que capturen o tráfico da rede. Como ao principio da sesión hai que identificarse co nome de usuario e contrasinal esto xa implica unha debilidade na conexión. Alguén malicioso pode quedarse con estes datos.

2. SSH

O protocolo SSH permite o acceso remoto a outro ordenador establecendo conexións seguras entre os dous equipos seguindo o modelo cliente-servidor. A diferencia con *telnet* reside na seguridade. Na primeira conexión, o cliente e o servidor establecen comunicación cando o cliente transmite ao servidor a información necesaria para a autenticación. Esta información xa vai en formato cifrado. Todos os datos que se envían e se reciben dende ese intre transfírense encriptados. As principais características do servicio SSH son as seguintes:

- Utiliza o porto 22 (TCP e UDP)
- Permite a autenticación dos usuarios mediante contraseña ou un sistema de chaves.
- Permite a súa integración con outros sistemas de autenticación como Kerberos, PGP o PAM.
- Está implementado para a meirande parte de sistemas operativos e plataformas, incluso para móbiles.
- O cliente pode executar aplicacións gráficas dende o terminal de forma segura.

O protocolo menos seguro é...

1. Telnet
2. SSH
3. FTP

Para transferir arquivos podo usar ...

1. só o protocolo FTP
2. só o protocolo SSH
3. SSH e tamén FTP

Para traballar con SSH precisamos instalar os paquetes correspondentes, tanto `ssh-client` coma `ssh-server`. Ambos están incluídos na instalación do paquete de código aberto chamado OpenSSH. O habitual é instalar ambos en cada equipo se queremos establecer unha comunicación bidirecional, é dicir que unha máquina poda acceder á outra e viceversa. Por cliente enténdese o ordenador que lanza a orde SSH e por servidor a máquina á que entramos en remoto e que contesta á nosa petición.

O protocolo SSH permite o acceso remoto pero tamén a transferencia segura de arquivos e a creación de túneles. O funcionamento deste protocolo descríbese na RFC 4251.

2.1. Cifrado

A comunicación entre cliente e servidor SSH está cifrada cunha chave simétrica para facer máis eficiente a transferencia de información. Nembargantes o establecimento da conexión e o intercambio desta chave simétrica realízase mediante un cifrado asimétrico, de forma que se reforza o punto máis feble do protocolo de intercambio de claves que é a autenticación.

2.2. Tunneling ou port forwarding

Traducido ás veces por reenvío de portos. A idea do túnel é encapsular un protocolo de rede dentro de outro. Por exemplo enviar un paquete HTTP dentro dun paquete SSH. Os proxy polos que viaxa só detectarán un paquete SSH sen ter xeito de averiguar o que vai nel. Vemos na figura 1 como conectarse dende un terminal usando o reenvío de portos. O porto 8080 do equipo local rediríxese ao porto 80 do servidor remoto. O porto 22 é o que se usa para a conexión SSH.

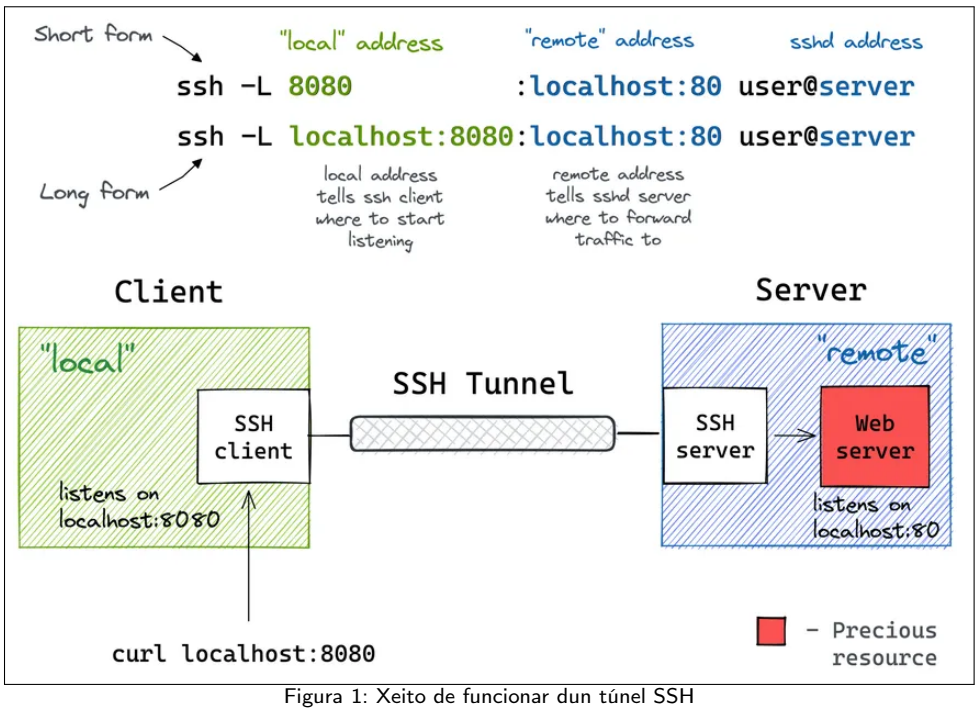

Figura 1: Xeito de funcionar dun túnel SSH

Se o único no que estamos interesados é na conexión remota para traer e levar ficheiros temos varias opcións:

SCP é unha ferramenta de transferencia de arquivos segura que permite a transferencia de arquivos entre dous equipos. SCP é unha extensión do protocolo SSH e emprega o porto 22. A súa principal vantaxe é a seguridade, xa que a información que se transmite vai cifrada.

SFTP vén sendo unha variante da conexión FTP. Lembramos que o acceso a un servidor FTP non é nada fiable. Se nos conectamos a un servidor FTP pero utilizando o protocolo SSH, a conexión xa é segura.

SFTP é un protocolo que permite a transferencia de arquivos entre dous equipos cifrando a información que se transmite grazas ao uso conxunto con SSH. SFTP é unha extensión do protocolo SSH e daquela emprega o porto 22. A información FTP vai dentro do SSH polo que non é necesario abrir un porto adicional no firewall.

SFTP permite usar todo o potencial do protocolo SSH, como a autenticación mediante chaves públicas e privadas para a transferencia de arquivos xunto con todas as posibilidades e comandos de FTP, como carga e descarga de ficheiros, creación de directorios, xestión de permisos, etc. todo iso dentro dun túnel SSH.

O cifrado en SSH...

1. sempre é simétrico
2. sempre é asimétrico
3. nuns casos é simétrico e noutros asimétrico

Tunneling permite...

1. enviar unha páxina web encriptada
2. encapsular o contrasinal do root
3. viaxar por un proxy sen cifrar

3. Outras conexións remotas

Tamén podemos emplegar clientes web que permiten manexar o equipo dende unha interfaz visible nunha páxina web, como por exemplo o escritorio remoto de Chrome.

3.1. VNC

VNC *Virtual Network Computing* é un servizo sobre TCP/IP de administración remota "tal cual" mediante terminal gráfico e multiplataforma. VNC mostra no cliente a pantalla do dispositivo servidor, polo que require unha conexión de red veloz. Pódese adaptar a calidade do servizo á velocidade cambiando parámetros como resolución, profundidade de cor, compresión de datos (con ou sen perda, etc.). Existen múltiples clientes/servidores para todas as plataformas. En Windows destacan **TightVNC** por ser gratuito e lixeiro e **TeamViewer** que permite o acceso a máquinas fóra da LAN.

Adoita usar os portos 5900 ou 5800 pero poden establecerse outros.

3.2. RDP

RDP *Remote Desktop Protocol* é un servizo sobre TCP/IP de administración remota mediante terminal gráfico exclusivo para servidores Windows. A vantaxe principal de RDP frente a VNC é o uso de primitivas propias de representación en pantalla de Windows para a representación no cliente, optimizandoo rendemento da administración remota en entornos Windows. Soporta conexiones autenticadas en Active Directory. El servidor se activa en `Panel de Control/Sistema/Acceso Remoto`. O porto que utiliza é o 3389.

Administro en remoto...

1. equipos sen teclado
2. servidores de correo
3. todas as respostas son correctas

Ferramentas de acceso remoto...

1. VLC
2. VNC
3. ambas son correctas

4. Máis información

- Vídeo moi bo sobre como funciona SSH en inglés
- Cifrado SSH
- Explicación dos túneles SSH

Material elaborado para traballar na asignatura *Servizos en rede* de SMR conxuntamente con:

irocho.worpress.com