

Mini Guía para usar las Keops en el ITAM

Adrián Puente Z.
Sala de Servidores
Instituto Tecnológico Autónomo de México

7 de abril de 2005

1. Introducción.

Cómo alumno de la materia de Sistemas Operativos he visto la necesidad de los alumnos de poder emplear las máquinas de Keops para poder hacer sus prácticas de UNIX. Por seguridad estas máquinas se encuentran detrás de un Firewall aparte de que los servicios de FTP y Telnet son extremadamente inseguros por transferir los datos en texto plano.

Con esta guía busco ayudar a los alumnos para facilitarle la manera de hacer sus prácticas y que aprenda un nuevo concepto cómo el tuneleo y el protocolo de SSH.

2. Algunos conceptos.

Es un protocolo que vino a sustituir el protocolo de telnet, rlogin y rsh que mostraron ser inseguros al transferir los datos de forma de texto plano que puede ser capturada con cualquier analizador de protocolos que se encuentre en la red (ataque de hombre en medio).

Este protocolo funciona con un intercambio de llaves formando un “túnel” de cifrado que sólo los poseedores de las llaves puedan acceder al contenido de el túnel. Este protocolo es muy dinámico, aparte de darnos una sesión interactiva de shell, también podemos transferir archivos y redirecciona puertos de otras máquinas permitiendo crear “túneles” para aplicaciones que son menos seguras.

Para esto un ejemplo:

Digamos que somos la máquina usuario y queremos acceder a la keops12.itam.mx por telnet desde nuestra casa. Obviamente no podemos por el Firewall instalado entre nosotros y la máquina keops12.itam.mx. Por otro lado tenemos la máquina alumnos.itam.mx de la cual tenemos un usuario válido y este nos da servicio de SSH y podemos alcanzarlo desde nuestra casa pues el Firewall tiene abierto ese puerto para la máquina alumnos.itam.mx.



Si usamos las propiedades que nos brinda este protocolo podemos crear un túnel seguro para poder acceder al puerto de Telnet de la máquina keops12 pasando a través de la máquina Shell. En pocas palabras vamos a conectarnos desde nuestra máquina a la máquina alumnos.itam.mx usando el protocolo de Secure Shell (puerto 22) para redirigirlo. Por ende podemos concluir que usamos la máquina servidor de SSH cómo Proxi para ingresar a servicios de otras máquinas que están bloqueadas por seguridad.

3. Menos charla mas acción.

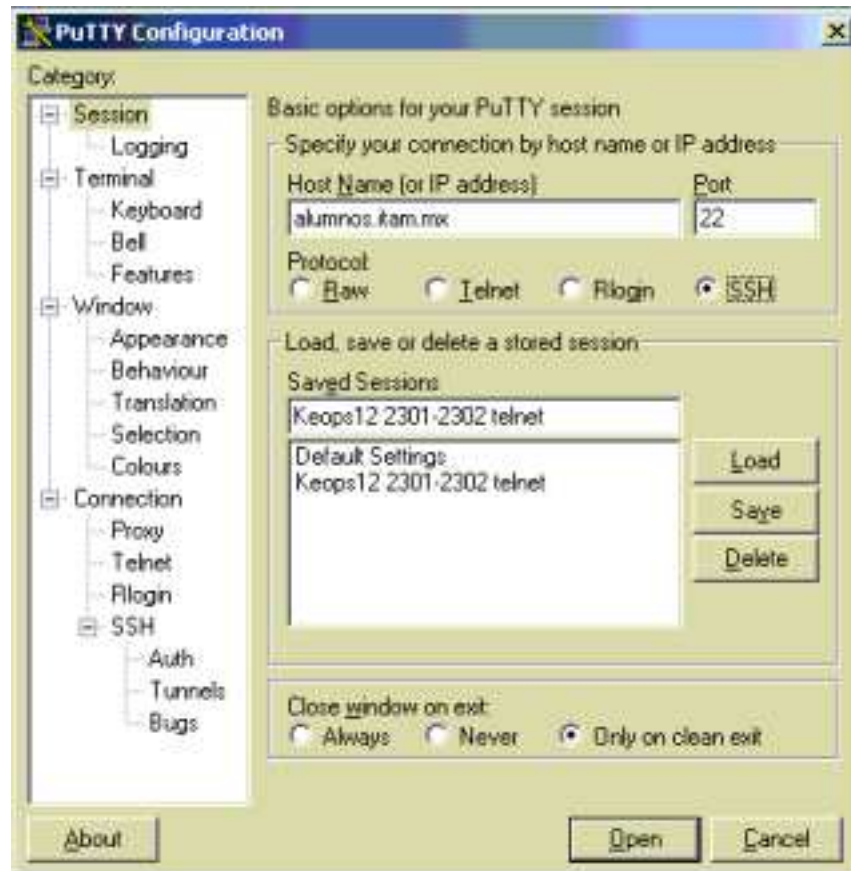
Para lograr esto en Windows necesitamos un cliente de Secure Shell que podemos descargar aquí <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Este funcional cliente aparte de que es pequeño, es cliente de Telnet y Secure Shell. empecemos con la configuración. Para lograr un Proxi de SSH tenemos que asignar un puerto local, el nombre o IP de la máquina a la que queremos accesar y el puerto remoto. El puerto local es en el cual nos hemos de conectar y que estará ligado con el túnel SSH al Proxi que nos redirigirá al puerto de la máquina remota.

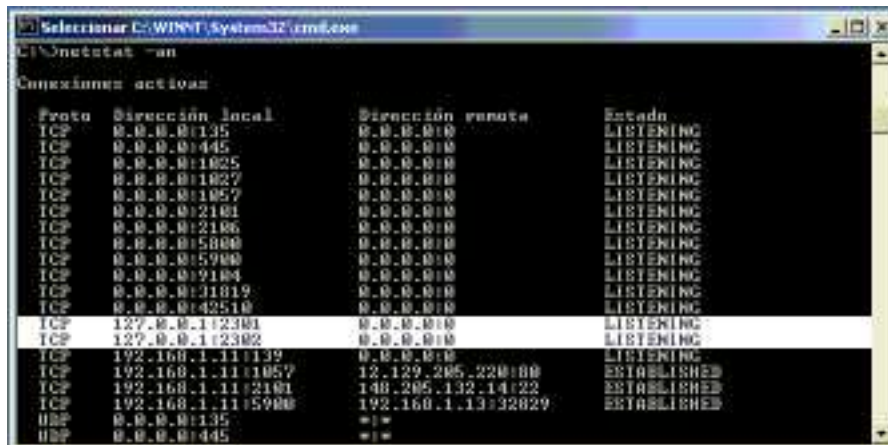
Abrimos el programa de Putty y nos vamos a la sección de túneles casi hasta el final de las opciones.



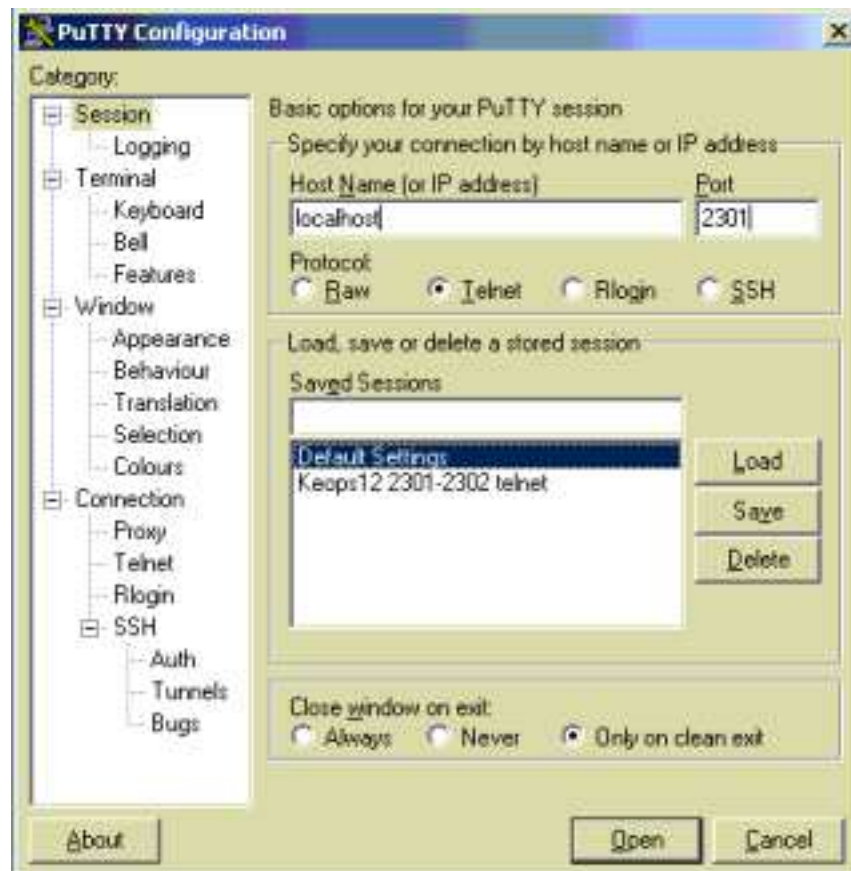
El source port es nuestro puerto local, al que vamos a conectarnos al túnel para hacer Telnet en este caso. El destino es la máquina con el puerto al que queremos conectarnos. Ahora debemos ingresar a las opciones que nos den la conexión al Proxi.



Podemos guardar nuestra configuración con un nombre bastante sugerente. En mi caso decidí usar los puertos 2301 y 2302 por varias razones, entre ellas que muchas veces se necesitan ciertos privilegios para abrir puertos de escuchar menores a 1024, porque 2301 me recuerda que es el puerto remoto 23 túnel 01 ya que para cada conexión hay que hacer un túnel diferente y cada túnel usa un puerto local. Ok, ingresamos el servidor que nos servirá de Proxi usando el protocolo de SSH. y nos conectamos. Este es el servidor de correo del ITAM. Todos los alumnos tienen cuenta en el y si no, lo pueden solicitar en el SYTI del ITAM. En fin, ingresamos nuestro usuario y contraseña válidos y ya que entremos al servicio podemos minimizar la pantalla pues con ella ya no haremos nada mas que usar los túneles que ha creado.



Si ejecutamos el comando netstat -an podemos ver cómo los puertos 2301 y el 2302 están abiertos en nuestra máquina y esperan conexión, misma que haremos con nuestro cliente de telnet.



Abrimos nuevamente nuestro cliente putty y ahora nos conectamos localmente al puerto que tiene el túnel, en mi caso es el 2301, usando el protocolo Telnet que es el que queremos usar para la keops12.itam.mx.



Cómo podemos ver el cliente putty se conecta localmente (mi máquina se llama Artemisa) pero vemos el login de la deseada keops12.itam.mx. En pocas palabras estamos haciendo un túnel SSH a la máquina alumnos.itam.mx y este nos redirige el contenido del túnel, en este caso la conexión telnet, a la máquina keops02.itam.mx.

4. Conclusiones.

SSH ha demostrado ser un protocolo muy dinámico, poderoso y seguro pues aparte de darnos privacidad de la información que estamos transmitiendo, nos da autenticación pues maneja huellas digitales de la llave RSA que empleamos y nos solicitarnos usuario y contraseña para ingresar al sistema y no repudiación al quedarse logeado el ingreso del usuario. Un protocolo lindo ¿no?

Este mismo método de Proxi también puede servir para otros protocolos cómo POP3 SMTP y FTP que carga información sensible y no tienen privacidad.