Seguridad en Sistemas Informáticos (SSI)

VNIVERSITAT DE VALÈNCIA OpenCourseWare

Laboratorio: Acceso remoto seguro con SSH

Carlos Pérez Conde

Departament d'Informàtica

Escola Técnica Superior d'Enginyeria

Universitat de València

SSH

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Objetivos:**
  - aprender a utilizar la herramienta SSH para aumentar la seguridad de los accesos remotos a sistemas informáticos
- **Actividades a realizar**
  - comprobación de la puesta en marcha del servidor
  - establecimiento de conexiones remotas
  - ejecución de órdenes remotas
  - autentificación mediante criptografía asimétrica
  - redirección de puertos

Puesta en marcha del servidor en “exta”

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Arrancar “exta” (“uml.sh a”)**
- **Entrar en la consola como “root”**
- **Comprobar que el servidor (sshd) está corriendo:**
  - netstat -atnp
    - debe aparecer una línea del estilo:
      tcp 0 0 :::22 :::* LISTEN 1106/sshd
    - Si no estuviese corriendo, ponerlo en marcha: /etc/init.d/ssh start
- **Probar a conectarse al propio nodo:**
  - ssh localhost
- **Identificar la conexión recién establecida**
  - pista: usar netstat con -t y buscar conexiones "ESTABLISHED"
- **Cerrar la conexión**

Establecimiento de conexiones remotas (desde “base”)

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Conectarse a “exta” desde “base”**
  - sugerencia: usar la opción “-X”, consultando antes en el manual para qué sirve
- **Identificar la conexión recién establecida**
- **Usar esta conexión para ejecutar 'xclock' en 2º plano**
- **Averiguar qué servidor X está utilizando**
  - sugerencia: utilizar 'echo $DISPLAY', netstat y consultar las transparencias del curso
- **Parar la aplicación xclock**
- **Cerrar la conexión SSH**

Ejecución de órdenes remotas

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Ejecutar en “exta” la orden 'date'**
- **Ejecutar en “exta” la orden 'xclock'**
  - sugerencia: utilizar las opciones -X y -f, consultando antes en el manual para qué sirven
- **Utilizando 'scp', copiar un fichero al directorio /tmp de “exta” (ej: scp fichero root@exta.example.net:/tmp/.)**
  - sugerencia: crear y después copiar un fichero con un par de líneas
- **Comprobar que el fichero ha sido transferido correctamente**
  - sugerencia: conectarse con 'ssh' y verlo con 'cat' o, alternativamente, comprobarlo con la ejecución remota de 'cat'

Autentificación con criptografía asimétrica

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **En “base”, crear un par de claves con 'ssh-keygen'**
  - crear las claves de tipo 'dsa' (sugerencia: utilizar la opción -t)
  - guardar la clave privada como $HOME/.ssh/id_dsa
  - utilizar una frase de paso
- **Añadir la clave pública ($HOME/.ssh/id_dsa.pub) al fichero $HOME/.ssh/authorized_keys de “exta”**
- **Conectarse a “exta” desde “base” utilizando 'ssh'**
- **Observar que ahora pide la frase de paso de la clave privada (y no la contraseña)**

Empleo del agente de autentificación

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- En 'base', añadir la clave privada al agente, introduciendo la frase de paso cuando sea solicitada
  - sugerencia: usar ssh-add
- Conectarse a “exta” desde “base” utilizando 'ssh'
- Observar que NO pide NI la frase de paso de la clave NI la contraseña
- Probar a ejecutar órdenes remotas y a copiar ficheros (no debe hacer falta contraseña)
- En 'base', eliminar la clave del agente (sugerencia: usar ssh-add con las opciones -d ó -D)

Utilización de claves para tareas concretas

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- Crear un nuevo par de claves DSA con frase de paso, utilizando 'copia_dsa' como nombre de la clave privada
- Añadir la clave pública ($HOME/.ssh/copia_dsa.pub) al fichero $HOME/.ssh/authorized_keys de “exta”
- Añadirla al agente
- Comprobar que funciona sin pedir contraseña
- Editar el fichero $HOME/.ssh/authorized_keys de “exta” para que cuando el cliente se autentifique con esa clave se ejecute la orden '/bin/date'
  - sugerencia: consultar las transparencias del curso
- Comprobar que sólo se puede ejecutar 'date'

Redirección de puertos

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- Poner en marcha 'netcat' en modo servidor en el puerto 20023 de “extc” (netcat -l -p 30023)
- Desde “base”, conectarse a “exta” de manera que las conexiones al puerto 30000 de “exta” sean redirigidas al puerto 30023 de “extc”
- Conectarse en “exta” con 'netcat' al puerto 30000 (netcat localhost 30000)
- Comprobar que no existen conexiones entre “exta” y “extc”, pero sí existen las siguientes:
  - SSH entre “base” y “exta”
  - conexión de “bae” al puerto 30023 de “extc”
- Cerrar la conexión

Redirección de puertos (2)

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- Desde “base”, conectarse a “exta” de manera que las conexiones al puerto 30000 de “base” sean redirigidas al puerto 30023 de “extc”
- Conectarse en “base” con 'netcat' al puerto 30000 (netcat localhost 30000)
- Comprobar que no existen conexiones entre “base” y “extc”, pero sí existen las siguientes:
  - SSH entre “base” y “exta”
  - conexión de “exta” al puerto 30023 de “extc”
- Cerrar la conexión