OpenSSH

I Jornadas Seguridad GNU/Linux

Jose Miguel Garrido (AugCyL)

Problema:

Conectarnos de forma segura a una maquina remota

El telnet NO es seguro

SSH

Secure shell

- Aplicacion de usuario
- Las contraseñas viajan encriptadas
- El contenido de la sesion se encripta
- No se pueden repetir las tramas
- Se evitan servidores falsos y otros problemas

Historia OpenSSH

- SSH se converte en no libre
- Grupo de gente ligada a OpenBSD crea OpenSSH
- Se soporta la version SSH 2 del protocolo
- Demanda legal de SSH

Protocolos

- SSH 1 -> 1.3 y 1.7
- SSH 2 -> Standard

OpenSSH como telnet

ssh usuario@maquina

Hace X forwading

Uso con llave publica

Solo el poseedor del la llave privada (nosotros) es autorizado a entrar

Creacion de la llave

- Para ssh 1
  - ssh-keygen
- para ssh 2
  - ssh-keygen -t dsa

Uso con llave publica (2)

Copiado al directorio remoto

- Debemos copiar este .pub fichero a
  - SSH 1 -> ~/.ssh/authorized_keys
  - SSH 2 -> ~/.ssh/authorized_keys2
- Usamos scp, no rcp o similar
  - scp ~/.ssh/*.pub usuario@sistema:
- Y con >> al fichero correspondiente

Uso con llave publica (y 3)

- Quitar permiso de escritura a group y others
- Ahora nos pide la frase de paso de la clave privada,no del servidor
- ¡Hemos perdido comodidad!

Uso de claves en memoria

- Con ssh-agent guardamos claves en memoria
- Primero debemos lanzarlo
  - ssh-agent ssh
  - ssh-agent startx
- Despues añadir claves con ssh-add
  - ssh-add
  - ssh-add ~/.ssh/id_dsa

Otros comandos

- scp - sustituto de rcp
- sftp - sustituto de ftp
- slogin - sinonimo de ssh
- ssh-keyscan - busca servidores en la red

Autentificacion de servidor

No solo los ususarios se autentifican, tambien los servidores

Las claves se almacenan por usuario y globalmente

Las claves se comprueban y se avisa en caso de cambio de servidor

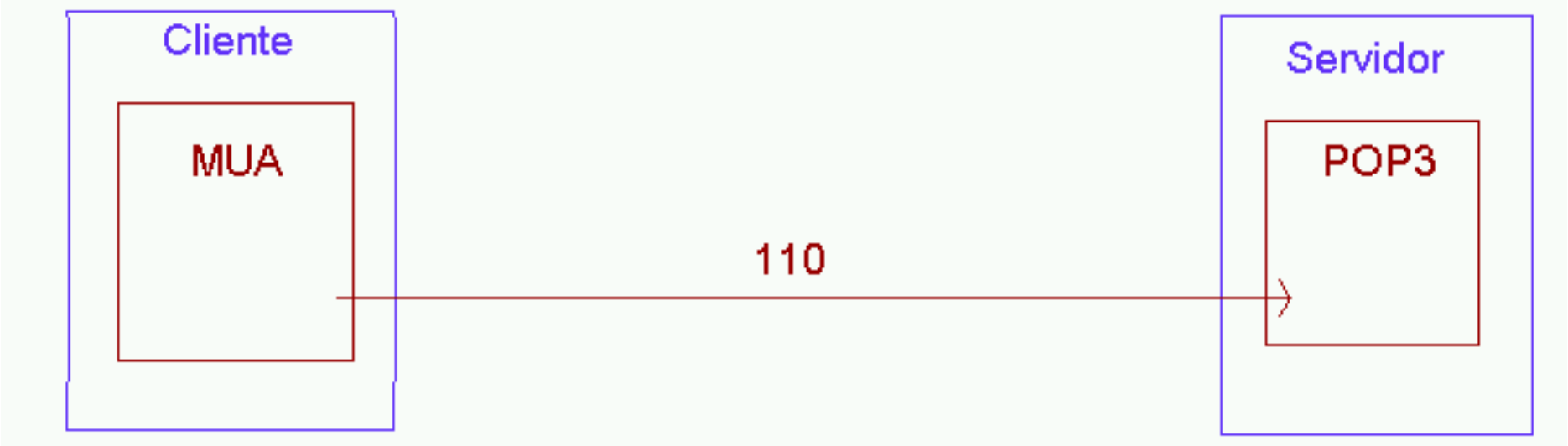
Configuracion

Existe configuracion global y por usuario

- /etc/ssh
  - ssh_known_hosts,ssh_known_hosts2
  - ssh_config
- ~/.ssh
  - ssh_known_hosts
  - config

Tuneles seguros

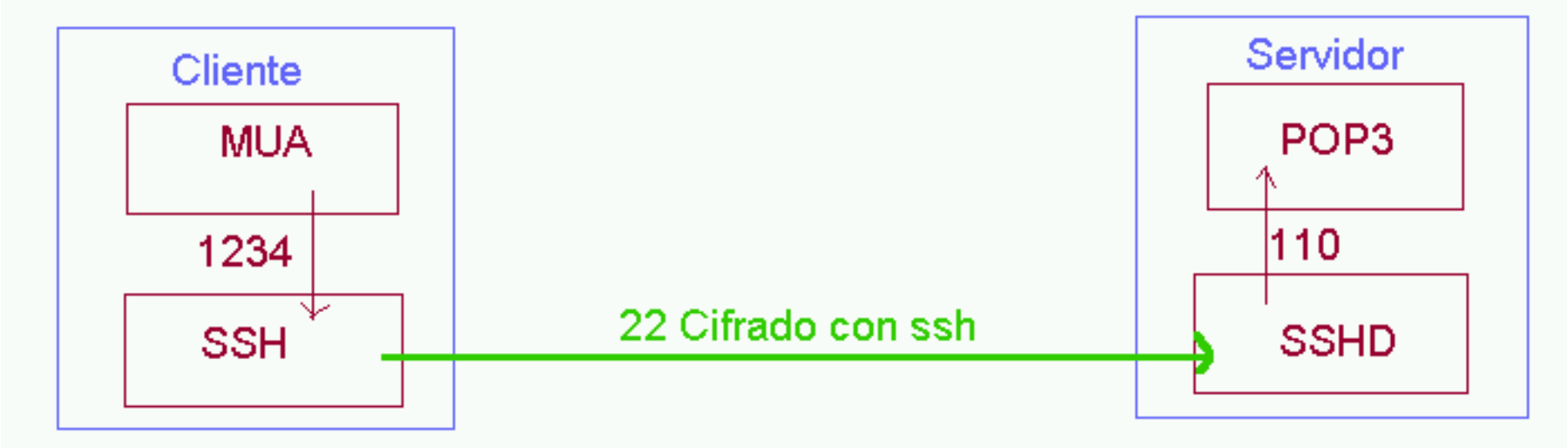
Se pueden crear tuneles seguros arbitrarios



Nuestras contraseñas viajan de forma no segura al servidor de correo

Tuneles seguros (y 2)

ssh -L 1234:servidor:110 servidor



Debo cambiar mi cliente de correo para que se conecte a 1234 local

Virtual Private Networks

Conexion transparente entre dos redes de forma segura

- IPsec
- ssh y ppp

Referencias

Ficheros manual

Libro "SSH, the secure shell" de O’Reilly 0-596-00011-1

Oficial www.openssh.org

Comercial www.ssh.com