Práctica IV.: Protocolos Seguros y Auditorías de Seguridad (2 sesiones - 4 horas)

Prof. A. Santos del Riego
Legislación y Seguridad Informática (LSI)
Facultad de Informática. Universidad de A Coruña
Fecha propuesta.: enero-2004
Última revisión.: agosto-2012

El objetivo de esta práctica es comprender la importancia de los algoritmos criptográficos, el uso de autoridades de certificación y su aplicación-funcionamiento en la forma de protocolos seguros. Hemos tratado en las clases teóricas el esquema de funcionamiento de la firma digital y la necesidad de autoridades certificadoras, así como la securización de los servicios mediante protocolos seguros. Se deberán aplicar los conceptos adquiridos en la resolución de los siguientes apartados:

1. Tomando como base de trabajo el SSH pruebe sus diversas utilidades:
    a. Abra un *shell* remoto sobre SSH y analice el proceso que se realiza. Configure su fichero `ssh_known_hosts` para dar soporte a la clave pública del servidor.
    b. Haga una copia remota de un fichero utilizando un algoritmo de cifrado determinado. Analice el proceso que se realiza.
    c. Configure su cliente y servidor para permitir conexiones basadas en un esquema de autenticación de usuario de clave pública.
    d. Mediante túneles SSH securice algún servicio no seguro.
    e. Securice su sevidor considerando que únicamente dará servicio ssh para sesiones de usuario desde determinadas IPs.
2. Tomando como base de trabajo el servidor Apache2
    a. Configure una Autoridad Certificadora en su equipo.
    b. Cree su propio certificado para ser firmado por la Autoridad Certificadora. Bueno, y fírmelo.
    c. Configure su Apache para que únicamente proporcione acceso a un determinado directorio del árbol web bajo la condición del uso de SSL y previa autenticación.
3. Tomando como base de trabajo el openVPN deberá configurar una VPN entre dos equipos virtuales del laboratorio que garanticen la confidencialidad entre sus comunicaciones.