

Práctica IV.: Criptografía y Protocolos Seguros [2010-2011]

Práctica propuesta.: enero 2004. Última revisión.: mayo 2011

Prof. A. Santos del Riego

Protección y Seguridad de la Información (PSI)

Facultad de Informática. Universidade da Coruña

El objetivo de esta práctica es comprender la importancia de los algoritmos criptográficos y su aplicación-funcionamiento en la forma de protocolos seguros. Hemos tratado en las clases teóricas los conceptos que rigen el funcionamiento de los criptosistemas simétricos y asimétricos, así como su integración híbrida en protocolos seguros. Se ha estudiado el esquema de funcionamiento de la firma digital y la necesidad de autoridades certificadoras. Finalmente, se ha presentado el funcionamiento de algunos protocolos y entornos seguros (SSH, GPG, SSL, etc.). Se deberán aplicar los conceptos adquiridos en la resolución de los siguientes apartados:

1. EN LA PRÁCTICA 1 se configuró una infraestructura con servidores y clientes NTP. Modifique la configuración e integre un esquema de autenticación entre clientes y servidores.
2. EN LA PRÁCTICA 1 se instalaron servidores y clientes de log. Configure un esquema que permita cifrar las comunicaciones..
3. 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 servidor considerando que únicamente dará servicio ssh para sesiones de usuario desde determinadas IPs.
4. 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.
5. Tomando como base de trabajo el openVPN deberá configurar una VPN entre dos equipos virtuales del laboratorio que garanticen la confidencialidad entre sus comunicaciones.
6. Al final de esta cuarta práctica, cada máquina virtual será servidor y cliente de diversos servicios (NTP, syslog, ssh, web, etc.). Configure un "firewall stateful" de máquina adecuado a la situación actual de su máquina.