Redes de computadoras

Practica 3

26 de febrero de 2018

Organizar los repositorios por práctica, y especificar en los README.md los integrantes del equipo que participaron en la realización

1. Leer la publicación llamada "New Directions in Cryptography" y resumir brevemente el esquema de intercambio de llaves propuesto por Diffie Hellman en un README.md
2. Realizar investigación sobre Public Key Infrastructure y resumir brevemente en un README.md lo que es e implica.
3. Implementar certificados en el servidor WEB
   - Incluir descripciones breves y capturas de pantallas en el README.md
   - Utilizar el script CA.pl para crear una nueva autoridad certificadora.
   - Emplear el mismo script CA.pl para crear una requisición de certificado.
   - Emplear el script CA.pl para generar el nuevo certificado.
   - Configurar el servidor WEB para que acepte conexiones por TLS/SSL a través del puerto 443, importando el certificado generado en los puntos anteriores.
4. Con el comando tcpdump, comprobar que el tráfico a través del puerto 443 viaja cifrado.