Quiz 5-6

Roy Chavarría Garita

Carné: 2018034199

Respuesta a

Sí es posible enviar datos no HTTPs por medio del puerto 443 al final es solo un puerto y como se menciona en el libro de Tanembau "Cuando HTTP se utiliza encima de SSL, se conoce como HTTPS (HTTP Seguro), aunque es el protocolo HTTP estándar. Sin embargo, algunas veces está disponible en un nuevo puerto (443) en lugar de en uno estándar (80). Además, SSL no está restringido a utilizarse sólo con navegadores Web, pero ésa es la aplicación más común." (Tanenbaum, 2003, p.813)

Respuesta b

Se tienen 2 puntos para realizar una conexión, el punto A y el punto B, primero el A solicita una conexión a B, esta solicitud lleva la versión de SSl que A está utilizando junto los algoritmos de compresión que puede soportar, luego B establece uno de los algoritmo soportado por A y envía un certificado de clave pública y de último envía otro mensaje indicando el turno de A. Una vez A recibe el último mensaje de B, A envía una clave premaestra encriptada con la clave pública de B. Una vez enviada la clave, B y A pueden calcular su clave de conexión en base a los mensajes que los 2 han enviado. Luego como los 2 pueden calcular esa clave de conexión, A le dice a B que la cambie hacia el nuevo cifrado y también le menciona que ya se ha realizado la conexión satisfactoriamente. Por último B confirma los últimos mensajes. (Tanenbaum, 2003, p. 814)

Respuesta c

Sí es posible enviar, una forma de hacerlo es incluyendolo dentro del cuerpo del paquete http.

Respuesta d

Como se menciona en el libro de Tanenbau, "Por lo general, los filtros de paquetes son manejados por tablas configuradas por el administrador del sistema. Dichas tablas listan orígenes y destinos aceptables, orígenes y destinos bloqueados, y reglas predeterminadas sobre lo que se debe hacer con los paquetes que van o vienen de otras máquinas." (Tanenbaum, 2003, p. 814)

Estas tablas se configuran manualmente y en la mayoría de tablas está configurado el puerto 80 normalmente para páginas web, si se utilizace el puerto TCP/666 se tendría que cambiar todas las tablas para que aceptase trafico de cualquier ip por medio de ese puerto y es no sería muy bueno.

Respuesta 2

La Infraestructura de Clave Pública posee componentes como usuarios, CAs, certificados y directorios. Su función es proporcionar una forma para estructurar estos componentes y definir estándares para los diversos documentos y protocolos. Una forma simple de PKI está dada por CAs otro nivel son las RAs las cuales son certificadas por las RAs.

Ejemplo de funcionamiento de PKI: Supongamos que necesito la clave publica de B para establecer una comunicación, por lo que Bbusca un certificado que la contiene, firmado por la CA 5. Pero nunca he escuchado de la CA5, por lo que puedo deducir que la CA 5 puede ser la hija de B. Por este problema puedo ir con la CA5 y decirle: prueba tu autenticidad, por lo que CA 5 responde con el certificado que obtuvo de la RA 2 que contiene la clave pública. Una vez tengo la clave pública de CA 5, puedo verificar la autenticidad y la legalidad. Para asegurarme que RA 2 no sea la hija de B, pido a la RA 2 que pruebe la autenticidad. B responde un certificado firmado por la raíz que contiene la clave pública RA 2. Por lo que ahora sí estoy seguro que tengo la clave úblic de B.

Pero cómo averiguo la clave pública de la raiz? la razón es porque todos conocen la clave pública. Por ejemplo el navegador pudo haber enviado con la vlave pública de la raíz integrada en él. Si B no quiere causar mucho trabajo, él me puede ahorrar la verificación de CA 5 y RA 2 recolectándolos y enviandomelos junto al de él. Por lo que se puede usar el conocimiento que tiene la clave pública de la raíz para verificar el certificado de nivel superior y la clave pública contenida ahí para verificar la segunda. Por tal razón no veo necesario contactar a nadie para realizar la verificación. Como todos están firmados, puedo detectar cualquier intento de alteración de contenido. (Tanenbaum, 2003, p. 769-770)

Referencia

Tanenbaum, A. Computer Networks. 4ta edición. Upper Saddle River, NJ:Prentice Hall, 2003.