Prueba Corta #9

Tecnológico de Costa Rica
Escuela de Ingeniería en Computación
Redes (IC 7602)
Primer Semestre 2023
Fecha de entrega: **30/05/23 antes de las 11:59 pm**
Tiempo estimado: **40 minutos**
Instrucciones:

- Conteste todas las preguntas con el nivel mínimo y suficiente de detalle para demostrar su conocimiento del tema.

Forma de entrega: **Email al profesor siguiendo los lineamientos del programa de curso, adjuntando documento y link al repositorio.**
Formato: **Markdown**
Nombre Archivo: **pc9.md**

---

1. Autrum Transfer Protocol (ATP), es un protocolo creado durante los años 90 para el envío de mensaje (este utilizaba el puerto TCP/666), este se volvió muy popular entre las personas jóvenes de la época que tenían acceso a una red, este protocolo era capaz de transportar cualquier carácter visible ASCII, parte de lo emocionante de este protocolo era lograr enviar los mensajes de forma cifrada y el proceso era enteramente manual, lo cual quiere decir que las personas involucradas en la transmisión conocían las llaves para cifrar y descifrar mensajes. ATP se ha puesto de moda en el 2022, el problema es que ATP es un protocolo sumamente débil en términos de seguridad y además usa un puerto poco convencional como lo es TCP/666, con el fin de evaluar sí es posible implementar una versión segura de este protocolo, se le solicita responder las siguientes preguntas:
    a. ¿Es posible enviar datos que no sean HTTPs sobre el puerto 443? Justifique su respuesta. (10 pts)
    b. Suponiendo que creamos el protocolo ATP over SSL (ATPs), describa un subprotocolo para el establecimiento de una conexión SSL. (40 pts)
    c. Si existe el protocolo ATPs, ¿Es posible transportar ATPs sobre HTTPs? Justifique su respuesta. (10 pts)
    d. Desde un punto de vista de firewalls, ¿Porqué sería muy conveniente usar el puerto TCP/80 en lugar de puerto TCP/666?.
2. Explique detalladamente el funcionamiento de RSA. (30 pts)

a. Si, HTTPs solo es un protocolo que indica el formato de los datos a enviar, y el puerto 443 es lo comun porque los firewalls ya estan configurados para permitir la recepcion de datos, pero si se configura otro puerto para que reciba HTTPs se puede hacer.

b. Podemos implementar un protocolo de llave publica y privada, para que solo los dos clientes participantes puedan desencriptar los mensajes que reciben.

c. Puesto a que ATP solo transporta caracteres ASCII que es algo que HTTP ya soporta y que el proceso de encriptacion en ATP es manual (echo por el usuario), si es posible montar ATP sobre HTTP, ademas HTTP tambien corre sobre TCP.

d. El puerto 80 en los firewalls ya esta configurado por defecto para recibir conexiones no seguras HTTP, por lo que no se requiere mayor configuracion en el firewall para que se acepte una conexion por este puerto.

2. RSA es el famoso protocolo que involucra llaves publica y privada, funciona en que la llave publica se utiliza para encriptar mensaje que solo pueden ser desencriptados por una llave privada, por lo que esta llave publica se puede compartir con quien sea y solo el propietario de la llave privada puede interpretar el mensaje, asi se establece una coneccion segura con mensajes encriptados.