Instituto Tecnológico de Costa Rica
Escuela de Computación
Redes GR 2
Prueba Corta 9
Profesor Gerardo Nereo Campos Araya
Estudiante Ary-El Durán Balestero Fecha de Entrega: 8/11/2022

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:
    1. ¿Es posible enviar datos que no sean HTTPs sobre el puerto 443? Justifique su respuesta. (10 pts)
        - Si es posible realizar esto, aunque el estandar diga que de ahi se corre la comunicación tipo HTTPs, se puede forzar una conexión tipo HTTP a este puerto.
    2. Suponiendo que creamos el protocolo ATP over SSL (ATPs), describa un subprotocolo para el establecimiento de una conexión SSL. (40 pts)
        - Se puede comenzar que los dos usuarios encargados de comunicarse entre ellos hablen sobre las opciones y preferencias de SSL que tienen para armar una conexión, luego se aseguran de que la claves de encriptación y decriptación sean las mismas, después de esto ya pueden comenzar a enviar mensajes entre ellos encriptando y descifrando.
    3. Si existe el protocolo ATPs, ¿Es posible transportar ATPs sobre HTTPs? Justifique su respuesta. (10 pts)
        - Si puede transmitir por HTTPs pero hay que asegurar de que las clave pública y secreta sean las mismas que las que ya conocen los usuarios, pero más que eso, si es totalmente posible correr ATPs sobre HTTPs
    4. Desde un punto de vista de firewalls, ¿Porqué sería muy conveniente usar el puerto TCP/80 en lugar de puerto TCP/666?.
        - El TCP/80 es el puerto default que se usa para la comnunicación tipo HTTP, eso significa que la mayoria de programas van a aceptar conexiones a este puerto sin problemas, ya que el puerto TCP/666 es mucho menos usado, esto podría significar que el firewall bloque las conexiones realizadas a este puerto.
2. Explique detalladamente el funcionamiento de RSA. (30 pts)
    - Primero se realizan los siguientes cálculos Seleccionar dos números primos, en este caso se van a representar como p y q Luego se calcula n = p _ q y z = (p - 1) _ (q - 1) Se selecciona un número primo respectoa a z, que se va a representar con d Conseguir un e que pueda hacer e * d = 1 mod z Se separa el texto en múltiples bloques y luego solo queda encriptar y decifrar los mensajes, en este caso el texto llano seria P y el encriptado seria C, esto se realizaría haciendo $C = P^{e} \pmod{n}$ para encriptar y $P = C^{d} \pmod{n}$ para desencriptar.