Trabajo Práctico N°5

Objetivos:

- Manipular librerías de networking y analizar la capa de transporte en sistemas encriptados

Requisitos:

- 2 PCs + Software de análisis/generación de tráfico (por ej. Wireshark)
- IDE + Librerías de Networking en un lenguaje de programación de tu preferencia

1) Desarrollar scripts para enviar y recibir secuencialmente y a intervalos de tiempo configurables paquetes TCP con contenido identificatorio único (puede ser el nombre del grupo más un número incremental). En general se utiliza un script "server" y un script "cliente". Podés usar el lenguaje de programación que prefieras (librerías net, socket son buenos lugares para empezar).

    a) Probar el script entre dos computadoras, capturando tráfico y verificando que los paquetes estén transitando correctamente. Documentar con capturas de pantalla. Tomar un paquete aleatorio de la secuencia e identificar la carga útil del mismo.
    b) Agregar una feature al programa que permita loguear (persistir en un archivo) los paquetes enviados y recibidos, con una etiqueta de tiempo (timestamp) del momento en que fueron enviados/recibidos.
    c) Con la información anterior, para una secuencia de 100 paquetes, calcular la latencia promedio, máxima, mínima y el jitter de la conexión. Utilizar una frecuencia de envío de ~1 seg.

2) Desarrollar un script análogo al punto anterior, pero para protocolo UDP. Repetir los ítems a), b) y c).

3) Comparar un paquete UDP y un paquete TCP capturados, mostrar las diferencias y elaborar una tabla comparativa para las métricas obtenidas en el punto C.

4) Sobre encriptación:

a) Investigar y desarrollar brevemente las diferencias entre encriptado simétrico y asimétrico.
b) Investigar sobre librerías para encriptar mensajes, e implementar la que más te guste en los scripts que desarrollaste (encriptar la carga útil), podés usar cualquier tipo de encriptación que quieras: sobre la que elegiste, resumí las principales características.
c) Ejecutar los scripts, tomar un paquete aleatorio de la secuencia e identificar la carga útil del mismo. Mostrar que la misma se encuentra encriptada, comparando con las tramas obtenidas en los ítems 1)a) y 2)a)
d) ¿Cómo harías para encriptar la comunicación entre las dos computadoras si las mismas se encuentran a kilómetros de distancia y nunca intercambiaron información en el pasado ? Explicar conceptualmente cómo implementarías esto en tus scripts (pero no hace falta que lo programes).