Trabajo Práctico Final Integrador

Análisis de protocolos

La entrega y aprobación de este Trabajo Práctico es condición necesaria (pero no suficiente) para aprobar la asignatura (promocionar o rendir el final). Esta actividad es de resolución personal.

Este trabajo práctico final tiene como objetivo principal la integración de los contenidos teóricos de la asignatura con las habilidades prácticas adquiridas, aplicándolos a un caso de estudio real que puede ocurrir en su vida profesional. Usted recibe una captura de tráfico de red que corresponde a una transferencia que se realizó en un momento. Se encuentra formada por diferentes archivos que corresponden a segmentos de red distintos. Usted debe realizar el análisis que le permita completar las siguientes actividades. En su reporte final incluya las respuestas a cada una de las consignas de manera explícita, clara y ordenada.

Actividades

1. Reconstruya la topología de la red, indicando:
   - *a*) Dispositivos existentes y su función.
   - *b*) Direcciones de capa 2 y 3 de cada interface de cada uno.
2. Arme el gráfico de topología con una herramienta adecuada y asigne a cada segmento de red el identificador de las capturas correspondientes (nombre del archivo `.pcap`).
3. Resuelva las siguientes consignas:
   - *a*) Realice gráficos con las distribución de mensajes por capas (unificando datos de todas las capturas).
   - *b*) Identifique las conexiones TCP. Por cada una indique: dispositivo cliente, dispositivo servidor, finalidad, sockets de ambos (cliente y servidor).
   - *c*) Para la conexión TCP establecida entre el servidor proxy y el servidor `www.example.com` indique la finalidad de cada PDU intercambiada a nivel de transporte y aplicación.
   - *d*) Indique qué programa utilizó y qué es lo que ve en su pantalla el usuario que inició el intercambio de mensajes analizado.
   - *e*) ¿Cómo se logra la redirección desde `www.example.com` al contenido alojado en otro servidor? ¿Cuál es la alternativa recomendada para lograrlo?
   - *f*) ¿Cuáles son los servidores dns autorizados para los dominios `tyr.org` y `example.com` (dirección IP y nombre mnemónico)
   - *g*) Genere un diagrama de intercambio de mensajes en el tiempo que muestre de manera unificada cómo se sucedieron los mensajes, incluyendo TODOS los dispositivos involucrados en TODAS las capturas. Por cada mensaje identifique los principales parámetros que hacen a la función del mismo. No utilice ningún software de generación automática del gráfico. El análisis debe corresponder a su interpretación de lo sucedido.
   - *h*) Confeccione una tabla con los diferentes protocolos involucrados, cantidad de PDUs, total en headers y total en datos. De allí, calcule el *overhead*[1] total y por protocolo generado para lograr la transferencia. Grafique adecuadamente.

[1] $Overhead = \frac{Total\_Datos\_Control\_Tx}{Total\_Datos\_Tx}$