Universidad del Valle de Guatemala
Facultad de Ingeniería
Departamento de Ciencias de la Computación
CC3067 Redes

Laboratorio 6

Monitoreo de Paquetes

1 Antecedentes

El monitoreo y análisis de paquetes, segmentos, tramas, etc., es de suma importancia en las Redes de Computadoras. Mediante el monitoreo y estudio de los mismos, se puede tener una noción completa de lo que acontece en las transmisiones de información, así como también estar al tanto de procesos o eventos "sospechosos" o maliciosos. La herramienta Wireshark (o cualquier otro sniffer) nos permite observar todos los paquetes que viajan en la red en la que nos encontramos, así como explorar sus payloads y encabezados.

2 Objetivos

- Utilizar Wireshark para observar paquetes y su contenido.
- Experimentar y analizar con un flujo de datos mediante el protocolo TCP.
- Observar las diferencias, similitudes y ventajas de utilizar TLS y mecanismos de seguridad.

3 Desarrollo

Sigan las siguientes instrucciones, respondiendo a cada pregunta y discusión. **Evidencie sus respuestas y progreso:**

1. Abrir Wireshark
2. Navegar a http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html y descargar el archivo alice.txt, el cual contiene el texto de Alicia en el Pais de las Maravillas, de Lewis Caroll, en ASCII.
3. Elegir el archivo descargado para subirlo (browse), pero todavía no darle submit/upload.
4. Luego, comenzar captura paquetes en Wireshark (pueden filtrar por tcp para una mejor visibilidad)
5. Hacer submit/upload, esperar a que complete la subida. Podrá notar los paquetes siendo capturados por el sniffer.
6. Al completar la subida, detener la captura y analizar los paquetes y segmentos recibidos. Luego de observarlos y analizarlos responda:
    a. *¿Desde qué puerto estamos enviando el archivo?*
    b. *¿Hacia qué puerto estamos enviando el archivo, hacia qué IP?*
    c. Analicemos los paquetes IPv4 que enviamos/recibimos:
        i. *¿Se está utilizando alguna clase de Servicios Diferenciados (QoS)? ¿Cómo lo sabe?* Evidencie.
        ii. *¿La transmisión soporta ECN?* Evidencie.
        iii. *¿Cuál es el TTL de los paquetes?* Evidencie.

d. *¿Cual es el sequence number del segmento que lleva el HTTP POST?*
e. *¿Qué puede observar al ver el payload de los segmentos que llevan el texto de Alicia?*
f. *¿Encontró alguna retransmisión de paquetes? Si, si, ¿cómo se dio cuenta?* Evidencie.
g. Recordemos y repasemos sobre el protocolo TCP. *Describa en sus palabras que es un Cummulative Ack. ¿Encontró indicios de ello en la transmisión?* Evidencie.
h. Si navegamos en Wireshark a: Statistics > TCP Stream Graphs > Time Sequence Graph (Stevens), podremos ver una representación gráfica de los Sequence Numbers en el tiempo. *Discuta lo que observa, procurando mencionar sobre "Slow Start" y AIMD para Control de Congestión. Evidencie.*

7. Navegar hacia https://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html para repetir las pruebas. Observe que ahora el sitio es HTTP**S.**

8. …repetir el proceso de elegir archivo a subir (alice.txt), comenzar a capturar, submit/upload, esperar a que termine la subida y detener la captura de paquetes. Luego, analice lo capturado, y responda a lo siguiente:
   a. *¿Se observa alguna diferencia al inicio de la transmisión?*
   b. *¿Qué puerto estamos usando esta vez para la transmisión?*
   c. *¿Encontró alguna retransmisión de paquetes? si, si, ¿cómo se dio cuenta? Evidencie.*
   d. *¿Encontró indicios de cumulative ack en la transmisión? Muestre una captura que lo evidencie.*
   e. *¿Hacia qué IP y puerto estamos enviando el archivo? Observando el puerto receptor, ¿qué nota de extraño?*
   f. *¿Qué puede observar al ver el payload de los segmentos que llevan el texto de Alicia? ¿A qué se debe esto, considerando que es una página HTTPS?* (Tip: explore el código fuente HTTP de la página [click derecho inspeccionar elemento])
   g. Editar el código fuente de la página para solventar la causa. Repita la captura de paquetes y envío de archivo. Luego, observe lo capturado y responda:
      i. *¿Qué diferencia puede observar ahora al inicio de la conexión?*
      ii. *¿Qué puede observar ahora al ver el payload de los segmentos que llevan el texto de Alicia*?

4 Reporte

Realizar un reporte con el formato UVG, donde responda las preguntas mencionadas y donde adjunte su evidencia. Guardar las capturas de paquetes realizadas durante cada experimento (hacia HTTP, hacia HTTPS, hacia HTTPS corregido).

4.1 Rúbrica de evaluación

A. Documento PDF con respuesta a todas las preguntas y su debida evidencia (capturas, screenshots, etc.): 100% (4pts.)