Universidad del Valle de Guatemala

Facultad de Ingeniería

Laboratorio 6 - Informe

Redes

Mariana David 201055

Guatemala 26 de octubre del 2023

Introducción

El monitoreo y análisis de paquetes en las redes de computadoras son actividades cruciales para comprender el flujo de información, identificar eventos sospechosos o maliciosos, y evaluar el rendimiento de las comunicaciones. Wireshark, una herramienta de análisis de tráfico de red, permite examinar los paquetes y sus contenidos. En este informe, se describen los objetivos, el desarrollo y las conclusiones de un experimento que involucra el uso de Wireshark para analizar la transmisión de un archivo de texto a través de los protocolos TCP y TLS en un entorno de red.

Objetivos

Los objetivos de este laboratorio son los siguientes:

1. Utilizar Wireshark para observar paquetes y su contenido en una transmisión de datos.
2. Experimentar y analizar un flujo de datos a través del protocolo TCP.
3. Observar las diferencias, similitudes y ventajas de utilizar TLS y mecanismos de seguridad en la transmisión de datos.

Cuerpo/Desarrollo

El desarrollo del experimento se dividió en varias etapas que implican la utilización de Wireshark para capturar y analizar el tráfico de red. A continuación, se resumen las principales observaciones y resultados. Se abrió Wireshark y se comenzó a capturar paquetes de una transmisión de un archivo. Como segunda instancia, se descargó el archivo "alice.txt" desde http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html. Continuamente, se eligió el archivo descargado para subirlo, pero aún no se completó la subida. Después, se inició la captura de paquetes en Wireshark, filtrando por el protocolo TCP para una mejor visibilidad. Se completó la subida del archivo y se detuvo la captura de paquetes.

Durante este proceso es posible resolver las siguientes preguntas:

a. ¿Desde qué puerto estamos enviando el archivo?

- 5131

b. ¿Hacia qué puerto estamos enviando el archivo y hacia qué IP?

- Puerto de destino: 80
- IP de destino: 192.168.5.206

c. Análisis de los paquetes IPv4:

i. ¿Se está utilizando alguna clase de Servicios Diferenciados (QoS)?

- Si al usar el campo Differientated Services Codepoint (DSCP

ii. ¿La transmisión soporta ECN?

- Se observa el campo Explicit Congestion Notification (ECN).

iii. ¿Cuál es el TTL de los paquetes?

- Es variante

d. ¿Cuál es el número de secuencia del segmento que lleva el HTTP POST?

- 1

e. ¿Qué se puede observar al ver el payload de los segmentos que llevan el texto de Alicia?

- Los segmentos contienen texto legible.

f. ¿Se encontró alguna retransmisión de paquetes?

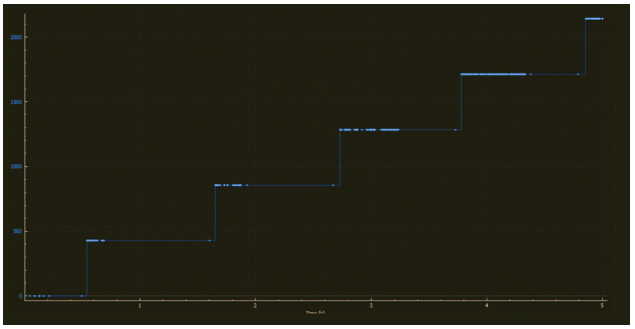
- Sí

g. Descripción de un Cumulative Ack (ACK acumulativo) y evidencia de su uso en la transmisión.

- Mecanismo en el protocolo TCP que implica la confirmación de múltiples paquetes como recibidos mediante un solo ACK.

h. Análisis del gráfico de Sequence Numbers en el tiempo y discusión sobre "Slow Start" y AIMD.

- El gráfico ilustra un patrón de evolución en los Sequence Numbers que es típico del inicio gradual, conocido como "Slow Start", con un incremento exponencial en la velocidad de transmisión al principio. Posteriormente, se aprecia un aumento más moderado en la tasa de transferencia y una disminución cuando se detectan pérdidas de paquetes, lo que indica la posible implementación de AIMD (Additive Increase, Multiplicative Decrease), un enfoque para el control de congestión.



Repitiendo el procedimiento

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

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:

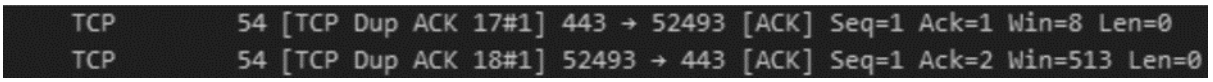
a. ¿Se observa alguna diferencia al inicio de la transmisión?

- El nuevo puerto de salida es 52463

b. ¿Qué puerto estamos usando esta vez para la transmisión?

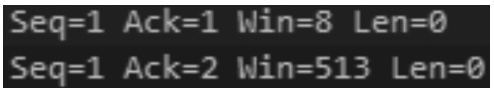
- 80

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.

- Sí



e. ¿Hacia qué IP y puerto estamos enviando el archivo? Observando el puerto receptor,
¿qué nota de extraño?

- IP 192.168.5.206
- PORT 443
- Lo extraño es que se convierten a los mismos de antes

f. ¿Qué puede observar al ver el payload de los segmentos que llevan el texto de Alicia?

- Son pecuniaries
- Contiene más legibilidad

¿A qué se debe esto, considerando que es una página HTTPS? (Tip: explore el código
fuente HTTP de la página [click derecho inspeccionar elemento])
Lo más notable del payload de los segmentos que llevan texto a Alicia es que la estructura del mismo es más ordenada, por lo que es más legible y provee más información.

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?

- El puerto de llegada continua siendo el mismo y la IP de la fuente y del destino son diferentes

ii. ¿Qué puede observar ahora al ver el payload de los segmentos que llevan el texto de Alicia?

- El resultado del payload es menor

Conclusiones

En conclusión, este laboratorio permite comprender la importancia del monitoreo de paquetes en las redes y cómo Wireshark puede utilizarse para analizar el tráfico. Se observaron diferencias en la transmisión de datos a través de los protocolos TCP y TLS. Se identificaron características como el uso de QoS, ECN, el número de secuencia, la presencia de retransmisiones y el comportamiento de control de congestión.

Al repetir el laboratorio con HTTPS, se notaron cambios en los puertos y en la legibilidad del payload. La edición del código fuente de la página permitió corregir estos aspectos y mejoró la transmisión. Este experimento brindó una valiosa experiencia en la comprensión de los aspectos técnicos de las comunicaciones en red.