|  |  |  |
| --- | --- | --- |
|  | Universidad del Valle de Guatemala Facultad de Ingeniería  Departamento de Ciencias de la Computación CC3067 - Redes | **Laboratorio #1 – Esquemas de comunicación e Introducción a**  **Wireshark**  Semestre II - 2025 |

**Reporte**

Nombre: Brandon Reyes Morales

Carné: 22992

## Segunda parte: Introducción a Wireshark

Se debe descargar e instalar el software de Wireshark. Es probable que para ejecutarlo pida permisos de administrador (sudo, click + run as admin, etc.).

### Personalización del entorno

En la primera parte se realizará la personalización del entorno de Wireshark, de modo que se adapte a nuestras preferencias de uso.

* + 1. Inicie Wireshark
    2. Cree un perfil con su primer nombre y primer apellido (edit -> configuration profile)
       1. Captura de pantalla de un celular

          El contenido generado por IA puede ser incorrecto.
    3. Descargue el archivo [https://www.cloudshark.org/captures/e6fb36096dbb](http://www.cloudshark.org/captures/e6fb36096dbb) (Export -> Download)
       1. Interfaz de usuario gráfica, Aplicación

          El contenido generado por IA puede ser incorrecto.
    4. Abra el archivo descargado, el archivo contiene transmisiones capturadas, y existen diversas columnas que representan la data.
       1. Captura de pantalla de computadora

          El contenido generado por IA puede ser incorrecto.
    5. Aplique el formato de tiempo Time of Day (view -> Time Display Format)
       1. Captura de pantalla de computadora

          El contenido generado por IA puede ser incorrecto.
    6. Agregue una columna con la longitud del protocolo (preferences -> column -> +)
       1. Captura de pantalla de computadora

          El contenido generado por IA puede ser incorrecto.
       2. Captura de pantalla de computadora

          El contenido generado por IA puede ser incorrecto.
    7. Elimine u oculte la columna Longitud (click derecho -> desmarcar columna)
       1. Una captura de pantalla de una computadora

          El contenido generado por IA puede ser incorrecto.
    8. Aplique un esquema de paneles que sea de su preferencia (que no sea el esquema por defecto) (preferences -> Layout)
       1. Captura de pantalla de computadora

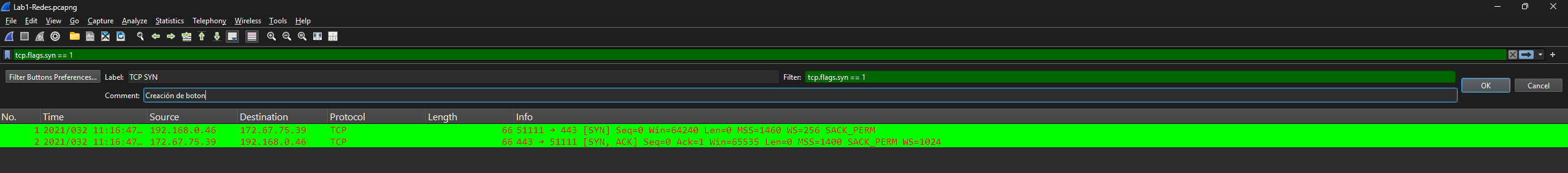
          El contenido generado por IA puede ser incorrecto.
    9. Aplique una regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia. (View -> coloring rules -> +)

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

* + 1. Cree un botón que aplique un filtro para paquetes TCP con la bandera SYN igual a 1. (esquina superior derecha -> +)
       1. 
    2. Oculte las interfaces virtuales (en caso aplique: capture -> options)

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Se debe realizar tomas de pantalla que muestren el entorno final personalizado, el nombre del perfil y el uso de las regla de color y botón del filtro, así como la lista simplificada de las interfaces de captura.

### Configuración de la captura de paquetes

En la segunda parte, se realizará una captura de paquetes con un ring buffer.

* + 1. Abra una terminal y ejecute el comando ifconfig/ipconfig (dependiendo de su OS). Detalle y explique lo observado, investigue (i.e.: ‘man ifconfig’, documentación) de ser necesario.
       1. Texto

          El contenido generado por IA puede ser incorrecto.
       2. Texto

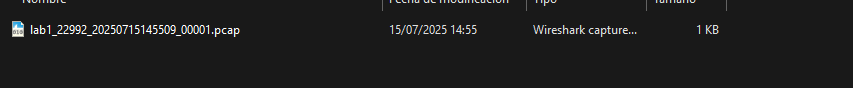
          El contenido generado por IA puede ser incorrecto.
       3. Interfaz seleccionada: Wi‑Fi – MediaTek Wi‑Fi 6 MT7921
       4. IPv4 192.168.0.9 – dirección asignada dinámicamente por el router doméstico.
       5. Máscara 255.255.255.0 – red /24; permite 254 hosts (192.168.0.1‑254).
       6. Puerta de enlace 192.168.0.1 – IP del router; dirige el tráfico a Internet.
       7. DHCP 192.168.0.1 – mismo router actúa como servidor DHCP.
       8. MAC F0‑A6‑54‑C0‑8E‑AD – identificador único de la tarjeta Wi‑Fi.
       9. Estado: conectada; será la interfaz desde la que generaré y capturaré tráfico real.
       10. Las demás interfaces (Ethernet, Bluetooth, Virtual Adapters) están desconectadas o son virtuales, por lo que fueron deshabilitadas en Wireshark para evitar ruido en la captura.
    2. Luego, retornando a Wireshark, desactive las interfaces virtuales o que no aplique.
    3. Realice una captura de paquetes con la interfaz de Ethernet o WiFi con una configuración de ring buffer, con un tamaño de 5 MB por archivo y un número máximo de 10 archivos (puede hacerlo por medio de la interfaz de usuario o por medio de comandos) Genere tráfico para que los archivos se creen. Defina el nombre de los archivos de la siguiente forma: lab1\_carnet.pgcap (options -> capture -> output)
       1. Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

          El contenido generado por IA puede ser incorrecto.

Se debe realizar tomas de pantalla de la configuración o comandos para la creación del ring buffer, así como los archivos generados.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.



### Análisis de paquetes

En la tercera parte se analizará el protocolo HTTP. Debe realizar tomas de pantalla que validen sus respuestas.

* + 1. Abra su navegador, inicie una captura de paquetes en Wireshark (sin filtro) en la interfaz y acceda a la siguiente direccion: [http://gaia.cs.umass.edu/wireshark- labs/INTRO-wireshark-file1.html](http://gaia.cs.umass.edu/wireshark-%20labs/INTRO-wireshark-file1.html)
       1. Interfaz de usuario gráfica

          El contenido generado por IA puede ser incorrecto.
    2. Detenga la captura de paquetes (si desea realizar una nueva captura de la página deberá borrar el caché de su navegador, de lo contrario no se realizará la captura del protocolo HTTP).
       1. Interfaz de usuario gráfica, Texto

          El contenido generado por IA puede ser incorrecto.
    3. Responda las siguientes preguntas:
       1. ¿Qué versión de HTTP está ejecutando su navegador?
          - HTTP/1.1
          - Captura de pantalla de computadora

            El contenido generado por IA puede ser incorrecto.
       2. ¿Qué versión de HTTP está ejecutando el servidor?
          - HTTP/1.1 200 OK
       3. ¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?
          - En la cabecera Accept-Language se indica que el navegador acepta los siguientes idiomas:

en-US

en

es

* + - 1. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
         * El servidor devolvió 393 bytes de contenido, según el campo Content-Length en el paquete de respuesta HTTP.
      2. En el caso que haya un problema de rendimiento mientras se descarga la página,

¿en que elementos de la red convendría “escuchar” los paquetes? ¿Es conveniente instalar Wireshark en el servidor? Justifique.

En caso de presentarse problemas de rendimiento al descargar una página, lo ideal es capturar los paquetes en puntos clave de la red como un switch con port mirroring, un firewall o un router, ya que estos permiten observar todo el tráfico entre cliente y servidor. No es recomendable instalar Wireshark directamente en el servidor de producción, pues puede afectar su rendimiento, comprometer la seguridad y violar políticas de TI.

Discusión sobre la actividad

Durante este laboratorio exploré dos aspectos esenciales: la configuración personalizada de Wireshark y el análisis de tráfico HTTP. En la primera parte, aprendí a crear perfiles, columnas personalizadas (frame.len), esquemas de paneles y filtros de color para destacar paquetes SYN TCP, lo cual mejoró mucho la visualización y comprensión del tráfico. En la segunda parte, capturé tráfico real visitando un sitio de laboratorio; identifiqué la versión HTTP (1.1) en ambas direcciones, revisé encabezados como Accept-Language y el Content-Length, y comprendí cómo se intercambia la información entre cliente y servidor. El uso del modo ring buffer me permitió gestionar automáticamente archivos de captura sin llenar el disco, lo cual me pareció muy útil para sesiones prolongadas.

Comentarios:

* Wireshark demostró ser una herramienta robusta y completa. Su interfaz facilita el aprendizaje, aunque requiere tiempo y paciencia para encontrar opciones rebuscadas.
* El rendimiento puede verse afectado en equipos con mucha carga de tráfico si se captura sin filtros, y la interfaz podría resultar compleja para principiantes.

Conclusiones

* En la parte práctica, pude capturar y analizar las solicitudes y respuestas HTTP, identificando correctamente versiones, idiomas aceptados y tamaño del contenido.
* Además, comprendí las implicaciones de monitoreo de red, especialmente por qué no es conveniente instalar Wireshark en servidores de producción y cómo usarlo responsablemente desde puntos de captura adecuados.

Referencias utilizadas

* Ryufath Soepeno, Wireshark: An Effective Tool for Network Analysis, ResearchGate – utilidad en seguridad y análisis de protocolosm <https://www.researchgate.net/publication/374675769_Wireshark_An_Effective_Tool_for_Network_Analysis?utm_source=chatgpt.com>
* Sanchit Gurukul, Advantages, Disadvantages, and Use Cases, resumen de ventajas y limitaciones de Wireshark <https://sanchitgurukul.com/exploring-wireshark-tool/?utm_source=chatgpt.com>
* What is Wireshark? Applications, Features & How It Works, KnowledgeHut – impacto en el rendimiento y desventajas <https://www.knowledgehut.com/blog/security/what-is-wireshark?utm_source=chatgpt.com>

