Laboratorio 9. HTTP y DNS.

Objetivos:

- Estudio del protocolo HTTP. Examen de algunos de los campos de la cabecera HTTP.
- Estudio de las consultas al DNS.

Realización:

- De la práctica anterior se conoce el manejo básico de la herramienta Wireshark.
- El alumno habrá leído el enunciado antes de realizar la práctica y habrá repasado los conceptos expuestos en la teoría sobre HTTP y DNS. Debe haber leído también el siguiente artículo de la Wikipedia: https://es.wikipedia.org/wiki/Favicon
- La duración estimada de la práctica es de una hora y cuarto. Las instrucciones de la práctica se proporcionan para su realización en alguno de los laboratorios del DIT. La última tarea de la práctica depende de información específica de cada grupo, de modo que debe utilizar información disponible en la tarea de entrega de su grupo en moodle.

Recursos:

- PC+Linux con configuración de red operativa y el software Wireshark instalado.
- **Se debe usar el navegador FIREFOX para hacer la práctica.**

Resultados:

- En el portal moodle se proporciona un formulario en el que se pide incluir determinados resultados pedidos en el enunciado (los que aparecen subrayados). Debe subir a moodle un fichero ZIP que incluya el formulario con los resultados pedidos, así como los ficheros de captura de pantalla que se piden en las tareas 3, 4 y 5. En la tarea de entrega se indican los detalles de la subida de resultados.
- En el formulario de entrega aparecen menos cuestiones que en este enunciado. Sin embargo, debe ser capaz de responder todas las cuestiones del enunciado, pues dichas cuestiones también pueden aparecer en los exámenes.

Estudio básico del protocolo HTTP.

- **Tarea 1. Arranque del analizador e inicio de la captura de tráfico.**
  - Arranque el navegador Firefox (se pide que se haga antes de iniciar la captura con Wireshark para evitar capturar el tráfico de la página de inicio).
  - Vacíe la caché de su navegador, para eliminar posibles copias de los ficheros descargados si ha accedido antes a la página que se cita en esta tarea. Para ello, en su navegador abra el menú de Preferencias, seleccione el apartado de Privacidad & Seguridad y en el apartado de Historial borre el historial completo marcando previamente todas las casillas que aparezcan.
  - Arranque el analizador Wireshark (en el menú de Aplicaciones→Laboratorios docentes del DIT). Cierre las ventanas de error iniciales que puedan aparecer.
  - En la ventana del analizador, a la izquierda, aparece una lista de "conexiones de red" de las que puede capturar. Para arrancar la captura, pique con el ratón sobre la interfaz de red de su ordenador (como ya hizo en la práctica anterior).

- **Tarea 2. Generación de tráfico y su captura.**
  - Acceda con el navegador a la página de dirección
    `http://www.dit.upm.es/~ftel/lab9.php`

- Cuando la página se haya mostrado, detenga la captura de tráfico en el analizador pulsando el icono con un botón de un cuadrado rojo, en la parte superior. No cierre el navegador.
- Aplique un filtro de presentación para mostrar sólo el tráfico HTTP de interés para la práctica. Para ello, escriba lo siguiente en el espacio junto a "Filter" y pulse "Apply":
  `http and (ip.addr == 138.4.2.56 or ip.addr == 138.100.200.6)`

- **Tarea 3. Estudio de las peticiones HTTP. En la captura realizada se van a estudiar las peticiones HTTP que se realizan.**
  - Para cada una de las peticiones GET que realiza su navegador, escriba cuál es el recurso que se está solicitando y la dirección IP del servidor.
    NOTA IMPORTANTE: si no observa **cuatro** peticiones GET, es posiblemente porque ya había cargado la página web en alguna ocasión anterior antes de hacer la captura. En ese caso salga **completamente** del navegador Firefox (**no puede quedar ninguna ventana abierta del navegador**) y vuelva a lanzarlo. Vacíe la caché del navegador como se ha indicado antes. Si tenía alguna captura lanzada con Wireshark, deténgala y arránquela de nuevo. Sólo entonces acceda a la página web indicada en esta tarea.
  - En el panel superior de Wireshark seleccione el paquete que realiza la petición GET correspondiente al recurso lab9.php. Vaya ahora al panel intermedio de Wireshark y expanda la cabecera de transporte. ¿Qué protocolo de transporte se usa? ¿Cuál es el puerto destino?
  - Expanda ahora el análisis del protocolo de aplicación. Observe que en la cabecera HTTP aparecen diversos campos que describen aspectos relacionados con la petición. Identifique:
    - Versión del protocolo que usa el navegador (HTTP1.0 o HTTP1.1).
    - ¿Cuál es la identificación del navegador que realiza la petición? ¿Cuál es el nombre de la línea de cabecera en la que va?
    - ¿Cuál es el nombre de la línea de cabecera que identifica la máquina a la que se hace la petición?
    - ¿Cuáles son los idiomas en los que se prefiere recibir la información que envíe el servidor? ¿Cuál es el nombre de la línea de cabecera donde se indican?
    - ¿Cuál es el nombre de la línea de cabecera donde se indica que el navegador puede aceptar texto HTML como contenido?
  - Haga una captura de pantalla en la que se muestre el panel intermedio del analizador y se vea dicha información. Guarde la captura en un fichero de nombre **`tarea3.png`**.
  - En el navegador Firefox pulse, con el botón derecho del ratón, sobre la página. En el menú que aparece seleccione "Ver código fuente de la página". A la vista del código mostrado y de lo que habrá leído en el artículo de la Wikipedia indicado al principio del enunciado, responda las siguientes cuestiones:
  - Explique por qué se realizan cuatro peticiones GET al servidor.
  - Indique las URL **completas** (http://...) que corresponden a cada uno de los cuatro recursos solicitados en las peticiones GET.
  - Concretamente, para la petición correspondiente al logotipo de FTEL, explique cómo ha deducido la URL completa observando el código fuente de la página. Explique también cómo se puede deducir dicha información observando el detalle de la petición GET correspondiente en el analizador Wireshark.

- **Tarea 4. Estudio de las respuestas a la petición HTTP.** Examine ahora el detalle de los paquetes que corresponden a las respuestas del servidor. Concretamente, identifique, **para la respuesta que corresponde al logotipo de la UPM:**
  - Dirección IP del servidor que responde.
  - Código de estado retornado en la respuesta.
  - Información acerca del tipo de servidor web que responde (Netscape, Apache, etc.), y nombre de la línea de la cabecera que la proporciona.
  - Formato del contenido descargado y nombre de la línea de cabecera donde aparece.
  - Tamaño del fichero del logotipo y dónde ha encontrado dicha información (que debe haberse obtenido usando Wireshark).
  - Haga una captura de pantalla en la que se muestre el panel intermedio del analizador y se observe la información anterior. Guarde la captura en un fichero de nombre **`tarea4.1.png`**.

- Vuelva a arrancar la captura de Wireshark. Cargue de nuevo la página web de la práctica (símbolo junto a cuadro de texto con la URL de la página). Una vez recargada, detenga la captura y examine en el analizador la petición GET que se refiere al logotipo de FTEL. ¿Aparece la línea de cabecera If-Modified-Since? En caso afirmativo, ¿cuál es el objetivo de incluir dicha línea en la petición?
- Examine las respuestas a las peticiones de las imágenes. ¿Qué código de estado aparece en ellas? ¿Qué significa eso para el navegador que recibe las respuestas?
- Haga una captura de pantalla en la que se muestre en el panel superior las peticiones GET y las respuestas correspondientes. Guárdela en un fichero de nombre **`tarea4.2.png`**.

Estudio básico de las consultas al DNS.

- **Tarea 5. Estudio de las peticiones y respuestas DNS.**
  - En una ventana de terminal dé la siguiente orden: **`sudo /usr/sbin/nscd -i hosts`**
  - En el navegador Firefox abra una nueva pestaña y teclee la siguiente URL en el cuadro de texto de introducción de la página a visitar: **`about:config`**
    Le aparecerá un aviso y pulse en el botón **`¡Acepto el riesgo!`**
    En la parte superior de la ventana que se muestra aparece un cuadro de Búsqueda. En ese cuadro teclee **`network.dnsCacheExpiration`**
    En la ventana de resultado entre otros debe aparecer una línea con el siguiente aspecto:
    `network.dnsCacheExpiration  default  integer  60`

    Haga doble click con el ratón sobre esta línea y aparecerá una ventana donde nos permite cambiar el valor 60. Tecleamos el valor 0 y pulsamos OK. Con esto se debe haber borrado el cache del dns del Firefox.
    Al pulsar OK vuelve a aparecer la misma línea de antes, pero ahora con el siguiente aspecto
    `network.dnsCacheExpiration  default  integer  0`

    Para volver a dejar el navegador en el mismo estado seleccionamos de nuevo la línea, escribimos 60 en la ventana, pulsamos OK y debe aparecer la línea con los valores originales:
    `network.dnsCacheExpiration  default  integer  60`

  - Arranque una captura de tráfico con Wireshark. En su navegador, vuelva a cargar la página **`http://www.dit.upm.es/~ftel/lab9.php`** (debe forzar que se vuelve a pedir la página al servidor pulsando con el ratón sobre el símbolo de "recarga" que hay cerca del cuadro de texto de la dirección web visitada).
  - Detenga la captura de Wireshark. En el cuadro de texto del filtro de presentación escriba el siguiente filtro y pulse el botón "Apply" una vez escrito:

    ```
    (dns.qry.name == www.dit.upm.es or dns.qry.name == www.upm.es) or
    (http and (ip.addr == 138.4.2.56 or ip.addr == 138.100.200.6))
    ```

  - En el panel intermedio de Wireshark observe el análisis del protocolo de transporte de una petición DNS (la dirección IP origen debe ser la de su ordenador). ¿Qué protocolo de transporte se usa? ¿Cuál es el puerto destino?
  - Estudie ahora el protocolo de aplicación. Expanda la línea "Queries". ¿Por qué tipo de registro DNS se pregunta? ¿Qué información se quiere obtener con dichas peticiones?
  - Estudie ahora las respuestas que le llegan. Expanda la línea "Answers" si es necesario. ¿Cuál es la dirección IP de la máquina que responde? ¿Qué función realiza dicha máquina? ¿Qué información proporcionan las respuestas? ¿Qué relación tiene esa información con las comunicaciones HTTP de los apartados anteriores?
  - Haga una captura de pantalla en la que se vea el panel intermedio del analizador y se observe la información de una respuesta. Guarde la captura en un fichero de nombre **`tarea5.png`**.

- **Tarea 6. Realización de consultas iterativas al DNS.** Se va a usar la herramienta "dig" para estudiar el tipo de consultas que realiza un servidor de DNS al que le llega una petición de un cliente para resolver un nombre que no es de su dominio. En las distribuciones de Linux suele estar disponible. Existen también sitios web que ofrecen acceso a dicha herramienta, y en la práctica se usará este procedimiento, ya que el cortafuegos del laboratorio prohíbe las consultas a servidores externos. En la tarea de entrega de su grupo se indicarán los nombres de **dos sitios web a estudiar**.
    - En el navegador, vaya a la dirección http://www.digwebinterface.com/ . **Para cada uno** de los sitios web indicados, realice los puntos que siguen.
        - En el cuadro de texto "Hostnames or IP addresses", escriba el nombre DNS del servidor web. En la columna "Options", marque la opción "trace". Pulse el botón "Dig".
        - Incluya en el formulario de la práctica la salida de la orden anterior.
        - Indique cuál es la dirección IP del servidor web buscado.
        - ¿El nombre del servidor web es un “alias”? ¿Por qué?
    - Describa los pasos que se siguen para obtener la dirección de un servidor DNS autoritativo del dominio del **primero** de los servidores correspondientes a su grupo.