Protocolos e Interfaces de Comunicación
Grado en Ingeniería Telemática
E.T.S.I. Telecomunicación
Curso 2021/2022

Práctica 1. Revisión de protocolos TCP/IP con Wireshark.

Se sugiere entregar una memoria respondiendo a las siguientes preguntas.

1. **Ejercicio 1. Realiza una captura del tráfico al entrar en www.uma.es**
    a. Señala al menos 3 protocolos diferentes que puedas observar en la captura.
    b. ¿Cuánto tiempo transcurre desde que se envía el primer HTTP GET hasta que se recibe el primer HTTP OK? *[recomendación: usar filtros y referencias de tiempo]*
    c. ¿Cuál es la IP de www.uma.es? ¿Y la de tu ordenador?
    d. ¿Cuántos mensajes HTTP GET ha enviado tu navegador?
    e. Imprime en un archivo de texto la información del primer paquete HTTP GET y HTTP OK. ¿Cuáles son las principales diferencias y similitudes que ves entre ellos?
        - ¿Cuál es la versión de HTTP que utiliza tu navegador? ¿y el servidor?
        - ¿Cuál es el código de HTTP GET? ¿Y el de HTTP OK? ¿Qué tipos de código utiliza HTTP? ¿Por qué el famoso error 404 empieza por 4?
        - ¿Cuándo fue modificado por última vez el documento que estás recibiendo?
2. **Ejercicio 2. Traza *Ping_1* y *Ping_2*.**
    a. Abre la primera traza. ¿Cuál es la dirección IP de "tu dispositivo"? ¿Y la del destino? Razona por qué has seleccionado una IP como el origen y la otra como el destino, y no al revés.
    b. Examina uno de los REQUEST de ping enviados. ¿Cuáles son el tipo de ICMP y el código? ¿Qué significa? ¿Qué otros campos tiene el paquete ICMP? ¿Cuántos bytes ocupa el checksum?
    c. Examina un paquete de respuesta de ping. ¿Cuáles son las diferencias encontradas con el anterior?
    d. Abre la segunda traza. Examina un mensaje de error y comenta cuáles son las diferencias con los paquetes anteriores.
    e. ¿Qué ocurre al final de la captura?
3. **Ejercicio 3. Traza *TCP_1*.**
    a. ¿Cuáles son los puertos de origen y de destino?
    b. ¿Cuáles son los flags de los tres primeros paquetes TCP (paquetes de establecimiento de conexión)? ¿Cuáles son los números de secuencia y de ACK de cada uno? Atiende a cómo evolucionan.
    c. ¿Qué paquete TCP corresponde al comando HTTP POST? *[recomendación: mirar en los datos en bruto de los paquetes]*
    d. En el paquete nº 5: ¿Cuál es la longitud del paquete capturado? ¿Cuál es la longitud del paquete IP (con cabecera)? ¿Cuál es la longitud del paquete TCP (sin cabecera)?
    e. ¿Qué está ocurriendo en esta captura? *[recomendación: usar la herramienta "follow" de Wireshark]*
4. **Ejercicio 4. Traza UDP_1.**
    a. ¿Cuántos campos hay en la cabecera UDP?
    b. A qué se refiere el valor "length" en este caso.
    c. ¿Cuál es el tamaño más grande posible de puerto?
    d. ¿En qué nivel de la pila se encuentra el protocolo UDP en la captura*?*
    e. ¿Qué es SNMP? Buscar para qué se utiliza.