Boletín SAD: Sniffers: Wireshark y tcpdump - práctica

1. FILTROS DE VISUALIZACIÓN: Usando Wireshark y en base a la captura boletin_sad_22_23.pcap (max.4,5 ptos)
   a. Indica el filter string para ver todas las tramas ethernet donde intervenga 00:16:3c:f1:fd:6d

   b. Indica el filter string para visualizar las tramas ethernet intercambiadas entre 0a:96:70:63:b7:82 y c8:53:4f:50:b0:c0

   c. Indica el filter string para ver todos las datagramas IP donde no intervenga 89.248.163.155

   d. Indica el filter string para ver los datagramas IP intercambiadas entre 172.70.131.42 y 198.71.247.91

   e. Indica el filter string para ver los mensajes ICMP de tipo Destino Inalcanzable por puerto inalcanzable.

   f. Indica el filter string para ver todos los mensajes ICMP de tipo Echo Request enviados desde 3.231.31.10 hacia 198.71.247.91

   g. Indica el filter string para ver los mensajes destinados al puerto tcp 80 de la máquina 198.71.247.91

   h. Indica el filter string para ver los mensajes http que contengan la palabra “jndi”.

   i. Indica el filter string para ver los mensajes con destino el puerto por defecto de SNMP.

   j. Instala y activa las librerías necesarias para tener Geolocalización en Wireshark e indica el filter string para ver únicamente los paquetes enviados desde China. y saca una foto donde se vea un paquete procedente de China con los campos de geolocalización visibles. Guárdala como *tunombre*_china.png

2. GRÁFICOS: En base a la captura boletin_sad_22_23.pcap haz un único gráfico donde:
   - Se vea la evolución temporal de todo el tráfico (estilo línea).
   - Además se vea superpuesta la contribución del tráfico HTTP (estilo línea)
   - Además se vea el tráfico asociado al equipo 3.231.31.10 (estilo bar).

   Haz una foto de toda la ventana del gráfico y guárdala como *tunombre*_grafico-ev1.png (max. 0,5 ptos)

3. ESTADISTICAS:En base a la captura boletin_sad_22_23.pcap responde:
   a. ¿Qué tanto por ciento del total de paquetes de la captura supone el tráfico ICMP? Indica el nº y qué opción del programa usaste para verlo. (max. 0,25 ptos)

   b. Recupera de la captura el archivo robots.txt pedido a pay2u.dev, guárdalo como *tunombre*_robots.txt e indica los pasos que sigues para hacerlo. (max. 0,25 ptos)

4. FILTROS DE CAPTURA (max. 4,3 ptos) Indica el filtro de captura para:
   a. Capturar únicamente las tramas ethernet con destino la pasarela predeterminada de tu red. (max. 0,7 ptos)

   b. Capturar comunicaciones https con www.xunta.gal (max. 0,7ptos)

   c. Capturar únicamente, los datagramas IP desde/hacia tu equipo con puerto destino tcp 443 (max. 0,7 ptos)

   d. Capturar mensajes ICMP Echo Reply intercambiados entre tu equipo y 8.8.8.8. (max. 0,7 ptos)

   ++++++++++ Usando la sintaxis avanzada ++++++++++

   e. Capturar mensajes tcp con destino algún puerto bien conocido. (max. 0,85 ptos)

   f. Capturar todos los mensajes TCP con los bits FIN y ACK a 1 en los flags. (max. 0,85 ptos)