Laboratorio 2 - Seguridad TI

Sebastián Dinator, Cristóbal Quijanes

Septiembre 2023

1. Wireshark

Wireshark es un poderoso programa que nos permite analizar protocolos y realizar ana´lisis en redes. Viene instalado por defecto en Kali Linux.

1.1. Descargue el archivo lab 1.pcap desde WebC, ábralo con Wireshark y responda las siguientes preguntas:

(A) ¿Cuál es. la dirección IP del Servidor y la del Cliente?

- Servidor: 10.2.0.1
- Cliente: 10.2.0.2

(B) ¿Cuál es la MAC address y Fabricante de la NIC del Servidor y de la NIC del Cliente?

- Servidor: NIC=Runtop_e1:5a:80 MAC= (00:20:78:e1:5a:80)
- Cliente: NIC=Lite-OnU_30:c8:db MAC= (00:a0:cc:30:c8:db)

(C) ¿Qué puerto TCP está usando el servidor y cuál el cliente?

- Servidor: 21
- Cliente: 1054

(D) ¿Qué acción representan los paquetes 1, 2 y 3 de la captura? ¿Fue esta acción exitosa?

- Representan la conexión entre el Cliente y el Servidor, esta fue exitosa, lo cual se comprueba al existir conversación entre ambas entidades.

(E) Indique Nombre y versión del software servidor.

- Scott's FTP Server 220-BisonWare BisonFTP server product V3.5

(F) Indique el nombre de usuario y password utilizados en este servicio.

- Usuario: fred
- Password: krueger

1.2. Descargue el archivo lab 2.pcap desde WebC, ábralo con Wireshark y responda

las siguientes preguntas:

(A) ¿Cuál es la dirección IP del Servidor y la del Cliente?

- Servidor: 128.121.136.217
- Cliente: 67.180.72.76

(B) ¿Cuál es la MAC address y Fabricante de la NIC del Servidor y de la NIC del Cliente?

- Servidor: NIC= Cadant_22:a5:82 MAC= (00:01:5c:22:a5:82)
- Cliente: NIC= QuantaCo_a9:08:20 MAC= (00:16:36:a9:08:20)

(C) ¿Qué puerto TCP está usando el servidor y cuál el cliente?

- Servidor: 21/30012
- Cliente: 4075/4076/4071/4072

(D) Recupere el archivo que está siendo transferido, ¿Quién aparece en la imagen?

- En la imagen aparece el equipo de Microsoft del año 1978, destacando que abajo a la izquierda con camiza azul se encuentra Bill Gates.

1.3. Descargue el archivo lab 3.pcap desde WebC, ábralo con Wireshark y responda las siguientes preguntas:

(A) ¿Cuantas conversaciones telefónicas existen en esta captura?

- Existen 3 conversaciones telefónicas.

(B) Escuche la primera de ellas y registre los números que son dictados en ella.

- 0514540005

(C) Filtre los paquetes SIP, ¿Cuántos paquetes quedaron?

- 14 paquetes

(D) ¿Qué versión de IP se está utilizando en estos paquetes?

- IPv4

(E) ¿Que TTLs se utilizan estos paquetes? ¿Por qué?

- TTLs: 255, 128
- Se utilizan los TTL como medida se seguridad, pues esto define la capacidad de enrutamiento de un paquete, generando que este no circule indefinidamente por la red. De igual forma permite generar diagnosticos de problemas de red, pues en caso que el paquete no llegue a destino te permite identificar el origen del problema.

(F) ¿Qué protocolo de transporte está en uso? ¿Por qué?

- UDP
- Se utiliza debido a que al ser un protocolo menos sobrecargado que TCP y no exigir garantias respecto a la entrega de los datos permite una mayor velocidad en la transferencia de paquetes y una latencia mínima.

Entregue sus respuestas formalmente en un archivo PDF indicando el nombre de sus integrantes, que deberá subir a WebC antes de la hora límite.

Formato de entrega: SDinator_CQuijanes_Lab2.pdf