Ayudantía 3 - Seguridad TI

Sebastián Dinator, Cristóbal Quijanes

Septiembre 2023

1. Wireshark

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

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

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

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

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

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

(E) Indique Nombre y versión del software servidor.

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

1.2. Descargue el archivo 2.pcap desde WebC, ábralo con Wireshark y responda las siguientes preguntas:

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

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

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

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

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

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

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

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

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

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

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