Reflexión individual - E1. Actividad Integradora 1

Josue Eduardo Sosa Martinez - A01411984:

Como sabemos la problemática se basa en las transmisiones de datos comprometidas, un problema que afecta a muchos usuarios comprometiendo sus datos personales. El código que realizamos ayuda a poder identificar las amenazas que están dentro de los otros archivos, funciona con secuencias específicas de bits peligrosos que se encuentren dentro de la transmisión, también detecta patrones como los palíndromos y analizamos las similitudes entre las transmisiones sospechosas. Estas acciones ayudan a evitar que haya intervenciones maliciosas entre ambas transmisiones y así evitar problemas en las comunicaciones.

En cuestión de los algoritmos empezamos con un readFile para que pueda leer el archivo y devolverlo en cadena de texto, se usa una función llamada contains para verificar el contenido que hay dentro de la transmisión (específicamente verificar si hay código malicioso). Utilizamos una función para encontrar el palíndromo más largo en una cadena llamada findLongestPalindrome donde cada carácter individual es un palindromo, busca palindromos de longitud 2 y de longitud mayor.

La complejidades de nuestras funciones son:
readFile: O(n)
contains: O(n * m)
findLongestPalindrome: $O(n^2)$
findLongestCommonSubstring: O(n1 * n2)

Alejandro Charles Gonzalez - A00835903:

En nuestro equipo, enfrentamos el reto de analizar transmisiones de datos para detectar posibles compromisos de seguridad. La situación era que, durante la transmisión de información, alguien podría interceptar los datos y modificar partes del mensaje, insertando código malicioso que afectaría el dispositivo receptor.

Nuestro enfoque se centró en identificar si las transmisiones contenían fragmentos de código malicioso que ya conocíamos, y lo logramos buscando estos patrones en los archivos de transmisión. Además, fuimos un paso más allá al detectar también palíndromos, ya que los atacantes podrían reorganizar el código de manera reflejada para evitar ser detectados.

También analizamos ambas transmisiones para encontrar similitudes entre ellas, buscando patrones comunes que podrían ser indicativos de una intervención maliciosa.

Alba Suarez Tapia - A01764346:

Esta actividad es fundamental en el ámbito de la seguridad informática, ya que nos permite trabajar en la detección de código malicioso y verificar la integridad de las transmisiones de datos. Al buscar fragmentos palíndromos en los archivos, simulamos cómo un sistema puede identificar vulnerabilidades o anomalías en el flujo de información, algo muy importante en la protección de los sistemas.

Además, esta práctica nos ayuda a desarrollar habilidades clave para la ciberseguridad, como la implementación de algoritmos para la detección de vulnerabilidades y el análisis eficiente de datos. El análisis de palíndromos y la comparación de substrings comunes son herramientas poderosas para identificar patrones sospechosos, que en la realidad podrían ser señales de ataques como la inyección de código malicioso. En un entorno donde las amenazas evolucionan constantemente, estas competencias son esenciales para proteger sistemas e información.