PEC1 - parte3

Primera practica no guiada

Durante la realización de los ejercicios sin guia, el mayor problema ha sido centrarme demasiado en la captura de trafico `.pcap`. En el primer ejercicio, estaba buscando el trafico generado por el IDS en las capturas de trafico, en vez de tener la capacidad de dar un paso atrás y ver que el `.zip` contenía un segundo archivo en el que aparecían los logs del IDS.

Segunda practica no guiada

Durante la realización de la segunda practica no guiada, el problema inicial ha sido buscar el punto en el que el sistema ha sido infectado. Desde el inicio, he detectado que el sistema infectado estaba enviando archivos al servidor controlado por el atacante, pero no he conseguido identificar el vector de infección.

En esta practica, lo primero que he hecho ha sido investigar los logs incluidos en el archivo `.zip`, ya que tienen la capacidad, aunque sea, de proporcionar contexto al ejercicio.