MÁSTER EN REVERSING, ANÁLISIS DE MALWARE Y BUG HUNTING

MÓDULO 5. REVERSING DE REDES Y PROTOCOLO – TAREA 2 – ANÁLISIS DE TRÁFICO

MÁSTER EN
ANÁLISIS DE MALWARE Y REVERSING

Campus Internacional CIBERSEGURIDAD

ENIIT INNOVA IT BUSINESS SCHOOL

UCAM UNIVERSIDAD CATÓLICA DE MURCIA

Actividad 2 – Análisis de tráfico

El objetivo de esta actividad individual es analizar con 'Wireshark' el tráfico de una aplicación desconocida a partir de una captura de tráfico de la misma.

En particular, hay que analizar el tráfico incluido en el fichero actividad2.pcap, que acompaña a este enunciado. Esa captura de tráfico se ha realizado en la misma máquina (192.168.1.33) donde se ejecuta el servidor de la aplicación a analizar y que corre en el puerto TCP/7000 (que no es el puerto estándar de ese protocolo).

El fichero de captura también incluye otro tipo de tráfico, que no está relacionado con la aplicación, por lo que se deberían utilizar los filtros de visualización de Wireshark para encontrar el tráfico de la aplicación.

1. Análisis del protocolo

El objetivo de la práctica es estudiar el protocolo empleado por la aplicación, identificar el tipo de mensajes intercambiados por el cliente y el servidor, así como intentar interpretar el contenido y significado de los mismos, e idealmente obtener la información intercambiada.

Opcionalmente se propone intentar identificar el protocolo exacto que está siendo empleado por la aplicación.

En la memoria de la actividad se deben incluir capturas de pantalla de 'Wireshark' para ilustrar la especificación del protocolo de la aplicación, así como capturas de pantalla de la información intercambiada entre el cliente y el servidor.