XUNTA DE GALICIA

FORMACIÓN PROFESIONAL INNOVA

IES San Clemente

CIFP Rodolfo Ucha Piñeiro

Forense en Windows

Parte 1

El ex-piloto de carreras John Tanner es ahora un policía infiltrado en la Mafia de Nueva York. Su capo, el señor Castaldi, planea un golpe de forma inminente. Suponemos que el elegido para llevarlo a cabo es el implacable asesino a sueldo Jean Paul, alias “El Francés”, y que, como de costumbre, Tanner conducirá el coche de la huida. Sin embargo, aún no sabemos cuál es el objetivo.

Lo que sí sabemos es que Tanner estuvo manteniendo conversaciones con el Sr. Castaldi a través de una aplicación de chat. Por desgracia, dicha aplicación está cifrada con un mecanismo conocido como Double Ratchet, similar al que usan WhatsApp y sus competidores y, por tanto, no hemos podido intervenir dichas comunicaciones.

Ahora, Tanner está desaparecido y su ordenador está frito, lo cual no es de extrañar, pues medio FBI y parte de la policía metropolitana están sobornados. Por suerte, poco antes del golpe, uno de nuestros técnicos pasó a Tanner un USB con un programa para ejecutar. Dicho programa, llamado DumpIt, sirve para recoger una imagen de memoria del equipo. Cuando nuestros hombres llegaron, el USB estaba en el escondrijo acordado, así que quizás los agentes corruptos del FBI no lo hayan tocado. Como era de esperar, allí había una imagen de memoria con lo último que Tanner ejecutó en el ordenador antes de salir. Además, como habíamos quedado, en la recepción del hotel de enfrente de su apartamento nos dejó una nota en la cual estaba escrito el código hash de la imagen creada: a518111a8f288d94fb4fb0069e36a884e1483f72b51b876303b6c7cfcb945715

Desafíos

1. ¿Cuál es el nombre del equipo? (100 puntos)
2. ¿Cuál es el hash de la contraseña del usuario Tanner? (sólo los 32 caracteres que están justo antes de la secuencia “:::”, en minúsculas) (100 puntos)
3. ¿Cuál es la contraseña correspondiente a dicho hash? (100 puntos)
4. Según el plugin consoles, ¿en qué dirección de memoria se encuentra la frase en la que se encuentra la frase en la que Tanner pregunta a quién van a asesinar? (100 puntos)
5. ¿Cómo se llama el archivo de proceso por lotes en el que se lanza la aplicación de chat? (100 puntos)
6. ¿Cuál es el identificador del proceso que tiene como hijo a una aplicación Java? (100 puntos)
7. ¿Cuál es el apellido que Castaldi menciona durante la conversación en la que se revela que van a matar al Presidente? (300 puntos)
8. ¿Cuál es el nombre de archivo (incluida la extensión) con la imagen JPG que se abrió un rato antes de que Tanner tuviera que abandonar el equipo? (100 puntos)
9. ¿Cuál es el identificador de proceso con el que se abrió dicha imagen? (200 puntos)

Parte 2

Finalmente unos expertos en hardware han logrado rescatar una imagen del disco de Tanner. Con la nueva información adquirida, podemos sacar algunos datos más de su actividad en los últimos días. Los hashes del archivo son los siguientes:

- MD5: 8712a3760e8fc801425309852ee1127a ExamenForense.img
- SHA-1: eaa88659a5dd2453527ffee0ccb13447c7223184 ExamenForense.img
- SHA-256: e4216bb636648b7a4188aacef3587c64aabfb05aade76b6070b3ce8d66d4568a ExamenForense.img

Evidencias aportadas:

- Captura de memoria RAM (DRIVERGAME-20220212-133941.dmp - 2GB).
  - mirror1
  - mirror2
  - mirror3
- Imagen disco duro (ExamenForense.img.zip - 7.1GB --> descomprimido 32,0 GB)
  - mirror1
  - mirror2
  - mirror3

Desafíos

10. ¿Cuál es la versión del SO? (incluida la edición y el service pack si los hubiera) (50 puntos)
11. ¿En qué fecha y hora hizo Tanner login por última vez? (formato DD/MM/AAAA HH:mm:ss, poniendo la hora en la zona horaria UTC) (50 puntos)
12. ¿En qué fecha y hora se equivocó por última vez Tanner al meter su password de usuario? (formato DD/MM/AAAA HH:MM:SS y zona horaria UTC) (50 puntos)
13. ¿Qué versión de Mozilla Firefox tenía Tanner instalada en su equipo? (Usar el formato major.minor, sin la letra “v” ni nada) (50 puntos)
14. Tanner ha estado mirando un vídeo sobre un terrorista. ¿Cuál es su nombre? (formato Nombre Apellido, sin diminutivos ni segundo nombre) (50 puntos)
15. Sabemos que Tanner se aloja en el Holiday Inn Manhattan Financial District, pero los mafiosos han alojado a Jean Paul en otro hotel y nuestro héroe tiene que ir a recogerlo allí. ¿Cuál es? (50 puntos)
16. ¿En qué lugar estará Tanner de vacaciones probablemente? (50 puntos)
17. En qué fecha y hora introdujo Tanner su pendrive por última vez en el equipo? (formato DD/MM/AAAA HH:mm:ss, poniendo la hora en la zona horaria CET) (50 puntos)
18. Tanner se descargó un libro en formato .doc ¿Cuál es el nombre completo del archivo? (100 puntos)