

Primera parte

Contexto

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:

a518111a8f288d94fb4fb0069e36a884e1483f72b51b876303b6c7cfc945715

Desafíos

[100pts] ¿Cuál es el nombre del equipo?

Solución: DRIVERGAME

[100pts] ¿Cuál es el hash de la contraseña del usuario Tanner? (sólo los 32 caracteres que están justo antes de la secuencia “:::”, en minúsculas)

Solución: 3ec585243c919f4217175e1918e07780

[100pts] ¿Cuál es la contraseña correspondiente a dicho hash?

Solución: abc123.

[100pts] 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?

Respuesta: 0x192050

[100pts] ¿Cómo se llama el archivo de proceso por lotes en el que se lanza la aplicación de chat?

chatApp2.bat

[100pts] ¿Cuál es el identificador del proceso que tiene como hijo a una aplicación Java?

Solución: 2956

[300pts] ¿Cuál es el apellido que Castaldi menciona durante la conversación en la que se revela que van a matar al Presidente?

Solución: Maddox

[100pts] ¿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?

driver_you_are_the_wheelman.jpg

[200pts] ¿Cuál es el identificador de proceso con el que se abrió dicha imagen?

2612

Segunda parte

Contexto

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

Desafíos

[50pts] ¿Cuál es la versión del SO? (incluida la edición y el service pack si los hubiera)

Windows 7 Professional N Service Pack 1

[50pts] ¿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)

13/02/2022 17:26:22

[50pts] ¿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)

13/02/2022 17:26:16

[50pts] ¿Qué versión de Mozilla Firefox tenía Tanner instalada en su equipo? (Usar el formato major.minor, sin la letra “v” ni nada)

97.0

[50pts] Tanner ha estado mirando un vídeo sobre un terrorista. ¿Cuál es su nombre? (formato Nombre Apellido, sin diminutivos ni segundo nombre)

Theodore Kaczynski

[50pts] 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?

Hilton Garden Inn

[50pts] ¿En qué lugar estará Tanner de vacaciones probablemente?

Cancún

[50pts] ¿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)

12-02-2022 14:39:17

[100pts] Tanner se descargó un libro en formato .doc ¿Cuál es el nombre completo del archivo?

Walden La Vida en los Bosques by Thoreau, Henry David (z-lib.org).doc