XUNTA DE GALICIA

FORMACIÓN PROFESIONAL INNOVA

IES San Clemente **CIFP Rodolfo Ucha Piñeiro**

Forense en Windows

Parte 1

O ex-piloto de carreiras John Tanner é agora un policía infiltrado na Mafia de Nova York. O seu capo, o señor Castaldi, planea un golpe de forma inminente. Supoñemos que o elixido para levalo a cabo é o implacable asasino a soldo Jean Paul, alias "O Francés", e que, como de costume, Tanner conducirá o coche da fuxida. Con todo, aínda non sabemos cal é o obxectivo.

O que si sabemos é que Tanner estivo a manter conversacións co Sr. Castaldi a través dunha aplicación de chat. Por desgraza, dita aplicación está cifrada cun mecanismo coñecido como Double Ratchet, similar ao que usan WhatsApp e os seus competidores e, por tanto, non puidemos intervir ditas comunicacións.

Agora, Tanner está desaparecido e o seu computador está frito, o cal non é de estrañar, pois medio FBI e parte da policía metropolitana están subornados. Por sorte, pouco antes do golpe, un dos nosos técnicos pasou a Tanner un USB cun programa para executar. Devandito programa, chamado DumpIt, serve para recoller unha imaxe de memoria do equipo. Cando os nosos homes chegaron, o USB estaba no agocho acordado, así que quizais os axentes corruptos do FBI non o tocaran. Como era de esperar, alí había unha imaxe de memoria co último que Tanner executou no computador antes de saír. Ademais, como quedaramos, na recepción do hotel de en fronte do seu apartamento deixounos unha nota na cal estaba escrito o código hash da imaxe creada: a518111a8f288d94fb4fb0069e36a884e1483f72b51b876303b6c7cfcb945715

Desafíos

1. Cal é o nome do equpo? Formato: XX.X.X.X (100 puntos)
2. Cal é o hash do contrasinal do usuario Tanner? (únicamente os 32 caracteres que están xusto antes da secuencia ":::", en minúsculas) (100 puntos)
3. Cal é o contrasinal correspondeente a dito hash? (100 puntos)
4. Segundo o plugin *consoles*, en qué dirección de memoria atópase a frase na que Tanner pregunta a quen van asasinar? (100 puntos)
5. Como se chama o arquivo de proceso por lotes no que se lanza a aplicación de chat? (100 puntos)
6. Cal é o identificador do proceso que ten como fillo a unha aplicación Java? (100 puntos)
7. Cal é o apelido que Castaldi menciona durante a conversa na que se revela que van a matar ó Presidente? (300 puntos)
8. Cal é o nome de arquivo (incluída a extensión) coa imaxe JPG que se abriu un rato antes de que Tanner tivera que abandoar o equipo? (100 puntos)
9. Cal é o identificador de proceso co que se abriu dita imaxe? (200 puntos)

Parte 2

Finalmente uns expertos en hardware lograron rescatar unha imaxe do disco de Tanner. Coa nova información adquirida, podemos sacar algúns datos mais da sua actividade nos últimos días. Os hashes do arquivo son os seguintes:

- 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
- Imaxe disco duro (ExamenForense.img.zip - 7.1GB --> descomprimido 32,0 GB)
  - mirror1
  - mirror2
  - mirror3

Desafíos

10. Cal é a versión do SO? (incluída a edición e o service pack se os houbese) (50 puntos)
11. En que data e hora fixo Tanner login por última vez? (formato DD/MM/AAAA HH:mm:ss, coa hora na zona horaria UTC) (50 puntos)
12. En que data e hora se equivocou por última vez Tanner ó meter o seu password de usuario? (formato DD/MM/AAAA HH:MM:SS e zona horaria UTC) (50 puntos)
13. Que versión de Mozilla Firefox tiña Tanner instalada no seu equipo? (Usar o formato major.minor, sen ea letra “v” nin nada) (50 puntos)
14. Tanner estivo mirando un vídeo sobre un terrorista. Cal é o seu nome? (formato Nome Apelido, sen diminutivos nin segundo nome) (50 puntos)
15. Sabemos que Tanner alóxase no Holiday Inn Manhattan Financial District, pero os mafiosos aloxaron a Jean Paul noutro hotel e o noseo heroe ten que ir a recollelo alí. Cal é? (50 puntos)
16. En qué lugar estará Tanner de vacacións probablemente? (50 puntos)
17. En qué datta e hora introduxo Tanner o seu pendrive por última vez no equipo? (formato DD/MM/AAAA HH:mm:ss, coa hora na zona horaria CET) (50 puntos)
18. Tanner descargou un libro en formato .doc ¿Cal é o nome completo do arquivo? (100 puntos)