




Víctor Manuel Martínez

Calificación final

Enviado 16/11/24 17:44 (CET)

Sin calificar

 Las puntuaciones de las preguntas aparecen después de publicar todas las calificaciones

Contenido de la actividad



¡Bienvenido al Reto de Forense!

Antes que nada, para poder realizar este desafío debes descargarte el siguiente .zip:

- Reto Forense (<https://drive.google.com/file/d/1Y0S8b4c80YzjMaAnWII3tL7TLVXy87hS/view>).

La contraseña para descomprimir el fichero es: **sleuth**

Una vez descomprimido verás tres partes, únicamente trabajaremos con la Parte 1 y 2, las cuales debes analizar a través de las herramientas que has visto a lo largo de este Sprint desde tu máquina Kali; por lo que una vez descargado y descomprimido el archivo deberás llevarte todos los elementos de su interior a tu máquina Kali para así comenzar con el proceso de análisis.

Como entrega final, deberás responder las siguientes cuestiones que te planteamos tras haber analizado cada una de las partes. Para no dar lugar a errores las preguntas se dividirán según cada una de las partes del archivo .zip que os hemos entregado.

¡¡Recuerda incluir la respuesta a cada una de las preguntas!!

¡Buena suerte!

PARTE 1 - ANALISIS DE IMAGEN DE DISCO

Pregunta 1

¿Qué tipo de sistema de ficheros tiene la imagen? Una imagen de disco en formato .raw , la cual, corresponde con una copia exacta y sin procesar de los datos contenidos en ella, siendo usado en análisis forense digital, debido a que contiene todos los datos del disco, incluidos sectores: vacíos, eliminados y metadatos. La imagen viene acompañada de un archivo .md5 con un hash que corresponde que el de la imagen analizada, por lo que se garantiza que no ha sido manipulada.

Pregunta 2

¿Cuántos directorios hay dentro de la imagen? La imagen .raw , se divide en 4 directorios principales: 1 - \$0CarvedFiles, el cual se encuentra vacío. 2 - \$CarvedFiles, el cual contiene 1 subdirectorio: (1). 3- \$Unalloc. sin subdirectorios. 4 - Docs, el cual contiene dos subdirectorios (private y Peics) y el 5, que es un archivo comprimido en .gz

Pregunta 3

¿Cuántos archivos borrados hay? Hay un total de 2 archivos borrados, ya que aunque aparecen 3 archivos , uno de ellos es un documento .doc llamado ReyHalif.dc, que se repite.

Pregunta 4

¿Cuántos archivos hay en la imagen? En total la imagen contiene 31 archivos de distintos formatos.

Pregunta 5

Obtén tres de las imágenes disponibles e impórtalas:

Su respuesta

En total Autopsy, detecta 7 archivos como imágenes (jpg, gif y bmp), pero 4 de los archivos presentan un **círculo amarillo con un triángulo invertido** , lo cual, indica que el archivo es **sospechoso para el programa** , significando generalmente que el archivo ha sido identificado por el sistema como potencialmente relevante para la investigación o que contiene algún tipo de anomalía. Por todo ello y ser interesantes para el caso, se exportan los 3 archivos mas interesantes en ese caso:





NOTA.- la ultima imagen venia el archivo en .dat, habiendo sido renombrado a formato .jpg.

PARTE 2 - ANALISIS DE CAPTURA DE TRAFICO

Pregunta 6

¿Cuáles son las dos IPs que están en la comunicación? Las IPs que torno a las cuales se efectúan la mayoría de la comunicaciones, así como las que mayores comunicaciones realizan entre si mismas son: la 192.168.2.5 y la 192.168.2.244.

Pregunta 7

¿A qué puerto se están conectando? la IP 192.168.2.5 envía y recibe la conexión a través del puerto 52242 y la IP 192.168.2.244 lo hace a través del puerto 4444.

Pregunta 8

¿Qué comando se ha realizado?

- ☐ A `echo "*umR@Q%4V&RC" | sudo -S apt update`
- ☐ B `echo "*umR@Q%4V&RC" | sudo -S apt install netcat`
- ☐ C `echo "*umR@Q%4V&RC" | sudo -S -i`
- ☐ D `echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 < /etc/passwd`

Pregunta 9

¿Qué servicio se ha levantado y en qué puerto? Se ha levantado por parte de la IP 192.168.2.5, un servidor en el puerto 9999, redirigiendo el contenido del archivo /etc/passwd, perteneciente a la IP atacada: 192.168.2.244.

Pregunta 10

¿Qué versión del paquete netcat se ha instalado? La versión del paquete es: netcat 1.10-41.1 amd 64.

Pregunta 11

¿Qué archivo se ha enviado? El archivo que ha enviado la IP 192.168.2.244, a través del servidor, es el archivo "passwd", del directorio etc/passwd, que contiene todos los usuarios de la máquina atacada.

Pregunta 12

¿Qué usuario está en el equipo? ¿Qué password se ha utilizado para elevar la shell? El usuario del equipo con IP 192.168.2.5 se ha conectado con el usuario "jtomato" usando, la password *umR@Q%4V&RC".

Pregunta 13

¿Qué versión y distribución de Linux se está utilizando? Linux 5.3.0-46-generic (ubuntu 18.04.0)

Pregunta 14

¿Cuántos usuarios hay en el sistema atacado? Los usuarios reales en el equipo atacado, son dos: el usuario "root", el cual tiene el UID de superusuario 0, con el /bin/bash, y el usuario estándar "jtomato" con UID 1000 junto al /bin/bash.

Contenido de entrega

En la parte 2, antes de empezar con las preguntas, se ha confirmado que el archivo no ha sido modificado antes de su recepción como se muestra en la imagen, aportan los mismos hashes:



HASHES_parte_2.pdf



Conversión en curso

Este documento se cargará automáticamente cuando finalice la conversión