Team Challenge | S.21

Esta evaluación contiene preguntas que pueden recibir crédito parcial o negativo.

Descartar

14 DE 14 PREGUNTAS RESTANTES

Contenido del cuestionario

¡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

1 punto

¿Qué tipo de sistema de ficheros tiene la imagen? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 2

1 punto

¿Cuántos directorios hay dentro de la imagen? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 3

1 punto

¿Cuántos archivos borrados hay? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 4

1 punto

¿Cuántos archivos hay en la imagen? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 5

1 punto

Obtén tres de las imágenes disponibles e impórtalas:

Use el editor para dar formato a la respuesta

PARTE 2 - ANALISIS DE CAPTURA DE TRAFICO

Pregunta 6

1 punto

¿Cuáles son las dos IPs que están en la comunicación? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 7

1 punto

¿A qué puerto se están conectando? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 8

1 punto

¿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

1 punto

¿Qué servicio se ha levantado y en qué puerto? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 10

1 punto

¿Qué versión del paquete netcat se ha instalado? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 11

1 punto

¿Qué archivo se ha enviado? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 12

1 punto

¿Qué usuario está en el equipo? ¿Qué password se ha utilizado para elevar la shell? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 13

1 punto

¿Qué versión y distribución de Linux se está utilizando? **En blanco 1**

En blanco 1 Agregue su respuesta

Pregunta 14

1 punto

¿Cuántos usuarios hay en el sistema atacado? **En blanco 1**

En blanco 1 Agregue su respuesta

Contenido adicional

Arrastre y suelte los archivos aquí o haga clic para agregar texto.

Filtro de preguntas (14) ▼

Guardar y cerrar

Enviar