Tema4.4.4.4.EnriqueGomezTagle

sábado, 17 de febrero de 2024 11:52

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

a. Consideren la siguiente entrada de registro. Fue generada por Apache, un servidor web popular.

```
[Wed Mar 22 11:23:12.207022 2017] [core:error] [pid 3548:tid 4682351596] [client
209.165.200.230] File does not exist: /var/www/apache/htdocs/favicon.ico
```

La entrada de registro anterior representa un evento web grabado por Apache. Ciertos fragmentos de información son importantes en transacciones web, como la dirección IP del cliente, la hora y los detalles de la transacción. La entrada anterior puede desglosarse en cinco partes principales:

Marca de hora: esta parte registra el momento en el que sucedió el evento. Es muy importante que el reloj del servidor esté sincronizado correctamente ya que eso permite definir referencias cruzadas exactas para realizar un seguimiento de eventos del pasado.

Tipo: este es el tipo de evento. En este caso, se trató de un error.

PID: contiene información sobre el ID de proceso que está utilizando Apache en ese momento.

Cliente: registra la dirección IP del cliente solicitante.

Descripción: contiene una descripción del evento.

Básense en la entrada de registro anterior para describir lo que sucedió.

Un cliente con cierta IP intento acceder a un archivo del sitio web. pero el archivo no existe en esa ruta

¿La salida anterior todavía se considera una transacción web? Expliquen por qué la salida del comando **cat** tiene un formato diferente al de la entrada única que se presenta en el punto (a).

Sí, es un evento web, orden diferente de campos pero tiene GET, IP, referencias a navegadores HTTP v1.1 Debe de haberse configurado diferente el cliente

<Some output omitted>

Observen que los eventos enumerados anteriormente son muy diferentes de los eventos de un servidor web. Como el propio sistema operativo está generando este registro, todos los eventos registrados son en relación con el SO en sí.

b. Si es necesario, presionen **Ctrl + C para** salir del comando anterior.

c. Los archivos de registro son muy importantes para la solución de problemas. Suponer que un usuario de ese sistema específico reporta que todas las operaciones de red eran lentas aproximadamente alrededor de las 4:20 am el 19 de mayo.

¿Pueden encontrar pruebas de ello en las entradas de registro de arriba? Si es así, ¿en qué líneas? Explique.

Miércoles 20 de marzo 14:28:33 - 14:29:05
líneas 5-12, tarjeta de red fluctuando de manera importante.

ejecuta journalctl con la opción –q (opción se suprime el mensaje de la sugerencia).

¿Cómo pueden ejecutar **journalctl** y ver todas las entradas de registro?

Si se ejecuta como root:
sudo journalctl