Práctica 5

AutoProcesamiento de logs (parte 2)

1. Objetivos

En esta práctica se realizarán una serie de programas que permitan la automatización de obtención de determinada información útil de los logs de sistema.

3. Programa a realizar

Se continuará con el programa realizado en la práctica anterior o si se prefiere se realizará un nuevo programa. Deberá leer desde parámetro el archivo de log que se desea procesar, de manera que podamos usar nuestro programa para procesar cualquier archivo de logs de cualquier servidor apache (Es el tipo de servidor web del que he obtenido los logs).

Se recuerda que se deséa obtener la información de de todas las IPs que **no sean la 127.0.0.1**. Recordemos que dicha dirección IP es la dirección de loopback, y se trata de peticiones internas que hace el propio servidor.

Los datos siguientes irán sobre las direcciones IP que **no** sean **la 127.0.0.1**.

Se deberá aportar el número de entradas por dirección IP ordenadas de mayor número de entradas a menor. El motivo de esto es que esta es una de las maneras de ver si alguien está intentando realizar un ataque de los llamados ataques de denegación de servicio (DOS). Si se detectan determinadas direcciones IP desde las que se hacen demasiadas peticiones esto es una referencia de que desde dicha dirección IP se está intentando atacar al servidor.

Se deberán imprimir también las direcciones IP que contengan la sentencia SELECT o select en la petición de la WEB. La petición se puede ver en el log porque tiene esta forma:

```
"GET /post.php?id=2 HTTP/1.1"
```

En la petición de arriba estaríamos accediendo o descargando la pagina web del servidor llamada post.php y lo que viene después del interrogante son variables que le da

el usuario al servidor para solicitar información. En el caso que nos ocupa el usuario está enviando al servidor la variable id con valor 2. En ese servidor eso quiere decir que el usuario esta intentando ver las características del articulo con identificador numero 2. Una forma de hackear los servidores web es introducir valores que el servidor no se espera, y en concreto las sentencias que llevan la sentencia **SELECT** o **select** están intentando hackear el servidor haciendo consultas forzadas a la base de datos (en este caso una base de datos de tipo SQL).

Al obtener las peticiones que contengan estas sentencias estaremos visualizando los hackers que están intentando forzar la obtención de datos internos de nuestra pagina web. Es lo que se conoce en el mundo del hacking como SQL Injection.

Por último deberemos listar las Direcciones IP que contengan la sentencia **system** en la petición. Al igual que se puede intentar forzar a que el servidor nos devuelva datos de la base de datos enviando variables especialmente diseñadas en la petición, también se puede forzar a que los servidores tengan una puerta trasera. El diseño típico de este tipo de peticiones suele tener la sentencia system en ellas, ya que system es la función de PHP (lenguaje de programación de servidores web) que permite la ejecución de comandos en la maquina servidor. Cuando vemos ese tipo de entradas en el log es que alguien esta intentando meter una puerta trasera en nuestro servidor, normalmente para realizar ataques a otros sitios utilizando la dirección IP de nuestro servidor web.

La salida del programa deberá tener la siguiente forma si se hace de forma independiente:

```
Total entradas por IP:
10.1.1.136: 840
10.1.1.132: 353
10.1.1.131: 99
10.1.1.142: 43
10.1.1.26: 5
Intentos de ataque SQL
10.1.1.132
10.1.1.136
10.1.1.142
Intentos de backdoors
10.1.1.132
10.1.1.136
10.1.1.142
```

En caso de continuar con el ejercicio de la práctica anterior la salida del programa deberá tener la siguiente forma:

```
Direcciones IP:
10.1.1.136
10.1.1.132
10.1.1.131
10.1.1.26
10.1.1.142
Datos generales:
Primera Entrada: [07/Nov/2016:10:10:09] [08/Nov/2016:10:33:24]
10.1.1.136 [07/Nov/2016:10:10:09] [07/Nov/2016:10:58:01]
10.1.1.132 [07/Nov/2016:10:10:10] [07/Nov/2016:10:57:57]
10.1.1.131 [07/Nov/2016:10:10:52] [07/Nov/2016:10:57:04]
10.1.1.26 [08/Nov/2016:07:30:06] [08/Nov/2016:07:30:30]
10.1.1.142 [08/Nov/2016:10:33:24] [08/Nov/2016:11:00:53]
Total entradas globales:
1340
Total entradas por IP:
10.1.1.136: 840
10.1.1.132: 353
10.1.1.131: 99
10.1.1.142: 43
10.1.1.26: 5
Intentos de ataque SQL
10.1.1.132
10.1.1.136
10.1.1.142
Intentos de backdoors
10.1.1.132
10.1.1.136
10.1.1.142
```