UNIVERSIDAD VERACRUZANA

FACULTAD DE ESTADÍSTICA E INFORMÁTICA

MAESTRÍA EN SISTEMAS INTERACTIVOS CENTRADOS EN EL USUARIO

Reporte del sistema de bitácoras

Alumno:
Jorge Luis Jácome Domínguez

Docente:
Gerardo Contreras Vega

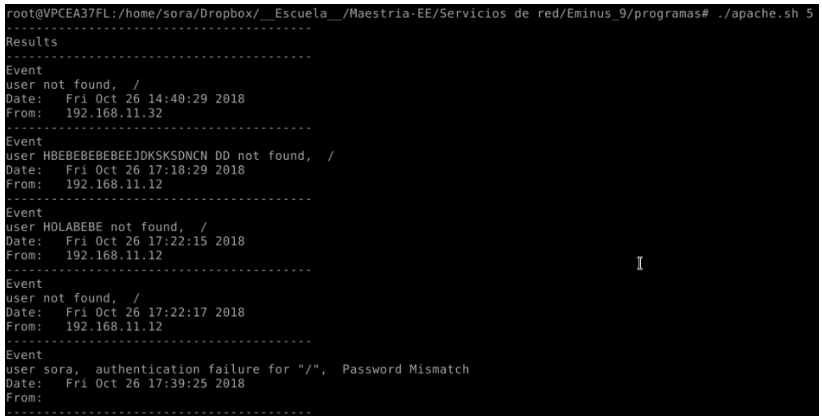
EE:
Servicios de Red.

Análisis de Logs

Log de Servicio “Apache”

Se escribió un script para leer y analizar las bitácoras del servicio de apache instalado en el sistema operativo Debia. Para, a través de este script, fuera posible ver los intentos de acceso fallidos que alguien háyase cometido al ingresar a las páginas del servidor web; mostrando información del usuario junto al error, en compañía de la fecha en la cual ocurrió el evento y el origen del mismo (si es remoto, se expondrá la dirección IP, si no, no se mostrara algo).

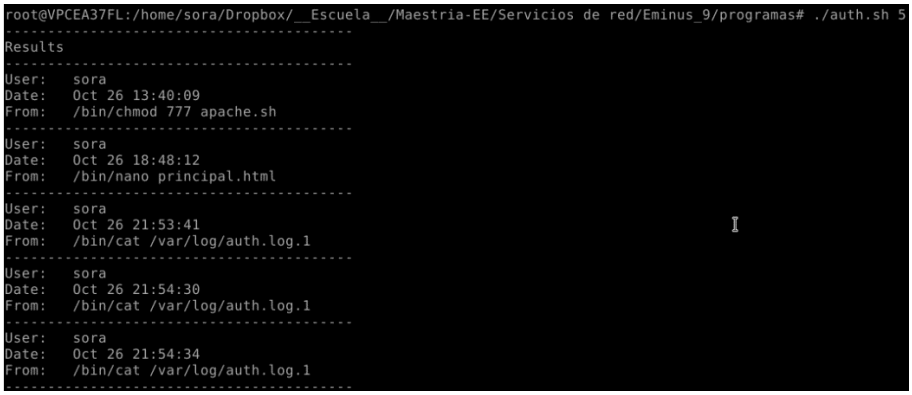
Después de finalizar de escribir el script, se le dio permisos de ejecución y se probó.
$ sudo chmod a+x apache.sh



Log de Bitácoras “Auth”

Se escribió un script para leer y analizar las bitácoras del servicio de auth del sistema operativo Debia. Para, a través de este script, fuera posible ver los comandos ejecutados en modo root por el usuario, acompañando a dicha información con la fecha en la cual se ejecuto una instrucción, y que instrucción fue la ejecutada.

Después de finalizar de escribir el script, se le dio permisos de ejecución y se probó.
$ sudo chmod a+x auth.sh



Sistema de bitácoras

¿Como funciona el sistema de bitácoras de Debian?

Los sistemas de bitácora apoyan al proceso de seguridad y administración, ya que, mediante ellos es posible registrar los eventos que ocurren en sistema operativo. Para el caso de Debian, su sistema de bitácoras funciona a través del demonio "syslogd", el cual se lanza automáticamente al arrancar el sistema operativo. Este demonio recibe los mensajes de diferentes partes del sistema, tal como el kernel y programas; además de tambien ser capaz de enviar mensajes a diferentes ubicaciones sean del mismo sistema o remotas. El demonio, sigue el criterio definido en el archivo “/etc/rsyslog.conf”; en este archivo (/etc/rsyslog.conf) se pueden especificar las reglas a seguir y gestionar el almacenamiento de mensajes en el sistema.

Los programas que generen mensajes de “syslog”, constan con 4 partes “el nombre del programa, el atributo facility (especificación del servicio o facilidad), la prioridad del programa, y el mensaje de ira en la bitácora”. Como ejemplo de su funcionamiento, a continua se expone parte de la configuración del archivo “/etc/rsyslog.conf”, para enviar algunos mensajes de syslog al correo electrónico.

```
# Des comentar para utilizar UDP
module(load="imudp")
input(type="imudp" port="514")

# Des comentar para utilizar TCP
module(load="imtcp")
input(type="imtcp" port="514")

# Cargar modulo para Emails
$ModLoad ommail

# Configurar envio de correo electrónico
$ActionMailSMTPServer localhost
$ActionMailFrom sora.vaio@sora.com
$ActionMailTo leon.blanco@hotmail.com
$template mailSubject,"Msj syslog desde '%hostname%'"
$template mailBody,"RSyslog desde %hostname%, dice que '%msg%'"
$ActionMailSubject mailSubject
$ActionExecOnlyOnceEveryInterval 30

# Configurar condición bajo la cual se enviarán los correos electrónicos
if $msg contains 'New session' or $msg contains 'Stopping' or $msg contains 'error' or $msg contains
'fatal' or $msg contains 'warning' or $msg contains 'critical' then :ommail:;mailBody
 $ActionExecOnlyOnceEveryInterval 0
```

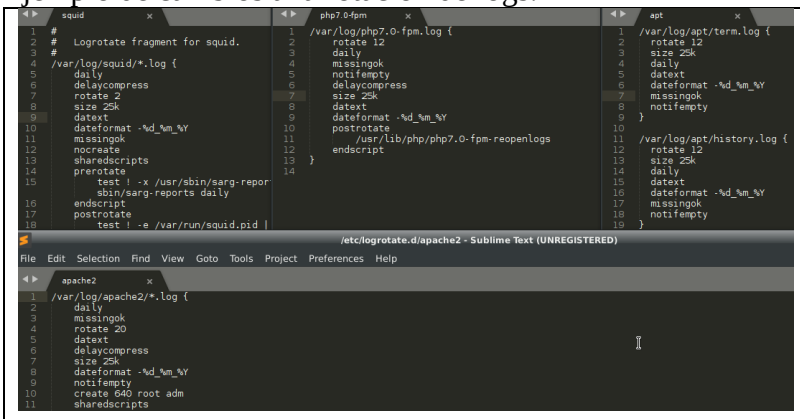
Configuración de la rotación de logs en Debian:

La rotación de logs en linux tiene por defecto a la herramienta lograte, a través de la cual es posible definir el tamaño máximo que tendrá el archivo log y las acciones que se pueden tomar (tales como eliminarlo, comprimirlo o renombrarlo) al rotarlo o al alcanzar su tamaño máximo. Asi mismo, lograte nos permite especificar el tiempo que se desea mantener vivos a los registros.

La configuración de la rotación de logs, puede especificarse a través del archivo "/etc/lograte.conf", asi como de los archivos de configuración contenidos en "/etc/lograte.d/*". Siendo algunas de los atributos que pueden utilizarse para configurar estos servicios, los siguientes:

- **compress**: Para indica que se tiene que comprimir el log que se va a rotar.
- **compresscmd**: Especifica la herramienta de compresión.
- **dateext**: Obliga al renombramiento de un log antiguo.
- **dateformat**: Sirve para indicar el formato de fecha a utilizar con la directiva anterior.
- **daily, weekly, o monthly**: Especificación de cada cuando se va a realizar la rotación de los logs, una vez por mes, por semana, o por mes.
- **notifempty**: Indica que no deben de rotarse los logs si el archivo está vacío.
- **size**: Obliga a que no se rote el log hasta que haya alcanzado por lo menos el tamaño indicado.
- **rotate n**: Indica a través del número que le sigue, cuántos logs deben conservarse luego de haber sido renombrado o comprimido.
- **create**: Especifica los permisos (de manera octal), junto con el dueño y grupo propietario de cada nuevo log creado por la rotación.

Ejemplo de cambios a la rotación de logs.




```
/var/log/apache2/*.log {
   daily // Para rotar diariamente
   rotate 20 // Guardar hasta 20 logs
   datext // Renombrar log
   dateformat -%d_%m_%Y
   create 640 root adm
   sharedscripts
   postrotate
   if /etc/init.d/apache2 status >
/dev/null ; then \
        /etc/init.d/apache2 reload >
/dev/null; \
   fi;
   endscript
   prerotate
   if [ -d /etc/logrotate.d/httpd-
prerotate ]; then \
      run-parts /etc/logrotate.d/httpd-
prerotate; \
   fi; \
   endscript
}
```