

Registro de Eventos

Introducción

¿Que es un Log?

Propósito de los logs

Administración de Logs

Consolidación de logs

Rotación de logs

Almacenamiento y aseguramiento de Logs

Herramientas y Estrategias para la Administración de Logs

Syslog

Tripwire

Logrotate

Conclusiones

Bibliografía

Registro de Eventos

Introducción

La centralización y administración de archivos de logs provenientes de redes y sistemas tiene muchas ventajas. Hay buenas fuentes de documentación sobre la información que debería ser registrada en los logs, como realizarlo de una forma óptima y como puede ser utilizada posteriormente [CenLog00], [LogCrit00], [LogCons00]. Sin embargo, los requerimientos para el uso de archivos de logs para propósitos técnicos, tal como la detección de intrusos, son diferentes y no siempre complementarios a los requerimientos para el uso de tales datos en una situación legal.

Un archivo de log viable como evidencia, es aquel que ha sido rastreado y protegido desde el momento que fue creado, y el cual contiene entradas o registros relacionados con un caso legal. [MaFor01]. En la mayoría de los casos, el requerimiento de uso de un determinado archivo de log en una investigación, es algún tiempo después que el archivo fue tomado y centralizado. Este documento busca realizar un recorrido a lo largo del tema de los logs como evidencia, iniciando en las definiciones de lo que se considera un log, la evidencia en si, su problemática, las características que deben poseer para poder ser considerados como tal, algunas técnicas para llevar a cabo este propósito y por ultimo se entrara a estudiar un poco en detalle algunas herramientas que ayudaran a conseguir el objetivo de lograr que los archivos de logs sean un material de evidencia en un caso legal.

¿Que es un Log?

LOGS (*término tomado del ingles, relacionado con la acción de Logging o registro de operaciones o acciones de los sistemas de información*) o registros de auditoria.

Los LOGS [WEBER 1999] representan la historia y evolución de los sistemas de información, es la memoria vigente del sistema operacional, del hardware o de la aplicación o aplicaciones, que le permite tanto al programador como a la organización conocer el comportamiento de éstos, así como la interacción de los usuarios en el desarrollo de sus funciones.

Propósito de los logs

El propósito de un log es proveer a los profesionales de seguridad informática la habilidad de monitorear las actividades de la aplicación o dispositivo. Revisando las salidas de los archivos de logs, se puede obtener una buena oportunidad para determinar los eventos, y tomar la acción necesaria para corregir el problema o iniciar una investigación en caso de un incidente de seguridad. (Ver Documento Evidencia digital)

Administración de Logs

Consolidación de Logs

La consolidación de logs ofrece un a manera ágil y útil de organizar, asegurar, correlacionar y controlar logs.

Principalmente se considerará dos escenarios a la hora de tener en cuenta la consolidación como un aspecto de la administración de logs. Los dos escenarios trabajan sobre un área centralizada para el almacenaje de logs.

Escenario A

La arquitectura de esta propuesta se basa en un único servidor central para la administración de logs. La información de logs puede ser utilizada en un centro de operaciones 7x24 como un dispositivo de alertas centralizado para un a consola de operaciones.

En este caso se requiere una buena capacidad de almacenamiento, y de acuerdo a la disponibilidad deseada es recomendable utilizar disco duros redundantes o un RAID[CenLog00].

Un problema con este tipo de arquitectura es que al tener un único y común servidor de logs se establece también un único punto de falla o ataque. El sistema por completo dependería de la disponibilidad de este punto e igualmente un atacante al obtener acceso a este servidor pondría en duda la validez de los logs y la utilización de estos como evidencia en una investigación formal. De esta forma un atacante podría cubrir su actividad delictiva removiendo o modificando cualquier log que contenga registro de su actividad. Centralizando logs de esta forma se hace mucho más fácil el trabajo para un atacante. Más adelante se abordará como combinando una serie de estrategias se puede llegar a un buen nivel de seguridad en este escenario.

Escenario B

Esta arquitectura utiliza un método más robusto, almacenaje de logs de acuerdo a una clasificación de los mismos. Cada servidor es usado para cada clase de fuente de log.

Más claramente al tener un servidor para grupos de fuentes de logs, si el servidor de logs de los servidores con sistema operativo Windows NT falla, seguirá estando disponible el servidor de los de las maquinas Unix y desde luego los servidores de los demás dispositivos. Una forma de aumentar la disponibilidad es tener una replica de los logs en otros servidores de logs, alta redundancia.

Los logs estarán centralizados y pueden ser utilizados en un ambiente de centro de control 7x24. Ahora si un atacante desear eliminar el rastro de sus actividades, tendrá mucho más trabajo por hacer y recorrer más de una maquina para ser efectivo en su labor. Un problema de este escenario se puede determinar fácilmente, el costo de la infraestructura que satisfaga los requerimientos planteados.

Rotación de Logs

Los archivos de log pueden rápidamente consumir gran cantidad de almacenamiento en un servidor centralizado de logs, (lo cual es relativamente costoso), de igual forma determinar que archivo de log en particular en un futuro será útil en una investigación o proceso legal es muy difícil. La técnica de rotación de logs permite limitar el volumen de datos que se tienen disponibles para examinar fácilmente, en este caso en el servidor de logs, y además controlar el número de archivos de logs que estarán expuestos a un posible daño por parte de un intruso. [ManLog]

La estrategia de rotación de logs se basa principalmente en cambiar la ubicación de los archivos de logs a una nueva locación y renombrarlos de esta manera podrán reflejar la rotación.

La rotación de logs es un evento que toma lugar luego de un intervalo de tiempo determinado, este intervalo se puede establecer generalmente en horas, días, semanas inclusive meses, en este aspecto entra en juego los

requerimientos propios del sistema al cual se quiere proteger, la cantidad y criticidad de la información producida.

Ya que la rotación depende del tiempo, es muy importante que tanto los servidores, como los dispositivos que producen los logs posean una alta exactitud en el tiempo. Para esto se puede utilizar el servicio Network Time protocol NTP[CenLog00].

El NTP permite a los dispositivos sincronizar sus relojes con un servidor de tiempo centralizado, el cual a su vez esta sincronizado con un sistema de posición global (Global Position System GPS), esta combinación asegura una exactitud de milisegundos. Este aspecto es de vital importancia a la hora de la rotación de logs y más aún para la correlación de los mismos y la utilización de logs como evidencia en un caso legal[LogCrit00].

Una rotación exitosa generará un número de logs que contendrán datos para la rotación de un log en particular. Como existe a generación de nuevos archivos a partir de log "Rotado", es muy importante prestar especial atención al nombrado de estos archivos de esta forma puedan ser de fácil identificación y clasificación a la hora de requerirlos.

Un sencillo ejemplo de cómo nombrar los archivos puede ser el siguiente: nombre del archivo: NT_System.log, luego de una rotación se generaran archivos que se podrán nombrar, en este caso una rotación programa en un intervalo de días, de la siguiente manera 06-14-2001-NT- System.log, 06-15-2001-NT- System.log, 06-16-2001-NT- System.log, etc.

Ahora cuando un incidente o evento ocurre, existe una manera correcta y eficiente de buscar información. Los logs se encontraran centralizados, organizados y exactos en el tiempo.

Almacenamiento y aseguramiento de Logs

La estrategia de almacenamiento de logs es útil en el momento de prevenir que la máquina o dispositivo (storage) donde se guardan los logs comience a alcanzar los límites máximos de capacidad rápidamente, sobre todo en aquellos ambientes especialmente activos.

Más importante aún, se tendrá un archivo de eventos de logs que han ocurrido en determinado lapso de tiempo, de esta manera se tendrá un efectivo archivo de evidencias que podrá utilizarse en cualquier momento que se necesite y los cuales cumplirán con los requisitos legales

Entre las formas comunes de almacenaje se encuentran aquellos dispositivos, medios y procedimientos estándares que utilizan las compañías para la realización de Backups de datos. Entre estos podemos encontrar el almacenaje en Cintas, CD-R, CD-RW, o Zip/Jazz drives.

Ahora, luego que tenemos una estrategia de almacenamiento, podemos pensar en como lograr que estos datos permanezcan incorruptibles a lo largo del tiempo, esto se puede lograr con estado de solo lectura. Una forma de almacenar los logs con un estado de solo lectura es utilizando medios que físicamente están protegidos contra escritura. Los medios CD-R son a menudo escogidos para este tipo almacenaje ya que están fabricados para ser escritos una sola vez y no soportan múltiples escrituras. En una forma sencilla almacenar datos en CD-R es un método para proteger datos contra procesos destructivos.

Otros aspectos que hay que considerar con respecto a los medios CD-R, es que tiene un limite de vida mucho más limitado que el relacionado con las cintas, algo menos de 10 años, de esta forma si se tiene pensado preservar los logs por un largo tiempo será una buena opción pensar en cintas[ManLog].

Por último, la encriptación de datos es recomendada en aquellos archivos de logs que posean datos críticos. Una buena costumbre a seguir es encriptar estos

archivos, almacenar las llaves de encriptación en un disco de 3 ½ o un "WORM CD-ROM" (WORM, Write Once, Read Many) y colocar estas en una lugar seguro como una caja fuerte [ManLog].

Herramientas y Estrategias para la Administración de Logs

Syslog

Syslog es un sistema de logs que se encarga principalmente de la administración de logs, los cuales son generados por eventos del sistema, sus programas o por el Kernel. Para lograr capturar y administrar los logs que se generan permanentemente sin ningún aviso, syslog utiliza un demonio que se encarga de capturar cualquier log generado. Este demonio se llama syslogd.

Tripwire

Es una herramienta diseñada especialmente para Sistemas Operacionales UNIX. Una versión muy versátil viene con varias distribuciones comerciales de Linux.

Dicha herramienta por medio de funciones se encarga de generar un Hash único por cada archivo que se le desee proteger su integridad. De esta forma cuando se presente un cambio en un log por parte del atacante, este cambio será notificado al administrador (enviándose un mail automático) ya que no reflejará el hash original.

Para realizar dichas detecciones Tripwire también se basa en:

- **CRC-32:** Es un checksum de redundancia cíclica con una firma de 32 bits que puede generar aproximadamente 4 billones de valores. Estos valores se generan a través de una tabla que maneja CRC de 256 posiciones. Cada posición tiene un valor que se genera a través de un polinomio que conoce previamente el algoritmo. [CRCWin].
- **MD5 :** Es un algoritmo que por medio de operaciones matemáticas crea un checksum de 128 bits. Para lograr este cometido el mensaje debe de ser congruente a 448 módulo 512, si la longitud del archivo no cumple con estas características, el algoritmo procede a extender el archivo hasta que la condición se cumpla. [MD5Home].
- **SHA:** Este algoritmo produce un "message digest" como salida el cual es irreplicable. Esto se logra a través de operaciones lógicas como and , or , xor, etc. Para empezar a procesar el archivo el algoritmo lee en bloques de 512 bits y a cada uno de estos bloques les aplica las operaciones predefinidas en el algoritmo (en total son 79 funciones lógicas aplicables). Después parte el bloque de 512 en palabras de 32 bits a las cuales son aplicadas las funciones produciendo salidas de 32 bits también. [SHA-1Doc].
- **HAVAL** (firma digital de 128 bits) Este algoritmo se encarga de producir un Hash de 128 bits, procesando en bloques de 1024 bits de la entrada (en este caso son los archivos de logs). En la actualidad es uno de los algoritmos más seguros. [HaOne93].

Logrotate

Esta herramienta alterna, comprime y envía logs de sistema. Está diseñada para facilitar la administración de los sistemas que generan un gran número de archivos de logs. Permite la rotación automática, comprensión, extracción y envío de los archivos de logs. Puede manipularse cada archivo log diaria, semanal o mensualmente, o cuando se haga demasiado grande.

Conclusiones

En el aspecto de centralización de logs, Syslog es una herramienta viable, disponible en diferentes plataformas y sin costo extra. De igual forma se debe tener en cuenta las fallas de seguridad intrínsecas al utilizar el protocolo UDP, de esta forma, al manejar información crítica se recomienda implementar metodologías para reforzar la seguridad, como el filtrado de paquetes en el puerto utilizado por Syslog (puerto 514).

El uso de las herramientas presentadas en este documento son de gran ayuda a la hora de administrar y conseguir que los logs puedan ser utilizados como evidencia. Pero sin la base de unas políticas de seguridad bien definidas e implementadas, se perderá objetivo de las mismas.

Cada una de las etapas descritas para la administración de logs es crítica, así si se cuenta con un sistema de centralización bien diseñado e implementado pero a su vez, no se logra un buen método de administración de los archivos en el servidor de logs (rotación y comprobación integridad), el sistema de administración como tal será ineficiente.

Los archivos de logs aunque son básicos a la hora de una investigación de intrusiones en los sistemas informáticos, siempre hay que tener en mente que son esenciales a la hora de tomar medidas legales contra esos intrusos.

Bibliografía

- [WEBER 1999]** WEBER, R. (1999) Information Systems Control and Audit. Prentice Hall.
- [MainCre]** Mark Burnett, Maintaining Credible IIS Log Files.
<http://www.securityfocus.com/infocus/1639>
- [ManLog]** Manage logging and other data collection mechanisms. CERT Coordination Center from Carnegie Mellon University.
<http://www.cert.org/security-improvement/practices/p092.html>
- [MaFor01]** Tom Ceresini. Maintaining the Forensic Viability of Logfiles.
<http://www.perimeterlabs.com/sitedocuments/Maintaining%20the%20Forensic%20Viability%20of%20Logfiles.pdf>
- [CenLog00]** Hunter, James. "Central Logging Security."
http://www.sans.org/infosecFAQ/unix/logging_sec.htm
- [LogCrit00]** Morton, Matt. "Logging and critical logs files: the Decision to Effectively and Proactively Manage System logging and Log Files."
<http://www.sans.org/infosecFAQ/securitybasics/logging.htm>
- [LogCons00]** Pitts, Donald. "Log Consolidation with syslog."
<http://www.sans.org/infosecFAQ/unix/syslog.htm>
- [CRCWin]** **CRC32 for Windows 9x/NT**
www.cyberdynesoftware.com/crc32.html
- [MD5Home]** MD5 Homepage
<http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html>
- [SHA-1Doc]** Description of SHA-1 and SHA-256.
<http://home.ecn.ab.ca/~jsavard/crypto/mi060501.htm>
- [HaOne93]** HAVAL A One-Way Hashing Algorithm with Variable Length of Output (1993) <http://citeseer.nj.nec.com/zheng93haval.html>