UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster Universitario en Seguridad Informática

Gestión de Logs

Trabajo Fin de Máster

presentado por: Mª Begoña Alonso-Alegre Díez

Director: Jose Luis Vazquez Poletti

Febrero de 2016

Mª Begoña Alonso-Alegre Díez

Master Universitario de Seguridad Informática

Resumen

El objetivo del TFM Gestión de Logs es señalar la importancia de la información que aportan los ficheros logs de los diferentes programas y aplicaciones, y de cómo su conocimiento y análisis ayuda a la gestión de la seguridad de la Organización.

Se presenta una metodología y forma de actuar, cuyo objetivo es ayudar a la recopilación y clasificación de los ficheros logs, así como el procedimiento para una detección de vulnerabilidades y fallos de software.

Palabras Clave:

Log Gestión Registros Análisis Vulnerabilidades

Abstract

The objective of "Gestión de Logs" (Logs's Management) document is to recognize the importance of the log files .The log files record an important information about the activity of different programs and applications, and we can appreciate how it's a necessary and useful activity to collect and analyze this information.

This document reflects a methodology where the log files collection and classification have assumed a great importance to find vulnerabilities or software bugs in order to security management.

Keywords:

Management Log Vulnerabilities Analysis

Mª Begoña Alonso-Alegre Díez

Master Universitario de Seguridad Informática

Gestión de Logs

Contenido

Resumen

El objetivo del trabajo *Gestión de logs* es desarrollar una metodología para recoger, clasificar, integrar, analizar e interrelacionar, todos los posibles ficheros logs o registros que pueden aportar los elementos de la infraestructura de red de una organización, y unificarlos en una única administración y gestión: ficheros que provienen de servidores web, intranet, DMZs, correo, servidores de aplicaciones internas, DNS, proxys, firewalls, etc.

Con todo esto, se pretende que la detección de vulnerabilidades, fallos de software, ataques o agujeros de seguridad, genere unas líneas de actuación, que permita conocer lo antes posible el alcance y posibles máquinas afectadas, es decir, la repercusión de ese incidente en la red y servidores.

Analizar los ficheros logs y la información que aportan, es de gran importancia para una eficaz administración y gestión de la red. El conocimiento del tráfico "normal" de la red y el control de accesos, son dos elementos clave para la detección del tráfico "anómalo", que con una metodología, y con una serie de pasos establecidos, se podrá detectar "dónde" y "hasta dónde" repercute esa alteración.

Introducción

El objetivo del presente trabajo es recoger la información que nos facilitan los diferentes elementos de una red, pero realizándolo de una forma metódica y ordenada.

En definitiva, lo que se pretende conocer es saber dónde está la información que puede aportar cada elemento de la red, bien sea por sus características de servidor o por su situación en la red, y analizarla ante fallos de software, ataques o intrusiones, fallos de configuración, con objeto de detectar la situación "anómala" y sus consecuencias a la mayor brevedad posible.

Creo conveniente, para establecer el marco donde se va a trabajar, dar una serie de definiciones y unos conceptos sobre log:

- La palabra **log** es un término anglosajón, equivalente a la palabra bitácora en español. [1]
- Es un registro oficial de eventos durante un rango de tiempo en particular.
- Debe responder a las W5: who, what, when, where y why (quién, qué, cuándo, dónde y por qué) un evento ocurre para un dispositivo en particular o aplicación.[2]
- También se le considera como aquel mensaje que genera el programador de un sistema operativo, alguna aplicación o algún proceso, en virtud del cual se muestra un evento del sistema.[1]
- Los logs son ficheros de texto que almacenan información relevante como conexiones remotas, eventos del sistema, etc. Existen varios que son de gran interés forense y que deben ser recopilados.[3]

En definitiva, son registros de información que nos llegan de diferentes orígenes ó fuentes a una Organización y, que actuando con una buena política de gestión de logs bien organizada y documentada, resulta muy conveniente para conocimiento correcto de la red y una detección temprana de errores, debilidades, vulnerabilidades y ataques a los Sistemas de Información.

El TFM se estructura de la siguiente manera:

- En primer lugar se pretende una búsqueda y análisis de metodologías ya existentes, que puedan complementar la realización del trabajo.
- A continuación se establecerá un esquema de los diferentes entornos que pueden configurar la red de una empresa (Host, linux, Windows, etc) para tomarlo como base y tener un primer contacto con los diferentes servidores en estos entornos (servidores correo, web, aplicaciones, DMZ, etc.). En función de la actividad de cada máquina, se recogerá y analizarán los diferentes logs que puedan proporcionar, con una descripción de la información que aporta cada uno.
- La siguiente fase consiste en la "interrelación" de los registros proporcionados. Es este apartado donde se trabaja principalmente la metodología o forma de actuación. Se trata de determinar, si el "evento" o "tráfico" detectado como posible "anómalo" en uno de los servidores, se repite o se detecta de forma similar en cualquiera de los registros de otros servidores.
- Se establecen ejemplos de actuaciones ante una situación de alteración de seguridad y a través del modelo que se establezca, saber si afecta a la organización, detectar puntos vulnerables, máquinas afectadas o consecuencias de los servidores de la red.
- En el último capítulo se presentarán soluciones Software que se podrían utilizar en la implantación para la gestión de logs, así como la propuesta de Big Data como solución avanzada para esta gestión.

Capítulo 1: Contexto

1.1 Búsqueda de Metodologías, estudios y documentos sobre Gestión de Logs

Existen numerosos motivos por los que la generación, recogida, almacenamiento, análisis y gestión de logs, pueda ser una necesidad en las empresas. Tales motivos pueden ser legales, económicos, intención de resolución problemas, auditoría, estadísticas, respuesta ante incidentes y análisis forense, etc.
Nos vamos a centrar en este trabajo principalmente, en los registros que son realmente interesantes desde el punto de vista de la Seguridad de los Sistemas de información, es decir, todos aquellos ficheros que nos puedan proporcionar información sobre lo que ocurre en la red informática de la Organización, y conocer de esta forma, si ese tráfico que circula por la red es el deseado y no está amenazado por posibles fallos de configuración o vulnerabilidades, entre otros peligros.

1.1.1 Resultados de la búsqueda.

Los resultados de la búsqueda realizada sobre Metodologías de Gestión de Logs se pueden resumir en los siguientes grupos:

- Metodologías y tratados sobre guías o procedimientos de Centralización de logs, por ejemplo :
    - *Guía metodológica para la gestión centralizada de registro de eventos de seguridad en PYMES [4]*
    - *Centralización de Logs: Una experiencia real* [5]
- Herramientas que proporcionan los propios sistemas operativos, para poder recoger y centralizar los ficheros log del sistema, como por ejemplo la configuración de **syslog.**
- Documentos sobre la consideración de buenas prácticas de gestión de logs, tanto en el desarrollo de aplicaciones como en la actividad diaria de rotación, ubicación (tanto local como remota), almacenamiento, periodos de retención, etc. Dentro de este trabajo NO se van a considerar tales aspectos:

- *ITIL: Mejores prácticas en la Gestión de Eventos como base de la operación de servicios de TI [6]*

- Programas de monitorización y analizadoras de logs: en este apartado podemos incluir programas como Nagios, Patrol, Tívoli, con los que, configurando a través del protocolo snmp, se puede alertar a la organización de fallos y problemas en la instalación.
- Guías para evaluación de seguridad de sistemas:
  - *Guia para la Evaluación de Seguridad en un Sistema – Universidad de Pamplona [7]*
- Análisis forense y modos de recopilar información, entre los que se encuentran análisis de logs.
  - Guía de toma de evidencias en entornos Windows (Incibe)

1.1.2 Consideraciones

Se convierte este documento en una guía didáctica con el objetivo de unificar en un documento la mayoría de los registros posibles de los diferentes sistemas operativos y aplicaciones más comunes.

Se pretende recopilar todos los logs posibles de diferentes entornos para una primera aproximación de usuarios y organizaciones a conocer los registros que pueden obtener para analizarlo en caso necesario.

Los ficheros logs son información, y en muchas ocasionas muy valiosa, tanto para conocer lo que está pasando, lo que ha sucedido anteriormente y como veremos al final del documento, incluso intentar conocer que puede pasar en un futuro tratando la gestión de riesgos y la incertidumbre.

No se van a considerar en este documento, aspectos tales como buenas prácticas de gestión de logs atendiendo a niveles de rotación, ubicación (tanto local como remota), almacenamiento o periodos de retención, etc.

Capítulo 2: Identificación de ficheros logs

En este capítulo se identifican gran cantidad de ficheros, en los que se puede recoger y analizar información. Se van a identificar, atendiendo a su origen, clasificándolos de la siguiente manera:

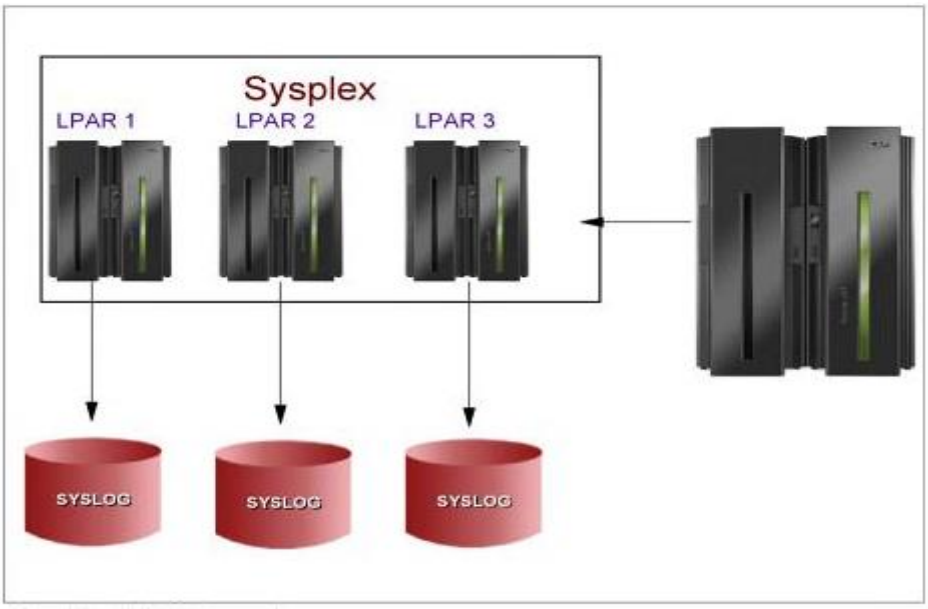
Clasificación según origen de ficheros logs

2.1 Logs de sistemas operativos y elementos de networking

2.1.1 HOST (Z/OS)

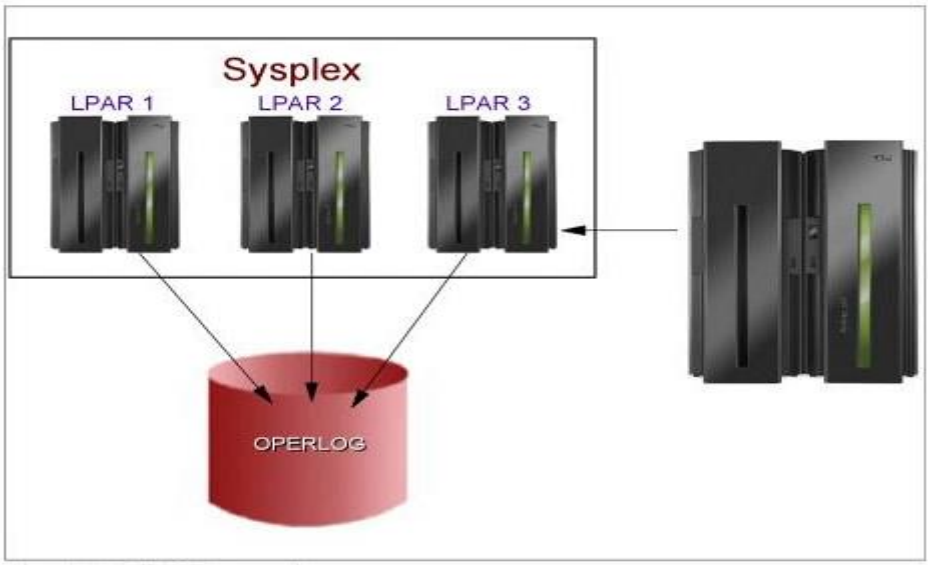
Es un entorno que en principio no presenta una amenaza grande en lo que en cuanto a vulnerabilidades y ataques se refiere, pero el conocimiento y análisis de los registros que se pueden recoger, pueden proporcionar información sobre problemas, intentos de accesos indebidos, errores de configuración ó tráfico extraño, etc.
Las fuentes principales de consulta y diagnósticos están contenidas en los mensajes proporcionados por el sistema en los siguientes registros:

- **Logs de la consola**: mensajes enviados a la consola, utilizados principalmente por los operadores. El sistema escribe en el "hard-copy" log todos los mensajes dirigidos a la consola, independientemente si el mensaje es representado en ella.
- **SYSLOG**: El sistema de log (SYSLOG) almacena mensajes y comando. Es la salida (SYSOUT) de un conjunto de datos proporcionados por el subsistema de entrada de Jobs. Una instalación debería imprimir el SYSLOG periódicamente para chequear si existen problemas. Puede ser utilizado por aplicaciones y programadores del sistema. El syslog consiste en lo siguiente:
    - Todos los mensajes publicados por macros WTL
    - Todos los mensajes introducidos por comandos del operador de LOG
    - Generalmente el log hard-copy
    - Cualquier mensaje dirigido al syslog desde cualquier componente o programa del sistema.



Proceso de SYSLOG

- **Job log:** mensajes enviados al Job log intencionadamente por los programadores al lanzar un job.
- **OPERLOG**: Los logs de Operación (OPERLOG) es una aplicación de registro de logs en un sistema MVS que registra y une mensajes sobre programas y funciones de cada sistema (el conjunto de mensajes hard copy) en un sysplex que activa OPERLOG.

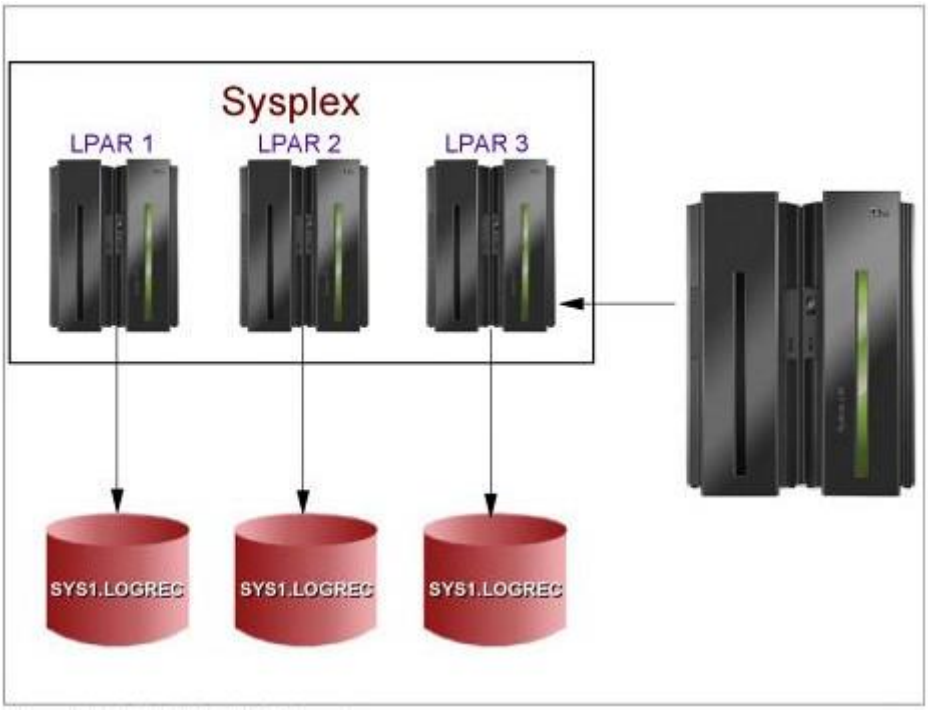


Proceso de OPERLOG

Se puede utilizar los logs de operaciones (OPERLOG) para registrar mensajes y comandos de todos los sistemas en un sysplex. El log de operaciones centraliza los datos del log en un sysplex.

- **Hard-copy log**: es un registro de todo el tráfico de mensajes del sistema:
  - Mensajes desde y para todas las consolas
  - Comandos y respuestas introducidos por el operador.

- **Logrec log**, es un aplicación de registros de log de MVS que recoge los fallos de hardware, errores de software seleccionados y condiciones del sistema seleccionados a través del sysplex.

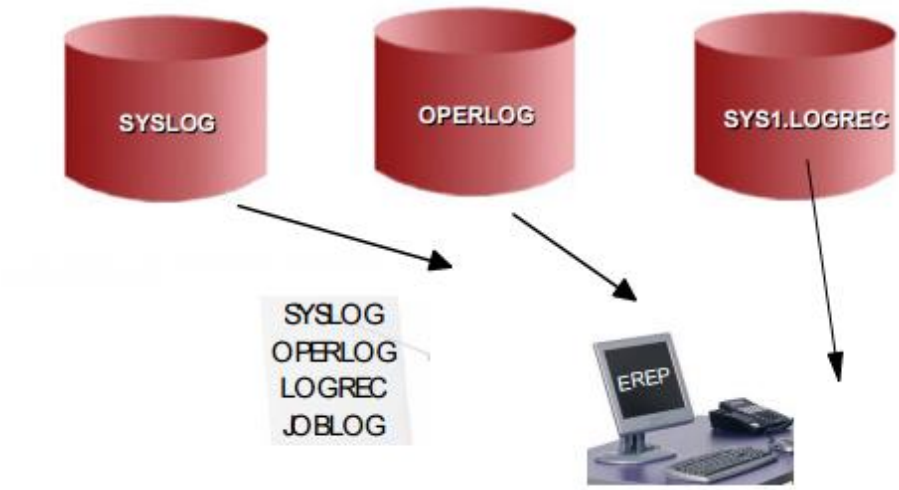


SYS1.LOGREC data sets

- **Job error logs:** Cada producto tiene su propio fichero de log en la plataforma Z/OS, que puede contener datos e información que puede aportar valor en el diagnóstico de un problema. Es particularmente importante mirar los eventos ya que puede predecir un fallo en muchas ocasiones.

REPORTES EREP (Environmental Record Editing and Printing Program)

EREP es un programa de diagnóstico que se ejecuta bajo sistemas operativos MVS, VM y VSE. El objetivo de EREP es ayudar al mantenimiento de la instalación.
Procesa los registros de error del sistema operativo con objeto de producir informes formateados, que pueden mostrar el estado de una completa instalación, subsistemas o de un dispositivo individual dependiendo del informe solicitado.



Proporciona información sobre el resultado errores de sistema o dispositivos, otros tipos de información y datos estadísticos. Se utiliza para determinar si existe un problema, de que se trata y donde localizarlo.

2.1.2 Linux – Unix

En un sistema UNIX, casi todas las actividades pueden ser en mayor o menor medida monitorizadas: accesos de usuarios, intentos fallidos de conexión, utilización de recursos, etc. Todo ello proporciona una gran ventaja para la seguridad, ya que se puede detectar usos indebidos en un tiempo relativamente corto, pero tiene el inconveniente de que puede llegar a ser complicado la gestión de esta información dado su volumen.

Por otro lado, la mayoría de estos ficheros, son ficheros planos que se pueden visualizar de forma sencilla lo facilita su lectura por parte del administrador del sistema, pero también facilítalo tenga muy fácil para modificar esos ficheros.
El sistema de logs en este entorno, se basa en dos "daemon" que gestionan los logs del sistema y se encargan de recoger los mensajes generados por los programas. En estos registros figura el programa fuente que genera el mensaje, el nivel de gravedad, fecha y hora.

Los niveles de prioridad de la información que se aporta son: debug, info,notice, warning, warn, err, error, crit, alert, emerg y panic) y los tipos de mensajes (auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, security , syslog, user, uucp y localo-local7). [8]

El objetivo de la siguiente exposición es mostrar a modo de orientación, la cantidad de ficheros de los que se puede extraer información. Quiero señalar que el nombre y la localización del fichero, dependerá en muchas ocasiones de la versión de LINUX/UNIX con la que estemos trabajando.

Archivos de registro comunes (pueden variar según la distribución):

La carpeta «/var/log/», contiene toda la lista de archivos *logs* del sistema operativo. Podemos ver que se escribe en cada uno de estos archivos leyendo el fichero de configuración «/etc/rsyslog.conf».
Aunque muchos programas manejan sus propios logs y los guardan en /var/log/<programa>. Además, es posible especificar múltiples destinos para un mismo mensaje.
Conclusión, en /var/log se almacenan todos los registros del sistema. No obstante, algunas aplicaciones como httpd incluyen ahí dentro un subdirectorio en el que almacenan sus propios archivos de registro.

- **syslog** es quizá el fichero log más importante del sistema, localizado en /var/adm ó /var/log. Se guardean mensajes relativos a la seguridad de la máquina,
- /var/log/**messages** ó /var/adm/**messages** registro de mensajes generales del sistema. Contiene mensajes del sistema en general, incluyendo los del inicio del mismo. Incluye trazas de mail, cron, kern, auth, y muchísimos más. Es uno de los

más importantes y que más información tienen. Encontraremos los logs que llegan con prioridad info (información), notice (notificación) o warn (aviso).

- /var/log/**auth.log**: log de autenticación. En este log se registran los login en el sistema, las veces que hacemos su, etc. Los intentos fallidos se registran en líneas con información del tipo invalid password o authentication failure. Conexiones al sistema incluidos los intentos fallidos y los accesos como root. Autorizaciones que hace el sistema, logins de usuarios y de software. Información sobre eventos de autenticación de usuarios.
- /var/adm/**sulog: s**e registran las ejecuciones de su, indicando fecha, hora, usuario que lanza el programa y usuario cuya identidad adopta, terminal asociada indicando si ha sido realizado con éxito o no.
- /var/log/**kern.log**: registro del kernel. Información que proporciona el kernel. Ayuda para arreglar problemas relacionados.
- /var/log/**cron.log**: registro de crond
- /var/log/**maillog**: registro del servidor de correo
- /var/log/**qmail/** : registro de Qmail
- /var/log/**httpd/**: registro de errores y accesos a Apache
- /var/log/**lighttpd**: registro de errores y accesos a Lighttpd
- /var/log/**boot.log** : registro de inicio del sistema
- /var/log/**mysqld.log**: registro de la base de datos MySQL
- /var/log/**secure**: log de autenticación. Información relacionada con autenticación y privilegios incluidos del SSH. SSH usa el **/var/log/secure** y nos será de una grandísima ayuda para saber por ejemplo si el fallo viene de que el usuario pone la contraseña mal o un intento de sudo indebido.
- /var/log**/utmp** or /var/log**/wtmp** : registro de logins. o utiliza el comando “who” para indicarnos quien está conectado, información relativa a cada conexión y desconexión al sistema, con información de usuarios conectados.
- /var/adm/**loginlog:** en algunas versiones de Unix (como Solaris), si creamos el archivo loginlog, cuando se produzcan cinco o mas intentos seguidos se registrarán en él.
- **/var/log/dmesg**: en este archivo se almacena la información que genera el kernel durante el arranque del sistema. Cuando el sistema arranca escribe aquí cada error que se produzca por ínfimo que sea sobre el hardware que detecta el kernel, Podemos ver su contenido con el comando dmesg.

- **/var/log/daemon.log –** información de varios daemons en segundo plano que funcionan en el sistema.
- **/var/log/rpmpks –** Contiene información cuando un paquete RPM es instalado o removido.
- **/var/log/Xorg.0.log –** Mensajes de las X. Información sobre el entorno gráfico. Registro del sistema X, primera pantalla (1, para el segundo, etc.).
- **/var/log/cups** Todos los mensajes relacionados con el sistema de impresión
- /var/log/**lastlog**: muestra para cada usuario cuando fue la última vez que entró en el sistema.
- /var/log/**btmp**: Intentos de ingreso fallidos.
- **/var/log/anaconda.log**. Todos los mensajes relacionados con la instalación del sistemas
- **/var/log/faillog** – Contiene intentos fallidos de login, se usa con el comando faillog para ver los resultados.
- **/var/log/yum.log** Información de los paquetes instalados con yum
- **/var/log/debug:** Información de depuración de los programas
- **/var/log/fontconfig.**log: Configuración de las fuentes del sistema
- **/var/log/samba** En este directorio se almacenan los logs relacionados con el servicio *samba*, el cual permite conectar equipos Windows con Linux

Otros logs de interés:

- El archivo «/etc/sudoers», indica qué usuarios pueden ejecutar comandos como administrador (mediante los comandos «su» o «sudo»).
- El archivo «.bash_history», el cual se encuentra en la carpeta del usuario y almacena el historial de comandos ejecutados en la consola del equipo.
- La carpeta «/var/spool/cron/crontabs» en la cual se almacenan las tareas programadas de cada uno de los usuarios del sistema.
- /var/adm/debug: información de depuración (de *debug*) de los programas que se ejecutan en la máquina; puede ser enviada por las propias aplicaciones o por el sistema operativo.
- X11 - Sistema X Windows: /usr/bin/X11/xauth: recoge errores de autenticación-

- X11 - Los logs de Xorg se localizan en /var/log/Xorg.x.log: información de cada dispositivo al que el servidor X11 se conecta.

Logs en el entorno gráfico:

En el entorno gráfico hay varias aplicaciones para monitorizar logs:

- **KSystemLog** (paquete ksystemlog): monitor de logs de KDE.
- **GNOME-System-Log** (paquete gnome-utils): monitor de logs de GNOME.
- **Xlogmaster** (paquete xlogmaster): monitor de logs del GNU.
- **Xwatch** (paquete xwatch): monitor de logs para las X.

Para terminar, en esta relación de ficheros logs, se deberá tener en cuenta los posibles "logs remotos" y "registros físicos" que puedan estar configurados en la organización.

2.1.3 Windows

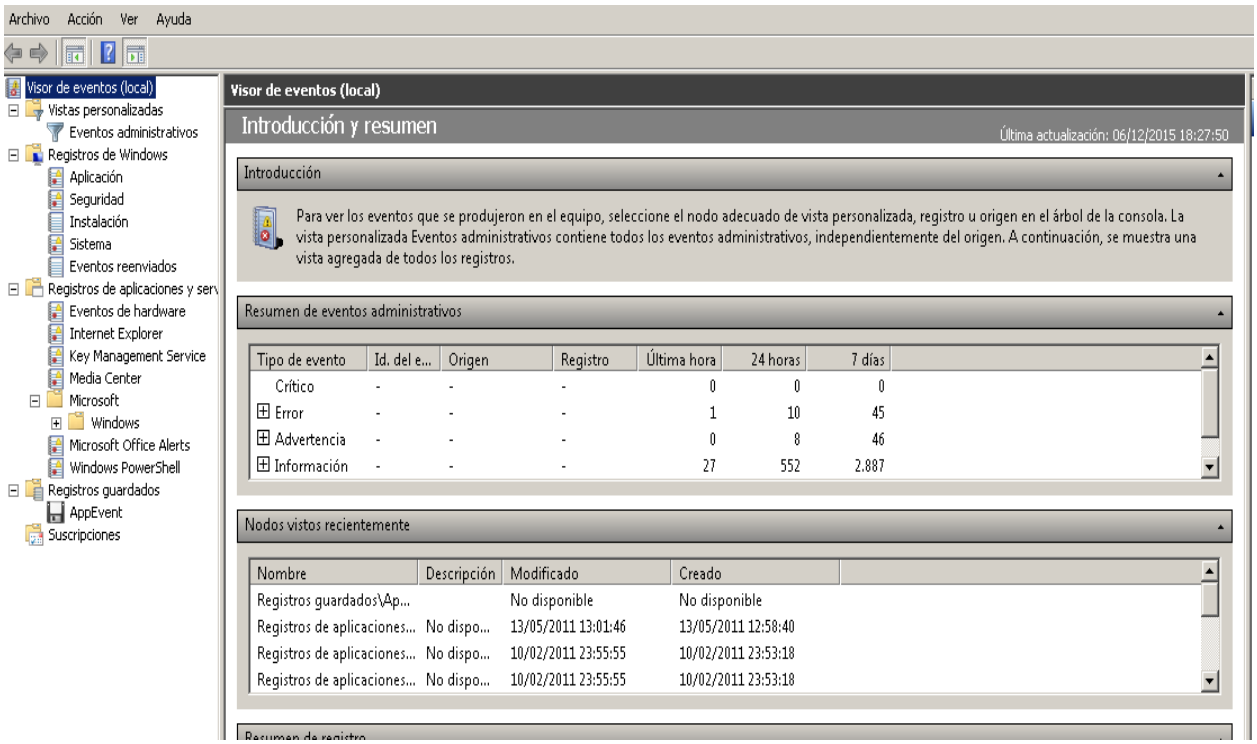
Cuando se busca información sobre registros en Windows, lo primero que se presenta son los registros de eventos y Visor de eventos.
Los registros de eventos son archivos especiales que registran los eventos importantes que tienen lugar en el equipo, como por ejemplo, cuando un usuario inicia una sesión en el equipo o cuando se produce un error en un programa. Siempre que se producen estos tipos de eventos, Windows los va incluyendo en un registro de eventos que se puede leer mediante el Visor de eventos.
En el Visor de eventos, la información se organiza en diversos registros. Los registros de Windows incluyen:

- **Eventos de aplicaciones (programas).** Cada evento se clasifica como **error**, **advertencia** o **información**, dependiendo de su gravedad. Un error es un problema importante, como una pérdida de datos. Una advertencia es un evento que no es importante necesariamente, pero puede indicar la posibilidad de

problemas en el futuro. Un evento de información describe la operación correcta de un programa, un controlador o un servicio.

- **Eventos relacionados con la seguridad.** Estos eventos se conocen como **auditorías** y se describen como correctos o con error, dependiendo del evento, como por ejemplo, si un usuario consigue iniciar una sesión en Windows correctamente.
- **Eventos de configuración.** Los equipos que se han configurado como controladores de dominio dispondrán de más registros aquí.
- **Eventos del sistema.** Los eventos del sistema los registran Windows y los servicios del sistema de Windows, y se pueden clasificar como error, advertencia o información.
- **Eventos reenviados.** Estos eventos se reenvían a este registro desde otros equipos.

Los registros de aplicaciones y servicios pueden variar. Incluyen registros independientes para los programas que se ejecutan en el equipo, así como registros más detallados relacionados con servicios específicos de Windows.



Pantalla del Visor de Eventos

Archivos Log del sistema

Los sistemas Windows basados en NT tienen su principal fuente de Log en los archivos de sistema siguientes:

- SysEvent.Evt. Registra los sucesos relativos al sistema
- SecEvent.Evt. Registra los sucesos relativos a la seguridad
- AppEvent.Evt. Registra los sucesos relativos a aplicaciones

En Windows XP Estos ficheros se encuentran en el directorio **%systemroot%\system32\config**.
En Windows 7/8 están ubicados en %systemroot%\system32\winevt\Logs

Para visualizar estos ficheros podremos utilizar la herramienta de Windows **eventvwr.msc**, comúnmente llamada Visor de Sucesos. Abriremos con esta herramienta el archivo SecEvent.Evt, que es el encargado de almacenar los sucesos

relativos a la seguridad, tales como ingresos en la máquina, cambio de directivas, etc... Por ejemplo, podríamos buscar todo acceso físico a la máquina, cambio de directivas y creación de cuentas de usuario.

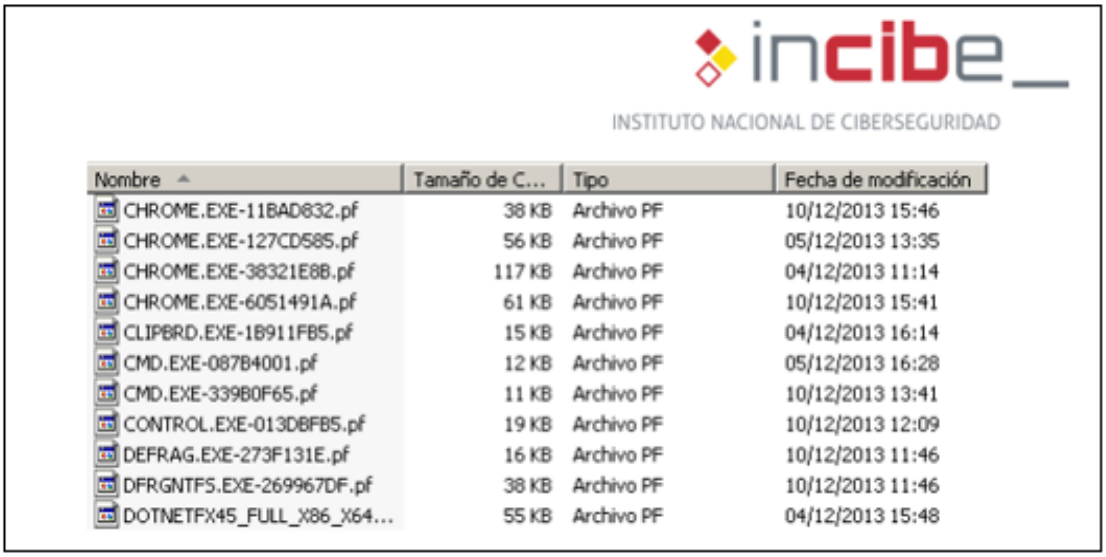
Otros ficheros de interés:

WindowsUpdate.log El fichero WindowsUpdate.log, ubicado en la carpeta %WinDir%, almacena el listado de actualizaciones correspondientes al sistema operativo que se han llevado a cabo en el equipo

Pfirewall.log El fichero pfirewall.log, ubicado en la carpeta %WinDir% (Windows XP) y en %WinDir%\System32\LogFiles\Firewall (Windows 7/8), almacena diferente información correspondiente al firewall de Windows como por ejemplo paquetes perdidos o conexiones que se han realizado correctamente.

Carpeta prefetch. Cada vez que enciende el equipo, Windows realiza un seguimiento de la forma en que se inicia el equipo y los programas que se abren habitualmente. Windows guarda esta información en una serie de pequeños archivos en la carpeta Prefetch. La próxima vez que encienda el equipo, Windows recurrirá a estos archivos para acelerar el proceso de inicio.

Se pueden visualizar accediendo a la carpeta %WinDir%\Prefetch, en la siguiente ilustración.



Nombre	Tamaño de C...	Tipo	Fecha de modificación
CHROME.EXE-11BAD832.pf	38 KB	Archivo PF	10/12/2013 15:46
CHROME.EXE-127CD585.pf	56 KB	Archivo PF	05/12/2013 13:35
CHROME.EXE-38321E8B.pf	117 KB	Archivo PF	04/12/2013 11:14
CHROME.EXE-6051491A.pf	61 KB	Archivo PF	10/12/2013 15:41
CLIPBRD.EXE-1B911FB5.pf	15 KB	Archivo PF	04/12/2013 16:14
CMD.EXE-087B4001.pf	12 KB	Archivo PF	05/12/2013 16:28
CMD.EXE-339B0F65.pf	11 KB	Archivo PF	10/12/2013 13:41
CONTROL.EXE-013DBFB5.pf	19 KB	Archivo PF	10/12/2013 12:09
DEFRAG.EXE-273F131E.pf	16 KB	Archivo PF	10/12/2013 11:46
DFRGNTFS.EXE-269967DF.pf	38 KB	Archivo PF	10/12/2013 11:46
DOTNETFX45_FULL_X86_X64...	55 KB	Archivo PF	04/12/2013 15:48

Contenido Carpeta Prefetch

Papelera de reciclaje Es posible obtener información de los elementos eliminados que hayan sido enviados a la papelera de reciclaje. Para ello se debe de tener en cuenta la siguiente tabla:

Sistema operativo	Localización
Windows XP	%SystemDrive%\Recycler
Windows 7/8	%SystemDrive%\$Recycle.Bin\

2.1.4. Elementos de Networking

Routers - Switches

Los routers pueden registrar información sobre una variedad de eventos, muchos de los cuales son importantes en lo referente a la seguridad. Estos son los tipos principales de registración usados por los routeres de Cisco:

- El AAA registrar-Recoge la información sobre las conexiones de acceso telefónico del usuario, los logines, los accessos del HTTP, las modificaciones del nivel de privilegio, los comandos ejecutados, y los acontecimientos similares.
- El SNMP trap registrar-Envía las notificaciones de los cambios importantes en el estado del sistema a las estaciones de la administración de SNMP.
- El sistema registrar-Registra una diversidad de eventos grande, que depende de la configuración del sistema. Los acontecimientos del registro del sistema se pueden señalar a una variedad de destinos, que incluyen éstos:

- El puerto de consola del sistema (**logging console**): por defecto el router envía todos los mensajes a la consola. Solo los usuarios conectados a la consola pueden verlos.
- Servidores que utilizan el protocolo del registro del sistema UNIX (**logging ip-address, logging trap**).
- Sesiones remotas en los VTY y sesiones locales en los TTY (monitor de inicio de sesión, monitor de terminal).
- Un búfer de registro en RAM de router (almacenamiento en búfer de registro).
- **Syslog Server logging** : Se puede utilizer syslog para reenviar los mensajes a un server syslog externo**.**
- **SNMP trap logging:** El router puede utilizr SNMP traps para enviar mensajes a un SNMP servidor

Desde el punto de vista de la seguridad, los eventos más importantes que normalmente se graban en el registro del sistema son los cambios de estado de interfaz, los cambios en la configuración del sistema, las coincidencias de listas de entrada y los eventos detectados por el firewall óptico y las funciones de detección de intrusos.

Cada acontecimiento del registro del sistema es etiquetado con un nivel de urgencia. Los niveles se extienden de la información de depuración (en la mínima urgencia), a las emergencias importantes del sistema. Cada destino de registro se puede configurar con una urgencia del umbral, y recibe los eventos de registro solamente en o sobre ese umbral. [8]

Si se utilizan listas de acceso, y se registran, se puede también utilizar para registrar el tráfico sospechoso y caracterizar el tráfico asociado a los ataques a la red. Al filtrar tráfico, se puede recoger paquetes que violan los criterios de filtrado.

Syslog Server

Cisco tiene la desventaja que luego de reiniciar el router/switch se pierden los logs del mismo, esto trae como consecuencia perdida de información por ejemplo de cuando

levanta/cae una sesión eigrp, bgp, estado de las interfaces, etc. Por ello recomiendo tener un syslog server externo (tal como syslog server ng en Linux) compilar los logs de tus equipos.

Mensajes de registro del router:

Nivel	Nombre Nivel	Mensajes Router
0	Emergencias	Sistema de cierre debido a que falta la bandeja de ventiladores
1	Alertas	Supera el límite de temperatura
2	Crítico	Errores de asignación de memoria
3	Errores	Interfaz de mensajes / Abajo
4	Advertencias	El archivo de configuración escrito al servidor, mediante solicitud SNMP
5	Notificaciones	Línea protocolo de arriba / abajo
6	Información	Access-list violación tala
7	Depuración	Mensajes de depuración

System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured. For more information, see the "Enabling and Disabling Sequence Numbers in Log Messages" section.
timestamp formats: *mm/dd hh:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (long uptime)	Date and time of the message or event. This information appears only if the **service timestamps log [datetime | log]** global configuration command is configured. For more information, see the "Enabling and Disabling Time Stamps on Log Messages" section.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 29-4.
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 29-3.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

2.2 Servicios / Aplicaciones

El intentar abarcar los diferentes logs que se generan en las aplicaciones que pueden instalarse en una organización, sería una tarea muy extensa y tediosa, y que en

definitiva terminaría con un listado de nombres de ficheros de logs, que no considero pueda resultar muy útil.

Me parece importante presentar los diferentes servicios que se pueden tener configurados, y que hay que tener en cuenta a la hora recoger los ficheros que nos puede aportar información.

Se van a nombrar a continuación una serie de servicios o aplicaciones que pueden ser más comunes, pero se deja a criterio de las organizaciones, el ampliar, reducir o modificar la lista que se presenta. Lo importante es conocer, los servicios que se prestan y asimismo, conocer de antemano los ficheros que nos pueden aportar información (en este caso de seguridad), para tratarlos o analizarlos en caso necesario.

2.2.1 Logs de Aplicaciones de Seguridad

Son una parte muy importante de la información a recoger y tratar en aspectos de seguridad. Los datos y registros que se aporten dependerá de la ubicación que tenga cada elemento en la red. Son datos muy importantes y se deben investigar y cruzar entre ellos con objeto de obtener la máxima información, especialmente para conocer el tráfico de la red y evitar posibles vulnerabilidades y amenazas.

Dado que existen muchos programas comerciales, no se identificarán ficheros de logs concretos; la recomendación es localizar en cada caso los ficheros que registran el tráfico o la actividad del programa instalado.

- Firewall

Los firewalls son elementos de hardware o software que se utilizan para rechazar o aceptar determinadas comunicaciones en las redes y proteger así ordenadores o redes. A lo largo de tiempo han ido evolucionando, pero a modo de resumen vamos a nombrar solo los firewalls de capa de red o filtrado de paquetes y los firewalls de capa de aplicación.

Cualquiera que sea el tipo de firewall instalado, dispondrá los ficheros logs correspondientes a la propia máquina o sistema operativo, pero además dispondrá de ficheros donde se registre toda la actividad y eventos de la red que defiendan y del

firewall. Son ficheros muy importantes en los que debe conocerse la información que aportan y monitorizarlos. Los propios firewalls, nos conducen a través de sus Guías a estos ficheros y alguno de ellos dispone de herramientas para su visualización.
Son datos muy importantes, entre los que se encuentran direcciones Ip origen, direcciones IP destino, protocolos, puertos origen y destino, Urls accedidas, aplicaciones o servicios utilizados, etc.

- Antivirus/Antimalware

Los Antivirus realizan "scaneos" en los ordenadores presentando todas las irregularidades encontradas en estos análisis. Los registros de estos programas nos mostrarán las posibles amenazas e infecciones que se hayan realizado en los ordenadores. Deben analizarse y controlar sus distribuciones, versiones y actualizaciones. Es importante recoger todos los logs y analizarlos en función de la información que puedan aportar, ya que puede ser muy valiosa, para una detección temprana de fallos de seguridad.

- IDS

Son sistemas de detección de intrusiones cuya finalidad generalmente es analizar el tráfico de red y detectar anomalías, ataques, accesos no autorizados, actividades maliciosas, etc. Se debe analizar los diferentes logs del IDS ya que el tráfico que registran alerta de potenciales brechas de seguridad.

- Proxy / proxy Inverso

Proxy es un servidor que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor, y en caso de proxy inverso, recoge todo el tráfico que tiene su origen por ejemplo en internet y lo dirigen a un servidor web, interno de la Organización.
Estos servidores proporcionan otra capa de seguridad y sus registros son también de interés.

- Servicios de Registros
    - Kerberos

  - LAN Manager Authentication
- Servidor de Autenticación
- VPN

Se puede seguir enumerando elementos de seguridad que puede adoptar una Organización con sus correspondientes logs, pero acabaría siendo una lista exhaustiva y en cierto modo, nada práctica.

Lo importante es tener en cuenta que cualquier programa/elemento de seguridad con el que se trabaje, va a aportar una información, en principio nada despreciable, que nos puede ser muy útil para una actividad de seguridad tanto proactiva como reactiva.

2.2.2 Logs del Servicio de Correo

Los ficheros logs de los servidores de correo pueden aportar información sobre el origen y destino de los mensajes:

- Dirección del Remitente
- Dirección del Destinatario
- IP remitente
- IP Destinatario
- Fechas de los mensajes
- ID del Mensaje

Si tenemos en cuenta los servidores de Unix/Linux, estos ficheros los encontraremos generalmente en el directorio /var/log/ ó /var/adsy suelen ser de tipo mail.log. Hay que recordar que el fichero syslog.conf nos dará la localización exacta de este fichero log si estuviera configurado.

Ejemplos de servidores de correo:

- Microsoft Outlook:
  - Archivos de datos: .pst
  - Archivos de datos sin conexión: .ost
  - Libreta Personal de direcciones: .pab
  - Libreta de direcciones sin dirección: .oab

Se encontrarán bajo directorios como:

- Documentos\Archivos de Outlook
- %UserProfile%\AppData\Local\Microsoft\Outlook
- Documents and Settings\usuario\Configuración local\Datos de programa\Microsoft\Outlook

- Servidor Correo Lotus Notes

  Ficheros logs:

  - Log.nsf

    Registra la actividad del servidor y proporciona información detallada sobre las bases de datos y usuarios del server.

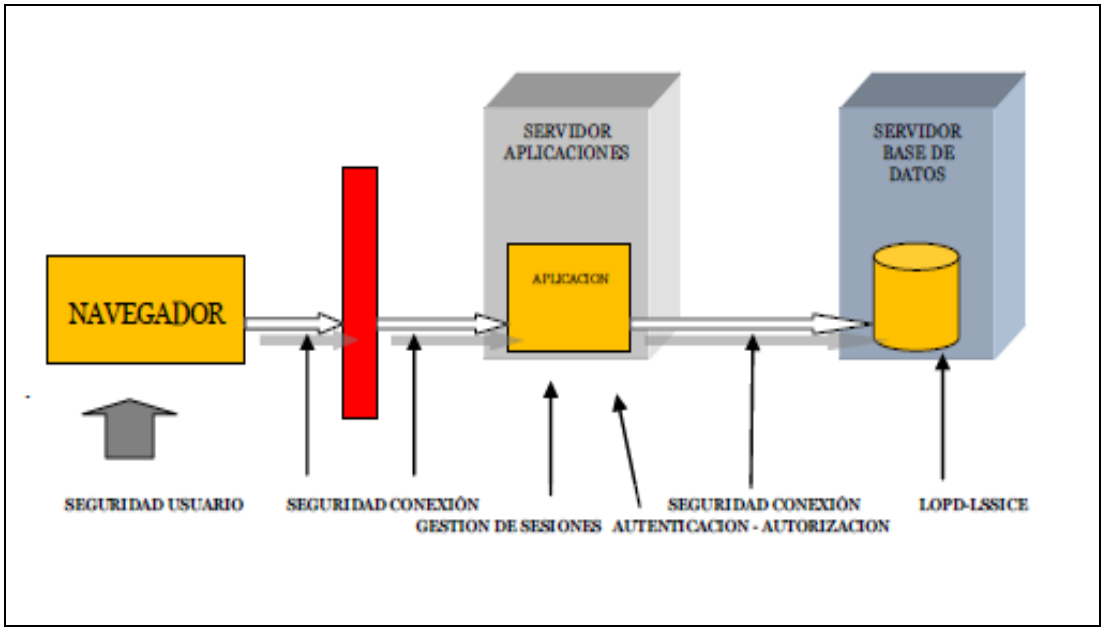
- Servidor Exchange:
  - Exchange transaction Log:

    Recoge los registros de los cambios que se realizan en la base de datos.

- Logs de programas de mensajería como Skype.

En este apartado, hay que destacar, la importancia por parte de la organización de la adecuación a la normativa legal, referente al análisis y gestión de la información, en concreto a la Ley de Servicios de la Sociedad de Información (LSSI) y la Ley Orgánica de Protección de datos (LOPD).

2.2.3 *Logs de Servidores de Aplicaciones*



Arquitectura de Seguridad de Aplicaciones Web{10]

Un servidor de aplicaciones a un servidor en una red de ordenadores que ejecuta ciertas aplicaciones, proporciona servicios de aplicación a los clientes. Un servidor de aplicaciones generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negocio y de acceso a los datos de la aplicación. [11]

Algunas de las implementaciones más utilizadas son las siguientes [12]:

- BEA WebLogic
- IBM WebSphere
- Sun-Netscape IPlanet
- Sun One
- Oracle IAS
- Borland AppServer
- HP Bluestone

Si tomamos como ejemplo IBM WebSphere:

1. Login en el servidor de aplicaciones

2. Menu de pantalla izquierdo; **Servers > Server Types** > **Websphere application servers** link.

   Elegir nombre del servidor

3. Sección **Troubleshooting** section, seleccionar **Logging and tracing** l

4. En la pantalla **General Properties**, seleccionar **JVM Logs**:

Cada servidor de aplicaciones indicará la ubicación de los ficheros de registros con objeto de poder analizar posibles errores.

2.2.4 Otros Servicios

En este apartado relaciono diferentes servicios que deben ser considerados a la hora de la recopilación y análisis de logs. Dependerá de los sistemas de información de la organización y de la actividad de ésta el tener establecidos estos servicios.

- **Servidores Web**

Es necesario registrar la actividad y rendimiento de los servidores web, tanto errores o problemas que pudieran ocurrir, como el registro de la actividad que por pase a través de él.

- **Apache**
  - El registro de errores del servidor, es el más importante de todos los registros. Apache enviará cualquier información de diagnóstico y registrará cualquier error que encuentre al procesar peticiones al archivo de registro seleccionado
  - Registro de Acceso: El servidor almacena en el registro de acceso información sobre todas las peticiones que procesa. La ubicación del fichero de registro y el contenido que se registra se pueden modificar
  - Registro de actividad de scripts (Script Log) permite guardar la entrada y la salida de los scripts CGI.

- **IIS**
- **Tomcat**
- **Cherokee**
- **Webfsd**

- **Bases de Datos:**

  - **Oracle**

Component	*Location*
Enterprise Manager	*ORACLE_HOME*/sysman/log
Forms	*ORACLE_HOME*/j2ee/OC4J_BI_FORMS/application-deployments/formsapp/*island*/application.log
HTTP Server	*ORACLE_HOME*/Apache/Apache/logs/error_log.*time*
InterConnect	*ORACLE_HOME*/oai/10.1.2/adapters/*adapter_name*/logs
Integration B2B	*ORACLE_HOME*/ip/log
BPEL Process Analytics	*ORACLE_HOME*/integration/bam/log
Log Loader	*ORACLE_HOME*/diagnostics/logs
OC4J *instance_name*	*ORACLE_HOME*/j2ee/*instance_name*/log *ORACLE_HOME*/j2ee/*instance_name*/application-deployments/*application_name*/application.log
OCA	From the command line, for administrator use only, messages are stored at: *ORACLE_HOME*/oca/logs/admin.log Logging for user and administrator usage, other than command line, is stored in the database and accessed through the Oracle Application Server Certificate Authority (OCA) Administrator web interface.
Oracle Internet Directory	*ORACLE_HOME*/ldap/log
OPMN	*ORACLE_HOME*/opmn/logs *ORACLE_HOME*/opmn/logs/*component_type*~...
Port Tunneling	*ORACLE_HOME*/iaspt/logs
Reports Server	*ORACLE_HOME*/reports/logs
Single Sign-On	*ORACLE_HOME*/sso/log
Universal Installer	*ORACLE_HOME*/cfgtoollogs
Web Cache	*ORACLE_HOME*/webcache/logs
Wireless	*ORACLE_HOME*/wireless/logs

Mensajes componentes de Oracle[13]

  - **DB2** (herramienta db2diag fichero db2diag.log)
  - **SQL Server**
  - Etc.

- Servidor de archivos
- Servidor FTP
- Servidor DHCP
- Servidor NTP: logfile /opt/ntp/ntp.log - /var/log/messages and /var/log/syslog
- Servidor DNS
- Servicios Impresión
- Acceso remoto: Utilidades de acceso remoto como WinVNC, pcAnywhere, etc.
- Virtualización
- Alta Disponibilidad

Cada organización, tiene sus propias características y actividad, y a estos servicios se podrán añadir otros como VoIp, sistemas de Radio y Telecomunicaciones, telefonía móvil, etc.

Todos los programas proporcionan ficheros log que deberemos conocer para analizar si nos puede interesar la información que registran o despreciarla en su caso, pero es interesante señalar la importancia por parte de los administradores de sistemas de conocerlos y analizarlos.

2.2.4 Sistemas de Monitorización

Disponer de un buen sistema de monitorización, especialmente aquellas instalaciones de gran número de sistemas, gran diversidad de servicios que se ofrecen ó dispersos geográficamente ayuda en gran medida a las organizaciones.

Un sistema de monitorización, es un programa cuyo objetivo es comprobar el correcto estado, funcionamiento y disponibilidad de los sistemas, servicios y redes, por ejemplo, servicios web, impresoras, routers, etc.).

Nagios, Patrol, Tivoli, son tres de los más conocidos sistemas de monitorización. Sus registros pueden ser muy valiosos para el conocimiento del estado de los sistemas y de la red.

Capítulo 3: Descripción de la metodología

En las grandes organizaciones, los departamentos de los sistemas de información o las áreas de informática, tienen en muchas ocasiones programas que monitorizan la red, personal especializado y dedicado a programas de seguridad, administradores de sistemas, etc. Este no suele ser el caso de las pequeñas y medianas empresas, en el que los departamentos de informática, no suelen contar con gran cantidad de personal, y muchas ocasiones esta actividad es objeto de subcontratación.

El objetivo de este trabajo, es subrayar la importancia de la información que aportan los ficheros logs de los diferentes programas y aplicaciones, y cómo el conocimiento de esta información, por parte de las organizaciones, puede ayudar en un periodo corto de tiempo, a identificar, entre otros, un problema de seguridad.

Como se verá en capítulos posteriores, existen herramientas y programas que facilitan esta actividad, pero es importante recalcar la importancia de conocer la relación de ficheros de los sistemas informáticos y la información que incluyen, o simplemente conocer que de cualquier programa se debe buscar los ficheros que recogen datos de auditoría sobre la actividad en ese programa, es ya un paso importante, para la administración de los sistemas.

Las actividades que se deben desarrollar para poner en práctica esta metodología son:

1.- Conocimiento de todos los elementos que forman los sistemas informáticos, tanto a nivel de software (programas y aplicaciones) como de hardware.

2.- Inventario de servidores, ordenadores de usuarios, elementos de networking, etc.

3.- Recopilación y análisis de todos los ficheros de registros que proporcionan los programas y aplicaciones.

4.- Clasificación de los ficheros analizados en función del origen y contenido.

5.- Acceder diariamente a páginas de información sobre seguridad informática.

6.- Comprobación si el fallo de seguridad puede afectar a la organización o no.

7.- En caso positivo, analizar logs de programas y realizar las acciones necesarias para solucionar el problema.

En este documento no se van a tratar los dos primeros apartados, ya que cada organización tendrá características muy diferentes en función de actividad, y sobre la recopilación y análisis, se ha tratado de una manera amplia en el capítulo 2 de este documento, y nos proporciona una idea de la enorme cantidad de ficheros e información que se pueden recoger.

A partir de ahora se describirá principalmente el esquema de actuación ante una sospecha o evidencia de vulnerabilidad, fallo de seguridad, etc. y el análisis y detección de máquinas y servicios que pudieran ser afectados.

Se indican varias URLs donde la información de últimas vulnerabilidades y avisos de seguridad se actualiza constantemente:

1.- www.cert.org

2.- www.incibe.es

3.- https://technet.microsoft.com/es-es/

Esta breve lista es orientativa. Existen otras páginas donde aparece este tipo de información. Lo importante es saber que existen, conocerlas y establecer la "rutina" de acceder a ellas para estar al día de la información y poder tomar las acciones adecuadas en caso necesario.

3.1 Métrica y Tipos de logs

En este apartado se va a definir las métricas con las que se van a clasificar los archivos. Con cada fichero log que se identifique, se debe en primer lugar, buscar y analizar la información que contiene. Así, le corresponderá una de las siguientes clasificaciones de cada tabla:

- **Primera clasificación**, en principio obvia, se realiza en función del **origen del fichero log,** es decir, teniendo en cuenta el origen de los ficheros: servidores ó networking.

1.- Sistema Operativo 1.1 Z/os 1.2 Linux – Unix 1.3 Windows 1.4 ……..	2.- Networking 2.1 Routers 2.2 Switches 2.3 ……

- **Segunda clasificación**: Bases de Datos/Programas/Aplicaciones

3.- Bases de Datos 3.1 Oracle 3.2 DB2 3.3 Microsoft Access 3.4 …….

4.- Aplicación/Servicio Sist. Informáticos 4.1 Servicio Web 4.2 Servicio Correo 4.3 Servidor de Archivos 4.4 Servidor de Impresión 4.5 Servicio NTP 4.6 Virtualización 4.7 Servicio de Monitorización 4.8. Aplicación de desarrollo 4.9 Servicio DHCP 4.10 Servicio DNS 4.11 Servidores de Aplicaciones 4.12 ……	5.- Aplicación/Servicio específicas de la Empresa 5.1 Contabilidad 5.2 Inventario 5.3 Almacén 5.4 Gestión 5.5 Pedidos 5.6 Nóminas 5.7 ……..

6.- Programa/Servicio Seguridad 6.1 Firewall 6.2 Proxy 6.3 Proxy Inverso 6.4 LDAP 6.5 IDS	6.7 IPS 6.8 Servidor autenticación 6.9 VPN 6.10 …...

- **La Tercera clasificación** se realizará en función del **tipo de información** de los datos que alberguen los ficheros log:

A.- Información de RED (Direcciones IP, Accesos a red, Protocolos, Direcciones MAC, puertos, Gateways, etc.

B.- Información de usuarios (accesos, cuentas, creación, modificación, eliminación, etc.)

C.- Eventos del sistema, Errores, Diagnósticos, configuración, alertas, etc.

D.- Registros propios de servicios informáticos (ftp, Schedulers, Backups, Restore, sudo etc)

E.- Eventos y registros de programas/aplicaciones específicos de la empresa como Contabilidad, nóminas, inventario, etc.

F.- Cualquier otro tipo de información que pueda ser interesante para la organización.

Esta clasificación debe realizarla la organización de manera minuciosa y lo más completa posible. Se identificará cada programa utilizado y el nombre del fichero log con la información que contenga, para proceder a su clasificación.
Todo fichero log registrado, que se considere en la organización debe tener una entrada en las tres clasificaciones, a excepción de los ficheros propios de sistemas operativos que solo tendrán en la primera y última.

Ejemplos de clasificación de logs:

a) **Fichero "db2diag.log":**

a.1.) Búsqueda de información: Fuente:

https://db2technologyblog.wordpress.com/2013/04/22/monitorizacion-de-base-de-datos-ibm-db2/

El log de DB2 está en /home/db2inst1/sqllib/db2dump/db2diag.log (o su equivalente en la ruta de la instancia en Windows). Lo ponemos consultar directamente o mediante el

comando db2diag y nos dará mucha información sobre crashes, modificación de valores de memoria, bloqueos, etc.

a.2.) Clasificación

Primera clasificación → **1.1 Linux**

Segunda clasificación → Base de Datos: **3.2 DB2**

Tercera clasificación → Diagnósticos: "**C" Eventos, errores, Diagnósticos, etc**

b) **DHCP Server log file**:

b.1) Búsqueda de información: Fuente

https://technet.microsoft.com/es-es/library/dd183591(v=ws.10).aspx

Formato del fichero log:

Field	Description
ID	A DHCP server event ID code.
Date	The date on which this entry was logged on the DHCP server.
Time	The time at which this entry was logged on the DHCP server.
Description	A description of this DHCP server event.
IP Address	The IP address of the DHCP client.
Host Name	The host name of the DHCP client.
MAC Address	The media access control address used by the network adapter hardware of the client.

Códigos de eventos:

Event ID	Description
00	The log was started.
01	The log was stopped.
02	The log was temporarily paused due to low disk space.
10	A new IP address was leased to a client.
11	A lease was renewed by a client.
12	A lease was released by a client.
13	An IP address was found in use on the network.
14	A lease request could not be satisfied because the address pool of the scope was exhausted.
15	A lease was denied.
20	A BOOTP address was leased to a client.

Eventos de actualización de DNS que registra DHCP log:

ID number	DHCP Event
30	DNS dynamic update request
31	DNS dynamic update failed
32	DNS dynamic update successful

b.2) **Clasificación:**

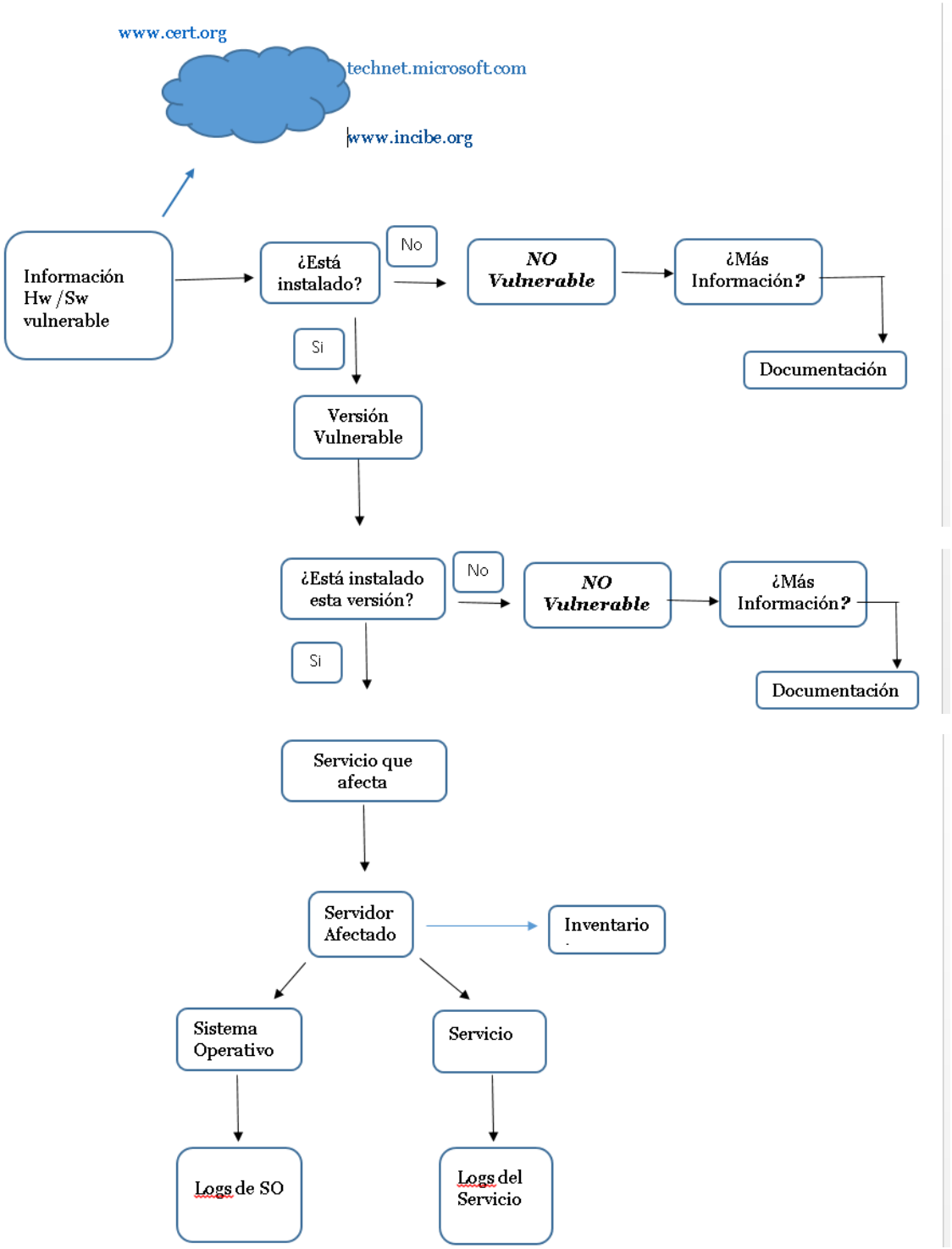
Primera clasificación → **1.1 Windows**

Segunda clasificación → 4.- Aplicación/Servicio Sist. Informáticos: **4.9 DHCP**

Tercera clasificación → Diagnósticos : "**A" Información de Red**

Diagnósticos : "**C" Eventos, errores, Diagnósticos,**

3.2 Arquitectura



Capítulo 4: Ejemplos de Actuación

4.1 Ejemplo 1:

En la comprobación diaria de vulnerabilidades se aprecia a día 10 de Diciembre de 2015 en la base de datos de vulnerabilidades de www.cert.org, la siguiente información:

Recent Vulnerability Notes

View Recent Vulnerability Notes Feed

10 Dec 2015VU#403568Netgear G54/N150 Wireless Router WNR1000v3 uses insufficiently random values for DNS queriesCVE-2015-8263

Vulnerability Note VU#403568
Netgear G54/N150 Wireless Router WNR1000v3 uses insufficiently random values for DNS queries
Original Release date: 10 dic 2015 | Last revised: 10 dic 2015

Overview

Netgear G54/N150 Wireless Router WNR1000v3, firmware version 1.0.2.68 and possibly earlier, uses insufficiently random values for DNS queries and is vulnerable to DNS spoofing attacks.

Description

CWE-330: Use of Insufficiently Random Values - CVE-2015-8263

The Netgear G54/N150 Wireless Router WNR1000v3 uses static source ports for all DNS queries originating from the local area network (LAN). An attacker with the ability to spoof DNS responses can cause WNR1000v3 LAN clients to contact incorrect or malicious hosts under the attacker's control.

Impact

A remote, unauthenticated attacker may be able to spoof DNS responses to cause WNR1000v3 LAN clients to contact attacker-controlled hosts.

Solution

The CERT/CC is currently unaware of a practical solution to this problem.

4.1.1 Descripción del ejemplo 1

Situación A:

¿Que HW ó Sw es vulnerable? Netgear G54/N150 Wireless Router WNR1000v3

¿Tengo instalado el HW/SW? NO

¿Soy vulnerable? NO

Informativo: ¿Qué impacto tiene?

¿Quién puede atacar? Atacante remoto no autenticado

¿Qué puede hacer? Spoofing a respuestas DNS y y provocar que clientes LAN WNR1003v3 se pongan en contacto con host controlados por el atacante.

Situación B:

Supongamos que la respuesta a ¿Tengo instalado el HW/SW? Sea afirmativa:

¿Que HW ó Sw es vulnerable? Netgear G54/N150 Wireless Router WNR1000v3

¿Tengo instalado el HW/SW? SI

¿Qué versión /es son vulnerables): WNR1000v3

¿Tengo instalada la versión? SI

¿Soy vulnerable? SI

¿Quién puede atacar? Atacante remoto no autenticado

¿Qué puede hacer? Spoofing a respuestas DNS y y provocar que clientes LAN WNR1003v3 se pongan en contacto con host controlados por el atacante.

¿Qué servicio afecta la vulnerabilidad? DNS

¿Qué sistema Operativo tiene DNS Server? Linux

¿Protocolo / puerto del servicio? Tcp/udp puerto 53

¿Qué servicios/máquinas tienen trafico DNS?

- Servidor DNS Coorporativo
- Servidor DNS Proveedor internet
- Firewalls

Controles a realizar:

- Tcp/udp puerto 53
- Logs de Netgear Wireless Router
- Ficheros logs de servidores DNS → named.conf → comprobar ubicación ficheros de logs
- Logs del firewall → TCP/UDP puerto 53
- Logs Sistema Operativo Servidor DNS

Soluciones:

- Existe Solución definitiva? NO
- Existe Workaround o fix SI

  Valoración de la instalación.

4.2 Ejemplo 2

En la comprobación diaria de Avisos de Seguridad de www.incibe.es (Instituto Nacional de Ciberseguridad de España), se aprecia a día 1 de Febrero de 2016 la siguiente información:

Denegación de servicio en Cisco Wide Area Application Service CIFS

Importancia:

4 - Alta

Fecha de publicación:

01/02/2016

Recursos afectados

La vulnerabilidad afecta a los siguientes productos Cisco WAAS, desde la versión de Cisco WAAS 5.1.1d hasta la 5.5:

Cisco WAAS appliances

Cisco Virtual WAAS (vWAAS)

Módulos Cisco WAAS

Descripción

Una vulnerabilidad en la optimización de CIFS en Cisco Wide Area Application Service puede causar una denegación de servicio.

Solución

Instalar la actualización correspondiente, según la rama de versión afectada:

Versiones Cisco WAAS 5.1 (desde 5.1.1.d) -> Actualizar a 5.3.5d

Versiones Cisco WAAS 5.2 y 5.3 -> Actualizar a 5.3.5d

Versiones Cisco WAAS 5.4 y 5.5 -> Actualizar a 5.5.3

Alternativamente, este problema puede evitarse desactivando el proceso de optimización cifs-ao, aunque repercute en el rendimiento del sistema. Para ello puede ejecutarse el comando:

 # accelerator cifs expert RxCIFS IOCTLHandling true

Detalle

La vulnerabilidad es debida a un tratamiento insuficiente del tráfico CIFS en Cisco Wide Area Application Service.

Un atacante remoto puede explotar esta vulnerabilidad generando tráfico malicioso para desbordar los recursos de búfer del sistema y provocar su reinicio.

4.2.1 Descripción del ejemplo 2

Se comprueba en la web los recursos afectados y una descripción del problema:

Una vulnerabilidad en la optimización de CIFS en Cisco Wide Area Application Service puede causar una denegación de servicio. La vulnerabilidad es debida a un tratamiento insuficiente del tráfico CIFS en Cisco Wide Area Application Service.

Un atacante remoto puede explotar esta vulnerabilidad generando tráfico malicioso para desbordar los recursos de búfer del sistema y provocar su reinicio.

Situación A:

¿Que HW ó Sw es vulnerable? Módulos Cisco WAAS

¿Tengo instalado el HW/SW? NO

¿Soy vulnerable? NO

Informativo: ¿Qué impacto tiene? Provocar indisponibilidad del sistema.

¿Quién puede atacar? Un atacante remoto puede explotar esta vulnerabilidad

¿Qué puede hacer? Generar tráfico malicioso para desbordar los recursos de búfer del sistema y provocar su reinicio

Situación B:

Supongamos que la respuesta a ¿Tengo instalado el HW/SW? Sea afirmativa:

¿Que HW ó Sw es vulnerable? Módulos Cisco WAAS

¿Tengo instalado el HW/SW? SI

¿Qué versión /es son vulnerables): Cisco WAAS 5.1.1d hasta la 5.5

¿Tengo instalada la versión? SI. Cisco WAAS 5.4

¿Soy vulnerable? SI

¿Qué impacto tiene? Puede provocar indisponibilidad del servicio.

¿Quién puede atacar? Atacante remoto.

¿Qué puede hacer? Generar tráfico malicioso para desbordar los recursos de búfer del sistema y provocar su reinicio.

¿Qué servicio afecta la vulnerabilidad? Tráfico TCP/IP de la Red.

Inventario: Que elementos de CISCO se ven afectados? Dispositivos de WAAS

Soluciones:

- Existe Solución definitiva? SI
- Existe Workaround o fix SI

Valoración de la instalación.

Una vez identificados los elementos CISCO involucrados, seguir las instrucciones indicadas en la página web de Incibe:

- Instalar la actualización correspondiente, como nuestra versión es 5.4, se actualizará a 5-5-3:
  Versiones Cisco WAAS 5.4 y 5.5 -> Actualizar a 5.5.3

- En caso de que por cualquier motivo no se pueda actualizar la versión instalada, se puede desactivar el proceso de optimización cifs-ao, como se indica en la web, ejecutando el comando:

  # accelerator cifs expert RxCIFS IOCTLHandling true

Capítulo 5.- Soluciones

5.1 Generalidades

Todo lo visto hasta este documento, es decir, el conocer los diferentes ficheros de registros y la información que pueden aportar, puede ser muy valioso y ayudarnos a conocer a través de esta información, características de nuestra red, análisis del tráfico y detectar, como se ha visto en los ejemplos, en un periodo corto de tiempo, donde puede existir una vulnerabilidad, amenaza ó simplemente un fallo de software.

En los ejemplos de actuación expuestos en el capítulo anterior, se aprecia que ante una alerta de vulnerabilidad, de una forma sencilla se detecta como puede influir a la organización, y como esta organización, con un esquema claro de su red, los programas instalados y la información que todo ello le aporta, puede detectar y localizar el punto vulnerable de su instalación.

Cuando se trata de análisis y tratamiento de grandes volúmenes de información, cuando los datos se producen muy rápidamente con un flujo y una variedad enorme, es cuando se necesita la utilización de herramientas y programas que puedan facilitarnos a recoger y analizar esa información.

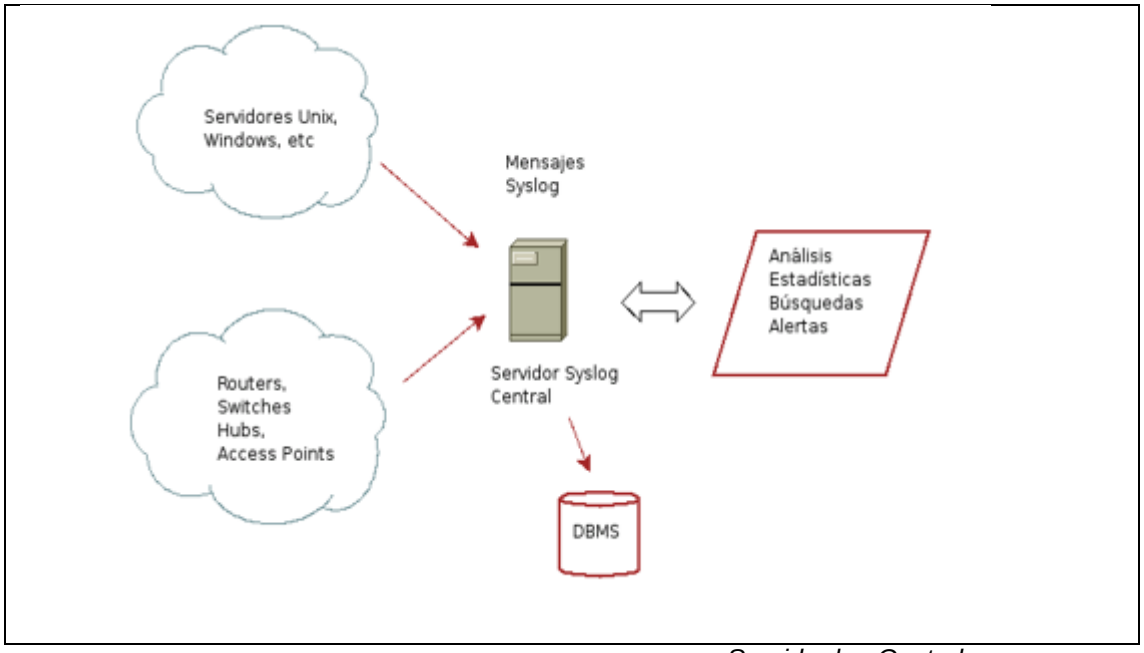
Se desarrolla a continuación, una serie de soluciones que facilitan esta labor:

- Configuración Servidor Log Central - SYSLOG
- Analizadores de Eventos y Logs
- Big Data

5.2 Configuración Servidor Central: SYSLOG

Se puede utilizar Syslog para centralizar y consolidar los archivos de log. El protocolo *syslog* es muy sencillo: existe el servidor de syslog, conocido como *syslogd* (daemon de syslog) y el cliente envía un pequeño mensaje de texto (de menos de 1024 bytes). Provee un servicio estándar (una interfaz API para aplicaciones) y de mensajes, en los que define niveles de seguridad y agrupaciones de mensajes por tipo. Pueden utilizarlo Routers, switches, servidores Unix y Windows.

Utiliza el protocolo UDP- puerto 514 y los mensajes de syslog tienen dos atributos además del mensaje en si: Facility y Level.



Servidor log Central

Grupos syslog (facilities) [14]

LOG_AUTH	Mensajes de seguridad/autenticación (descontinuado)
LOG_AUTHPRIV	Mensajes de seguridad/autenticación (privado)
LOG_CRON	Servicio CRON
LOG_DAEMON	Daemons del sistema
LOG_FTP	Daemon FTP
LOG_KERN	Mensajes del Kernel
LOG_LOCAL[0-7]	Reservados para uso local
LOG_LPR	Sub-sistema de impresión
LOG_MAIL	Sub-sistema de correo
LOG_NEWS	Sub-sistema de noticias USENET
LOG_SYSLOG	Mensajes generados internamente por Syslogd
LOG_USER (default)	Mensajes de nivel de usuario genéricos
LOG_UUCP	Sub-sistema UUCP

Niveles de syslog [14]

LOG_EMERG	Sistema en estado inútil
LOG_ALERT	Se requiere acción inmediata
LOG_CRIT	Condiciones críticas
LOG_ERR	Condiciones de Error
LOG_WARNING	Condiciones de precaución
LOG_NOTICE	Condición normal, pero significativa
LOG_INFO	Mensaje informativo
LOG_DEBUG	Mensaje de depuración

Normalmente syslog es ayudado de programas como Log Watcher para monitorizar y buscar patrones de actuación en los ficheros.

5.3 Analizadores de Eventos y Logs

Permiten centralizar y analizar los logs y registros de eventos. Su objetivo es desde un repositorio central, analizar, buscar y generar informes que aportan información sobre lo que ocurre en la red corporativa, pudiendo generar alertas en tiempo real [15] es un sistema de alto rendimiento para recopilar, analizar, archivar y almacenar grandes volúmenes de registros de sucesos de red y seguridad. Las características que ofrecen estos analizadores, variarán en función del programa elegido, pero en general, las características de estas herramientas son:

- Recogida de logs de fuentes heteregéneas (Unix, Windows, routers, firewall, etc.),
- Generación informes
- Correlación de eventos en tiempo real, establecimiento de reglas para gestión proactiva de amenazas.
- Búsquedas de registros
- Alertas en tiempo real
- Análisis forense
- Algunos de ellos ofrecen opciones de alta disponibilidad y recuperación tras desastres.

5.4 Gestión de Logs con Big Data

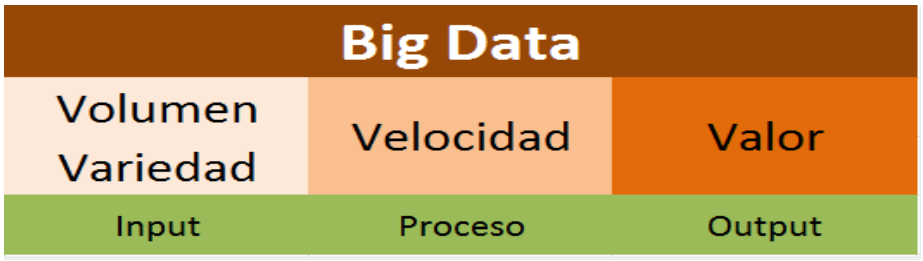
La evolución en las tecnologías de la información y las nuevas necesidades en el manejo de la información, ha dado lugar al nacimiento de un nuevo concepto: Big Data.

Entre las definiciones que podemos encontrar, una de las más sencilla es: el manejo de grandes volúmenes de información que vienen de diferentes fuentes de datos (estructurados, no estructurados, XML, HTML, etc.) de una manera rápida sin afectar la disponibilidad de la información y operación de los sistemas.

Big Data es en el sector de tecnologías de la información y la comunicación, una referencia a los sistemas que manipulan grandes conjuntos de datos.

Big Data se refiere a las herramientas, procesos y procedimientos que permiten a las organizaciones generar, manipular y administrar grandes cantidades de datos, de múltiples orígenes y en diversos formatos, para explotarlos en su beneficio, teniendo en cuenta que las consultas hechas en Big Data ayudan al análisis y a la toma de decisiones.

Una vez que hemos realizado una aproximación en capítulos anteriores a la gran variedad de diferentes registros de ficheros logs que se pueden recopilar, y teniendo en cuenta el concepto de Big Data, expuesto en este apartado, lleva a pensar en una gran oportunidad de aplicarlo en la Gestión de Logs.



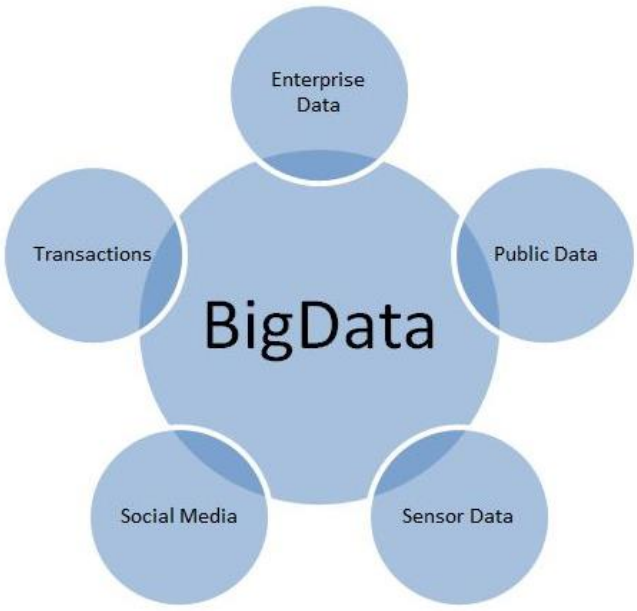
Big Data

Si solo nos concentramos en volúmenes de datos, no podemos hablar de Big Data. Hace falta también diversidad de orígenes, correlacionarlos, técnicas analíticas para obtener conocimiento.

Al hablar de diversidad de orígenes, podemos englobar los diferentes tipos de datos y fuentes de información que pueden recoger las organizaciones:

Tipos y fuentes de datos

La mayor parte de las organizaciones centran la atención en analizar datos estructurados, sin embargo, con Big Data se ofrece la oportunidad de analizar múltiples tipos de datos, que pueden incluso ser completamente nuevos para muchas de estas organizaciones:



Fuentes de Big Data

El origen de la información puede ser desde las redes sociales, publicaciones hasta los más tradicionales de tecnologías de información.

Fuentes de Big Data [16]:

Con todo esto quiero expresar el potencial tan enorme que puede llegar a tener el trato de la información en una instalación de este tipo, todo ello en tiempo real.

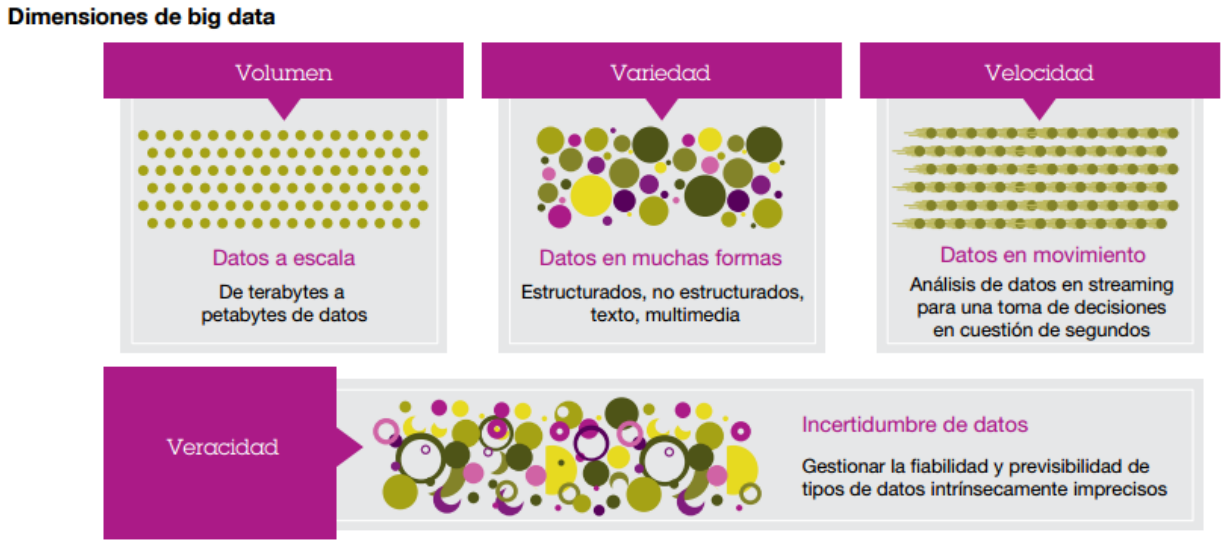
Como funcionalidades analíticas de Big Data, se pueden mencionar: [16]

Big Data cubre la necesidad de consolidar la gran cantidad de información que se presenta en una organización para reforzar la toma de decisiones.

Cuando se busca información sobre Big Data, las diferentes propuestas parece que se corresponden a un conjunto de características, cuyos vocablos empiezan todos por la letra "V" (Volumen, Variedad, Velocidad, Variabilidad, Veracidad… Valor). Algunas de ellas como volumen, variedad, ya se han tratado. Respecto a la velocidad, tiene dos importantes interpretaciones:

- Cantidad de información por unidad de tiempo que se obtiene a la vez de los diferentes orígenes de datos para almacenarla o tratarla.
- Cuantos más volúmenes de datos, el valor de estos tiende a disminuir más rápidamente en el tiempo, por lo que las organizaciones deben de poder analizar de los datos en tiempo real.

El presente Trabajo Fin de Master se comenzó con la idea inicial de recolección, estudio, información y clasificación de los logs, con objeto de llegar al conocimiento de toda la información que nos aportan y poder utilizarla para detectar tráfico anómalo, vulnerabilidades, etc. Pero si a esto le añadimos, todo el abanico de posibilidades que nos ofrece Big Data para interrelacionar, analizar, toma de decisiones, etc. y toda ello en tiempo real, es realmente impresionante.



Cuatro dimensiones de Big Data

Muchas organizaciones llevan años trabajando con volúmenes enormes de datos e incluso con millones de transacciones por minutos. Lo que hace la idea de Big Data algo completamente nuevo son dos tendencias importantes:

- La digitalización de prácticamente "todo" da lugar a nuevos tipos de grandes datos en tiempo real en un amplio abanico de sectores. Muchos de ellos son datos no normalizados: por ejemplo, datos en streaming, geoespaciales o generados por sensores que no encajan bien en los warehouses relacionales, tradicionales y estructurados.
- Las tecnologías y técnicas de análisis avanzado de hoy en día permiten a las empresas extraer conocimientos de los datos con un nivel de sofisticación, velocidad y precisión nunca antes visto. [16]

5.4.1 Ejemplos de Big Data en Gestión de Logs

Principales aplicaciones de Big Data [17]:

- Explotación de grandes datos: Tres 'V' del Big Data (velocidad, volumen y variedad) reflejan el reto al que se enfrentan las grandes compañías a la hora de dar a los datos un valor para tomar mejores decisiones, mejorar las operaciones y reducir los riesgos. → Veracidad (La cuarta V)
- 360º de visión sobre el cliente: las compañías deben obtener información de fuentes internas y externa. Entender comportamientos y predecir futuras acciones. En nuestro caso sería el tema de gestión y tratamiento de logs e información en su totalidad.
- Extensión de la seguridad/inteligencia: Mecanismos para localizar anomalías y prevenir ataques.
    - Análisis de datos en movimiento y en reposo para encontrar asociaciones o descubrir patrones.

  - Previsión y atenuación de ataques cibernéticos en tiempo real: analizando el tráfico de la red, se puede descubrir amenazas nuevas y prevenir ataques de hackers, intrusos, fraude cibernético e incluso ciberterrorismo.
  - Predicción y prevención del crimen: la capacidad para analizar datos de la red de telecomunicaciones y de redes sociales permite detectar amenazas y adelantarse a los criminales antes de que actúen.
- Análisis de operaciones: permite obtener visibilidad en tiempo real de las operaciones, la experiencia del cliente, transacciones y comportamiento.
- Aumenta el almacén de datos o Wharehouse

A continuación relaciono una serie de ejemplos concretos en los que la utilización de Big Data refleja el gran potencial que se puede desarrollar.

a) Toma de decisiones o acciones inmediatas en tiempo real, ante la aparición de un problema de seguridad, como por ejemplo:
   - Divulgación de nueva vulnerabilidad o amenaza en la Red.
   - Puesto de usuario infectado de virus/malware
   - Reintentos de accesos no autorizados
   - Instalación de programas no deseados por parte de los usuarios.
   - Detección de accesos no deseados a bases de datos
   - Etc.

b) Estudio del impacto de una nueva legislación, norma o recomendación sobre la privacidad que pueda influir en la infraestructura de la Organización.
c) Conocimiento de acceso y comportamiento de los visitantes a las páginas web de la organización para posterior análisis de tendencias y mejorar el servicio.
d) Estudio e impacto de la Incorporación de lectores biométricos como mecanismo de seguridad
e) Estudio y control de accesos físicos a instalaciones cruzando datos de videos y mecanismos de control de puertas.
f) Certeza por parte de la Organización, de la no existencia de “tráfico no deseado”

g) Conocimiento en tiempo real, análisis y tratamiento de noticias de interés para la seguridad de la Organización en cuanto a información que aparezca en redes sociales como blogs, tweets, etc.
h) Conocimiento de la imagen de la empresa a través de redes sociales, y diferentes medios de comunicación.
i) Análisis y conocimiento de patrones de ataque más comunes para establecimiento de defensa y acciones por parte de la Organización.
j) Análisis e identificación de tráfico anómalo en tiempo real, así como identificación de fallos de configuración y puntos débiles de la red.
k) El análisis y cruce de datos de la actividad "atacante" que se utilizará para orientar la actuación de la organización, estudiando las tendencias y poniendo mayor énfasis en vigila aquellas zonas de más riesgo.
l) Manejar los datos para conocer los programas que proporcionan mayor indisponibilidad u otro tipo de problemas que preocupen a la Organización.
m) Análisis predictivo ante una nueva vulnerabilidad o amenaza.
n) Control de disponibilidad y rendimiento de infraestructuras interconectadas de servidores y elementos de red.
o) Seguimiento mediante análisis histórico de amenazas y vulnerabilidades
p) Seguimiento de los accesos a bases de datos para controlar las operaciones de añadir, modificar ó borrar.
q) Etc.

5.4.2 Big Data y la incertidumbre

Uno de los aspectos que más he destacado en el aprendizaje del Master ha sido el análisis y la gestión del riesgo. Se ha visto que asociado al tratamiento del riesgo y su disminución, aparece la idea del tratamiento explícito de la incertidumbre:

"La gestión de riesgos tiene como objetivo gestionar o tratar el riesgo hasta disminuir el riesgo residual a los niveles asumibles por la dirección, y debe:

- *Ser una parte integral de todos los procesos de negocio.*
- *Crear y proteger el valor.*
- *Formar parte de la toma de decisiones.*
- *Tratar explícitamente la incertidumbre.*
- *Ser sistemática, estructurada y oportuna.*

- *Estar basada en la mejor información posible.*
- *Ser adaptable.*
- *Integrar factores humanos y culturales.*
- *Ser transparente y participada por las partes interesadas de la organización.*
- *Ser dinámica, iterativa y responde a los cambios.*
- *Facilitar la mejora continua."*

(Apuntes de Gestión de Riesgos, Master Universitarios de Seguridad Informática. UNIR)

En la diversidad de los datos que se pueden recoger en una organización, algunos de ellos pueden ser intrínsecamente inciertos, por ejemplo, sentimientos, reacciones ante determinados hechos, tendencias, condiciones climatológicas o factores económicos, y a pesar de su incertidumbre los datos siguen conteniendo información muy valiosa.

Para realizar una gestión de la incertidumbre, se ha de crear un contexto en torno a los datos: la combinación de múltiples fuentes menos fiables y la utilización de matemáticas avanzadas engloban, como sólidas técnicas de optimización y planteamientos de lógica difusa. Se debe reconocer la incertidumbre, aceptar y aplicarla en la organización.

Ventajas de Big Data:

• Decisiones más inteligentes – Aprovechar nuevas fuentes de datos para mejorar la calidad de la toma de decisiones.
• Decisiones más rápidas – Permitir una captura y análisis de datos en tiempo más real para respaldar la toma de decisiones en el "punto de impacto", por ejemplo cuando un cliente está navegando por su sitio web o al teléfono con un representante del servicio de atención al cliente.
• Decisiones que marquen la diferencia – Centrar las iniciativas de big data en ámbitos que proporcionen una verdadera diferenciación.

Big Data, aporta por sus características, una GRAN solución para análisis y gestión de Logs, junto a la gestión de riesgos y trato de la incertidumbre.

Referencias y Bibliografía

- *[1] Wikipedia*
- *[2] RedIRIS (Seguridad Lógica)*
- *[3] Guía de toma de evidencias en entornos Windows (INCIBE) Ver ejemplos*
- *[4] http://pegasus.javeriana.edu.co/~regisegu/Docs/documento.pdf*
- *[5] https://www.rediris.es/jt/jt2006/archivo/.../Centralizacion_logs-UPC.ppt - Facultad Informática de Cataluña*
- *[6] https://www.ibm.com/developerworks/community/blogs/b35561d9-e0ef-48e0-b455-001f4a64b4da/entry/itil_mejores_practicas_gestion_de_eventos?lang=en*
- *[7] 52.1.175.72/portal/sites/all/themes/argo/assets/img/.../pamplona.doc*
- *[8] https://www.rediris.es/cert/doc/unixsec/node12.html*
- *[9] Networking: http://ww.cisco.com/cisco/web/support http://www.cisco.com/cisco/web/support/LA/7/74/74465_21.html#logging https://supportforums.cisco.com/document/24661/how-configure-logging-cisco-ios*
- *[10] Apuntes del profesor tema 1: Arquitectura de las aplicaciones web y bases de datos. Asignatura Seguridad Aplicaciones online y Bases de Datos UNIR.*
- *[11] Wikipedia Servidor de aplicaciones.*
- *[12] http://www.jtech.ua.es/j2ee/2003-2004/abierto-j2ee-2003-2004/sa/sesion1-apuntes.htm*
- *[13] Log File Messages by Component http://docs.oracle.com/*
- *[14] http://www.monografias.com/trabajos107/gestion-logs/gestion-logs.shtml*
- *[15] Event Log Analyzer - https://www.manageengine.com/es/eventlog*
- *[15] IBM Security QRadar Log Manager (http://www-03.ibm.com/software/products/es/qradar-log-manager)*
- *[16] http://www-05.ibm.com/services/es/gbs/consulting/pdf/El_uso_de_Big_Data_en_el_mundo_real.pdf*
- *[17] http://www.lantares.com/blog/las-cinco-principales-aplicaciones-de-big-dat*
- *http:/ www.iso27000.es/herramientas.html EL PORTAL DE ISO 27001 EN ESPAÑOLNormas y buenas prácticas:*
  Gestión centralizada de Logs
  Guía en español de una metodología para la gestión centralizada de registro de eventos de seguridad en Pymes

- *GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-812) SEGURIDAD EN ENTORNOS Y APLICACIONES WEB*
- *http://www.rediris.es/cert/doc/*
- *https://www.ccn-cert.cni.es/*
- *GESTIÓN DE INCIDENTES: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Incidentes.pdf (Sitio Web oficial del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia)*
- *https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/*
- *Guía de administración de los servidores Oracle® serie X5 https://docs.oracle.com/cd/E50691_01/html/E58595/gnfka.html*
- *http://blog.takipi.com/las-7-herramientas-para-el-manejo-de-logs-registros-que-todo-desarrollador-java-debe-conocer/*
- *http://www.websecurity.es/analisis-los-ficheros-logsparte-i - www.Websecurity.es*
- *Visor de eventos de Windows: http://windows.microsoft.com/es-xl/windows/what-information-event-logs-event-viewer#1TC=windows-7*
- *https://www.elhacker.net/InfoForenseWindows2.html*
- *Analisis Forense: análisis de las evidencias. Mirar ese tema para posibles patrones de ataques.*
- *https://www.rediris.es/cert/doc/unixsec/node12.html#SECTION053410000000000000000*
- *https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_toma_evidencias_analisis_forense.pdf*
- *http://www.nexolinux.com/ficheros-de-logs-en-el-directorio-varlog/*
- *http://www.expertosdelinux.com/*
- *Guía de seguridad en servicios DNS (INCIBE)*
- *ABC's of z/OS System Programming Volume 8 (IBM Redbook)*
- *http://www.aspectosprofesionales.info/2013/11/big-data-no-sin-gobierno-no-sin-gestion.html*
- *http://anibalgoicochea.com/tag/big-data/*
- *https://www.manageengine.com/es/eventlog/ (EventLog analyzer)*
- *https://support.office.com/es-ES/article/%C2%BFD%C3%B3nde-guarda-Microsoft-Outlook-2010-mi-informaci%C3%B3n-y-mis-configuraciones-e178f6d6-1515-4c7e-8202-6c7f4794c0a3*