Publicación quincenal editada por el Departamento de Telecomunicaciones y Telemática del Instituto Superior Politécnico José Antonio Echeverría
Auspiciada por el Ministerio de la Informática y las Comunicaciones

Año VII No. 17

ISSN: 1729-3804

Telem@tica

Diciembre 11, 2008
"Año 50 de la Revolución"

REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

FRASE DE LA SEMANA

"El ignorante afirma, el sabio duda y reflexiona."
Aristóteles

SUMARIO

Contáctenos

REVISTA TELEM@TICA
Departamento de Telemática
Facultad de Ingeniería Eléctrica

Instituto Superior Politécnico
José Antonio Echeverría

Calle 114, No. 11901, entre 119
y 127, Municipio Marianao,
Habana,Cuba

Teléfono:
+53 (7) 2606279 / 2679880

Fax:
+53 (7) 2671576

Telematica@revistas.cujae.edu.cu

Sitio Web:
http://www.cujae.edu.cu/revistas/telematica

IR al SUMARIO

NOTA DEL EDITOR

Estimado lector:

Con el avance de la tecnología y el surgimiento continuo de amenazas en las redes de comunicaciones, la seguridad de la información se ha convertido en una de las principales preocupaciones para los administradores en este campo. Por ello, las organizaciones protegen sus recursos, equipos, soluciones de software y procesos con el uso de herramientas de seguridad como: monitores de tráfico de red, scanner de vulnerabilidades, detectores de anomalías, IDS/IPS, Firewall, ACL's, antivirus, etc., que ayudan a gestionar sus problemas de seguridad. Sin una gestión inteligente, centralizada y una correlación automatizada, muchas organizaciones han descubierto que sus infraestructuras de seguridad se han convertido en un complejo laberinto de sistemas dispares que generan un enorme flujo de datos y ofrecen poca visibilidad de los verdaderos ataques y amenazas.

Nos encontraremos nuevamente en el próximo número.

Los Editores.

TÉCNICAMENTE HABLANDO

Seguridad: Se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien

Seguridad informática: Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Gestión de Red: Consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.

Centralizar: Es la tendencia a concentrar la autoridad de toma de decisiones en un grupo reducido de personas.

Eventos: Eventos que se generan por todas las herramientas de seguridad indicando el estatus del sistema para la cual fue creada.

ARTÍCULO

Propuesta de una Plataforma de Gestión de Información de Seguridad en la Intranet de la UCLV “Marta Abreu”.

Ing. Antonio Nuñez Martínez

Es Ingeniero en Telecomunicaciones y Electrónica, por la Universidad Central “Marta Abreu” de Las Villas. (UCLV)

Cursa estudios de Master en Telemática.

Antonio@uclv.edu.cu

INTRODUCCIÓN

Uno de los aspectos importantes para toda entidad es la Seguridad de la Información, pero continuamente aparecen nuevas amenazas como: virus, spyware, sabotajes informáticos, robos de información, accesos no autorizados, entre otros, que atentan contra la confidencialidad, integridad y disponibilidad de la información. Debido a esto, los administradores de seguridad buscan la manera de minimizar los ataques, mediante la implementación de medidas de seguridad, como: un adecuado esquema de red, políticas y herramientas.

Existe una variedad de herramientas de seguridad, tales como: herramientas de monitoreo de tráfico de red, scanner de vulnerabilidades, detectores de anomalías, IDS/IPS (Sistema de Detección/Prevención de Intrusos), Firewall, ACL's, antivirus, etc., que ayudan a minorizar los problemas de seguridad, pero la información que generan no da una perspectiva real de lo que ocurre en la red, cada herramienta o mecanismo tiene su propia plataforma, formato y arquitectura.

La tecnología SIM aplaca estos problemas integrando varias herramientas de seguridad, para recoger, ordenar y correlacionar la información sobre el estado de la red, de las máquinas y los comportamientos de los sistemas y usuarios. Le ofrece a los administradores la posibilidad de encontrar indicios de ataques que hayan ocurrido o que puedan suceder en un futuro.

Con esta tecnología, se han desarrollado productos tanto de software como de hardware, para estandarizar los eventos, y así los administradores tengan la información centralizada y ordenada. Existen herramientas como: ArcSight ESM, Cisco Works SIMS, Cisco MARS que son comerciales y OSSIM de código libre.

Como entidad educativa, se promueve la investigación y desarrollo de nuevas tecnologías, y en el caso de Gestión de Seguridad se propone implementar una herramienta de código libre (OSSIM) por sus ventajas respecto al costo y flexibilidad de configuración.

Esta plataforma ofrece un marco para centralizar, organizar y mejorar las capacidades de detección y visibilidad de los eventos de seguridad de la organización. La componen más de veintidós herramientas líderes en el campo de la Seguridad Informática, y posee una arquitectura formada por cuatro componentes: servidor (consola de Gestión), framework (interacción entre módulos), base de datos (eventos) y agentes (sensores colectores).

El artículo presenta las fases a seguir para la implementación de OSSIM en una red de una entidad dinámica, debido al tipo de usuarios, tales como: estudiantes, docentes e investigadores.

Para su implementación se debe tener un conocimiento claro del sistema de red que se maneje, el flujo de datos, servicios que presta, funcionamiento de la herramienta, determinación de una arquitectura de monitoreo, evaluación de funcionalidad y rendimiento.

IR al SUMARIO

ANÁLISIS DEL SISTEMA ACTUAL.

El objetivo de esta primera fase es conocer sobre la estructura de la red, servicios en producción, hardware y software utilizado y determinar los servicios más críticos.
Involucra además, actividades como: entrevistar a los administradores de servicios y seguridad, analizar e interpretar el esquema de red y realizar una priorización de los servicios. Esto sobre la base del papel que desempeña un servicio dentro de las actividades operativas de la entidad.
Con la información recolectada se tiene una noción del estado actual de la entidad y se pueden definir cuales son los servicios más críticos para la misma.

Políticas de seguridad
Las entidades se basan en un conjunto de normas, políticas y estándares de seguridad para mantener un nivel de seguridad. Se estudian y se evalúan para un buen uso de los recursos de información.

Herramientas de seguridad
Conocer las herramientas de hardware y software de seguridad con las que cuenta la entidad, para tener claridad de los mecanismos implementados, así como su funcionamiento, volumen de información que generan y tipos de datos.

Servicios
Conocer la variedad de servicios que ofrece la entidad a los usuarios internos y externos, y de acuerdo a su funcionalidad definir el nivel de criticidad que poseen.

Priorización de los servicios [1]

Se deben considerar algunos aspectos para determinar los servicios a monitorear, de acuerdo al nivel de importancia dentro de la entidad. El objetivo principal de la priorización es identificar los servicios críticos que se deben proteger y mantener en correcto funcionamiento según su nivel de importancia, así como también los servicios cuya inhabilitación causan detenciones prolongadas de otros.
A continuación se presentan algunos puntos a evaluar.

- **Tipo de datos.** Nivel de criticidad de la información que maneja el servicio.

TABLA I

Niveles de datos

Información	Nivel de Criticidad
Sensible	5
Muy critico	4
Critico	3
Medio critico	2
Bajo	1
Despreciable	0

- **Magnitud.** Cantidad de sistemas que afecta, en el caso de que el servicio falle.

TABLA II

Servicios afectados

Numero de servicios que afecta	Nivel de criticidad
0	1
1	2
2	3
3	4
4	5

- **Impacto financiero.** Es el efecto a nivel de causa cuantificado en términos monetarios, siendo la medida de pérdidas económicas de la entidad. Para cuantificar el impacto financiero es necesario determinar el costo por hora que implica brindar cada uno de los servicios involucrados.

TABLA III
Impacto financiero

Costo por hora ($)	Nivel de criticidad
0 – 5	1
5 – 10	2
10 – 15	3
15 – 20	4
20 – 25	5

- **Impacto a usuarios.** Es la cantidad de usuarios que serán afectados si deja de funcionar un servicio.

TABLA IV
Usuarios afectados

Números de usuarios	Nivel de criticidad
0 – 250	1
250 – 500	2
500 – 750	3
750 – 1000	4

Las tablas descritas pueden ser tomadas como ejemplos por los administradores de seguridad y acoplarlos de acuerdo a la conveniencia de la entidad, para determinar el nivel de importancia de cada servicio.

Hardware y software.
Luego del análisis de los servicios, se determinan los servidores con los que se cuenta y se realiza un inventario de hardware y sistema operativo que posee cada uno de ellos, con el fin de determinar las plataformas y aplicaciones con las que trabajan. Estas serían las herramientas con las que va a trabajar OSSIM; ya que existen herramientas para servicios específicos, que funcionan en determinada plataforma y otras en varias.

Tráfico.
Se determina el tráfico normal que fluye en la entidad, por ejemplo: servicios utilizados en la red, cantidad de protocolos, flujo de tráfico entre los servidores, entre otros, con el fin de saber el tráfico con el que trabajara SIM.

Esquema de red.
Conocer la infraestructura de red presente para los usuarios internos y externos, siendo necesario analizar la ubicación de los equipos que prestan cada uno de los servicios; para determinar los segmentos de red que existen y la arquitectura de SIM, como la ubicación del servidor central y de los agentes.

ANÁLISIS DE LA HERRAMIENTA SIM

El objetivo de este análisis es tener conocimiento sobre OSSIM, como: los componentes, las herramientas que la integran y como interactúan. La información recolectada en la fase anterior se usa para trabajar en su implementación.

OSSIM (Open Source Security Information Management). [2]
Esta plataforma es una solución de seguridad, que puede ser personalizada a las necesidades de cada entidad. Permite la visibilidad de todos los eventos de los sistemas en un punto central y en un mismo formato. Mediante la correlación[4] relaciona y procesa la información minimizando así los “falsos positivos”[5] y “falsos negativos”[6]. A continuación se presenta un diagrama del funcionamiento de OSSIM.

Figura 1. Funcionamiento de OSSIM.

Se realiza una monitorización de todos los niveles desde el más bajo (firmas detalladas de un IDS) hasta el más alto (Cuadro de mandos), pasando por: consola forense, niveles de correlación, inventarios de activos y monitores de riesgo.

Componentes de OSSIM. [3]

Esta herramienta esta formado por cuatro componentes:

- **Servidor.** Es el componente principal de OSSIM.. Recibe los eventos enviados por los distintos agentes y realiza además las funciones de priorización y correlación.
- **Agente.** Son hosts distribuidos en diferentes segmentos de la red, para monitarizar los distintos eventos. Estos se distribuyen sobre la base de los servicios que se van a monitorear. Cada agente o sensor tendrá configurado un conjunto de detectores o monitores, que generan eventos para que el agente los recolecte y reporte al servidor central.
- **Framework.** Es el intermediario entre el servidor central y el usuario. La herramienta de administración utilizada para configurar y organizar los diferentes módulos tanto externos como propios que integra OSSIM.. Contribuye a definir una topología, inventariar activos, definir políticas de seguridad, reglas de correlación y unir las diferentes herramientas integradas.
- **Base de datos.** Aquí se almacenan los diferentes eventos recolectados por los agentes, y las configuraciones de las distintas herramientas y OSSIM.

Los componentes Servidor, Framework y la Base de Datos se encuentran ubicados en un equipo que se desempaña como servidor central de OSSIM y los agentes pueden estar distribuidos en los distintos equipos.

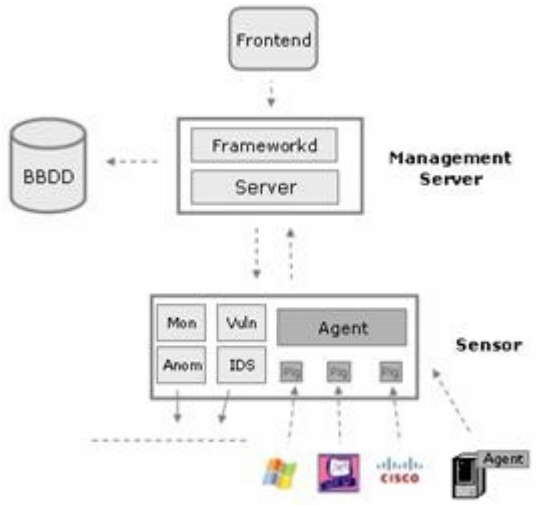

Figura 2. Componentes de OSSIM.

Correlación.

Con la correlación se relacionan varios eventos para tener una información de mayor valor. Se realiza teniendo en cuenta dos métodos:

- Correlación mediante secuencia de eventos: basada en patrones y comportamientos conocidos que define un ataque. Es la aplicación de reglas, por ejemplo: "si ocurre el evento A y luego B y luego C, haz la acción D".
- Correlación mediante algoritmos heurísticos: Se detecta situaciones de riesgo sin conocer ni ofrecer detalles de los mismos. Utiliza un algoritmo por acumulación de eventos con el fin de recibir como entrada un alto volumen de eventos y obtener como salida un indicador del estado general de la seguridad de la red, este algoritmo es llamado CALM[7]. La acumulación de eventos se realiza a través de la suma de "riesgos instantáneos"[8] de cada evento mediante dos variables: El "Nivel de Compromiso"[9] (C) y "Nivel de Ataque"[10] (A).

Herramientas que Integra OSSIM.

Para la implementación de OSSIM se determinan las herramientas que serán utilizadas para la monitorización de los eventos de seguridad en la entidad, es necesario conocer el

[4] Es el análisis de un conjunto de eventos para obtener una información de mayor valor.
[5] Patrones normales que son tomados como ataques.
[6] Patrones de ataque que son tomados como normales.
[7] Monitor de nivel de ataque y compromiso.
[8] Situación de riesgo producida por la recepción de una alerta.
[9] mide el posible riesgo debido a los ataques recibidos.
[10] Sistema de detección de intrusos de Red

funcionamiento de cada una de ellas y determinar que herramientas conviene implementar.
A continuación se detalla una clasificación de las herramientas que conforman OSSIM.

TABLE V

IDS'S (Sistema De Detección De Intrusos)

Herramienta	Función
Snort [4]	IDS de red. Implementa un motor de detección de ataques y barrido de puertos que permite registrar y alertar ante cualquier anomalía previamente definida.
Cisco IDS [5]	IDS de la familia de Cisco, esta basado en firmas. Puede tomar una respuesta contra un ataque, como bloquear la IP comprometida.
Osiris [6]	IDS de Host que comprueba la integridad del sistema de ficheros. Si existe algún cambio en los ficheros es reportado al administrador del sistema.
Prelude [7]	Considerado como un IDS Híbrido, esto significa que no sólo realiza la funcionalidad de un NIDS, sino que es un framework que unifica la información y centraliza los eventos proporcionados por los diversos sistemas IDS.
Realsecure [8]	IDS comercial. Analiza la entrada y salida de la actividad de la red y los sistemas informáticos, a fin de evitar que actividad mal intencionada dañe los activos.

TABLE VI

Detectores

Herramienta	Función
Pads [9]	Motor de detección basado en firmas, usado para detectar pasivamente los activos de la red.
Spade [10]	Preprocesador de datos, permite la detección de paquetes sospechosos utilizando técnicas de detección de anomalías.
Arpwatch [11]	Mantiene una tabla MAC/IP, para tener así un control de quién es cada uno en la red. Esto ayuda a evitar ataques de envenenamiento.
P0f [12]	Sniffer que los sistemas operativos de una forma pasiva
Router Cisco [13]	Tiene la capacidad de enviar mensajes a un servidor Syslog, para reportar los eventos que observa el router.

TABLE VII

Monitores

Herramienta	Función
Ntop [14]	Colector de información, permite monitorear la actividad de la red, como: protocolos utilizados, host presentes en la red, direcciones IP, tráfico que genera cada máquina, porcentaje de saturación de la red, datos enviados y recibidos.
Tcptrack [15]	Sniffer que despliega información sobre las conexiones TCP observadas en la interfaz de red, como: dirección origen/destino, puerto origen/destino y estado de la conexión
Opennms [16]	Herramienta comercial. Administra los servicios que presta la red y recoge la información de los hosts remotos usando SNMP

TABLE VIII

Scanners

Herramienta	Función
Nessus [17]	Utilizado para detectar vulnerabilidades existentes en la red, como por ejemplo: errores de software, puertas traseras, entre otros, generando reportes y las posibles soluciones a implementar.
Nmap [18]	Efectúa escaneos de puertos, para identificar servicios abiertos y sistema operativo utilizado por una determinada computadora o un grupo de computadores, de una forma activa.

TABLE IX

Syslogs

Herramienta	Función
Ntsyslog [19]	Analizador de logs para Windows, similar al Syslog de Linux. Recoge información sobre el sistema, la seguridad y los eventos de las aplicaciones. Para luego enviar a un servidor Syslog.
Syslog [20]	Es un estándar para la transferencia de mensajes de eventos y alertas. Los mensajes son enviados por el Sistema Operativo, al inicio o fin de una aplicación, o reporte actual de un proceso.
Snarewindows [21]	Trabaja como un manejador de logs y reporte de incidentes.

TABLE X

Firewalls

Herramienta	Función
Cisco PIX [22]	Solución de seguridad ofrecidas por Cisco Systems, permite controlar el tráfico entre la red interna y externa. Integra un syslog para registrar eventos como conexiones establecidas, conexiones fallidas, errores en las configuraciones, entre otros.
Iptables [23]	Filtra el tráfico utilizando reglas que examinan el origen/destino de los paquetes y el protocolo. Recolecta los eventos de las iptables.

TABLE XI

Servidor Web

Herramienta	Función
IIS [24]	Servidor de páginas Web de Microsoft, tiene la capacidad de registrar los eventos del servidor, peticiones y errores.
Apache [25]	Servidor HTTP de código abierto, puede ser utilizado en plataformas Unix y Windows. En los Log File se registra: la actividad, rendimiento y los problemas que puedan ocurrir en el servidor HTTP.

IR al SUMARIO

Inventario de activos y redes.

También se necesita conocer los distintos activos, redes y subredes de la entidad para el correcto funcionamiento de OSSIM (información adquirida en el análisis anterior), registrados en dos tipos de inventarios:

- Inventario de activos: conforman los servidores y los equipos de los administradores.
- Inventario de redes: formado por las redes y subredes a monitorear.

Para realizar el inventario de activos y de redes se especifican algunos parámetros definidos por OSSIM, como son:

- Hostname o Name, nombre del activo o nombre de la red.
- IP o IPs, dirección IP interna del activo o segmento de red.
- Asset, grado de importancia que tiene el activo o red dentro de la entidad. El nivel de prioridad puede variar de 0 a 5.
- Threshold C, umbral del Nivel de Compromiso.
- Threshold A, umbral del Nivel de Ataque.
- RRD Profile, perfil del activo o red.
- Sensors, específica el Agente que va a vigilar el tráfico del activo o red.
- Scan options, habilita el escaneo mediante la herramienta NESSUS o NAGIOS.
- Description, espacio para describir la función del activo o red.

Los siguientes parámetros solo se deben especificar en el inventario de los activos.

- NAT, dirección IP nateada.
- OS, Sistema Operativo que utiliza el activo.
- Mac, dirección física de la tarjeta de red.
- Mac Vendor, fabricante de la tarjeta de red.

IMPLEMENTACIÓN DE OSSIM

Para la implementación de la plataforma SIM se deben conocer los requerimientos mínimos tanto de software como de hardware para que no existan problemas, como: lentitud del servicio en el monitoreo, bloqueo del sistema, limitación de espacio en disco, entre otros.

Es importante también, tener definida una arquitectura de monitoreo adecuada para su implementación, ubicando el servidor y los agentes de manera estratégica en la Red y definir las herramientas que se instalará en los agentes, de acuerdo a los servicios a monitorear. Conocer como afecta la introducción de este nuevo servicio en la red es vital: nuevos protocolos, cantidad de tráfico adicional que se genera.

Requerimientos de hardware.

Los requerimientos mínimos de hardware a tomar en cuenta son: procesador, memoria y disco duro, ya que en el servidor se almacenan y se procesan los logs que envían los agentes, y estos tendrán además diferentes procesos corriendo, de acuerdo a las herramientas instaladas en los mismos.

Para ello, se realiza un análisis del tráfico que genera la red, se determina la cantidad de equipos y redes que se van a monitorear, y de acuerdo a estos aspectos se obtienen los requerimientos mínimos de hardware, tanto para el servidor como para los agentes que serán incorporados en la red.

Requerimientos de Software.

Se recomienda el trabajo con la distribución Debian, ya que existe mayor soporte para esta plataforma.

Antes de la instalación de los paquetes de ossim-server, ossim-agent y ossim-framework se comprueba que existan todas las dependencias requeridas por cada uno de ellos. Estos pueden ser descargados desde el sitio oficial de OSSIM www.ossim.net/download.php.

Arquitectura de monitoreo.

Para diseñar una adecuada arquitectura de OSSIM dentro de la red, es importante tomar en cuenta algunos aspectos, como:

- El servidor OSSIM debe estar ubicado en un punto central de la red, con la seguridad adecuada para prevenir accesos no autorizados
- Los distintos agentes pueden estar distribuidos en cada segmento de red, en la forma que el administrador de seguridad crea la más conveniente según los análisis anteriores.
- De acuerdo a la distribución de los agentes, se determinan las herramientas que conformarán cada uno de ellos, de acuerdo a los servicios que se van a monitorear.

IR al SUMARIO

A continuación se presenta un diagrama de la arquitectura de monitoreo.

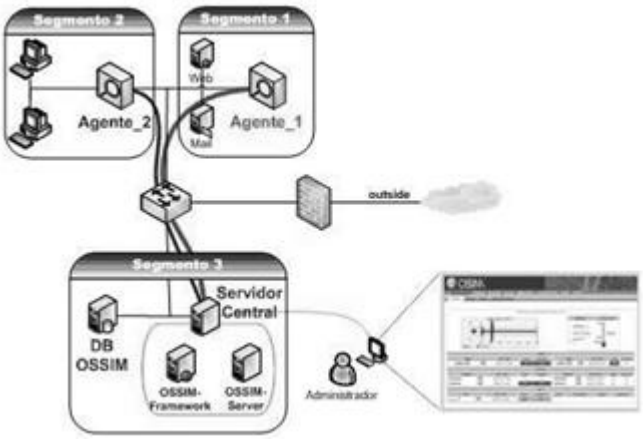

Figura 3. Arquitectura de Monitoreo

EVALUACIÓN DE LA HERRAMIENTA OSSIM

La plataforma SIM implementada se evalúa de acuerdo a su funcionalidad y su rendimiento. Se advierte que no sean las únicas variantes de evaluación de la herramienta y se haga en períodos de tiempo prolongados con un análisis profundo de acuerdo a los objetivos para lo cual fue desarrollada e implementada la misma.
Las evaluaciones de funcionalidad se basan en la utilización de la herramienta en un ambiente real, esto puede ser mediante la observación de:

- Envío de los logs desde los agentes al servidor central.
- La recepción de los eventos en el servidor central. A continuación se presenta un evento recibido por el servidor central.

2008-09-07 4:15:13 OSSIM-Message: Event received: event id="0" alarm="0" type="detector" date="2008-09-07 4:15:15" plugin_id="1514" plugin_sid="106001" src_ip="85.120.78.1" dst_ip="0.0.0.0" sensor="127.0.0.1" interface="eth1" protocol="OTHER" priority="2" asset_src="1" asset_dst="1" log="Jul 9 4:15:15 192.168.254.252 Jul 09 2008 4:17:12: %ASA2-106001: Inbound TCP connection denied from 85.120.78.1/39906 to DevServer-out/80 flags SYN on interface outside"

- El correcto funcionamiento de las herramientas que integra OSSIM.
- La correlación que realiza.

Figura 3. Resultados de Correlación de eventos

- El almacenamiento correcto de la información en la base de datos.
- Estadísticas del Nivel de Compromiso y Ataque.

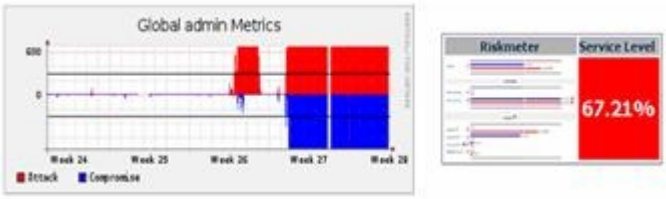

Figura 4. Estadísticas de nivel de compromiso y ataque.

IR al SUMARIO

Con respecto al rendimiento, se analiza el tráfico adicional en la red. Se puede emplear una herramienta de monitoreo, que presente estadísticas del tráfico de entrada y salida del servidor central, los agentes y el segmento de red donde se encuentran. Con el fin de establecer cual es el porcentaje en el que incrementa la carga en la red por la incorporación de OSSIM.
En este caso se tomó un segmento donde se encuentra el servidor central y un agente, y el incremento de tráfico generado en la entrada fue de 18,5% y en la salida de 17,4%, estos porcentajes varían de acuerdo con el número de activos y redes que se van a monitorear.

VENTAJAS Y DESVENTAJAS

Ventajas:

- Integra diferentes aplicaciones de seguridad informática reconocidas en este campo.
- Disminuye los falso positivos y falsos negativos con la ayuda de la correlación automatizada.
- Permite realizar análisis forenses con los eventos almacenados.
- Tiene soporte de una comunidad abierta mundial que se encuentra en crecimiento constante.

Desventajas:

- Solo se encargan de almacenar los eventos y reportarlos, no realiza ninguna acción para detener los ataques.

IR al SUMARIO

CONCLUSIONES

Es importante la utilización de una solución SIM en la Universidad, ya que se centraliza en un solo lugar y con un mismo formato todos los eventos reportados por las herramientas de seguridad.
Para la selección de la herramienta SIM a implementar, se consideraron soluciones comerciales y open source, tomándose en cuenta parámetros como: costo, plataforma, arquitectura y funcionamiento. Se determina que OSSIM cubre los requerimientos identificados.
De las veintidós herramientas de seguridad que integra la plataforma, se tomaron un grupo de ellas, teniendo en cuenta la infraestructura de la red, el ambiente de trabajo, equipos con los que trabaja y los servicios que presta la Universidad.
El análisis del sistema de seguridad actual de la Universidad, permitió identificar falencias como, falta de centralización y clasificación de la información que las herramientas de seguridad generan, y con ello tomar decisiones que contribuyan a una mejor gestión de seguridad.
Es importante determinar una arquitectura de monitoreo adecuada, teniendo en cuenta la cantidad de equipos que se va a monitorear, ya que en el caso de ser un gran número, se debe emplear agentes en diferentes segmentos de red con el fin de distribuir la carga de monitoreo entre ellos.
Las miles de alertas que se tienen de los diferentes dispositivos y aplicaciones de seguridad se administran por OSSIM, mediante una centralización, normalización y priorización de cada una de ellas, y con la correlación automatizada se disminuyen las falsas alarmas, haciendo más fácil y rápido el entendimiento para el administrador de seguridad de lo que está sucediendo en la red.
La administración de los eventos a través de OSSIM, facilita al administrador tener una vista clara de la arquitectura de seguridad, ya que se ofrecen reportes de: incidentes, vulnerabilidades, eventos, alarmas y estado de los equipos. Siendo una manera ágil para la identificación de incidentes de seguridad.
Las directivas dentro de la correlación lógica, ayuda al personal de seguridad a definir eventos complejos y específicos que para la entidad son incidentes de seguridad, permitiendo la personalización y parametrización de acuerdo a los requerimientos específicos del administrador.
Para incorporar nuevas herramientas a OSSIM, se requiere un estudio previo, donde se analice que la nueva integración no afecte a lo que trabaja correctamente, como por ejemplo: inconvenientes con otras herramientas, disminución del rendimiento, consumo excesivo de ancho de banda, entre otras. Entendiendo su funcionamiento y acoplarlo sin inconveniente.
Con la implementación de OSSIM, se contribuye a cumplir uno de los objetivos que persigue la Universidad en el área de tecnología, utilizar soluciones de código libre (Open Source), ya que es la línea de trabajo encaminada en el país.
Se realizan análisis forenses, dado que los eventos referentes a un incidente de seguridad son almacenados. Permitiendo reconstruir y estudiar lo referente al hecho, y con ello encontrar soluciones a los problemas presentados.
De acuerdo a la infraestructura, equipos y servicios que posee la Universidad, se puede afirmar que la herramienta OSSIM se encuentra funcionando en un ambiente de producción.
OSSIM no causa problemas en el rendimiento de la Red de la Universidad. Trabaja con varias herramientas, pero esto no es inconveniente en el ancho de banda, ya que el tráfico de entrada y salida generado no es considerable respecto al tráfico total.

RECOMENDACIONES

Realizar auditorías a la gestión de seguridad, al menos dos veces al año, para validar si se cumplen los requerimientos de seguridad que necesita la entidad y si la herramienta OSSIM cubre las exigencias de monitoreo de red, o se necesita la adquisición de una herramienta comercial.
La implementación de OSSIM se enfoca específicamente a nivel de servidores críticos que posee la Universidad Central “Marta Abreu” de Las Villas, se recomienda su extensión para incorporar los demás segmentos de red y las herramientas o equipos de seguridad necesarios. Ampliando de esta manera el monitoreo de seguridad de la entidad.
La documentación es escasa acerca de su funcionamiento interno y sus configuraciones, se necesita ampliar la misma para impedir cualquier duda, inquietud o problema que se tenga con su implementación.
Como OSSIM está al tanto de lo que ocurre en la red, en el caso de la UTPL que es una entidad educativa y el número de activos a monitorear no es grande.

IR al SUMARIO

Cuando la cantidad de activos a monitorear aumente y los eventos no puedan ser manejados por una persona, se debe crear un SOC (Security Operations Center) para la distribución de monitoreo de red.
El administrador debe estar al tanto de las actualizaciones para OSSIM, para seguir explotándolo y ampliando sus ventajas. Así como la actualización de las herramientas que la integran.
Los cambios de configuraciones, habilitación o eliminación de servicios que se realicen, deben hacerse primero en un ambiente de prueba, y luego de los resultados obtenidos satisfactoriamente incorporarlo al ambiente real.
Para cada configuración que se realice en el servidor OSSIM, se recomienda sacar un respaldo como medida de prevención ante algún incidente que se pueda tener con las mismas.

REFERENCIAS

[1] Corletti Estrada, Alejandro, “Auditoria, Evaluación,Test de Seguridad → metodología abierta ¿OSSTMM…?” [En línea] Disponible: http://www.shellsec.net/documentacion.php?id=20
[2] OSSIM. OSSIM Descripción. [En línea] Disponible: http://www.ossim.net/whatis_es.php
[3] Asensio, Gonzalo, “Gestión de la Seguridad con OSSIM”. [En línea] Disponible: http://www.csae.map.es/csi/tecnimap/tecnimap_2006/taller/Taller_swl_T2006_ITDeusto_OSSIM.pdf , mayo2006
[4] Snort. [En línea] Disponible: http://www.snort.org
[5] Cisco. “Introducing Cisco Intrusion Detection System,Configuration and Operations Guide Version 2.2.2”. [En línea] Disponible: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids5/csidscog/overview.htm
[6] Osiris [En línea] Disponible: <http://osiris.shmoo.com>
[7] Prelude. [En línea] Disponible:http://www.prelude-ids.org
[8] Realsecure. [En línea] Disponible: http://www.conqwest.com/solutions_ISSrealsecure.as
[9] Pads[En línea] Disponible:http://passive.sourceforge.net
[10] Spade. [En línea] Disponible: http://www.sans.org/resources/idfaq/anomaly_detection.php
[11] Demuth, Thomas and Leitner, Achim, “Arp Spoofingand poisoning TRAFFIC TRICKS”. [En línea] Disponible: http://www.linuxmagazine.com/issue/56/ARP_Spoofing.pdf, julio 2005
[12] P0f. [En línea] Disponible: http://www.stearns.org/p0f/
[13] Router Cisco. [En línea] Disponible: http://www.linuxhomenetworking.com/ciscohn/syslog-cisco.htm
[14] Ntop. [En línea] Disponible: http://www.ntop.org
[15] Tcptrack. [En línea] Disponible: http://www.rhythm.cx/~steve/devel/tcptrack/release/1.1.5/docs/tcptrack.1.html
[16] Opennms. [En línea] Disponible: http://www.opennms.org
[17] Nessus. [En línea] Disponible: http://www.nessus.org
[18] Nmap. [En línea] Disponible: http://insecure.org/nmap
[19] Ntsyslog. [En línea] Disponible: http://ntsyslog.sourceforge.net
[20] Syslog. [En línea] Disponible: http://es.wikipedia.org/wiki/Syslog
[21] Snarewindows. [En línea] Disponible: http://www.intersectalliance.com/projects/SnareWindows
[22] Cisco PIX Firewall. [En línea] Disponible: http://www.cisco.com/warp/public/110/pixsyslog.html
[23] Iptables. [En línea] Disponible: http://www.netfilter.org/projects/iptables/index.html
[24] IIS. [En línea] Disponible: http://www.intersectalliance.com/projects/SnareWindows
[25] Apache. [En línea] Disponible: http://httpd.apache.org/docs/2.0/es/logs.html

IR al SUMARIO

EVENTOS

Informática 2009
XIII CONVENCIÓN Y FERIA INTERNACIONAL

Estimados colegas:

Del 9 al 13 de febrero de 2009, La Habana acogerá la XIII edición de la Convención y Feria Internacional Informática 2009, que sesionará en el Palacio de Convenciones de La Habana y en el recinto ferial PABEXPO. ¨Las Tecnologías de la Información y las Comunicaciones como soporte para el desarrollo endógeno y la soberanía tecnológica de los pueblos¨, es el tema central que promoverá el evento, y es la fuente de la invitación a la discusión científico tecnológica, a la exposición de proyectos e iniciativas que promuevan los propósitos y acciones que emprenden los países para impulsar el uso de las TIC en el desarrollo de la sociedad.
Informática 2009 estimulará el intercambio entre profesionales, científicos, técnicos, empresarios, representantes gubernamentales, organismos internacionales y público en general, interesados en investigar, promover, analizar y conocer sobre el avance de las tecnologías de la información, las telecomunicaciones, la electrónica y la automática, así como sus aplicaciones actuales en los diversos sectores de la sociedad.
El Comité Organizador de INFORMÁTICA 2009 les reitera la invitación a presentar sus contribuciones profesionales y muestras comerciales con la garantía de que alcanzaremos los objetivos comunes en un clima de amistad y solidaridad.

Dr. Jorge Luis Perdomo Di-Lella
Presidente Ejecutivo del Comité Organizador
Viceministro de la Informática y las Comunicaciones

AVG Antivirus 6.0 Free Edition

Por:

Ing. Julio Cesar Camps

Email: camps@tesla.cujae.edu.cu

Ficha Técnica	
Fecha:	Septiembre 8/2004
Nombre:	AVG Antivirus 6.0 Free Edition
Propiedad:	GRISOFT Inc.
Versiones:	AVG Antivirus 6.0.756 Free Edition
Tamaño:	6.784Mb
Plataformas	Windows 95/98/Me/NT/2000/XP
Idiomas	Inglés
Clasificación	Downloads/windows/utilidades/antivirus
URL	http://www.grisoft.com
Descripción	AVG Anti-virus Free Edition es una herramienta de protección contra virus bastante bien conocida. Actualizaciones rápidas de sus bases de datos de virus están disponibles durante toda la vida del producto, brindando de esta forma el alto nivel de capacidad de detección que se necesita en la actualidad para proteger nuestras computadoras. Es de muy fácil configuración e instalacion, amén de una muy baja utilización de los recursos del sistema.
Observaciones	Hoy por hoy uno de los mejores Antivirus gratis existentes.
Calificación	Excelente @ @ @ @ @

Características

Calificado como excelente (5 estrellas) en SOFOTEX, www.sofotex.com, se constituye en una herramienta indispensable para los usuarios que desean una adecuada protección y no disponen de grandes recursos en hardware, debido a su ínfimo consumo de recursos. Es un potente paquete antivirus, que se ejecuta en background y chequea el sistema en busca de indicios de infección. Además permite la integración con el cliente de mensajería electrónica Outlook Express de forma que previene la descarga de correos electrónicos infectados.

Podemos enumerar algunas de las características:

1. Actualización automatica del programa y de su base de datos de virus.
2. El AVG resident shield brinda protección en tiempo real.
3. El AVG E-mail Scanner protege tu correo.
4. EL AVG On-Demand Scanner, permite la planificación de tests o su ejecución manual.
5. El AVG Virus Vault permite la manipulación segura de los ficheros infectados.

Resumen

AVG Anti-Virus es un gran programa. Posee todo lo que se espera de un programa antivirus y lo mejor de todo es que es "GRATIS". Asi, que esperas?? Tu PC te lo agradecerá, recuérdalo.

SEGURIDAD

Nuevo objetivo del spam malicioso 09/12/2008

Sophos advierte a los usuarios que extremen las precauciones sobre aquellos mensajes relativos a vuelos, ya que se trata de una campaña de spam maliciosa que dice ofrecer información relativa a transacciones inexistentes.

Los correos electrónicos simulan venir de conocidas líneas aéreas tales como US Airways, Delta y Virgin con mensajes que informan al usuario de que ha registrado una cuenta con una línea aérea y que su tarjeta de crédito ha sido cargada.

Fuente: http://www.diarioti.com

SOFTWARE

Pronostican que Windows 7 será más difícil de usar 09/12/2008

Paul Thurrott, quien ha escrito numerosos manuales sobre los sistemas operativos de Microsoft, siente preocupación de que Windows 7 será innecesariamente complicado. En un comentario en su blog , el experto escribe que los planes de Microsoft de simplificar el interfase podría, paradójicamente, hacer que el sucesor de Windows Vista fuesen más difícil de usar.

Tal apreciación se basa en un análisis preliminar de la versión pre-beta de Windows 7.

Fuente: http://www.diarioti.com

IR al SUMARIO

HARDWARE

Fujitsu presenta nuevo sistema de seguridad para portátiles 09/12/2008

Fujitsu Siemens Computers acaba de presentar un sistema de seguridad disponible durante el primer trimestre de 2009, que permite proteger el ordenador y su información como si de una tarjeta de crédito se tratara.

En concreto, la compañía presenta dos soluciones, System Track y Data Protect, que pueden ser contratadas como opción cuando se compre un ordenador. Las herramientas antirrobo facilitan tanto el rastreo del ordenador ante una pérdida o robo, como la eliminación de la información para que no pueda acceder nadie a él.

Fuente: http://www.diarioti.com

TECNOLOGIA

Gigabyte presenta su tecnología Ultra Durable 3 05/12/2008

Gigabyte anunció la disponibilidad de la tecnología Ultra Durable3 y su placa EP45-UD3.

“Gigabyte da un paso más con su tecnología Ultra Durable 3, el primer diseño de placas de sobremesa con doble lámina de cobre de 2 onzas de peso, para las capas de alimentación y toma de tierra, que proporciona un descenso de la temperatura del sistema, mejorando la eficiencia energética e incrementando la estabilidad en overclocking", dijo Hernán Chapitel, Country Manager para Cono Sur, de Gigabyte.

Fuente: http://www.diarioti.com

IR al SUMARIO

SEGURIDAD

Apple se retracta: "Macintosh no necesita antivirus" 04/12/2008

En los foros dedicados a Apple se ha comentado intensamente la sorpresiva recomendación hecha la víspera por la compañía a los usuarios de Macintosh, en el sentido de usar software antivirus.

El artículo en cuestión, escrito por el departamento de soporte de Apple, ha sido eliminado de su sitio web, supuestamente por contener inexactitudes e información caducada.

"Hemos eliminado el artículo de soporte pues era antiguo e incorrecto", comentó el portavoz e Apple, Bill Evans, a Cnet.

Fuente: http://www.diarioti.com

TELEM@TICA

PARA INSCRIBIRSE EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-subscribe@cujae.edu.cu

PARA ANULAR SU INSCRIPCIÓN EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-unsubscribe@cujae.edu.cu

PARA AUTORES QUE DESEEN PUBLICAR EN TELEM@TICA

Para la publicación en nuestra revista los interesados deberán enviar su propuesta escrita indicando claramente: Título del artículo, glosario de términos (No más de media cuartilla), imágenes referenciadas (No más de 200Kb), nombre de los autores, sus fotografías y la institución a la que pertenecen, así como alguna forma de comunicación (teléfono, Fax o correo electrónico). Para una guía más detallada descargue el formato de publicación de la dirección: http://www.cujae.edu.cu/revistas/telematica/Soporte_Tecnico/formato.doc
Su artículo se someterá a revisión por un comité de árbitros que decidirá sobre la publicación del mismo. Deberán acompañar igualmente (en no más de media cuartilla) un glosario, de los términos más importantes utilizados en el artículo. Puede contactarnos a través de nuestro email telematica@revistas.cujae.edu.cu