AUTOMATIZACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA EN LA UCF

Automation Of Computer Security Controls At UCF

Juan Manuel Castellanos[1]
Elizabeth Toledo[2]
Leónides Castellanos[3]

Resumen: La investigación tuvo como objetivo el automatizar controles de seguridad informática para la seguridad de la información en la Universidad de Cienfuegos (UCF). Se realizó una revisión de las normas, estándares, recomendaciones y controles de seguridad informática. Se determinaron los controles automatizables, CAGv 4. Se caracteriza la red de datos de la UCF, se describen los controles y su implementación. Se realiza una breve descripción de cada una de las herramientas a utilizar en cada control. Se empleó el software libre Alient Vault OSSIM como herramienta de soporte técnico principal y se automatizaron los controles de seguridad informática.

Palabras clave: CAGv 4, Alient Vault, OSSIM.

Abstract: The research aimed to automate computer security controls for information security at the University of Cienfuegos (UCF). A review of the rules, standards, recommendations and computer security controls was carried out. Automated controls were determined, CAGv 4. The data network of the UCF was characterized, the controls and their implementation are described. A brief description is made of each of the tools used in each control. Alient Vault OSSIM free software was used as the main technical support tool and computer security controls were automated.

Keywords: CAGV 4, AlienVault, OSSIM

[1]Ingeniero. Ministerio de Turismo, Cienfuegos Cuba. juanma@get.cfg.tur.cu
[2]Ingeniera. Programa de informática. Universidad de Cienfuegos. Carretera de Rodas Km 4, Cienfuegos, Cuba.
[3]Doctor. Universidad de Pamplona, Carretera Bucaramanga Km1 Pamplona

1. INTRODUCCIÓN

Los servicios de la informática y las telecomunicaciones son de vital importancia para el desarrollo de las organizaciones (Núñez-Pérez, 2015). Actualmente los datos son almacenados, procesados e intercambiados, por lo que, en formato digital es muy fácil su utilización y manejo (Tangarife-Chalarca, 2013). El desarrollo de Internet ha significado que la información esté ahora en muchos sitios, lo que lleva consigo un incremento de las amenazas en la Seguridad de la Información (Santos-Jaimes & Flórez-Fuentes, 2013).

Los delitos informáticos tienen un alcance mayor y pueden incluir delitos tradicionales, como: el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos, en los cuales ordenadores y redes han sido utilizados como medio (Informática Forense Colombia, 2017). Esta diversidad de delitos tiene como objetivos destruir y dañar medios electrónicos y redes de Internet que afectan a cualquier institución (Bustamante-Zapata et al., 2013). Estos delitos provocan grandes pérdidas a cualquier empresa o institución. La seguridad de la información, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento (Montesino-Perurena, 2012), cuyos conceptos son:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

La investigación tuvo como objetivo el automatizar controles de seguridad informática para la seguridad de la información en la Universidad de Cienfuegos (UCF).

2. METODOLOGIA

El proyecto es de tipo descriptivo con enfoque cualitativo (Zuluaga-Duque, 2017). Inicialmente, se determinan los antecedentes y el estado actual de las normativas y estándares nacionales e internacionales, que se emplean en la automatización de controles de seguridad informática, evaluándose su utilización en diferentes casos de estudio. A partir de esta revisión, se seleccionará la más conveniente para la UCF.

A partir del análisis realizado sobre las normativas y estándares existentes, se selecciona la variante a emplear en la UCF y se describen las características y especificidades, exponiéndose además los aspectos teóricos y conceptos asociados al dominio del problema.

Finalmente se realiza la validación de la propuesta de automatización de controles de seguridad informática realizada en la Institución.

3. RESULTADOS

Se revisaron los siguientes estándares:

ISO/IEC 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones (Pinto-Salamanca et al., 2015). ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Esta norma establece un conjunto de 30 actividades para la gestión de la seguridad, define 11 áreas principales de control, para cada una establece 39 objetivos de control y 133 controles (Castellanos-Hernández, 2012).

El NIST SP800-53 tiene como objetivo proporcionar un conjunto rico de controles de seguridad, que satisfacen la amplitud y profundidad de requisitos de seguridad aplicado a los sistemas de información, y que son coherentes y complementarios con otras normas de seguridad establecidas (Cadena-Muñoz et al., 2015).

El objetivo de los CAGv4 (Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines) es la de proteger los activos críticos, la infraestructura y la información mediante el fortalecimiento de la postura defensiva de su organización a través de la protección automatizada y seguimiento permanente de su sensible infraestructura de tecnología de la información, para reducir compromisos, reducir al mínimo la necesidad de los esfuerzos de recuperación, y reducir los costos asociados. Existen veinte controles que son críticos e indispensables en un sistema de seguridad informática. Estos representan un subconjunto de los controles identificados como prioridad uno en el estándar NIST SP 800-53 (CSRC, 2007).

Principales estándares y regulaciones sobre seguridad informática

En el contexto de la seguridad informática existen estándares que constituyen normas certificables, marcos de trabajo que representan una recopilación de mejores prácticas y regulaciones que son de obligatorio cumplimiento en determinadas naciones.

ISO/IEC 27001 y 27002

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a

cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, el intercambio de información y contribuir a la transferencia de tecnologías. La familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad que proporciona un marco para la gestión de la seguridad, los estándares de ISO/IEC 27001 y ISO/IEC 27002 están directamente relacionados con la gestión de la seguridad informática (Montesino-Perurena, 2012). Esta es la principal en cuanto a los requisitos del sistema de gestión de seguridad de la información. Incorpora el típico Plan-Do-Check-Act (PDCA) que significa "Planificar-Hacer-Controlar-Actuar" siendo este un enfoque de mejora continua (Alvarez-Meneses, 2013).

ISF-SoGP. Recomendación de buenas prácticas de seguridad

El Foro de Seguridad de la Información (ISF) es una asociación sin fines de lucro que dedica su actividad a la cibernética, seguridad de la información y gestión de riesgos. Ha publicado el Estándar de Buenas Prácticas (SoGP), un informe que se actualiza anualmente por la organización para reflejar los últimos aspectos de la industria de la seguridad de TI (Giraldo-Plaza et al., 2017). El estándar está dividido en seis aspectos fundamentales, para los cuales se establecen 36 objetivos y 166 controles. Los aspectos son: gestión de la seguridad informática, aplicaciones de negocio críticas, instalaciones de sistemas, redes, desarrollo de sistemas y entorno del usuario final (Díaz-Ricardo et al., 2014).

ISM3. Modelo de madurez para la gestión de la seguridad informática.

ISM3 compuesto por varias empresas y organizaciones, ha desarrollado el Modelo de Madurez de Gestión de la Seguridad Informática (ISM3 por sus siglas en inglés).

Este modelo pretende alcanzar un nivel de seguridad definido, también conocido como riesgo aceptable, en lugar de buscar la invulnerabilidad (Avella-Ibáñez et al., 2017). ISM3 tiene como objetivo la seguridad de la información, el garantizar la consecución de objetivos de negocio. La visión tradicional de que la seguridad de la información, trata de la prevención de ataques es incompleta. ISM3 relaciona directamente los objetivos de negocio (como entregar productos a tiempo) de una organización con los objetivos de seguridad (como dar acceso a las bases de datos sólo a los usuarios autorizados) (Márquez et al., 2017).

Estándares y regulaciones para sectores específicos: PCI DSS, HIPAA.

En la protección de la seguridad de la información en el ámbito de la salud y en el sector del comercio existen estándares a nivel internacional los cuales son HIPAA y PCI DSS respectivamente.

La HIPAA (Health Insurance Portability and Accountability Act) es muy conocida en la esfera de la seguridad informática, fue promulgada por el Congreso de los Estados Unidos. Esta tiene como objetivo ofrecer la posibilidad de transferir y continuar con la cobertura de seguro para millones de trabajadores estadounidenses y sus familias, cuando cambian o pierden sus puestos de trabajo; reduce el fraude de atención médica y el abuso (Techopedia, 2018). El estándar PCI-DSS (Payment Card Industry Data Security Standard) consiste en una serie de normas de seguridad que exigen doce requerimientos de seguridad agrupados en seis categorías (DSS, 2016).

Estándares y regulaciones de alcance regional. Existen también otras guías y regulaciones que tienen un carácter regional. En general la mayoría de los países poseen regulaciones relacionadas con la seguridad informática. Algunas recomendaciones son conocidas fuera de sus fronteras porque constituyen guías de buenas prácticas aplicables a diferentes organizaciones. Cabe mencionar aquí al IT Baseline; Protection Catalog (IT-Grundschutz) de Alemania (Softpedia, 2015), y el Manual de Seguridad de la Información (ISM) de Australia (Criptored, 2015).

En el caso de Cuba la Resolución 127/2007 del MIC, constituye el marco regulatorio nacional en materia de seguridad de la información. Esta resolución posee cien artículos de los cuales ochenta y nueve constituyen controles de seguridad informática que deben ser implementados en las instituciones.

CAG. 20 controles críticos de seguridad

De acuerdo a un estudio realizado por un gran número de expertos de seguridad informática, que fue publicado bajo el título Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG), existen 20 controles de seguridad técnicos específicos que se consideran eficaces, la selección de estos controles está basado en los actualmente conocidos ataques de alta prioridad, así como esos tipos de ataque esperados en el futuro próximo (TCSCECD, 2011).

Métricas de Seguridad Informática

En seguridad informática es más común el término “métrica” la cual se define como una medida o conjunto de medidas que permiten caracterizar, conocer, estimar o evaluar un atributo especificado (Mercado-Ramos et al., 2015).

Tipos de métricas

La madurez de una organización y de su sistema de seguridad informática determinan los tipos de métricas que pueden utilizarse. Esta madurez está determinada por la existencia e institucionalización de procesos y procedimientos en la organización. Las métricas de seguridad

informática se clasifican entonces de la siguiente manera (Villegas, 2016): Métricas de implementación: Métricas de efectividad y Métricas de impacto en el negocio:

Fuentes de datos para las métricas

Para calcular los indicadores de seguridad informática que se definan, es necesario obtener los datos que permitan realizar los análisis correspondientes. Los datos para las métricas de seguridad informática pueden provenir de una gran variedad de fuentes, entre las que cabe mencionar las siguientes (Voutssas, 2010):

Selección de métricas e indicadores

Es evidente que existen un sin fin de métricas e indicadores posibles a desarrollar y que la mayoría de ellos sean interesantes para la compañía. Sin embargo, los recursos de cualquier compañía son limitados (y muchas veces escasos) por lo tanto, sólo se deben desarrollar aquellos que son rentables para la compañía, es decir, aquellos para los cuales la importancia de la información que aporten justifique el esfuerzo que hay que realizar para su obtención.

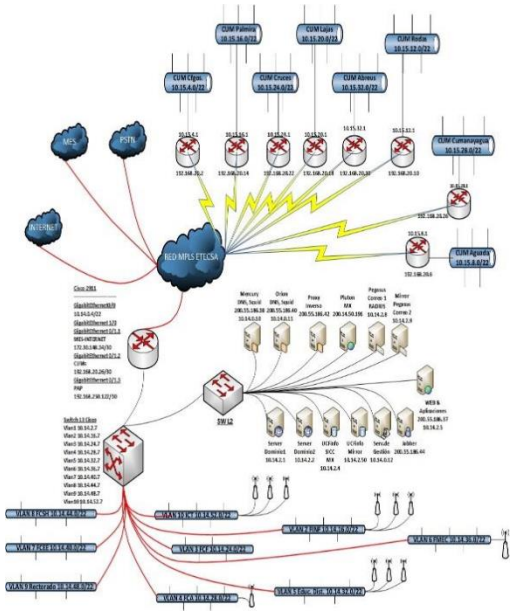
Caracterización de la red de datos de la UCF

La Universidad de Cienfuegos cuenta con 1336 trabajadores y 2013 estudiantes, con un total de 3349 usuarios en la red. Está conformada por la sede principal "Carlos Rafael Rodríguez", el pedagógico "Conrado Benítez" y los 7 Centros Universitarios Municipales (CUM, para brindar los diferentes servicios cuenta con una red IP de comunicación de datos WAN y para el establecimiento de la comunicación entre las diferentes subredes se utiliza el protocolo Frame Relay y Ethernet (Jiménez & Barrera, 2018).

El nodo central está ubicado en la oficina de los Administradores de Red en la Sede "Carlos Rafael Rodríguez", la topología utilizada para la conexión es la tipa estrella, ya que todos los nodos se conectan a este nodo central. Este se ubica en la oficina de los Administradores de red, se conecta a Internet, a la red universitaria (MES) y la PSTN mediante el router cisco 2911, a través de una fibra óptica mono modo que se conecta a la red MPLS de ETECSA. La conexión con ETECSA está compuesta por tres VPN, la primera está destinada para la red del MES e Internet con una velocidad de 20Mbits/s, la cual tiene un ancho de banda de 13 Mbps y 7 Mbps, respectivamente.

El tráfico procedente de la sede "Conrado Benítez" y de las 7 CUMs, está destinado a la segunda VPN es de 4Mbits/s; con ancho de banda de 2Mbps y las 7 restantes a 128 Kbps. Todas conectadas a ETECSA por Frame Relay, La tercera VPN es de 512 Kbps y está orientada al PAP.

En el nodo central se encuentran ubicados todos los servidores, como servidores de correo, de dominio, web y proxi. El router 2911 se conecta a un Switch capa 3 al que se vinculan varias VLAN, las cuales identifican a cada facultad de la universidad, la conexión de estas con el nodo central es Gigabit Ethernet y se hace a través de fibra óptica que se muestra en la figura 1.



Gestión automatizada de controles de seguridad informática.

En la elaboración de un modelo de gestión establecido en la integración y automatización de controles, es necesario tener en cuenta el concepto de gestión automatizada de controles (Castellanos-Hernández, 2012). Los controles necesitan ser adecuadamente establecidos, implementados, operados, monitorizados, revisados, mantenidos y mejorados, para garantizar el cumplimiento de los objetivos del sistema de seguridad informática. Por tanto, gestionar los controles de seguridad informática implica realizar las siete acciones mencionadas (Castellanos-Hernández, 2012). La gestión automatizada de un control de seguridad informática implica que la operación, monitorización y revisión del mismo se realizan de forma automática, mediante sistemas informáticos y/o herramientas de hardware existentes; sin que se produzca intervención humana en la realización de estas acciones.

Controles de seguridad informática automatizables

Según el concepto de automatización en la sección anterior, los controles automatizables que se pueden implementar mediante sistemas informáticos y/o herramientas de hardware son los que están relacionados con medios técnicos. Dentro del estudio de los veinte controles

críticos existen quince controles que pueden ser automatizados, cinco de estos necesitan intervención humana para su automatización (Montesino-Perurena, 2012).

Control Críticos 1: Inventario de dispositivos autorizados y no autorizados.
Control Críticos 2: Inventario de software autorizado y no autorizado.
Control Críticos 3: Configuraciones de seguridad para hardware y software
Control Críticos 4: Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches.
Control Críticos 5: Límites de Defensa.
Control Críticos 6: Mantenimiento, Monitoreo y Análisis de Seguridad de Registros de Auditoría. Control Críticos 7: Aplicación de Software de Seguridad.
Control Críticos 8: Uso controlado de privilegios administrativos.
Control Críticos 9: Acceso controlado Basado en necesidad de saber
Control Críticos 10: Evaluación de la vulnerabilidad continua y Remediación.
Control Críticos 11: Monitoreo y Control de Cuenta.
Control Críticos 12: Defensa de malware.
Control Críticos 13: Limitación y Control de Red de puertos, protocolos y servicios.
Control Críticos 14: Control de dispositivos inalámbricos.
Control Críticos 15: Prevención de Pérdida de Datos.

Existe una relación entre las normas ISO/IEC 27001, el estándar NIST 800-53 y los Veinte Controles Críticos CAGv 4.

Ejemplos de controles que no son automatizables

En la lista de los veinte controles críticos, cinco de estos no pueden ser monitoreados de forma automática, sino que se necesita de intervención humana:

Control Críticos 16. Seguros de Ingeniería de Red
Control Críticos 17. Pruebas de Penetración y Equipo Rojo Ejercicios
Control Críticos 18. Respuesta a Incidentes de Capacidad
Control Críticos 19. Capacidad de Recuperación de Datos de Seguridad
Control Críticos 20. Evaluación de Habilidades y formación adecuadas para colmar las lagunas.

Herramienta utilizada para la automatización de controles.

Para la gestión automatizada de controles de seguridad informática se necesita un sistema que analice, visualice y gestione de manera centralizada los eventos que ocurren en los componentes de la infraestructura IT de la UCF, obteniendo de esta forma mayor efectividad a la hora de monitorear y de encontrar errores y vulnerabilidades en la seguridad de la red Miranda-Cairo et al., 2016().

Existen diversas aplicaciones para la automatización de controles de seguridad informática, algunas gratuitas y otras de pago. En la siguiente tabla se muestra una comparación de algunas herramientas.

	OSSI M	**Hyperi c HQ**	**Securi a SGSI**	**RSA**	**NET IQ**
Tipo de licencia	Gratis	Gratis	Gra/Pa	Pagad	Pagad
Exploración de redes	Si	No	Si	Si	Si
Detección de intrusos	Si	Si	Si	Si	Si
Detección de vulnerabilidades	Si	No	Si	No	No
Monitorización	Si	Si	No	Si	Si
Plugins free	Si	Si	Si	No	No
Notificaciones	Si	Si	No	Si	Si
Network IDS	Si	No	No	No	No
Interfaz Web	Si	Si	Si	No	No

Tabla 1. Comparación de herramientas.

Características de OSSIM son:

Realiza detección a bajo nivel y en tiempo real de la actividad anómala:

Análisis de comportamiento de red

Gestión de registros forenses

Realiza análisis del riesgo de seguridad

Presenta informes ejecutivos y técnicos

Arquitectura escalable de alto rendimiento

Es gratuito

Características de Hyperic HQ

Rápida implementación.

Trabaja correctamente en múltiples plataformas como Unix, Linux, Windows, Solaris, AIX, HPUX, VMware, y Amazon Web Services. Monitorea todo tipo de aplicaciones: Monitoreo de hardware, métricas de rendimiento, accesos, cambios de configuración.

Características de Securia SGSI

Es una herramienta de compliance totalmente gratuita y de código cerrado.

Esta herramienta realiza un seguimiento de la implementación de la norma ISO/IEC 27001:2005, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información. Es un software completamente gratuito que se estructura en cuatro módulos:

Módulo de Gestión Documental.

Módulo de Análisis y Gestión de Riesgos.

Módulo de Gestión de Incidencias y No Conformidades.

Módulo de Mejora Continua.

Características de RSA

Es un sistema criptográfico asimétrico, este funciona mediante el cálculo de llaves públicas que se realiza en secreto en la computadora en la que se va a guardar la llave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

Características de NET IQ

Gestor de Identidades con Interfaz de Usuario: una intuitiva interfaz de usuario de negocios para la solicitud y aprobación de accesos.

Administrador de Catálogo de Roles y Recursos: es una interfaz de analista de negocios para la gestión de roles y recursos.

Aprobaciones desde Móvil: una aplicación móvil nativa para gerentes ocupados, con el fin de proporcionar aprobaciones de acceso.

Servicio de Recolección de Autorizaciones y Conciliación: automatiza la gestión de autorizaciones (derechos) en los sistemas conectados para mantener recursos disponibles en el catálogo.

Al comparar y realizar una caracterización de cada una de las herramientas, se pudo llegar a la conclusión que la herramienta más íntegra es OSSIM para la automatización de controles de seguridad informática en la UCF

OSSIM: Definición

La sigla OSSIM se deriva para Open Source Security Information Management (Herramienta de código Abierto para la Gestión de Seguridad de la Información). OSSIM no es una herramienta única, al decir OSSIM se entiende que es un conjunto de herramientas unidas en un solo programa que facilita el análisis, visualización y la gestión de manera centralizada de los eventos que ocurren en los diferentes componentes de la infraestructura IT de la empresa, obteniendo de esta forma mayor efectividad a la hora del monitoreo y de encontrar errores y vulnerabilidades en la seguridad de la red.

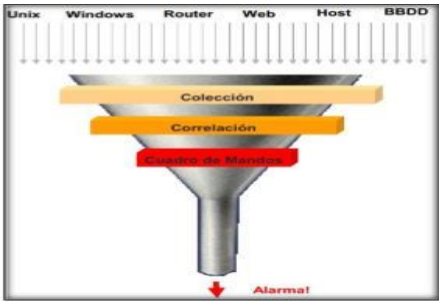


Figura 2 Modelo de OSSIM

Ventajas: Tiene muchas ventajas para hacer la vida fácil al administrador de red, ya que su prioridad es presentar un ambiente centralizado para el fácil monitoreo y correcciones. En esta herramienta se puede destacar dos funciones primordiales y que son de gran ayuda a la hora de hacer un plan de mejoras en la seguridad de la red: Correlación y Valoración de Riesgo.

Desventajas: No presenta una mayor desventaja ya que es una herramienta fácil de usar y de manipular, además se le puede añadir herramientas como sea necesario. Otra de las desventajas es que esta herramienta solo almacena los logs en los cuales están todos los problemas e inconvenientes que pasa en la red y en los servidores, y solo los reporta a la persona encargada.

Informes de vulnerabilidades y alarmas en general

Los informes de las vulnerabilidades se realizan a través de los dispositivos de red que son monitoreados por OSSIM, en esta sección se presentan las diferentes herramientas que se instalaron con sus respectivos reportes.

El reporte de alertas se realiza mediante la herramienta de código abierto Nagios, la cual es la encargada de la monitorización de redes, que vigila los equipos (hadware) y servicios (software) alertando cuando el comportamiento de los mismos es no deseado.

Esta herramienta ayuda a los administradores de red en el control de lo qué está pasando en la red, y a conocer los problemas que ocurren en la infraestructura que administran antes de que los usuarios de la misma los perciban, para así, poder tomar la iniciativa; decidir en cada momento lo que se quiere hacer y cómo se va a hacer. Este software nos permite obtener datos, interpretarlos y tomar decisiones (Sans Institute, 2015). Las alarmas brindan diversas informaciones como el estado en red, tiempo arriba, puertos abiertos, servicios y procesos corriendo, carga de CPU, carga de memoria física, carga de memoria virtual, espacio en disco, interfaces de red activas.

En la siguiente figura se muestran diferentes tipos de alarmas: Compromiso del Sistema, Explotación e Instalación, Entrega y Ataque, Reconocimiento y Sonido, Advertencia Ambiental. En la de tipo Explotación e Instalación existen un mensaje, esto quiere decir, que esta alarma se ha activado por fuerza bruta.

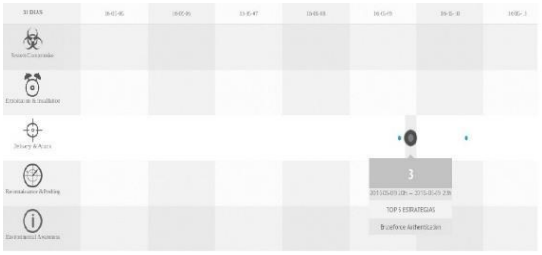


Figura 3 Reportes de alarmas

El presente Gráfico brinda un análisis estadístico de los últimos eventos generados por los diferentes servicios delservidor Linux OSSIM.

Figura 4. Análisis estadísticos de los últimos eventos

Este informe presenta una estadística resumida de todos los sensores o plugins configurados para recolectar la información.

Figura 5 Análisis resumidos de los sensores

Generación de informes de los eventos de la red

El servidor de OSSIM realiza un escaneo a las redes o red a las que tenga acceso, lo que da un reporte de los activos que están siendo censados por OSSIM; a esto se le llama eventos de red.

El reporte de eventos en la red se ejecuta mediante la herramienta OpenVas, es un software, que ofrece un marco de trabajo para integrar servicios, herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos y el control de accesos e intrusos. Permite analizar un PC o un servidor local/remoto y realizar varios tipos de informes sobre las vulnerabilidades detectadas.

Generación de informes del tráfico de red

En el escaneo del tráfico de red se utilizó la herramienta nfsen que utiliza el protocolo de red

Netflow, desarrollado por Cisco, esta recolecta la información de las interfaces y comprende mejor el comportamiento de éstas en la red.

Es utilizada para la optimización de la red con una visión holística acerca del ancho de banda de red y los patrones de tráfico. Es una solución unificada que recoge, analiza e informa sobre quién y para qué se ha utilizado el ancho de banda de la red (Santos-Jaimes & Flórez-Fuentes, 2013). El tráfico de red de Internet y el MES se muestra en la siguiente figura donde se observa un alto consumo del ancho de banda en algunos intervalos de tiempo llegando a consumir hasta 6 M/s y 7 M/s respectivamente. El tráfico de salida (IN) es muy elevado respecto al de entrada (OUT).

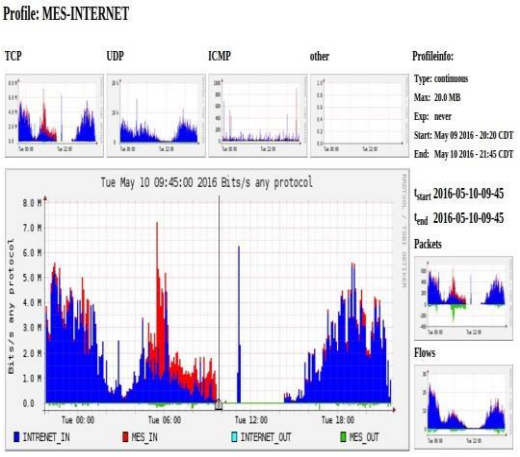


Figura 3.5 Reporte de tráfico de red

La automatización de los controles critico 1: Inventario de dispositivos autorizados y no autorizados, 2: Inventario de software autorizado y no autorizado; se alcanzó mediante la implementación de esta herramienta. Esta brinda en gran medida una ayuda primordial a los administradores de red, ya que, ofrece un reporte detallado con cada dispositivo o software sospechoso que se conecta a la red de datos.

En el caso de ser un dispositivo, nos brinda como información su dirección IP, tipo de dispositivo, si es vulnerable o no.

En el caso de ser un software, nos alerta acerca de su sistema operativo y las aplicaciones que existen en él.

Generación de informes de logs

Fail2ban es una aplicación que escanea ficheros de log y restringe las IPs que muestran un comportamiento malicioso, como por ejemplo múltiples intentos fallidos de inicio de sesión a través de SSH. Generalmente Fail2ban se utiliza para actualizar las reglas de un firewall y rechazar las direcciones IP durante un período especificado de tiempo, aunque cualquier otra acción, como por ejemplo el envío de un correo electrónico, también puede ser configurada.

Dentro de sus principales características se encuentran:

- Arquitectura cliente/servidor.
- Altamente configurable.
- Analiza los archivos de registro log y busca patrones específicos.
- Gestiona la rotación de los archivos de log.
- Puede manejar múltiples servicios (sshd, apache, vsftpd, etc)

4. CONCLUSIONES

Se identificaron las normas y estándares referentes a la automatización de controles de seguridad informática, destacándose los controles CAG v4 y NIST 800-53.

Se caracterizó la red de datos UCF, con respecto a la seguridad informática.

La automatización de controles de seguridad informática se diseñó mediante el software Alient Vault OSSIM, este muestra los informes de vulnerabilidades y alarmas.

REFERENCIAS

Avella-Ibáñez, C. P., Sandoval-Valero, E. M., & Montañez-Torres, C. (2017). Selección de herramientas web para la creación de actividades de aprendizaje en Cibermutua. Revista de investigación, Desarrollo e Innovación, 8(1), 107-120. doi: 10.19053/20278306.v8.n1.2017.7372

Bustamante-Zapata, L. F., Porto-Pérez, I. A., & Hernández-Taboada, F. (2013). Gestión estratégica de las áreas funcionales de la empresa: una perspectiva competitiva internacional. Revista de Investigación, Desarrollo e Innovación, 4 (1), 56-68. doi: 10.19053/20278306.2607

Cadena-Muñoz, E., Eslava-Blanco, H. J., Páez-Parra, I. P. (2015). CAPA FÍSICA Y ALGORITMOS DE PLANIFICACIÓN DE ENLACE DESCENDENTE EN LTE Y WiMAX. Revista Colombiana de Tecnologías De Avanzada, 2 (26), 28–30.

Castellanos-Hernández, J. M. (2012). Implementación de un Centro de Monitoreo y Servicios TI para CUVENPETROL S.A. basado en ITIL. Universidad Central «Marta Abreu» de Las Villas, Villa Clara, Cuba.

Computer Security Resource Center, CSRC. (diciembre de 2007). NIST SP 800-53 Revision 2. Recuperado de: https://csrc.nist.gov/publications/detail/sp/800-53/rev-2/archive/2007-12-19.

Criptored (2015). ISM3 v1.20: Information Security Management Maturity Model. Recuperado de: http://www.criptored.upm.es/guiateoria/gt_m446a. htm.

Díaz-Ricardo, Y., Pérez-del Cerro, Y., & Proenza-Pupo, D. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. Ciencias Holguín, 20 (2).

DSS, P. (2016). Payment Card Industry Data Security Standards. International Information Security standard.

Informática Forense Colombia (marzo 12 de 2017). Delito informático. Recuperado de: https://www.informaticaforense.com.co/delito-informatico/

Giraldo-Plaza, J. E., Ruiz-Nuñez, M. A., Rosero-Noguera, C. A., & Zapata-Puerta, L. N. (2017). Formación en competencias específicas para la industria del software colombiano. Experiencias del uso del aprendizaje basado en proyectos. Revista Colombiana de Tecnologías de Avanzada, 1 (27). Recuperado de: http://ojs.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/2529/0

Jiménez, R., & Barrera, D. (2018). Comunicación OPC para el enlace entre los sofware de rockwel automation del plc allen bradley micrologix 1000 e intouch. Infometric@ - Serie Ingeniería, Básicas y Agrícolas, 1 (1), 184-190. Recuperado de: http://cienciometrica.com/infometrica/index.php/syh/article/view/26

Márquez, L., Lara, Y., & Ángulo, F. (2017). Prototipo de control de acceso a aulas y registro automatico de asistencia. Revista colombiana de Tecnologías de Avanzada, 2 (26). Recuperado de: http://ojs.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/viewFile/2397/1193

Mercado-Ramos, V. H., Zapata, J., & Ceballos, Y. F. (2015). Herramientas y buenas prácticas para el aseguramiento de calidad de software con metodologías ágiles. Revista de Investigación, Desarrollo e Innovación, 6(1), 73–83. doi: https://doi.org/10.19053/20278306.3277

Miranda-Cairo, M., Valdés Puga, O., Pérez-Mallea, I., Portelles-Cobas, R., & Sánchez-Zequeira, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Revista Cubana de Ciencias Informáticas, 10(2), 14-26.

Montesino-Perurena, R. (2012). MODELO PARA LA GESTIÓN AUTOMATIZADA E INTEGRADA DE CONTROLES DE SEGURIDAD INFORMÁTICA. Universidad de las Ciencias Informáticas, La Habana, Cuba.

Núñez-Pérez, V. (2015). Pedagogía social e interculturalismo: una lectura posible. Revista de Investigación, Desarrollo e Innovación, 5 (2), 141–149. doi: 10.19053/20278306.3716

Pinto-Salamanca, M. L., Sofrony-Esmeral, J. I., & Jiménez, D. F. (2015). Detección de colisiones con librerías V-Collide y PhysX para interacción virtual con interfaces hápticas. Revista de Investigación, Desarrollo e Innovación, 5 (2), 119–128. doi: 10.19053/20278306.3721

Resolución 127/2007 MIC. Reglamento de seguridad para las tecnologías de la información.” Ministerio de la informática y las comunicaciones (MIC), 2007.» .

Sans Institute (2015). CIS Critical Security Controls. Recuperado de: https://www.sans.org/critical-security-controls. [Accedido: 01-jun-2016].

Santos-Jaimes, L. M., & Flórez-Fuentes, A. (2013). Metodología para el análisis forense en Linux. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA, 2 (20), 90-96. Recuperado de : http://revistas.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/194

Softpedia (2015). Standard of Good Practice 2013 Released by Information Security Forum. Recuperado de: http://news.softpedia.com/news/Standard-of-Good- Practice-2013-Released-by-Information-Security- Forum-369424.shtml.

Tangarife-Chalarca, D. (2013). Desarrollo de una aplicación web para el montaje de una mesa quirúrgica en el área de traumatología. Revista de Investigación, Desarrollo e Innovación, 4(1), 32-44. doi: https://doi.org/10.19053/20278306.2124

Techopedia(enero de 2018). What is NIST 800-53?. Recuperado de: https://www.techopedia.com/definition/28830/nist-800-53.

TCSCECD (2011). Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG). Recuperado de: www.thecre.com/fisma/wp-content/uploads/2011/02/Twenty_Critical

Villegas , A. (2016). Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática. Recuperado de: http://publicaciones.urbe.edu/index.php/telematiqu e/article/viewArticle/975/html.

Voutssas, M. (2010). Preservación documental digital y seguridad informática. Investigación bibliotecológica, 24(50), 127-155.

Zuluaga-Duque, J. F. (2017). Relación entre conocimientos, saberes y valores: un afán por legitimar los saberes más allá de las ciencias. Revista de Investigación, Desarrollo e Innovación, 8(1), 61-76. doi: 10.19053/20278306.v8.n1.2017.5973