11

Fecha de presentación: septiembre, 2018
Fecha de aceptación: diciembre, 2018
Fecha de publicación: enero, 2019

SISTEMA

DE GESTIÓN DE COMUNICACIONES PARA EVALUAR RIESGOS DE SEGURIDAD

COMMUNICATIONS MANAGEMENT SYSTEM TO ASSESS SECURITY RISKS

Yury A. Toro Flores[1]
E-mail: ytoro@unsa.edu.pe
ORCID: http://orcid.org/0000-0002-3129-481X
Fancy U. Rivas Almonte[1]
E-mail: frivas@unsa.edu.pe
Osbaldo Turpo Gebera[1]
E-mail: oturpo@unsa.edu.pe
ORCID: http://orcid.org/0000-0003-2199-561X
Luis Cuadros Paz[1]
E-mail: lcuadrosp@unsa.edu.pe
Walter Fernández Gambarini[1]
E-mail: wfernandezg@unsa.edu.pe
Enrique Valderrama Chauca[1]
E-mail: evalderrama@unsa.edu.pe
[1]Universidad Nacional de San Agustín. Arequipa. Perú.

Cita sugerida (APA, sexta edición)

Toro Flores, Y. A., Rivas Almonte, F. U., Turpo Gebera, O., Cuadros Paz, C., Fernández Gambarini, W., & Valderrama Chauca, E. (2019). Sistema de gestión de comunicaciones para evaluar riesgos de seguridad. *Universidad y Sociedad, 11*(1), 86-92. Recuperado de http://rus.ucf.edu.cu/index.php/rus

RESUMEN

En el artículo se realiza la evaluación del tráfico y la seguridad en la red a partir de la metodología de seguridad informática de Benson (2001), para detallar cada una de sus fases y mitigar los riesgos. En los resultados obtenidos se puede observar el análisis de los logs generados por Suricata-IDS, un resumen de cuadros con el tráfico generado en la organización durante un periodo de tiempo determinado, así como un resumen de los ataques que fueron procesados o que se encuentran en cuarentena esperando ser analizados. Como conclusión, se obtiene que es de gran ayuda el almacenamiento de tráfico generado para evaluar los riesgos de seguridad, cada vez que un nuevo fallo de seguridad es descubierto para establecer controles de seguridad y reducir así la superficie de ataque y exposición, así como la presentación de resultados ante el usuario de una forma comprensible para la ayuda en la toma de decisiones respecto a las políticas de seguridad implementadas.

Palabras clave: Sistema de detección de intrusos, Control de seguridad, Logs, Superficie de ataque.

ABSTRACT

In the article is made the evaluation of the traffic and the security in the network is made starting from the methodology of computer security of Benson (2001), fordetail each of its phases to mitigate risks. In the results you can see the analysis of logs generated by Suricata IDS, a summary of pictures with traffic generated in the organization over a given time period and a summary of the attacks were prosecuted or found in quarantine, waiting to be analyzed. In conclusión, it is obtained that is helpful storage traffic generated to assess security risks every time a new security flaw is discovered to establish security control and reduce the attack surface and exposure, as well as the presentation of results to the user in an understandable for help in making decisions on security policies implemented.

Keywords: Intrusion detection system, Security control, Logs, Attack Surface.

INTRODUCCIÓN

En vista de la importancia que han tomado las redes de datos en las distintas organizaciones como empresas, universidades, etc. Todas buscan tener la mayor seguridad en su arquitectura de red para evitar pérdidas económicas, así como evitar poner en riesgo los pilares de seguridad informática (Poljak, Ševo & Livaja, 2016). En vista que la información representa el factor primordial por el cual muchos usuarios malintencionados cometen actos ilícitos, con herramientas y técnicas que requieren muy poco nivel técnico, logrando en la mayor cantidad de casos comprometer la seguridad de las comunicaciones. En ese entender, se hace posible disminuir el nivel de riesgo de forma significativa y con ello la materialización de las amenazas y la reducción del impacto sin necesidad de realizar elevadas inversiones ni contar con una gran estructura de personal, para ello, se hace necesario conocer y gestionar de manera ordenada los riesgos a los que está sometido el sistema informático, considerando procedimientos adecuados y planificando e implantando los controles de seguridad que correspondan (Maheshwari, Krishna & Brahma, 2014). Así también, resulta importante llevar un registro histórico del tráfico generado para poder revisarlo cada vez que un fallo de seguridad desconocido se hace público, para de esta manera, poder medir el impacto de dicho fallo en la organización. En esa intención, se tiene como objetivo servir como medio de consulta para apoyar la implementación de nuevos sistemas de seguridad (Al-Dalky, Salah, Al-Qutayri & Otrok, 2014).

A. Objetivos del estudio

- Detección temprana de ataques nuevos en la red para poder optar por medidas correctivas.
- Encontrar las vulnerabilidades que tienen las organizaciones en sus sistemas de comunicaciones.
- Control de acceso a servicios restringidos mediante políticas de seguridad.
- Identificar el impacto operacional por fallas en los sistemas de información y comunicaciones de una organización.
- Relacionar las diferentes formas de prevención a los diversos ataques a las infraestructuras de red.
- Control de tráfico por parte del personal para evaluación del desempeño.
- La importancia de los objetivos mencionados tiene que ver con brindar a la organización total transparencia en las comunicaciones, para poder tomar medidas ante acontecimientos que puedan poner en riesgo la organización, así como preservar los pilares de la seguridad informática que, según Amran & Saad (2014), son:
- Confidencialidad: Se refiere a la protección de datos frente a la difusión no autorizada.
- Disponibilidad: Se refiere a la continuidad operativa de la entidad, la perdida de disponibilidad puede implicar, la pérdida de productividad.
- Integridad: Es necesario asegurar que los datos no sufran cambios no autorizados.

B. Estado del arte

En Han, Kwon, Hahn, Koo & Jur (2016), se describe un Man-in-the middle (MITM) que permite a un atacante supervisar el intercambio de comunicación entre dos partes, dirigiendo el tráfico entre ellos, para pasar por la máquina del atacante. La mayoría de los sistemas existentes que descubren el MITM se centran en detectar los mecanismos que utilizan los atacantes para dirigir el tráfico a sus dispositivos. En este trabajo se presenta un nuevo esquema de detección que se basa en la coincidencia de la carga útil de las tramas intercambiadas en la red. El esquema propuesto es independiente del mecanismo utilizado para lanzar el ataque MITM. El resultado experimental muestra que el esquema propuesto puede alcanzar un excelente rendimiento de detección con la elección adecuada de los parámetros de ajuste del régimen. Según Husák, Cermák, Jirsík & Celeda (2015); y Al-dalky, Salah, Al-qutayri & Otrok (2014), explican como un ataque MITM (man-in-the-middle) se hace generalmente por spoofing entre la red de punto de acceso y los clientes. En este trabajo, se propone un algoritmo, SAL-HASH, para detectar ataques MITM sin necesidad de certificaciones (Atanasovski & León-García, 2015). En este artículo se estudia que en la simulación de IP, las direcciones IP se pueden falsificar fácilmente, por lo tanto, hace que sea difícil para filtrar los paquetes legítimos de los falsificados, en Chakraborty, Chaki & Cortesi (2010) se presenta un sistema de correlación de alertas para mitigar el problema de los falsos positivos en los sistemas de detección de intrusos, cuando se aplican técnicas de detección de anomalías. El sistema permite la evaluación cuantitativa de la probabilidad de que una alerta emitida a causa de una anomalía se convierte en una amenaza real.

MATERIALES Y MÉTODOS

La metodología de seguridad informática, según Benson (2001), específicamente, fue diseñada para apoyar a quienes trabajan con el desarrollo de la seguridad, las estrategias y planes para la protección de la disponibilidad, integridad y confidencialidad de los datos de los sistemas

informáticos. Como se puede ver en una descripción definida en la figura 1.

Existen cuatro pasos a seguir dentro de esta metodología.

1. Identificar métodos, herramientas y técnicas de ataques probables: Métodos, herramientas y técnicas de ataques que pueden abarcar, desde algo como los diversos virus existentes hasta las nuevas metodologías de implantación codificada de sistemas que alteran e infringen contra la integridad y estabilidad de los datos.
2. Establecer estrategias pro-activas y reactivas: Nos encamina a reducir al mínimo las directivas de seguridad así como de desarrollar planes de contingencia.
3. Pruebas: Se debe llevar a cabo luego de que se haya puesto en marcha las estrategias pro-activas y reactivas, con el fin de mejorar las directivas y controles de seguridad a implementar posteriormente.
4. Formar equipos de respuestas a incidentes: Se identifican herramientas de software para responder a incidentes, realización de actividades formativas, junto con la ejecución de estudios a ataques al sistema.

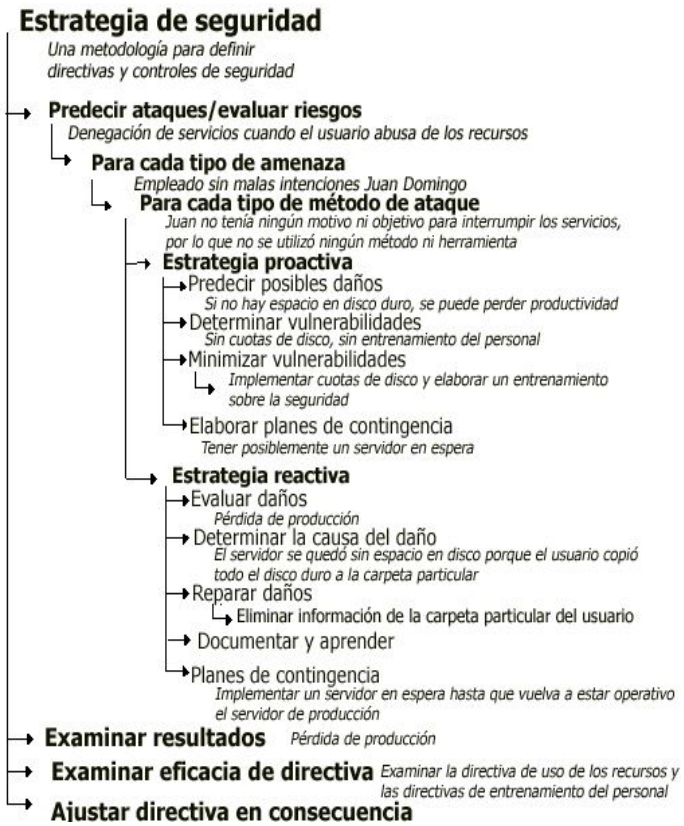

Figura 1. Metodología de seguridad según Benson (2001).

En conjunto, con esta metodología se tomó en cuenta para la implementación de SGSI (Sistema de Gestión de Seguridad de Información), como se aprecia en la figura 2 y se detalla en la tabla 1:

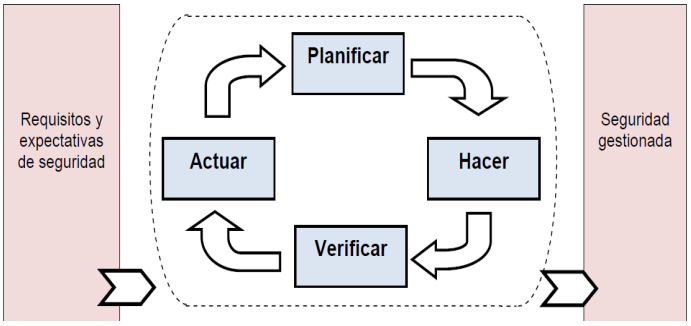

Figura 2. Modelo PHVA para desarrollo de un SGSI.

Tabla 1. Modelo PHVA SGSI.

Planificar	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la organización.
Hacer	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos
Verificar	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión
Actuar	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

RESULTADOS

En los resultados obtenidos, como se observa en la figura 3, se define que el guardar los registros de tráfico generado en la red de datos con un gran detalle, facilita la inspección de los mismos para el análisis de posteriores eventualidades en casos específicos, donde se necesite realizar una auditoría de una conexión en concreto.

```
"Nagata" : "        [Destination GeoIP Country: Peru]" }
"Nagata" : "        [Destination GeoIP Latitude: -12.043300]" }
"Nagata" : "        [Destination GeoIP Longitude: -77.028297]" }
"Nagata" : "User Datagram Protocol, Src Port: 15092 (15092), Dst Port: 53 (53)" }
"Nagata" : "    Source Port: 15092" }
"Nagata" : "    Destination Port: 53" }
"Nagata" : "    Length: 43" }
"Nagata" : "    Checksum: 0x5fe6 [validation disabled]" }
"Nagata" : "        [Good Checksum: False]" }

"Nagata" : "        [Bad Checksum: False]" }
"Nagata" : "    [Stream index: 0]" }
"Nagata" : "Domain Name System (query)" }
"Nagata" : "    Transaction ID: 0xf81a" }
"Nagata" : "    Flags: 0x0100 Standard query" }
"Nagata" : "        0... .... .... .... = Response: Message is a query" }
"Nagata" : "        .000 0... .... .... = Opcode: Standard query (0)" }
"Nagata" : "        .... ..0. .... .... = Truncated: Message is not truncated" }
"Nagata" : "        .... ...1 .... .... = Recursion desired: Do query recursively" }
"Nagata" : "        .... .... .0.. .... = Z: reserved (0)" }
"Nagata" : "        .... .... ...0 .... = Non-authenticated data: Unacceptable" }
"Nagata" : "    Questions: 1" }
"Nagata" : "    Answer RRs: 0" }
"Nagata" : "    Authority RRs: 0" }
"Nagata" : "    Additional RRs: 0" }
"Nagata" : "    Queries" }
"Nagata" : "        www.google.com.pe: type A, class IN" }
"Nagata" : "            Name: www.google.com.pe" }
"Nagata" : "            [Name Length: 17]" }
"Nagata" : "            [Label Count: 4]" }

"Nagata" : "            Type: A (Host Address) (1)" }
"Nagata" : "            Class: IN (0x0001)" }
"Nagata" : "" }
"Nagata" : "     2 0.000000       192.168.1.5           200.48.225.130        DNS
"Nagata" : "" }
"Nagata" : "Frame 2: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)" }
"Nagata" : "    Encapsulation type: Ethernet (1)" }
"Nagata" : "    Arrival Time: Aug 24, 2016 01:42:00.000000000 PET" }
"Nagata" : "    [Time shift for this packet: 0.000000000 seconds]" }
"Nagata" : "    Epoch Time: 1472020920.000000000 seconds" }
"Nagata" : "    [Time delta from previous captured frame: 0.000000000 seconds]" }
"Nagata" : "    [Time delta from previous displayed frame: 0.000000000 seconds]" }
"Nagata" : "    [Time since reference or first frame: 0.000000000 seconds]" }
"Nagata" : "    Frame Number: 2" }
```


Figura 3. Análisis de tráfico almacenado.

En la figura 4, se observa el despliegue de un dashboard en un navegador web, con el objetivo de facilitar la tarea, tanto del análisis de seguridad como el de estadísticas del tráfico interno, siendo objetivo también el análisis de los ciber-ataques realizados en determinado periodo de tiempo, el dashboard permite apreciar un panorama general de tráfico generado y alertas de seguridad para entrar en detalle en cada uno de ellos.

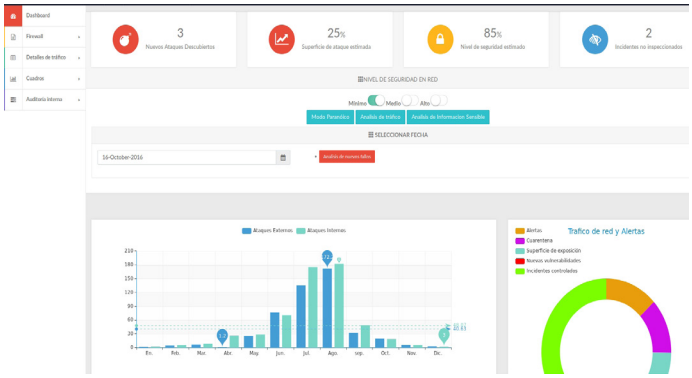

Figura 4. Dashboard.

Como se aprecia en la figura 5 de seleccionar el modo de seguridad más alto el sistema consumirá más recursos computacionales ya que internamente se evaluarán conexiones de dudosa procedencia, como se o

bserva en la figura 6 se procede a eliminar el excesivo tráfico fuera de control que podría ser categorizado como un ataque DOS/DDOS, el IDS entra en una configuración en la que almacenará todas las imágenes que se quieran transmitir por la red de datos y analizará cada una extrayendo en texto que estas contengan, en la figura 7 se observa el paso de una imagen, la cual al ser analizada se detecta que el texto contiene la palabra “confidencial”, por lo cual se tomará acción según las normas establecidas pudiendo ser estas la de eliminar la conexión, realizar seguimiento de la conexión o disparar cierto tipo de alertas a las personas encargadas.

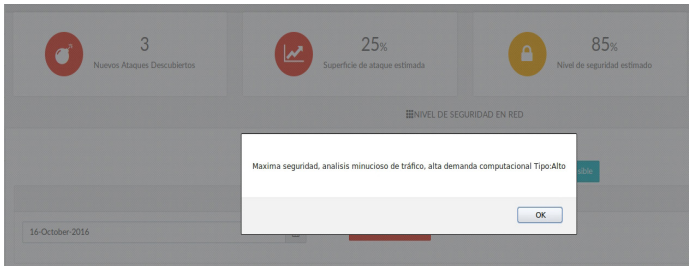

Figura 5. Mensaje de selección de seguridad al máximo.

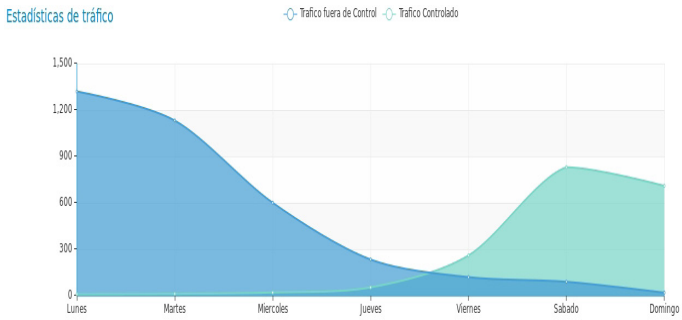

Figura 6. Estadísticas de tráfico fuera de control y tráfico controlado.

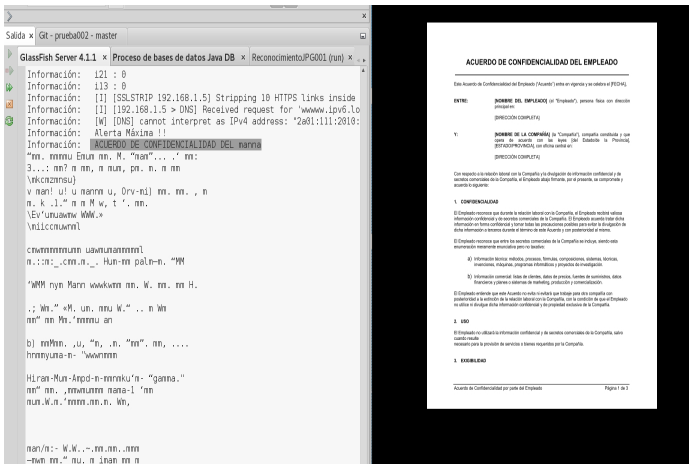

Figura 7. Análisis de texto en imágenes.

Los gráficos de barras son una herramienta muy útil al momento de analizar el tráfico realizados por los empleados de la organización, podemos inspeccionar la actividad en las redes internas para luego obtener problemas de desempeño o Incidentes en la red. En la figura 8, se observa entre otros, las alertas de nuevos ataques tras pasar el tráfico histórico por el sistema de detección de intrusos luego de actualizar las firmas de seguridad con ataques recién descubiertos, esto da una perspectiva de cuanto impacto tuvieron estos ataques sobre la organización.

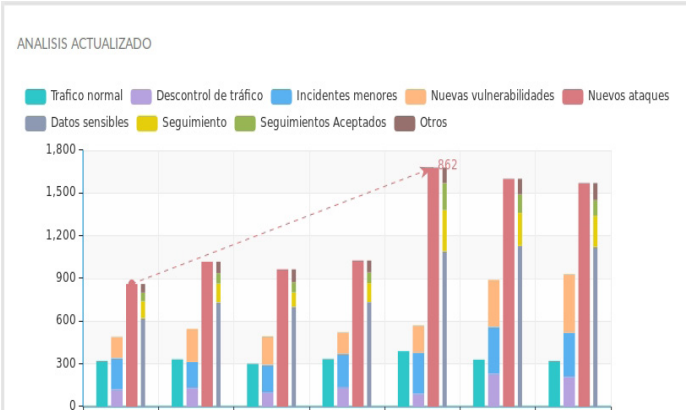

Figura 8. Resultado de análisis en cuadro de barras.

En la figura 9, se aprecia un cuadro de barras detallado con el número de conexiones especificas entre las clasificadas, se puede observar el tráfico normal, descontrol de tráfico, incidentes clasificados como menos, nuevas vulnerabilidades a controlar y nuevos ataques dentro de la organización.

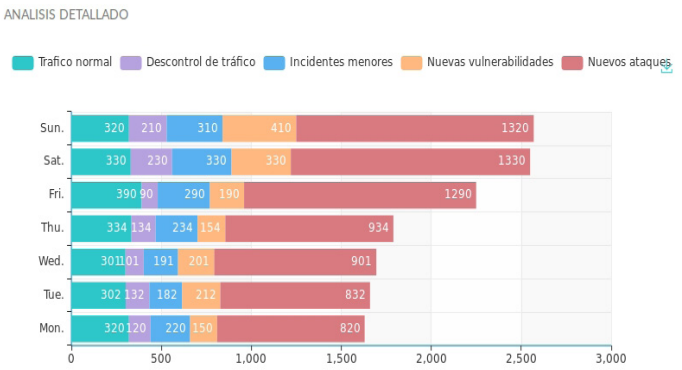

Figura 9. Resultado de análisis detallado.

En la figura 10 se aprecia un gráfico de barras sobre los ataques realizados tanto de manera interna como de manera externa.

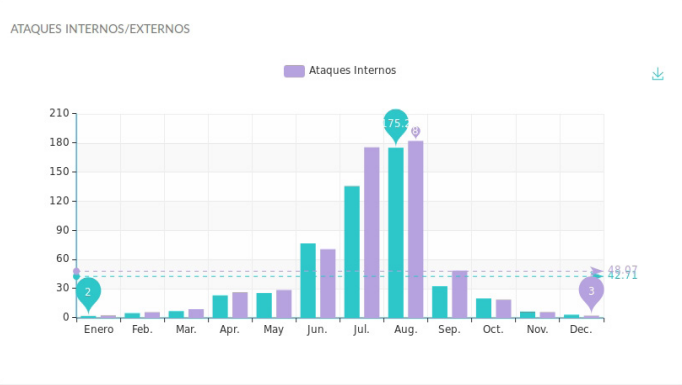

Figura 10. Diagrama de barras respecto de ataques internos/externos

Podemos observar una cuestión particular al realizar la monitorización de tráfico, cualquier servicio al que se acceda que no cuente con una implementación de conexión segura, es decir, certificados de seguridad (SSL), podrá ser inspeccionada poniendo en riesgo información sensible, tales como credenciales de seguridad, también existen distintas técnicas capaces de burlar el protocolo de seguridad HTTPS o HSTS, como se explica en Selvi (2014).

Figura 11. Credenciales de seguridad después de comprometer el protocolo HSTS.

DISCUSIÓN

El presente estudio muestra las medidas de seguridad a tomar en contra de muchos de los incidentes que ocurren en las redes de datos, comúnmente suelen pasar inadvertidos, ya que técnicas de evasión de seguridad, tales como Spoofing, en Urueña (2015) o Rogue AP based MitM en Zhang (2014), son cada vez más sofisticadas y requieren de un menor nivel técnico. Este estudio presenta que aunque la organización sea atacada con técnicas nuevas que no son reconocidas por los sistemas de seguridad, al contar con todo el tráfico de la red almacenado, se podrá analizar comportamientos sospechosos, los cuales se mantendrán en cuarentena hasta tomar las medidas de seguridad respectiva (Vidal, Orozco, Villalba & Member, 2015).

CONCLUSIONES

Tener una métrica sobre los ataques, así como el impacto de éstos, mantiene nuestra matriz de riesgos actualizada.

La detección temprana de ataques logra mitigar en gran medida un fallo de seguridad, si la organización no se encuentra pendiente.

Auditar las redes constantemente disminuye en gran medida la superficie de ataque.

Al contar con una detección temprana de intrusos y evaluar el tráfico interno permite evaluar una seguridad perimetral a más detalle, así como tomar medidas para controlar los lugares a los que se tiene acceso por medio de la red de datos, haciendo cumplir de esta manera nuestras políticas de seguridad y salvaguardando los pilares por los que vela la seguridad informática (CIA).

Facilitar el establecimiento de políticas de seguridad hace que los usuarios inspeccionen más detalladamente los eventos de la red.

El control de tráfico es vital para obtener pistas de auditoría en cualquier momento.

REFERENCIAS BIBLIOGRÁFICAS

Al-Dalky, R., Salah, K., Al-Qutayri, M., & Otrok, H. (2014, July). Framework for a NetFPGA-based Snort NIDS. Recuperado de https://www.researchgate.net/publication/282722223_Framework_for_a_NetFPGA-based_snort_NIDS

Al-Dalky, R., Salah, K., Otrok, H., & Al-Qutayri, M. (2014, August). Accelerating snort NIDS using NetFPGA-based Bloom filter. In ***Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International*** (pp. 869-874). IEEE.

Amran, A. R., & Saad, A. (2014). An evidential network forensics analysis model with adversarial capability and layering. In ***Computer Applications and Information Systems (WCCAIS), 2014 World Congress on*** (pp. 1-9). IEEE.

Atanasovski, V., & Leon-Garcia, A. (2015). ***Future Access Enablers for Ubiquitous and Intelligent Infrastructures***. Berlin: Springer.

Benson, C. (2001). ***Estrategias de Seguridad***. Birkirkara: Inobis Consulting Pty Ltd.

Chakraborty, M., Chaki, N., & Cortesi, A. (2014). A New Intrusion Prevention System for Protecting Smart Grids from ICMPv6 Vulnerabilities. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 1539–1547. Recuoperado de https://www.researchgate.net/publication/277006112_A_New_Intrusion_Prevention_System_for_Protecting_Smart_Grids_from_ICMPv6_Vulnerabilities

Han, S. W., Kwon, H., Hahn, C., Koo, D., & Hur, J. (2016). A survey on MITM and its countermeasures in the TLS handshake protocol. Eighth International Conference on Ubiquitous and Future Networks. Recuoperado de https://www.researchgate.net/publication/322880501_OpenFlow_Communications_and_TLS_Security_in_Software-Defined_Networks

Husák, M., Cermák, M., Jirsík, T., & Celeda, P. (2015, August). Network-based HTTPS client identification using SSL/TLS fingerprinting. In ***Availability, Reliability and Security.*** 10th International Conference on Availability, Reliability and Security. Recuperado de https://is.muni.cz/repo/1299983/https_client_identification-paper.pdf

Lee, K., & Yun, S. (2015). Hybrid memory-efficient multimatch packet classification for NIDS. ***Microprocessors and Microsystems***, ***39***(2), 113-121. Recuperado de https://www.infona.pl/resource/bwmeta1.element.elsevier-6344b26a-11d2-3898-ac7f-c396955137fa

Maheshwari, R., Krishna, C. R., & Brahma, M. S. (2014). Defending network system against IP spoofing based distributed DoS attacks using DPHCF-RTT packet filtering technique. International Conference on Issues and Challenges in Intelligent Computing Technique.

Poljak, N., Ševo, M., & Livaja, I. (2016). Security and privacy in an IT context—A low-cost WIDS employed against MITM attacks (concept). ***39th International Convention on Information and Communication Technology, Electronics and Microelectronics.*** Recuperado de https://ieeexplore.ieee.org/document/7522396/

Selvi, J. (2014). Bypassing HTTP strict transport security. ***Black Hat Europe***. Recuperado de https://www.blackhat.com/docs/eu-14/materials/eu-14-Selvi-Bypassing-HTTP-Strict-Transport-Security-wp.pdf

Urueña, F. (2015). Ciberataques, la mayor amenaza actual. ***Documento de Opinión***, ***9***. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Vidal, J. M., Orozco, A. L. S., & Villalba, L. J. G. (2015). Quantitative criteria for alert correlation of anomalies-based nids. ***IEEE Latin America Transactions***, ***13***(10), 3461-3466. Recuperado de https://ieeexplore.ieee.org/abstract/document/7387255

Zhang, Y. P. (2014). Design for the Application Layer of Network Security Solutions. In ***Advanced Materials Research***, (998-999), 1113-1116). Recuperado de https://www.scientific.net/AMR.998-999.1113