Una Visión de los Sistemas de Detección de Intrusiones en el Campo del Análisis Informático Forense

Jose Miguel Guzmán Chauca
Ciencia de la Computación
Universidad Católica San Pablo
jose.guzman@ucsp.edu.pe

***Abstract*—A lo largo de los años, las redes y la seguridad informática se han vuelto un punto transcendental e imprescindible en todos los sistemas. Gracias a esto, el análisis forense se abrió campo para poder servir de herramienta en las más arduas investigaciones digitales. Entre sus distintas herramientas es muy resaltante el hecho que nunca se haya realizado una recopilación de propuestas para trabajar con los sistemas de detección de intrusiones de forma eficiente en este campo. Para tal fin, se investigó y analizó los distintos trabajos e investigaciones que se han ido elaborando a lo largo de las últimas décadas para poder identificar los aportes funcionales que pueden brindar los sistemas de detección de intrusiones al campo forense y poder elaborar una taxonomía que los agrupe y los ordene con el objetivo principal de que esta pueda servir como un punto de partida, con el estado del arte actualizado, para futuros aportes en este campo.**

***Index Terms*—Seguridad Informática, Análisis Informático Forense, Herramientas, IDS, SIDS, AIDS, Hibrido, Recopilación, Detección, Historiales de Logs, Arquitectura**

I. Introducción

En la última década que hemos pasado, hemos podido contemplar el aumento radical de la tecnología para distintos campos, ya sea para telecomunicaciones, para industrias o fábricas, para el trabajo y la vida cotidiana e incluso en el entretenimiento. Todo esto ha ido de la mano con el despegue del acceso a Internet, donde hoy por hoy, es indispensable tener por lo menos un dispositivo que pueda conectarse a la red. Si bien estos avances han sido de gran ayuda, esto también ha significado el incremento significativo de personas que intentan atentar contra la seguridad informática con maliciosos fines. Por este motivo, se han ido desarrollando a la par muchos mecanismos de defensa a lo largo del tiempo, los cuales nos permiten lidiar con este tipo de situaciones y de alguna forma mantenernos lo más seguros posible ante estas amenazas.

Es entonces que allá por los años 90, entra a jugar un papel muy importante lo que vendría a ser el análisis informático forense, el cual para definirlo correctamente tenemos que hacer hincapié en las partes que lo conforman. Por una parte, tenemos al Análisis Forense, el cual ”se puede definir como la metodología científica que se aplica al estudiar un delito para recabar pistas que permitan encontrar o descifrar quien lo cometió, que utilizó para su cometido y como se llevó a cabo”[1]. Por otro lado resultante de este, tenemos la informática forense que es ”la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos”[1]. Es así que al resultado del conjunto de esta metodología y sus aplicaciones se le denomina el área del análisis informático forense, donde el objetivo principal que dirige esta es buscar elementos que puedan servir de indicios y una posterior prueba de un delito informático, estos se pretenden utilizar para que podamos identificar como es que se dio origen a este incidente y que técnicas han usado los ciberdelincuentes para llevarlo a cabo, de ser posible una reconstrucción muy fiable. También esto nos sirve mucho para que la víctima pueda conocer bien sus vulnerabilidades y poder proceder con acciones que correspondan a la mitigación de las mismas.

Para todo esto se hacen necesarias distintos tipos de herramientas para diferentes tareas, que nos permitan llevar a cabo todas estas labores con mayor facilidad y rapidez que en este contexto se hace tan necesaria. Entre los distintos tipos que hay podemos encontrar herramientas de encriptación, de virtualización, de recuperación de datos, de análisis e investigación, de red y otros cuantos tipos más. Es aquí donde entran a figurar los sistemas de detección de intrusiones(IDS) los cuales son definidos como ”herramientas utilizadas para proteger las infraestructuras de manejo de información, los cuales detectan, identifican y responden a actividades no autorizadas o anormales”[2].

Ahora bien, estas investigaciones son muy importantes y de interés, ya que los campos donde llega a tener aplicabilidad esto son bastante diversos y esto se da porque la seguridad es un aspecto fundamental en todos los sistemas, la cual no puede ser dejada de lado porque, al ser no está perfecta, siempre se puede suscitar un ataque. Desde investigaciones científicas donde se realice el estudio de amenazas y se trate de encontrar la forma de poder reducirlas para que ocasionen el menor daño posible hasta investigaciones criminales donde se necesite pruebas para poder dar veredicto a procesos judiciales. Inclusive se puede aplicar para la vida cotidiana, en donde un usuario pretenda monitorear su seguridad o incluso poder recuperar datos borrados muy relevantes de forma accidental.

Pero también hay que figurar algunas de las principales problemáticas que se suscitan con el uso de estos distintos

sistemas y que pueden ser un punto importante en su manejo. ”La más importante dificultad es definir qué es algo indeseado o en contra de los intereses de la empresa, los IDS no lo saben y esperan que nosotros se lo digamos a través de configuraciones y ajustes”[3]. Por eso es algo muy fundamental que, al momento de trabajar con estos sistemas, se tenga en claro cómo es que se realiza la instalación correcta de estos, su adecuado funcionamiento y ajustes y como es que se tiene que mantener estos sistemas. El no comprender correctamente o el no tener conocimiento de cómo se realizar esto, puede hacer que los usuarios, ya sean empresas o personales, tengan más conflictos que soluciones.

Por tales motivos, este articulo tiene como objetivo dar una visión general de cómo es que funcionan estos sistemas de detección de intrusiones en el campo de la informática forense y que papel toman. Además, también se pretende lograr identificar y resaltar cuales son los problemas actuales que existen con el uso de estos sistemas y que técnicas o soluciones se han desarrollado para contrarrestar esto o denotar aquellos problemas que actualmente no cuentan con soluciones optimas y son potenciales riesgos en la informática actual.

Este trabajo esta organizado de la siguiente manera: la sección 2 describe los trabajos relacionados hechos con anterioridad donde figuran aportes a estos objetivos; la sección 3 describe la taxonomía propuesta y analiza los métodos descritos; por último la sección 4 aborda la conclusión.

II. Trabajos Relacionados

Se sabe que los IDS toman un papel muy importante como herramienta en este campo forense, en cumplimiento de la misma función que les denomina el nombre, la detección de intrusiones. Pero a lo largo del tiempo se ha ido experimentado y probando las capacidades de estos distintos sistemas, siempre con la visión de tener mejoras y optimizaciones que permitan mayor rango de fiabilidad y eficiencia. Es entonces que surgió una gran controversia[4] cuando se consideró que estos sistemas podían, además de cumplir con su función principal, utilizar la gran cantidad de información que recopilaban como elementos de prueba forense, como pruebas digitales y así cubrir un objetivo mayor en el análisis informático forense. Por un lado, se tenía que no era pertinente que los sistemas de detección de intrusiones generaran y guardaran datos de pruebas forenses porque no eran adecuados para tal labor. Por otra mano, se consideraba que, al contrario, estos podrían ser los más adecuados para esta tarea de recoger elementos que sirvan de alguna prueba por su funcionalidad de reconstrucción en el tiempo. Es entonces que algunos investigadores han tratado de aportar a esta teoría con propuestas donde se pueda garantizar esta recopilación de datos.

Entonces tenemos que los IDS han ido evolucionando en su funcionamiento de dos maneras distintas cuando hablamos del campo forense:

A. Recopilación de Información

Empezando por el trabajo de Sommer [5] donde si bien menciona y destaca la capacidad principal de los IDS para el desarrollo de medidas de evasión, también menciona que otra capacidad importante podría ser el recojo de pruebas para aspectos legales. Aunque da a resaltar que posiblemente la arquitectura en la que está diseñada estos sistemas, no permitiría que esta labor se realice de forma fiable, planteando así la idea de un rediseño en la arquitectura de los IDS con un nuevo objetivo.

Más adelante en el artículo de Stephenson [6] se utiliza un entorno controlado de laboratorio para así poder medir de alguna manera la utilidad de los IDS en la forensia y cuan aceptable puede ser la información que este brinda, llegando así a proponer un modelo y una arquitectura nueva para estos sistemas con la idea de que se vayan a realizar trabajos forenses.

En el trabajo de Scaria, Balon y Stovall [7], se aborda los IDS y una visión de sus aplicaciones forenses. En él nos detallan como es que se podría utilizar los IDS en la forensia y muestran algunas de las ventajas y desventajas que esto conlleva. Además, también se mencionan distintas maneras de cómo se recuperan y administran los datos en un análisis forense, tomando en cuenta las herramientas disponibles, entre ellas los IDS.

Luego, en la publicación de Krotoski y Passwaters [8] se habla principalmente de los historiales de registros (también conocidos como ”logs”) que pueden contener una gran cantidad de pruebas en una investigación, ya sea datos importantes de la víctima o del atacante como tipos de ataque, las maquinas utilizadas, identificadores, etc.; resaltan la importancia de las marcas de tiempo que se generan en estos sistemas para una posible reconstrucción de hechos. Pero también mencionan la posibilidad latente de reescritura por parte de un tercero, lo que pone en tela la fiabilidad en estos.

Después, en el trabajo de Etoundi y Achille [16] se tomaron en cuenta las investigaciones de Grobler [9] y de Alharbi [10] para proponer un modelado de procesos de investigación forense, el cual toma en cuenta distintos procesos, los cuales dividieron en tres componentes forenses: proactivo, reactivo y activo, refiriéndose al componente proactivo como la capacidad de identificación, recolección y análisis y a los componentes reactivo y activo en la generación de documentación automatizada. Posteriormente esta modelo seria aplicado por ellos en un nuevo trabajo [4] donde proponen una nueva arquitectura de IDS para fines forenses y muestran su aplicación con IDS´s reconocidos como SNORT.

B. Detección de Intrusiones

A lo largo de años, aproximadamente por 1988 se empezaría una serie de investigaciones que tendrían línea hasta la actualidad donde se abarca una recopilación de datos y técnicas para los IDS. Empezando por el trabajo de Lunt [11] donde muestra un estudio de las técnicas de análisis de pistas de auditoría automatizadas y los IDS hasta ese momento. En este, habla de dos enfoques distintos para los sistemas de detección de intrusiones basados en firmas (SIDS) y como un IDS debería incorporar varios enfoques diferentes para ser robusto.

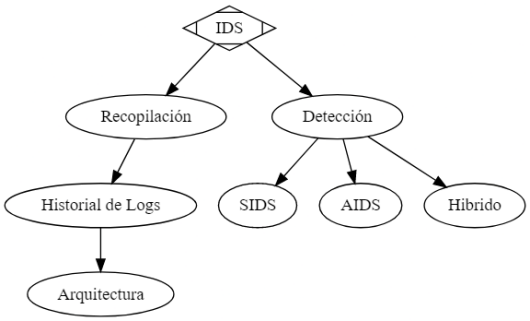

Fig. 1. Taxonomía

En el tan conocido trabajo de Axelsson [12] este presenta una nueva clasificación para los IDS basándose en los métodos y principios de detección y en los aspectos operativos de estos.

Más adelante en la investigación de Liao, Lin, Lin y Tung [13] se destaca una amplia literatura en la gran atención que empezaron a ganar estos sistemas y también en esta, la gran cantidad de retos nacientes. Proponen una nueva clasificación basada en metodologías (basado en firmas, basado en anomalías y por análisis de protocolo) y en características (basado en estadísticas, basado en patrones, basado en reglas, basado en estados y basado en heurísticas).

Después, en el artículo de Khraisat, Gondal, Vamplew y Kamruzzaman [14] se menciona las crecientes dificultades y riesgos que podría significar la falta de credibilidad en estos sistemas de seguridad. Es así que toman en cuenta para la clasificación el principio de detección de firmas, detección de anomalías y la detección hibrida. También se revisa exhaustivamente los problemas existentes con los conjuntos de datos, las técnicas de evasión más comunes utilizadas por los atacantes y diferentes tipos de ataques.

III. Cuerpo del Survey

Se ha hablado entonces de las dos funciones que toman los IDS en el campo forense y de algunos de los trabajos que se han venido realizando a lo largo de este tiempo para poder profundizar y mejorar las técnicas y los métodos que existen para estos. Es por eso que en este artículo se propone una clasificación en función de estas dos grandes labores la cual figura en Fig.1.

En este trabajo se enfocará con mayor profundidad y detenimiento la sección de la recopilación de datos, esto debido a que esta aplicabilidad no ha sido muy abarcada en las investigaciones y es la función que podría simbolizar el objetivo más importante de estos sistemas cuando nos referimos al ámbito forense. El ámbito de la detección de intrusiones también será abarcado de forma más ligera con una clasificación moderna basada en sus metodologías.

A. Recopilación de Información

1) Historial de Logs: Cuando hablamos de recopilación de la información o recolección de evidencia, podemos ver que la parte fundamental de esta tarea recae en los historiales de logs, los cuales podemos referir como una grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular [31].

Normalmente la mayor parte de los sistemas tienen la posibilidad de almacenar los eventos que suceden en ellos en sus servidores en forma de archivos log. Estos pueden guardar distintos tipos de datos como por ejemplo horas de acceso, maquinaria utilizada, acciones realizadas, direcciones de red, tipos de ataques y muchos otros que dependen del tipo de log que se maneje.

Estos elementos podrían ser algo transcendental en una investigación por la cantidad de información que manejan, pero normalmente se considera un área que es infravalorada y de la cual no se obtiene todo el potencial que se podría conseguir en distintos aspectos, especialmente en el aspecto probatorio. Y esto es algo bastante problemático porque inclusive en casos donde haya habido eliminación masiva de datos, deterioro o muerte de sistemas o simplemente los sistemas ya no sean accesibles, hay altas posibilidades de recuperar estos logs y puedan detallar lo sucedido. Esta alta accesibilidad es la que luego da la característica de reconstrucción de hechos en el tiempo [8] y demuestra que, si pasáramos por alto o no tomáramos en consideración estos historiales, estaríamos dejando ir pruebas que serían potencialmente poderosas.

Kruse y Heiser [15] detallaron un listado donde se podía ver algunos de los ejemplos donde estos historiales podrían estar indicando situaciones problemáticas, entre los cuales tenemos:

- Perdida de logs
- Actividad inusual
- Sobredimensionamiento en los logs
- Entradas de fuentes inusuales

¿Como se Generan? Para llevar un ataque informático o la infección de un sistema es necesario que el agresor viaje a través de las redes para poder llegar a su objetivo, esto quiere decir que en este trayecto ha tenido que pasar por una moderada cantidad de dispositivos. Ahora en cada uno de estos dispositivos los historiales están registrando la actividad y los eventos que suceden en ellos y los están almacenando, cada evento o acción es monitoreada y crea nuevos logs. Es así que, a lo largo de todo un suceso, los historiales irán progresando y tendremos distintas fuentes de información donde podremos consultarlos.

¿Como se Manejan? El manejo correcto de estos archivos recae en un conjunto de pasos que se deben seguir para evitar cualquier tipo de perdida. Estos pasos se han ido definiendo y variando en el paso del tiempo empezando en la preservación, recuperación y examinación de datos [7] o llegando a expandirse en recogida, normalización, análisis, correlación de datos e informe [8].

Tomando esto en cuenta se puede a llegar a definir que se deben realizar tres grandes pasos para el correcto manejo de logs, los cuales pueden contener todas las actividades necesarias a realizar, los cuales son: Identificación, Conservación y Análisis.

En el caso de la identificación, el ideal es saber discernir entre la cantidad de información que se tenga, cuales son aquellos logs que van a ser provechosos para nuestro trabajo

y cuales no nos sirven. La recomendación más grande que se puede llegar a realizar es la de separar o retener el sistema víctima, porque esta es la forma más segura de mantener los datos incólumes, aunque en la mayoría de las oportunidades esto no se puede dar, ya que los sistemas pueden seguir en funcionamiento y esta no suele ser una razón tan justificada como para desconectarlos el tiempo que dure el análisis. Otra dificultad con la desconexión puede existir con la memoria, ya que los historiales tienen un tiempo determinado en el que se mantendrán en el sistema y este suele ser muy limitado, puede variar entre un par de días o inclusive llegar a la semana, aunque esto suele depender mucho del tipo del sistema, su arquitectura y la administración.

Ahora bien, para una adecuada conservación de los historiales se hace necesario algunas prácticas para una mayor protección [7]. Entre algunas de estas figuran:

- Utilizar un soporte protegido contra escrituras
- El uso de las funciones Hash para el aumento de la integridad
- Realizar copias de disco a disco
- Realizar el montado en unidades de solo lectura.

Guardar la integridad de estos historiales es fundamental, en el caso de una investigación o en el caso de poder utilizar estos como pruebas, la más pequeña contaminación o corrupción puede tachar el análisis posterior y la completa validez de la prueba. Este, como ya se mencionó con anterioridad, fue una de las principales controversias al momento de introducir el uso de historiales de logs como pruebas y que llamo a una nueva propuesta para estos mismos en la arquitectura.

Análisis

Analizando un poco más estos historiales de logs, se hace necesario resaltar el riesgo que existe con ellos y que se ha podido ir vislumbrando a lo largo de su utilización. El principal problema y riesgo con estos historiales es la posibilidad de una manipulación externa en ellos. Estos archivos realmente no suponen una dificultad al momento que un atacante decide modificarlos o eliminarlos para poder encubrir su camino y es ahí donde radica la falta de fiabilidad de estos archivos. Ahora bien, esto es de alguna forma es controlado con el hecho, que ya se mencionó con anterioridad, de que estamos hablando de una red e historiales marcados por todo el camino, las posibilidades de que se manipulen todos los historiales a lo largo del camino son muy pocas, pero si todo el camino fuera comprometido, esto sería posible.

2) Cambio en la Arquitectura: Cuando hablamos de un cambio en la arquitectura de los IDS, no estamos hablando de una técnica distinta a la que se ha mencionado antes, de los historiales de logs que estos guardan, sino que estamos hablando de un paso más allá en esta técnica, ya que las propuestas que se han ido realizando proponen básicamente un cambio en la arquitectura predefinida de los IDS, para que el objetivo primordial de detectar intrusiones cambie de enfoque a la recopilación de información donde justamente figuran estos logs. Para esto se ha necesitado tomar mano de los modelos forenses existentes y analizar su posible aplicación en un IDS.

Atsa y Mboupda [4] llegaron a proponer una arquitectura distinta para la obtención de estos datos utilizando el mismo modelo que ellos habían propuesto [16] donde se resalta que en los modelos existentes hasta ese momento no se llegaba a tocar ni tratar en totalidad tres componentes importantes en un modelo de investigación forense, los cuales describen como:

- Proactivo: Este componente figura como el mayormente utilizado y citado por todos los modelos, básicamente es el que se encarga de toda la administración de las pruebas, llámese generación, recolección y manejo, para que de esta forma puedan facilitarse al momento de la investigación después de un evento o una solicitud. Resaltan la diferencia que tiene este componente con un IDS normal por su capacidad para conservar las pruebas garantizando integridad y preservación de manera forense.
- Reactivo: Este componente se enfoca más en el momento de la misma investigación, la cual puede ocurrir después de un evento. Acá destacan partes como la investigación física, la identificación, la recolección y el análisis. También destacan algunos objetivos como el éxito de la investigación y la determinación de causas y autores de ser posible.
- Activo: Finalmente este componente lo definen como el nivel de habilidad que posee la empresa para poder identificar, obtener y resguardar las pruebas en tiempo real. Aquí destacan objetivos como la reducción del impacto de un ataque y la generación de un punto de partida para las investigaciones.

Aplicación

Es así que teniendo en cuenta este modelo, Atsa y Mboupda [4] recogieron la arquitectura básica de los IDS para fines forenses y llegan a proponer una arquitectura nueva para los IDS donde se aplican los componentes ya mencionados. Esta nueva arquitectura propuesta está conformada básicamente por un sensor, el motor de detección de intrusiones, la base de conocimiento, el dispositivo de configuración, el componente de decisiones y los componentes forenses digitales proactivo, reactivo y activo. También experimentaron la arquitectura diseñada para el IDS en un entorno forense utilizando SNORT, el cual es uno de los sistemas de detección y prevención de intrusiones más importante del mundo, actualizando su arquitectura y archivos de configuración y se ha demostrado cómo los logs pueden ser explotados en un propósito forense de investigación con ataques de prueba.

Análisis

Esto comparado con un IDS normal ha permitido analizar esta técnica, mostrando que la modificación en la arquitectura puede ser muy eficiente en aspectos forenses sin perder la eficacia en sus labores normales o principales, que claramente es la detección de intrusiones, ya que la comparación entre paquetes recibidos, detectados y alertados por estos sistemas es casi ínfima, lo que la hace inconsiderable. Y en el caso de almacenamiento de datos(logs) se destaca que las evidencias ya no se almacenaban en un directorio predeterminado, sino

en un archivo seguro aparte que obtenía los datos mediante una cadena de custodia.

Es muy importante resaltar que esto claramente no simboliza que los historiales de logs van a ser inmanipulables por externos, ya que eso no es factible, pero añade una capa de seguridad extra. Por eso muchas veces se repite que no se puede confiar solamente en sistemas de detección para la protección, sino que es necesario hacer uso de más herramientas.

B. Detección de Intrusiones

1) Sistema de Detección Basados en Firmas (SIDS): Los sistemas de detección de intrusiones basados en firmas (SIDS) son aquellos que se basan en técnicas de similitud para poder encontrar patrones que ya hayan sido conocidos antes como ataques, por ese motivo también se les conoce como sistemas que están basados en el conocimiento. Básicamente lo que hacen los SIDS es monitorear constantemente los logs que existen en el host para así poder encontrar patrones que ya hayan detectado o conocido antes y de esta forma si encuentran algo sospechoso, envían un mensaje de alarma [14]. Se dice que estos sistemas cumplen una muy buena tarea en lo que es detección de patrones ya conocidos, pero su flaqueza claramente se encuentra cuando se esté generando un ataque en tiempo real o de día cero y el sistema no lo conozca.

2) Sistema de Detección Basados en Anomalías (AIDS): Los sistemas de detección de intrusiones basados en anomalías (AIDS) aparecieron para cubrir estas deficiencias que se presentaban en los SIDS. Estos sistemas se basan en modelos de comportamiento y utilizan distintos métodos para poder aprenderlo, ya sean métodos estadísticos, heurísticos, de patrones, basados en IA y demás [13]. Esto lo realizan en dos pasos [14], primeramente, está el paso del entrenamiento, donde el sistema aprende el comportamiento típico del usuario para poder así definir que es un comportamiento normal. Luego está el paso de prueba, donde aquí se le brinda al sistema un comportamiento atípico para que de esta forma pueda identificarlo. Su funcionamiento luego será de monitorear y en el momento en el que detecte algún comportamiento anómalo que sea considerable, lanzará el mensaje de alarma.

Al contrario de los SIDS entonces, con estos sistemas si existe la posibilidad de detectar ataques en tiempo real o ataques de día cero, ya que posiblemente la actividad realizada para este, sea detectada por el sistema como un comportamiento anómalo y no depende si alguna vez se realizó ese ataque o no. Otra ventaja muy grande, es el hecho del desconocimiento y la dificultad que puede tener un atacante para identificar que ha entendido el AIDS como comportamiento normal.

3) Sistema de Detección Híbridos: Los sistemas de detección de intrusiones híbridos, como su nombre lo sugiere, se basan en una combinación entre los SIDS y los AIDS. Estos sistemas surgieron al conocer las distintas problemáticas que existen con los IDS en general, las cuales varían entre falta de identificación de ataques nuevos, falta de flexibilidad para modificarse y principalmente, problemas con la precisión y una tasa altísima de falsos positivos. Estos sistemas dicen superar estas problemáticas conocidas para ambas metodologías, AIDS y SIDS [32].

TABLE I
INVESTIGACIONES EN DETECCIÓN DE INTRUSIONES

Autor	SIDS	AIDS	Hibridos	Pruebas con Datasets
Lunt [11]	X			
Axelsson [12]	X	X		
Liao [13]	X	X	X	
Khraisat [14]	X	X	X	X

En la siguiente tabla (Table I) se procederá a hacer una recopilación de esta secuencia de surveys que se han ido presentando a lo largo del tiempo para las metodologías en los IDS, destacando en que metodologías hicieron énfasis.

IV. CONCLUSIONES

Este trabajo ocupa una breve contextualización al campo del análisis digital forense y los sistemas de detección de intrusiones. Se ha logrado identificar y resaltar dos grandes funcionalidades en la que los IDS forman parte del mundo forense, donde se ha hecho un gran énfasis en la recolección de datos por la gran importancia que significa para las investigaciones y por la poca relevancia que ha tenido en el desarrollo de nuevas técnicas. Es así también que se pudo identificar la manera en que se recuperan estos datos en los IDS mediante historiales de logs y como esta idea ha ido mejorando en medidas de seguridad hasta la propuesta de remodelar la arquitectura misma de estos sistemas en base a modelos forenses existentes, sin perder el rendimiento en las tareas principales. En el ámbito de la misma detección también se pudo apreciar una línea de investigaciones importantes que vienen a lo largo del tiempo y que demuestra que la importancia de los IDS en la actualidad va en aumento a medida que las redes crecen.

En trabajos futuros, se podría tomar en cuenta las metodologías que se van identificando y el conocimiento claro en el funcionamiento de estos sistemas, para hacer propuestas nuevas en el campo de la recolección de datos y en la creación de arquitecturas que pueden garantizar mayor integridad sin tener que sacrificar eficiencia.

REFERENCES

[1] P. Arnedo Blanco, "Herramientas de analisis forense y su aplicabilidad en la investigacion de delitos informaticos", Master en Seguridad Informatica, Universidad Internacional de la Rioja, 2014.

[2] Xu, Congyuan Shen, Jizhong Du, Xin. (2020). A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2020.2991876.

[3] S. Garcia, "La (otra) realidad de los Sistemas de Detección de Intrusiones", CYBSEC Security Systems.

[4] Achille, Mboupda Moyo and Atsa Etoundi Roger. "Obtaining Digital Evidence from Intrusion Detection Systems." International Journal of Computer Applications 95 (2014): 34-41.

[5] P. Sommer, "Intrusion detection systems as evidence", Computer Networks, vol. 31, no. 23-24, pp. 2477-2487, 1999. Available: 10.1016/s1389-1286(99)00113-9.

[6] Stephenson, Peter. (2000). The Application of Intrusion Detection Systems in a Forensic Environment.

[7] Balon, N., Ronald Stovall and Thomas Scaria. "Computer Intrusion Forensics Research Paper." (2003).

[8] M. L. Krotoski and J. Passwaters, "Using Log Record Analysis to Show Internet and Computer Activity in Criminal Cases", The United States Attorneys' Bulletin, pp. 1-15, 2011.

[9] CP Grobler, CP Louwrens, SH von Solms "A multicomponent view of Digital Forensics". International Conference on Availability, Reliability and Security, 2010.

[10] Soltan Alharbi, Jens Weber-Jahnke, Issa Traore: "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review". International Journal of Security and Its Applications Vol. 5 No. 4, October, 2011.

[11] T. F. Lunt, "Automated audit trail analysis and intrusion detection: a survey," in Proceedings of the 11th National Computer Security Conference, 1988, vol. 353: Baltimore, MD

[12] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy", 2000.

[13] H. Liao, C. Richard Lin, Y. Lin and K. Tung, "Intrusion detection system: A comprehensive review", Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16-24, 2013. Available: 10.1016/j.jnca.2012.09.004.

[14] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges", Cybersecurity, vol. 2, no. 1, 2019. Available: 10.1186/s42400-019-0038-7

[15] W. Kruse and J. Heiser, Computer forensics. Boston: Addison-Wesley, 2008.

[16] A. EtoundiRoger and M. Moyo Achille, "Multiperspective Cybercrime Investigation Process Modeling", International Journal of Applied Information Systems, vol. 2, no. 8, pp. 14-20, 2012. Available: 10.5120/ijais12-450401.

[17] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion detection systems," in Annales des télécommunications, 2000, vol. 55, Springer

[18] Ameli, A., Hooshyar, A., El-Saadany, E. and Youssef, A., 2020. An Intrusion Detection Method for Line Current Differential Relays. IEEE Transactions on Information Forensics and Security, 15.

[19] Leu, F., Tsai, K., Hsiao, Y. and Yang, C., 2017. An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques. IEEE Systems Journal.

[20] Mohammad, R., 2018. A Neural Network based Digital Forensics Classification. 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA).

[21] Nisioti, A., Mylonas, A., Yoo, P. and Katos, V., 2018. From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods. IEEE Communications Surveys Tutorials.

[22] Sharma, B., Joseph, M., Jacob, B. and Miranda, B., 2019. Emerging trends in Digital Forensic and Cyber security- An Overview. 2019 Sixth HCT Information Technology Trends (ITT).

[23] Xu, W., Yan, J. and Chi, H., 2019. A Forensic Evidence Acquisition Model for Data Leakage Attacks. 2019 IEEE International Conference on Intelligence and Security Informatics (ISI).

[24] Babiker, M., Karaarslan, E. and Hoscan, Y., 2018. Web application attack detection and forensics: A survey. 2018 6th International Symposium on Digital Forensic and Security (ISDFS).

[25] Rostamipour, M. and Sadeghiyan, B., 2015. Network attack origin forensics with fuzzy logic. 2015 5th International Conference on Computer and Knowledge Engineering (ICCKE).

[26] Sivaprasad, A., 2017. Secured Proactive Network Forensic Framework. 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC).

[27] Naqvi, S., Sommer, P. and Josephs, M., 2019. A Research-Led Practice-Driven Digital Forensic Curriculum to Train Next Generation of Cyber Firefighters. IEEE Global Engineering Education Conference (EDUCON), Page 1204.

[28] Ocampo, C., Castro Bermúdez, Y. and Solarte Martínez, G., 2017. Sistema de detección de intrusos en redes corporativas. Scientia et Technica Año XXII, Vol. 22, No. 1, marzo de 2017. Universidad Tecnológica de Pereira.

[29] Panwar, A., 2015. A kernel based Atanassov's intuitionistic fuzzy clustering for network forensics and intrusion detection. 2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS).

[30] Sangher, K. and Singh, A., 2019. A Systematic Review – Intrusion Detection Algorithms Optimisation for Network Forensic Analysis and Investigation. 2019 International Conference on Automation, Computational and Technology Management (ICACTM).

[31]"Log (informática) - Wikipedia, la enciclopedia libre", Es.wikipedia.org, 2021. [Online]. Available: https://es.wikipedia.org/wiki/Log(inform

[32]Farid, Dewan Nouria, Harbi Zahidur Rahman, Mohammad. (2010). Combining Naive Bayes and Decision Tree for Adaptive Intrusion Detection. International Journal of Network Security Its Applications. 2. 10.5121/ijnsa.2010.2202.