FORENSIA EN REDES INALÁMBRICAS, INFRAESTRUCTURA EN LA EVIDENCIA DIGITAL

Edwin Gerardo Herrera Rios
edwinherreraing@gmail.com

Universidad Piloto de Colombia

***Resumen*— En este documento se presenta la propuesta de una infraestructura para la identificación, preservación y análisis de evidencia digital en las redes inalámbricas teniendo en cuenta la integridad, disponibilidad, autenticidad obtenida de la misma evidencia.**

La información que se pretende almacenar en el momento de algún incidente en la red, es una labor que se le realiza seguimiento realizando un monitoreo y análisis de los sucesos que ocurren en la red, teniendo en cuenta las posibles anomalías que los usuarios y el mismo analista de la red detecten dentro del buen funcionamiento del servicio, al ser información volátiles es de suma importancia tener los controles pertinentes y la respectiva capacitación en el momento que se presente el incidente saber actuar, en el caso de no contar con estas características es mejor no tocar la evidencia para así prevenir que se contamine.

Es necesario contar con los elementos, políticas y servicios para generar una buena infraestructura y así generar una evidencia digital que pueda ser presentada en el caso de ser necesaria y contar con la validez que sea pertinente.

***Palabras clave*—redes inalámbricas, registros de eventos, mejores prácticas, caracterización, infraestructura, análisis de impacto, análisis de riesgo, forense.**

***Abstract*— The proposal of an infrastructure for the identification, preservation and analysis of digital evidence in wireless networks considering the integrity, availability, authenticity obtained from the same evidence is presented in this paper.**

The information is to be stored at the time of an incident on the network, is a task that is performed by performing a follow-up monitoring and analysis of events that occur in the network, taking into account the possible anomalies that users and the same network analyst detected within the smooth operation of the service, to be volatile information is extremely important to have relevant training and the respective controls at the time that this incident know how to act in case of not having these features is better not touch the evidence in order to prevent contamination.

Is needed elements, policies and services to generate a good infrastructure and generate a digital evidence that may be presented in the case and if necessary have the validity that is relevant

***Index Terms*— wireless networks, event logs, best practices, characterization, infrastructure, impact analysis, risk analysis, forensic.**

I. INTRODUCCIÓN

La forma como ha avanzado la tecnología de forma vertiginosamente al hecho de contar que cualquier dispositivo electrónico pueda acceder, interactuar, transmitir información por medio del espectro aéreo, radio frecuencia, requieren de monitoreo y análisis de la actividad de datos en la red y adicionalmente mecanismos que aseguren la autenticidad, integridad y confidencialidad. Hay que tener en cuenta que los datos que se encuentran al momento de presentarse un incidente en la red, es información volátil que debe ser recolectada en el menor tiempo posible puesto que tiende a desaparecer si no es capturada en el momento adecuado, cabe resaltar que al ser información dinámica suele resultar impredecible.

Es necesario establecer que al momento de realizar la captura de la evidencia, es conveniente tener los controles pertinentes para no contaminar o modificar la evidencia, ya que se corre el riesgo por ser información volátil, que se pierda o que no sea correctamente almacenada, además es de suma importancia tener un control detallado de los procedimientos al momento de embalar la información. Si la evidencia no ha seguido con un estricto control, una cadena de custodia, es posible y lo más seguro que al momento de ser presentada a las autoridades competentes pierda credibilidad dentro de un proceso de investigación sean piezas claves al momento de ser presentadas ante un juez para así establecer la veracidad de los hecho y de los posibles implicados en el hecho que aconteció.

La tecnología avanza a pasos agigantados del modo que al pasar los minutos algo que se consideraba seguro ya no lo es, es por eso que se deben contar con las herramientas tecnológicas y los conocimientos pertinentes para prevenir estos posibles incidentes, el hecho de que se cuente con los mecanismos de seguridad más sofisticados no significa que no sean vulnerables de un posible ataque , pero resulta un control

de lo que sucede en la red y establecer las posibles alertas que genere un tráfico sospechoso, recordando que lo valioso o lo que se está protegiendo es la información que está viajando en la red inalámbrica, es por eso que cuando se presente una anomalía por lo menos tener algo de conocimiento del tema para administrar una evidencia. La seguridad de la red inalámbrica ha ido evolucionando y se han presentado dispositivos, políticas, controles y auditorias para contrarrestar los posibles accesos a la red, pero que pasa cuando sucede un incidente, en el momento donde se está realizando el monitoreo o simplemente un usuario a indicado alguna anomalía es difícil definir un protocolo para administrar el suceso en una red inalámbrica, debido a que al momento de definir, producir, obtener y analizar los eventos que se están presentando, la imposibilidad de tener disponible el dispositivo desde el cual se realizó la conexión a la red inalámbrica y analizarlo, obliga a relacionar directamente este problema con lo que llamamos forensia en redes, puesto que esta parte del tema forense, específica que la evidencia debe ser evento de la red como tal.

Es necesario contar con los controles pertinentes y un posible plan de contingencia y por lo menos tener un procedimiento de como recaudar la evidencia digital, de una forma ordenada, entendible, coherente y además la validez con la forma como se realizó el embalaje de esta y ser utilizada como una prueba dentro de una posible investigación.

II. Planteamiento del problema

Generalmente se escuchan términos en los cuales se indica que la red inalámbrica ha sido vulnerada por medio de software o vulnerabilidades que se posibiliten el acceso, hay que tener en cuenta que la información, los datos viajan por medio del aire, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

Un problema que actualmente se presenta ocasionalmente es que el administrador o el jefe de seguridad de una red inalámbrica, si es el caso, no tienen claro el procedimiento sencillo y eficaz para manejar los incidentes que ocurran al momento de presentarse un incidente en la red inalámbrica.

En el mercado actual existen estándares, metodologías y marcos de referencia que involucran la gestión de la forma como se debe almacenar una evidencia en una red inalámbrica, pero surge un gran cuestionamiento:

¿Cómo plantear una infraestructura válida para la elaboración de evidencia digital en las redes inalámbricas?

III. Objetivos

Plantear una infraestructura para la elaboración de evidencia digital en las redes inalámbricas.

Los objetivos específicos son:

- Análisis y definición de requerimientos necesarios para el diseño y almacenamiento de registros electrónicos en redes inalámbricas teniendo en cuenta las técnicas más usadas en forensia digital enfocada en redes inalámbricas.
- Proponer un planteamiento de registros electrónicos en redes inalámbricas teniendo en cuenta su admisibilidad y relevancia como evidencia digital.
- Realizar pruebas para verificar que la producción de la evidencia sea integra y confiable.
- Implementar una infraestructura para la producción de evidencia digital en redes inalámbricas teniendo en cuenta el diseño de los registros electrónicos.
- Ejecutar pruebas para verificar la fabricación de la evidencia mediante un caso particular.

IV. Alcance

El trabajo se centrará en el campo de la ciencia forense, ya que proporciona los principios y técnicas que facilitan la investigación del delito criminal en las redes inalámbricas. Con respecto al ciclo de vida de la evidencia únicamente se tomará en cuenta las dos primeras fases del ciclo, correspondientes al diseño y a la producción de evidencia digital.

Este trabajo se centrará en el planteamiento para fortalecer la admisibilidad y relevancia de la evidencia digital y producción de la misma en redes inalámbricas teniendo en cuenta el concepto de forensia en redes anteriormente explicado.

Es de gran importancia definir una infraestructura para el proceso de gestión de la evidencia en una red inalámbrica, teniendo en cuenta buenas prácticas, para que luego alguna persona capacitada pueda recolectarla de forma sencilla, colaborando con todo el proceso (diseño, producción, recolección, análisis, y reporte y presentación) y al conocer cuál es la evidencia digital en las redes inalámbricas, se procederá directamente a buscarla.

V. Antecedentes

En las redes inalámbricas actualmente encontramos un problema al intentar administrar la evidencia digital, debido a que es difícil definir, producir, obtener y analizar la evidencia e implica un esfuerzo mayor el hecho de aplicar computación forense. La imposibilidad de aplicar computación forense por no tener disponible el dispositivo desde el cual se realizó la conexión a la red inalámbrica y analizarlo, obliga a relacionar directamente este problema con lo que llamamos forensia en redes, puesto que esta parte del tema forense, específica que la evidencia deben ser eventos de la red como tal. Para poder abarcar el tema se debe comenzar por el diseño de registros electrónicos para fortalecer la admisibilidad y relevancia de la

evidencia y la producción de los mismos en las redes inalámbricas.

El diseño y producción de los registros electrónicos es de vital importancia en la gestión de evidencia digital, de estos pasos depende que la evidencia digital exista de forma coherente y luego pueda ser recolectada y utilizada como prueba incriminatoria o registro valido. La informática forense es de suma importancia por su aplicación en la actualidad y en algún futuro cercano se espera que este trabajo sea una base para personas, empresas y universidades, del desarrollo de un campo vital como lo es la seguridad informática.

Los conceptos necesarios para el entendimiento de este proyecto de investigación y en los cuales fue basada parte de la investigación, están relacionados con el estándar de Redes inalámbricas IEEE 802.11, teniendo en cuenta su infraestructura, funcionamiento, ventajas y desventajas, vulnerabilidades, ataques, entre otros. Por ultimo, la importancia de los temas relacionados con informática forense, enfocado a forensia en redes, pero sin descuidar los aspectos generales de la informática forense.

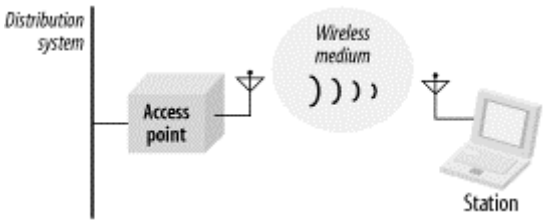
VI. REDES INALÁMBRICAS

La norma IEEE 802.11 estableció en junio de 1997 el estándar para redes inalámbricas. Una red de área local inalámbrica puede definirse como a una red de alcance local que se transmite a través de frecuencias de radio. Una red de área local o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, etc.).

El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

La nomenclatura básica usada en redes inalámbricas en la siguiente:

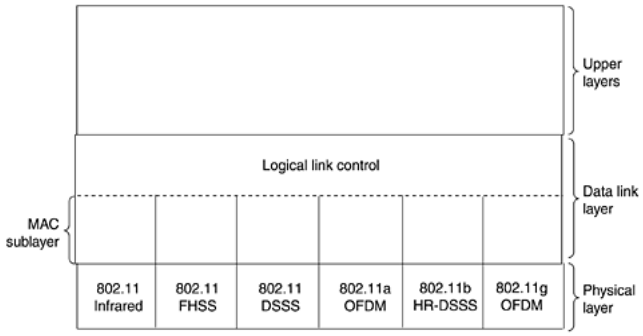
Figura 1: Diseño Básico de una red 802.1 1



Fuente: Gast, Matthew. “802.11 Wireless Networks: The Definitive Guide”. Editorial O’Reilly 2002.

Los protocolos utilizados por todas las variantes 802, tienen ciertas similitudes de estructura como se puede observar en la Figura 2; la cual muestra una vista parcial de la pila de protocolos del estándar 802.11. Como se puede observar la capa física corresponde con la capa física OSI, pero la capa de enlace de datos (Data link layer) de todos los protocolos 802 se divide en dos o mas subcapas. En el estándar 802.11 la subcapa MAC (Medium Access Control layer) determina la forma en que se asigna el canal. Arriba de esta se encuentra la subcapa de control lógico de enlace (LLC) cuyo trabajo es ocultar las diferencias entre las variantes 802.

Figura 2: Parte de la pila de protocolos 1



Fuente: Gast, Matthew. “802.11 Wireless Networks: The Definitive Guide”. Editorial O’Reilly 2002.

El uso de ondas de radio en la capa física es relativamente complejo por ello este es dividido en dos componentes genéricos: PLCP (Physical Layer Convergente Procedure), para mapear los paquetes (frames) de la MAC dentro del medio, adicionando algunos campos a los paquetes, por ello sobrepasa el limite entre la MAC y la capa física, y la PMD (Physical Medium Dependent) que es el sistema para transmitir esos paquetes.

VII. METODOLOGÍA

La propuesta está orientada a la gestión de evidencia digital en redes inalámbricas, específicamente en dos etapas: diseño y producción de evidencia digital. Como reto principal se quiere contribuir a fortalecer la admisibilidad y relevancia de la evidencia producida por las redes inalámbricas.

Será desarrollado por etapas, inicialmente apropiarse del conocimiento relacionado con redes inalámbricas, seguridad informática e informática forense.

Luego de obtener el conocimiento relacionado con el desarrollo del proyecto, se realiza un análisis de qué tipos de registros de eventos existen en las redes inalámbricas y un análisis de los requerimientos para el diseño y producción de los mismos.

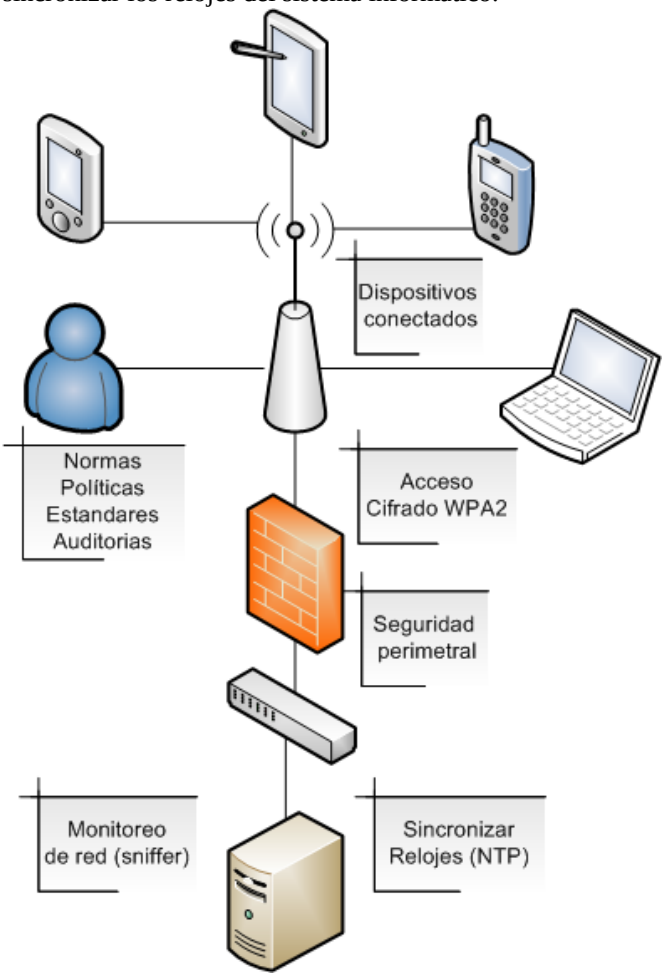
Después, se estudian varias alternativas de solución de seguridad en redes inalámbricas revisando qué requerimientos puede llegar a cumplir. Con esto se escoge la mejor alternativa de seguridad la cual será complementada con recomendaciones, buenas prácticas e infraestructura adicional, esto con el fin de ayudar a cumplir los requerimientos establecidos.

Por último se validará la infraestructura establecida con casos de estudio previamente establecidos y unas pruebas que ayudaran a establecer su funcionamiento.

VIII. PLANTEAMIENTO DE LA INFRAESTRUCTURA

La siguiente propuesta de la forma como manejar un incidente en una red inalámbrica, se plantea la siguiente infraestructura al momento de manejar una evidencia digital.

Se debe tener un monitoreo constante de la red, lo cual permite la adquisición de información de conexiones realizadas mediante logs almacenados por medio de un sniffer de red para administrar los eventos que estén sucediendo o hayan sucedido, para garantizar que con exactitud que la adquisición, la secuencia de los datos almacenados en los logs se emplea un protocolo de internet NTP (Netwok Time Protocol) para sincronizar los relojes del sistema informático.



Las políticas, normas, estándares establecidos dentro del sistema de red inalámbrico permiten esclarecer los protocolos de seguridad que han sido vulnerados mediante auditorias programadas y aleatorias establecidas dentro de la misma políticas, con esto se verifica que es lo que esta fuera de los parámetros iniciales.

La seguridad perimetral también protege el acceso indebido a la red, adicionalmente almacena información de las conexiones realizadas, permisos y restricciones.

El uso de acceso cifrado a la red por medio del sistema WPA2 (sistema basado en el estándar IEEE 802.11i), el cual permite identificar y autenticar al dispositivo conectado permitiendo así la confidencialidad, integridad de la información que se está trasmitiendo.

IX. RESULTADOS ESPERADOS

La propuesta de una infraestructura al momento de realizar seguimiento al momento de un posible incidente de seguridad informático, es un conjunto de varias posibilidades que ya están establecidas pero que se propone como una alternativa al momento que se requiera realizar un procedimiento forense en la red.

Es necesario indicar que actualmente existen bastantes formas o técnicas antiforenses, las cuales pueden entorpecer la investigación que se está realizando al momento de realizar el monitoreo y la recolección de la evidencia. Es necesario estar actualizado en identificar cuando se están ejecutando estas técnicas que pueden entorpecer la presentación de la evidencia.

Es necesario contar con la respectiva capacitación al momento de atender un incidente de una red inalambrica, es recomendable pues son procedimientos que requieren de un profesional en el tema, que tenga los conocimientos necesarios al momento de realizar la respectiva recolección de la evidencia.

El estándar IEEE 802.11i, es un buen garante de seguridad pero que no funciona solo, requiere de otros complementos que permitan garantizar la transparencia al momento de realizar conexiones.

En conclusión se pretende que esta sea una guía al momento de presentarse un incidente, es necesario seguir investigando en el tema ya que día a día los cambios, las técnicas y formas de vulnerar la red se van transformando en un tema que se debe tener en cuenta en cualquier parte del mundo.

REFERENCIAS

[1] ARDITA Julio Cesar. Experiencias en Análisis Forense Informático. CYBSEC S.A. Security Systems, 2006 Disponible en: http://www.criptored.upm.es/guiateoria/gt_m241c.htm

[2] CANO Jeimy J. Computación forense. México, Editorial Alfaomega Grupo Editor, S.A. 2009.

[3] CANO MARTINEZ Jeimy J. Introducción a la informática forense. Revista ACIS Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[4] CANO MARTINEZ Jeimy J. Admisibilidad de la Evidencia Digital: Algunos elementos de revisión y análisis. Disponible en: http://www.alfa-redi.org/node/9368

[5] CRIPTORED.Lección 12 Seguridad en redes WiFi. Intypedia http://www.intypedia.com/

[6] GÓMEZ VIEITES Álvaro. Enciclopedia de la seguridad informática. México, Editorial Alfaomega Grupo Editor, S.A. 2 edición 2011.

[7] LOPEZ DELGADO Miguel. Análisis Forense Digital. Criptored Junio de 2007 Disponible en: http://www.criptored.upm.es/guiateoria/gt_m335a.htm

[8] TORI S. Carlos. Hacking ético. Argentina, Editorial autoedición, edición 2008.

Edwin Gerardo Herrera Rios Ingeniero de sistemas con énfasis en telecomunicaciones egresado de la Universidad Cooperativa de Colombia, con experiencia en soporte en el área de infraestructura, actualmente se desempeña como ingeniero de soporte mssp.