Sistema de medición de riesgos en enrutadores bajo el estándar 802.11g basándose en los lineamientos planteados por la OSSTMM

Risk measurement system for 802.11g routers based on guidelines proposed by OSSTMM

Robinson Jesús Navarro Illera. Ing., Adolfo Eduardo García Muñoz. Ing., & Siler Amador Donado. Ing.
1. Ing. Universidad del Cauca, Colombia
rnavarro@unicauca.edu.co, aegarcia@unicauca.edu.co, samador@unicauca.edu.co, rnavarro,agarcia,samador@unicauca.edu.co

Recibido para revisión 21 de febrero de 2011, aceptado 18 de octubre de 2011, versión final 22 de noviembre de 2011

***Resumen* — Un inconveniente en las redes inalámbricases la seguridad, debido a que la emisión de señales es por aire. Usualmente los enrutadores bajo el estándar 802.11g pueden ser víctimas de usuarios no autorizadosque se adhieren a la red con el objetivo de violar la integridad, confidencialidad e integridad de los datos. Por ello es vital la implementación de mecanismos que aseguren la disponibilidad del enrutador inalámbrico empleado por el usuario, brindando información sobre el riesgo que supone usar configuraciones por defecto, o por falencias en su configuración. Este proyecto busca generar un informe de riesgo que logre disminuir la vulnerabilidad del dispositivo por medio de cambios en las características inalámbricas básicas del dispositivo de interconexión, conociendo su configuración y posible estado de vulnerabilidad y contando con una base de información acerca de lineamientos de seguridad y buenas prácticas de seguridad informática, mostradas al usuario por medio de una aplicación.**

***Palabras claves* — Estándar IEEE 802.11, Análisis de riesgo, enrutamiento, LAN inalámbrica.**

***Abstract* — an issue in wireless networks is security, because the signal is broadcast over the air. Usually routers under the standard 802.11g can be victims of unauthorized users that attach to the network with the aim of violating the data integrity and confidentiality. Therefore it is essential implement mechanisms to ensure the availability of the wireless router used by the user, providing information on the risk of using default settings, or flaws in its configuration. This project seeks to generate a risk report that achieves reduce the vulnerability of the device by means of changes in the wireless networking device basic features, knowing their own status and potential vulnerability, and with a base of information about safety guidelines and good computer security practices, shown to the user through an application.**

***Keywords* — IEEE 802.11 Standards,RiskAnalisis,Routing,Wireless LAN.**

I. INTRODUCCIÓN

Las tecnologías de acceso inalámbrico en los últimos años han presentado una gran aceptación en la sociedad, en mayor parte por usuarios Small Office Home Office SOHO dadas sus ventajas tanto en la parte económica como tecnológica. Debido a que las señales circulan por el aire se presentan problemas de seguridad en la transmisión de datos, por esta razón surgen como una alternativa diferentes protocolos de cifrado que ayudan al control de acceso a las redes inalámbricas como lo son Wired Encription Privacy(WEP),Wi-Fi Protect Access (WPA), WPA2 basados en el estándar IEEE 802.11i[1].

Aunque las recomendaciones están dadas, un gran porcentaje de usuarios no tienen el conocimiento suficiente sobre comunicación inalámbrica [2], siendo una consecuencia la defectuosa configuración por parte del usuario de los mecanismos y parámetros de seguridad existentes para su enrutadores, además, estudios realizados demuestran que la mayoría de enrutadores al ser entregados al usuario se encuentran configurados con parámetros de fábrica que no ofrecen buena seguridad [3].

Se busca la disminución del riesgo causado por la mala configuración del enrutador, para esto además de asegurar el control de acceso físico al enrutador se debe restringir o en caso extremo impedir el acceso no autorizado a la lógica del dispositivo, el acceso lógico se refiere al ingreso a él mediante la interfaz web de administración de usuario con un nombre y una contraseña, lo cual permite realizar cambios en su funcionamiento.

El desarrollo del Sistema de Medición de Riesgo (SiMeR) toma como referencia el Manual de Metodología Abierta OSSTMM (*Open Source Security Testing Metodology Manual*) [4],que es una guía que permite evaluar el nivel de seguridad

Revista Avances en Sistemas e Informática, Vol.8 No. 3, diciembre de 2011 - Medellín. ISSN 1657-7663

en las Tecnologías de Información (*InformationTecnologies*) IT, que provee a los administradores que desean evaluar la seguridad informática de una amplia gama de sistemas de comunicación una manera ordenada y detallada, por medio de instrucciones detalladas sobre cómo probarlos de una manera adecuada, y la forma de evaluar e informar sobre los resultados. Este manual es empleado como fuente de información para la generación de lineamientos de seguridad y buenas prácticas sobre enrutadores inalámbricos.

Además de OSSTMM, SiMeR aplica las tablas de evaluación de *GovermentAcountability Office* (GAO) [5], con lo cual se enfatiza en la evaluación del riesgo siendo esta uno de los elementos más importantes dentro de la administración de IT para garantizar el buen funcionamiento de los dispositivos o en general de una organización o empresa evaluada, particularmente GAO, provee una base para establecer políticas apropiadas y seleccionar técnicas efectivas para implementar estas políticas[4].

Con las anteriores bases se crea una aplicación Java, capaz de generar un informe de riesgo a partir de la evaluación de seguridad presente en el enrutador, y brindar un grupo de controlespara disminuir los problemas encontrados, apoyándose en una base de datos con información acerca de vulnerabilidades de losenrutadores que soporten 802.11g y que hayan sido estudiados.

II. MARCO TEÓRICO

Para definir lineamientos de seguridad y poder realizar un análisis de riesgos debemos conocer el estado actual de los enrutadores, sus amenazas y vulnerabilidades, al igual que algunas características básicas como el cifrado o las características de seguridad que deseamos cuidar, sin dejar a un lado el ambiente en el que se encuentran los enrutadores.

La seguridad informática toma mayor relevancia cada día[6], dado que el incremento de delitos informáticos afecta de mayor manera la integridad, confidencialidad y disponibilidad de la información[3]

La manera correcta en que la aplicación creada puede recolectar la información que necesita desde en el enrutador debe ser no intrusiva. La obtención de la informacióndebe ser autorizada(ej. la configuración del cifrado usado, WEP o WPA2)de tal forma que no sea incluida como un causante de alguno de los problemas de seguridad informáticos, como los listados en la tabla 1, donde se describen una serie de ataques que tienen lugar en las redes inalámbricas:

Tabla I. Ataques comunes a redes inalámbricas.

Ataque	Descripción
Eavesdropping	Como la onda RF viaja a través del aire, un atacante puede analizar el tráfico y capturar información privilegiada, como claves para acceder a más información sin que nadie se entere.
Spoofing	Consiste en el uso de técnicas de suplantación de identidad generalmente con fines maliciosos.
Wardriving	Búsqueda de redes *Wireless* desde un vehículo en movimiento para conocer su posición.
Warchalking	Notificar a otros atacantes acerca de la configuración de la red.
Ataques*DoS*	Saturar las bandas de frecuencia con ruido.

Los dispositivos utilizados en este son enrutadores bajo el estándar 802.11g en la figura 1,esto incluye entre sus características principales, mecanismos de cifrado tal como WEP y WPA que se encargan de codificar la información transmitida, es necesario conocerlos para comprender la funcionalidad de algunos lineamientos de seguridad que se encontraran en OSSTMM y a lo largo de este documento.

Figura 1. Casos de estudio, D-Link524 y WRT54Gh.

III. IDENTIFICACIÓN DE VARIABLES Y CUANTIFICACIÓN DE RIESGO

Para brindar al usuario un informe comprensible se debe realizar una cuantificación del riesgo que es un tanto difícil de evaluar [7], para esto se cuenta con la guía Sistema Común de Puntuación para Vulnerabilidades (CVSS, *CommonVulnerabilityScoringSystem*) Además del riesgo cada enrutador posee parámetros de configuración que permiten ajustar las características de seguridad tanto inalámbrica como cableada, la elección de las variables está orientada solo al modo inalámbrico y a la disponibilidad de estas variables en el *webconfig*, esta elecciónes soportada con auditorias y medidas de eliminación de vulnerabilidades.

La guía CVSS es utilizada para darle un puntaje a las vulnerabilidades, es aplicada también en administración de riesgo[8], con el objetivo de calcular el nivel de amenaza o riesgo en un enrutador, la aplicación desarrollada integra las ecuaciones especificadas en la guía más las bases de datos de vulnerabilidades y sus respectivas formas de mitigación, brindando a los usuarios más información acerca de su nivel de riesgo.

las características propias de un dispositivo de direccionamiento inalámbrico como; servidor DHCP, Credenciales de acceso, difusión de la SSID, interfaces de administración Web, entre otras, presentan vulnerabilidades que son recopiladasEn la Base de Datos Nacional (NVD, *NationalVulnerabilityDatabase*) y la Base de Datos de código abierto de vulnerabilidades (OSVDB, *Open SourceVulnerabilityDataBase*) al igual que otras iniciativas han hecho un esfuerzo por almacenar la gran cantidad de vulnerabilidades en la IT, luego de encontrar una redundancia de información en las bases de datos mencionadas, se optó por usar solo la información de NVD. Esta búsqueda de vulnerabilidades se realiza solo para los casos de estudio, dejando abierta la posibilidad de ingresar más datos para diferentes modelos de enrutadores en trabajos posteriores.

No solo se utilizaron las Vulnerabilidades de NVD si no que se instalaron algunas herramientas que proveían algún grado de información parecida para los casos de estudio, con estos hallazgos se puede completar la Base de datos del Proyecto (figura 2).

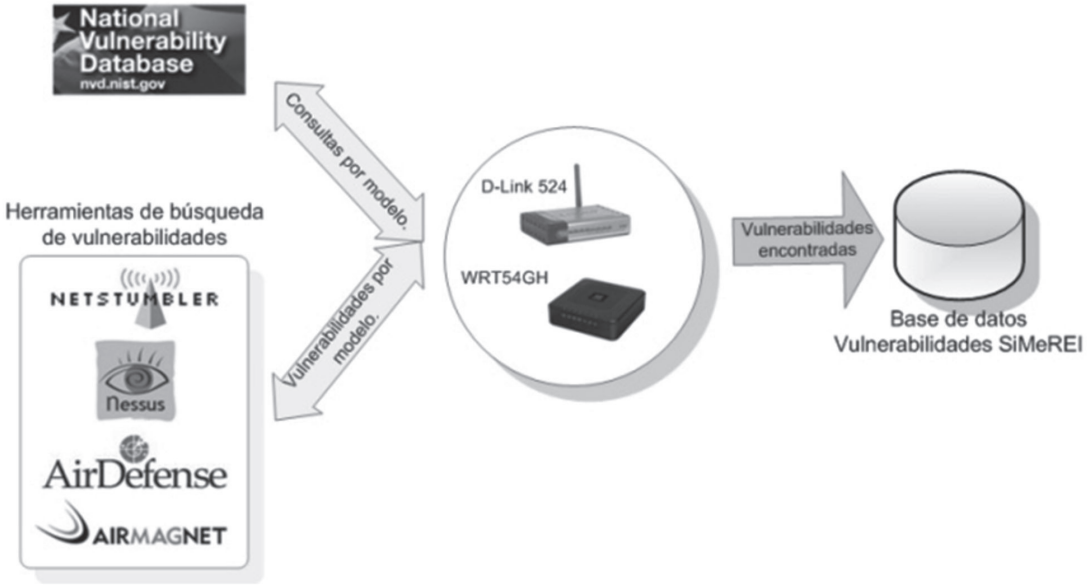

Figura 2. Obtención de las vulnerabilidades para la base de datos.

Las vulnerabilidades orientadas directamente hacia los casos de estudio crean la necesidad de la mitigación de las mismas. Por medio del seguimiento de estas se encuentran soluciones o procedimientos asociados a cada una, con el objetivo de eliminarlas.Para tener una gestión adecuada tanto de los problemas como de las soluciones, se construye una Base de Datos Relacional (BD), destinada a la administración de la información y a complementar la aplicación desarrollada, para así brindar al usuario un informe más completo acerca de su enrutador, las vulnerabilidades que contiene, y el riesgo que esto implica.

Por otra parte los procedimientos y políticas que adicionaran seguridad al enrutador implican la modificación de ciertos parámetros o variables propias de estos dispositivos de direccionamiento como la contraseña (*password)* de administración, el cifrado, el SSID etc. No hay que olvidar que la selección de estas variables se realiza a partir de observación de la página web de configuración *web config* de cada enrutador estudiado (la aplicación obtiene estas variables del *web config*), y del objetivo planteado de conseguir más seguridad inalámbrica.Las variables seleccionas, son modificables por medio del *web config*de cada *router*y son las siguientes:

Revista Avances en Sistemas e Informática, Vol.8 No. 3, diciembre de 2011 - Medellín. ISSN 1657-7663

Tabla II. Variables modificables de los casos de estudio

Nombre	Descripción
SSID	Nombre que los enrutadores emplean para su red inalámbrica en el caso del WRT54GH es *Linksys*, conocido ampliamente.
Contraseña	Estos dispositivos inalámbricos, piden una contraseña cuando se quiere acceder a ellos o cambiar su configuración, este *password* está predeterminado y es *admin*.
Filtrado MAC*Media Access Control*	El enrutador Linksys y el D-Link tienen la capacidad de permitir el control de acceso al medio mediante filtrado de direcciones, esta opción viene deshabilitada por defecto.
Cifrado	El cifrado ayuda a proteger los datos transmitidos a través de una conexión inalámbrica, *Wi-Fi* ofrece diferentes niveles de seguridad.
Configuración DHCP	El servidor *Dynamic Host ConfigurationProtocol*(DHCP)viene predeterminado, se encarga de asignar dinámicamente direcciones *Internet Protocol* (IP).
Firmware	Descargando la última versión desde la página web del fabricante podemos mitigar un gran número de vulnerabilidades.

Luego de la definición de las Variables es necesario asignar a estas un peso dentro del análisis de riesgo, para esto se emplea la guíaCVSS que define una serie de fórmulas y a partir de un grupo de métricas observados en lafigura 3, asocia una puntuación a una determinada vulnerabilidad o variable, para nuestro caso de estudio consideramos que las métricas base son las más acordes para determinar el riesgo.

La aplicación de la guía en las variables de la tabla III arroja valores numéricos utilizados para mostrarle al usuario un informe de riesgo cuantitativo y cualitativo, con el objetivo de hacer más clara la necesidad de implementar medidas que disminuyan el riesgo presente. El ejemplo de la tabla III muestra como asignar cada métrica a una variable elegida, teniendo en cuenta las características descritas en la justificación.

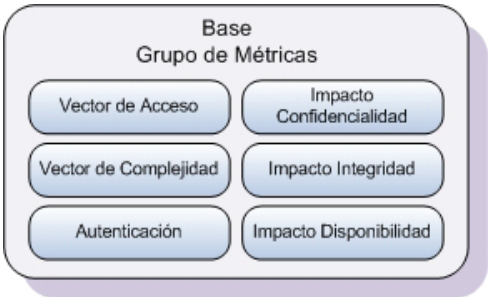

Figura 3 Grupos de métrica de CVSS.

Tabla III. Ejemplo de la aplicación de la guía CVSS a variable Contraseña.

Variable	Contraseña de Administración del Enrutador			Descripción
Nombre Estado de Vulnerabilidad	Débil	Mediana	Fuerte	
Vector de acceso	1	1	1	El fácil acceso a las contraseñas por defecto de los enrutadores, y la importancia de la autenticación como administrador implica impactos mayores.
Complejidad de Acceso	0,71	0,61	0,35	
Autenticación	0,70	0,56	0,45	
Explotabilidad	10,0	6,83	3,15	
Impacto de Confidencialidad	0,66	0,66	0,28	
Impacto de Integridad	0,00	0,00	0,00	
Impacto de Disponibilidad	0,00	0,00	0,00	
Impacto Total	6,87	6,87	2,86	
Puntaje de Severidad	7,79	6,30	1,74	

La comparación entre el nivel de severidad de las siete variables se refleja en la figura 4, donde se observa que la variable cifrado implica una de las mayores severidades luego de la aplicación de la guía CVSS, además son mostrados los estados de vulnerabilidad de cada variable, por ejemplo para el cifrado son cuatro estados; deshabilitado, WEP, WPA y WPA2 cada uno de ellos con diferentes puntajes de severidad.

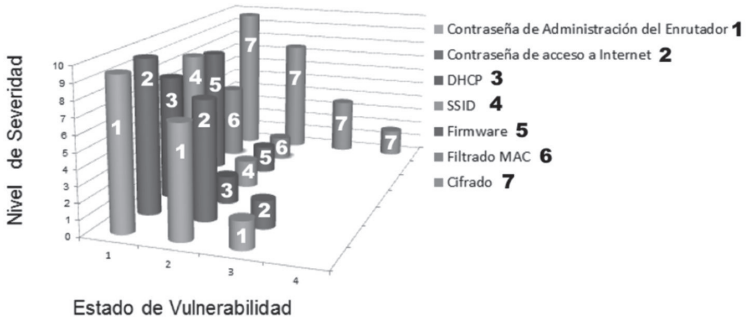

Figura 4. Visualización del Impacto Total Según el Estado de Vulnerabilidad

IV. LINEAMIENTOS DE SEGURIDAD

Para efectuar una disminución del riesgo según el puntaje asignado a cada variable, o según las vulnerabilidades almacenadas en la BD que afecten a un modelo de enrutador, es necesario realizar cambios en las variables descritas, este cambio se realiza a partir de lineamientos de seguridad.

El manual de metodología abierta de testeo de seguridad OSSTMM ha generado una lista de buenas prácticas a las redes inalámbricas, algunas de estas se aplican directamente sobre enrutadores, por esto OSSTMM es la principal fuente de información para elaborar los lineamientos descritos en este capítulo[11].

Además de contar con OSSTMM, las auditorías realizadas por el instituto SANS a enrutadores [12],[13], [14], permiten comprender muchas de las vulnerabilidades y amenazas que se encuentran en una situación real, los *checklist* permiten focalizar en nuestro proyecto las variables y lineamientos de seguridad.

Otra fuente para los lineamientos son los manuales de buenas prácticas de seguridad de cada fabricante, donde enfatizan por ejemplo en la problemática de la configuración por defecto y el cifrado indicado.

La figura 5 muestra las fuentes descritas anteriormente que son las que se usan para elaborar los lineamientos de seguridad para el sistema elaborado.

Luego de obtenidas la fuentes, es posible elaborar un buen número de lineamientos que recaen sobre las variables.

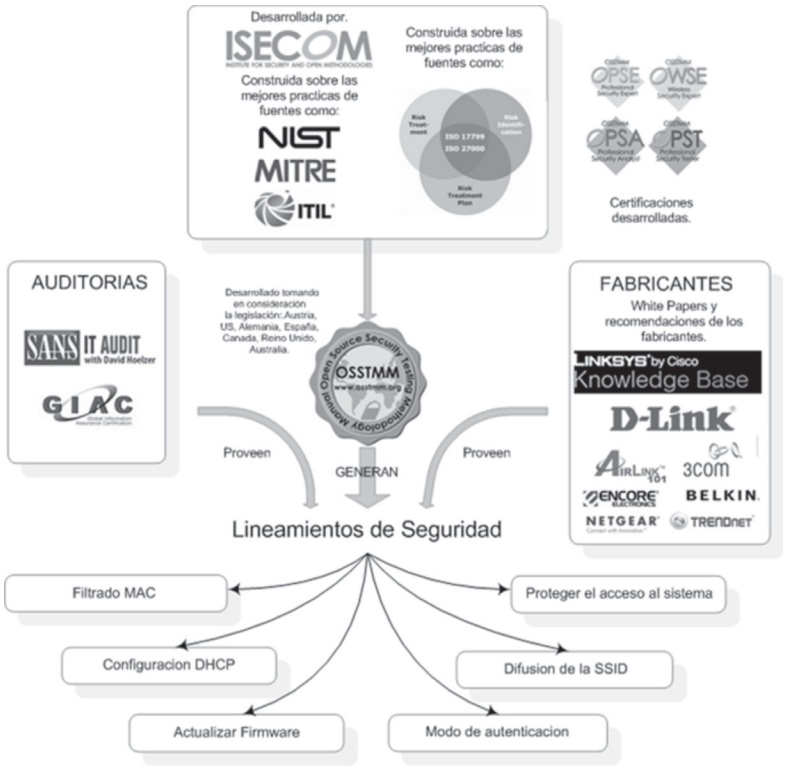

Figura 5. Obtención de los lineamientos de seguridad para el proyecto.

Revista Avances en Sistemas e Informática, Vol.8 No. 3, diciembre de 2011 - Medellín. ISSN 1657-7663

En seguida se resumirá uno de los lineamientos mencionados en la gráfica.

Proteger el acceso al sistema

Cambiar el nombre de usuario y contraseña por defecto, además, la contraseña debe tener mínimo 14 caracteres [15] y cambiarse regularmente.

El cambio de estos parámetros tiene como objetivo aumentar la seguridad del enrutador, ya que son públicamente conocidas, solo difieren del modelo y fabricante de cada enrutador [16], con lo cual se pretende garantizar que el enrutador va a presentar resistencia frente a ataques como "*password guessing*" y "*password cracking*" [17], evitando que un atacante remoto adquiera los privilegios de administrador del enrutador.

Otro parámetro a tener en cuenta es la fortaleza de la contraseña, debido a que existen amenazas que buscan vulnerarla [18], además actualizar el Firmware del dispositivo para evitar fallas de fábrica [19].

Después de evaluar lineamientos diseñados, se van a elaborar controles para ser implementados por el usuario SiMeR. Con la definición de los lineamientos el usuario logrará disminuir el riesgo presente en su enrutador, pero debe seguir una serie de pasos que logren modificar la variable indicada y llevarla al estado que brinde más seguridad.

Cuanto mayor sea el riesgo perteneciente a cada estado de vulnerabilidad en una variable, mayores deberán ser los controles y cambios que deben ser aplicados para disminuir el riesgo asociado, estos controles serán aplicados directamente sobre el enrutador por medio de la interfaz web de configuración del enrutador. Los cambios van desde modificar la contraseña, hasta lo más simple como deshabilitar o habilitar una variable.

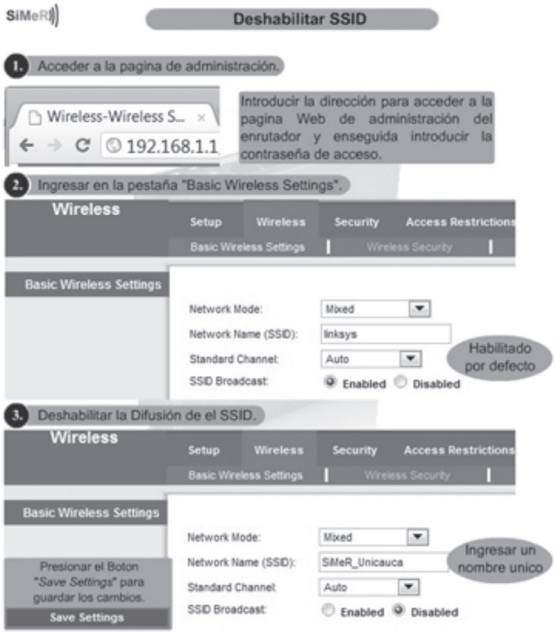

Figura 6. Control para deshabilitar el SSID.

Uno de los requerimientos para aplicar cada uno de los controles es necesariamente estar autorizado para ingresar a la página web de configuración del enrutador, esto implica tener credenciales de ingreso, un usuario y una contraseña (si es la primera vez las credenciales estarán por defecto). Estos controles son mostrados al usuario SiMeR por medio de la aplicación diseñada, según sean necesarios. Un ejemplo de ellos es mostrado en la figura 6.

V. PROTOTIPO Y RESULTADOS

El sistema de medición de riesgo propuesto, busca informar al usuario acerca del estado actual de la configuración de su enrutador, las falencias derivadas a esta, y cuantifica el riesgo presente, basado en las vulnerabilidades del modelo de enrutador 802.11ganalizado, verificando las variables que proveen seguridad inalámbrica, y así proponer al usuario lineamientos que le permitan disminuir el riesgo.

El sistema debe proveer las siguientes características:

Permitir la adición, modificación y en general la administración de las vulnerabilidades, los modelos de enrutadores y variables, por ejemplo, cada una de vulnerabilidades tiene una descripción, un identificador CVE y un puntaje CVSS.

Relacionar el modelo del enrutador, con sus respectivas vulnerabilidades a través de sus variables, las cuales pueden tener un estado definido.

Presentar al usuario las variables del enrutador en su estado actual.

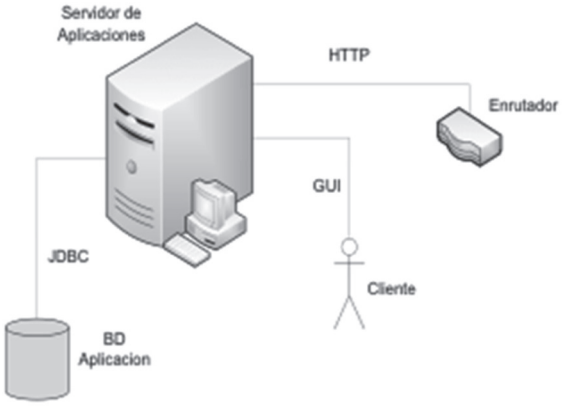

Figura 7. Arquitectura del sistema SiMeR.

Analizar el estado de vulnerabilidad de cada una de las variables del enrutador para calcular el nivel de riesgo, el cual debe ser mostrado al usuario de forma gráfica.

Los controles elaborados, deben ser mostrados al usuario de forma gráfica y detallada, de tal forma que permitan configurar adecuadamente las variables de configuración del enrutador y

con ello ayudar a mitigar las vulnerabilidades que presenta el enrutador.

En la arquitectura de despliegue se da una idea general del proyecto SiMeR y se explica el funcionamiento general del mismo, como podemos observar en la figura 7. Servidor de Aplicaciones

El servidor de aplicaciones corresponde al sistema de medición de riesgos, contiene las interfaces de administrador y cliente, además, el control que permite la comunicación y gestión con el enrutador.

• Modulo Comunicación HTTP

Este módulo es el intermediario entre el servidor y el enrutador inalámbrico, permite que el servidor tenga conexión y comunicación con el enrutador inalámbrico mediante la librería HTTPClient (recepción de datos).

• Servidor Base de Datos

El servidor de base de datos permite almacenar información, es una base de datos relacional, diseñada en MySQL y se accede a ella a través de JDBC.

En la figura8 se plasma el diagrama de despliegue de la Aplicación, consta de tres nodos de vital importancia; el primero corresponde al enrutador, el cual contiene la configuración de las variables a examinar. El segundo, el servidor de aplicaciones que brinda las herramientas necesarias para que el usuario y el administrador utilicen el sistema. Por último la Base de Datos que permite gestionar la información desde la aplicación diseñada.

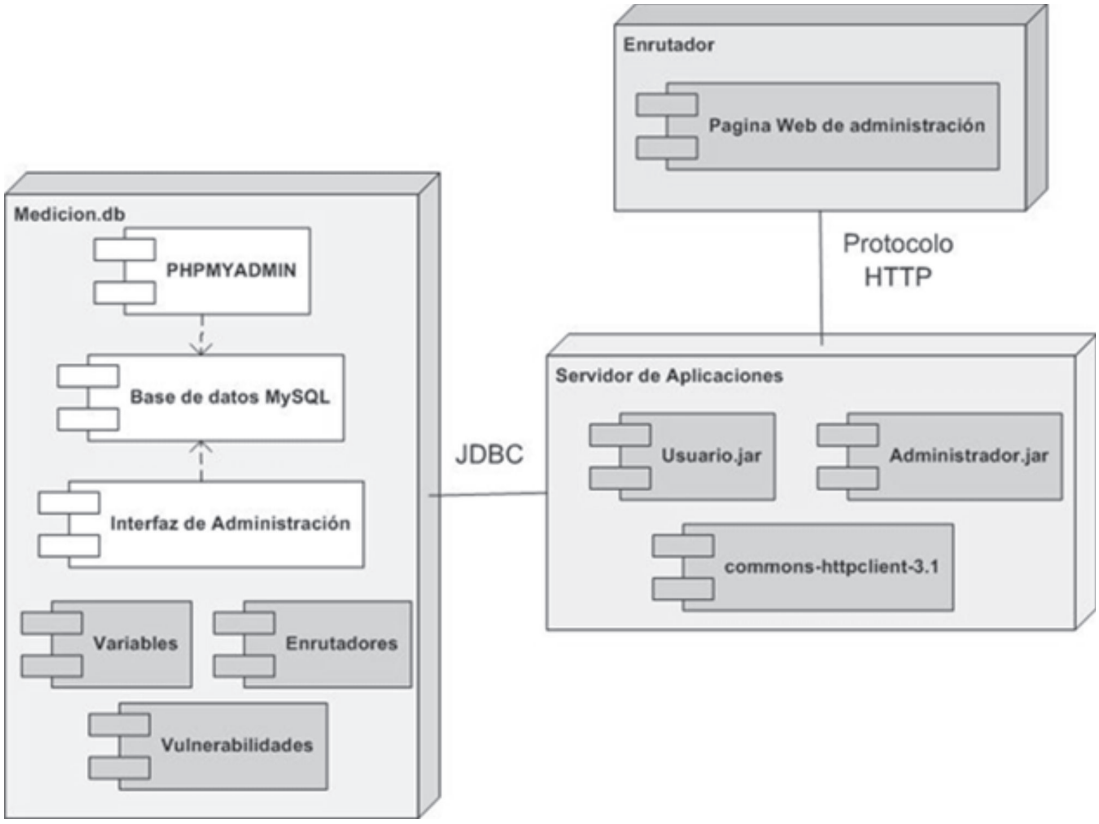

Figura 8. Diagrama de despliegue de la Aplicación diseñada.

VI. EXPERIMENTACIÓN Y PRUEBAS

Las pruebas se realizaronen un escenario SOHO con un enrutador inalámbrico WRT54GH configurado por defecto,

Se verifica el acceso por medio de las credenciales de usuario, se prueba la obtención del estado actual de su enrutador, realizando el escaneo de las variables por medio de la ejecución de la aplicación, estos valores son mostrados en la interfaz principal de Medición del Riesgo, en caso de cambiar la configuración de alguna variable, la aplicación registra esto en una ejecución posterior y deshabilitar el despliegue del control apropiado.

La cuantificación del riesgo se realiza internamente cotejando las vulnerabilidades encontradas y las variables afectadas, y este valor cuantitativo es mostrado al usuario en forma gráfica. Igualmente en una ejecución posterior luego de realizar cambios positivos el riesgo disminuye.

Ingresar con la contraseña de administración de SiMeR por medio de la interfaz de la figura 9. Luego de presionar el botón de validar se verificara el correcto ingreso de los anteriores parámetros.

Revista Avances en Sistemas e Informática, Vol.8 No. 3, diciembre de 2011 - Medellín. ISSN 1657-7663

Figura 9. Interfaz para el ingreso del Administrador del Sistema.

Ahora se presenta la interfaz para la administración de SiMeR, donde puede gestionar los aspectos del sistema de medición, que se observan en la figura 10.

Figura 10. Interfaz de Administración de SiMeR.

Como un ejemplo de la gestión del sistema accedemos a la interfaz mostrada en la figura 11, donde es posible modificar vulnerabilidades, podemos observar el identificador estandarizado de la NVD con el puntaje CVSS asignado y una descripción de la vulnerabilidad, además de buscarla en la BD del SiMeR, el administrador puede modificar su puntaje y su descripción que serán almacenados de nuevo en la BD.

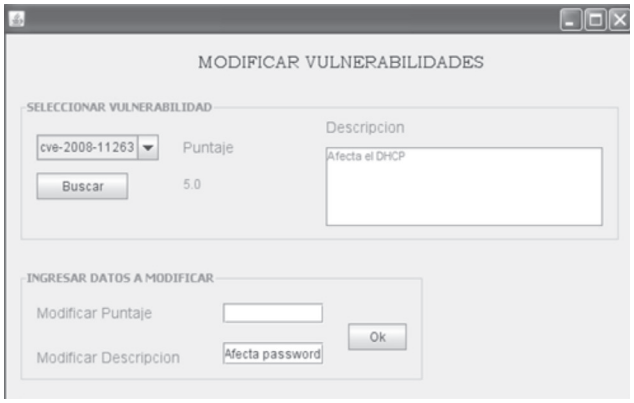

Figura 11. Modificación de una vulnerabilidad contenida en la BD.

La BD está disponible en el gestor de bases de datos phpMyAdmin, así es posible verificar el correcto almacenamiento de la información del sistema de medición de riesgo.

El ingreso del usuario se da por medio de la interfaz mostrada en la figura 12. Estas credenciales son las de administración del enrutador, por defecto están la mismas indicadas anteriormente, la parte adicional es la elección del enrutador que se procede a analizar, este elemento debe ser adicionado previamente por el administrador de SiMeR.

Figura 12. Interfaz inicial para el acceso del Usuario.

Luego de presionar el botón analizar, se observa el despliegue de la interfaz principal, mostrada en la figura 13, de esta forma se prueba que las variables del enrutador son abstraídas del mismo y mostradas al usuario en su estado actual, permitiendo a la lógica del sistema realizar una caracterización de cada una de ellas para luego hacer la cuantificación del riesgo presente.

Figura 13. Interfaz principal de SiMeR con el enrutador configurado por defecto.

En la figura anterior observamos que el riesgo es mostrado de forma gráfica con una barra de colores y un porcentaje que indica un rango de advertencia para el usuario que realiza la medición. Las vulnerabilidades asociadas a ese modelo de

enrutador pueden ser leídas en la parte derecha de la interfaz, adicionalmente los controles que permitirán disminuir el riesgo son desplegados según las variables que estén con fallas en su configuración.

En la figura 14está plasmada la medición posterior a la implementación de los controles activados mostrados en la figura 13, se observa que el riesgo disminuyo y los estados de las variables han cambiado según la modificación realizada en el enrutador inalámbrico.

Figura 14. Interfaz principal de SiMeR luego de implementar los controles.

La realización de una encuesta (Tabla IV)arroja la figura 15 donde se evalúa la interacción del usuario SOHO con SiMeR, con el fin de conocer su nivel de funcionalidad y desempeño.

Tabla IV. Cuestionario realizado a los usuario SOHO que prueban SIMER.

Característica	Descripción
Funcionalidad	¿La forma como la aplicación SiMeR muestra el nivel de riesgo y los controles asociados a cada variable fueron útiles?
Confiabilidad	Durante la medición y la obtención de un nivel de riesgo aceptable, ¿la aplicación permitió realizar la medición las veces necesarias sin interrupciones?
Usabilidad	¿Los controles fueron desplegados de forma eficiente y su implementación fue sencilla?
Eficiencia	¿La aplicación permitió la disminución del riesgo eficientemente y en un tiempo prudente?
Portabilidad	¿La instalación de la aplicación SiMeR en su ambiente de trabajo se realizó con éxito?

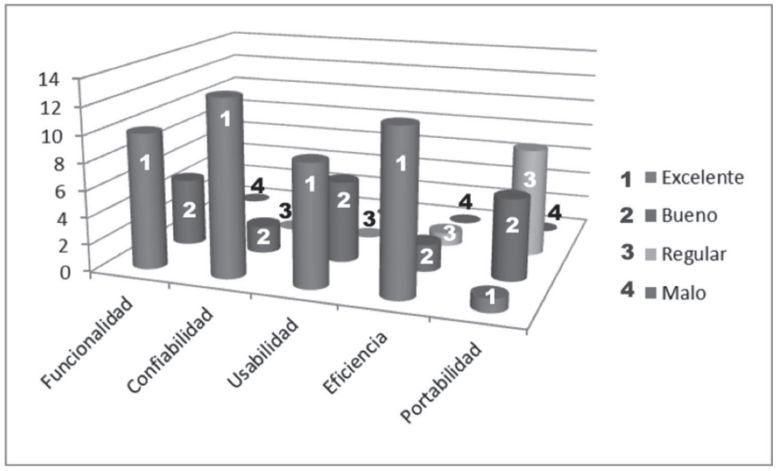

Figura 15. Resultados de las pruebas realizadas al prototipo SIMER.

VII. CONCLUSIONES

Se obtiene una disminución del riesgo presente en los enrutadores 802.11g con la modificación de las variables seleccionadas y la aplicación de los lineamientos de seguridad propuestos.

La logra la protección de la información mediante la adecuada configuración de los parámetros del enrutador, gracias a la utilización de SiMeR.

Existe desconocimiento por parte de los usuarios SoHo del conjunto de parámetros configurables de los enrutadores que les permitirán proteger sus activos.

SiMeR fue concebido inicialmente como un sistema de medición del riesgo, adicionalmente brinda un conjunto de controles gráficos que le permiten aumentar el nivel de seguridad de los enrutadores inalámbricos que soportan el estándar 802.11g.

REFERENCIAS

[1] IEEE Computer Society, *802.11Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)specifications*. 23 julio 2004.

[2] Airwave, *Gartner Group Wireless LAN's, and HIPAA*. http://airwave.com/docs/brochures/amp-hipaa.pdf.

[3] Hao Hu, Steven Myers, VittoriaColizza, Alessandro Vespignani, *WiFi Epidemiology: Can Your Neighbors Router Make Yours Sick?*.Febrero 3, 2008.

[4] P. Hertzog. "OSSTMM - *Open Source Security Testing Methodology Manual*,"Institute for Security and Open Methodologies, ISECOM. Disponible: http://www.isecom.org/osstmm/.
[5] United States General Accounting Office*, Information Security Risk Assessment Practices Of Leading Organizations*, Noviembre 1999.
[6] Go Wireless,*Open up new possibilities for work and play.* Disponible en: http://h20331.www2.hp.com/ hpsub/downloads /356395-001-web.pdf.
[7] Berkley University, *Intercepting Mobile Communications: The Insecurity of 802.11*. http://www.isaac.cs.berkeley.edu/isaac/ mobicom.pdf.
[8] Peter Mell, Karen Scarfone, Sasha Romanosky, *A Complete Guide To The Common Vulnerability Scoring System Version 2.0*, FIRST, Junio 2007.
[9] José Manuel Huidrobo, *qué es… seguridad en Wi-Fi*, Agosto 2005.
[10] Robert Moskowitz, *WLAN Testing Reports "Debunking the Myth of SSID Hiding",* ICSA Labs.Diciembre 1 de 2003.
[11] Pete Herzog*, Osstmm Wireless 2.9.1 Wireless Security Testing Section Open-Source Security Testing Methodology Manual*, 30 Octubre 2003.
[12] Ryan Stall *, Auditing A Cisco Aironet Wireless Network Forma N Auditor Perspective*, GSNA V2.1 Practical, SANS Conference 2002 Washington D.C
[13] Raul SilesPelaez, *Auditing 802.11 Wireless Networks Focusing On The Linksys BEFW11S4 Access Point*, Febrero 17, 2004.
[14] Ryan Lowdermilk, *Auditing The Cisco Aironet 1200 Wireless Access Point In A Small To Medium Size Business Environment (SMB)*, GSNA V2.1 Practical, Octubre 10, 2003.
[15] Johanna Quintero, *Recomendaciones de uso de contraseñas seguras*, Global Crossing, Colombia, 9 Marzo de 2010.
[16] Default Password List, Disponible en: http://www.phenoelit-us. org/dpl/dpl.html
[17] SysWoody*, Ataque contra contraseñas*, Disponible en: http:// www.syswoody.com/analisis-forense/ataque-contra-contrasenas
[18] NVD, *vulnerabilidad CVE-2008-1264*, Disponible en: http://web. nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1264
[19] Cisco, *Manual de usuario*, Linksys, disponible en: http://www. linksysbycisco.com/LATAM/es/support/WRT54GH/download