METODOLOGÍA Y ANÁLISIS ORIENTADO A LA SEGURIDAD WEB

JONNATTAN ARLEY GONZÁLEZ RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2018

METODOLOGÍA Y ANÁLISIS ORIENTADO A LA SEGURIDAD WEB

Jonnattan Arley González Ruiz

ASESOR DE PROYECTO
Yolima Mercado Palencia

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2018

AGRADECIMIENTOS

En primer lugar quiero agradecer a Dios, por guiarme en el camino, brindarme una excelente familia y fortalecerme espiritualmente para empezar un camino lleno de éxito.

De igual manera, quiero mostrar mi más sincera gratitud a todas aquellas personas que estuvieron presentes en la realización de este proyecto, en especial a los tutores e ingenieros por todos sus aportes, sus conocimientos, sus consejos y su dedicación.

Muestro mis más sinceros agradecimientos a mi tutora de proyecto, quien con su conocimiento y su guía fue una pieza clave para que pudiera desarrollar cada etapa de desarrollo del proyecto.

Por último, quiero agradecer a la base de todo, a mi familia, en especial a mis padres, que quienes con sus consejos fueron el motor de arranque y mi constante motivación, muchas gracias por su paciencia y comprensión, y sobre todo por su amor.

¡Muchas gracias por todo!

CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

Actualmente los avances en las tecnologías de información y en las telecomunicaciones demandan medidas de seguridad para salvaguardar el recurso más importante de toda organización, entidad o negocio, la información.

La falta de medidas de seguridad en las aplicaciones web causa un gran impacto, debido a que los riesgos, ataques y amenazas permanecen latentes en la sociedad. Por tanto, la vulnerabilidad de los sistemas de información es mayor. Lo anterior, obedece a que a medida que crecen los mecanismos de seguridad, surgen nuevos ataques y amenazas más especializados, obligando a buscar nuevos mecanismos de seguridad que permitan la protección de las aplicaciones web en la red de redes internet.

La seguridad informática es un tema amplio y se encarga principalmente de evitar que factores como la curiosidad, robo de información, competitividad desleal, entre otros, vulneren los sistemas de información. Por consiguiente, nace la necesidad de implantar medidas, procesos y procedimientos que velen por la integridad, disponibilidad y confidencialidad de dichos sistemas.

TITULO DEL PROYECTO

METODOLOGÍA Y ANÁLISIS ORIENTADO A LA SEGURIDAD WEB

1. PLANTEAMIENTO DEL PROBLEMA

Las organizaciones o empresas que actualmente tienen disponibles sus páginas web en internet, se encuentran expuestos a amenazas y ataques que ponen en riesgo su permanencia e información. Razón por la cual, se hace necesario que las empresas conozcan a través de una metodología, la importancia de la seguridad en las aplicaciones web con respecto a su protección y prevención, así mismo, que logren considerar la implementación de la seguridad en sus aplicaciones web.

La elaboración de una metodología que incorpore políticas de seguridad informática, permite a las empresas y personas tener claridad de la importancia de mantener aplicaciones web seguras, más aún, cuando la seguridad es una de las prioridades más bajas a la hora de disponer una aplicación web en producción tal y como expone Juliana Rodríguez, *"Según Gartner el 75% de los ataques están dirigidos a estas plataformas, sin embargo para muchas organizaciones aún no es una prioridad la implementación de tecnologías para su protección."*.[1]

Ahora bien, Juliana Rodríguez en su texto manifiesta que en los últimos años han ocurrido una serie de eventos informáticos que han afectado de manera importante la sociedad colombiana, casos como el sucedido en julio de 2014, en donde se vieron afectados alrededor de 25 sitios web gubernamentales por ataques como el defacement y la denegación de servicio, los cuales fueron ejecutados por Anonymus Colombia. De igual manera, un grupo de hackers colombianos en enero de 2015, llevo a cabo un ataque por más de ocho horas a la página web del Ministerio del Interior, tema que pudo ser constatado debido a que la pagina no se encontraba disponible y al ingresar a la misma arrojaba un mensaje que indicaba que la pagina había sido hackeada.[2]

Por consiguiente, es necesario dar a conocer la importancia de la seguridad en las aplicaciones web y diferentes medidas de seguridad, las cuales orientarán a las organizaciones o personas para tener la capacidad de garantizar la seguridad de la información en sus aplicaciones, ya sea protegiendo, previniendo, detectando y/ o corrigiendo. Esto enfocado firmemente en desarrollar una metodología que permita mejorar y mantener la disponibilidad, confidencialidad e integración de la información de las empresas y usuarios.

---

[1] RODRÍGUEZ, Juliana. ¿Debo priorizar la seguridad de las aplicaciones web? [En Línea], mayo 2015. Disponible en: <https://www.b-secure.co/blog/debo-priorizar-la-seguridad-de-las-aplicaciones-web>.

[2] RODRÍGUEZ, Juliana. ¿Debo priorizar la seguridad de las aplicaciones web? [En Línea], mayo 2015. Disponible en: <https://www.b-secure.co/blog/debo-priorizar-la-seguridad-de-las-aplicaciones-web>.

Por lo plasmado anteriormente, es válido que la seguridad de una aplicación web es un tema de gran relevancia, por tanto, se debe llevar a cabo con las mayores garantías incorporando en todos y cada uno de los pasos del ciclo de vida de la aplicación, desde su concepción inicial hasta su puesta en producción.

Los sitios web hoy en día presentan problemas de vulnerabilidades bastante graves y con tendencia al aumento, esto debido a que la mayoría de las empresas en su afán de entregar a tiempo el desarrollo de las aplicaciones y servicios web para satisfacer al cliente, no contemplan los controles y seguridad de estos desarrollos omitiendo por completo el ciclo del desarrollo antes de su puesta en producción, tema que efectivamente expone estos productos ataques y amenazas en la red.

Lo anterior, se puede constatar en el artículo de Tamara Naudi dispuesto onasystems.net en donde indica: *"Acunetix, pionero en software de automatización de seguridad de aplicaciones web, nos muestra que el 55% de los sitios web presenta problemas de vulnerabilidades graves y con tendencia al aumento, Acunetix anuncia en su informe anual (Web App Seguridad 2016). Las vulnerabilidades web están en aumento y se presentan en la mayoría de páginas web en todo el mundo.*

Las vulnerabilidades han aumentado en un 9% en el último año debido principalmente a que las empresas exigen ciclos de lanzamiento de aplicaciones de manera más rápida.

De acuerdo al informe este analizó a 45.000 sitios web y red escaneos sobre 5.700 objetos de análisis a partir de abril de 2015 hasta marzo de 2016, los resultados muestran que el 55% de los sitios web tienen una o más vulnerabilidades de gravedad alta, este tipo de comportamiento se ha deteriorado significativamente en sólo un año, un crecimiento del 9% respecto al informe del año 2015. Además, se encontró que el 84% de las aplicaciones de Internet pueden tener vulnerabilidades de mediana gravedad, mientras que el 16% de los activos de la red perimetral también fueron susceptibles a al menos una vulnerabilidad de gravedad media.".[3]

Por otra parte, las empresas y/o organizaciones deben documentarse y tener claridad de lo que representa la presencia de una vulnerabilidad y los alcances

[3] NAUDI, Tamara. El segundo informe de seguridad de la aplicación web de Acunetix muestra que el 55% de los sitios web tienen vulnerabilidades graves (y aumentan) [En Línea], agosto 2016. Disponible en: <https://www.acunetix.com/blog/news/web-app-security-report-2016/>.

que puede tener un atacante al llevar a cabo un acceso no autorizado a la información financiera, de salud, de secreto comercial, de clientes entre otros. Esto teniendo en cuenta que *"son varias las modalidades de las cuales hoy en día deben cuidarse las organizaciones. La denegación de servicio, el robo de información usando inyecciones SQL, el robo de sesiones de usuario mediante Cross Site Request Forgery (CSRF), son solo algunas de las que nuestro equipo de consultores ven más seguido."*.[4]

Por consiguiente, es necesario que las personas y/o empresas conozcan y entiendan la importancia de la seguridad en las aplicaciones web, para así mismo evitar las problemáticas como las mencionadas anteriormente. Es aquí, donde un método o metodología, contribuye a la sociedad brindando información de primer nivel sobre la importancia de la seguridad en las aplicaciones web para su prevención, detección y corrección.

En base en lo presentado en esta sección, es posible plantear la siguiente pregunta problema:

¿Cómo se puede brindar a las organizaciones o empresas, información de primer nivel frente a la importancia de la seguridad en las aplicaciones web para a su protección, prevención, detección y corrección?

[4] RODRÍGUEZ, Juliana. ¿Debo priorizar la seguridad de las aplicaciones web? [En Línea], mayo 2015. Disponible en: <https://www.b-secure.co/blog/debo-priorizar-la-seguridad-de-las-aplicaciones-web>.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Elaborar una metodología, sistemática y completa, que brinde información de primer nivel a las organizaciones frente a la seguridad en las aplicaciones web.

2.2. OBJETIVOS ESPECÍFICOS

- Contextualizar a las organizaciones acerca de los diferentes conceptos, pasos y acciones que hacen parte de la Seguridad en las Aplicaciones Web.

- Consultar mecanismos de protección tanto de software como de hardware que permitan la detección, mitigación y/o control de los diferentes riesgos y vulnerabilidades que presenten las Aplicaciones Web.

- Identificar los diferentes riesgos, amenazas y ataques presentados en las aplicaciones web de las organizaciones y/o empresas.

- Generar una metodología que indique métodos de protección, mitigación de los riesgos, amenazas y vulnerabilidades que se presenten en las aplicaciones web.

- Establecer una metodología que permita la creación de una política de seguridad de la información corporativa que incorpore controles que protejan y mantengan aplicaciones web seguras.

3. JUSTIFICACIÓN

El propósito de esta metodología es tratar a fondo las vulnerabilidades, amenazas y riesgos a los que se encuentran expuestas las aplicaciones web en la internet desde las grandes empresas hasta los usuarios y por ende ayudar a contribuir a la seguridad la información, esto mediante un elemento que brinde información de primer nivel que permita velar por la integridad, disponibilidad y confidencialidad de la información; teniendo en cuenta que en la sociedad actual la internet juega un papel fundamental, siendo una de las redes más usadas y como medio de comunicación, bien sea, para la descarga de información, consulta, tramites, transacciones, mensajería, transferencia de datos, entre otras.

La seguridad de un sistema o aplicación es un tema delicado y de suma importancia. Esto teniendo en cuenta que la privacidad, integridad de datos y protección de los mismos, están muy expuestos a personas que tienen propósitos delictivos. Por tanto, una aplicación web segura tanto para las empresas como para los usuarios, es hoy en día uno de los retos más importantes, razón por la cual, deben considerarse opciones de seguridad necesarias y sencillas pero eficientes, que ayuden a mitigar cualquier característica que las hagan vulnerables.

Ahora bien, las personas con propósitos delictivos como es el caso de los hackers están a la espera de atacar un sitio web para obtener información muy específica, o llevar a cabo actividades con objetivos mayores como el poder alterar un sitio web o tomar el control por completo con el objetivo de obtener beneficios económicos por la información que allí contienen a través de sus bases de datos.

Teniendo en cuenta lo anterior, cualquier empresa o persona puede ser víctima del espionaje o robo de información, más aún si las aplicaciones web no cuentan con la respectiva seguridad. Es por este motivo que surge la necesidad de que las aplicaciones web cuenten con altos niveles de seguridad, permitiendo de esta manera a las organizaciones generar valor y a su vez confianza a los usuarios o clientes, lo que termina siendo al final una gran estrategia comercial.

Corroborando lo anteriormente descrito, Tamara Naudi expone claramente que *“Las organizaciones están bajo intensa presión para entregar aplicaciones y servicios web para satisfacer las demandas de los clientes digitales modernas. Sin embargo, la seguridad aplicación no está a la par con el ciclo de desarrollo, que amplía la superficie amenaza de una marca. Por lo tanto, hoy en día hay un*

número significativamente mayor de defectos potenciales atacantes cibernéticos de explotar que hace 12 meses.", y que "Las organizaciones tienen que tener claro lo que esto significa - una vulnerabilidad alta severidad podría permitir a un atacante obtener acceso no autorizado a los datos y sistemas, potencialmente sensibles a la financiera, cliente, datos de salud y los secretos comerciales. También podrían trasladarse a otros sistemas para escalar el ataque aún más.[5]

De igual manera, surge la necesidad de que las páginas web cuenten con la debida seguridad y controles, para evitar riesgos y ataques que afecten las disponibilidad, confidencialidad e integridad de la información, ya que es sumamente valiosa tanto para las empresas como para los usuarios.

En consecuencia, un punto a resaltar obedece a que actualmente existe un elevado porcentaje de organizaciones que desarrollan sus aplicaciones web, sin tener en cuenta durante el ciclo de desarrollo la seguridad en elementos tan básicos como el acceso y control de los mismos. Esto tema genera brechas muy amplias para las personas como los hackers.

Es por esto que el desarrollo de este proyecto se centra en el estudio de la protección y seguridad de las aplicaciones web, métodos y soluciones para evitar ataques o intrusiones que generen perdidas económicas, de disponibilidad, confidencialidad e integridad de la información, tanto a organización como clientes y todo mediante un elemento que brinda información teniendo en cuenta documentos, artículos y experiencias.

Finalmente, se indica que la intención de esta metodología es brindar información de primer nivel sobre la importancia de la seguridad en las aplicaciones web, indicar medidas de seguridad tanto para la prevención, detección y corrección a las organizaciones o personas para que a su vez garanticen la seguridad de la información. Siempre enfocado a mejorar y mantener la disponibilidad, confidencialidad e integración de la información de las empresas y los usuarios.

[5] NAUDI, Tamara. El segundo informe de seguridad de la aplicación web de Acunetix muestra que el 55% de los sitios web tienen vulnerabilidades graves (y aumentan) [En Línea], agosto 2016. Disponible en: <https://www.acunetix.com/blog/news/web-app-security-report-2016/>.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El alcance de este proyecto es proporcionar un elemento de información como lo es una metodología, la cual tiene como fin brindar información de primer nivel a las empresas u organizaciones con respecto a la seguridad en las aplicaciones web, a su vez, indica medidas de seguridad tanto para la prevención, detección y corrección de infiltraciones, intrusiones, violaciones a la información o la obtención de recursos vitales de una organización o persona.

Este proyecto solo abarca fines informativos, proporcionando el detalle necesario para que una organización o usuario adquiera los conocimientos a los que se encuentra expuesta una aplicación web en internet, al igual que las medidas que se pueden tomar para que estos sitios web sean seguros y menos vulnerables frente ataques.

Todo lo anterior con la finalidad de que las empresas u organizaciones propendan en mantener la integridad, confidencialidad, disponibilidad y autenticidad de la información en una organización.

5. METODOLOGÍA DE TRABAJO

5.1. FOCALIZACIÓN

El proyecto se focaliza en el estudio de una situación que existe en un determinado grupo humano, en el cual se buscan conceptos que puedan determinar la realidad y entendimiento en profundidad.

En consecuencia, el proyecto se desarrolla de formar descriptivo-explicativo, toda vez que se ha llevado a cabo un trabajo de recopilación de información para conocer y entender los hechos, procesos, estructuras y personas en su totalidad, frente a la seguridad en las aplicaciones web para la implementación de procedimientos que dan un carácter único a las observaciones.

Por otra parte, se establece el uso de procedimientos para reducir la generalización del tema y ser puntual con la información a comunicar mediante una metodología.

Finalmente, durante la ejecución de este proyecto se desarrolla o afirma pautas y problemas centrales dentro del trabajo, orientando el proceso de la seguridad en las aplicaciones web.

5.2. MÉTODO

El método de trabajo aplicado este proyecto, se basa en la exploración, en donde se llega a interactuar en un tema de poco conocimiento por parte de las organizaciones, pero que tiene una gran relevancia a nivel organizacional y el cual se denomina seguridad en las aplicaciones web, tema que no ha sido abordado de una manera apropiada, total y concreta.

Este método, permite la identificación de conceptos o variables en donde inicialmente se realiza una observación particular o individual de los hechos, actividades, procesos, objetos y personas. Lo cual conlleva a un análisis y

generación de conclusiones generales que permitan establecer hipótesis precisas mediante una metodología.

5.3. FASES DE DESARROLLO DEL PROYECTO

Consiste en disponer información de primera mano, que permita dar a conocer y entender la importancia de la seguridad en las aplicaciones web; orientando toda su información a la prevención, detección y corrección ante ataques mediante la unificación de alternativas, software o herramientas que mitiguen o controlen los riesgos y vulnerabilidades.

Lo anterior se detalla a través de fases y actividades:

- **Fase 1:** Contextualizar a las organizaciones de los diferentes conceptos, pasos y acciones que hacen parte de la Seguridad en las Aplicaciones Web.

  Actividad 1: Consultar las formas de prevención, detección y corrección de ataques a las aplicaciones web, para así mismo, informar cuáles son los métodos más comunes de protección. De igual manera, concientizar a las personas u organizaciones sobre la importancia de aplicar mecanismos de seguridad en las aplicaciones web, exponiendo cada uno de los riesgos y amenazas que se presentan en la actualidad.

- **Fase 2:** Consultar mecanismos de protección tanto de software como de hardware que permitan la detección, mitigación y/o control de los diferentes riesgos y vulnerabilidades que presenten las aplicaciones web.

  Actividad 1: Conocer e informar las herramientas o aplicaciones que permitan identificar ataques o vulnerabilidades de las aplicaciones web, de igual manera, validar la existencia de software que controle o permita establecer aplicaciones web seguras.

- **Fase 3:** Identificar los diferentes riesgos, amenazas y ataques presentados en las aplicaciones web de las organizaciones y/o empresas.

Actividad: Realizar una exploración de los diferentes tipos de ataques a las a las aplicaciones web, para identificar y dar a conocer las vulnerabilidades y riesgos a los que está expuesto una aplicación, ya sea a nivel hogar, personal o empresarial. Así mismo, identificar los diferentes mecanismos de seguridad que garanticen la seguridad de la información en las organizaciones y/o personas.

- **Fase 4:** Generar una metodología que indique métodos de protección, mitigación de los riesgos, amenazas y vulnerabilidades que se presenten en las aplicaciones web.

  Actividad 1: Teniendo en cuenta la recopilación de información realizada, se debe establecer cada una de estas medidas con el propósito de contribuir a la seguridad la información, esto mediante elementos que permitan velar por la integridad, disponibilidad y confidencialidad de la información.

  Actividad 2: Considerar cada una de las opciones de seguridades necesarias y eficientes que apoyen la mitigación de riesgos y vulnerabilidades en las aplicaciones web.

- **Fase 5:** Establecer una metodología que permita la creación de una política de seguridad de la información corporativa que incorpore controles que protejan y mantengan aplicaciones web seguras.

  Actividad 1: Presentar al lector un documento que le permita comprender los conceptos necesarios de la importancia de la seguridad en las aplicaciones web, de igual forma, conocer los métodos, software y herramientas que establezcan aplicaciones web seguras tanto para personas como para organizaciones.

  Actividad 2: Concientizar de la necesidad de poner en práctica una serie de estrategias de seguridad para blindar y utilizar aplicaciones web seguras.

6. MARCO REFERENCIAL

6.1. ANTECEDENTES

6.1.1. Informe Acunetix

En el Segundo Informe Web App de Seguridad por Acunetix, Tamara Naudi da a conocer que el 55% de los sitios web tienen vulnerabilidades graves y estas en aumento. Por consiguiente, el informe brinda una estadística clara de la problemática que actualmente viven las aplicaciones web frente a su seguridad, ya que las vulnerabilidades se encuentran en aumento y para lo cual la seguridad de la información de las empresas y usuarios está más comprometida y expuesta a ataques.[6]

De igual manera, como apoyo para el desarrollo del proyecto, muestra sus datos estadísticos que permiten claramente establecer la necesidad de brindar información de primer nivel con respecto a la importancia de la seguridad en las aplicaciones web para su prevención, detección y corrección tanto a usuarios como a empresas.

6.1.2. Más de 760.000 sitios web fueron vulnerados en un año

El articulo brindado por eltiempo.com – Tecnósfera, establece información con respecto al estudio realizado por Google y la Universidad de Berkeley, y el cual revela que más de 760.000 aplicaciones web fueron vulneradas entre julio de 2014 a junio de 2015.[7]

[6] NAUDI, Tamara. El segundo informe de seguridad de la aplicación web de Acunetix muestra que el 55% de los sitios web tienen vulnerabilidades graves (y aumentan) [En Línea], agosto 2016. Disponible en: <https://www.acunetix.com/blog/news/web-app-security-report-2016/>.

[7] El Tiempo. "Tecnósfera. Más de 760.000 sitios web fueron vulnerados en un año" [En Línea], abril 2016. Disponible en: <http://www.eltiempo.com/archivo/documento/CMS-16567844>.

Claramente el artículo indica que los sitios web son poco seguros y están expuestos a diferentes ataques informáticos. Lo cual requiere de una atención pronta e inmediata para brindar una mejor seguridad de la información.

6.1.3. Hechos

- **Hallado virus informático en una central nuclear Alemana" Frankfurt 27/04/2016 7:45.**

  La Central nuclear Alemana descubrió en el año 2016, la existencia del virus que incluye W32 Ramnit y Conficker, en el sistema informático que se encontraba encargado de mover barras de combustible nuclear; esto sobre 18 unidades de datos extraíbles como lo son las memorias USB.

  El virus W32 Ramnit, fue diseñado para robar archivos e información de los equipos de cómputo que fueron infectados al igual que las tarjetas de software de Microsoft Windows. El virus W32 Ramnit se propaga a través de la red y con copias de sí mismo en unidades de datos extraíbles.

  Opera cuando el atacante consigue el control remoto de un sistema cuando está conectado a Internet.

  Generalmente este ataque, es controlado a tiempo, pero no deja de preocupar, por ser el blanco del ataque una planta nuclear.[8]

- **Enigma (Noticia de seguridad, mayo 11 de 2016)**

  El software malicioso presentado el pasado 11 de mayo de 2016 obedece a un ransomware, el cual fue detectado por primera vez a finales de pasado mes de abril de este mismo año. Sin embargo, este se presentó como Enigma y el cual utiliza un algoritmo AES mediante el cual se cifran los datos de cada una de sus víctimas y solicita el pago de alrededor de 200 dólares para recuperar la información. Los atacantes al recibir el respectivo pago entregan una clave

[8]FRANKFURT. Hallado un virus informático en una central nuclear alemana [En Línea], abril 2016. Disponible en: <http://internacional.elpais.com/internacional/2016/04/27/actualidad/1461751859_118617.html>.

de recuperación de los datos ya que el ransomware no elimina las Shadow Volume Copies de NTFS.

El troyano mencionado anteriormente, posee en su ejecutable o instalador la inyección de un código HTML/JS. El fichero HTML elaborado con JavaScript tiene todo lo necesario para compilar el sistema binario en el sistema de la víctima y abrir el navegador web de la víctima para terminar la descarga del ransomware, *"el propio código JavaScript ejecutará automáticamente este fichero, dando lugar al comienzo del cifrado de los datos; los datos cifrados pasarán a tener la extensión .enigma. Una vez finalice la infección se ejecutará un nuevo fichero llamado enigma.hta, el cual mostrará la nota de rescate, la cual está 100% en ruso y que, si traducimos, veremos que, como siempre, nos piden realizar un pago a través de la red Tor en un monedero concreto de Bitcoin"*.[9]

- **Troyano BPlug**

Es un malware troyano que se distribuye por Facebook, consiste en enviar mensajes infectados a los amigos de Facebook de la persona que accede al enlace enviado. Logra obtener contraseñas y toma el control de la red social. Crean un grupo, donde reúne todos los contactos que se tengan en la red social, se les envía un video que al momento de acceder al enlace, descarga e instala una nueva extensión del navegador Chrome, dando cabida al troyano.

La forma de evitar propagar este ataque: es detenerse a abrir estos videos con contenido pornográfico, violento, religiosos, cadena, entre otros asa provengan de fuentes conocidas.[10]

6.1.4. Aspectos Básicos de la Seguridad en Aplicaciones Web

El texto elaborado en abril de 2016 por Andrés Romero Mier y Terán y Mario Alejandro Vásquez Martínez, informa de manera clara las medidas básicas y practicas ante los posibles ataques que se puedan presentar en las aplicaciones web. En cuanto a las buenas prácticas indica el balanceo de riesgo y usabilidad,

[9]Noticias de Seguridad Informática. "¿Cuáles son los riesgos y ataques de seguridad en aplicaciones web?" [En Línea], marzo 2016. Disponible en: <http://noticiasseguridad.com/importantes/cuales-son-los-riesgos-y-ataques-de-seguridad-en-aplicaciones-web/>.

[10] Redeszone. El troyano bplug se dedica a molestar a tus amigos de Facebook [En Línea], abril 2016. Disponible en: <http://noticiasseguridad.com/malware-virus/el-troyano-bplug-se-dedica-molestar-tus-amigos-de-facebook/>.

rastrear el paso de los datos, filtrar entradas y validar el escapado de salidas. Con respecto a los ataques a los sitios web, da a conocer algunos de los más comunes como lo son Cross-Site Request Forgery, URL de tipo semántico, Cross-Site Scripting, Peticiones HTTP falsificadas, SQL Injection, Ataques de fuerza bruta, Password Sniffing etc.[11]

A su vez Andrés Romero Mier y Terán y Mario Alejandro Vásquez Martínez, establecen que el crecimiento del impacto que genera la red de redes internet sobre la información que se maneja día a día en las aplicaciones web es alto, lo que da a conocer las diferentes problemáticas que poseen las páginas web en cuanto a su programación y usabilidad. Lo anterior, proporciona una guía en el momento de identificar las diferentes vulnerabilidades a las que se encuentra expuesta una aplicación web y de las cuales los atacantes pueden aprovecharse y obtener información mediante las tecnologías en las que se basan los sistemas web. En consecuencia, aporta al proyecto medidas básicas y prácticas ante los posibles ataques que se puedan presentar en los sitios web, esto con el fin de garantizar la confidencialidad e integridad de la información transmitida.

6.1.5. Seguridad en Sitios Web

El Instituto Nacional de Tecnologías de la Comunicación S.A. (INTECO), a través de su guía de Seguridad en Sitios Web, se basa en informar al personal responsable de la seguridad informática de sitios web en adoptar medidas de seguridad para minimizar posibles daños, detectar ataques y tomar medidas preventivas de seguridad para que las aplicaciones web no se vean comprometidas. Esto teniendo en cuenta las actuales necesidades y problemas que se presentan día a día y lo cuales en varias ocasiones resultan ser desastrosos tanto para los usuarios como para las empresas.[12]

En consecuencia, la guía da a comprender y entender algunas técnicas que eviten a los atacantes obtener información confidencial, comprometer el funcionamiento de equipos y uso del espacio web para alojar diversos contenidos con fines fraudulentos o maliciosos.

Finalmente la guía, brinda un lineamiento claro de la detección y actuación frente a los ataques a los que se encuentran expuestos los sitios web, de igual manera, da a conocer una directriz clara de las actividades a ejecutar en cuenta a la prevención de ataques.

---

[11] MIER Y TERÁN, Andrés Romero - VÁSQUEZ MARTÍNEZ, Mario Alejandro Aspectos Básicos de la Seguridad en Aplicaciones Web [En Línea], abril 2016. Disponible en: <http://www.seguridad.unam.mx/documento/?id=17>.

[12] Instituto Nacional de Tecnologías de la Comunicación S.A. (INTECO). Seguridad en Sitios Web [En Línea], abril 2011. Disponible en: <https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridadwebsites.pdf>.

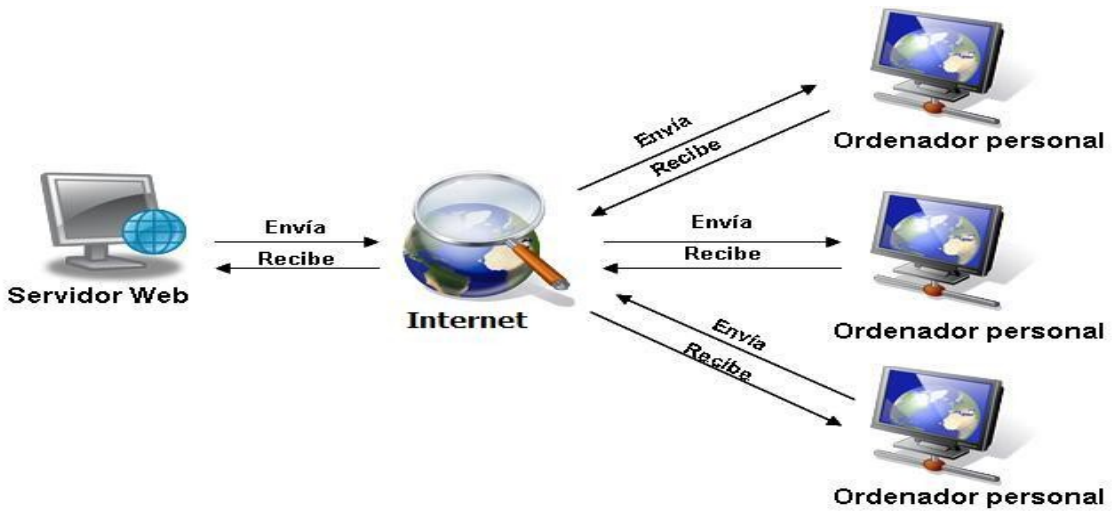
6.2. MARCO TEÓRICO

6.2.1. Aplicación Web

"Las aplicaciones web son aquellas que están ejecutadas en el entorno de un Cliente (navegador, explorador o visualizador) interpretadas por un Servidor (servidor web) realizando la comunicación mediante un protocolo de comunicación HTTP.". [13]

En consecuencia, la web es una aplicación cliente – servidor en donde el navegador web corresponde al cliente, el servidor web y el protocolo http que media como medio de comunicación. A continuación, en la figura 1, se presenta el esquema de funcionamiento y peticiones de equipos cliente a un servidor web los cuales se comunican a través del protocolo http de internet.

Figura 1. Aplicación Web - Cliente Servidor



Fuente: culturacion.com

[13] LUJÁN, Sergio. Programación de Aplicaciones Web: Historia, Principios Básicos y Clientes Web. Editorial Club Universitario. (2002). Pág. 48.

Las aplicaciones web se ejecutan entorno denominado navegador web, en donde la aplicación cuenta con el cliente, su servidor y protocolos claramente definidos. Es allí en donde un elemento de suma importancia como es el internet hace parte de este entorno y mediante el cual se estable la conexión y comunicación a través de sus protocolos.
En consecuencia, existen aplicaciones Multi-channel u Cross-channel: *"Multi-channel: El usuario puede trabajar con la misma aplicación a través de distintos canales (ordenador, PDA, teléfono móvil, web TV, etc.).*

Cross-channel: Los efectos producidos en una aplicación a través de un canal pueden ser percibidos por el usuario a través de otros canales.".[14]

6.2.2. Protocolos de seguridad

Los protocolos de seguridad son el conjunto de reglas establecidas que permiten el intercambio de información entre dispositivos electrónicos e informáticos forma no indeterminada. Por consiguiente los computadores que se encuentran conectados a una red hacen uso de protocolos para que esta manera exista el envío y recepción de la información que se desea trasmitir, protocolos como el TCP/IP establece reglas para que la información pueda ser transmitida a través de internet. Los protocolos de seguridad fueron desarrollados para un proyecto de investigación del Departamento de Defensa de los Estados Unidos, e integra un conjunto de servicios (que incluyen correo electrónico, la transferencia de archivos y la conexión remota) y que puede establecerse entre muchos ordenadores sobre una red local o en redes de un área más amplia.

"Los protocolos TCP/IP permanecieron bajo secreto militar hasta 1989. La World Wide Web llegó en 1991.

Los protocolos son, pues, una serie de reglas que utilizan los ordenadores para comunicarse entre sí. El protocolo utilizado determinará las acciones posibles entre dos ordenadores. Para hacer referencia a ellos en el acceso se escribe el protocolo en minúsculas seguido por "://". Por ejemplo http://www.hipertexto.info, ftp://ftp.hipertexto.info, etc.".[15]

[14] Universidad de Alicante. Que es una aplicación web [En Línea], 2006-2007. Disponible en: <https://rua.ua.es/dspace/bitstream/10045/4412/5/03c-AplicacionesWeb.pdf>.

Samuel Noriega establece en su artículo *"Los navegadores web para cargar las páginas de internet usan uno de dos protocolos: HTTP o HTTPS. El primero es el predeterminado y el segundo permite la navegación segura.*

HTTP es el método predeterminado y más usado en internet, utiliza el puerto 80. Para cargar las páginas se efectúan una serie de peticiones y respuestas entre el navegador y el servidor en la red. Los navegadores modernos en la barra de direcciones omiten el protocolo (http://) ya que se supone es el predeterminado, por lo solo vemos el nombre de dominio y a continuación la ruta a la página.

HTTPS es el segundo de los protocolos y el menos utilizado. Usa el puerto 443. Permite realizar una conexión segura o sea de esa forma toda la información que viaja por internet hacia dicho sitio o viceversa, es encriptada y nadie la puede interceptar. Es usado en bancos, tiendas online y todos los sitios donde se realice cualquier tipo de operación financiera, pero también en sitios o servicios donde es necesario autentificarse con un nombre de usuario y una contraseña. HTTPS utiliza un cifrado basado en SSL (capa de conexión segura) o TLS (seguridad de la capa de transporte), dos protocolos que proporcionan comunicaciones seguras por una red.

Los certificados SSL, certificados digitales o certificados de clave pública, son certificaciones que comúnmente utilizan los servicios de estos protocolos. Asimismo, los certificados son expedidos por empresas de seguridad informática reconocidas como "Autoridades de certificación" sobre el estado de un sitio web, cuando este usa sus servicios. En esos casos estas empresas escanean constantemente el contenido de dicho sitio en busca de malware u otro contenido malicioso, lo protegen y lo validan. Es por ello que si se quiere dotar de seguridad a una página, sin dudas se debe optar por instalar un certificado SSL.".[16]

6.2.3. Ataques, riesgos y amenazas sobre las páginas web

- **Espionaje de usuario a usuario**

[15] LAMARCA LAPUENTE, María Jesús. Hipertexto: El nuevo concepto de documento en la cultura de la imagen [En Línea], diciembre 2013. Disponible en: <http://www.hipertexto.info/documentos/internet_tegn.htm>.

[16] NORIEGA, Samuel. Protocolos de Seguridad Básicos ¿Qué tan seguro es tu sitio web? [En Línea], 2015. Disponible en: <https://www.certsuperior.com/Blog/protocolos-de-seguridad-sitio-web-seguro>.

Las amenazas como el espionaje no siempre se generan desde sitios o lugares externos. Los mismos clientes o empleados al interior pueden realizar espionaje al tráfico y paquetes de datos en la red para observar la información de otros usuarios, por consiguiente, es de suma importancia tener en cuenta que esta situación se puede presentar a nivel empresarial tanto interno como externo y se debe controlar.

- **Sesiones de cuentas de secuestro**

En la actualidad una gran cantidad de herramientas tienen como propósito realizar el secuestro de sesión para así mismo tener acceso a la cuenta y tomar total control sin la necesidad de ingresar contraseñas.

- **Puntos de acceso falso**

Los puntos de acceso que pueden detectar los dispositivos o computadores y que a su vez no tienen contraseña entre otros denominado acceso abierto, se catalogan como no seguros, ya que pueden generar problemas o pérdida de la información de los equipos.

- **Malware en Internet**

Los Malwares son un software malicioso y los cuales se pueden encontrar al momento de navegar una página web, a su vez puede asociarse con virus como gusanos o troyanos e infectar a los equipos asociados a la red, causando el borrado de datos, perdida de información y captura de contraseñas, emails etc.

- **Access Point Spoofing**

Los ataques Access Point Spoofing tienen como propósito que la víctima se conecte a una red errónea (diferente) y al momento de establecer la conexión con esta red errónea se captura la información, al finalizar dicho proceso se reestablece la conexión al punto real siendo este un ataque inadvertido.

- **ARP Poisoning**

Es un ataque que afecta directamente el protocolo ARP, situando en medio de la conexión de red un invasor de tal manera que la comunicación o envió de paquetes de un punto a otro tenga que pasar en medio del sujeto y así captura o altera los paquetes de información.

- **MAC Spoofing**

Consiste en suplantar la dirección MAC de un cliente autorizado, esto ocurre por los permisos que existen para cambiar las MAC.

- **Denial of Service (DoS)**

  - Tiene como propósito saturar la red a través de peticiones, logrando que el servicio se vuelva indisponible para los clientes. En redes como las inalámbricas la manera de saturar es mediante peticiones de segregación.

  - Otro objetivo del Denial of Service consiste en colapsar totalmente la navegación o que esta sea lenta, es decir denegar el servicio, para lo cual se establecen tres categorías de denegación:

    - Inundación de conexiones: A través de sus peticiones de reenvió de paquetes perdidos establece cientos de conexiones hasta colapsar el servicio.

    - Inundación de ancho de banda: Mediante las peticiones distribuidas las personas con finalidades malintencionadas envían una gran cantidad paquetes, lo que impide el paso de los paquetes que contienen la información correcta o valiosa.

    - Ataque de vulnerabilidad: Este ataque se centra en que la persona envía mensajes construidos con el propósito específico de provocar fallos.

- **Sniffing o Sniffers**

Los sniffing o sniffers interceptan el tráfico en una red de cómputo, este ataque funciona únicamente cuando el atacante y la víctima se encuentran dentro de la misma red y cuando estas son inseguras, abiertas y públicas.

- **Spoofing**

Es un ataque que busca la manera de suplantar la identidad de un usuario o personas con propósitos y fines delictivos.

Entre los ataques más reconocidos a los servidores web, se encuentra:

- Inyección SQL: Este ataque tiene como propósito realizar modificaciones a de las consultas SQL de un servidor web, para proceder con consultas con fines.

- LFI (Local File Inclusion): Este ataque se enfoca en que un servidor ejecute un script que está almacenado en el mismo.

- RFI (Remote File Inclusion): En relación a este tipo ataque, tiene como propósito realizar la misma acción que el LFI, a diferencia que este se ejecuta en una máquina remota.

- XSS (Cross site scripting): Su propósito es tomar un servidor web y vulnerar su seguridad para proceder a la ejecución de un script malicioso en el navegador del cliente.

6.2.4. Ataques a servidores web

Entre los ataques más reconocidos a los servidores web, tenemos:

- Inyección SQL: Este ataque consiste en modificar las consultas SQL de un servidor web, para poder realizar consultas maliciosas.

- LFI (Local File Inclusion): Este ataque hace que un servidor ejecute un script que está alojado en el mismo servidor.

- RFI (Remote File Inclusion): Este consiste en hacer que un servidor ejecute un scrip que está alojado en una máquina remota.

- XSS (Cross site scripting): Este consiste en engañar al servidor web para que ejecute un script malicioso en el navegador del cliente que visita una página determinada.

6.2.5. Tips de seguridad para sitios web

Teniendo en cuenta que los sitios web emplean contraseñas y que a su vez requieren de información personal se hace necesario que estos sitios web se encuentren protegidos para que ningún ente externo tenga acceso y haga uso de esta información.

Es por este motivo que Marcos Velázquez establece en el artículo denominado Tips de seguridad para tu sitio web, cómo implementar la seguridad en las aplicaciones web por medio de la actualización constante, contraseñas seguras, hospedaje web, cambios de configuración por defecto del CMS y la implementación del protocolo SSL[17]. De igual manera concluye que *"La seguridad de un sitio web es primordial. Vendas productos o no, la información que manejes es confidencial y no debe ser expuesta por algún externo. Aplica estos tips a tu sitio web para aumentar la seguridad y recuerda estar prevenido ante cualquier ciberamenaza."*.[18]

6.2.6. Cuáles son los riesgos y ataques de seguridad en aplicaciones web

El artículo realizado por noticiasseguridad.com permite entender que acorde a las auditorías realizadas por consultores a los sitios web es posible clasificar los riesgos a los que están expuesto estos sitios. De igual manera, resalta que esta clasificación de riesgos de seguridad web es de suma importancia, en donde los desarrolladores de aplicaciones deben tener total conocimiento y claridad del tema. Por tanto, es importante que Profesionales de TI aprendan sobre riesgos informáticos, ataques a nivel aplicación, auditoría de sitio web, seguridad etc., en

[17] Toyoutome. "Tips de seguridad para tu sitio web" [En Línea], octubre. 2015. Disponible en: <http://toyoutome.es/blog/tips-de-seguridad-para-tu-sitio-web/37521>.

[18] Toyoutome. "Tips de seguridad para tu sitio web" [En Línea], octubre. 2015. Disponible en: <http://toyoutome.es/blog/tips-de-seguridad-para-tu-sitio-web/37521>.

consecuencia es necesario que los profesionales en sus empresas tomen cursos de seguridad web adquieran conocimientos de metodologías de revisión de seguridad independientes, se establezcan guías de programación segura, se apliquen las normas internacionales, se realice pruebas de seguridad web constantes utilizando metodologías de explotación y ataques a nivel aplicación.

Finalmente, el artículo menciona los ataques más frecuentes a las aplicaciones web:

- Fuerza bruta: Es un ataque cuyo propósito es tratar de averiguar una contraseña utilizando la cantidad necesaria de combinaciones posibles.

- Autenticación incompleta y débil validación: Se presenta cuando un atacante o hacker ingresa fácilmente a una aplicación sin necesidad de realizar la autenticación completa.

- Autorización insuficiente: Este ataque obedece al acceso que tiene un usuario a la administración del sistema o aplicación sin ningún tipo de restricción.

- Secuestro de sesión: Este tipo de ataque se presenta cuando se forza un ID de sesión de usuario a un valor explícito o el atacante deduce o adivina la sesión.

- Cross-site scripting: Se presenta en el momento en que un usuario se encuentra logueado en una página web y el atacante ejecuta un comando o script con el cual puede llegar a obtener y modificar datos sensibles.

- Desbordamiento de buffer: En este caso el atacante ejecuta un ataque a nivel de sistema operativo para exceder el tamaño de memoria del buffer y así afectar el flujo de una aplicación con código malicioso.

- Inyección de código SQL: A través de instrucciones en leguaje SQL, el atacante puede tener control total de la base de datos o en su defecto obtener, alterar y eliminar información.

- Indexación de directorio: Mediante comandos de DOS el atacante puede acceder a los directorios del servidor en forma de HTML, tomar control y provocar fugas de información.

- Path traversal: Se presenta cuando el atacante detecta y accede a los ficheros y/o directorios root, los cuales contienen ejecutables que hacen parte fundamental o básica del funcionamiento de las aplicaciones.
- Denegación de servicio: Este ataque tiene como propósito detener o degradar los servicios o recursos de espacio en disco, CPU, memoria, conexiones [19].

6.3. MARCO CONCEPTUAL

A continuación se describe de manera general a información y conceptos utilizados para el proceso de la metodología.

6.3.1. Seguridad informática

Es aquella que se encarga de la protección de toda la infraestructura computacional y de la información contenida en la misma. Por tanto en la seguridad informática existen una serie de estándares y reglas para que durante el procesamiento de datos y su almacenamiento se garantice la confidencialidad, integridad y disponibilidad.

Se enfoca a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento para garantizar la confidencialidad, integridad y disponibilidad. La seguridad informática se basa principalmente en conocer el peligro, clasificarlo y después protegerse de estos, es decir de los daños e impactos que pueda causar obre los datos. Para proteger la información, primero es necesario conocer todos sobre los tipos de ataques y de qué manera invaden la información, ya sea para destruirla o clonarla, incluso publicarse sin autorización en la red, de esta manera se puede proteger una red que sea vulnerable.

La seguridad informática no se trata solo de ejecutar procesos que eviten otros de vulnerabilidad mayor, sino también está basada en el estudio del flujo de la información, el concepto más exacto es conocido como Investigación.

[19] Noticias de Seguridad Informática. "¿Cuáles son los riesgos y ataques de seguridad en aplicaciones web?" [En Línea], marzo 2016. Disponible en: <http://noticiasseguridad.com/importantes/cuales-son-los-riesgos-y-ataques-de-seguridad-en-aplicaciones-web/>.

Generalmente lo que se hace en este campo es restringir los accesos a la información con más importancia dentro de cualquier entidad.

En la seguridad informática se manejan elementos que son importantes para su aplicación, esto se logra a través de una jerarquía que debe cumplirse de la siguiente manera:

- **Disponibilidad:** Si se habla de disponibilidad se refiere directamente a la posibilidad de tener acceso a servicios o información digital por los usuarios cuando estos se requieran, es decir manipular y recuperar la información siempre que se considere necesario.

- **Confidencialidad:** La confidencialidad de la información es aplicada a los usuarios que estrictamente tengan acceso a esta y a otros que no puedan tenerlo, por estrictas reglas de seguridad, de la misma manera se refiere a la manipulación de información única por usuario que contiene datos personales o delicados para una entidad empresarial.

- **Integridad:** La integridad de datos, es la manipulación adecuada que reciben los documentos o la misma información digital, garantizando que la modificación de un documento original no se haga y se creen nuevas versiones que preserven el original.

6.3.2. Seguridad de la información

Es aquella que tiene un fin en común y el cual obedece a proteger la información, esto mediante medidas de protección para mantener la total confidencialidad, integridad y disponibilidad de los datos ante los riesgos.

- Define una Política de Seguridad.

- Identifica de riesgos.

- Elaboración de Controles.

- Define métricas e indicadores de la eficiencia de los controles.

- Establece un Plan de Tratamiento de Riesgos.

6.3.3. El hosting y la seguridad de su sitio web

"La gestión de las actualizaciones diarias necesarias para mantener el sitio web seguro, demanda un equipo administrativo altamente calificado. Una empresa de gestión de sitio web de terceros ofrece tanto alojamiento gestionado como seguridad, pero la seguridad del sitio depende en gran medida del proveedor.".[20]

El articulo nos permite entrar en materia de con respecto a que las empresas hoy en día deben estar altamente calificadas y actualizadas con respecto a la seguridad informática teniendo en cuenta la gran cantidad de vulnerabilidades y ataques que presentan los sitios web hoy en día.

Es por lo anterior que las empresas deben contar con plataformas seguras, hosting seguro y estar atento a las actualizaciones de cada uno de los elementos que hagan parte de la plataforma donde se encuentre establecido el sitio web. En el caso de que la empresa no cuente con los recursos económicos necesarios, el artículo sugiere alojar la información en sitios que ofrecen empresas como Synapsis, Level 3 y IFX es el caso de Colombia para proteger la información.

Sin embargo, por encima de lo anterior Anderson indica que *"Uno de los beneficios de tener un sitio web gestionado es que la empresa cuenta con un equipo dedicado de personal de operaciones de desarrollo que se han especializado en el servidor de seguridad". La seguridad y la accesibilidad son dos de las preocupaciones más importantes con los sitios web."*.[21] Por tanto, en mejor que la empresa gestione por su propia cuenta la seguridad de las aplicaciones web estando estas aún más monitoreadas y seguras.

---

[20] Segured. "El hosting y la seguridad de su sitio web" [En Línea], 2017. Disponible en: <http://segured.com/el-hosting-y-la-seguridad-de-su-sitio-web/>.

[21] Segured. "El hosting y la seguridad de su sitio web" [En Línea], 2017. Disponible en: <http://segured.com/el-hosting-y-la-seguridad-de-su-sitio-web/>.

6.3.4. Prueba de penetración como mecanismo de protección

Las pruebas de penetración conocidas también como “pen testing”, tienen una serie de actividades sobre la infraestructura sobre la cual se desea realizar el test, ya que este proceso requiere identificar las vulnerabilidades que podrían materializarse más adelante, además de los daños que podrían causar en la infraestructura tecnológica, ya sea por el atacante o por la penetración. El proceso de hacking ético a realizar, tiene como propósito identificar qué incidentes de seguridad pueden ocurrir antes de que estos se materialicen y, posteriormente, corregir o mejorar el sistema, para así garantizar la confidencialidad, integridad y disponibilidad de la información.

En las pruebas de penetración, los métodos y herramientas que se utilizan simulan lo que habitualmente utilizaría un delincuente informático para tener acceso a la información de la empresa u organización, pero con la diferencia y característica que se actúa bajo un entorno totalmente controlado, en donde realmente la finalidad es encontrar las fallas de seguridad que puedan existir para su posterior corrección.

Existen tres tipos de pruebas de Penetración Caja Negra, Caja Blanca y Caja Gris y a su vez está compuesta por fases las cuales se presentan a continuación:

- Fase de reconocimiento: Es la fase en la cual se determina el objetivo y obtiene toda la información posible que permita realizar un ataque exitoso, esto mediante buscadores, herramientas de análisis de DNS, whois y demás herramientas para obtener información de nuestra víctima.

  Aquí, se recopila toda la información que se utilizara en las próximas fases. Ninguna información es irrelevante para estos casos todo es necesario y tiene el mismo grado de importancia.

- Fase de escaneo: En esta fase se utiliza la información obtenida en la fase de reconocimiento con el objetivo de detectar posibles vectores de ataque para realizar el escaneo de puertos y servicios. En consecuencia, se lleva a cabo un escaneo extendido a las vulnerabilidades que permitan definir los vectores de ataque, encontrar fallas que puedan afectar la red, definir eventos, conocerlos y finalmente tener claro como eliminarlos definitivamente. Para realizar estas acciones se pueden utilizar herramientas como SYN stealth can, FIN scan, XMAS tree scan, NULL scan, FIN scan.

- Fase de enumeración: En la tercera fase de una prueba de penetración se deben obtener datos referentes a los usuarios, nombres de equipos, servicios de red, contraseñas válidas de su entorno servicios y aplicaciones accesibles. Lo anterior, permitirá explotar la vulnerabilidad y obtener el control.

- Fase de acceso: Durante esta fase se tiene en cuenta todas y cada una de las vulnerabilidades detectadas para acceder a los sistemas de información y obtener las evidencias e información necesaria. Allí, se accede al sistema y se logra a partir de la extracción de todos los puntos donde se detectan las vulnerabilidades que fueron utilizadas por el auditor del sistema. El proceso de acceso puede hacerse mediante herramientas automáticas como metasploit.
  Sin embargo, si el propósito es llegar más allá, se podrá tomar el control de la máquina, encontrar el método para escalar los permisos necesarios y generar actividades o ejecuciones de acciones deseadas sobre la máquina intervenida.

- Fase de mantenimiento de acceso: Al lograrse el acceso al sistema se debe preservar el sistema comprometido a disposición de quien lo ha atacado de mediante la instalación y ejecución de programas maliciosos que permitan realizar los respectivos ataques.

6.3.5. Herramientas para desarrollo de un test de penetración

- **Kali Linux**

Una distribución de GNU/Linux sin dudarlo una de las más completas si hablamos de la capacidad y herramientas con las cuales cuenta para manejar el área de la seguridad de vulnerabilidad de datos. Esta distribución dedicada a la seguridad informática, para prevención de todo tipo de ataques más no para causar infracciones ilegales es una de las herramientas más recomendadas que posee su vez otras potentes herramientas.

.

- **Aplicaciones de Kali Linux**

  Kali Linux cuenta con aplicaciones para recopilación de información, análisis de vulnerabilidad, aplicaciones, evaluación de bases de datos, ataques de contraseñas, ataques wireless ingeniería reversa, herramientas de

explotación, aplicaciones para husmear o envenenar, herramienta de forensia entre otros.

A continuación la relación y detalle de herramientas de Kali que se pueden ejecutar a sitios web:

- **Apache-users**: Herramienta que procede a Enumera nombres de usuarios de los diferentes aplicaciones o sistemas que utilice Apache con UserDir.

- **Burpsuite**: Esta herramienta que cuenta funcionalidades de scanner, araña, repetidor, decodificación, comparación, extensión y secuenciador tanto de forma manual como automática y es utilizada en auditorias de seguridad de aplicaciones web.

- **Cutycapt:** A través de vectoriales y de mapa de bits, svg, pdf, ps, png, jpeg, tiff, gif, y bmp. Permite la captura de la representación webKit de una página web.

- **Dirbuster:** Esta herramienta de fuerza bruta se encuentra diseñada para ataques a directorios y nombres de archivos de las aplicaciones web.

- **Vega:** Plataforma que permite probar la seguridad aplicaciones web a través de su scanner y código abierto es posible encontrar y validar ataques como Inyección SQL y Cross-Site Scripting (XSS).

- **Webscarab**: Permite depurar problemas o vulnerabilidades de la aplicaciones web mediante la exposición del funcionamiento de la misma.

- **Webslayer:** Herramienta de fuerza bruta de aplicaciones web, con el fin de encontrar directorios, servlets, scripts y archivos que no se encuentren correctamente vinculados. Esto mediante su generador de carga y analizador de resultados.

- **Zaproxy**: Herramienta de OWASP de pruebas de penetración para encontrar vulnerabilidades de los sitios web.

- **Webmitm:** A través de la redirección de snnifer olfatea y trasmite de forma transparente el trafico HTTP / HTTPS, cuyo propósito es capturar inicios de sesión de correos web encriptados con SSL y envíos de formularios.

- **Webspy:** Se ejecuta desde un equipo local con el propósito de que un cliente remita URLs olfateadas a un navegador Netscape para su localización en tiempo real.

- **Burpsuite:** Esta plataforma permite realizar pruebas de seguridad de aplicaciones web a través del mapeo y análisis de ataque a aplicaciones web para encontrar y explotar vulnerabilidades.

- **Dnsspoof:** Herramienta útil para interceptar las consultas DNS de los clientes de la LAN a las aplicaciones web tomando controles de acceso basados en nombre del host.

- **Driftnet:** Esta herramienta tiene como propósito de capturar imágenes que busca en línea el usuario que es atacado.

- **Ferret**: Esta utilidad tiene como fin robar o explotar sesiones, tomando cookies HTTP mágicas para autenticar un usuario desde un equipo remoto.

- **Mitmproxy**: Consola de interface gráfica que permite inspeccionar los flujos de tráfico de las aplicaciones web en tiempo real y a su vez editarlos.

- **Urlsnarf**: Genera los enlaces de sitios web a los que la víctima se encuentra ingresando mediante las olfateadas del trafico HTTTP.

- **Nikto**: Scanner de código abierto que permite realizar pruebas a servidores web en el menor tiempo posible, validando objetos obsoletos, proxy, textos planos, codificación ID, autenticación host etc.

- **Burp Scanner**: Al igual que BurpSuite esta herramienta se encuentra diseñada para pruebas de seguridad de aplicaciones web.

- **BeEF**: Herramienta de explotación de navegadores web, que permite evaluar la postura de seguridad mediante ataques con vectores los cuales identifican los perímetros de red, sistema del cliente y capacidad de explotación del navegador web.

- **Sqlmap**: Herramienta que permite llevar a cabo ataques de inyección de código sql automáticamente. Por consiguiente, tiene como objetivo detectar y aprovechar las vulnerabilidades de inyección SQL de las aplicaciones web.

- **NESSUS**

Escáner de vulnerabilidades con arquitectura cliente-servidor y la cual en la actualidad es una de las herramientas más actualizadas del mercado. Su funcionabilidad se enfoca en la actualización de plugins que permiten la detección de las debilidades existentes de las aplicaciones.

- **Acunetix**

Escáner de vulnerabilidades diseñado específicamente para auditar e identificar las vulnerabilidades de los sistemas web. Posee un poderoso generador de reportes con una interface completamente entendible para el usuario.

- **Metasploit Framework**

Es una herramienta framework de explotación de vulnerabilidades que genera ataques mediante la ejecución de exploits contra las víctimas consiguiendo ejecutar scripts de cobro o ejecutar comandos arbitrarios, controlar dispositivos, pantallas, navegar, cargar y descargar archivos además de la evasión ante las defensas de los antivirus. Esta herramienta es también de uso libre.

- **AppDetectivePro y DbProtect**

Herramientas que permiten realizar análisis a las bases de datos y detectar los errores de configuración que se posean, dificultades de identificación y control de acceso. De igual manera, informa sobre las configuraciones que pueden provocar fugas de información, ataques de denegación de servicio, modificaciones de información y uso no autorizado de accesos.

- **DVWA**

Es una aplicación para el entrenamiento de explotación de vulnerabilidades web y diseñada en PHP y MySQL. DVWA Posee funcionalidades como Command Execution que permite ejecutar comandos de consola desde la web, facilita ver, modificar y eliminar archivos y directorios de un servidor.

Otra funcionalidad que haces parte de DWVA es XSS (Cross-site scripting) que concede realizar la ejecución de código HTML o Javascript sobre un sitio web para cambiar totalmente la interfaz del mismo sitio.

Continuando con las funcionalidades de DVWA nos encontramos con RFI (Remote File Inclusion) funcionalidad que permite incluir archivos externos a un sitio web. De igual forma posee la aplicación SQL Injection que hace factible inyectar código SQL por medio de consultas para extraer datos e información de una base de datos.

Una herramienta que permite insertar código malicioso por medio de formularios es la Unrestricted File Upload. Así mismo, la funcionalidad Cross Site Request Forgery (CSRF) envía ataques una web (víctima) y que al momento de ingresar o abrirlas, sin darse cuenta un script hace una petición a un sitio en específico haciéndose pasar como ese usuario logueado y aplicando acciones.

Finalmente, otra funcionalidad es Brute Force envía combinaciones para loguearse como un usuario ya sea usando un diccionario con palabras habituales o generando palabras aleatoriamente.

- **Nmap / Zenmap**

Es un software de comunidad libre, el cual funciona como escáner de puertos en donde su principal función es identificar el sistema operativo, maquinas en red, puertos abiertos, servicios en ejecución y especificaciones de cada las máquinas

de las victimas mediante el envío de paquetes y la respuesta de los mismos. Fue desarrollado para el sistema Linux, sin embargo en la actualidad ya está dispuesto como multiplataforma.

6.3.6. Principios de seguridad propuestos por OWASP

Teniendo en cuenta la liberación de nuevas tecnologías con nuevas debilidades y defensas incorporadas OWASP establece un Top 10 para crear conciencia e identificación de riesgos críticos, estos a su vez son:

- A1 – Inyección: Contempla las diferentes fallas de inyección como lo son SQL, OS, y LDAP, las cuales se presentan cuando existe la presencia de datos no confiables que son enviados a un intérprete a través de comandos en donde el atacante trata de engañar al intérprete.

- A2 – Pérdida de Autenticación y Gestión de Sesiones: En la mayoría de situaciones la autenticación y gestión de sesiones son vulnerables ante los atacantes, permitiendo así capturar contraseñas, claves, tokens etc. Esto con el propósito de ingresar a las aplicaciones las credenciales de usuarios registrados en el sistema.

- A3 – Secuencia de Comandos en Sitos Cruzados (XSS): Los atacantes se encuentran en capacidad de ejecutar sentencias de comandos sobre los navegadores web con el propósito de capturar sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.

- A4 – Referencia Directa Insegura a Objetos: Los directorios, ficheros o bases de datos que son elementos internos, en algunas ocasiones no son protegidos con accesos o controles por parte de los desarrolladores de las aplicaciones, por tanto, los atacantes están al acecho de acceder a estas referencias para su manipulación.

- A5 – Configuración de Seguridad Incorrecta: La configuración de los diferentes servidores que componen los sistemas de información, deben estar definidas de forma lineal, para su mantenimiento y correcto funcionamiento, al igual, deben estar actualizados el software y librerías de

código de los que se compone cada uno. Esto evitara ataques directos a los servidores.

- A6 – Exposición de Datos Sensibles: En una gran mayoría las aplicaciones web no cuentan con seguridad a datos sensibles como los son el número de tarjetas crédito o débito y credenciales de autenticación. Por tanto, se requiere que las aplicaciones contemplen métodos de protección de cifrado de datos para evitar robos, fraudes y delitos.

- A7 – Ausencia de Control de Acceso a las Funciones: Las aplicaciones requieren de la validación del control de acceso en sus servidores. Ya que al no realizar esta actividad las solicitudes de acceso no se verifican, y los atacantes tendrán la capacidad de realizar peticiones sin ningún tipo de autorización hasta conseguir algún tipo de delito informático.

- A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF): Los atacantes están en la capacidad de forzar a los navegadores a través de peticiones HTTP legítimas, están son provenientes de las víctimas con sesión autenticada, lo que permite la falsificación y acceso a información sensible.

- A9 – Uso de Componentes con Vulnerabilidades Conocidas: Los componentes denominados librerías, los frameworks y otros módulos de software tienen privilegios de funcionamiento. Sin embargo, si el atacante vulnera alguno de estos elementos, se facilita el ingreso a intrusos exponiendo así la perdida de información.

- A10 – Redirecciones y reenvíos no validados: Las aplicaciones web constantemente poseen links que redirigen a otros sitios web que pueden tener información o estructura no confiable, por tanto, los usuarios se pueden convertir en victimas malware o phising.[22]

En consecuencia y relación a lo anterior Los principios son:

- Seguridad a profundidad: la seguridad debe estar en mecanismos por capas y no depender de una sola regla o mecanismo de seguridad.

[22] OWASP FOUNDATION, Metodología OWASP [En Línea], octubre 2011. Disponible en: <https://www.owasp.org/images/8/80/Guía_de_pruebas_de_OWASP_ver_3.0.pdf>.

- Modelo positivo de seguridad: en este modelo se define como lista blanca lo que está permitido y lo demás se rechaza para ser comparado con listas negras.

- Fallar seguro: se debe dar un manejo adecuado a los errores de ejecución para que estos no develen pistas sobre a conformación general del programa.

- Vaya con el mínimo privilegio: asignar la cantidad mínima de privilegios para que un usuario pueda realizar la acción definida.

- Evite la seguridad por oscuridad: el diseño y lógica de un control de seguridad debe estar hecho sobre principios probados y conocidos.

- Mantener la seguridad simple: Utilizar mecanismos verificables y confiables.

- Detectar intrusiones: revisar logs y tareas rutinarias para detectar anomalías.

- No confiar en la infraestructura: Las aplicaciones deben de tener mecanismos propios de defensa para no delegar actividades importantes sobre las máquinas.

- No confiar en los servicios: Los servicios por lo general son administrados por un tercero, no se tiene la certeza del trato en seguridad para este servicio.

- Establecer configuración predeterminada segura: se deben implementar mecanismos seguros por defecto sin delegar configuraciones de seguridad a los usuarios.

6.3.7. Mejorar la seguridad en los servicios Web.

- Cambiar la Configuración Predeterminada de la CMS para controlar comentarios, usuarios y la visibilidad de la información del usuario.

- Utilizar balanceadores de carga independiente y no hacerlo directamente desde el servidor para distribuir las peticiones de sesiones que se hacen hacia las aplicaciones, pues esto genera un procesamiento innecesario del servidor físico.

- El registro de eventos debe contener suficiente información para reconstruir confiablemente la cadena de eventos y rastrear de vuelta a los que llamaron funciones sin autentificación previa.

- Seguridad en la comunicación.

- Auditorias.

- Instalar SSL que encripta la comunicación entre el Punto A y el Punto B – el servidor web y el navegador.

- Actualizar los prefijos por defecto de las bases de datos para evitar la extracción de usuarios y contraseñas de acceso.

- Configurar los permisos CHMOD a las carpetas y archivo de la página web que se encuentren almacenados en el servidor.

- Los mensajes SOAP (Simple Object Access Protocol) que son enviados en la red deben ser entregados confiablemente y sin modificaciones.

- Realizar copias backups semanales que se almacenen en una NAS de almacenamiento y manejar versiones con base a los módulos que sean más utilizados. Si las aplicaciones tienen procesos transaccionales o de paso de información confidencial, se deben tener certificados de seguridad de sitio. El almacenamiento de estas copias de seguridad deben ser almacenadas en un lugar seguro y de custodia.

6.3.8. Medidas para reforzar la seguridad de las páginas web

"La seguridad debe ser uno de las principales preocupaciones para cualquier usuario tecnológico, especialmente para las que están presentes en Internet, que

no deben descuidar la seguridad de su página web. Y es que, todas las aplicaciones web pueden llegar a ser vulnerables a ciertos tipos de ataques, algo que los delincuentes saben y explotan en su propio beneficio. Para protegerse ante cualquier riesgo y reforzar cualquier web ante posibles amenazas, Arsys ofrece un decálogo de buenas prácticas muy fáciles de llevar a cabo.

1. *Alojar la web en un proveedor de hosting de confianza, que proporcione información sobre las medidas de seguridad que aplica, medidas entre las que es recomendable disponer de un Sistema de Detección y Prevención de Intrusos, así como distintas tecnologías de firewall, sistemas antivirus y antispam.*

2. *Establecer contraseñas robustas, no emplear la misma para varios servicios y cambiarlas periódicamente.*

3. *Fijar una política de perfiles para el acceso, escritura y modificación de directorios y archivos comunes, aplicando permisos lo más restrictivos posibles, tanto a las carpetas y ficheros como a los usuarios.*

4. *Al introducir los elementos de programación en la página web, establecer validaciones en todos los campos de datos, y evitar usar instrucciones SQL en las que concatenen cadenas aportadas por los propios usuarios.*

5. *Controlar la información que muestran los mensajes de errores, de cara al autodiagnóstico y evaluación de la robustez de la plataforma.*

6. *Mantener los sistemas actualizados a las últimas versiones que liberan los fabricantes de software, que no sólo incorporan nuevas funcionalidades, sino que también corrigen vulnerabilidades y agujeros de seguridad.*

7. *Emplear un certificado de seguridad SSL a la hora de gestionar datos de carácter personal, ya que garantiza que el intercambio de información entre un usuario y la página se establece de forma segura y cifrada, garantizando la confidencialidad de los datos.*

8. *Al trabajar con bases de datos es recomendable encriptar toda la información sensible, como logins de usuario, contraseñas y, por supuesto, los datos bancarios y de carácter personal.*

9. *Realizar periódicamente copias de seguridad de la página web y de las bases de datos.*

10. *Disponer de algún servicio de seguridad que permita comprobar de forma periódica si nuestra web tiene alguna vulnerabilidad o malware.".*[23]

6.4. MARCO LEGAL

6.4.1. Ley 1273 de 2009 delitos informáticos en Colombia

En la Ley 1273 de 2009, se establecieron nuevas penalizaciones relacionadas con delitos informáticos y la protección de información además de los datos, para lo cual, se identificaron una serie de conductas relacionadas con el manejo de los datos.[24]

De igual manera, la ley 1273 de 2009 tienen muy en cuenta aquellos atentados que se han sufrido las empresas frente a la confidencialidad, la integridad y la disponibilidad de los datos las conductas que resalta la ley son:

- Manipulación de software malicioso: ya sea desarrollar, adquirir, distribuir, ejecutar programas con efectos dañinos.

- Violación de datos personales: aquel que en beneficio propio o de un tercero obtenga información personal de bases de datos o archivos confidenciales.

- Suplantar sitios web o dominios con la finalidad de indebidamente obtener datos personales.

---

[23] GÓMEZ, Hilda. Medidas para reforzar la seguridad de las páginas web [En Línea], junio 2015. Disponible en: <http://cso.computerworld.es/ciberseguridad/medidas-para-reforzar-la-seguridad-de-las-paginas-web>.

[24] MINTIC. Ley Nº. 1273 [En Línea], enero 2009. Disponible en: <http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>.

- Acceso no autorizado a un sistema informático.

- Transferencia no autorizada de activos, quien valiéndose de artificios o manipulación logre realizar la transferencia de un activo perjudicando a un tercero o quien desarrolle o reproduzca software para realizar dicho delito.

- Efectuar daños informáticos como borrar, alterar, destruir información de un sistema.

- Obstaculizar una red o sistema de información.

- En otras circunstancias, también se consideran delitos mayores aquellos que afecten redes informáticas o de comunicaciones gubernamentales u oficiales, que hagan parte del sector bancario, nacional o internacional; que sean ejecutadas por un servidor público aprovechando el ejercicio de sus funciones y la confianza depositada, obteniendo beneficios propios o a terceros o con fines terroristas.

- Interceptar datos de un sistema.

- De la misma manera se encuentran aspectos con respecto a los atentados informáticos u otras infracciones como: Hurto por medios informáticos y por medio de la suplantación de usuarios autorizados en los sistemas de autenticación.

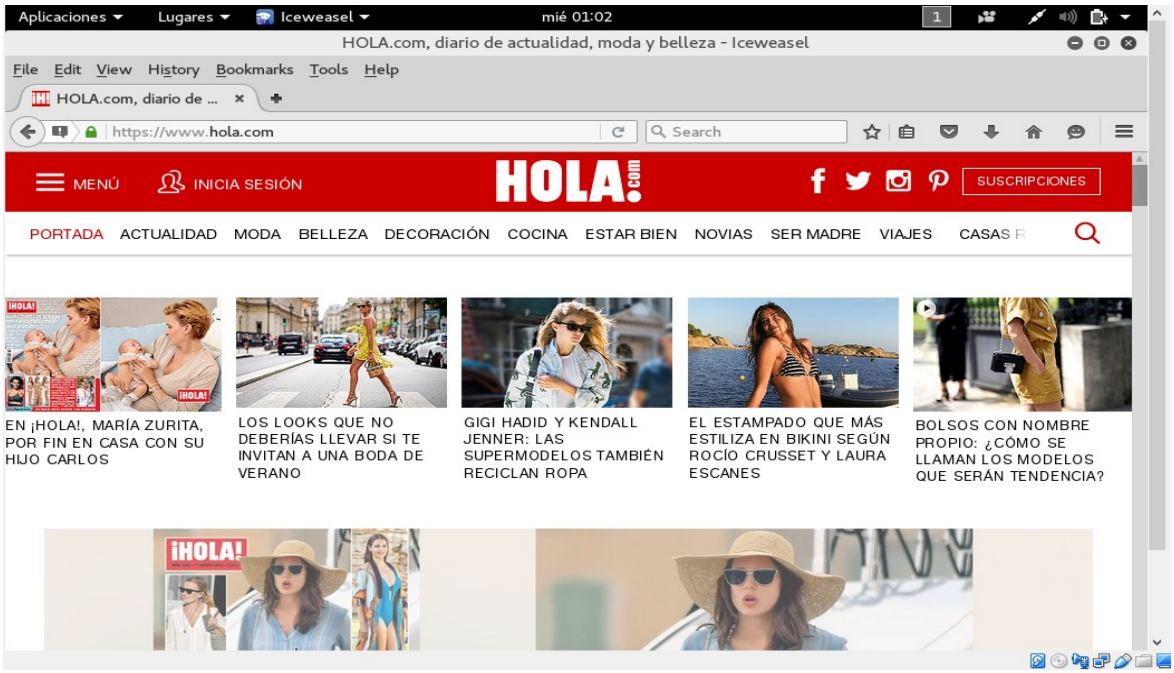
7. IDENTIFICACIÓN DE RIESGOS, AMENAZAS Y ATAQUES A SITIOS WEB

Con el propósito de evaluar algunas medidas de seguridad de una aplicación web de una organización, se presentan a continuación el desarrollo de una actividad de ataque y búsqueda de vulnerabilidades a las páginas web www.hola.com y www.bogota.gov.co.

- **www.hola.com**

A continuación se presenta en la figura 2 la página de internet www.hola.com.

Figura 2. Página web www.hola.com

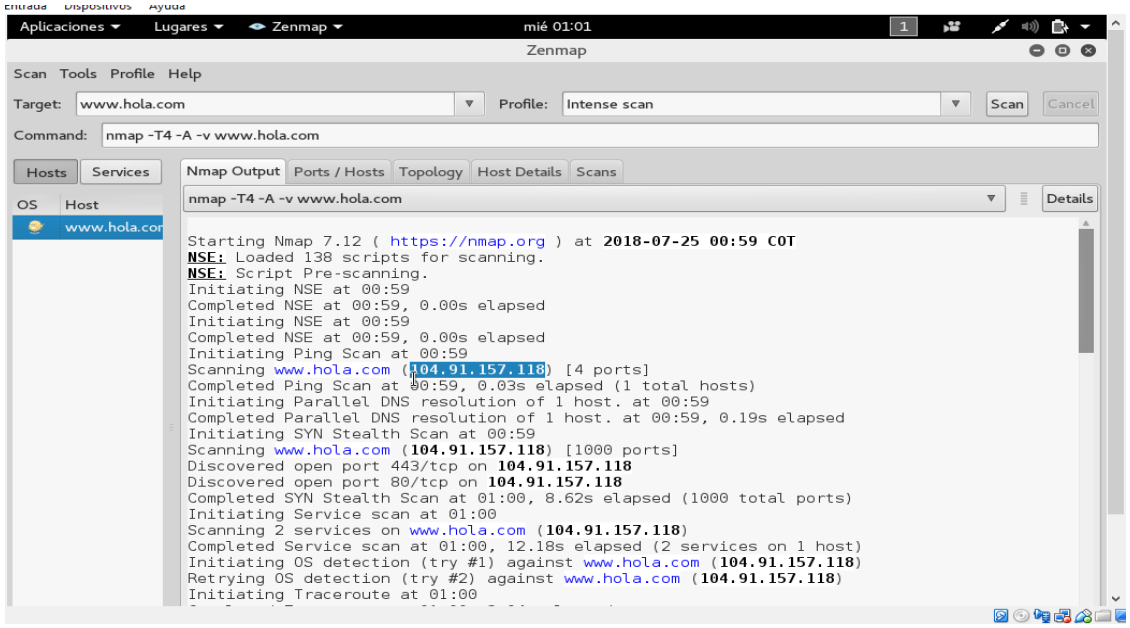


Fuente: www.hola.com

a). Usando la herramienta zenmap:

1. Se identificó con la herramienta zenmap que la página web www.hola.com tiene la IP 104.91.157.118, tal y como se evidencia en la figura 3:

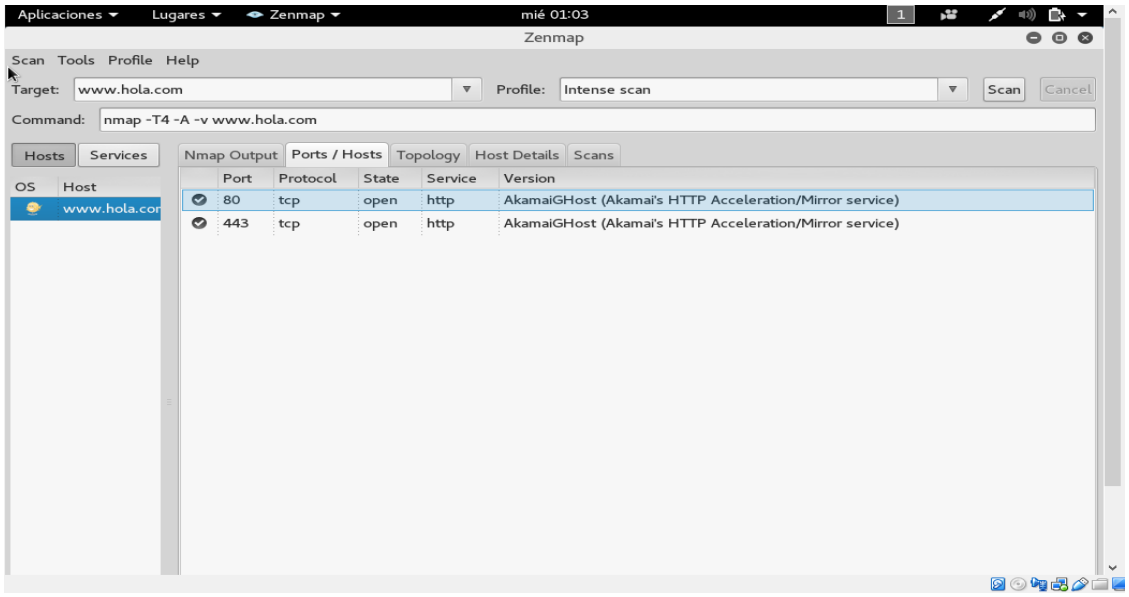
Figura 3. Identificación IP zenmap



Fuente: El autor

2. En la figura 4 se observa que se identificaron los puertos 80 y 443 en estado abierto con sus respectivos servicios:

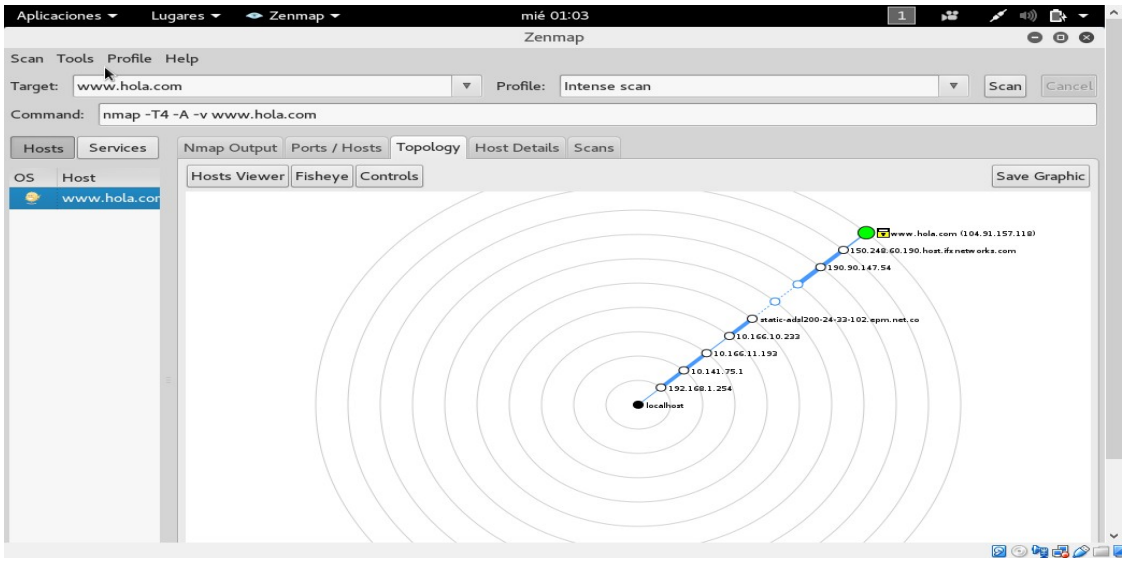
Figura 4. Identificación zenmap puertos abiertos



Fuente: El autor

3. Por otra parte, podemos visualizar en la figura 5 la topología en donde identificamos el camino desde nuestro equipo hasta la página web.

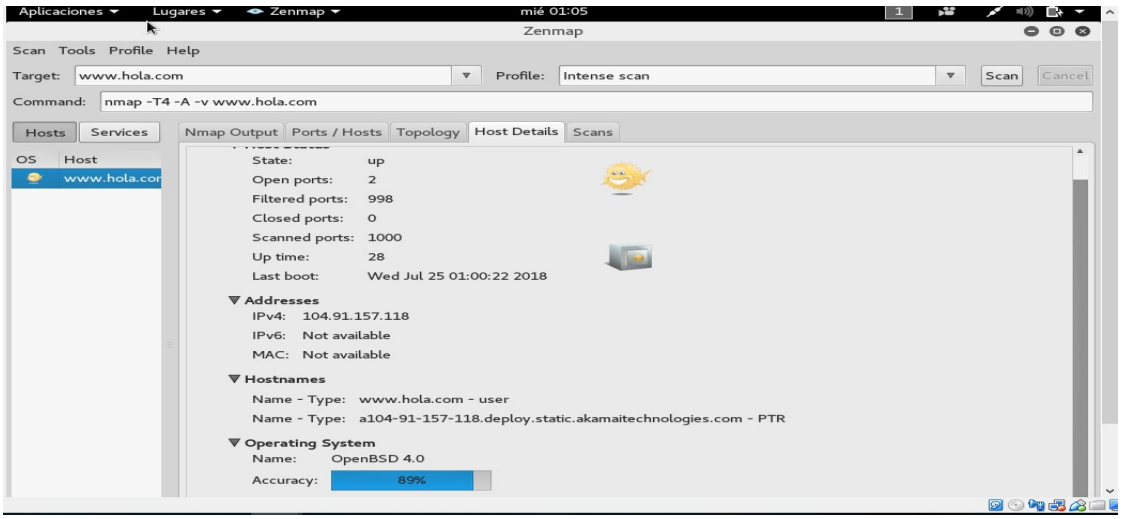
Figura 5. Identificación zenmap topología de red



Fuente: El autor

4. Además observamos información adicional de nuestro host, gracias a zenmap como se detalla en la figura 6 Identificación zenmap Detalles Host.

Figura 6. Identificación zenmap Detalles Host

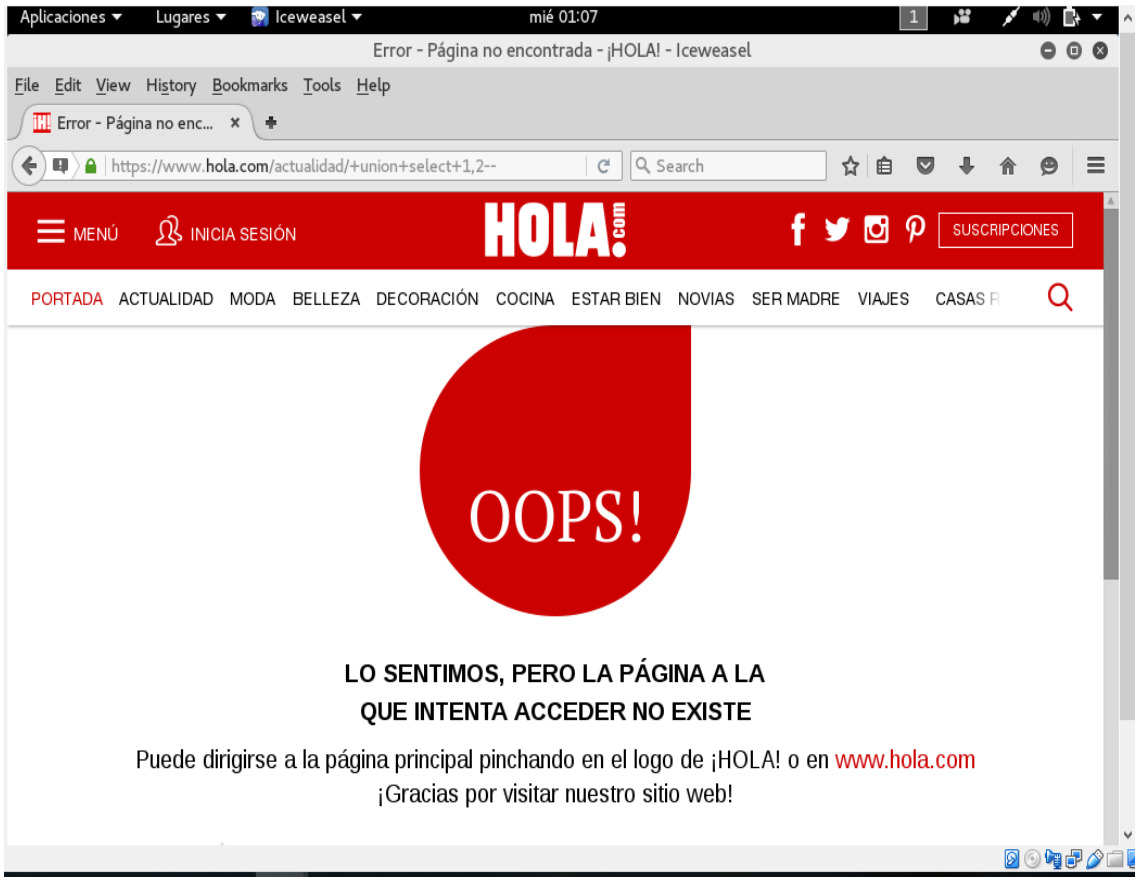


Fuente: El autor

b). Inyección sql:

1. Nos dirigimos a la páginawww.hola.com, seleccionamos alguno de los menús y adicionamos a la dirección el siguiente comando +union+select+1,2--. Al realizar este ataque la página indica que *"la página a la que se intenta acceder no existe",* tema que se observa en la figura 7 Ataque sql injection.

Figura 7. Ataque sql injection

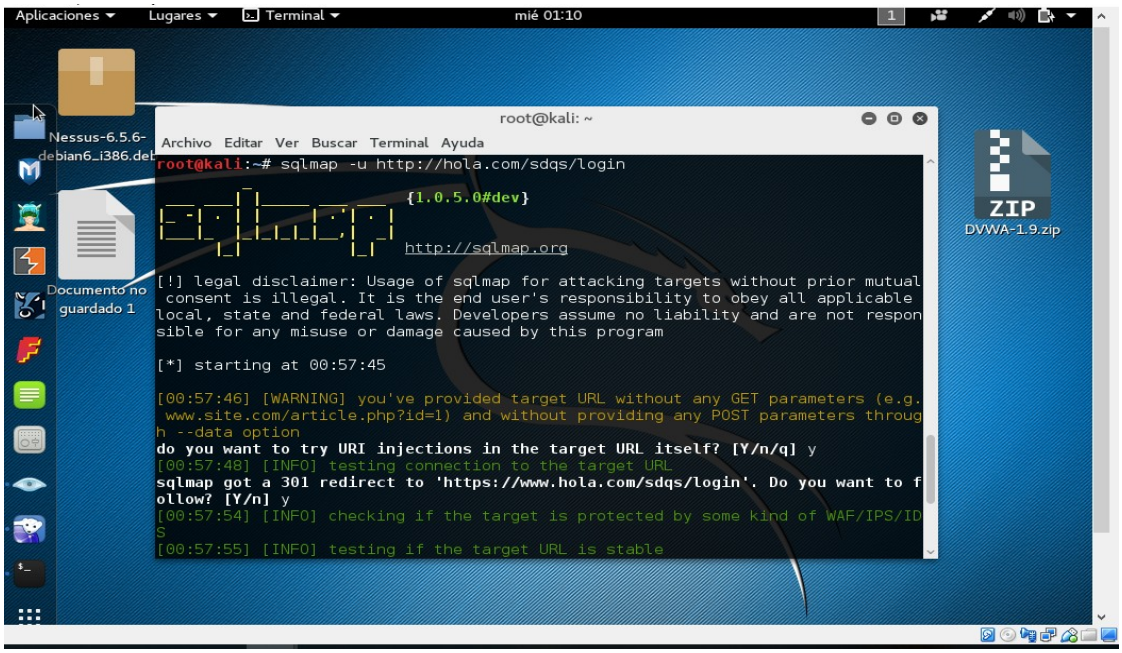


Fuente: El autor

c). Slqmap

1. En la figura 8 se da conocer que al ingresar a la página http://pwnable.kr/ opción acceder, copiamos la dirección y seguidamente después de ejecutar sqlmap digitamos el comando *sqlmap -u http://pwnable.kr/sdqs/login.*

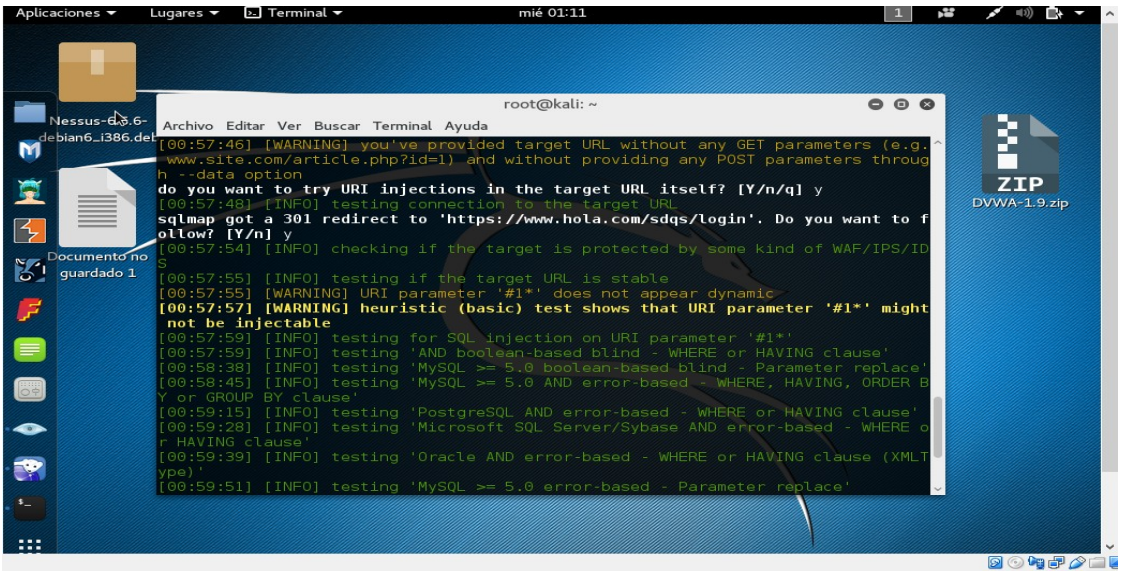
Figura 8. Ataque sqlmap



Fuente: El autor

2. Por otra parte, sqlmap arroja información del inicio del ataque como se observa en la figura 9:

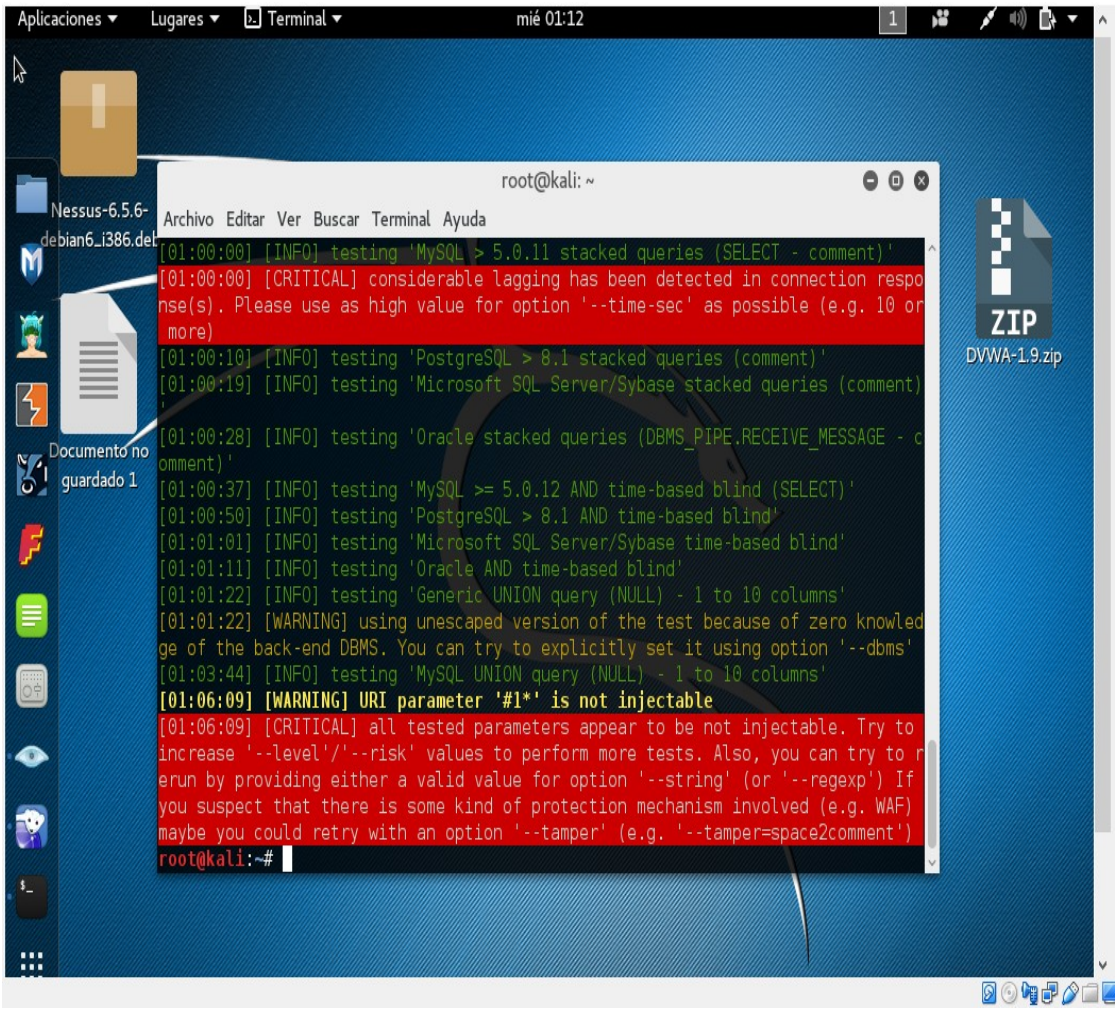
Figura 9. Ataque sqlmap 2



Fuente: El autor

3. Ahora nos indica que el parámetro p_p_id no es inyectable por tanto la seguridad de la página no acepta este tipo de ataque, tal y como se observa en la figura 10 Ataque sqlmap parámetro p_p_id.

Figura 10. Ataque sqlmap parámetro p_p_id

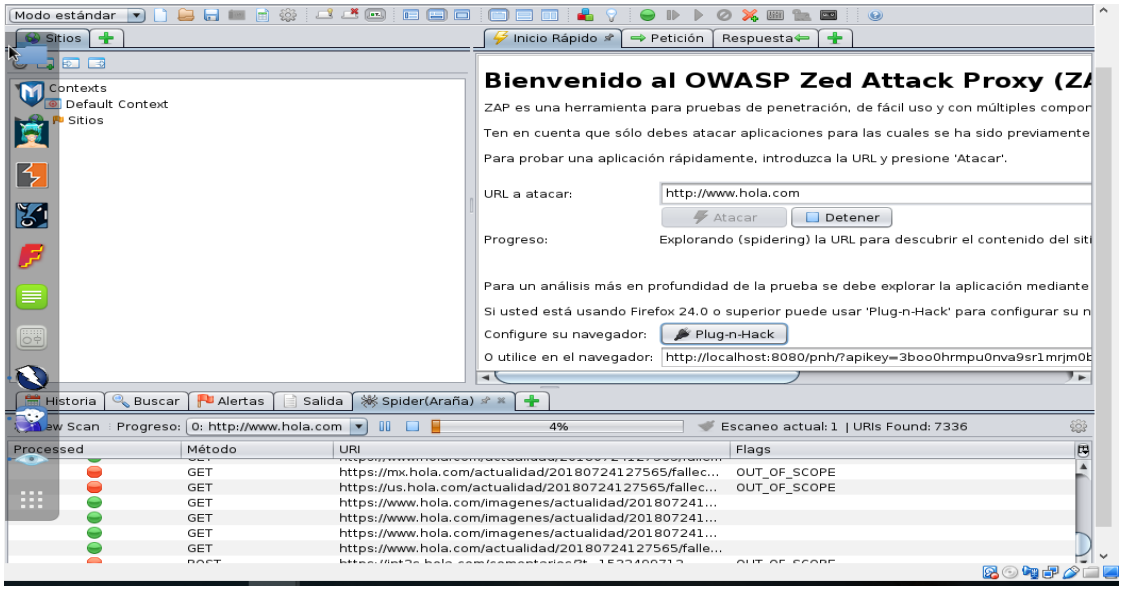


Fuente: El autor

d). Ahora bien utilizaremos otra herramienta denominada OWASP para identificar otras vulnerabilidades.

1. Al abrir esta aplicación diligenciamos la página www.hola.com y seleccionamos atacar, para realizar el análisis como se evidencia en la figura 11.

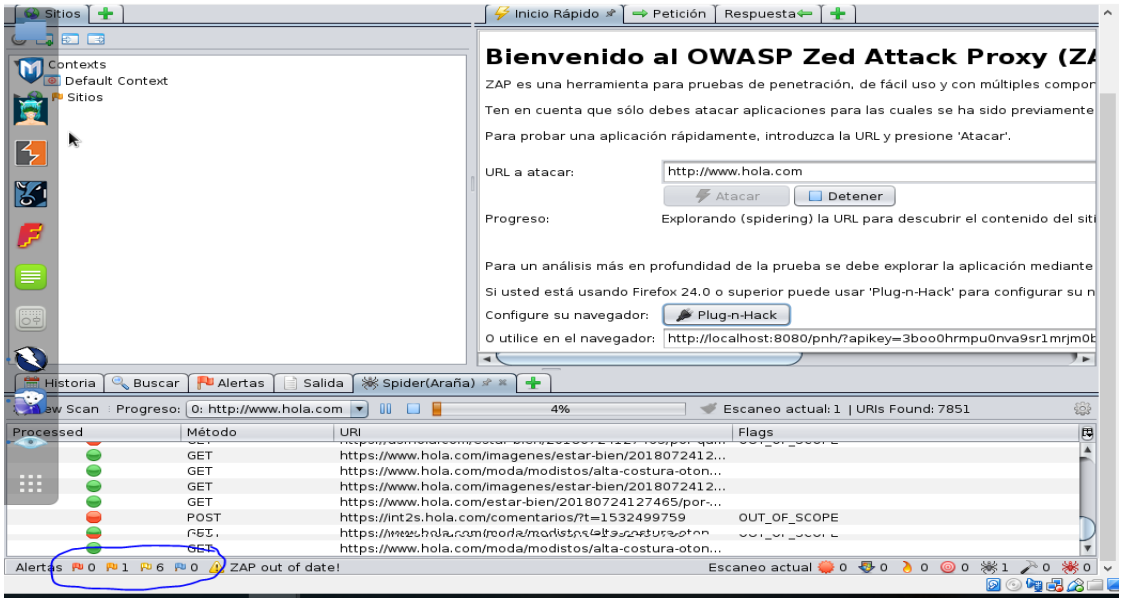
Figura 11. Análisis OWASP



Fuente: El autor

2. Como se muestra en la figura 12, OWASP realiza un escaneo total a la página para los cual nos empieza a mostrar alertas de diferente tipo de criticidad en este caso 7.

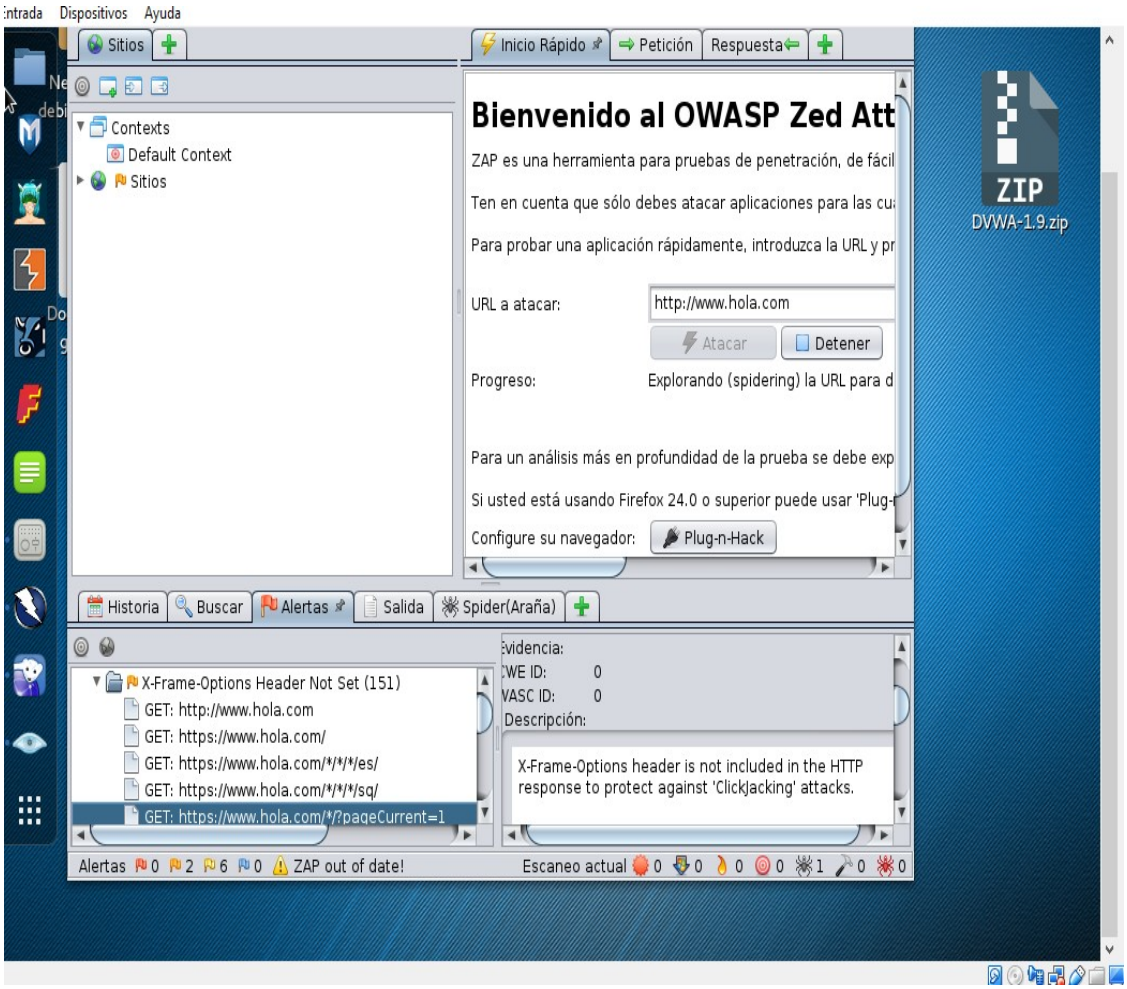
Figura 12. Alertas Análisis OWASP



Fuente: El autor

3. Nos dirigimos a la pestaña alertas como se muestra en la figura 13 denominada Detalle Alertas OWASP y seleccionamos en este caso la de criticidad media X-Frame-Options Header Not Set. Desplegamos el listado, seleccionamos alguna de las urls y evidenciamos que nos informa que X-Frame-Options no está incluido en la respuesta para HTTP para protegerse de ataques clicjaking. Por tanto es una vulnerabilidad que se debe corregir.

Figura 13. Detalle Alertas OWASP

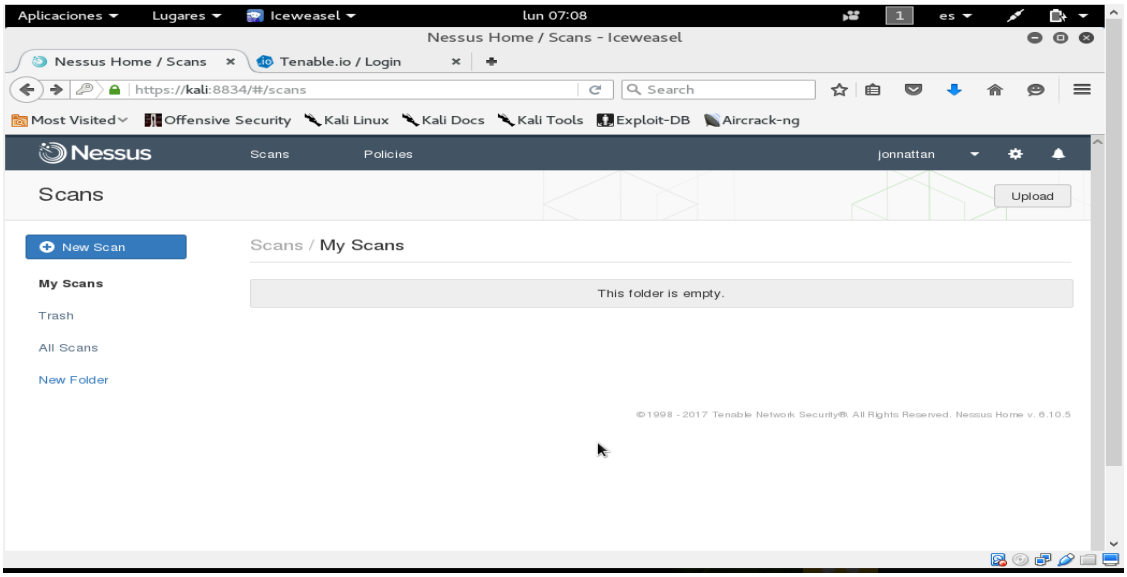


Fuente: El autor

e). Finalmente utilizamos la herramienta Nessus

1. Seleccionamos New Scan que se evidencia en la pantalla principal de Nessus como se observa en la figura 14.

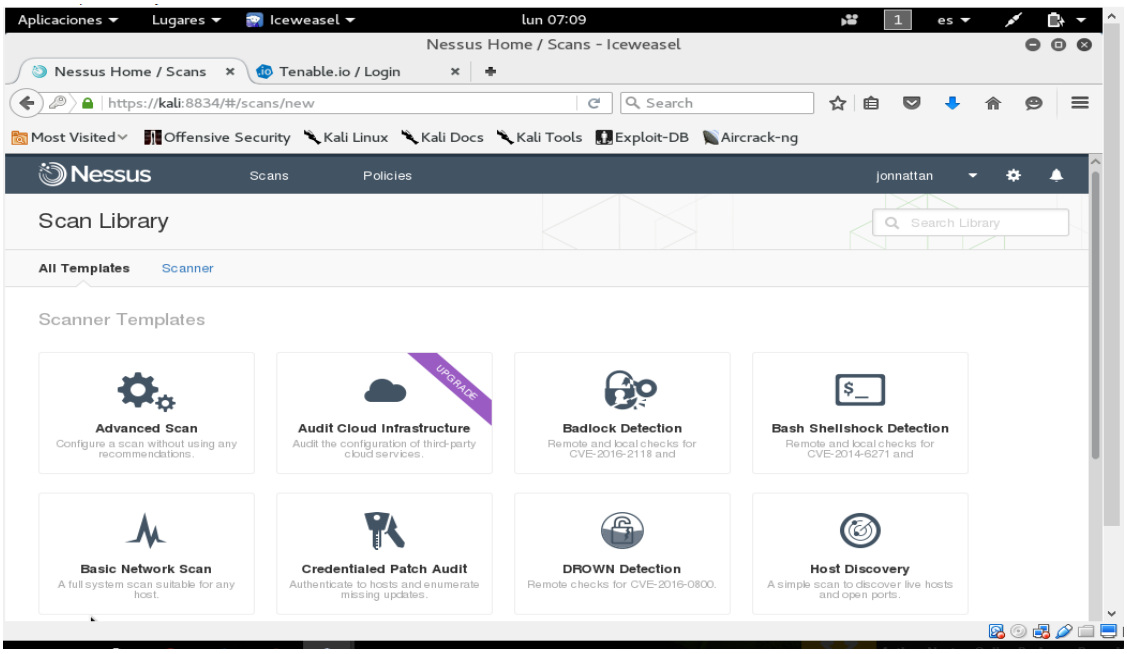
Figura 14. Nessus



Fuente: El autor

2. Seguidamente se selecciona Advanced Scan en Nessus para inciar el escaneo avanzado. Ver figura 15.

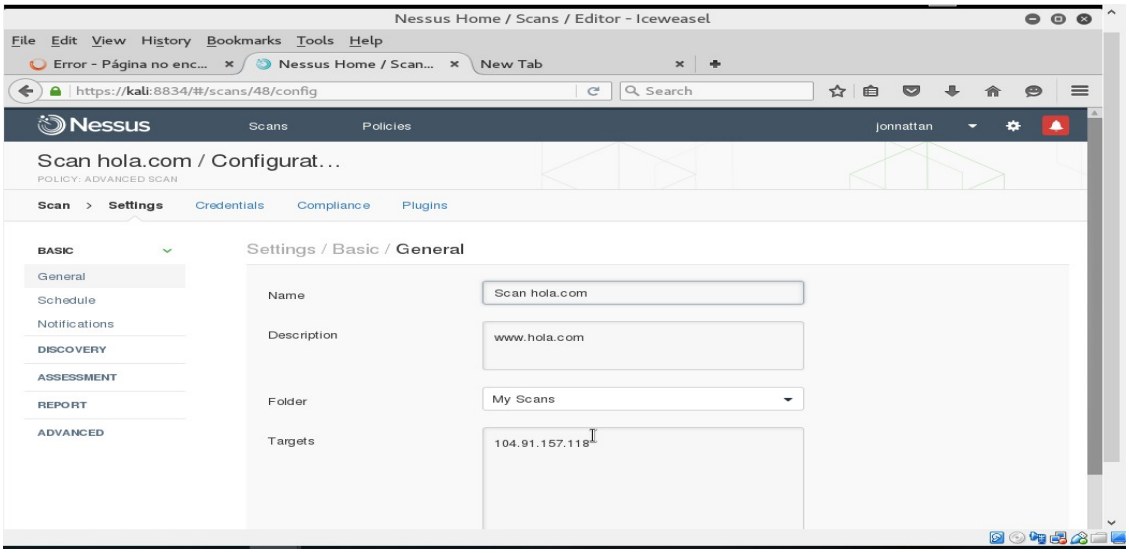
Figura 15. Nessus escaneo avanzado



Fuente: El autor

3. En la figura 16, se observa el momento en que diligenciamos nombre, descripción y en targets la IP 104.91.157.118 la cual deseamos escanear. Posteriormente clic en save.

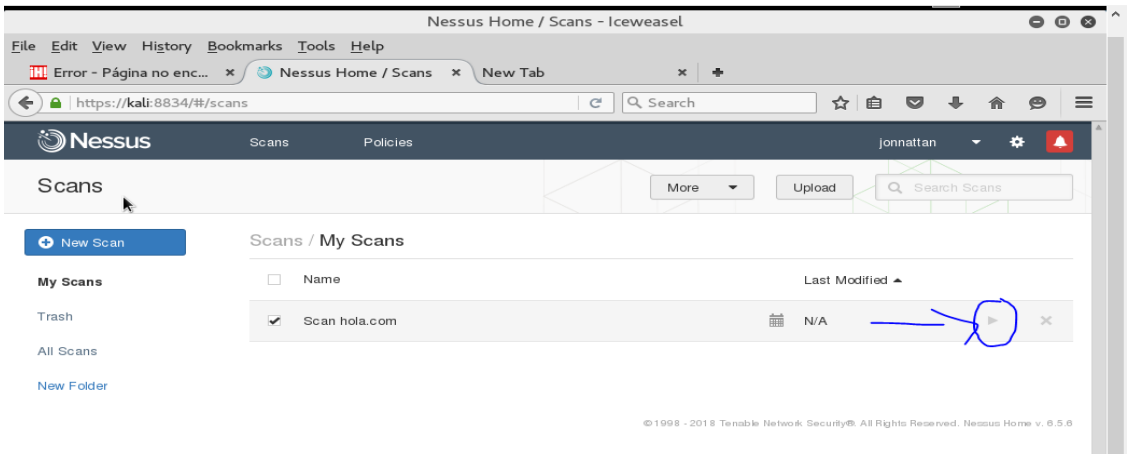
Figura 16. Nessus configuración escaneo avanzado



Fuente: El autor

4. Ahora bien, damos clic en el icono de ejecución del scan creado “scan hola.com” y esperamos que finalice el respectivo escáner. Tema que se da a conocer en la figura 17 denominada Nessus ejecución escaneo avanzado.

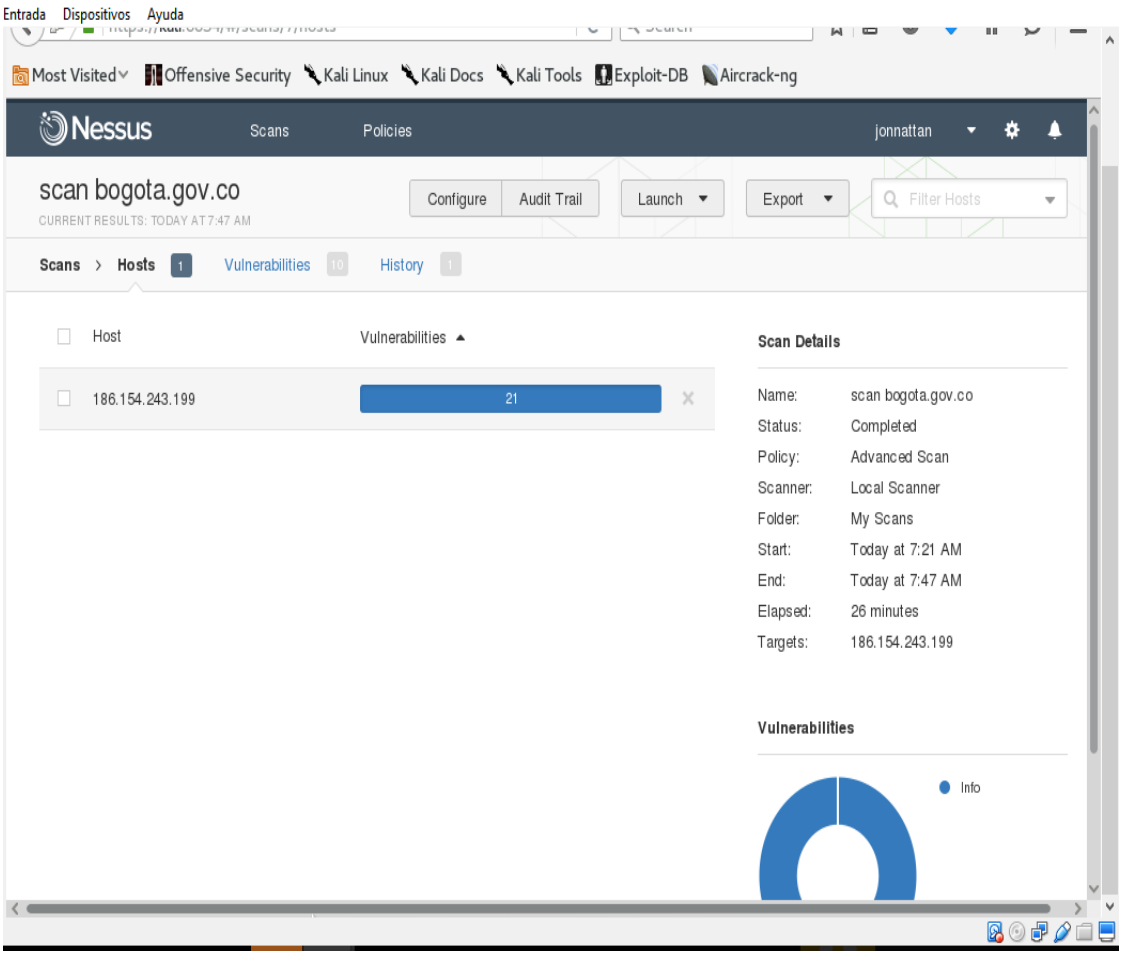
Figura 17. Nessus ejecución escaneo avanzado



Fuente: El autor

5. Cuando aparezca el chulo, este indica que el escáner ha finalizado, por lo tanto damos clic en “scan bogota.gov.co” para visualizar los respectivos resultados. Allí encontramos que la dirección 104.91.157.118 posee 21 vulnerabilidades informativas. Para ver el detalle de las mismas, damos clic en la dirección 104.91.157.118. Ver figura 18.

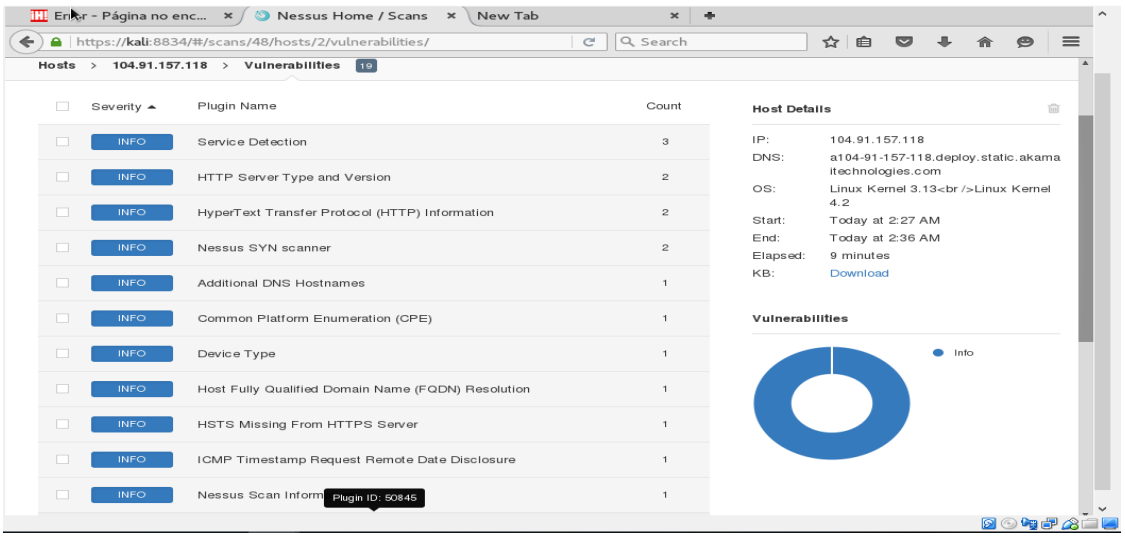
Figura 18. Nessus finalización escaneo avanzado



Fuente: El autor

6. Como resultado, se evidencio en la figura 19 que las vulnerabilidades informativas obedecen a Service Detection, HTTP Server Type and Version, HyperText Transfer Protocol (HTTP) Information, Nessus SYN Scanner, Additional DNS Hostnames, Device Type, Host Fully Qualified Domanin Name, OS identification, OpenSSL Detection etc.

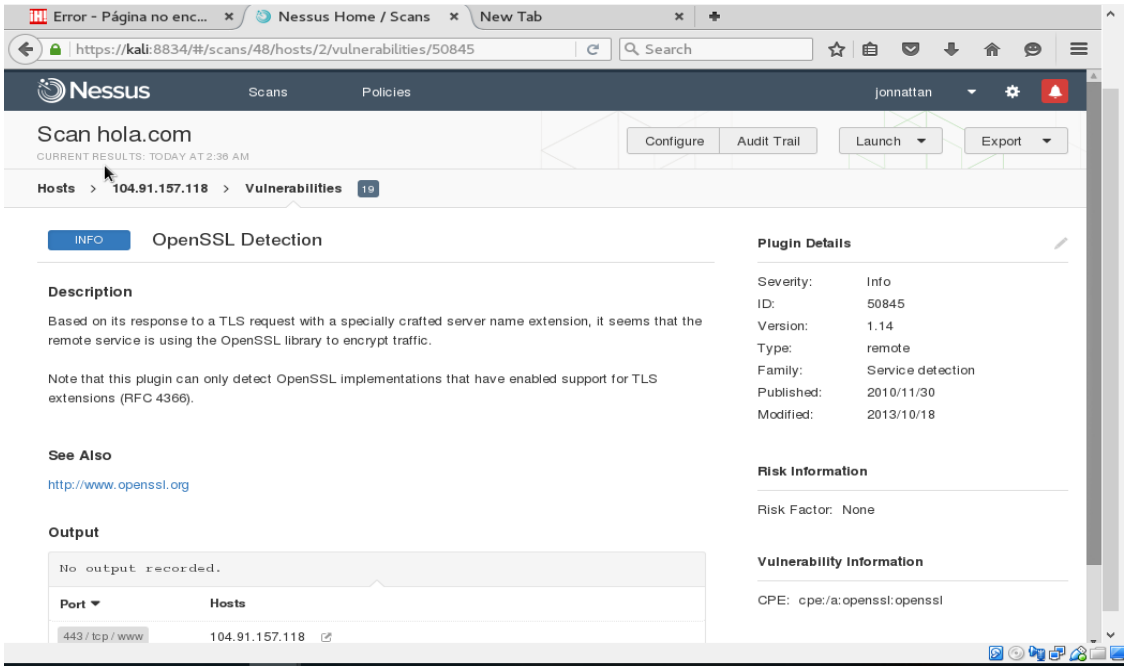
Figura 19. Nessus Vulnerabilidades



Fuente: El autor

7. Finalmente, se muestra en la figura 20 que al dar clic en INFO podemos encontrar el detalle de la vulnerabilidad y la solución de la misma.

Figura 20. Nessus Detalle Vulnerabilidades



Fuente: El autor
Descripción:

Dependiendo de su respuesta a una solicitud de TLS con una extensión de nombre de servidor especialmente diseñada, parece que el servicio remoto esta utilización una biblioteca de OpenSSL para encriptar el tráfico.

Tenga en cuenta que este complemento solo puede detectar implementaciones de OpenSSL que tengan habilitada la compatibilidad con extensiones TLS (RFC 4366).

Solución:

Si desea probarlos, vuelva a escanear utilizando la sintaxis de host especial como por ejemplo www.example.com [192.0.32.10].

8. Resultados

Después de realizar las respectivas pruebas y ataques de penetración se evidencio que la página www.hola.com presenta vulnerabilidades como:

a) Los puertos 80 y 443 se encuentran abiertos, lo cual hace que esta se encuentre en riesgo de ataques.

b) Se visualizó la topología de red que se utiliza para lograr la conexión a la página web, identificando otras IP las cuales se podrían atacar o vulnerar.

c) Que X-Frame-Options no está incluido en la respuesta para HTTP para protegerse de ataques clicjaking.

d) Se evidencio las vulnerabilidades informativas como Service Detection, HTTP Server Type and Version, HyperText Transfer Protocol (HTTP) Information, Nessus SYN Scanner, Additional DNS Hostnames, Device Type, Host Fully Qualified Domanin Name, OS identification, OpenSSL Detection.

- **www.bogota.gov.co**

A continuación se presenta en la figura 21 la página de internet www.bogota.gov.co.

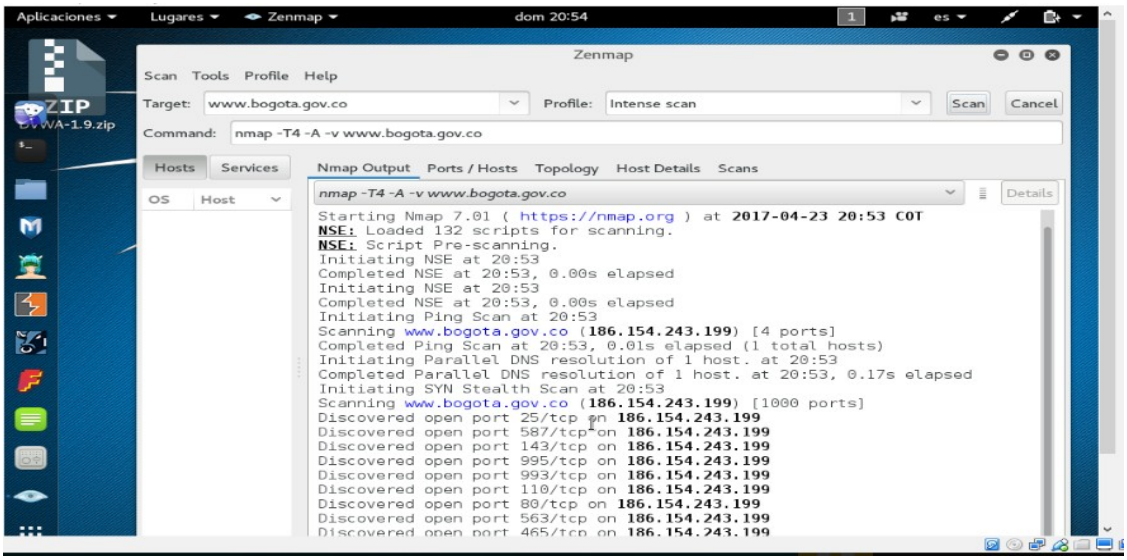
Figura 21. Página web www.bogota.gov.co

Fuente: www.bogota.gov.co

a). Usando la herramienta zenmap:

1. Se identificó con la herramienta zenmap que la página web www.bogota.gov.co tiene la IP 186.154.243.199, tal y como se evidencia en la figura 22:

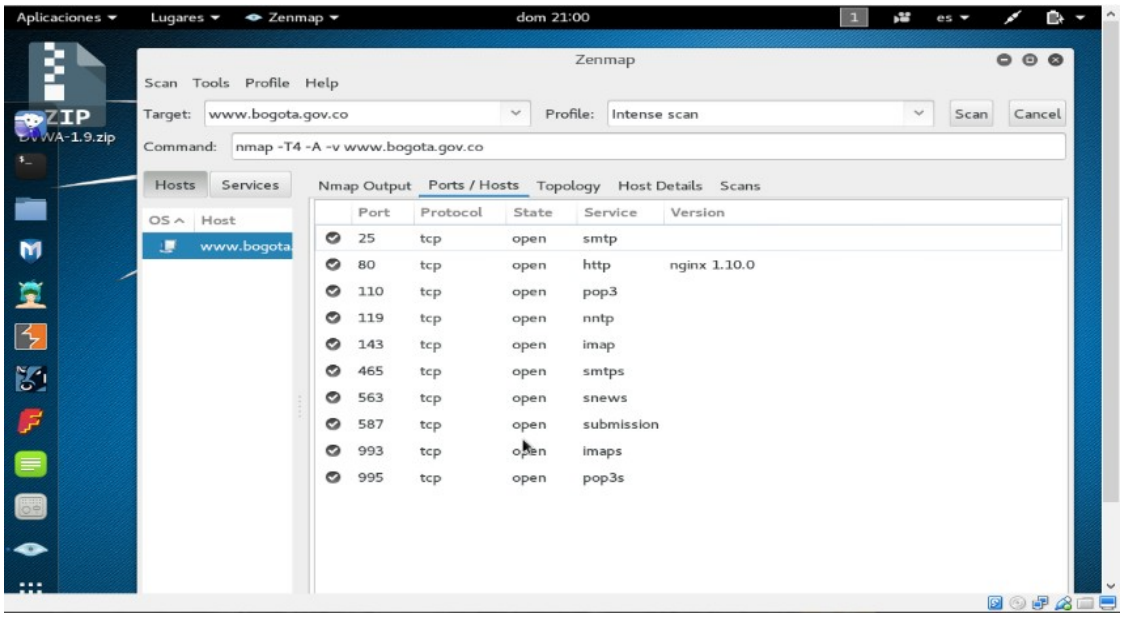
Figura 22. Identificación IP zenmap



Fuente: El autor

2. En la figura 23 se observa que se identificaron los puertos 993, 995, 143, 25, 80, 110, 587, 465, 563 y 119, y su estado:

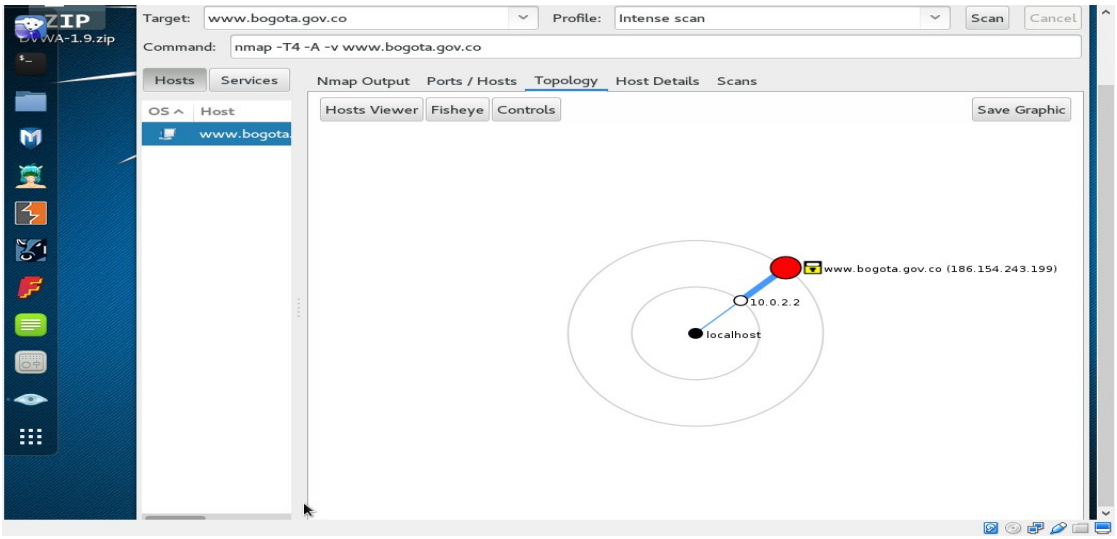
Figura 23. Identificación zenmap puertos abiertos



Fuente: El autor

3. Por otra parte, Por otra parte, podemos visualizar en la figura 24 la topología en donde identificamos el camino desde nuestro equipo hasta la página web.

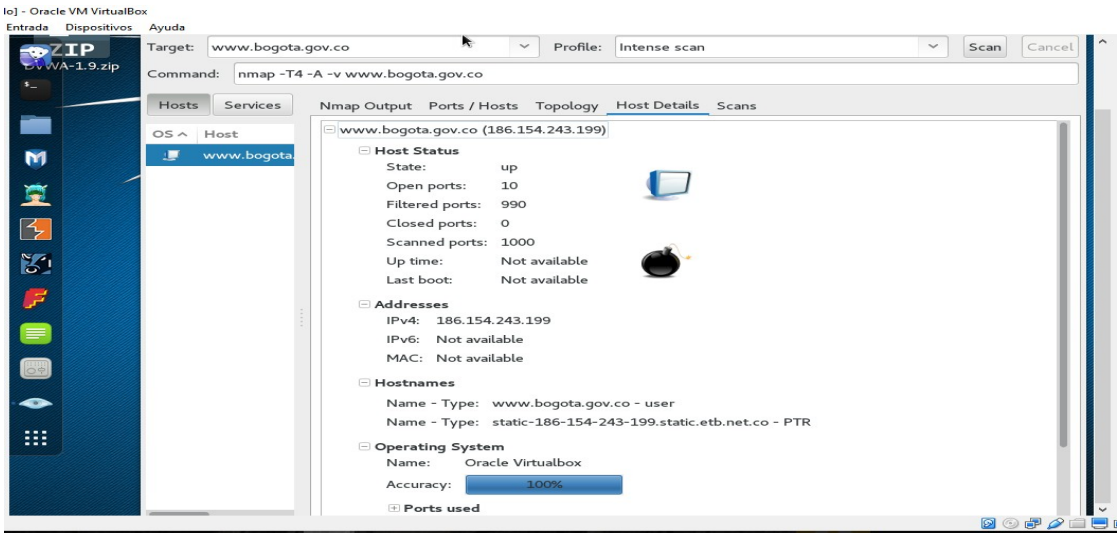
Figura 24. Identificación zenmap topología de red



Fuente: El autor

4. Además observamos información adicional de nuestro host, gracias a zenmap como se detalla en la figura 25 Identificación zenmap Detalles Host.

Figura 25. Identificación zenmap Detalles Host

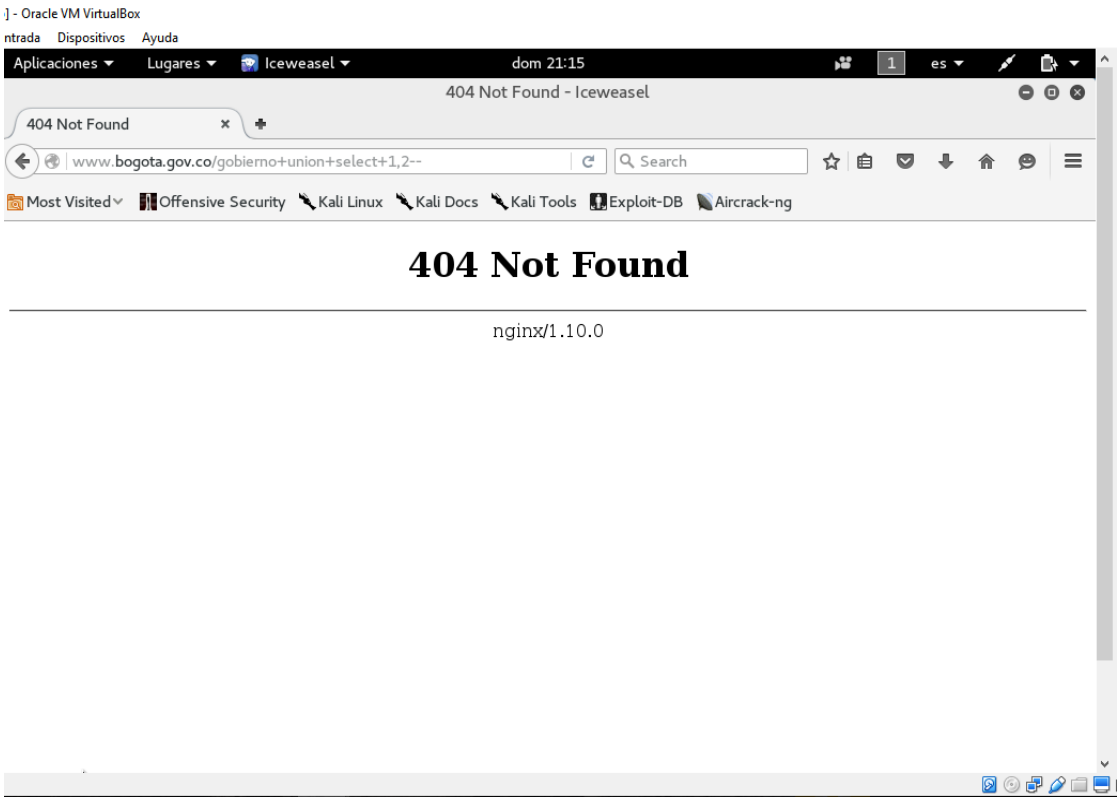


Fuente: El autor

b). Inyección sql:

1. Nos dirigimos a la página www.bogota.gov.co, seleccionamos alguno de los menús y adicionamos a la dirección el siguiente comando +union+select+1,2--. Al realizar este ataque la página nos indica que *"Los sistemas de seguridad del Ministerio de Minas han bloqueado esta petición, ya que se detecta como una posible amenaza"* tema observado en la figura 26 Ataque sql injection.

Figura 26. Ataque sql injection

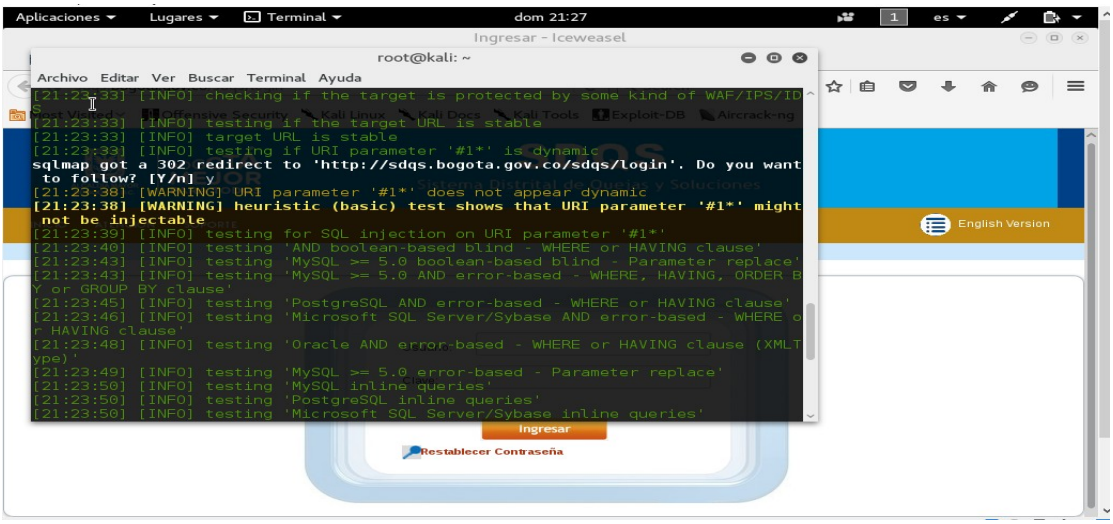


Fuente: El autor

c). Slqmap

1. En la figura 27 se da conocer que al ingresar a la página www.bogota.gov.co opción acceder, copiamos la dirección y seguidamente después de ejecutar sqlmap digitamos el comando *sqlmap -u http://sdqs.bogota.gov.co/sdqs/login.*

Figura 27. Ataque sqlmap



Fuente: El autor

2. Ahora nos indica que el parámetro p_p_id no es inyectable por tanto la seguridad de la página no acepta este tipo de ataque, tal y como se observa en la figura 28 Ataque sqlmap parámetro p_p_id

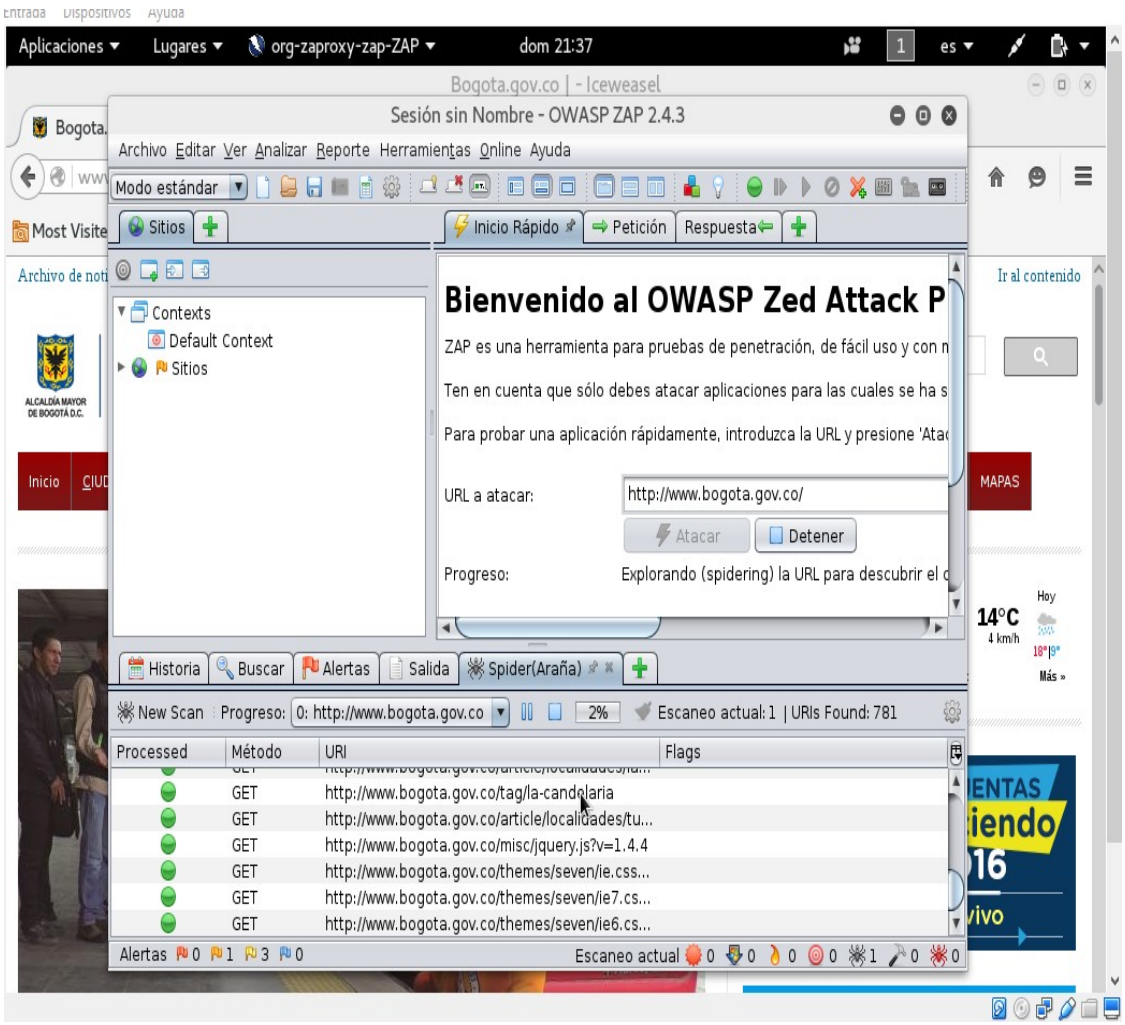
Figura 28. Ataque sqlmap parámetro p_p_id

Fuente: El autor

d). Ahora bien utilizaremos otra herramienta denominada OWASP para identificar otras vulnerabilidades.

1. Al abrir esta aplicación diligenciamos la página www.bogota.gov.co y seleccionamos atacar, para realizar el análisis como se evidencia en la figura 29.

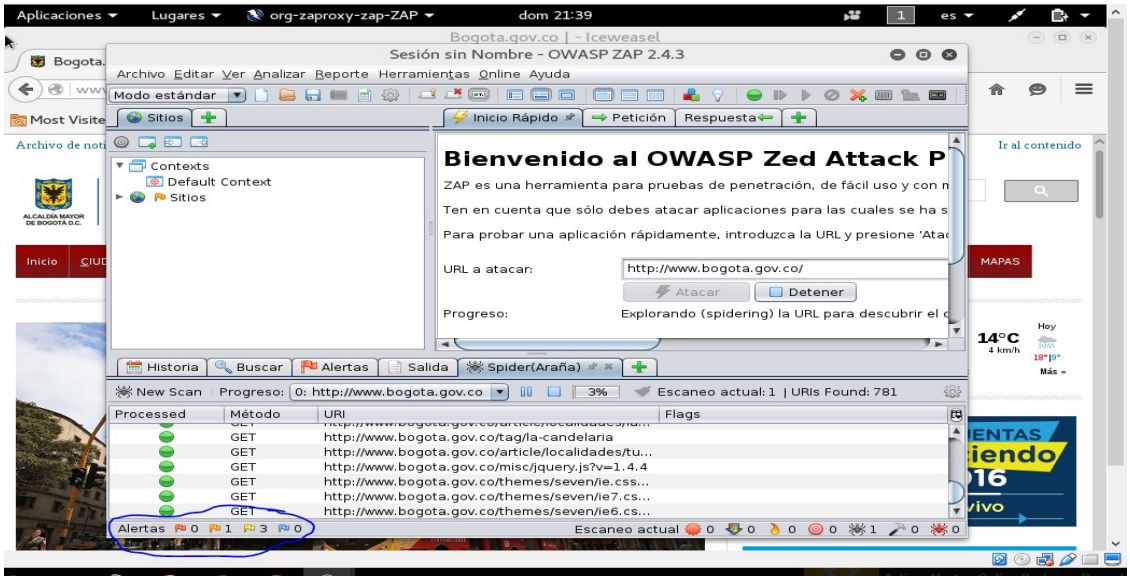
Figura 29. Análisis OWASP



Fuente: El autor

2. Como se muestra en la figura 30, OWASP realiza un escaneo total a la página para los cual nos empieza a mostrar alertas de diferente tipo de criticidad en este caso 8.

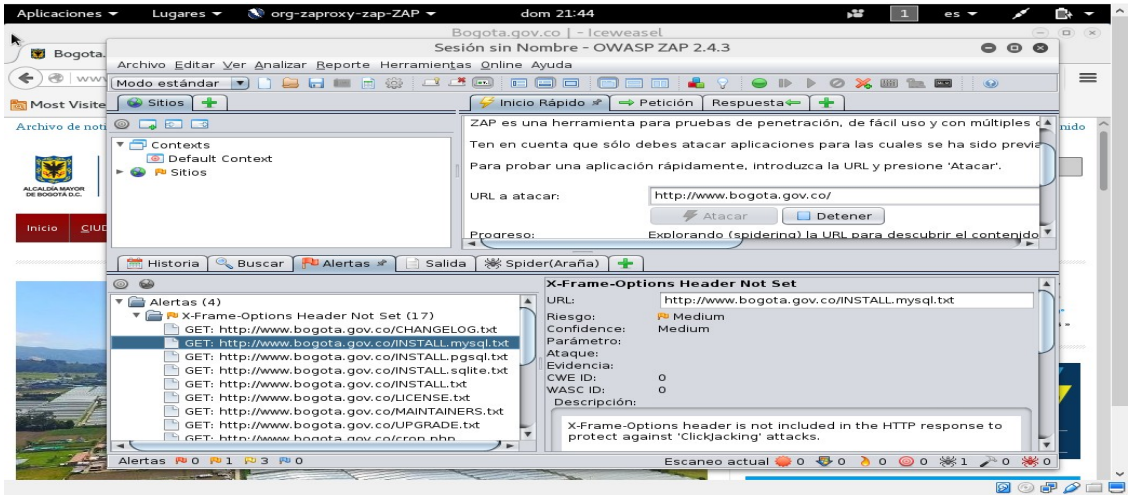
Figura 30. Alertas Análisis OWASP



Fuente: El autor

3. Nos dirigimos a la pestaña alertas como se muestra en la figura 31 denominada Detalle Alertas OWASP y seleccionamos en este caso la de criticidad media X-Frame-Options Header Not Set. Desplegamos el listado, seleccionamos alguna de las urls y evidenciamos que nos informa que X-Frame-Options no está incluido en la respuesta para HTTP para protegerse de ataques clicjaking. Por tanto es una vulnerabilidad que se debe corregir.

Figura 31. Detalle Alertas OWASP

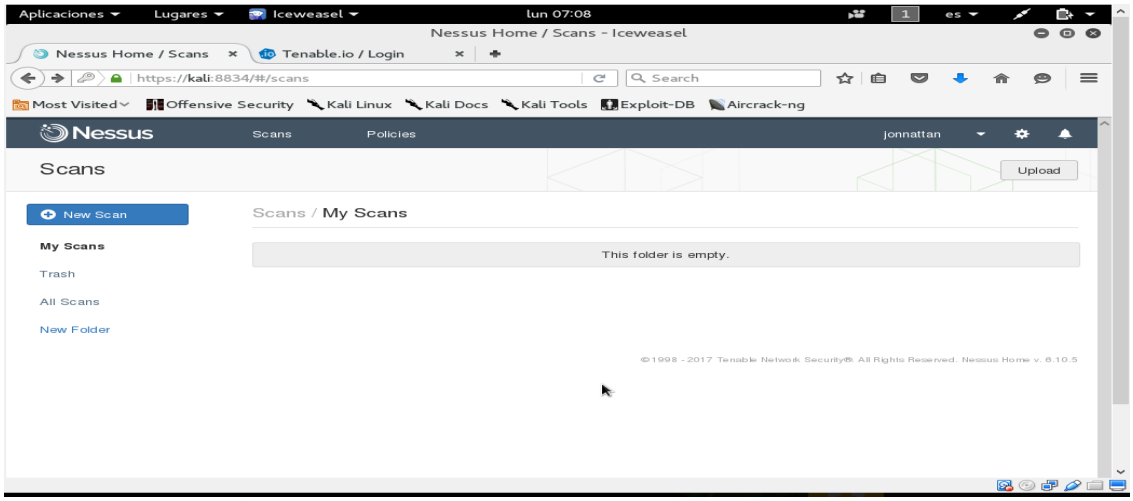


Fuente: El autor

e). Finalmente utilizamos la herramienta Nessus

1. Seleccionamos New Scan que se evidencia en la pantalla principal de Nessus como se observa en la figura 32.

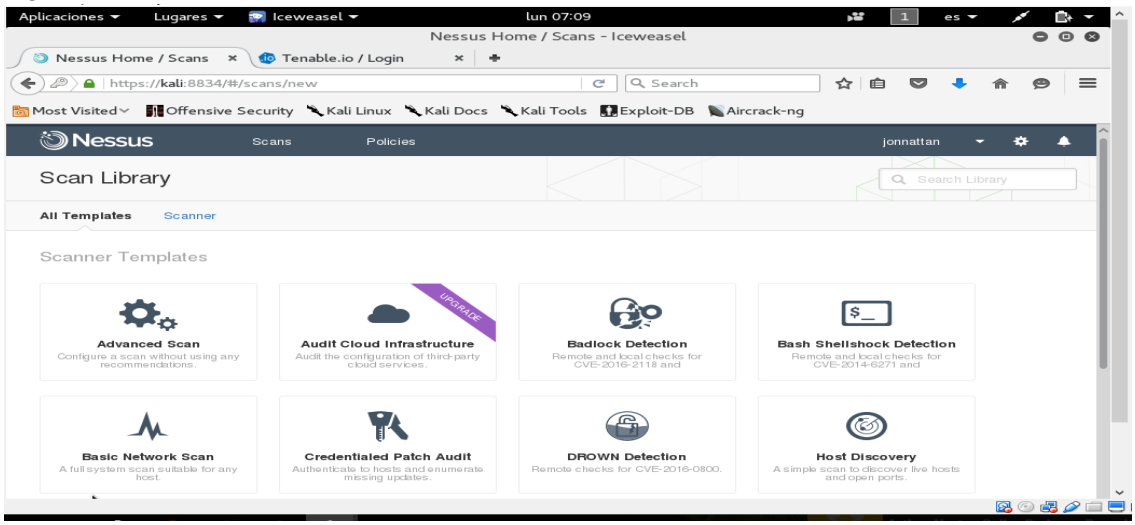
Figura 32. Nessus



Fuente: El autor

2. Seguidamente se selecciona Advanced Scan en Nessus para inciar el escaneo avanzado. Ver figura 33.

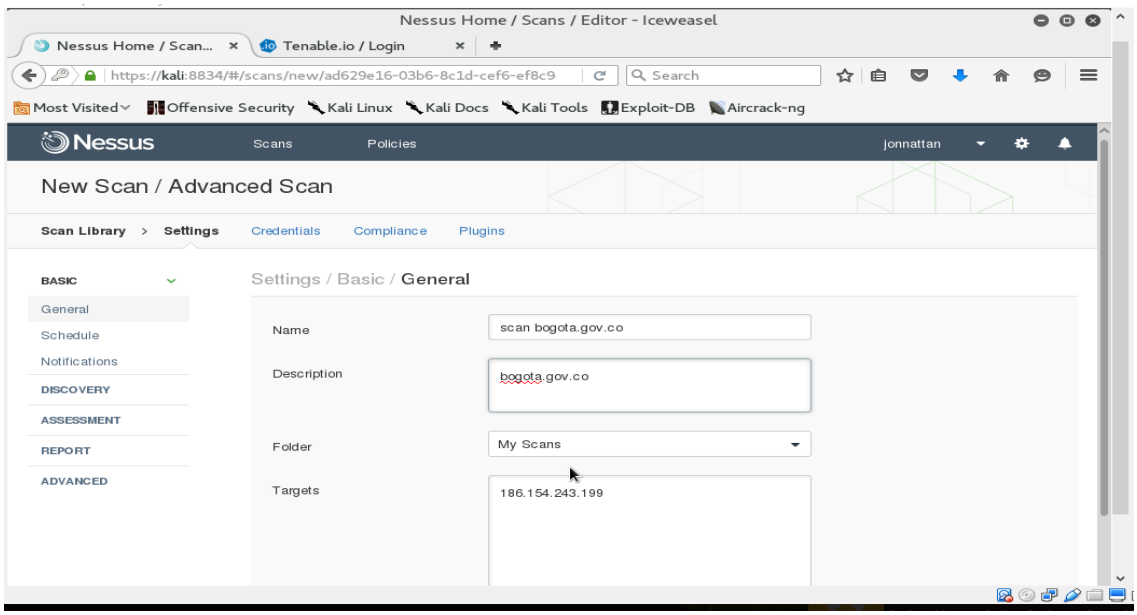
Figura 33. Nessus escaneo avanzado



Fuente: El autor

3. En la figura 34, se observa el momento en que diligenciamos nombre, descripción y en targets la IP 186.154.243.199 que deseamos escanear. Posteriormente clic en save.

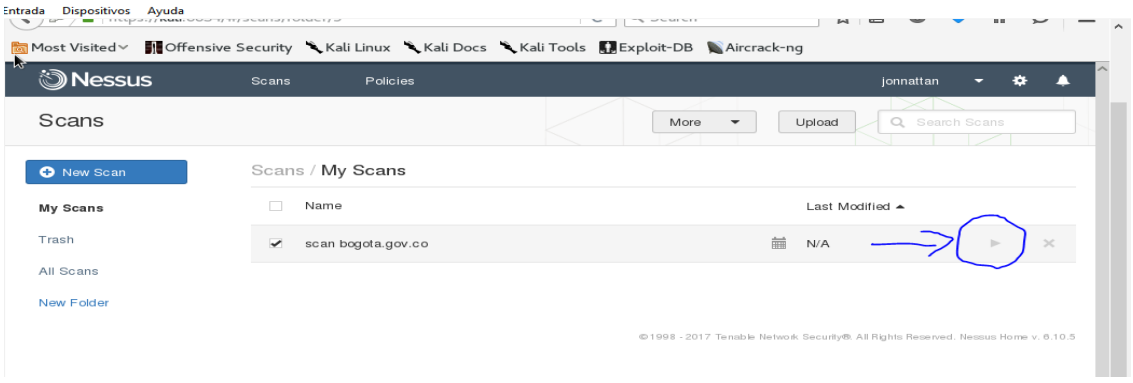
Figura 34. Nessus configuración escaneo avanzado



Fuente: El autor

4. Ahora bien, damos clic en el icono de ejecución del scan creado “scan bogota.gov.co” y esperamos que finalice el respectivo escáner. Tema que se da a conocer en la figura 35 denominada Nessus ejecución escaneo avanzado.

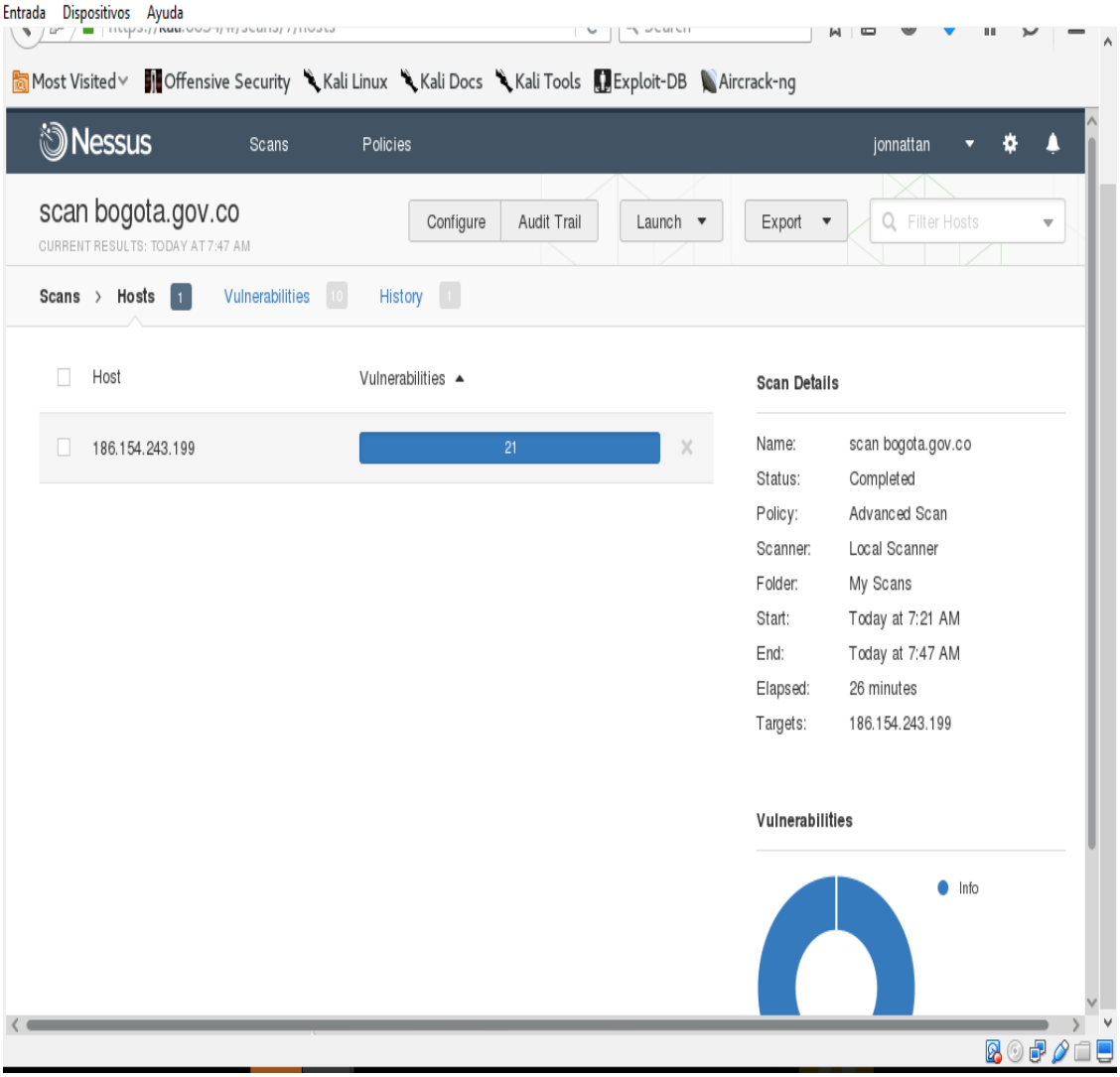
Figura 35. Nessus ejecución escaneo avanzado



Fuente: El autor

5. Cuando aparezca el chulo, este indica que el escáner ha finalizado, por lo tanto damos clic en “scan bogota.gov.co” para visualizar los respectivos resultados. Allí encontramos que la dirección 186.154.243.199 posee 21 vulnerabilidades informativas. Para ver el detalle de las mismas, damos clic en la dirección 186.154.243.199. Ver figura 36.

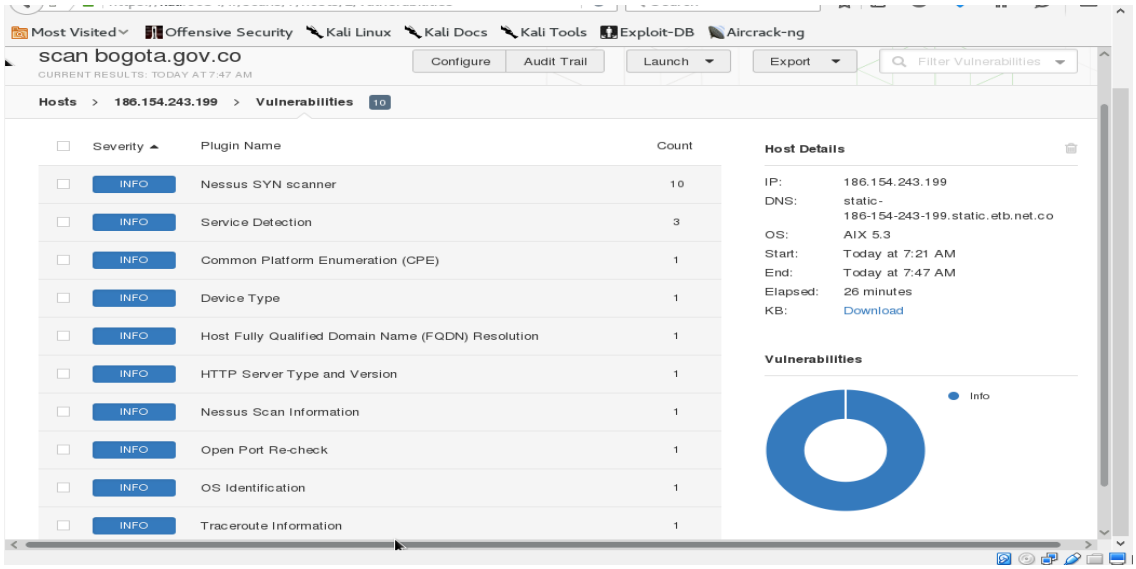
Figura 36. Nessus finalización escaneo avanzado



Fuente: El autor

6. Como resultado, se evidencio en la figura 37 que las vulnerabilidades informativas obedecen a Nessus SYN scanner, Service Detection, Common Plattform Enumeration (CEP), Device Type, Host Fully Qualified Domanin Name, HTTP Server Type and Version etc.

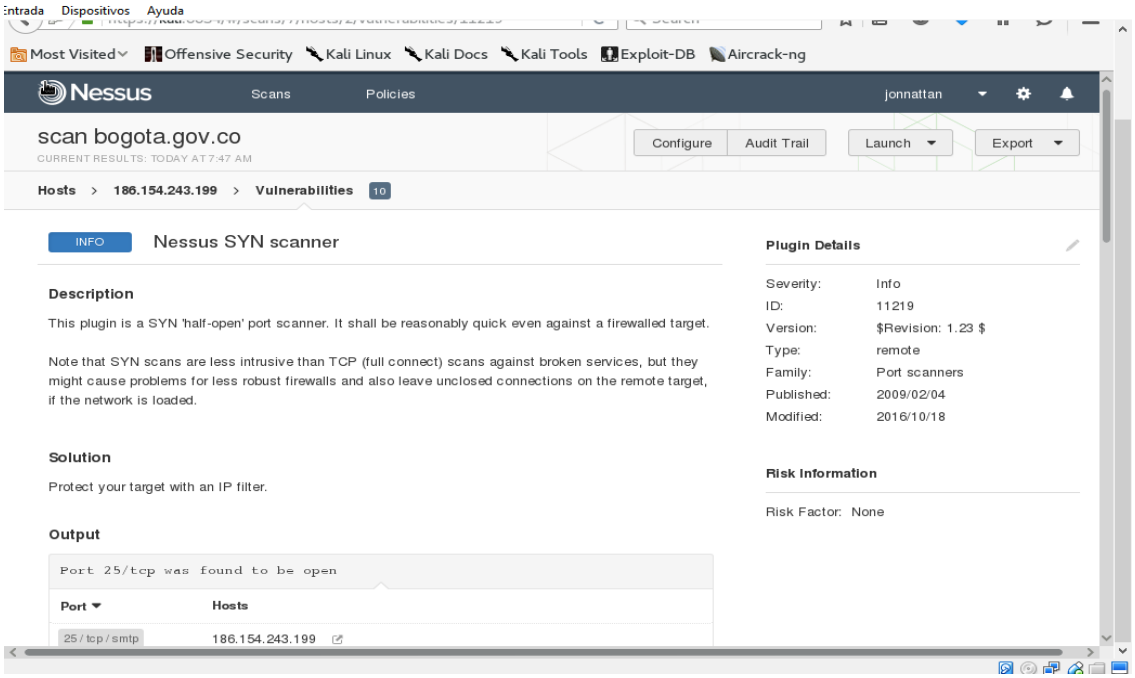
Figura 37. Nessus Vulnerabilidades



Fuente: El autor

7. Finalmente, se muestra en la figura 38 que al dar clic en INFO podemos encontrar el detalle de la vulnerabilidad y la solución de la misma.

Figura 38. Nessus Detalle Vulnerabilidades



Fuente: El autor

Descripción:

Este complemento es un escáner de puerto “medio abierto” SYN. Debe Ser razonablemente rápido incluso contra un blanco de fuego.

Tenga en cuenta que las exploraciones SYN son menos intrusivas que las exploraciones TCP (full connect) contra los servicios rotos, pero pueden provocar problemas para cortafuegos menos robustos y también dejar conexiones no cerradas en el destino remoto si la red está cargada.

Solución:

Proteja su objetivo con un filtro IP.

8. Resultados:

Después de realizar las respectivas pruebas y ataques de penetración se evidencio que la página www.bogota.gov.co presenta vulnerabilidades como:

e) Los puertos 993, 995, 143, 25, 80, 110, 587, 465, 563 y 119 se encuentran abiertos, lo cual hace que esta se encuentre en riesgo de ataques.

f) Se visualizó la topología de red que se utiliza para lograr la conexión a la página web, identificando otras IP las cuales se podrían atacar o vulnerar.

g) Que X-Frame-Options no está incluido en la respuesta para HTTP para protegerse de ataques clicjaking.

h) Se evidencio las vulnerabilidades informativas como Nessus SYN scanner, Service Detection, Common Plattform Enumeration (CEP), Device Type, Host Fully Qualified Domanin Name, HTTP Server Type and Version.

Por otra parte, al realizar los respectivos ataques para lograr acceder a las bases de datos u obtener alguna información de ellas, no fue posible ya que se evidencia una sólida configuración de seguridad ante este tipo de ataques.

8. METODOLOGIA Y ANALISIS ORIENTADO A LA SEGURIDAD WEB

La importancia de la seguridad en las aplicaciones web, indica medidas de seguridad tanto para la prevención, detección y corrección que puedan ejecutar las organizaciones o personas, quienes a su vez puedan garantizar la seguridad de la información en sus aplicaciones web. Esto enfocado firmemente a mejorar y mantener la disponibilidad, confidencialidad e integración de la información de las empresas y usuarios.

La elaboración de esta metodología permite a las empresas y personas tener claridad de lo importante de tener aplicaciones web seguras, más aun cuando la seguridad es una de las prioridades más bajas a la hora de disponer una aplicación web en producción tal y como lo expone Juliana Rodríguez, *"Según Gartner el 75% de los ataques están dirigidos a estas plataformas, sin embargo para muchas organizaciones aún no es una prioridad la implementación de tecnologías para su protección.".*[25]

En consecuencia de lo anterior, se presentan casos tales como *"Tan solo en Colombia en los últimos años se han presentado varias irrupciones, algunas muy recordadas como aquella ocurrida en julio de 2014 cuando al menos 25 sitios web de entidades gubernamentales, entre las que se encuentran las páginas de la alcaldía de Armenia, Coldeportes, y el Concejo de Medellín, fueron atacadas por Anonymus Colombia, bajo las modalidades de defacement y denegación de servicio. Al igual que en enero de este año cuando la web del Ministerio del Interior durante más de ocho horas mostró un mensaje que indicaba había sido hackeada por un grupo de hackers colombianos.".* (Rodríguez Juliana, 2015).

Por consiguiente, las personas y empresas requieren comprender la importancia de la seguridad en las aplicaciones web, para así mismo evitar las problemáticas que como anteriormente se mencionó y es aquí donde la metodología contribuye a la sociedad brindando información de nivel sobre la importancia de la seguridad en las aplicaciones web para su prevención, detección y corrección.

[25] RODRÍGUEZ, Juliana. ¿Debo priorizar la seguridad de las aplicaciones web? [En Línea], mayo 2015. Disponible en: <https://www.b-secure.co/blog/debo-priorizar-la-seguridad-de-las-aplicaciones-web>.

Finalmente es de manifestar que la seguridad de una aplicación web no es tema de poca relevancia y que por el contrario, si se requiere realizar con las mayores garantías se debe incorporar en todos y cada uno de los pasos del ciclo de vida de la aplicación, desde su concepción inicial hasta su puesta en producción.

8.1. EL PERÍMETRO DE SEGURIDAD DE UNA APLICACIÓN WEB

El perímetro de seguridad de una aplicación es medido a través del método OWASP, para definir el perímetro de seguridad ha de tenerse en cuenta las rutas que llevan a los diferentes procesos de una aplicación, estas rutas son bases de obtención de información pero también son riesgosas pues cada una se define como un punto de vulnerabilidad es por esa razón que es necesario definir el perímetro de seguridad de una aplicación.

La seguridad perimetral es un concepto clave para proteger cualquier web de cualquier daño o ataque que busque perjudicar su correcto funcionamiento, por ello la seguridad perimetral:

- Es una estrategia para proteger los recursos de una web conectada a la red.

- Establecer y desarrollar la práctica de la política de seguridad sobre un sitio web, permite que la seguridad perimetral sea efectiva.

- Permite que la página web expuesta en internet genere confiabilidad y credibilidad.

Para definir el perímetro de seguridad en las aplicaciones web, se debe tener en cuenta la arquitectura y elementos de red que hacen parte de la aplicación o aplicaciones web. Por tanto, debe contener los siguientes elementos y configuraciones:

- Debe tener la Instalación de cortafuegos o firewall definiendo allí la política de accesos, permitiendo o denegando el tráfico a través de reglas.

- Establecer una DMZ Zona Desmilitarizada con el propósito que no se permiten conexiones a la red interna.

- Política restrictiva, para denegar todo menos lo que se acepta explícitamente.

- Realizar la Instalación de antispam y antivirus que permitan proteger la red de ataques que se transmitan por medio de la red o medios.

- Implementación de sistemas de detección y prevención de Intrusos que monitorizan y generan alertas de seguridad, registra de eventos y bloquea ataques.

- Las sesiones establecidas de la misma manera deben ser matadas o terminadas en el momento en el cual el usuario finalice sus actividades dentro de la aplicación.

- La manipulación de los datos es vital en las aplicaciones, si la información es expuesta la aplicación no será segura.

- Detección de malware en pasarelas web y servidores de correo.

- Clientes VPN para permitir el ingreso a la red e infraestructura pública privada de forma confiable.

- Los certificados de seguridad SSL y de acceso siempre son más confiables que accesos directos a través del puerto 80 es por eso que la garantía de acceder a servicios por puertos seguros minimiza el riesgo.

Por otra parte, se deben implementar los siguientes protocolos PPTP, L2F, L2TP, SSL/TLS, SSH, que a su vez generan seguridad, facilidad, mantenimiento y tipos de clientes soportados.

8.2. MEJORAS A LA SEGURIDAD PERIMETRAL

La seguridad perimetral está basada en el método en el cual la información puede ser manejada y utilizada de forma segura. Por consiguiente, es necesario incorporar credenciales de acceso las cuales deben cumplir con un estándar de

valores hexadecimales, ya que la autenticación tiene como objetivo, proveer servicios de validación de ingreso seguro a las aplicaciones Web, proporcionando controles de autenticación de acuerdo al riesgo al que este expuesto la aplicación y a su vez denegando el acceso a posibles atacantes del sistema.

Por lo anterior, es necesario implementar y definir reglas claras de permisos basadas en accesos por puertos y también por aplicaciones como las que se presentan a continuación.

- Fortalecimiento de control de acceso:
    - Password en donde se solicite un mínimo de caracteres, combinación de caracteres, caracteres especiales, etc.
    - Exigir expiración de contraseñas mínimo cada 45 días.
    - Bajar el tiempo de inactividad de los usuarios.
- Revisión Periódica de las Actualizaciones que se lleven a cabo en el sistema.
- Crear Políticas Específicas por Servicio. En donde Las políticas de Firewall se establecen para los servicios que se requiere publicar.
- Establecer de DoS, las cuales son independientes de las políticas de seguridad de Firewall, ya que se aplican directamente en la Interface por donde el tráfico llega a nuestra aplicación web.

En cuanto a herramientas para una seguridad perimetral que verifican que el código con el que se está creando la aplicación no contenga debilidades o vulnerabilidades comparando dicho código con otros conocidos como potencialmente débiles o susceptibles de ser atacados, estas son:

a). Pruebas de seguridad estáticas (SAST): se analiza el código y se compara con patrones para detectar problemas de seguridad conocidos.

b). Pruebas de seguridad dinámicas (DAST): en este tipo de pruebas se analiza una porción de código con técnicas de ofuscamiento para analizar la respuesta del código y determinar si se crean riesgos de seguridad.

c). Pruebas de seguridad interactivas (IAST): Esta técnica es la combinación de las dos anteriores proporcionando más precisión en las pruebas.

Para las aplicaciones en producción se tienen:

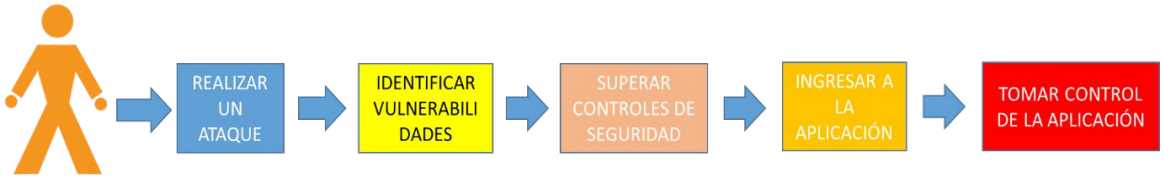
d). Autoprotección en tiempo de ejecución (RASP): en esta herramienta la aplicación reescribe código para manejar las tareas de seguridad sin dejar que estas tareas sean ejecutadas por procesos externos, esta protección requiere de grandes conocimientos de la aplicación y si se implementa mal puede generar problemas de desempeño de la aplicación.

e). Firewall de aplicaciones web (WAF): con este tipo de herramienta se tiene la posibilidad de filtrar código mal intencionado hacia una aplicación web, estas herramientas son capaces de escanear tráfico y aprender sobre lo que está permitido o no y complementar listas negras y blancas

Para lograr obtener control de una aplicación web, se debe iniciar por él envió de un ataque para identificar las vulnerabilidades del sistema. A partir de esto se conocen las vulnerabilidades, se rompen los sellos de seguridad y/o acceso, acceder a la aplicación y tomar el control de la aplicación.

De esta manera se podrá realizar ataques que busquen superar los controles de seguridad para ingresar a la aplicación y finalmente tomar total control de la aplicación. En consecuencia, se describe en la figura 39 el flujo y cada uno de los pasos mencionados para realizar una prueba de penetración:

Figura 39. Pasos Prueba Penetración



Fuente: El autor

8.3. PRUEBA DE PENETRACIÓN

En el entorno de las organizaciones es muy común que las vulnerabilidades potenciales en su gran mayoría son el producto de las fallas en el software desarrollado y puesto en producción, tema que comprende desde las configuraciones inapropiadas de los sistemas, la operación deficiente en los procesos o protecciones técnicas y como parte del mismo el factor humano. Es por esta razón, que mediante los diferentes resultados que se obtienen de una prueba de penetración, es posible que se pueden mejorar los mecanismos de seguridad y mitigar las vulnerabilidades que se presenten.

Este servicio es recomendado para los empresarios, pues permite proteger la información y mantenerla lejos de manos criminales. En consecuencia, la prueba de penetración debe ejecutarse en su totalidad, cada etapa ambientada de una manera muy diferente y las fases de análisis siempre deben ser autorizadas por el cliente.

8.3.1. Fase de reconocimiento

Es la fase en la cual se determina el objetivo y obtiene toda la información posible que permita realizar un ataque exitoso, esto mediante buscadores, herramientas de análisis de DNS, whois y demás herramientas para obtener información de nuestra víctima. *"La información que se busca abarca desde nombres y direcciones de correo de los empleados de la organización, hasta la topología de la red, direcciones IP, entre otros."*.[26]

Aquí, se recopila toda la información que se utilizara en las próximas fases. Ninguna información es irrelevante para estos casos todo es necesario y tiene el mismo grado de importancia.

8.3.2. Fase de escaneo

En esta fase se utiliza la información obtenida en la fase de reconocimiento con el objetivo de detectar posibles vectores de ataque para realizar el escaneo de

[26] CATOIRA, Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit Framework [En Línea], septiembre 2013. Disponible en: <http://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>.

puertos y servicios. En consecuencia, se lleva a cabo un escaneo extendido a las vulnerabilidades que permitan definir los vectores de ataque, encontrar fallas que puedan afectar la red, definir eventos, conocerlos y finalmente tener claro como eliminarlos definitivamente. Para realizar estas acciones se pueden utilizar herramientas como SYN stealth can, FIN scan, XMAS tree scan, NULL scan, FIN scan.

8.3.3. Fase de enumeración

En la tercera fase de una prueba de penetración se deben obtener datos referentes a los usuarios, nombres de equipos, servicios de red, contraseñas válidas de su entorno servicios y aplicaciones accesibles. Lo anterior, permitirá explotar la vulnerabilidad y obtener el control.

8.3.4. Fase de acceso

Durante esta fase se tiene en cuenta todas y cada una de las vulnerabilidades detectadas para acceder a los sistemas de información y obtener las evidencias e información necesaria. Allí, se accede al sistema y se logra a partir de la extracción de todos los puntos donde se detectan las vulnerabilidades que fueron utilizadas por el auditor del sistema. El proceso de acceso puede hacerse mediante herramientas automáticas como metasploit.

Sin embargo, si el propósito es llegar más allá, se podrá tomar el control de la máquina, encontrar el método para escalar los permisos necesarios y generar actividades o ejecuciones de acciones deseadas sobre la máquina intervenida.
Fase de mantenimiento de acceso

Ahora bien, al lograrse el acceso al sistema se debe preservar el sistema comprometido a disposición de quien lo ha atacado de mediante la instalación y ejecución de programas maliciosos que permitan realizar los respectivos ataques.

8.4. ETHICAL HACKING (Tests de penetración).

Mecanismo que se utiliza para evaluar las medidas de seguridad de un sistema de información con las que se cuenta en una organización. Este consiste en realizar

ataques ofensivos al sistema de seguridad a través del ingreso de un profesional de la información interno o externo.

Esta prueba tiene como propósito, detectar los puntos débiles que se puedan tener en un sistema determinado, donde se expone la confidencialidad, integridad y disponibilidad de la información.

8.5. HERRAMIENTAS

Las herramientas que se pueden utilizar para el desarrollo de un Test de Penetración a través del sistema operativo Kali Linux son:

- Nmap: Es un software de comunidad libre, el cual funciona como escáner de puertos en donde su principal función es identificar el sistema operativo, maquinas en red, puertos abiertos, servicios en ejecución y especificaciones de cada las máquinas de las victimas mediante el envío de paquetes y la respuesta de los mismos. Fue desarrollado para el sistema Linux, sin embargo en la actualidad ya está dispuesto como multiplataforma.

- Nessus: Escáner de vulnerabilidades con arquitectura cliente-servidor y la cual en la actualidad es una de las herramientas más actualizadas del mercado. Su funcionabilidad se enfoca en la actualización de plugins que permiten la detección de las debilidades existentes de las aplicaciones.

- Metasploit Framework: Es una herramienta framework de explotación de vulnerabilidades que genera ataques mediante la ejecución de exploits contra las víctimas consiguiendo ejecutar scripts de cobro o ejecutar comandos arbitrarios, controlar dispositivos, pantallas, navegar, cargar y descargar archivos además de la evasión ante las defensas de los antivirus. Esta herramienta es también de uso libre.

- Acunetix: Escáner de vulnerabilidades diseñado específicamente para auditar e identificar las vulnerabilidades de los sistemas web. Posee un poderoso generador de reportes con una interface completamente entendible para el usuario.

- AppDetectivePro y DbProtect: Herramientas que permiten realizar análisis a las bases de datos y detectar los errores de configuración que se posean, dificultades de identificación y control de acceso. De igual manera, informa sobre las configuraciones que pueden provocar fugas de información, ataques de denegación de servicio, modificaciones de información y uso no autorizado de accesos.

- DVL – DVWA: Es una aplicación para el entrenamiento de explotación de vulnerabilidades web y diseñada en PHP y MySQL. DVWA Posee funcionalidades como Command Execution que permite ejecutar comandos de consola desde la web, facilita ver, modificar y eliminar archivos y directorios de un servidor.

A continuación, se presentan las herramientas que se pueden utilizar en cada fase de la prueba:

- Fase de reconocimiento: NMAP, acccheck ace-voip, Amap, Automater, bing-ip2hosts, braa, CaseFile, CDPSnarf.

- Fase de escaneo: NESSUS, BBQSQL BED, cisco-auditing-tool, cisco-global-exploiter, cisco-ocs, cisco-torch, copy-router-config, DBPwAudit, Doona, DotDotPwn, Greenbone, Security Assistant, GSD, HexorBase, Inguma, jSQL.

- Fase de enumeración: Pinger, Fiendly Pinger, WS_Ping_Pro.

- Fase de acceso y fase de mantenimiento de acceso: DVL – DVWA.

8.6. PRINCIPIOS DE SEGURIDAD PROPUESTOS POR OWASP

Los principios de seguridad de OWASP permiten crear conciencia de los riesgos críticos a los que están expuestos, las diferentes puestas en producción de nuevas aplicaciones web y por tanto nos da a conocer 10 casos para la identificación de los riesgos:

- A1 – Inyección: Contempla las diferentes fallas de inyección como lo son SQL, OS, y LDAP, las cuales se presentan cuando existe la presencia de datos no

confiables que son enviados a un intérprete a través de comandos en donde el atacante trata de engañar al intérprete.

- A2 – Pérdida de Autenticación y Gestión de Sesiones: En la mayoría de situaciones la autenticación y gestión de sesiones son vulnerables ante los atacantes, permitiendo así capturar contraseñas, claves, tokens etc. Esto con el propósito de ingresar a las aplicaciones las credenciales de usuarios registrados en el sistema.

- A3 – Secuencia de Comandos en Sitos Cruzados (XSS): Los atacantes se encuentran en capacidad de ejecutar sentencias de comandos sobre los navegadores web con el propósito de capturar sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.

- A4 – Referencia Directa Insegura a Objetos: Los directorios, ficheros o bases de datos que son elementos internos, en algunas ocasiones no son protegidos con accesos o controles por parte de los desarrolladores de las aplicaciones, por tanto, los atacantes están al acecho de acceder a estas referencias para su manipulación.

- A5 – Configuración de Seguridad Incorrecta: La configuración de los diferentes servidores que componen los sistemas de información, deben estar definidas de forma lineal, para su mantenimiento y correcto funcionamiento, al igual, deben estar actualizados el software y librerías de código de los que se compone cada uno. Esto evitara ataques directos a los servidores.

- A6 – Exposición de Datos Sensibles: En una gran mayoría las aplicaciones web no cuentan con seguridad a datos sensibles como los son el número de tarjetas crédito o débito y credenciales de autenticación. Por tanto, se requiere que las aplicaciones contemplen métodos de protección de cifrado de datos para evitar robos, fraudes y delitos.

- A7 – Ausencia de Control de Acceso a las Funciones: Las aplicaciones requieren de la validación del control de acceso en sus servidores. Ya que al no realizar esta actividad las solicitudes de acceso no se verifican, y los atacantes tendrán la capacidad de realizar peticiones sin ningún tipo de autorización hasta conseguir algún tipo de delito informático.

- A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF): Los atacantes están en la capacidad de forzar a los navegadores a través de peticiones

HTTP legítimas, están son provenientes de las víctimas con sesión autenticada, lo que permite la falsificación y acceso a información sensible.

- A9 – Uso de Componentes con Vulnerabilidades Conocidas: Los componentes denominados librerías, los frameworks y otros módulos de software tienen privilegios de funcionamiento. Sin embargo, si el atacante vulnera alguno de estos elementos, se facilita el ingreso a intrusos exponiendo así la perdida de información.

- A10 – Redirecciones y reenvios no validados: Las aplicaciones web constantemente poseen links que redirigen a otros sitios web que pueden tener información o estructura no confiable, por tanto, los usuarios se pueden convertir en victimas malware o phising.[27]

En consecuencia y relación a lo anterior Los principios de seguridad propuestos por OWASP son:

- Seguridad a profundidad: la seguridad debe estar en mecanismos por capas y no depender de una sola regla o mecanismo de seguridad.

- Modelo positivo de seguridad: en este modelo se define como lista blanca lo que está permitido y lo demás se rechaza para ser comparado con listas negras.

- Fallar seguro: se debe dar un manejo adecuado a los errores de ejecución para que estos no develen pistas sobre a conformación general del programa.

- Vaya con el mínimo privilegio: asignar la cantidad mínima de privilegios para que un usuario pueda realizar la acción definida.

- Evite la seguridad por oscuridad: el diseño y lógica de un control de seguridad debe estar hecho sobre principios probados y conocidos.

- Mantener la seguridad simple: Utilizar mecanismos verificables y confiables.

[27] OWASP Foundation, Metodología OWASP [En Línea], octubre 2011. Disponible en: <https://www.owasp.org/images/8/80/Guía_de_pruebas_de_OWASP_ver_3.0.pdf)>.

- Detectar intrusiones: revisar logs y tareas rutinarias para detectar anomalías.

- No confiar en la infraestructura: Las aplicaciones deben de tener mecanismos propios de defensa para no delegar actividades importantes sobre las máquinas.

- No confiar en los servicios: Los servicios por lo general son administrados por un tercero, no se tiene la certeza del trato en seguridad para este servicio.

- Establecer configuración predeterminada segura: se deben implementar mecanismos seguros por defecto sin delegar configuraciones de seguridad a los usuarios.

Es necesario definir estrategias pero también asignar procesos y herramientas que cumplan con la función de aprender y proteger, pues todo está basado en procesos repetitivos pero que también deben ser analizados después de ser reconocidos para identificar si su comportamiento ha cambiado y pueda causar daño.

8.7. ESTRATEGIAS FRENTE EL PHISING

- La principal estrategia para evitar el phishing es la educación al usuario, es muy importante explicar a los usuarios de una aplicación de lo que se trata este tipo de estafa en términos claros sin extenderse en lenguajes técnicos que la mayoría no comprende, estas políticas deberían publicarse en el sitio web para el alcance de todos los usuarios.

- El acceso a las páginas web es permitido únicamente a través de puerto seguro https con su respectivo certificado de seguridad SSL, esto no evita que sea accesado de manera forzada pero si minimiza el riesgo en los sitios web.

- No realizar envíos de información personal utilizando mensajes de correo electrónico. Esto teniendo en cuenta que el no usar técnicas de cifrado y/o firma digital, convierten este medio en no seguro para enviar información personal o confidencial.

- Se debe realizar el aseguramiento utilizando el protocolo https y a su vez establecer el símbolo del candado relacionado con el certificado digital.

- Asegurarse que el navegador y antivirus estén siempre actualizados con las últimas versiones.

- Manejar un único idioma en los sitios web, pues los phishing pueden traducir la información de las páginas web y hacerse pasar por legítimo, hay que tener en cuenta que esto también es un gancho para robar credenciales.

- No ingresar a páginas web comerciales, financieras o bancarias desde los enlaces allegados al interior de correos electrónicos.

- No remitir datos personales a través de correo electrónico (números de cuenta, claves etc.).

- Evitar diligenciar encuestas con información personal o privada, tales como números de tarjeta de crédito, usuarios con claves o contraseñas, PIN para reactivar cuentas.

- No hagas clic en los enlaces que te pidan tus datos personales.

- Asegurarse que el navegador y antivirus estén siempre actualizados con las últimas versiones.

- Identificar los correos electrónicos sospechosos para determinar si son phishing que busca robar información, esto normalmente es detectado cuando los correos llegan desde empresas con nombre y logo esto es un punto altamente engañoso, también aquellos mails que lleguen con ofertas o regalos bloquearlos como phishing directamente desde un mitigador de ataques.

- Evitar las suscripciones a diferentes sitios con los correos electrónicos de la empresa.

- Realizar campañas educativas en donde se capacite a los usuarios y se les indique que para ingresar al sitio siempre hay que escribir la URL de acceso del sitio sin copiar y pegar el acceso o a través de enlaces enviados por la empresa.

- No acceder desde lugares públicos a sitios web como lo son una entidad financiera o de comercio electrónico, desde lugares no seguros como un cyber-café, locutorio u otro lugar público.

- No abrir ni descargar archivos de fuentes no confiables, ya que estos archivos suelen poseer virus o software malicioso que permiten a los atacantes acceder a los equipos de cómputo y a la información que almacene o introduzca en ésta.

8.8. CÓMO MEJORAR LA SEGURIDAD EN LOS SERVICIOS WEB.

Teniendo en cuenta las diferentes estrategias, principios fases, herramientas y conceptos presentados, a continuación se da a conocer una serie de ítems que permiten que a los servicios de las aplicaciones que contemplen una mejor seguridad:

- En primera instancia y de manera objetiva se deben cambiar las configuraciones que se encuentren como predeterminadas de la CMS para así tener control de los usuarios, comentarios y la información que es visible para el usuario.

- Utilizar balanceadores de carga independiente y no hacerlo directamente desde el servidor para distribuir las peticiones de sesiones que se hacen hacia las aplicaciones, pues esto genera un procesamiento innecesario del servidor físico.

- El registro de eventos debe contener suficiente información para reconstruir confiablemente la cadena de eventos y rastrear de vuelta a los que llamaron funciones sin autentificación previa.

    - Seguridad en la comunicación.

- Auditorias.

- Instalar SSL que encripta la comunicación entre el Punto A y el Punto B – el servidor web y el navegador.

- Actualizar los prefijos por defecto de la bases de datos para evitar la extracción de usuarios y contraseñas de acceso.

- Configurar los permisos CHMOD a las carpetas y archivo de la página web que se encuentren almacenados en el servidor.

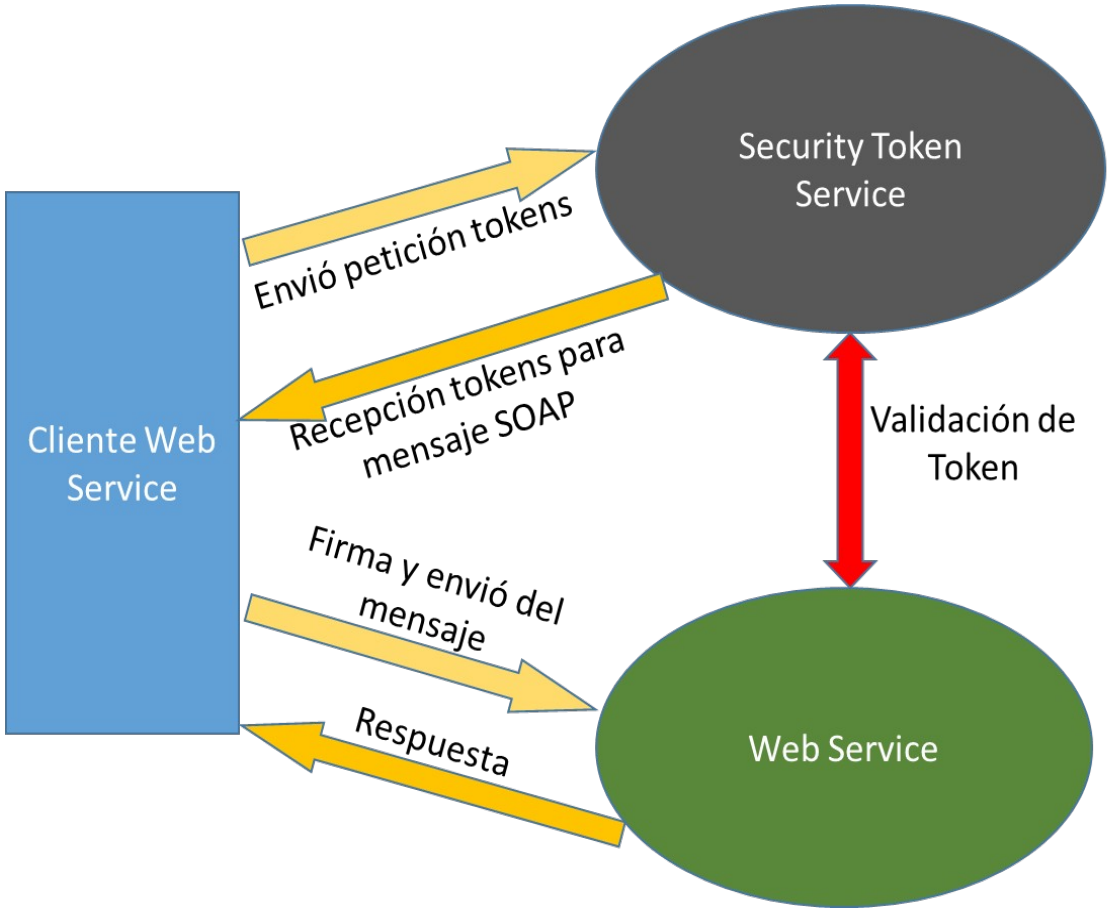
- Realizar copias backups semanales que se almacenen en una NAS de almacenamiento y manejar versiones con base a los módulos que sean más utilizados. Si las aplicaciones tienen procesos transaccionales o de paso de información confidencial, se deben tener certificados de seguridad de sitio. El almacenamiento de estas copias de seguridad deben ser almacenadas en un lugar seguro y de custodia.

8.8.1. Firmado o cifrado de cabeceras SOAP

El soporte de OASIS Web Services Security (WS-Security) ofrece una forma estándar de cifrar y firmar cabeceras SOAP. Para firmar o cifrar mensajes SOAP. Los mensajes SOAP (Simple Object Access Protocol) que son enviados en la red deben ser entregados confiablemente y sin modificaciones.

A continuación, se presenta en la figura 40 el funcionamiento del proceso SOAP, en donde a través de Tokens de seguridad el cliente solicita y recibe información de forma segura desde un web service.

Figura 40. Proceso SOAP



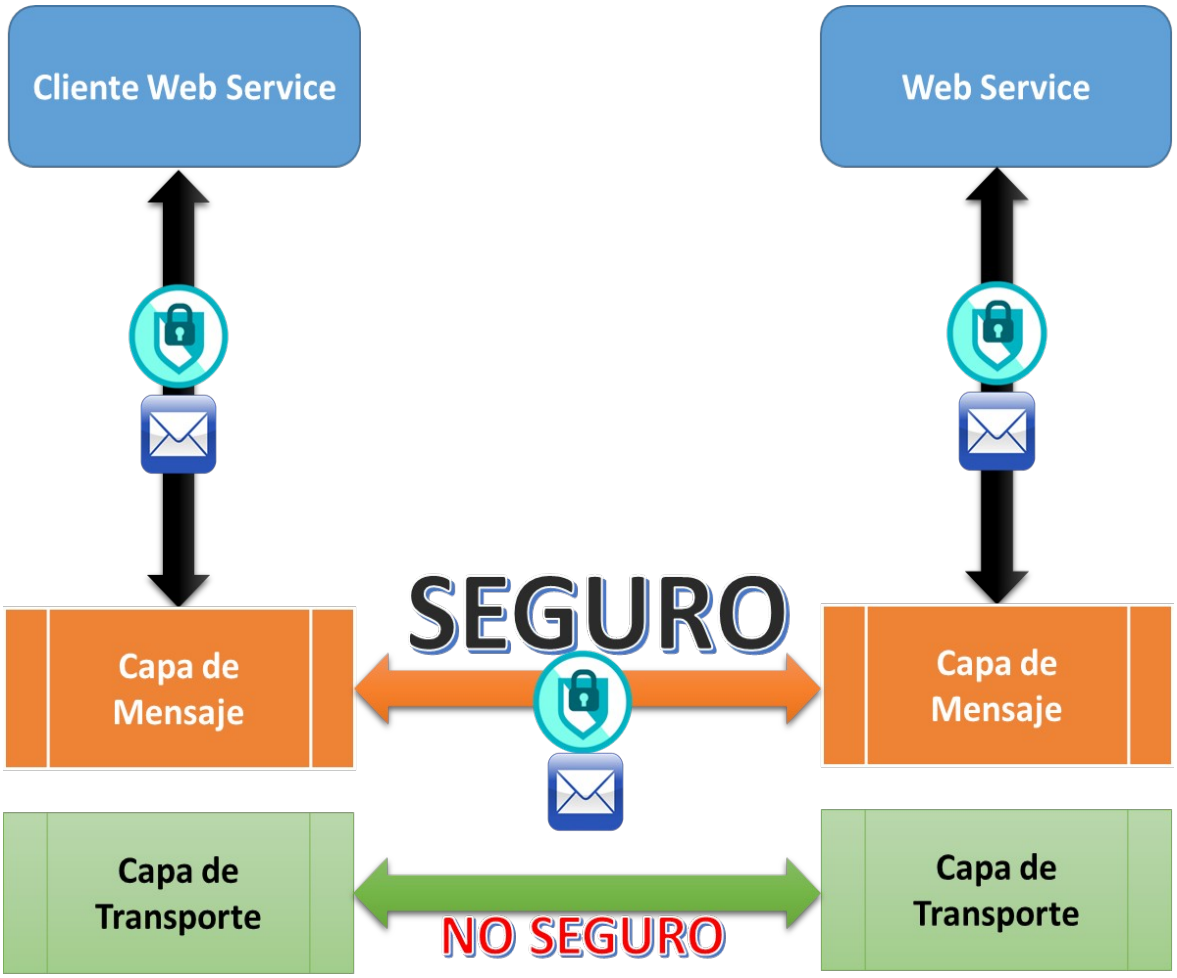
Fuente: El autor

8.8.2. Protección de mensajes basados en sesiones

El Web Services Secure Conversation es un servicio web que tiene como propósito suministrar una sesión de tipo segura para intercambiar mensajes de larga ejecución. De igual forma, este servicio utiliza el algoritmo criptográfico simétrico. WS como se denomina realmente para proteger los patrones de intercambio de mensajes mediante seguridad básica y la cual se encuentra basada en sesiones Web Services Security Reliable Messaging (WS-ReliableMessaging).

A continuación, se muestra la seguridad del Web Services Secure Conversation desde las peticiones realizadas por un cliente al Web Service ver figura 41, en la cual se evidencia que la capa de transporte no posee seguridad mientras que en su capa de mensaje si se encuentra establecida.

Figura 41. Proceso Servicio Web de Conversación Segura



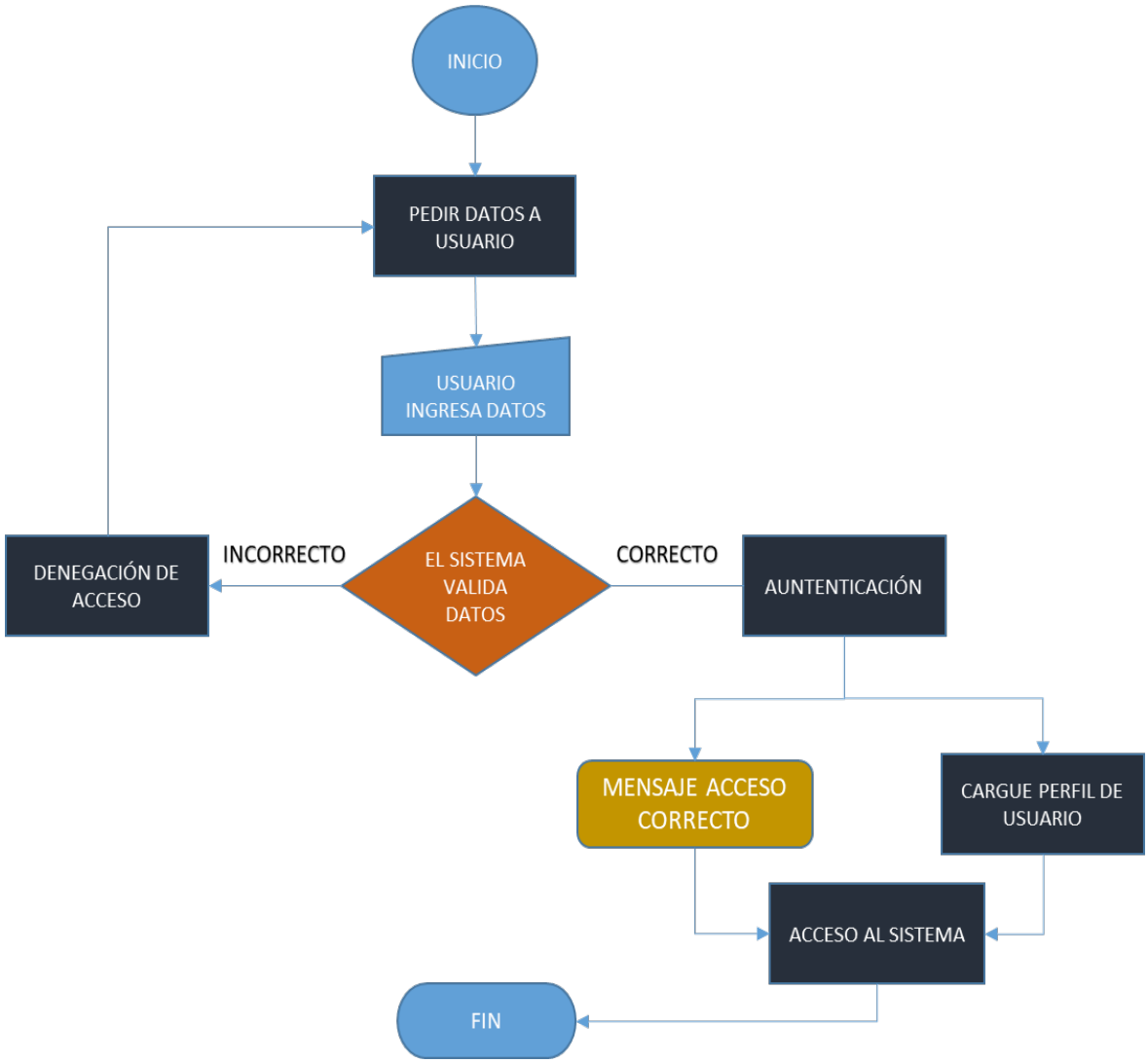
Fuente: El autor

8.9. CÓMO MEJORAR LA SEGURIDAD EN LA AUTENTICACIÓN

La autenticación como seguridad informática tiene como propósito, proveer servicios de autenticación segura a las aplicaciones Web, proporcionando los controles necesarios de acuerdo al riesgo de la aplicación a la que se encuentra expuesta una aplicación web, denegando el acceso a posibles atacantes del sistema.

En consecuencia, se presenta en la figura 42 el paso a paso del proceso de autenticación, cuando un usuario ingresa a un sistema de información o aplicación web:

Figura 42. Flujo autenticación



Fuente: El autor

- La seguridad de la autenticación para sitios web puede funcionar de manera correcta, sin embargo la implementación y uso de Certificados de autenticación por SSL, actividad que se desarrolla a través de través del Firewall permite tener una autenticación más robusta y segura.

En la siguiente figura 43 Autenticación SSL, se explica el funcionamiento del certificado de autenticación SSL, en donde se observa que el firewall juega un papel importante, ya que no permite el acceso de intrusos y se realiza la transferencia de información de manera segura:

Figura 43. Autenticación SSL

Fuente: El autor

- Contraseñas: Deben ser únicas de uso personal e intransferible, complejas con caracteres al azar, largas con más de 12 caracteres entre letras, números y símbolos. Esto permite que la contraseña sea segura y no pueda ser adivinada o descifrada fácilmente.

- Otro método que es muy efectivo no solo para las aplicaciones web sino para la red, es la integración de usuarios a través de LDAP. A través de este directorio es posible manejar los privilegios de autenticación de usuarios y garantizar una conexión permitida siempre y cuando se proteja de manera

correcta el acceso a este directorio activo de forma centralizada obteniendo toda la información y accesos para los usuarios.

A continuación, se presenta el paso a paso de autenticación de un cliente a través de un servidor LDAP. Ver figura 44.

Figura 44. Autenticación LDAP

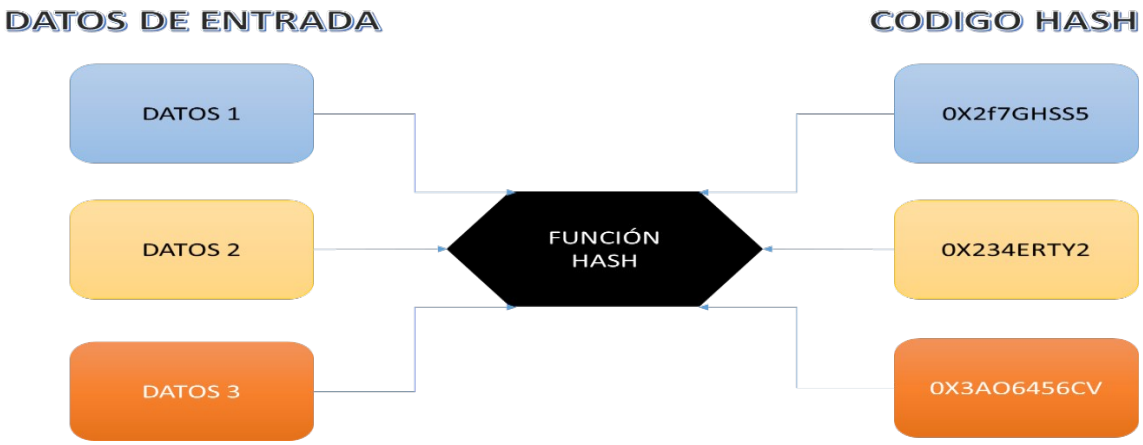
Fuente: El autor

- Fomentar el uso de frases claves en lugar de palabras claves.

- Definir mecanismos de autorización por niveles y dar más o menos privilegios a un usuario en particular dependiendo del nivel de acceso que se requiera.

- Emplear mecanismos de verificación por HASH contra bases de datos o certificados digitales con los que se firmen los mensajes. Mediante la función HASH es posible convertir información en cadenas alfanuméricas como se observa a continuación en la figura 45 denominada Proceso HASH:

Figura 45. Proceso HASH



Fuente: El autor

8.10. POLITICA DE MEJORA DE SEGURIDAD DE LAS APLICACIONES WEB

Con el propósito de que las aplicaciones web sean fiables y confiables frente a su seguridad, se describen a continuación pasos básicos a realizar como propuesta de mejora a su seguridad:

a). Inspeccionar logs y bitácoras de seguridad.

- Descripción:

  En primer instancia, se crea una bitácora para registrar eventos (quién, qué, cuándo, dónde y por qué) que se presenten en el sistema de información de la aplicación web. Se agrupan los eventos que atentan contra los recursos tecnológicos por uso.

  Por otra parte, se debe realizar revisión semanal de los “logs” del servidor y aplicación web para detectar situaciones anómalas, haciendo utilidad de software denominados TANGO04 y Webalizer que permiten evaluar este tipo de información.

- Actividades:

  Revisar el contenido de los archivos de registro de eventos de la página web, de acuerdo a una periodicidad no superior a un mes, considerando:

- Alarmas generadas por el sistema.

- Eventos de acceso no autorizado.

- Acceso a la aplicación.

- Comportamientos anormales.

- Entregable:

  Reporte resultante detallando las situaciones encontradas. Para posteriormente actualizar la bitácora de monitoreo.

- Responsable:

  El administrador de la plataforma debe enviar al analista de monitoreo el informe de acciones implantadas para eventos detectados.

- Propósito:

  Asegurar el adecuado registro de los eventos, revisado máximo en un mes, revisando los siguientes aspectos: inhabilitación de registro a nivel de aplicación o SO, ejecución de procesos automáticos y configuraciones de opciones de logs.

b). Detección de virus.

- Descripción:

  Comprende la introducción de código malicioso en la aplicación. Por tanto, los servidores que conforman el sistema de información de la aplicación web deben tener antivirus licenciados, instalados y actualizados como lo

son Norton Security, Kaspersky Total Security, Bitdefender, ESET Internet Security y AVG Utimate. .

En consecuencia, la utilización de Acunetix que es un antivirus para la protección de aplicación web, permite la identificación de problemas y además la ejecución de test para analizar el contenido de la página web, garantizando una performance efectivo mediante la generación de sus reportes.

- Actividades:

  Detectar y dar tratamiento de solución de código malicioso en la en la aplicación.

- Entregable:

  Documentar hallazgos de virus informáticos o código malicioso, detallando el tipo de virus, el recurso afectado y estado del mismo.

- Responsable:

  El administrador de la plataforma envía al analista de monitoreo el informe de aplicación para atender los eventos de virus.

- Propósito:

  Coordinar la ejecución de herramientas de antivirus en modo detección, por medio de mecanismos para la detección centralizada y automática.

c). Actividad de usuarios.

- Descripción:

Revisión y monitoreo de cada una de las actividades realizadas por los usuarios sobre la aplicación web.

Se debe llevar a cabo con herramientas gratuitas como lo son Hotjar, Google Analtyisc, Hootsuite o en su defecto con herramientas licenciadas como PRTG, herramientas que permiten observar a detalle el flujo de visitas, tendencias y la apreciación que los usuarios tienen de su página en internet, además de la disponibilidad del sitio web, procesos, características, y tiempos y de carga.

Por otra parte, se debe realizar revisión semanal de los “logs” del servidor y aplicación web para detectar situaciones anómalas, haciendo utilidad de software denominados TANGO04 y Webalizer que permiten evaluar este tipo de información.

- Actividades:

  - Solicitar al administrador de la plataforma registros de logs y eventos para obtener información de la actividad de los usuarios.

  - Recolectar la información con el fin de obtener las fuentes para el análisis.

  - Verificar si se encuentran eventos como ataques, violaciones o incidentes de seguridad.

- Entregable:

  Documentar los hallazgos en el informe de monitoreo, incluyendo: situación de operación, incidentes de seguridad, usuarios inactivos, patrones de comportamiento y otros problemas.

- Responsable:

  El responsable define acciones para solucionar o atender hallazgos: Si se detectan incidentes, debe revisar la implantación de acciones y aplicar la

gestión de incidentes; si se encuentran usuarios inactivos o patrones anormales, debe revisar y ajustar los perfiles de usuario y evaluar otros mecanismos de registro y control.

- Propósito:

  Realizar el análisis de la información obtenida con el fin de verificar: verificar la actividad de los usuarios, establecer los patrones anormales de comportamiento, usuarios inactivos, violaciones o incidentes de seguridad, intentos de ataque, incumplimiento de políticas.

d). Autenticación de usuarios.

- Descripción:

  Comprende todo tipo de ingreso y operación autorizado o no a los sistemas. Se debe solicitar la bitácora de eventos presentados en el sistema de información de la aplicación web.

  Por otra parte, se revisan “logs” del servidor y aplicación web que presentaron situaciones anómalas acorde a los informes de las aplicaciones TANGO04 y Webalizer.

- Actividades:

  - Solicitar al administrador el recurso, la lista de usuarios activos con sus respectivos perfiles.

  - Confrontar la información proporcionada contra la matriz de perfilamiento de acceso a recursos IT.

  - Actualizar la matriz de perfilamiento de acuerdo al informe enviado.

  - Análisis de eventos e informes con situaciones anómalas.

- Entregable:

  Informe de los hallazgos dejando anotación de las diferencias encontradas.

- Responsable:

  Asegurar por parte de los responsables, la ejecución de las actividades de mantenimiento de usuarios y perfiles.

- Propósito:

  Validar la situación de la entidad en cuanto a usuarios y perfiles, tener la documentación correspondiente y mantener actualizada la matriz de acuerdo a las solicitudes de modificación realizadas.

e). Auditoria de Sistemas.

- Descripción:

  Definir plan de tratamiento de riesgos: Establecer un plan de auditoria de riesgos permite identificar las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

  Ejecución de Test de Penetración que incluya el informe de vulnerabilidades, riesgos y actividades a ejecutar sobre la aplicación web.

- Entregable:

  - Implementación de un plan de tratamiento de riesgos, el cual se encuentre conformado por objetivos que permitan llevar a cabo el desarrollo e identificación de controles.

- Informe de vulnerabilidades, riesgos y acciones a ejecutar.

- Establecer los controles: Estos permiten reforzar la seguridad con el fin de neutralizar cual quiera amenaza detectada en el sistema de información.
- Formación y concienciación: Todo el personal de las organizaciones debe estar concientizado de la importancia frente a la seguridad de la información al interior de las compañías.

- Desarrollo del marco normativo necesario: Es importante establecer en las organizaciones normas, manuales, procedimientos e instrucciones con respecto a la SGSI.

- Gestionar las operaciones del SGSI y todos los recursos que se le asignen:

    - Constantemente llevar a cabo la revisión del Sistema de Gestión de Seguridad de la Información por el área de seguridad de la información de las compañías.

    - Llevar a cabo la ejecución de procedimientos, controles, monitoreo y revisión del sistema de información que permitan detectar errores en resultados de procesamiento, brechas e incidentes de seguridad. Para así, establecer si las acciones ejecutadas para resolver incidentes de seguridad han sido eficaces.

    - Se debe revisar de manera regular la eficacia del SGSI en función de los resultados de auditorías de seguridad.

    - Establecer y divulgar procedimientos, controles de detección y respuesta a incidentes de seguridad.

    - Llevar a cabo de forma constante la revisión de la evaluación de riesgos y seguimiento a influencian los cambios en la organización, además de la tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles y resultados.

- Ejecutar auditorías internas con el propósito que permitan determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de la ISO 27001.

- Propósito:

  Establecer el plan de auditoria que permita detectar vulnerabilidades desde diferentes aspectos, para así mismo proceder a ejecutar los respectivos planes de acción y controles.

Finalmente, como reflexión y recomendación frente a la seguridad en aplicaciones Web que tiene como actor y responsable principal a los desarrolladores, en base a que las aplicaciones desarrolladas por estos mismos presentan con gran frecuencia defectos que son aprovechados por atacantes que se encuentran a la espera de la disposición de nuevas aplicaciones para así realizar ataques. Los desarrolladores no se centran en los conocimientos de la seguridad de los sistemas web y no consideran la importancia de las posibilidades de que los atacantes descubran los huecos de seguridad que pueden tener las aplicaciones y más aún cuando se desconocen las propiedades e uso del protocolo HTTP, así mismo que se puede acceder a las aplicaciones web con herramientas diferentes a los navegadores web del mercado.

En consecuencia, los desarrolladores y programadores deben concientizarse de que de ellos depende que las aplicaciones desarrolladas y puestas en producción posean las configuraciones necesarias para rechazar o filtrar peticiones que no cumplan con las características esperadas o predefinidas. De igual manera, es de precisar que ningún ingreso al sistema debe ser de digna de confianza y que por el contrario están deben pasar por un filtrado de datos para confirmar la correcta usabilidad.

Es por este motivo que al momento de realizar el desarrollo y antes de su puesta en producción de aplicaciones web, los desarrolladores tomen conciencia a lo que se están exponiendo estos desarrollos. Esto con el propósito de evitar problemas tanto a usuarios como clientes, ya que se puede ocasionar la pérdida de información confidencial del sistema sin que el propietario de la aplicación Web note algún tipo de ataque en su aplicación. Es de aclarar, que en la actualidad existe una gran cantidad de ataques sin embargo las medidas para evitar la mayoría de estos problemas son el filtrado, que con las respectivas precauciones

de entradas o peticiones a la aplicación web con respecto a las infectadas se puede disminuir la probabilidad de sufrir ataques lo que permite hacer más útil y confiables las aplicaciones web.

9. CONCLUSIONES

- La metodología desarrollada permite a las empresas u organizaciones, comprender y entender los diferentes conceptos que hacen parte de la Seguridad en Aplicaciones Web, además de las diferentes actividades, pasos y acciones a realizar para garantizar la seguridad de la información dispuesta en la red de redes internet.

- El desarrollo de esta metodología permite a las empresas y/o usuarios consultar mecanismos de protección tanto de software como de hardware que permiten la detección, mitigación y/o control de los diferentes riesgos y vulnerabilidades que pueden presentar sus aplicaciones web.

- Las medidas de protección informática establecidas en la metodología permiten identificar los diferentes riesgos, amenazas y ataques a los que se encuentra expuesta la información web, con el propósito de hacer compatibles las estrategias de desarrollo que se establezcan al interior de las organizaciones enfocadas en la protección de la información.

- La metodología, se convierte para las empresas u organizaciones en un elemento de vital importancia ante los ataques, amenazas y vulnerabilidades informáticas a las que se encuentran expuestas sus aplicaciones web, ya que en el momento de requerir la prevención o actuar ante los mismos, la misma se convierte en una herramienta muy útil para mantener la disponibilidad, confidencialidad e integralidad de la información.

- La metodología establece para los usuarios una serie de actividades dentro de una política, esto con el propósito de incentivar a las organizaciones a adoptar las mismas, y así lograr que la seguridad de las aplicaciones web de sus empresas, sea la mejor posible, confiable y donde se mantenga la disponibilidad, confidencial e integridad de la información.

- Siempre la información está expuesta ante todos los ciberdelincuentes, por tanto, esta metodología brinda la información propicia en búsqueda de que las empresas implementen y mantengan una buena seguridad en las aplicaciones web y deje de ser una razón para temer en el momento de acceder a la información tanto por los usuarios o administradores de las aplicaciones.

10. REFERENCIAS BIBLIOGRÁFICAS

CALLES, Juan Antonio. Wi-Fis: Tipos de ataque y recomendaciones de seguridad [En Línea], octubre 2013. Disponible en: <http://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html>.

CATOIRA, Fernando. Penetration Test, ¿en qué consiste? [En Línea], julio 2012. Disponible en: <http://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/>.

CATOIRA, Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit Framework [En Línea], septiembre 2013. Disponible en: <http://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>.

Culturación. "Cómo convertir un PC en servidor web" [En Línea]. Recuperado de <http://culturacion.com/como-convertir-un-pc-en-servidor-web/>.

El Tiempo. "Tecnósfera. Más de 760.000 sitios web fueron vulnerados en un año" [En Línea], abril 2016. Disponible en: <http://www.eltiempo.com/archivo/documento/CMS-16567844>.

FRANKFURT. Hallado un virus informático en una central nuclear alemana [En Línea], abril 2016. Disponible en: <http://internacional.elpais.com/internacional/2016/04/27/actualidad/1461751859_118617.html>.

GÓMEZ, Hilda. Medidas para reforzar la seguridad de las páginas web [En Línea], junio 2015. Disponible en: <http://cso.computerworld.es/ciberseguridad/medidas-para-reforzar-la-seguridad-de-las-paginas-web>.

Icetex. Manual de políticas de seguridad de la información [En Línea], octubre 2014. Disponible en: <http://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf#search="manuales">.

Instituto Nacional de Tecnologías de la Comunicación S.A. (INTECO). Seguridad en Sitios Web [En Línea], abril 2011. Disponible en: <https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridadwebsites.pdf>.

Kali Linux Penetration Testing Tools [En Línea], 2017. Disponible en: <https://tools.kali.org/>.

LAMARCA LAPUENTE, María Jesús. Hipertexto: El nuevo concepto de documento en la cultura de la imagen [En Línea], diciembre 2013. Disponible en: <http://www.hipertexto.info/documentos/internet_tegn.htm>.

LUJÁN, Sergio. Programación de Aplicaciones Web: Historia, Principios Básicos y Clientes Web. Editorial Club Universitario. (2002). Pág. 48.

MANTILLA, Carolina. Normas Icontec 1486 Última Actualización [En Línea], 2008. Recuperado de: <https://es.slideshare.net/carolinamantilla/normas-icontec-1486-ultima-actualizacion>.

MIER Y TERÁN, Andrés Romero - VÁSQUEZ MARTÍNEZ, Mario Alejandro Aspectos Básicos de la Seguridad en Aplicaciones Web [En Línea], abril 2016. Disponible en: <http://www.seguridad.unam.mx/documento/?id=17>.

MINTIC. Ley Nº. 1273 [En Línea], enero 2009. Disponible en: <http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>.

Monografías. “Aplicación Web de Seguridad Informática en la Universidad de Pinar del Río” [En Línea]. Recuperado de: <http://www.monografias.com/trabajos14/segur-informatica/segur-informatica.shtml>.

NAUDI, Tamara. El segundo informe de seguridad de la aplicación web de Acunetix muestra que el 55% de los sitios web tienen vulnerabilidades graves (y aumentan) [En Línea], agosto 2016. Disponible en: <https://www.acunetix.com/blog/news/web-app-security-report-2016/>.

NORIEGA, Samuel. Protocolos de Seguridad Básicos ¿Qué tan seguro es tu sitio web? [En Línea], 2015. Disponible en: <https://www.certsuperior.com/Blog/protocolos-de-seguridad-sitio-web-seguro>.
Noticias de Seguridad Informática. "¿Cuáles son los riesgos y ataques de seguridad en aplicaciones web?" [En Línea], marzo 2016. Disponible en: <http://noticiasseguridad.com/importantes/cuales-son-los-riesgos-y-ataques-de-seguridad-en-aplicaciones-web/>.

Noticias de Seguridad Informática. "El troyano bplug se dedica a molestar a tus amigos de facebook Ataques recientes" [En Línea], abril 2016. Disponible en: <http://noticiasseguridad.com/malware-virus/el-troyano-bplug-se-dedica-molestar-tus-amigos-de-facebook/>.

OWASP Foundation, Metodología OWASP [En Línea], octubre 2011. Disponible en:
<https://www.owasp.org/images/8/80/Guía_de_pruebas_de_OWASP_ver_3.0.pdf)
>.

Redeszone. El troyano bplug se dedica a molestar a tus amigos de Facebook [En Línea], abril 2016. Disponible en: <http://noticiasseguridad.com/malware-virus/el-troyano-bplug-se-dedica-molestar-tus-amigos-de-facebook/>.

RODRÍGUEZ, Juliana. ¿Debo priorizar la seguridad de las aplicaciones web? [En Línea], mayo 2015. Disponible en: <https://www.b-secure.co/blog/debo-priorizar-la-seguridad-de-las-aplicaciones-web>.

ROMERO MIER, Andrés – VÁSQUEZ MARTÍNEZ, Mario Alejandro. Aspectos Básicos de la Seguridad en Aplicaciones Web [En Línea]. Recuperado de: <http://www.seguridad.unam.mx/documento/?id=17>.

Segured. "El hosting y la seguridad de su sitio web" [En Línea], 2017. Disponible en: <http://segured.com/el-hosting-y-la-seguridad-de-su-sitio-web/>.

Toyoutome. “Tips de seguridad para tu sitio web” [En Línea], octubre. 2015. Disponible en: <http://toyoutome.es/blog/tips-de-seguridad-para-tu-sitio-web/37521>.

TUMERO, pablo. Desarrollo de aplicaciones Web [En Línea]. Recuperado de: <http://www.monografias.com/trabajos106/desarrollo-aplicaciones-web/desarrollo-aplicaciones-web2.shtml>.

TURNER, Sam. Seguridad de sitios web: problemas, peligros y amenazas [En Línea]. Recuperado de: <http://blog.iweb.com/es/2014/02/seguridad-web-amenazas/2457.html>.

UNIPAMPLONA. NORMA TÉCNICA COLOMBIANA - NTC 1486 [En Línea], Recuperado de: <http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf>.

Universidad de Alicante. Que es una aplicación web [En Línea], 2006-2007. Disponible en: <https://rua.ua.es/dspace/bitstream/10045/4412/5/03c-AplicacionesWeb.pdf>.