ANÁLISIS DE LA SEGURIDAD DEL SITIO WEB DEL MINISTERIO DEL TRABAJO APLICANDO PRUEBAS DE PENTESTING EN LA SEDE PRINCIPAL DE LA CIUDAD DE BOGOTÁ

HENRY ARMANDO FERNÁNDEZ MIRANDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2019

ANÁLISIS DE LA SEGURIDAD DEL SITIO WEB DEL MINISTERIO DEL TRABAJO APLICANDO PRUEBAS DE PENTESTING EN LA SEDE PRINCIPAL DE LA CIUDAD DE BOGOTÁ

Trabajo de grado previo a la obtención del título de
Especialista en Seguridad Informática

HENRY ARMANDO FERNÁNDEZ MIRANDA

FERNANDO JOSÉ DÍAZ MARTÍNEZ
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2019

Nota de aceptación:

Firma del presidente del jurado

Firma del Jurado

Firma del Jurado

Bogotá, 01 de abril 2019

Dedico este proyecto a mis padres, mi esposa y mi hijo, quienes con su apoyo han logrado que todas mis tareas y objetivos sean finalizados, su ánimo en los momentos difíciles, caídas que he tenido han sido fundamentales para lograr salir adelante.

A mi hijo Joel Matías motor de mi vida y la razón de buscar el mejor futuro, de poder entregar lo mejor de mí en el trabajo, en cada labor que realice y que ese amor se vea reflejado en la finalización de estos.

AGRADECIMIENTOS

Agradezco a Dios por guiarme en el camino y permitir culminar este proyecto, a toda mi familia por el apoyo que me dan siempre y en todo momento, a los docentes y tutores de mi proyecto, al tutor Fernando José Díaz Martínez y a quienes con su experiencia y conocimiento ha guiado mi trabajo ajustando el rumbo a seguir, así como sus valiosos aportes para avanzar en cada etapa de mismo.

CONTENIDO

LISTA DE FIGURAS

LISTA DE CUADROS

RESUMEN

Este trabajo tiene como objeto identificar las vulnerabilidades del sitio Web del Ministerio del Trabajo, usando como referencia la lista de vulnerabilidades del Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés) entregar las recomendaciones o controles que deben aplicarse para la corrección o mitigación, se indican algunas herramientas usadas en el proceso del cual se realiza la documentación de las pruebas del análisis de seguridad realizado, la información recolectada o resultado, igualmente resalta la importancia que tienen las auditorias periódicas de los sistemas, todo esto profundizando en los aspectos que se consideran importantes para mantener la seguridad de una plataforma web, como conclusión del proyecto se encuentra una serie de vulnerabilidades identificadas, controles recomendados y las conclusiones del proyecto.

Palabras claves

Hacking Ético, Pentest, Seguridad informática, Kali Linux, nmap.

GLOSARIO

- Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.[1]

- Ataque combinado: Es uno de los ataques más agresivos ya que se vale de métodos y técnicas muy sofisticadas que combinan distintos virus informáticos, gusanos, troyanos y códigos maliciosos, entre otros. Esta amenaza se caracteriza por utilizar el servidor y vulnerabilidades de Internet para iniciar, transmitir y difundir el ataque extendiéndose rápidamente y ocasionando graves daños, en su mayor parte, sin requerir intervención humana para su propagación.[2]

- Auditor: Persona que realiza pruebas o se encarga de auditar. También puede referirse a quien se encarga de verificar o comprobar.

- Autenticación: Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.[3]

- Ciberataque: Son actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio de computadoras y a través de la Internet. No necesariamente pueden ser cometidos totalmente por estos medios, sino también a partir de los mismos.[4]

- CMS: Sistema de control de contenido, en ingles Content Management System, hace referencia al programa o aplicación informática que permite la

---

[1] Instituto Nacional de Ciberseguridad, 2017, Disponible en la web https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf, p 8

[2] Ibíd., p. 9

[3] Ibíd., p. 10

[4] https://www.auditool.org/, 9 de junio de 2015, Disponible en la web https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque

creación de una estructura de soporte (framework) para la gestionar el contenido, principalmente aplica a portales WEB.

- Confidencialidad: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. [5]

- CVE: lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único. De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.
- Denegación de servicio: Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él.[6]

- Disponibilidad: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. [7]

- Exploit: Hace referencia a pequeñas aplicaciones programadas con el fin único de acceder al sistema que contiene la vulnerabilidad, para tomar su control o para provocar un funcionamiento indebido. Metasploit es un referente en lo que se refiere a exploits, un proyecto Open Source que recopila vulnerabilidades e informa de éstas, colaborando posteriormente con grandes compañías para desarrollar o mejorar sistemas de detección de intrusos y malware. [8]

- Fuga de datos: La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de

---

[5] Instituto Nacional de Ciberseguridad, 2017, Disponible en la web https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf, p 17

[6] Ibíd., p. 20

[7] Ibíd., p. 21

[8] Openwebinars, Febrero 2016, Disponible en https://openwebinars.net/que-es-el-pentesting/

personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.[9]

- Hacker: Define a un especialista en sistemas y según la RAE corresponde a un pirata informático, sin embargo, en el proyecto se hace referencia a la persona que busca vulnerabilidades en un sistema.

- Impacto: Grado de afectación de una vulnerabilidad o importancia que debe aplicarse.

- Incidente: Interrupción en el servicio proporcionado o disminución de la calidad en la prestación de estos, también hace referencia a la degradación del servicio.

- Incidente de seguridad: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.[10]

- Integridad: La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que, de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de estos.[11]

- Intrusión: Hace referencia a actividades sospechosas o anormales en el tráfico de red.

- Inyección SQL: Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que

---

[9] Instituto Nacional de Ciberseguridad, 2017, Disponible en la web https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf, p 22

[10] Instituto Nacional de Ciberseguridad, 2017, Disponible en la web https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf, p 24

[11] Ibíd., p. 25

puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.[12]

- Kali Linux: Conjunto de herramientas disponibles para el análisis de sistemas y que están diseñadas para pruebas y hacking ético.

- No repudio: El no repudio en el envío de información a través de las redes es capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser. El problema del control de autenticidad dentro de los sistemas de información a través de la Red, en relación tanto de la identidad del sujeto como del contenido de los datos, puede ser resuelto mediante la utilización de la firma electrónica (o digital). [13]

- Payload: Es un término al que no se puede dejar de hacer mención siempre que se habla de exploits. Por definirlo de una forma simple, un payload es una pequeña aplicación que aprovecha una vulnerabilidad afectada por un exploit para obtener el control del sistema víctima. Lo más común en un ataque es aprovechar una vulnerabilidad con un exploit básico para inyectar un payload para obtener el control del equipo al que atacamos. Si para los exploits hablábamos de Metasploit, para los payload, no tenemos que salir de esa aplicación para encontrar un subproyecto dentro del propio Metasploit, el denominado Meterpreter. Con esta solución, podremos cargar payloads que nos permitirán realizar multitud de acciones sobre nuestra víctima, desde acceder al sistema de archivos del equipo víctima a incluso que podamos ver en nuestra pantalla lo que muestra la pantalla del ordenador atacado.[14]

- Pentester: Termino usado para referirse a la persona encargada de las pruebas o test.

- Pentesting: Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos

---

[12] Ibíd., p. 25

[13] Instituto Nacional de Ciberseguridad, 2017, Disponible en la web https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf, p 27

[14] Openwebinars, Fecbrero 2016, Disponible en https://openwebinars.net/que-es-el-pentesting/

de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.[15]

- Pentest: Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad. Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de vulnerabilidades de seguridad. Tras la realización del ataque se presentará una evaluación de seguridad del sistema, indicando todos los problemas de seguridad detectados junto con una propuesta de mitigación o una solución técnica. La intención de una prueba de penetración es determinar la viabilidad de un ataque y el impacto en el negocio de un ataque exitoso.[16] Un test de penetración es el arte de ejecutar hacking ético donde un grupo de especialistas en seguridad de la información verifican y documentan la seguridad o los controles de protección de una plataforma tecnológica con las mismas técnicas de un hacker/cracker con el fin de lograr comprometer a algún activo alcanzable por algún punto de la superficie de ataque de un sistema.[17]

- Riesgo Informatico: Estimación de grado de exposición de uno o más activos de información ante la materialización de una amenaza y que pueda impactar significativamente o causar daños a la organización.

- Servidor: Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él. Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de software encargado de gestionar dicha información y ofrecerla.

- Spoofing: Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de *malware*. Los ataques de seguridad en las redes

---

[15] Ibíd.

[16] Instituto Nacional de Ciberseguridad, 2017, Disponible en la web https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf, p 28

[17] MCCLURE, SM Stuart. Hackers 2, Secretos y soluciones para seguridad de redes, Osborne McGraw-Hill 2001

usando técnicas de *spoofing* ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.[18]

- Website: Hace referencia al conjunto de servicios y archivos de un servidor web dentro de un esquema o estructura jerárquica definida.

[18] Instituto Nacional de Ciberseguridad, 2017, Disponible en la web https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf, p 61

INTRODUCCIÓN

Como un concepto de moda en las empresas es visto el pentest y cuando nos referimos al mismo estamos hablando del conjunto de herramientas y actividades que buscan encontrar y explotar las vulnerabilidades que tenemos en la red o a las cuales se ve expuesta nuestra plataforma con el principal objetivo de ser corregido a tiempo evitando un daño mayor dado que un atacante el cual puede ser externo o interno aproveche la falla. Para la Seguridad Informática el aumento de los ciberataques pone una alarma ante la cual no podemos dejar pasar por alto pequeños detalles que pueden ser la causa de grandes problemas de seguridad, por tanto este trabajo pretende ser una guía para un tema que reviste gran importancia en este ámbito y para las empresas que no deben desconocer que la seguridad es dinámica, por tanto algo seguro hoy mañana no lo es para ello se debe tener presente que lo que se busca es minimizar los riesgos, estar atentos a corregir las fallas y reaccionar rápidamente pues la tecnología también nos impulsa a mejorar.

Figura 1 Aumento titulares de Ciberataques 2014 - 2015

Fuente: https://www.certsi.es/blog/titulares-de-ciberseguridad-del-2015

Como se aprecia en la Figura 1 tenemos una aumento significativo en el número incidentes o ataques cibernéticos, pero no solamente se debe tener en cuenta que

incremento este número sino que adicionalmente hay incidentes como el robo de información que se ve reflejado en la Figura 2 en donde se aprecia que seguido a los ataques cibernéticos encontramos la fuga de información y por tanto esto es un reflejo de la importancia que debe darse a los incidentes relacionados con este tema dado que debemos estar atentos para proteger los sistemas usando para ellos las mejores prácticas y las herramientas, las metodologías que se ajusten a la necesidad. Además de ser relevante el hecho de contar con elementos de uso libre que aportan a la seguridad, solo debemos disponer del conocimiento para sacar provecho de estas.

Figura 2 Top de clasificación tipo de evento

Fuente: https://www.certsi.es/blog/titulares-de-ciberseguridad-del-2015

En el trabajo se documenta el paso a paso del pentest, el uso de una metodología sencilla de aplicar para una auditoria de este tipo, pero a la vez muestra que es muy importante no olvidar la fase de mantenimiento de los sistemas de información por cuanto las debidas auditorias y la seguridad informática permite a las empresas cerrar las brechas que generan las diferentes vulnerabilidades que van a aparecer en el día a día, así como lo relevantes que son las auditorias periódicas para contrarrestar ataques. El objetivo del trabajo no es ser una guía definitiva de cómo proceder en un pentest, pero si profundizar en un caso mostrar las fases, la metodología y herramientas usadas, sin embargo, debe ser evaluado el ambiente que se trabaje, dado que la aplicación de una metodología o el elaborar un set de pruebas es muy particular en cada empresa, así como, igualmente es importante valorar que el personal que efectué las pruebas, intentar asimilar la situación al entorno real de ataque y con ello el resultado será favorable para la entidad.

1 PLANTEAMIENTO DEL PROBLEMA

Teniendo en cuenta la evolución de las tecnologías, así como, el crecimiento de las empresas y la importancia de contar con información oportuna, además de la continuidad del negocio, el manejo de incidentes, la documentación de procedimientos de operación, el manejo protegido de la información física y digital, la seguridad respecto al control de acceso a la misma. Se evidencia que es muy importante para las empresas conocer el estado de sus sitios web, en razón a que deben estar verificando que el control de acceso a la información está correctamente administrado, ya sea por la herramienta de control de contenido del sitio o los procedimientos usados, que la información confidencial que se maneja y la de carácter público no se pierde, es sustraída por terceros. Que aparte de permitir exponer información el sitio, no es una puerta de acceso a la infraestructura interna o que pueda ser usado el portal para atacar a un tercero, de igual manera, el estar expuesto a internet el sitio triplica el riesgo de amenaza que puede afectar la confidencialidad e integridad de la información.

Es necesario de igual manera saber que los diferentes accesos publicados cuentan con las protecciones y controles necesarios para que solo los usuarios que requieren acceder a la información cuenten con dicho permiso, los que no deben acceder estén bloqueados para consultar, ver o modificar esos datos de acuerdo con el permiso que tengan.

Como principal problema que presenta en el sitio del Ministerio del Trabajo es que hay incidentes poco frecuentes pero en los cuales se ha detectado accesos no autorizados a las plataformas WEB de la entidad, puesto que los usuarios comparten las contraseñas de acceso, situación que se detecta en el proceso de soporte a usuario por parte de la mesa de servicio, de igual manera, el implementar nuevas soluciones que no están alineadas con los requerimientos de seguridad de una empresa de orden nacional y gubernamental como el Ministerio del Trabajo, requiere que la entidad evalué uno de los riesgos a los que está expuesta la información en un sitio web, teniendo en cuenta que puede haber expuesta información sensible de los ciudadanos o la entidad. De manera general, las empresas quieren ahorrar recurso humano y económico para prevenir daños o perdidas de información, pero la creciente demanda de tecnología, la globalización del acceso a la red (Internet) aumenta la superficie de ataque a la que se expone un sitio web, así mismo, aparecen más vulnerabilidades que pueden ser explotadas.

1.1 FORMULACIÓN DE PROBLEMA

¿Qué controles deben implementarse en el sitio web del Ministerio del Trabajo de la sede principal en la ciudad de Bogotá para las vulnerabilidades que con la aplicación de pruebas de pentesting se identifiquen?

1.2 OBJETIVOS

1.2.1 General

Identificar los controles necesarios para el sitio web del Ministerio del Trabajo en la sede principal en la ciudad de Bogotá aplicando pruebas de pentesting.

1.2.2 Específicos

- Determinar las vulnerabilidades existentes en el sitio web del Ministerio del Trabajo.
- Analizar las pruebas e información recolectada del sitio web del Ministerio del Trabajo.
- Listar las remediaciones o controles que deberían implementarse en la plataforma.

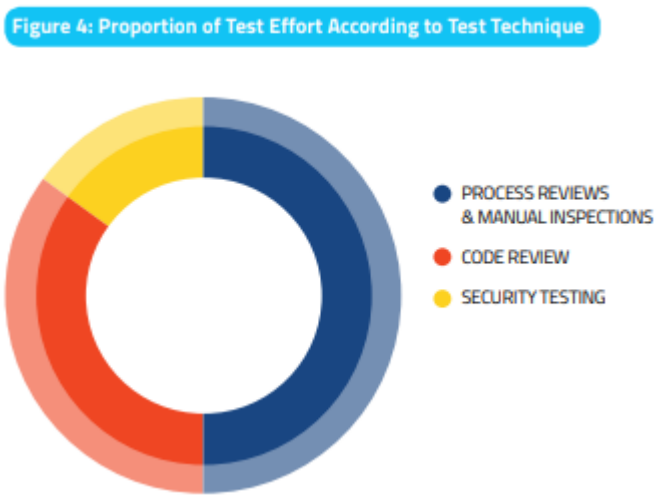
1.3 JUSTIFICACIÓN

El contar con un informe del estado del sitio entrega las pautas para garantizar que la información está protegida de accesos no autorizados, dando la confianza al administrador de este y los responsables de la administración de la información que no estarán expuestos a temas legales, por publicar información confidencial o datos que deben tener las garantías de protección y seguridad de la información contempladas por la ley.

El Ministerio del Trabajo desconoce el estado de la seguridad que tiene el sitio Web de la entidad y si la información almacenada en los servidores puede o ha sido sustraída, también se desconoce si las actualizaciones de seguridad aplicadas en la plataforma ha corregido las vulnerabilidades que tenía el sitio y que no está expuesto a las amenazas reportadas o si por el contrario cuenta con fallas de seguridad sobre sus sistemas, con esto la empresa podrá minimizar los riesgos existentes e implementar los recomendaciones entregadas en el informe, de igual manera podrá conocer cómo proceder y prevenir los ataques que reciba la empresa en su sitio.

Esto a la vez, tiene valor agregado a sus clientes dado que muestra el interés de la empresa por la seguridad de la información, los datos que tiene de sus funcionarios y ciudadanos, así como mantener una buena imagen respecto del uso adecuado de la tecnología e inversión de recursos públicos que maneja la entidad.

Figura 3 Proporción de esfuerzo de la prueba según la técnica aplicada



Fuente: https://www.owasp.org/images/1/19/OTGv4.pdf, Sep 2014, pág. 15

Las ventajas de contar con el reporte de estado de la seguridad pueden ayudar a evitar que a futuro las amenazas actuales sean mitigadas, eliminadas o su efecto si es el caso, que algunos de los riesgos expuestos por el informe sean asumidos por la entidad. La Figura muestra una representación de las técnicas de comprobación usadas para la revisión de las aplicaciones en las cuales vemos que solo un 15 % aproximadamente del esfuerzo es usado para realizar pruebas de seguridad de las cuales se debe sugerir que dichas pruebas sean adecuadas al entorno o ajustadas a la necesidad a fin de mejorar su efectividad.

Hacer un pentesting permite a una empresa contar con una foto del estado de la seguridad y tomar acciones para corregir los fallos que pueda encontrar en dicha evaluación, permite conocer si los controles implementados o que se tienen están funcionando correctamente, que las tareas proactivas como las auditorias y pruebas permitan encontrar soluciones antes de que ciberdelincuentes las aprovechen.

Con el panorama citado se puede decir que con el hecho de contar con pruebas periódicas podemos:

- Reducir el tiempo de respuesta y esfuerzo a la solución de las vulnerabilidades o riesgos, ya que si los identificamos podemos solucionarlo antes de ser explotados por el atacante.
- Tener un listado de malas configuraciones o posibles riesgos, así como el grado de afectación de estos, reduce la posibilidad de desencadenar un problema mayor se seguridad o legal para la empresa.
- Ayudamos a garantizar la confidencialidad de la información
- La disponibilidad de los datos es un aporte más que puede entregar esta buena práctica. Además de reducir el impacto de usar un plan de recuperación de desastres que normalmente dejaría tiempos de indisponibilidad de la plataforma o pérdidas de datos y tiempo, causados por un ataque.
- Por último, se puede decir que lo más importante que permite hacer estas pruebas es cumplir lo reglamentado en la ***ley Estatutaria 1581 De 2012,*** que obliga a garantizar la protección de datos.

1.4 DELIMITACIÓN

El proyecto tiene como alcance realizar las pruebas de pentest al sitio www.mintrabajo.gov.co para la empresa Ministerio del Trabajo en la sede principal en la ciudad de Bogotá.

En las pruebas se busca identificar si están correctamente asegurados los puertos expuestos a internet usando un escaneo de puertos, de igual manera se busca

analizar con las pruebas el nivel de seguridad si el sitio es atacado mediante inyección de código SQL pruebas que se desarrollaran en la página principal del sitio no buscar revisar o conocer el estado para los demás subniveles o categorías del sitio.

No contempla implementar un estándar para la entidad solo se entregará un informe detallado de las recomendaciones para solucionar las vulnerabilidades detectadas y listado de las fallas encontradas para que las mismas sean sometidas a estudio y futura aplicación o corrección por parte del personal encargado.

2 MARCO DE REFERENCIA

2.1 ANTECEDENTES

Como punto de referencia para el trabajo se ha revisado algunos documentos en los cuales se estudia la seguridad informática en los sitios web y se muestran herramientas aplicables a pruebas de vulnerabilidad, con estos se evalúa cuáles pueden ser aplicados al problema que se expone en el proyecto y se usan estos elementos en las pruebas aplicadas, a continuación se relacionan estos trabajos que se usaron como referencia al presente trabajo de investigación de análisis de la seguridad del sitio web del Ministerio del Trabajo aplicando pruebas de pentesting en la sede principal de la ciudad de Bogotá, no hay aplicación de pruebas pentesting en los últimos años de acuerdo con la información suministrada por el coordinador del grupo de Soporte Informático en la entrevista realizada en el año 2016 en el Ministerio, pero se valida que la entidad tiene previsto aplicar al menos una revisión anual del estado de la plataforma, así como encuestas tecnológicas que faciliten la recolección de información de la infraestructura de la entidad.

Cuadro 1 Estado del arte

Titulo/ Autor(es)	Resumen
"Desarrollo e implementación práctica de un PENTEST" Rafael Manuel Martí Talón	Muestra las fases que debe tener una auditoria de seguridad informática, listando las herramientas usadas en cada fase partiendo Penetration Testing Execution Standard, se amplía con fuentes actuales y lugares donde pueden aplicarse, así mismo indica herramientas más comunes que son usadas para las pruebas. El trabajo es realizado en Gandía, España en 2016 y por tanto es una referencia actualizada para apoyar el proyecto, el documento aporta o entrega una visión de las fases del pentest y las herramientas que se pueden usar en cada una de las fases, dichas herramientas en su mayoría están montadas sobre un kali Linux, también incluye una auditoria en la que se prueba la metodología y las herramientas con máquinas virtuales vulnerables en la red, en los resultados se encontraron que se cumplió el

	objetivo del trabajo mostrando como efectuar un pentest.[19]
"Análisis De Las Herramientas Para El Proceso De Auditoría De Seguridad Informática Utilizando Kali Linux" Ericka Yánez Cedeño	Resume las herramientas que pueden usarse para realizar tareas de auditoría y seguridad, además de presentación y análisis de las que se usan en cada fase del hacking ético. [20] De este trabajo se toma referencia de las herramientas utilizadas, el uso de estas, así como la aplicación unas de ellas para el desarrollo del trabajo, facilitando la documentación del proyecto. El documento muestra las herramientas necesarias para la capacitación o introducción al mundo de la seguridad informática y que conceptos debe manejar un hacker ético. Se listan unas metodologías usadas y se presenta un comparativo de las mismas, a fin de facilitar un panorama y a la vez ayudar a seleccionar una metodología de acuerdo con el escenario donde se pretende realizar el pentesting. Se lista en detalle la evolución que ha tenido Kali Linux y las mejoras de cada versión. Se profundiza en cada una de las opciones que tiene disponibles las herramientas, hay incluso el detalle de como instalar una máquina virtual para las pruebas que se requieren aplicar y muestra cómo puede hacerse uso de estas en cada fase del proceso de pentesting. El proyecto tiene mucha profundidad en las herramientas y detalle de uso, aporta a la investigación del como ejecutar un pentesting y que debo usar en cada fase.

[19] Martí Talón, 2016, Desarrollo e implementación práctica de un PENTEST, Disponible en la web https://riunet.upv.es/handle/10251/70164

[20]Yánez Cedeño, 2016, Análisis De Las Herramientas Para El Proceso De Auditoría De Seguridad Informática Utilizando Kali Linux, disponible en la web http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf

“Metodológica Para Determinar La Seguridad En Una Aplicación Web” Martha Ascencio Mendoza Pedro Julian Moreno Patiño	Presenta una propuesta metodológica para determinar la seguridad en una aplicación Web, analiza los conceptos y fundamentos de la seguridad en aplicaciones, lista herramientas usadas para el análisis de seguridad, muestra las principales características de las metodologías existentes, este documento de 2011[21], este documento permite profundizar en algunos conceptos necesarios para entender y profundizar las pruebas, además de entregar unos lineamientos para la aplicación de las pruebas al sitio web. En las metodologías usadas se trabaja con OWASP e ISSAF, igualmente se trabaja el estándar ISO 27001, con el documento se logra presentar varias herramientas para explotar las vulnerabilidades de luan aplicación WEB y se comparan las características de las metodologías tratadas se hace énfasis en la documentación del proceso y las características generales de los informes de seguridad, igualmente presenta las características de ciclo de desarrollo de software recalcando que la fase manteniendo es muy importante por cuanto debe estar en constante evaluación para garantizar la seguridad de los desarrollos.

Fuente: El autor

2.1.1 Marco Contextual

El Ministerio del Trabajo tiene su origen en 1938 mediante una ley en la cual se crea el Ministerio del Trabajo, Higiene y Previsión Social; posteriormente se trasforma en departamento administrativo de la antigua superintendencia de cooperativas hacia 1981, hacia 2002 con el mandato de Álvaro Uribe Vélez se fusiona el Ministerio del

[21] Ascencio Mendoza & Moreno Patiño, 2011, Repositorio Universidad Tecnologica de Pereira http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf?sequence=1

Trabajo junto con el Ministerio de Salud creando el Ministerio de la Protección Social, el cual para 2012 es dividido en el mandato de Juan Manuel Santos generando unos nuevos objetivos para las nuevas entidades resultantes de la división de dicho Ministerio.

Estructura organizacional del área informática, los cargos y funciones: El Ministerio de encuentra dividido en dos viceministerios y una secretaria general áreas de las cuales dependen las demás oficinas y departamentos, los cuales a su vez cuentan con grupos de trabajo, para el caso puntual se tiene el grupo de soporte informático ubicado dentro del organigrama en la Subdirección Administrativa y Financiera la cual depende a su vez de la Secretaria General.

Coordinador: Se encarga de la supervisión de los contratos de servicios Informáticos, coordinar actividades de soporte y mantenimiento con los proveedores, además de los servicios que están en outsourcing. Atender los requerimientos de las diferentes areas en temas de soporte tecnologico.

Profesional Especializado: Soporte a los servidores, Bases de datos y Aplicativos del área Administrativa y financiera (Correspondencia, Bancos, Inventarios y Cobro) y Las Direcciones Territoriales de Bogotá y Cundinamarca.

Administrador de bases de Datos - DBA : Profesional certificado en Oracle encargado de la administración de las diferentes bases de datos, monitoreo de las mismas, manteniemiento y verificación de las copias de seguridad.

Técnico Administrativo: Encargado de realizar las publicaciones de contratos y anexos de los mismos en la página del secoop de las 32 Direcciones Territoriales y las Oficinas Especiales.

Auxiliar Administrativo: Se encarga del apoyo a los demás cargos del grupo, realizando gestion de la documentación en el sistema de correspondencia.
Outsourcing Mesa De Servicio
Grupo de Une , el equipo outsourcing o esta conformado por:

- Coordinador
- Dos especialistas en servidores
- Un administrador de redes
- Un WebMaster: encargado de publicaciones en la página web.
- Un Tecnologo encargado de telefonía Ip y herramienta de conferencias
- Un técnico especialista para Impresoras y Scanners
- Técnicos de soporte en sitio nivel 1 para la sede central y en las principales sedes del Ministerio.

Teniendo como necesidad determinar el estado de la seguridad de una plataforma de servicios como lo es la página WEB del Ministerio del Trabajo y adicionalmente en aras de garantizar que los servicios mantengan su operación, confiabilidad y disponibilidad para el ciudadano es necesario que se revisen los antecedentes en materia que tiene el análisis de intrusión para el sitio WEB de la entidad.

2.1.2 Organigrama.

Dentro del organigrama general se encuentra el grupo de soporte informático y la oficina de información y la Comunicación – TIC, la primera es la encargada de toda de infraestructura de cómputo y soporte del mismo, la segunda área es encargada de la generación y administración de proyectos.

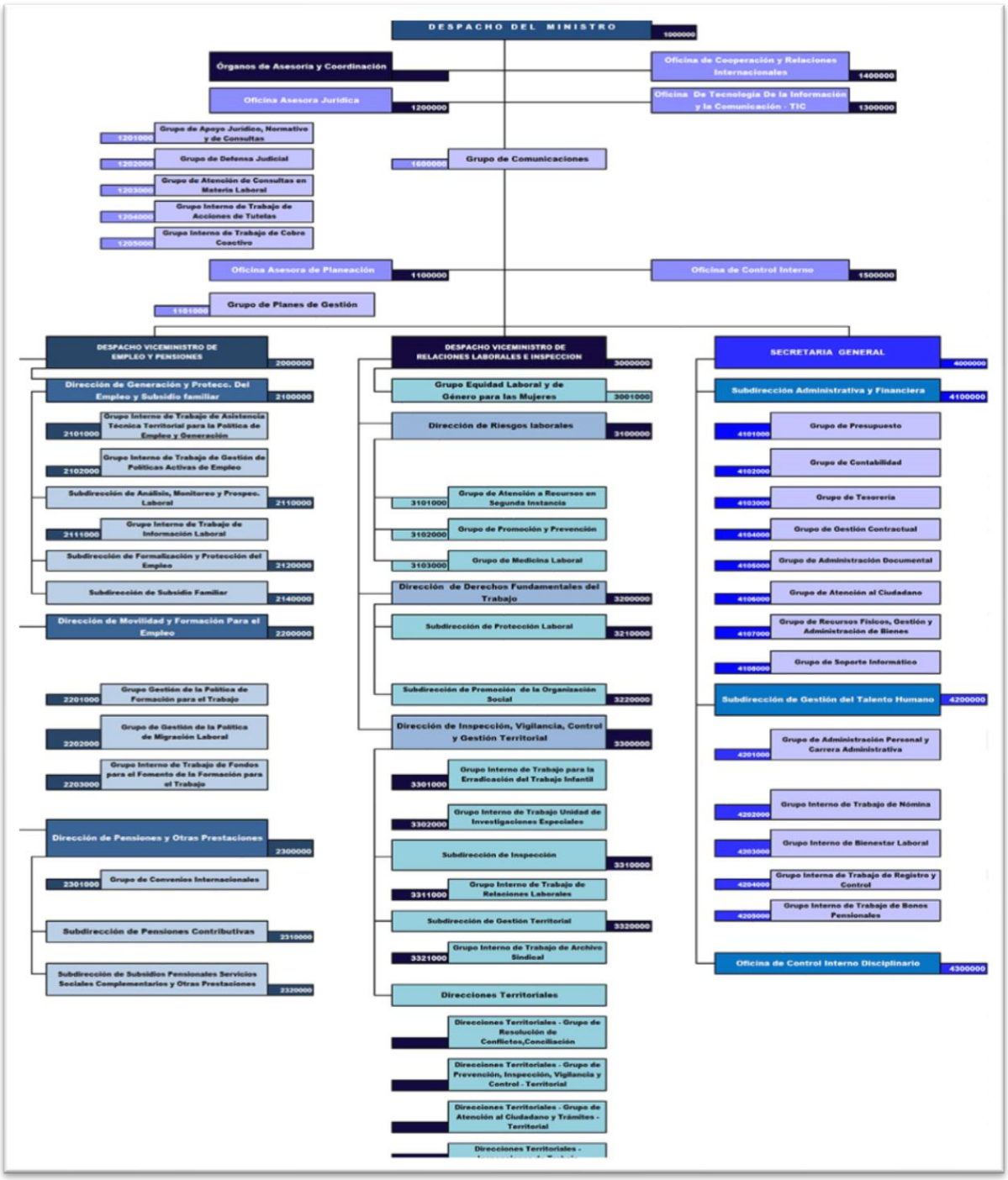
Mision: Formular, adoptar y orientar la política pública en materia laboral que contribuya a mejorar la calidad de vida de los colombianos, para garantizar el derecho al trabajo decente, mediante la identificación e implementación de estrategias de generación y formalización del empleo; respeto a los derechos fundamentales del trabajo y la promoción del diálogo social y el aseguramiento para la vejez.

Vision: Para 2018, ser reconocidos como el Ministerio que promueve la protección, vinculación, formalización y el acceso al trabajo de los colombianos en las diferentes etapas de su ciclo de vida laboral, en el marco del trabajo decente; gestionando la consolidación del Sistema de Protección para la vejez y la articulación intersectorial. El sitio WEB del Ministerio tiene varios servicios disponibles a los ciudadanos entre los cuales estan:

- Centro de orientacion y atencion laboral
- PQRSD (Peticiones,quejas, reclamos, solicitudes y denuncias)
- Tramite empresas temporales
- Fuente información laboral de Colombia (FILCO)
- Elabora (Elaboración Hoja de Vida)
- Mi Calculadora (ayuda a calcular la liquidación de prestaciones sociales)
- Biblioteca Virtual
- Sistema de Información de Gestión (SIG)
- Sistema de información integrado para la identificación, registro y caracterización del trabajo infantil y sus peores formas (SIRITI).
- Ventanilla unica de tramites y servicios
- Agendamiento WEB

Entre estos y otros servicios que pueden ser encontrados en la pagina principal del sitio o alguna de sus sesiones internas.

Figura 4 Organigrama Mintrabajo



somos/organigrama.html

2.2 MARCO TEÓRICO

2.2.1 Seguridad Informática

También conocida como ciberseguridad o seguridad de las tecnologías, abarca un conjunto de medidas técnicas que tiene como principal objetivo garantizar la confidencialidad, integridad y disponibilidad de la información, además puede incluir propiedades como autenticidad, responsabilidad, fiabilidad y el no repudio. No puede confundirse con seguridad de la información la cual solo busca proteger la información mientras que la anterior involucra todos sus elementos e infraestructura.

En la búsqueda de proteger la información y salvaguardar los principios de esta (confidencialidad, integridad y disponibilidad), la seguridad informática emplea metodologías y herramientas que ayudan proteger la información de las diferentes amenazas, por esto las áreas encargadas de la seguridad informática están con la responsabilidad de prevenir, mitigar, evadir, así como por último asumir el riesgo que nos afecta.

Podemos definir qué es la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.[22]

La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.[23]

Este documento expone un proceso llevado a cabo para identificar los controles que deben aplicarse a las vulnerabilidades encontradas en unas pruebas de penetración, también conocidas como pentesting, que de acuerdo con la comunidad OWASP (Open Web Application Security Project) consisten básicamente en “probar una aplicación de forma remota para encontrar vulnerabilidades sin conocer los

[22] ¿Qué es la seguridad informática y cómo puede ayudarme?, 9 septiembre de 2016. Disponible en internet http://www.viu.es/la-seguridad-informatica-puede-ayudarme/

[23] ¿Qué es la seguridad informática y cómo puede ayudarme?, 9 septiembre de 2016. Disponible en internet http://www.viu.es/la-seguridad-informatica-puede-ayudarme/

procesos internos de la aplicación". El objeto de las pruebas es encontrar fallos en la seguridad de información y que para ello se efectúan en contexto de hacking ético (ethical hacking) para que dichas fallas sean corregidas antes de ser explotadas por los atacantes.

Las fases del pentest básicamente tienen las siguientes etapas:

- Reconocimiento
- Escaneo
- Enumeración
- Acceso
- Mantenimiento

Para las pruebas actualmente se tienen herramientas que automatizan dichos procesos en cada fase para evaluar la seguridad de la información, por ejemplo, en el sistema operativo Kali Linux podemos encontrar diferentes herramientas que se clasifican o especializan en cada una de las fases anteriormente citadas que al final permiten generar un reporte de la vulnerabilidad encontrada.

Según la ISO 27000 en la cual se tiene un panorama general y vocabulario para los sistemas de gestión de la seguridad de la información ISO, una vulnerabilidad se define como: "una debilidad de un activo o control que puede ser explotado por una o más amenazas", además se define que una amenaza es cualquier potencial causa de un incidente no deseado, con posibilidad de generar daño a un sistema u organización", en ese orden de ideas es posible indicar que una amenaza puede explotar una debilidad una vez la encuentre, esta debilidad puede ser originada en el diseño, implementación, configuración, mantenimiento y operación del sistema o activo.

2.2.2 Vulnerabilidades en los sitios WEB

Como es esperado para un atacante hoy en día el principal objetivo va a ser la información, así que debido a esto muchos profesionales de la seguridad se han preocupado por apoyar el proyecto OWASP (Open Web Aplication Security Project) el cual tiene como primer paso crear conciencia sobre la seguridad en aplicaciones, para esto se procede revelar algunos riesgos.[24]

OWASP, entrega un listado de los 10 riesgos más críticos que a nivel de nos de dichas vulnerabilidades, con aras de conocer las consecuencias de las vulnerabilidades más relevantes que existen en la web, dentro de los cuales menciona los siguientes:

[24] (Foundation, 2017)Foundation, Owasp, noviembre de 2018, Disponible en la Web https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

A1: 2017-Inyección: Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados. OWASP Top 10

A2:2017 – Pérdida de Autenticación: Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, llaves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios de manera total o permanentemente.

A3:2017 – Exposición de datos sensibles: Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.

A4:2017 Entidades Externas XML (XXE) - Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).

A5:2017 – Pérdida de Control de Acceso: Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.

A6:2017 – Configuración de Seguridad Incorrecta: La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc.

A7:2017 –Secuencia de Comandos en Sitios Cruzados (XSS): Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (defacement) los sitios web, o redireccionar al usuario hacia un sitio malicioso.

A8:2017 - Deserialización Insegura: Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

A9:2017 – Componentes con vulnerabilidades conocidas: Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.

A10:2017 –Registro y Monitoreo Insuficientes: El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos. [25]

Figura 5 Pilares de la seguridad de la información

Fuente: http://www.inseguridadinformatica.com/2012/03/introduccion-la-seguridad-de-la.html

[25] (Foundation, 2017) Foundation, Owasp, noviembre de 2018, Disponible en la Web https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf, Pág. 6

“La Seguridad Informática se basa en tres principios fundamentales”[26]:

✓ Confidencialidad

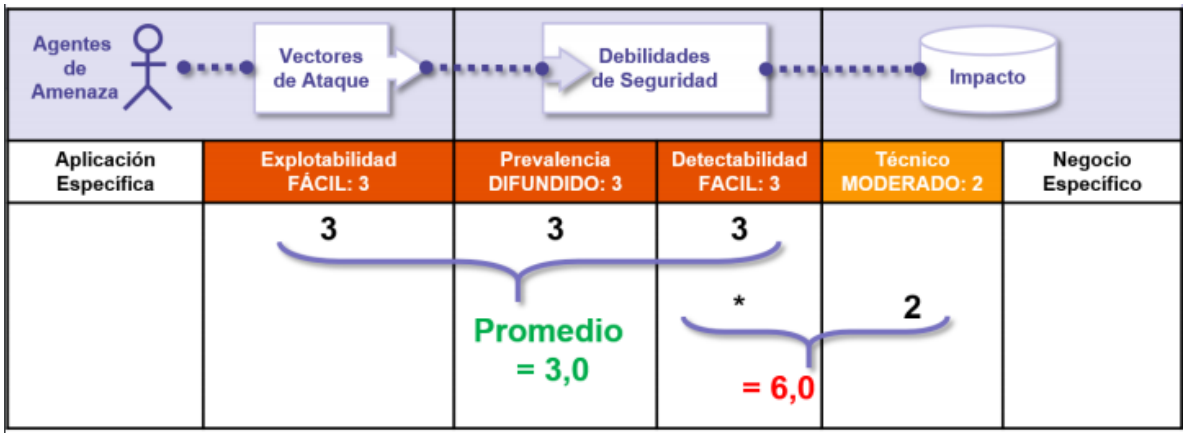
✓ Integridad

✓ Disponibilidad

Teniendo en cuenta que la seguridad es de gran importancia para fortalecer el activo más importante que pueda tener cualquier organización que es la información, es que la seguridad informática se convierte en un pilar fundamental y que en la figura 5 se pueden observar las dimensiones o pilares básicos de la misma: confidencialidad, integridad y disponibilidad de la información, además debe tenerse presente que tiene un valor estratégico, económico y legal para una organización, puesto que la misma ayuda a garantizar la continuidad e imagen de una entidad.

2.2.3 Factores de Riesgo

Figura 6 Resumen de factores de riesgo Top 10



Fuente: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

De la figura 6, se puede indicar que los factores pueden ajustarse a la situación particular de la empresa o del sistema y pueden ser el impacto un factor que para algunos es dinámico, por ello es importante su revisión periódica.

[26] ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP EDICIONES. ARGENTINA. 1997. Pág. 22

Figura 7 Resumen de factores de riesgo Top 10

Riesgo	Agentes de Amenaza	Vectores de Ataque	Debilidades de Seguridad		Impacto		Puntuación
		Explotabilidad	Prevalencia	Detectabilidad	Técnico	Negocio	
A1: 2017- Inyección	Específico de la Aplicación	FACIL: 3	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	8,0
A2: 2017 - Pérdida de Autenticación	Específico de la Aplicación	FACIL: 3	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A3: 2017 - Exposición de Datos Sensibles	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A4: 2017 - Entidad Externa de XML (XXE)	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	7,0
A5: 2017 - Pérdida de Control de Acceso	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	6,0
A6: 2017 - Configuración de Seguridad Incorrecta	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A7: 2017 - Secuencia de Comandos en Sitios Cruzados (XSS)	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A8: 2017 - Deserialización Insegura	Específico de la Aplicación	DIFICIL: 1	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	5,0
A9: 2017 - Componentes con Vulnerabilidades Conocidas	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	MODERADO: 2	Específico de la Aplicación	4,7
A10: 2017 - Registro y Monitoreo Insuficientes	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	DIFICIL: 1	MODERADO: 2	Específico de la Aplicación	4,0

Fuente: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Del anterior Figura 7, se puede revisar que la valoración también debe incluir una valoración que permita considerar las amenazas e impactos del negocio propios de la aplicación u organización que se desea evaluar, esos factores son particulares y el grado de afectación que puede ocasionar una vulnerabilidad afecta menos o más a cada negocio o sistema, igualmente en cada ambiente se deben considerar otras amenazas o riesgos que no se encuentran en este listado.

2.2.4 ISO 27001

Corresponde a una norma internacional expedida por la Organización Internacional de Normalización (ISO), en la cual se detalla cómo gestionar la seguridad de la información en una empresa. Se abarcan temas que indican como proteger los pilares de la información: la confidencialidad, integridad y disponibilidad enunciados anteriormente y dado que la información en uno de los activos más importantes de una empresa muchas de ellas se certifican en el cumplimiento de esta normativa.

La última revisión de esta norma es la ISO/IEC 27001:2013, corresponde a la primera revisión que efectuada a la norma ISO 27001:2005. Entre las principales ventajas de esta versión, esta:

- Su flexibilidad para implementación y por ser un estándar puede implementarse en toda empresa sin importar su tamaño o tipo.
- Tiene una fácil integración con otras normas o estándares de gestión relacionadas

2.2.5 Control

El concepto de “Control” corresponde a lo que permite garantizar que cada aspecto, que se valora con un cierto riesgo, queda cubierto y auditable, el ¿Cómo se hace? tiene como respuesta muchas formas posibles de realizarse o cumplirse, para ello según la ISO/IEC 27002:2013, los controles que se enuncian están separados en 14 dominios de seguridad y se enuncian 114 controles aproximadamente en la norma. De la norma se extraen los siguientes dominios:

1. Política de seguridad
2. Aspectos organizativos de la seguridad de la información
3. Seguridad ligada a los recursos humanos
4. Gestión de activos
5. Control de accesos
6. Cifrado
7. Seguridad física y del entorno
8. Seguridad operativa
9. Seguridad en las telecomunicaciones
10. Adquisición, desarrollo y mantenimiento de los sistemas de información
11. Relaciones con los proveedores
12. Gestión de los incidentes en la seguridad de la información
13. Aspectos de seguridad en la gestión de la continuidad del negocio
14. Cumplimiento

De los anteriores dominios, se toma como referente los relacionados con el control de acceso, la Seguridad en las telecomunicaciones, Adquisición, desarrollo y mantenimiento de los sistemas de información, Relaciones con los proveedores y por último Gestión de los incidentes en la seguridad de la información, es decir, aquí se resume que de los 14 dominios hay controles relacionados se tienen 6 en los cuales se puede revisar que controles se deben evaluar o ajustar para un proyecto de pentesting, sin embargo, sobra decir que cada entidad funciona diferente y en algunas es probable que se requiera revisar otros dominios.

De la gestión de los incidentes en la seguridad de la información, se puede resumir que para los incidentes de seguridad se puede proceder de dos formas:

1. Proteger y proceder, es decir, cerrar, apagar, desconectar, esto solo soluciona momentáneamente.
2. Seguir y perseguir, esta opción va a permitir analizar paso a paso el accionar del enemigo y solucionar la falla.

2.3 HACKING ÉTICO

Para entrar en materia respecto al tema es claro que el hacking ético es aquel que nos permite efectuar pruebas controladas de intrusión con las cuales podemos establecer el nivel de seguridad que tienen los sistemas informáticos y con esto poder protegerlos de ataques futuros.

2.3.1 El Hacker Ético

El termino hacker es definido por la RAE como “pirata informático o persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora”[27], pero más allá de entrar en esa discusión lo que es preciso indicar es que gracias a estos especialistas y apasionados por la tecnología se pueden encontrar fallos en los sistemas y proceder a corregir dichas vulnerabilidades, por esto el termino hacker debe unirse al concepto de ético, a fin de indicar que estos especialistas son los encargados de efectuar las pruebas en nuestros sistemas para mejorar la tecnología y los sistemas que todos usamos.

2.3.2 Aplicación Web

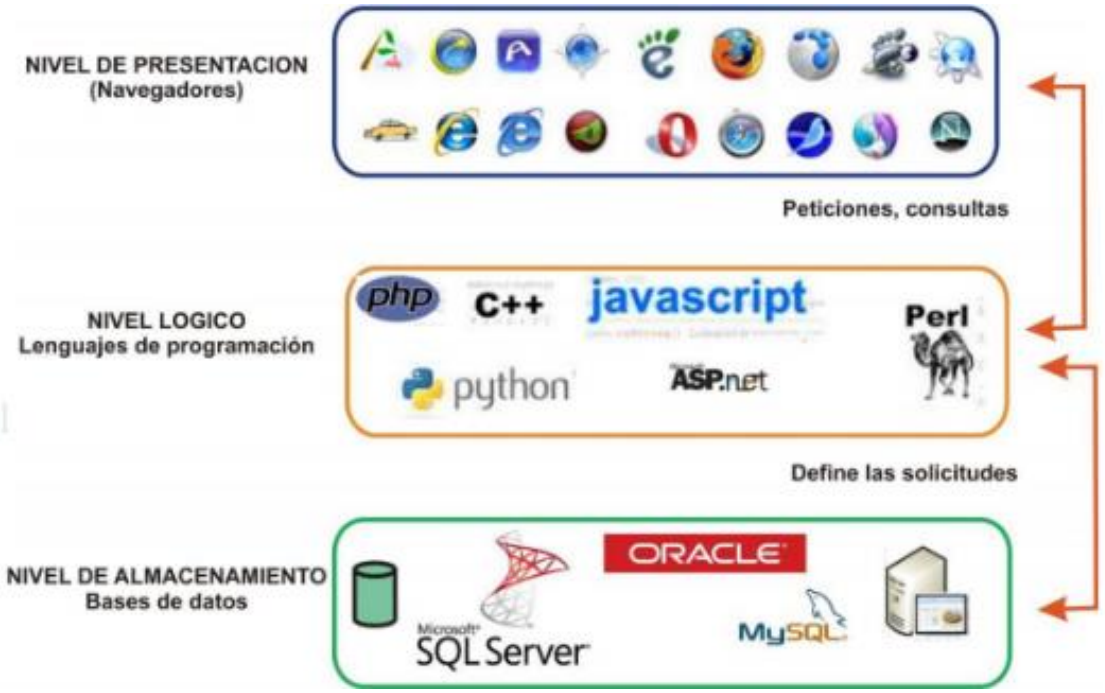
En ingeniería de software una aplicación WEB es aquella a la cual se accede mediante el uso de un navegador WEB usado sobre una red, ya sea local o externa, es decir, sobre internet. Las aplicaciones usan diferentes lenguajes que deben ser soportados por el navegador y de igual manera estar alineados a un estándar.

La arquitectura base de una aplicación WEB puede estar dividida en tres (3) niveles: nivel de presentación, nivel lógico y nivel de almacenamiento o base de datos ver.

Figura 8 Arquitectura WEB - 3 Capas.

[27] RAE, Actualizacion 2017, Disponible en internet http://dle.rae.es/?id=JxlUKkm

Figura 8 Arquitectura WEB - 3 Capas



Fuente: http://datateca.unad.edu.co/contenidos/301122/UNIDAD_3/L.Material12-ModuloSeguridaddeAplicacionesWebUNAD.pdf

El proceso normal cuando un cliente realiza una petición a un servidor sigue los siguientes pasos:

A. Un usuario accede a una URL, usando para ello un enlace de un documento HTML o introduciéndola directamente en la barra de direcciones del navegador.
B. El cliente web (navegador o explorador) descodifica la URL, separando sus diferentes componentes. En este paso identifica el protocolo de acceso, la dirección DNS o IP del servidor, el puerto (por defecto es 80) y el objeto solicitado del servidor.
C. Paso siguiente abre una conexión TCP/IP con el servidor, llamando al puerto TCP.

D. En la petición se hace uso de un comando (GET, POST, HEAD, etc..), otras variables como capacidades del navegador, dirección del objeto - URL siguiente a la dirección del servidor entre otros parámetros.
E. Se retorna una respuesta al cliente con un código de estado y el tipo de dato MIME de la información devuelta seguida de la propia información requerida.
F. Paso seguido se cierra la conexión TCP. En caso de no usar el modo HTTP Keep Alive, se repite el proceso para cada acceso.

Es importante indicar que para el dialogo entre servidores Web se usan mensajes de texto y tienen dos tipos de mensajes, uno para respuesta y otro para las peticiones.

2.3.3 Lenguaje

Un lenguaje de programación es básicamente un sistema estructurado de comunicación, similar al humano, el cual permite comunicación por medio de signos, ya sean palabras, sonidos o gestos. Se refiriere a los aparatos, este sistema está organizado para que se entiendan entre sí y a su vez interprete las instrucciones que debe ejecutar.[28]

2.3.3.1 Php

(Acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto usado para el desarrollo web y que puede ser incrustado en HTML, a diferencia de algunos lenguajes PHP no requiere ser compilado para ejecutarse.[29]

2.3.3.2 Javascript

Abreviatura usada para definir el lenguaje interpretado y llamado normalmente como JS, está orientado a objeto y hace uso de clases, puede trabajar del lado del cliente y del servidor, dentro de su diseño se asimila a C y tiene una estructura como la de Java en nombres y convenciones, pero el uso y semántica son diferentes.

2.3.3.3 Html

Abreviatura usada para definir el lenguaje de marcas de hipertexto, el cual es usado en el desarrollo de páginas Web, actualmente se tiene la versión 5.[30]

---

[28] Morales, 2014, Disponible en la web https://colombiadigital.net/actualidad/articulos-informativos/item/7669-lenguajes-de-programacion-que-son-y-para-que-sirven.html

[29] PHP, Enero de 2017, Disponible en internet http://php.net/manual/es/intro-whatis.php

[30] Alvarez, M. A.,Abril de 2017 Disponible en internet https://desarrolloweb.com/articulos/que-es-html.html

2.4 MARCO CONCEPTUAL

En Colombia y en el mundo de manera general, los datos de las empresas, entidades, y demás organizaciones son unos de los activos más valiosos con los que cuentan cada una de ellas, por lo que es de mucha importancia que quienes requieren acceso a la información puedan hacerlo de manera confiable, segura, oportuna en la que se garantice la integridad y confidencialidad de esta.

Para lograr esa autenticidad, integridad y confidencialidad de la información, se debe garantizar que una aplicación Web, cuente con todos los componentes de seguridad, los cuales ayuden a evitar, bloquear, mitiguen los riesgos y amenazas que afectan esta cualidades o pilares de la información, por tal motivo mediante este proyecto se busca evaluar los niveles de seguridad que tiene.

Se definen algunos conceptos que van a ser objeto de análisis en el presente proyecto y que se quieren medir para conocer el estado de estos.

2.4.1 Hacking Ético:

El hacking ético nos permite encontrar las vulnerabilidades en nuestras aplicaciones y sistemas de manera anticipada y preventiva, facilitando prevenir y corregir dichas fallas, de esta manera estamos atentos a actuar ante un ataque puesto que ya conocemos nuestros puertos que se encuentran abiertos o no están asegurados, el software que no está debidamente parchado, a fin de poder reaccionar de manera oportuna.

2.4.2 Protocolo HTTP

El http es un protocolo de transferencia de hipertexto que trabaja cliente-servidor permitiendo el intercambio de información entre un cliente que usa un navegador web y los servidores http. Funciona sobre servicios de conexión TCP/IP que normalmente cuenta con un proceso que escucha u opera sobre el puerto 80 como estándar para establecer la comunicación con los clientes los cuales una vez se conectan al servidor el protocolo TCP se encarga de garantizar dicho intercambio de información usando operaciones de solicitud / respuesta, en estas operaciones el navegador siempre recibe una respuesta del servidor bajo un código catalogado bajo 5 categorías que indican el estado de la solicitud, es decir, respuestas informativas, de error o de redirección.

2.4.3 Protocolo TLS

Es un protocolo que permite la trasferencia segura de datos, el cual permite establecer un canal en el cual se cifra la información que se intercambia, permitiendo una protección a los datos ante una interceptación de estos o el robo.

El protocolo se divide en dos capas Handshake y el protocolo de registro, la primera capa se encarga de negociar los parámetros de seguridad, el protocolo de registro se encarga de fragmentar, comprimir y cifrar los datos, para esto usa el MAC (Código de autenticación del mensaje).
La Autenticación Web: Consiste en un mecanismo mediante el cual se valida el acceso al recurso de la aplicación o servidor y la misma puede ser:

- Básica
- Digest
- NTLM
- Biometría**.**

STRIDE y DREAD: Son modelos mediante los cuales se identifican y representan amenazas de una aplicación. El esquema STRIDE está compuesto de los siguientes pasos: Suplantación de identidad, falsificación, repudio, revelación de información, denegación de servicio y elevación de privilegios. Para el esquema DREAD se divide en: Daño potencial, reproducibilidad, explotabilidad, usuarios afectados y descubrimiento.
Pruebas de penetración: Para las pruebas de penetración disponemos de las siguientes fases:

- Reconocimiento: Esta fase es la que permite evaluar el objetivo a atacar y las técnicas o métodos que puedo usar para efectuar el plan de testeo.
- Escaneo: Se evalúa la infraestructura que se va a atacar
- Enumeración En esta fase se estable cuáles son las fallas que presenta el objetivo, es decir, se identifica cuáles son los puertos que serán el blanco del ataque.
- Acceso: En esta fase se efectúa propiamente la vulneración del sistema
- Mantenimiento: La última fase permite al atacante eliminar huellas, guardar el camino a seguir para un próximo ataque, encontramos que puede alterarse privilegios, etc.

Estas fases también están sujetas a cambios dependiendo de la metodología que se use, pero guardan una relación en los pasos a seguir, es decir, cambian los pasos a seguir, pero se evalúa otros aspectos como por ejemplo la información que se tiene del sistema a atacar, la plataforma, la disposición de las pruebas, por último, hace referencia a que las pruebas se hagan internamente o sean realizadas desde afuera y con las misma información o características que tiene un ataque real. Este análisis puede ser llamado caja negra, caja gris o caja blanca en los cuales la variable será la información que se tiene del objetivo a atacar. A continuación, se detallan los tipos de prueba:

- Black-Box: no se cuenta con conocimiento alguno sobre el objetivo a probar, es la prueba más similar a la de un atacante externo, el cual escanea para obtener la información sobre el objetivo de la prueba.

- White-Box: Para este tipo de prueba la información sobre el objetivo o sistema que se va a auditar es suministrada, pueden ser datos como sistema operativo que se usa, segmento de red y topología, entre otros, aquí la idea es minimizar los tiempos.
- Grey-Box: Esta opción permite hacer un uso combinado de las anteriores, se tiene un conocimiento parcial del objetivo.

Cuadro 2 Clasificación de la Severidad de una Vulnerabilidad según Microsoft.

VALORACIÓN	DEFINICIÓN
Crítico	Vulnerabilidad que podría dar lugar a la propagación de un gusano de Internet si no interviene el usuario.
Importante	Vulnerabilidad que podría poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios; o bien la integridad o disponibilidad de los recursos de procesamiento.
Moderado	La explotabilidad podría reducirse en gran medida a través de diversos factores, como una configuración predeterminada, auditoría o dificultad para aprovechar la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Fuente: https://www.microsoft.com/latam/technet/seguridad/boletines/rating.mspx

El impacto mide de las vulnerabilidades es usado para establecer la importancia y la necesidad de aplicar un parche de seguridad que corrija la falla, esto es aplicado a los boletines de seguridad que genera Microsoft.

OWASP (Open Web Application Security Project): es una metodología de pruebas para seguridad de aplicaciones la cual busca establecer la relación costo beneficio que otorga el contar con una aplicación segura. Además, que usando esta metodología se contempla que para este proyecto se adapte la misma bajo el estándar de pruebas de caja gris el cual tiene las mismas fases de pruebas de caja negra, pero pues al conocer más información de la empresa se pueden adaptar ciertas pruebas para evaluar aquellos aspectos que se consideran más sensibles ya que de igual manera no se cuentan con recursos ilimitados de tiempo para las pruebas.[31]

[31] Foundation, 2008, Disponible en la web https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

2.5 MARCO LEGAL

Dentro del marco legal del proyecto se incorpora la normatividad que está relacionada con el uso de servicios tecnológicos y el acceso a la información, indica que se especifica a manera general la normatividad que de una u otra manera es aplicable al presente proyecto

2.5.1 Ley 527 de 1999

Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

2.5.2 Ley 599 de 2000

Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de violación ilícita de comunicaciones, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el Acceso abusivo a un sistema informático.

2.5.3 Ley 962 de 2005

Dicta disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o presten servicios públicos.

2.5.4 Ley 1273 de 2009

Modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[32]. En esta ley se enmarcan los delitos contra la información en sus principios fundamentales la confidencialidad, la integridad y la disponibilidad.

2.5.5 Ley 1581 de 2012

Esta ley fue expedida por el congreso el 17 de octubre de 2012 y es obligatoria para todas las empresas desde abril 18 de 2013, conocida como Ley Estatutaria de Protección de Datos Personales (LEPD) y existe la ley 1266 de 2008 para el tema de datos personales financieros, en esta última se estipula lo referente a los datos personales que se recolectan y usan para cálculo de riesgo crediticio

---

32 Congreso de Colombia, Ley 1273 de 2009 [En línea], https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf, [Citado el 17 de septiembre de 2018]

2.5.6 Decreto 2693 de 2012

Establece los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.

2.5.7 Ley 1712 de 2014

Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, en esta ley se busca es regular el derecho de acceso a la información pública, es decir que los ciudadanos y entidades del estado puedan interactuar bajo unos principios claros de que información puede ser divulgada y bajo que procedimiento se pueda hacer.

2.5.8 Ley 1753 de 2015

Ley en la cual se expide el Plan Nacional de Desarrollo 2014-2018[33]

33 Congreso de Colombia, Ley 1753 de 2015, [En linea], http://www.mincit.gov.co/loader.php?lServicio=Documentos&lFuncion=verPdf&id=78676&name=LEY_1753_DE_2015.pdf&prefijo=file, [Citado el 17 de septiembre de 2018]

3 METODOLOGIA

Para el proyecto se estructuraron tres fases, en una primera etapa se realiza una revisión de los antecedentes o investigación bibliográfica del tema, en una segunda parte se analiza o documenta cómo estaba estructurado el Ministerio del Trabajo y su grupo de soporte Informatico, a fin de poder mirar cómo está conformada el área de sistemas, por último, se diseña un plan de controles para la página Web de la entidad.

Se realiza una búsqueda de fuentes de información entre las cuales se revisan libros, artículos y tutoriales relacionados con el tema de la investigación, donde se identifica la más confiable y que permitía apoyar la realización del proyecto.

Para la segunda fase se procede a documentar y conocer el Ministerio del Trabajo, donde se identifican las particularidad de cómo está estructurado el grupo de soporte Informatico, cuáles son los procedimientos o procesos que deben surtirse para actualizar un contenido en la página web de la entidad, teniendo en cuenta que todas las entidades no funcionan igual, de igual manera se revisa como se efectúan las auditorías internas, como se revisa la seguridad de la plataforma y que elementos de apoyo tienen para que este proceso se realice de manera exitosa y con resultados confiables.

Por último se presenta una propuesta en la cual se expone la necesidad de poder evaluar la seguridad de la plataforma de la página Web mediante un pentesting, donde se indican el alcance y se revisan las herramientas que apoyarían la realización de test, con esto se logra la aprobación de la actividad, en el resultado esperado por la entidad se debe documentar las conclusiones, recomendaciones, controles sugeridos y exponer las vulnerabilidades identificadas para que con ello se pueda tomar acciones de mejora para implementar o aplicar en la seguridad de la infraestructura.

4 RESULTADO

En la Metodología OWASP, se plantea una fase para recolectar información del objetivo, donde se identificar mediante pruebas y actividades el foco de ataque, en el ejercicio también se busca que con las pruebas y herramientas no afecte la disponibilidad del sitio, con la mayor información posible el ataque parece muy real, pero a la vez no se presenten caídas de servicio, se establece un ambiente controlado para las pruebas, con este escenario se identifican las vulnerabilidades que pueda tener el sitio, pero sin afectar la disponibilidad del portal, las vulnerabilidades identificadas se clasifican de acuerdo con el Top 10 de Owasp 2017.

Para facilitar el proceso de pentesting y cumplir los objetivos a evaluar en el sitio web, los responsables del sitio web previa autorización proporcionaron la siguiente información relacionada con direcciones IP, descripción de los servidores y elementos a evaluar:

Servidor:	MINTRAB100
Dirección IP:	172.20.22.243
Sistema operativo:	Microsoft Windows Server 2012 R2 Standard
URL :	http://www.mintrabajo.gov.co/web/guest/inicio
Base de Datos	Oracle 12c

Se ejecutan pruebas para identificar los puertos y servicios abiertos o disponibles, identificar amenazas potenciales, para llegar a la definición de las pruebas, se tienen en cuenta factores como las características propias del servidor, la plataforma o ambiente de pruebas elaborado, arquitectura y aquellas particularidades que permiten identificar inicialmente la posible existencia de un riesgo. Estas pruebas pretenden simular el ataque real pero no una denegación de servicio y enunciar los riesgos a los que se encuentra expuesto el sitio web del Ministerio.

Para el desarrollo de las pruebas se implementa un ambiente virtualizado, con el sistema operativo Kali Linux 4.15.0 (2018-03-21) y 4.19.0 (2019-01-03) virtualizado sobre Hyper V, configurado con el mismo segmento de red del servidor objeto de las pruebas para el test interno y se utilizan las herramientas contenidas en el sistema operativo base de acuerdo con el plan de pruebas definido y aprobado, con este ambiente las pruebas se realizan de manera similar a como accede un usuario de la red LAN y cumpliendo con la arquitectura del entorno real.

4.1 VULNERABILIDADES DE LAS PAGINAS WEB

En las vulnerabilidades encontradas relacionadas con seguridad y que afectan el contenido o información publicada, comprometiendo la entidad o dueño de sitio, se revisa que las mismas estén registradas en la base conocida como CVE (Common Vulnerabilty Exposure), allí se puede ver si se encuentra catalogada y registrada como fallo, además de facilitar detalles que permiten precisar el parche a aplicar para protegerse de las vulnerabilidades.

Para avanzar en el proceso de intrusión se realiza la recopilación de información del objetivo. Esta es la etapa identificada como footprinting o huella, se realiza la recolección de todos los datos disponibles de la organización. Para ello se usa herramientas de footprinting como Google o cualquier otra en la cual se pueda recolectar y comprobar información del objetivo entre los datos recolectados se valida:

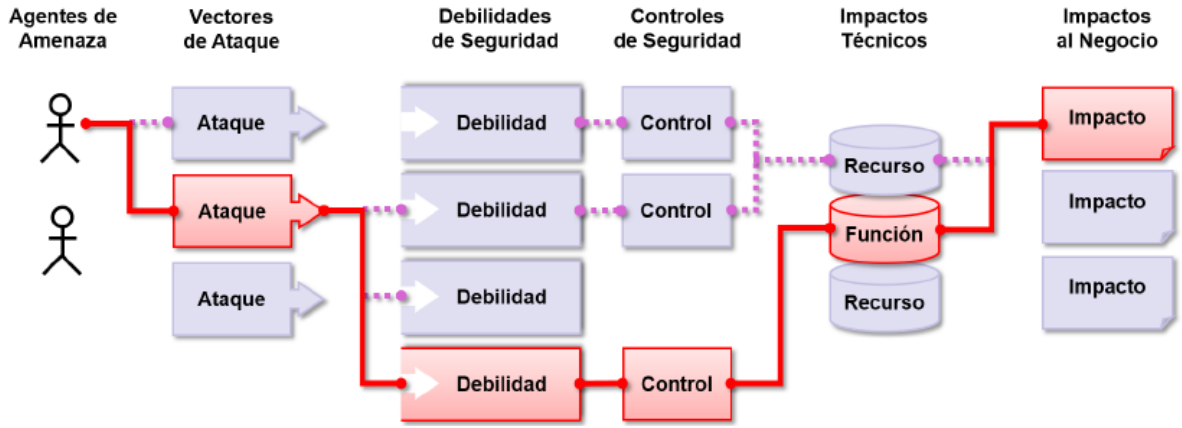
- ✓ Estructura de la organización.
- ✓ Áreas o dependencias, organización jerárquica (directores, jefes, líderes de proyectos, etc.).
- ✓ Infraestructura, incluyendo rango de direcciones IP y topología de red.
- ✓ Tecnología usada (hardware y software)
- ✓ Direcciones de correo electrónico de empleados.
- ✓ Contratistas, colaboradores y empresas afiliadas de la Organización.
- ✓ Ubicación física de la organización o de sus departamentos.
- ✓ Números de teléfono.
- ✓ Sistema operativo
- ✓ Versión
- ✓ Aplicaciones ejecutadas
- ✓ Nombre del dominio
- ✓ Servicios de red
- ✓ Arquitectura
- ✓ IDS
- ✓ Mecanismos de autenticación

El objeto de esta etapa es contar con la mayor cantidad de información del sistema entre los cuales pueda saber cuáles son las capacidades de acceso, puertos, servicios y seguridad del objetivo, para hacer un ataque efectivo y usar las herramientas adecuadas. Se emplea utilitarios disponibles en Kali Linux, para esta actividad, se usa la última versión del paquete de herramientas, a fin de contar con las actualizaciones que permitan explotar la vulnerabilidad buscada en la prueba.

“Los atacantes pueden, potencialmente, utilizar diferentes rutas a través de su aplicación para perjudicar su negocio u organización. Cada uno de estos caminos

representa un riesgo que puede o no ser suficientemente grave como para merecer atención."[34]

Figura 9 Riesgos en la Seguridad de las Aplicaciones

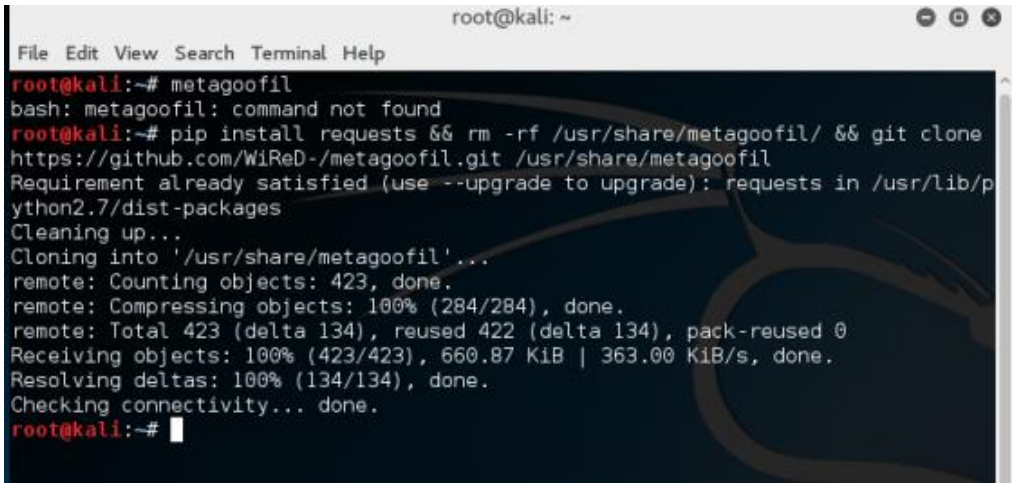


Fuente: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

De acuerdo con la Figura 9 Riesgos en la Seguridad de las Aplicaciones, se muestra una amenaza que puede explorar la superficie de ataque, la cual entre más amplia más posibilidades de acceder y consumar la vulnerabilidad tiene, además de la técnica que busca escalar y moverse lateralmente para explotar o desde allí afectar a otro blanco, sin embargo estas fases pueden tomar tiempo.

34 OWASP, HERRAMIENTAS, Herramientas OWASP [Disponible en] https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf, pág. 5.

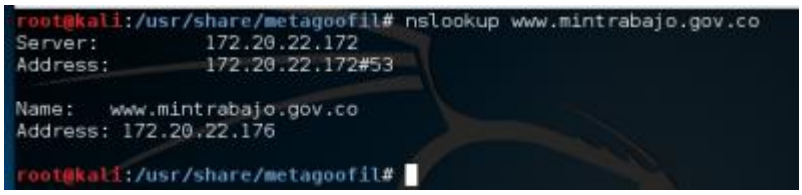
Figura 10 Captura Metagoofil - Kali Linux



Fuente: El autor

En la Figura 10, se observa herramienta Metagoofil, se realiza inicialmente la actualización de esta para poder pasar al proceso de búsqueda de la información del objetivo, para este caso la información que recopila la herramienta es la referente al servidor web en el cual se encuentra alojada la página de la entidad, mediante una consulta al servidor dns se obtiene el registro name con la ip asignada.

Figura 11 Captura Metagoofil - Kali Linux



Fuente: El autor

Al final se obtiene o entrega un reporte como el que se observa en la Figura 11, con el detalle de la información capturada del sitio, el mismo puede ser incluido en el informe gerencial del pentesting realizado, a fin de entregar algún detalle que sea relevante o tenga su grado de importancia respecto del análisis efectuado al sitio objeto de la prueba.

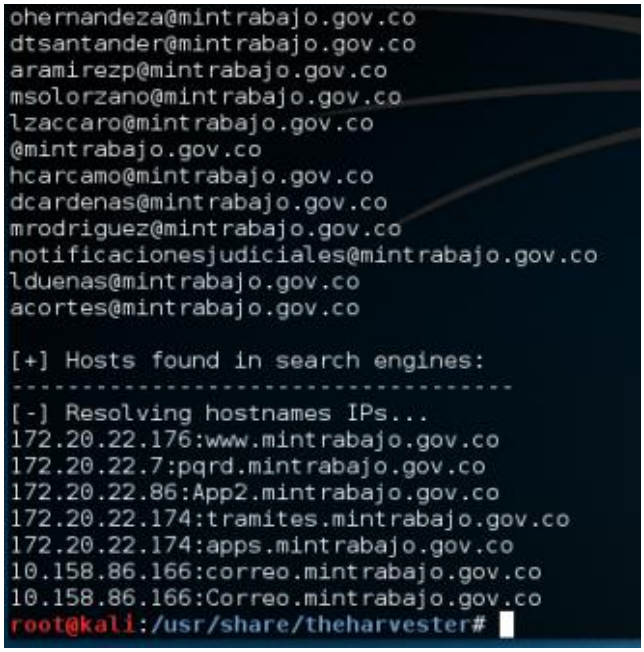
En la herramienta Metagoofil como se observa en la Figura 12, muestra el comando que se digita para que la aplicación proceda con el test, los datos básicos que se visualizan me indican la versión del software, la búsqueda de información del sitio, como el dominio, posteriormente se listan los usuarios, software, email y rutas del servidor que pueden ser capturadas por la herramienta en el análisis efectuado.

Figura 12 Avance del test

Fuente: El autor

En la Figura 13 se genera un reporte de la herramienta Metagoofil en el cual se entrega un listado de nombres, correos electrónicos, servidores y rutas del servidor web, en este reporte preliminar no aparecen resultados para ser explotados por un atacante de manera exitosa, pero con estos datos puede efectuarse un ataque ingeniería social y puede escalarse a un robo de información, igualmente puede usarse para el ataque a otro sitio o entidad.

Figura 13 Lista de correos encontrados



Fuente: El autor

La información capturada con la herramienta Thehavester (Cuadro 3) es muy útil para el atacante dado que recopila correos electrónicos, usuarios, dominios internos y direcciones IP

Cuadro 3 Listado de correos electrónicos

Emails encontrados en el Sitio
mmarulanda@mintrabajo.gov.co
rpardo@mintrabajo.gov.co
dtvichada@mintrabajo.gov.co
teletrabajo@mintrabajo.gov.co
grupoarchivosindical@mintrabajo.gov.co
quejasyreclamos@mintrabajo.gov.co
atencionalciudadano@mintrabajo.gov.co
eventos.sgsst@mintrabajo.gov.co
ebejarano@mintrabajo.gov.co
mcorrea@mintrabajo.gov.co
mdelahoz@mintrabajo.gov.co
lbohorquez@mintrabajo.gov.co
carangoa@mintrabajo.gov.co
gospina@mintrabajo.gov.co

Emails encontrados en el Sitio
nserna@mintrabajo.gov.co
ggaviria@mintrabajo.gov.co
implementacion.sgsst@mintrabajo.gov.co
ohernandeza@mintrabajo.gov.co
dtsantander@mintrabajo.gov.co
aramirezp@mintrabajo.gov.co
msolorzano@mintrabajo.gov.co
lzaccaro@mintrabajo.gov.co
hcarcamo@mintrabajo.gov.co
dcardenas@mintrabajo.gov.co
mrodriguez@mintrabajo.gov.co
notificacionesjudiciales@mintrabajo.gov.co
lduenas@mintrabajo.gov.co
acortes@mintrabajo.gov.co

Fuente: El autor

Con la herramienta se elabora el listado de subdominios de mintrabajo.gov.co con las respectivas IP´s y que permiten mostrar un panorama del direccionamiento de los equipos, servicios disponibles, correos y esto va a permitir al atacante armar un esquema del objetivo.

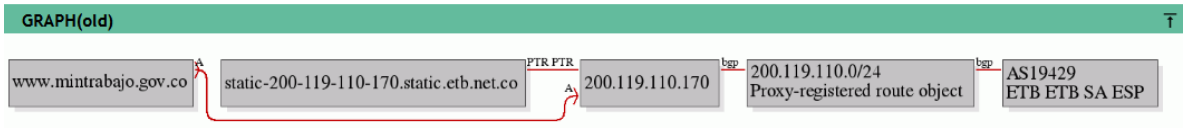
Cuadro 4 Lista de dominios

IP	Dominio asociado
172.x.x.x	www.mintrabajo.gov.co
172.x.x.x	pqrd.mintrabajo.gov.co
172.x.x.x	App2.mintrabajo.gov.co
172.x.x.x	tramites.mintrabajo.gov.co
172.x.x.x	apps.mintrabajo.gov.co
x.x.x.166	correo.mintrabajo.gov.co
x.x.x166	Correo.mintrabajo.gov.co

Fuente: El autor

Dentro de la recopilación de información del sitio aparte de realizar la captura de información interna, también se documenta aquellos datos que pueden tomarse externamente, para ello con una consulta en una dirección de internet es posible recolectar dominios, subdominios, dns, ip, sin interactuar con la organización objeto de test https://www.robtex.com/?dns=www.mintrabajo.gov.co

Figura 14 Verificación en URL https://www.robtex.com



Fuente: El autor

Como se puede observar en las Figuras 14 a la Figura 16, se encuentran datos que se consultan sin mayor esfuerzo en la web pero que sirve de apoyo para la revisión externa del objetivo usando herramientas o fuentes públicas. En esta consulta se puede obtener información de los registros DNS que tiene la entidad para la página WEB, proveedor del servicio de Internet (ISP), subdominios asociados, DNS público del proveedor, ip asociada al dominio.

La herramienta permite realizar una consulta rápida donde se coloca la información básica del dominio que se está analizando, allí se puede ver detalles como ip publica, servidores públicos de DNS, ver el proveedor del servicio de conectividad y que servidores se encargan de la resolución de nombres o de servidores de reenvió.

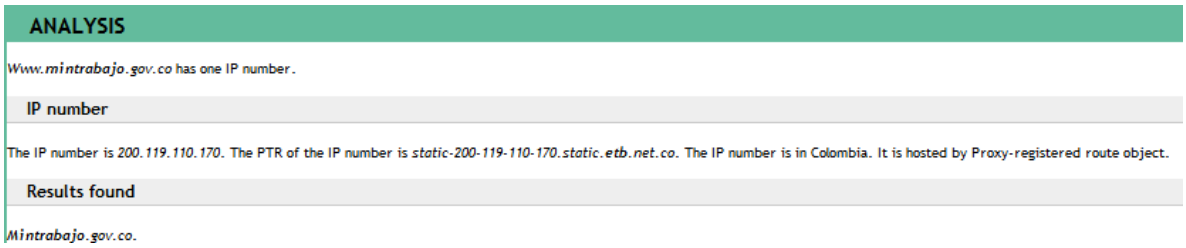
Figura 15 Información rápida del dominio

www.mintrabajo.gov.co quick info

General	
FQDN	www.mintrabajo.gov.co
Host Name	www
Domain Name	mintrabajo.gov.co
Registry	gov.co
TLD	co
DNS	
IP numbers	*200.13.237.174*
Domain DNS	
Name servers	*birlocha.**une**.net.co* *lauta.**une**.net.co*
Mail servers	*avas1.**une**.net.co*
IP Numbers	*200.13.237.174*

Fuente: El autor

Figura 16 Consulta dominio



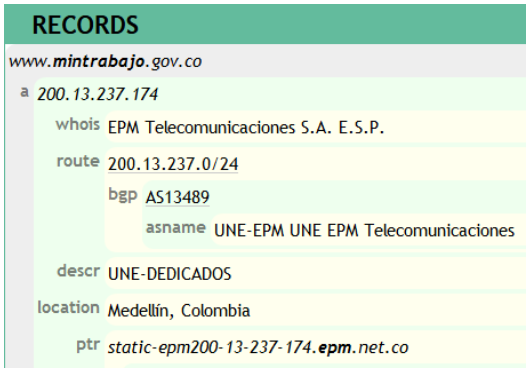
Fuente: El autor https://www.robtex.com

En las figuras anteriores se puede detallar información del proveedor del servicio, detalles de la localización y los segmentos de red que están en servicio para este dominio. En la figura 17 se evidencia el registro mail de la entidad y que corresponde a office 365.

Figura 17 Servidor de correo

Fuente: El autor

Figura 18 Proveedor de registro DNS



Fuente: El autor

En la figura 19, se encuentra un listado de los subdominios relacionados con el dominio que se analiza, la consulta arroja además de la ip pública del dominio consultado. Información que para un atacante permite revisar y elegir cual es el objetivo por vulnerar, entre sus posibilidades estarían aplicaciones, servicio de correo, un centro alterno o contingencia, servicios no críticos pero que tendrían menos seguridad y por tanto mayores posibilidades se ser suplantados. En esta información de dominios puede ser diciente el nombre, pues este daría indicios de cuál es el servicio al que se accede.

Figura 19 Listado de subdominios

SHARED

IP numbers	Sharing IP numbers
200.13.237.174	***mintrabajo**.gov.co*
1 results shown.	1 results shown.

Siblings

Siblings are domains or hostnames on the same level, under the same parent level. Not necessarily related in any other way

*app2.**mintrabajo**.gov.co*
*app3.**mintrabajo**.gov.co*
*apps.**mintrabajo**.gov.co*
*correo.**mintrabajo**.gov.co*
*correo1.**mintrabajo**.gov.co*
*filco.**mintrabajo**.gov.co*
*pqrd.**mintrabajo**.gov.co*
*tramites.**mintrabajo**.gov.co*

8 results shown.

On other TLD:s and domains

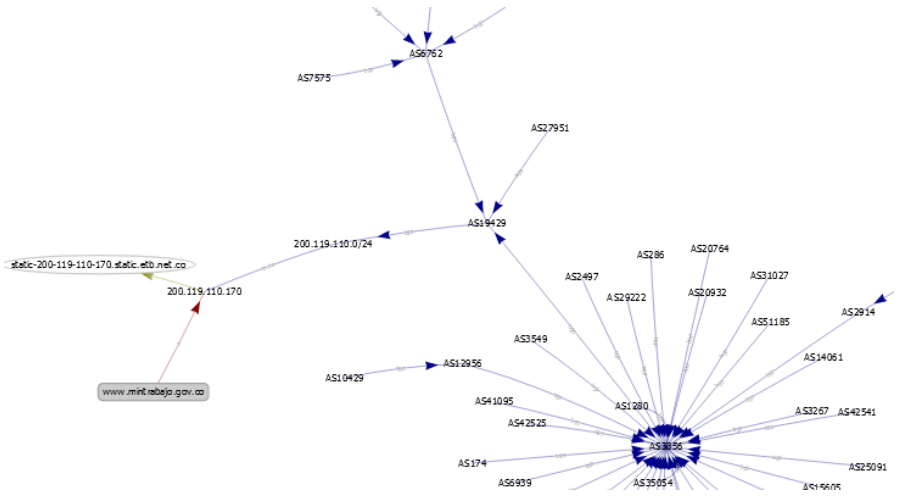
This sub section shows this name on other top level domains.

***mintrabajo**.gov.co*

1 results shown.

Fuente: El autor

Figura 20 Grafica de acceso al dominio



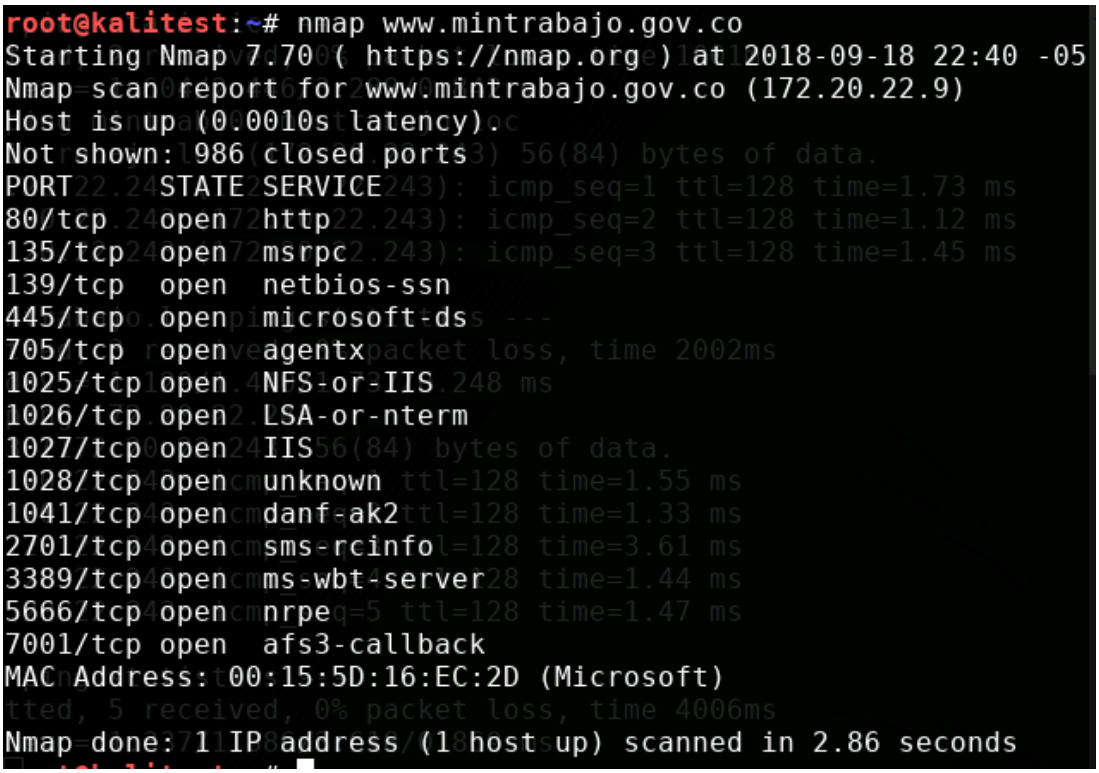
Fuente: El autor

Dentro de los datos relevantes que requiere el atacante también se encuentra:

- La infraestructura, dentro de este ítem podemos documentar las tecnologías en uso, diagramas de cableado o conectividad, mapas de red o aplicaciones a nivel de usuario y que forman parte de la infraestructura.
- Configuración de los sistemas, se debe incluir la documentación, listas de comprobación de configuración, procedimientos de endurecimiento, políticas de grupo e inventario de software.

Contraseñas, accesos VPN e información de privilegios para usuarios con perfil administrador o usuario básico.

Figura 21 Puertos NMAP



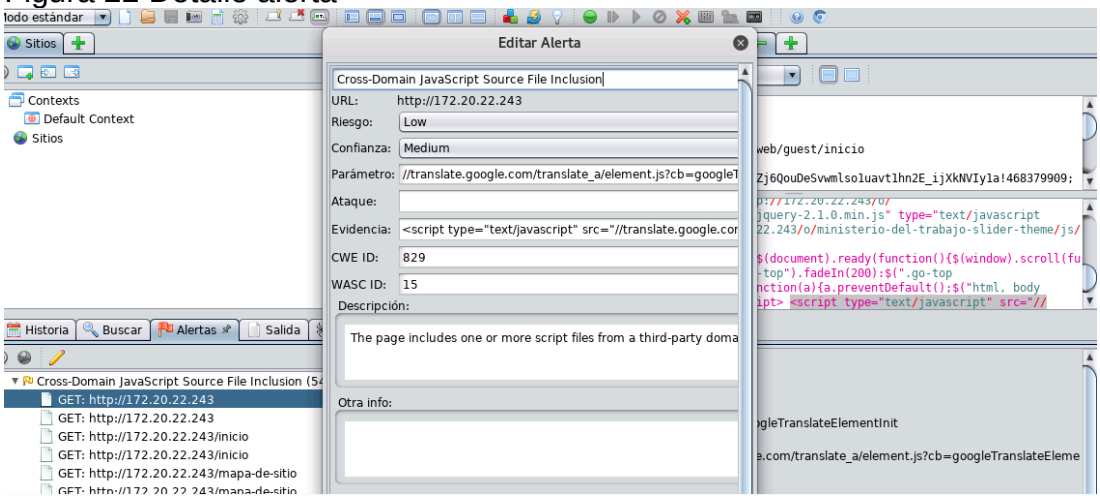
Fuente: El autor

Con el uso de la herramienta nmap se puede escanear los puertos del servidor web en donde se evidencia que la revisión de estos, es posible realizarla desde un punto de la red cualquiera con solo ser un cliente o instalar un equipo en la misma, es

decir, el acceso al servidor a un puerto diferente al web y para este caso es posible identificar el puerto 22 del servicio ssh estaría disponible para su ataque.

Al realizar un escaneo con la herramienta OWASP ZAP, esta herramienta está diseñada para analizar las vulnerabilidades de las aplicaciones Web, teniendo en cuenta que el sitio al cual se le va a realizar el test, cuenta con gestor de contenido, en la Figura 22 se puede ver que una vulnerabilidad identificada está catalogada como *alerta de riesgo bajo.*

Figura 22 Detalle alerta

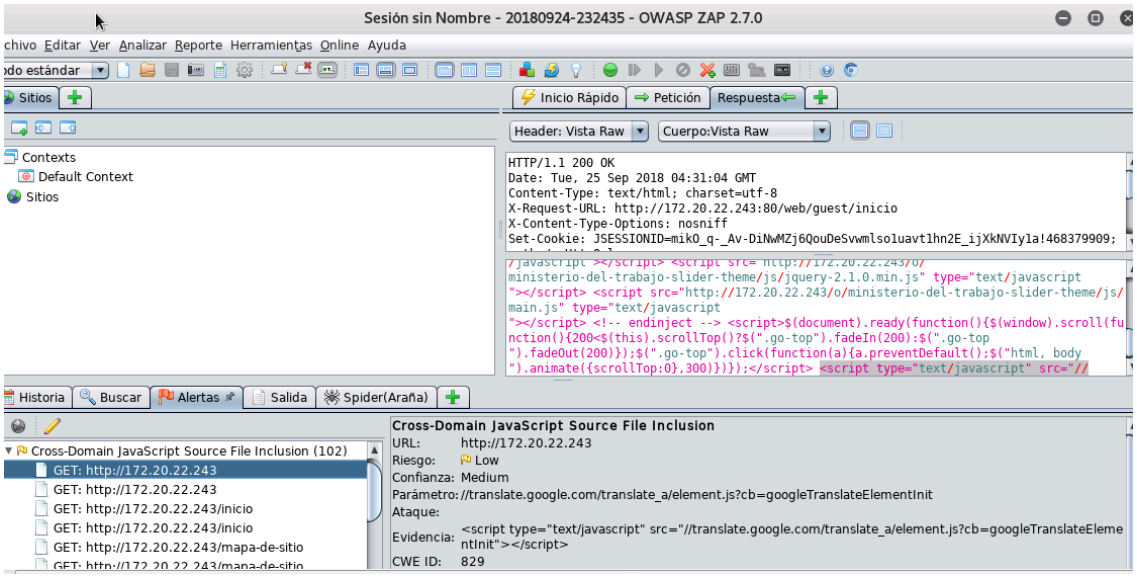


Fuente: El autor

En la

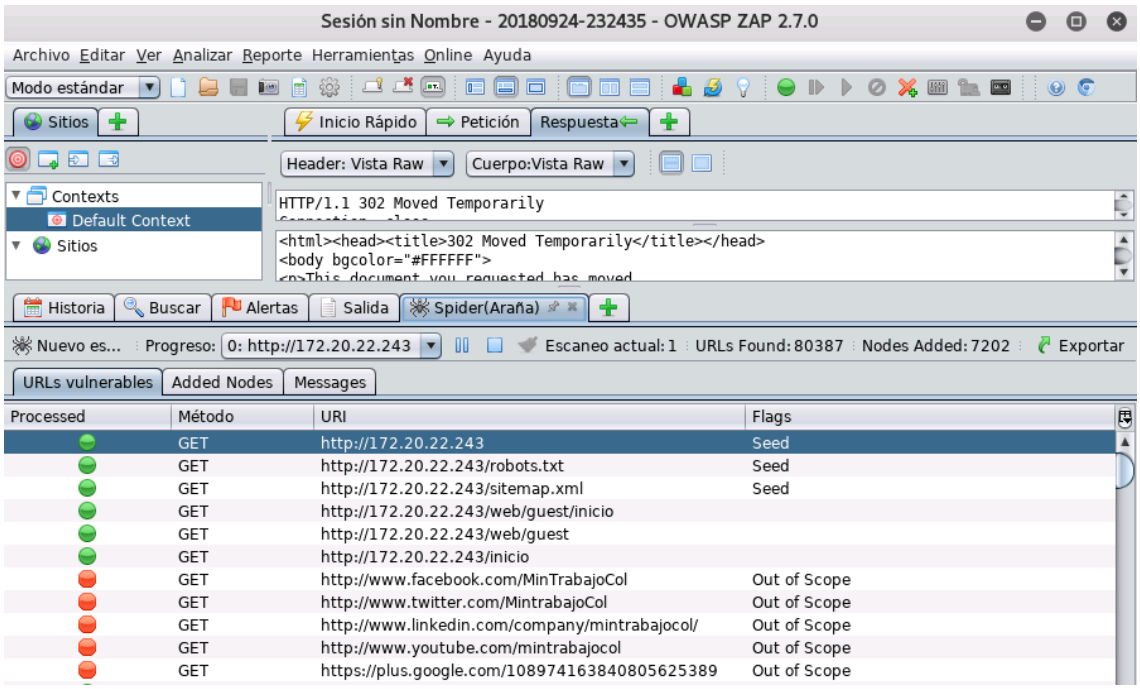
Figura 23 Alertas por Cross-Domain JavaScript, se identifica que hay 102 vulnerabilidades por incrustar archivos por medio de java script, pero igualmente se puede ver que la herramienta identifica las mismas con riesgo bajo, sin embargo, como recomendación la herramienta indica que debe usarse fuentes seguras.

Figura 23 Alertas por Cross-Domain JavaScript



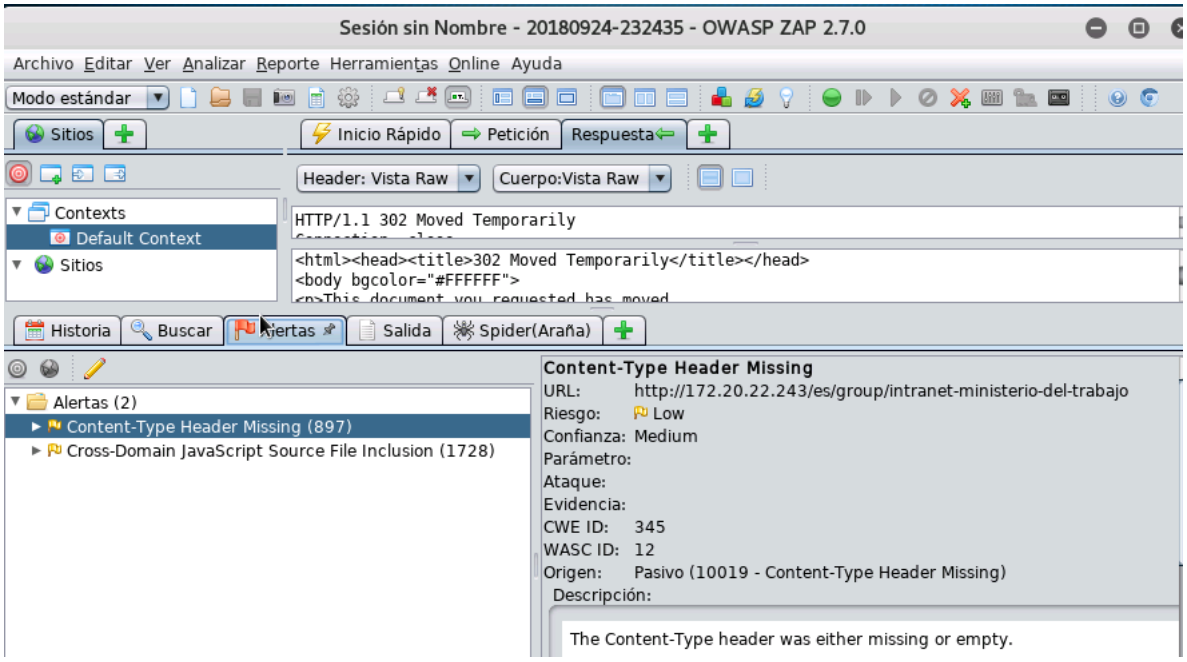
Fuente: El autor

Figura 24 URL Vulnerables



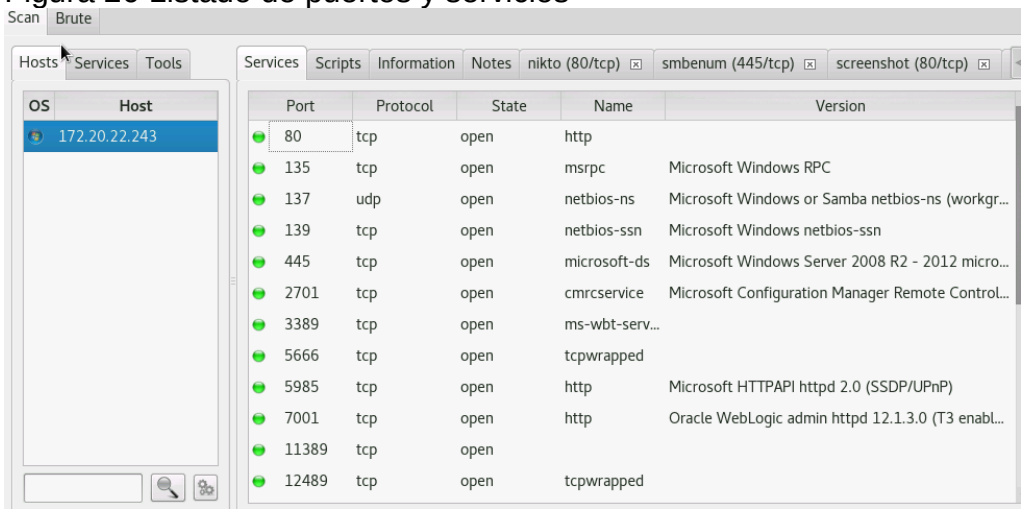
Fuente: El autor

Figura 25 Alertas de Owasp



Fuente: El autor

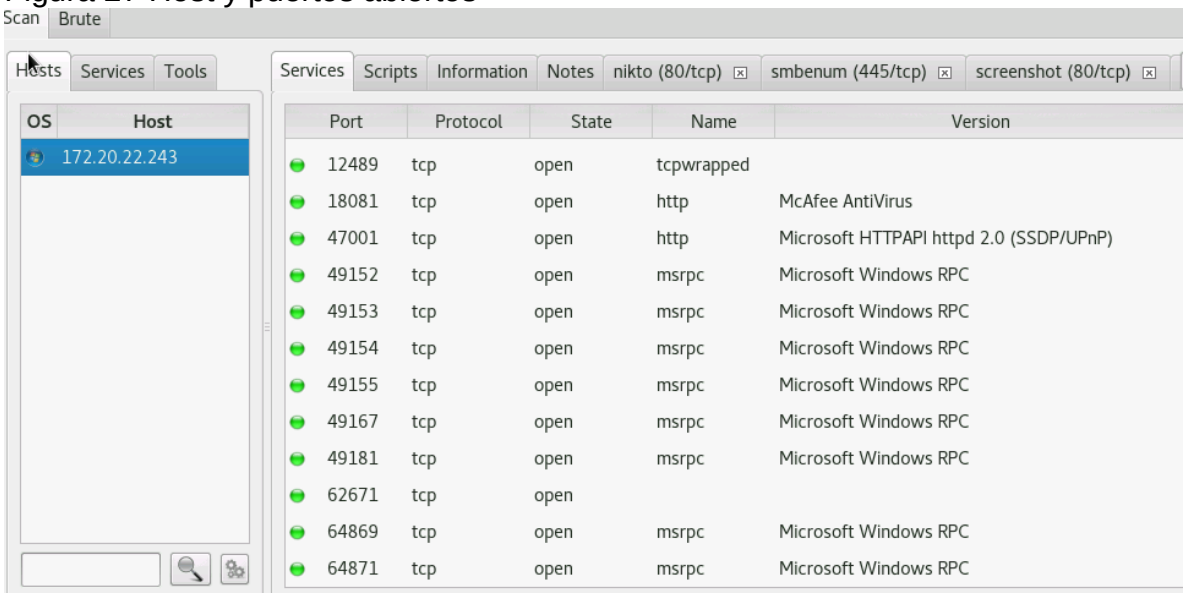
Figura 26 Listado de puertos y servicios



Fuente: El autor

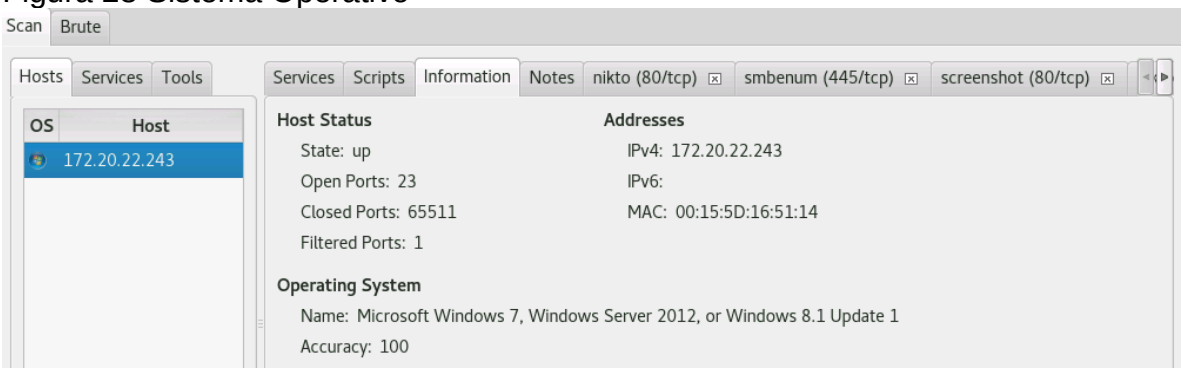
De acuerdo con las Figuras 22 a la Figura 28, se puede identificar que hay más de 2.500 vulnerabilidades de las cuales se puede corroborar que las mismas tienen un nivel de riesgo bajo, por tanto, su corrección, está sujeta la gestión del administrador del sitio Web, pero a la vez se puede proceder a su corrección con buenas prácticas y la tarea de ajustar las fallas reportadas por la herramienta.

Figura 27 Host y puertos abiertos



Fuente: El autor

Figura 28 Sistema Operativo



Fuente: El autor

En la Figura 28, se detalla que la herramienta usada puede identificar el sistema operativo, la ip, mac y estado del puerto que se está revisando.

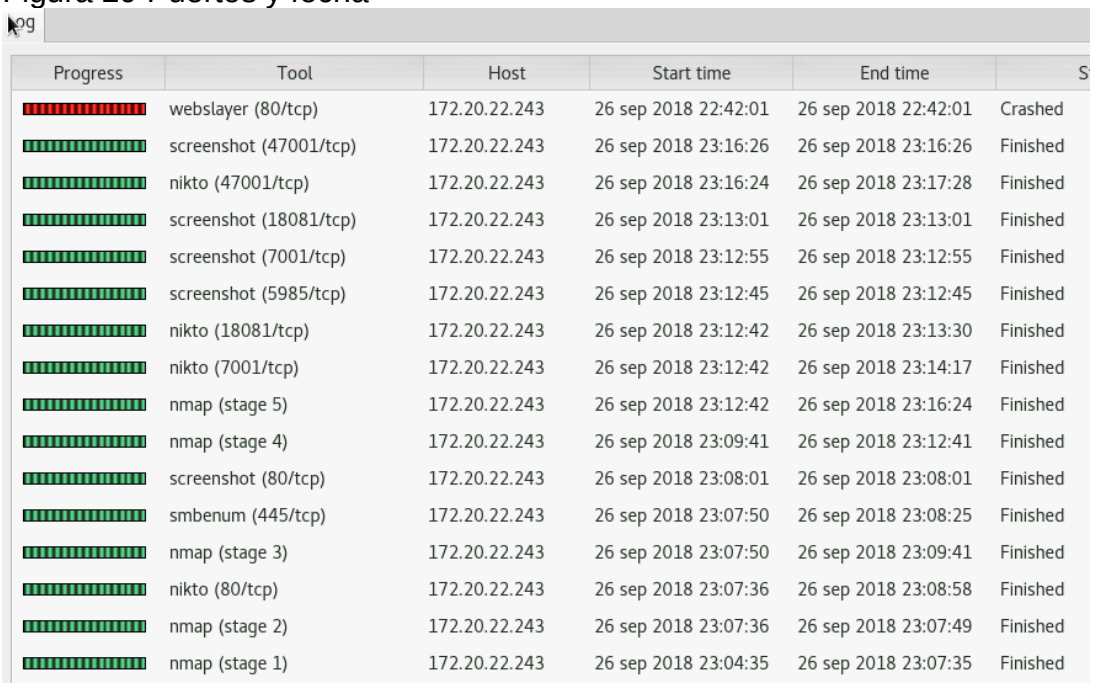
Cuadro 5 Lista de servicios y puertos

Puerto		Servicio	Detalle
80	Tcp	http	Web
135	Tcp	msrpc	Microsoft Windows RPC
139	Tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	Tcp	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
2701	Tcp	cmrcservice	Microsoft Configuration Manager Remote Control service
3389	Tcp	ms-wbt-server	Microsoft Terminal Service
5666	tcp	tcpwrapped	Nrpe Nagios
7001	tcp	http	Oracle WebLogic admin httpd
49152	tcp	msrpc	Microsoft Windows RPC
49153	tcp	msrpc	Microsoft Windows RPC
49154	tcp	msrpc	Microsoft Windows RPC
49155	tcp	msrpc	Microsoft Windows RPC

Fuente: El autor

En el Cuadro 5, se listan algunos de los principales o más conocidos puertos que tiene abiertos el servidor, adicionalmente se tiene el servicio que este asociado.

Figura 29 Puertos y fecha



Progress	Tool	Host	Start time	End time	S
	webslayer (80/tcp)	172.20.22.243	26 sep 2018 22:42:01	26 sep 2018 22:42:01	Crashed
	screenshot (47001/tcp)	172.20.22.243	26 sep 2018 23:16:26	26 sep 2018 23:16:26	Finished
	nikto (47001/tcp)	172.20.22.243	26 sep 2018 23:16:24	26 sep 2018 23:17:28	Finished
	screenshot (18081/tcp)	172.20.22.243	26 sep 2018 23:13:01	26 sep 2018 23:13:01	Finished
	screenshot (7001/tcp)	172.20.22.243	26 sep 2018 23:12:55	26 sep 2018 23:12:55	Finished
	screenshot (5985/tcp)	172.20.22.243	26 sep 2018 23:12:45	26 sep 2018 23:12:45	Finished
	nikto (18081/tcp)	172.20.22.243	26 sep 2018 23:12:42	26 sep 2018 23:13:30	Finished
	nikto (7001/tcp)	172.20.22.243	26 sep 2018 23:12:42	26 sep 2018 23:14:17	Finished
	nmap (stage 5)	172.20.22.243	26 sep 2018 23:12:42	26 sep 2018 23:16:24	Finished
	nmap (stage 4)	172.20.22.243	26 sep 2018 23:09:41	26 sep 2018 23:12:41	Finished
	screenshot (80/tcp)	172.20.22.243	26 sep 2018 23:08:01	26 sep 2018 23:08:01	Finished
	smbenum (445/tcp)	172.20.22.243	26 sep 2018 23:07:50	26 sep 2018 23:08:25	Finished
	nmap (stage 3)	172.20.22.243	26 sep 2018 23:07:50	26 sep 2018 23:09:41	Finished
	nikto (80/tcp)	172.20.22.243	26 sep 2018 23:07:36	26 sep 2018 23:08:58	Finished
	nmap (stage 2)	172.20.22.243	26 sep 2018 23:07:36	26 sep 2018 23:07:49	Finished
	nmap (stage 1)	172.20.22.243	26 sep 2018 23:04:35	26 sep 2018 23:07:35	Finished

Fuente: El autor

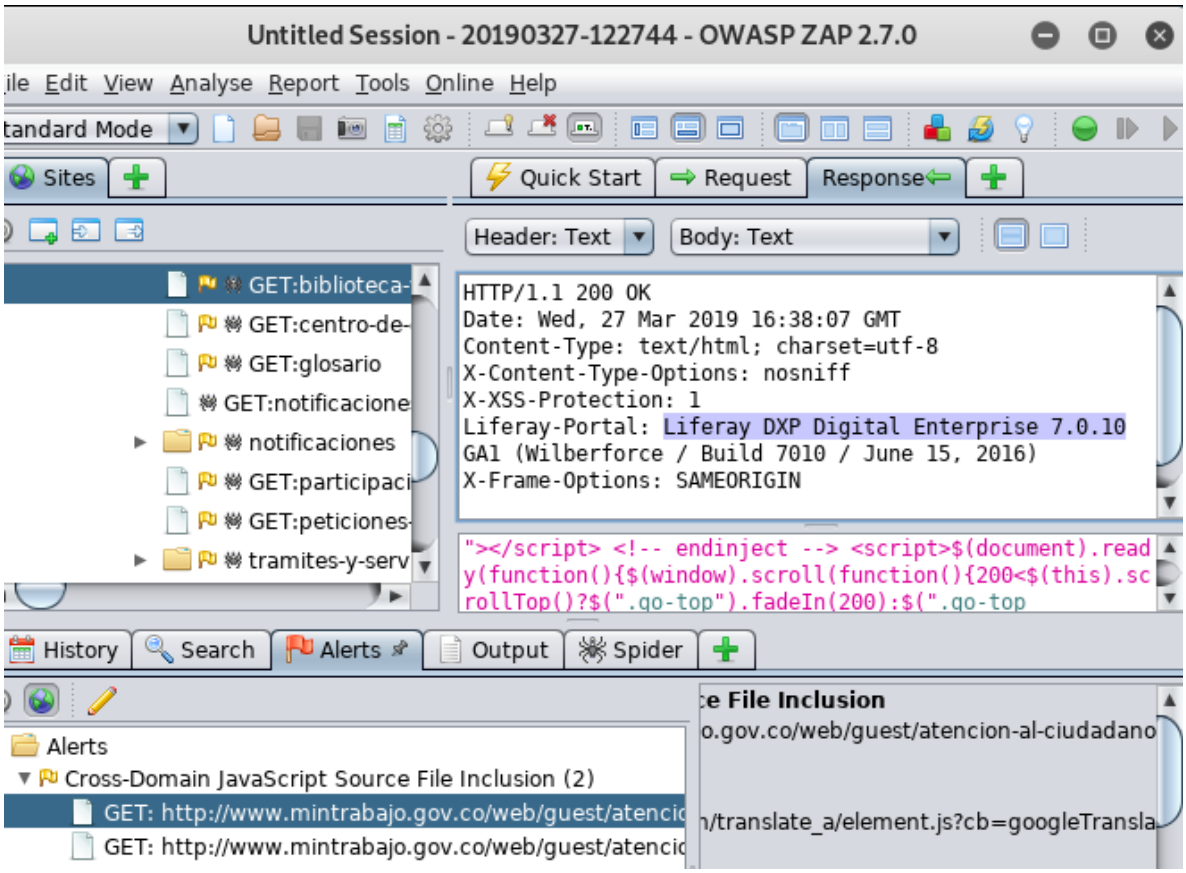
En la Figura 31 Puertos y fecha, se encuentra un listado de puertos que se evidencia están abiertos y pueden ser accedidos desde la red, además de ver cual herramienta fue usada en la verificación con el tiempo que fue requerido para identificar el puerto. Con Resultado de la evaluación de la vulnerabilidad con Owasp Zap: En el cuadro se detallan dos tipos de alertas con un total de 2.625 eventos reportados. Como resultado de la evaluación se listan las vulnerabilidades:

Cuadro 6 Vulnerabilidades Owasp Zap

Alerta	Identificadas	Riesgo
Falta el encabezado de tipo de contenido	897	BAJO
Inclusión de archivos de código Javascript de dominios cruzados	1728	BAJO

Fuente: El Autor

Figura 30 Owasp Zap -CMS

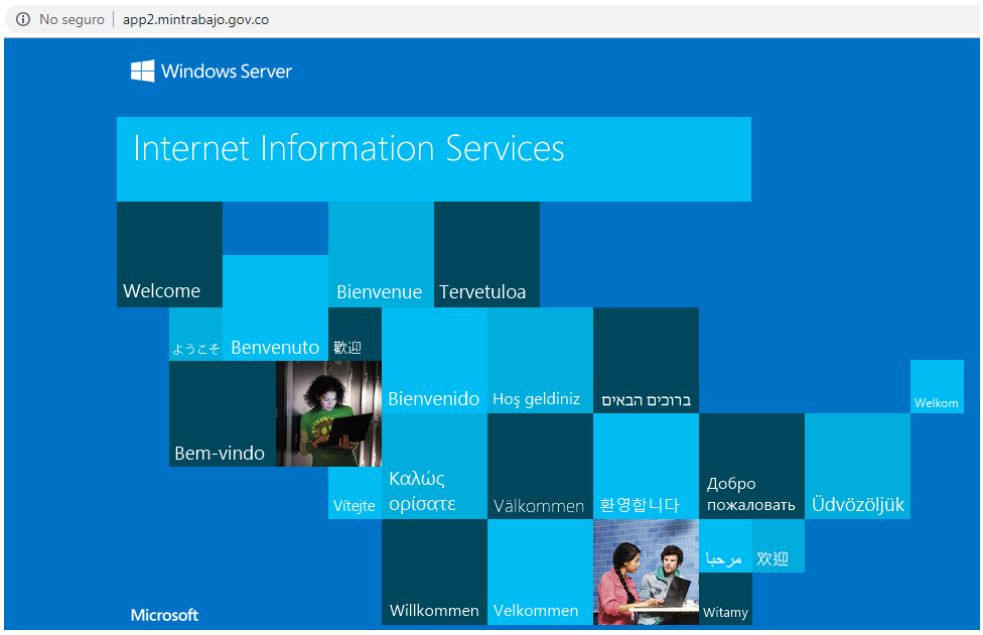


Fuente: EL autor

Con la información que entrega OWASP ZAP se identifica que el portal tiene un gestor de contenido soportado sobre la plataforma Liferay Portal 7.0.10, con esta información se hace la búsqueda de los fallos de seguridad que tiene esa versión y que pueden ser objeto de afectación. Igualmente, con esta herramienta se identifica y categoriza dos diferentes tipos de fallos relacionados con

A6 :2017 Configuración de Seguridad Incorrecta

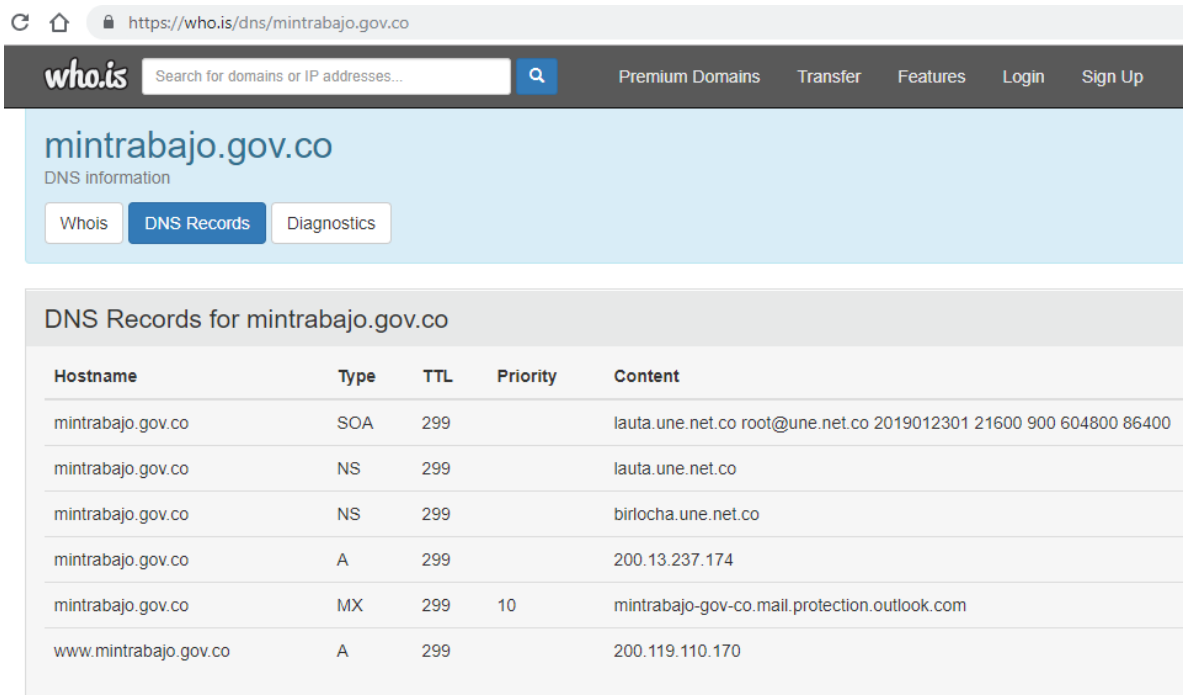
Figura 31 Configuración predeterminada en URL del sitio



Fuente: El autor

Se identifica una url a la cual se direcciona desde la página web y en esta se identifica el servidor web IIS y el sistema operativo del mismo Windows.

Figura 32 Who IS registros DNS y TTL



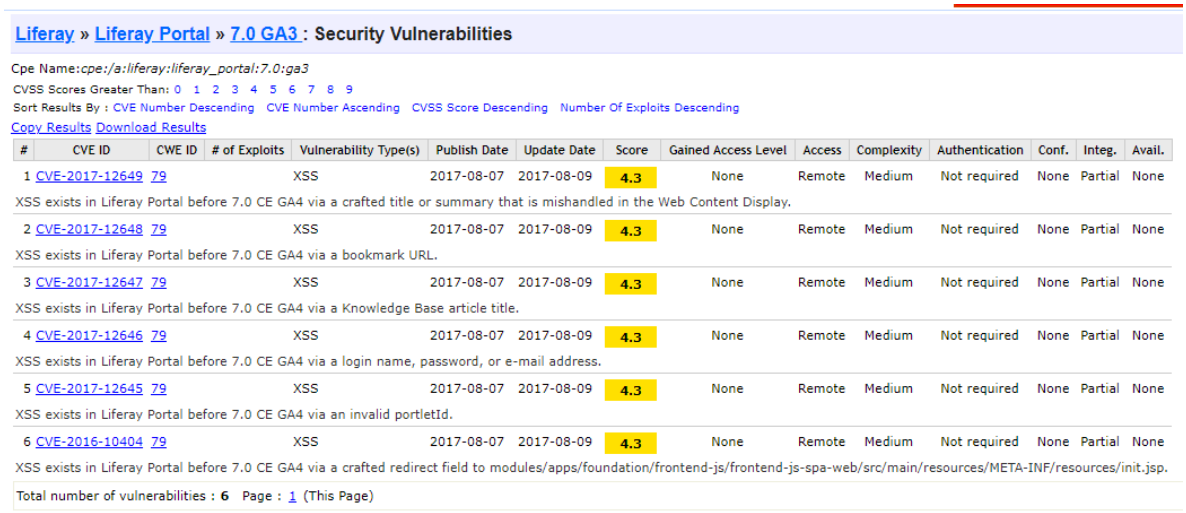
Fuente: El autor

Se identifica que existe un registro tipo A para la ip 200.119.110.170 con el nombre dns www.mintrabajo.gov.co y el mismo permite acceder a una página web o servicio de la entidad objeto de análisis del presente documento.

A7:2017 Cross-Site Scripting (XSS)

Se identifica que el portal está expuesto a los 6 fallos de seguridad publicados en la base de datos https://www.cvedetails.com/index.php por cuanto el gestor de contenido es Liferay Portal versión 7

Figura 33 Vulnerabilidades identificadas Portal Liferay 7.0



Liferay » Liferay Portal » 7.0 GA3 : Security Vulnerabilities

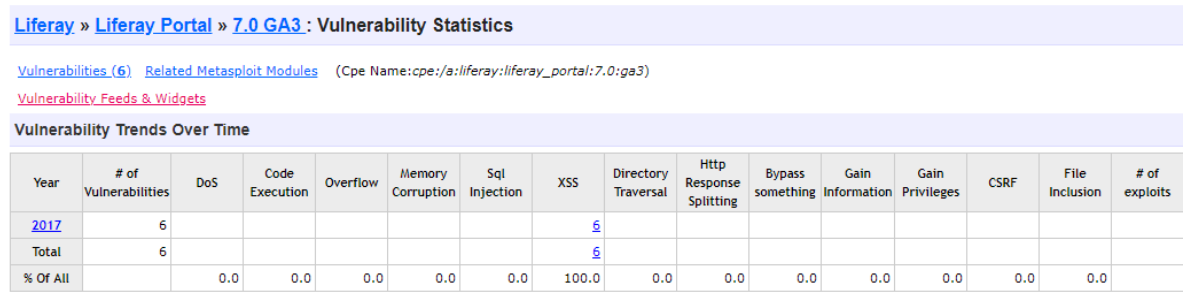
Cpe Name:*cpe:/a:liferay:liferay_portal:7.0:ga3*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-12649	79		XSS	2017-08-07	2017-08-09	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in Liferay Portal before 7.0 CE GA4 via a crafted title or summary that is mishandled in the Web Content Display.														
2	CVE-2017-12648	79		XSS	2017-08-07	2017-08-09	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in Liferay Portal before 7.0 CE GA4 via a bookmark URL.														
3	CVE-2017-12647	79		XSS	2017-08-07	2017-08-09	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in Liferay Portal before 7.0 CE GA4 via a Knowledge Base article title.														
4	CVE-2017-12646	79		XSS	2017-08-07	2017-08-09	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in Liferay Portal before 7.0 CE GA4 via a login name, password, or e-mail address.														
5	CVE-2017-12645	79		XSS	2017-08-07	2017-08-09	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in Liferay Portal before 7.0 CE GA4 via an invalid portletId.														
6	CVE-2016-10404	79		XSS	2017-08-07	2017-08-09	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in Liferay Portal before 7.0 CE GA4 via a crafted redirect field to modules/apps/foundation/frontend-js/frontend-js-spa-web/src/main/resources/META-INF/resources/init.jsp.														

Total number of vulnerabilities : **6** Page : 1 (This Page)

Fuente: https://www.cvedetails.com/vulnerability-list/vendor_id-2114/product_id-18625/version_id-219986/Liferay-Liferay-Portal-7.0.html

Figura 34 Tipos de vulnerabilidad identificadas en 2017



Liferay » Liferay Portal » 7.0 GA3 : Vulnerability Statistics

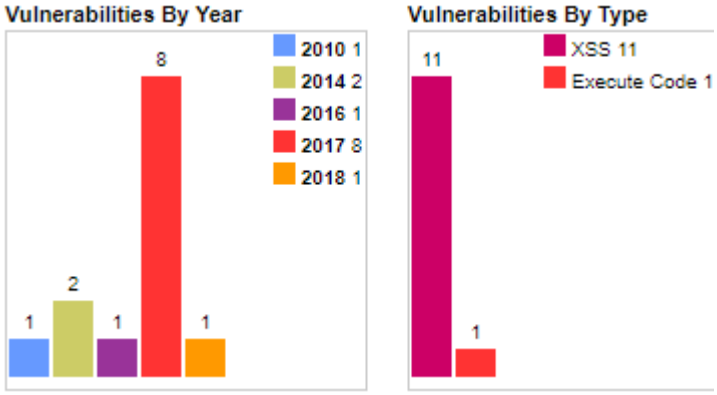
Vulnerabilities (6) Related Metasploit Modules (Cpe Name:*cpe:/a:liferay:liferay_portal:7.0:ga3*)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2017	6						6								
Total	6						6								
% Of All		0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	

Fuente: https://www.cvedetails.com/version/219986/Liferay-Liferay-Portal-7.0.html

Figura 35 Vulnerabilidades por año Liferay



Fuente: https://www.cvedetails.com/product/18625/Liferay-Liferay-Portal.html?vendor_id=2114

Figura 36 Resumen reporte Nikto

URI	/lcds-samples/messagebroker/httpsecure
HTTP Method	GET
Description	/lcds-samples/messagebroker/httpsecure: Adobe BlazeDS is vulnerable to an XXE (CVE-2009-3960)
Test Links	http://www.mintrabajo.gov.co:80/lcds-samples/messagebroker/httpsecure http://200.119.110.170:80/lcds-samples/messagebroker/httpsecure
OSVDB Entries	OSVDB-62292

Host Summary

Start Time	2019-03-30 20:02:11
End Time	2019-03-30 20:40:40
Elapsed Time	2309 seconds
Statistics	7727 requests, 1 errors, 196 findings

Scan Summary

Software Details	Nikto 2.1.6
CLI Options	-host www.mintrabajo.gov.co -Format html -o /root/report.html
Hosts Tested	1
Start Time	Sat Mar 30 20:02:09 2019
End Time	Sat Mar 30 20:40:40 2019
Elapsed Time	2311 seconds

Fuente: El autor

Se identificaron 196 fallos distribuidos en 7 diferentes vulnerabilidades catalogadas en la base de datos CVE que se listan aquí:

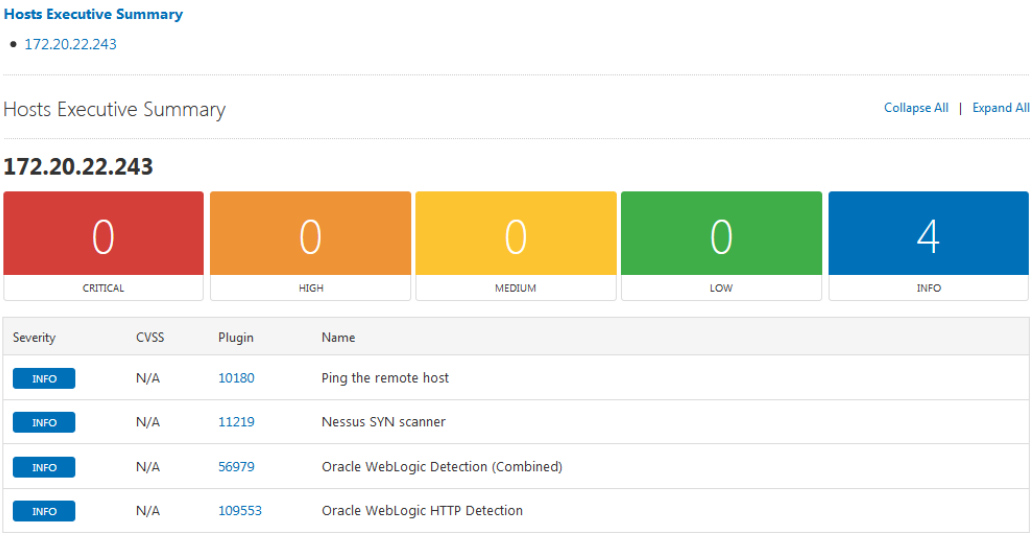
1. CVE-2002-0434 Ejecución de código
2. CVE-2001-0320 Ejecución de código XSS SQL Abuso de Privilegios
3. CVE-2003-0243 Ejecución de código
4. CVE-2001-0321 Ataque remoto
5. CVE-2001-0900 Perdida de control de acceso (Path traversal)
6. CVE-2009-0932 Perdida de control de acceso (Path traversal) y Ejecución de código

7. CVE-2009-3960 Extraer información sensible - Entidades Externas XML

4.2 ANÁLISIS DE LOS RESULTADOS

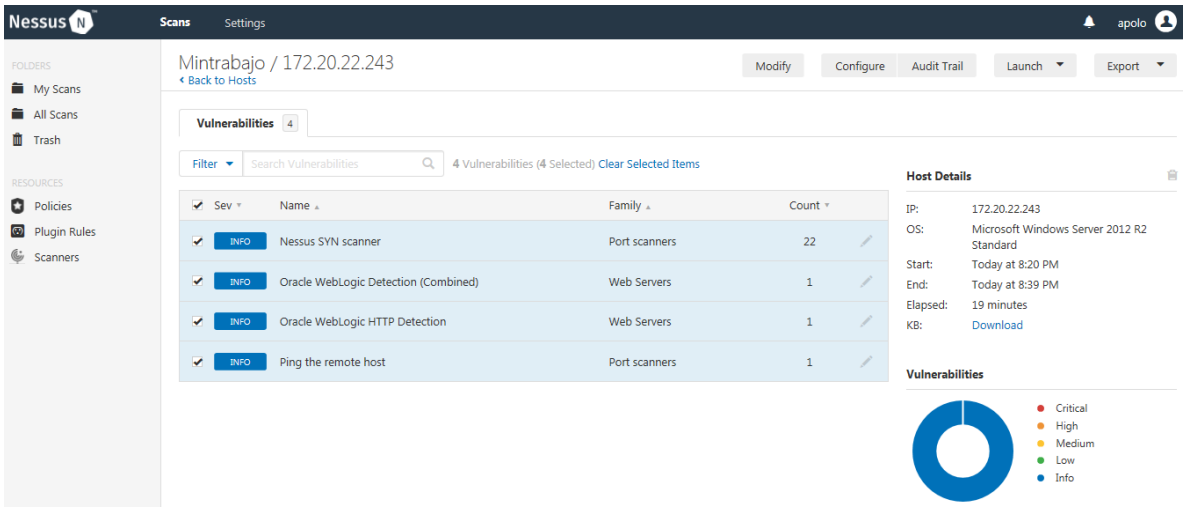
Teniendo en cuenta los resultados de las pruebas, se puede destacar que al haber revisado con varias herramientas en la pruebas se identifican los mismos puertos abiertos, al usar Nessus el reporte generado se muestra vulnerabilidades de tipo crítico, alto, media y baja en cero (0) para el objetivo evaluado, se identifican solo vulnerabilidades de tipo informativo, pero igualmente se resalta que de las vulnerabilidades identificadas corresponden a riesgo bajo, sin embargo, es importante destacar que los servicios que no se requieren deben ser bajados o bloqueador para no tener puertas traseras, con esto se disminuye la superficie de ataque. Este riesgo que se clasifica como de bajo impacto ya que no afecta a la información del sistema, de forma aislada no resulta peligroso, sin embargo, al combinarse con otros ataques de inyección de código podría generar un impacto mayor.
En las pruebas no se identifican vulnerabilidades de riesgo alto y medio, por lo cual no se necesitaría aplicar controles para ellos, pero se sugiere mantener monitoreo preventivo para evitar exponer la plataforma.

Figura 37 Reporte de Host



Fuente: El autor

Figura 38 Detalle vulnerabilidades por familia



Fuente: El autor

Información Host
Netbios Name: MINTRAB100
IP: 172.20.22.243
OS: Microsoft Windows Server 2012 R2 Standard

Vulnerabilidades

10180 - (**22 Eventos**) Hacer ping al host remoto
Sinopsis
Fue posible identificar el estado del host remoto (Activo o apagado).

Descripción
Con el uso de Nessus se pudo determinar si el host remoto está activo utilizando uno o más de los siguientes tipos de ping:
- Un ping ARP, siempre que el host esté en la subred local y Nessus se esté ejecutando a través de Ethernet.
- Un ping ICMP.
- Un ping TCP, en el que el complemento envía al host remoto un paquete con el indicador SYN, y el host responderá con un RST o un SYN / ACK.
- Un ping UDP (por ejemplo, DNS, RPC y NTP).

Solución

n / A
Factor de riesgo

Ninguno
Información del complemento:

Publicado el 1999/06/24, modificado: 2018/08/27
Salida de plugin

tcp / 0

El host remoto está arriba

El host remoto respondió a un paquete TCP SYN enviado al puerto 139 con un paquete SYN, ACK

11219 – (**22 Eventos**) escáner Nessus SYN

Sinopsis
Es posible determinar qué puertos TCP están abiertos.

Descripción
Este plugin es un escáner de puertos SYN 'semiabierto'. Será razonablemente rápido incluso contra un objetivo con cortafuegos.
Se debe tener en cuenta que los escaneos SYN son menos intrusivos que los escaneos TCP (conexión completa) contra servicios rotos, pero pueden causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.

Solución
Protege tu objetivo con un filtro de IP si el servicio es requerido para ser expuesto a un usuario o administrador, asegurando que solo quien requiere el acceso lo tenga y protegiendo los accesos no autorizados.

Factor de riesgo
Ninguna

Información del complemento:
Publicado: 02/02/2009, modificado: 2018/07/19

Salida de plugin
172.20.22.243 (tcp / 80)
El puerto 80 / tcp se encontró abierto

172.20.22.243 (tcp / 135)
El puerto 135 / tcp se encontró abierto

172.20.22.243 (tcp / 139)
El puerto 139 / tcp se encontró abierto

172.20.22.243 (tcp / 445)

El puerto 445 / tcp se encontró abierto

172.20.22.243 (tcp / 2701)
El puerto 2701 / tcp se encontró abierto

172.20.22.243 (tcp / 3389)
El puerto 3389 / tcp se encontró abierto

172.20.22.243 (tcp / 5666)
El puerto 5666 / tcp se encontró abierto

172.20.22.243 (tcp / 5985)
El puerto 5985 / tcp se encontró abierto

172.20.22.243 (tcp / 7001)
El puerto 7001 / tcp se encontró abierto

172.20.22.243 (tcp / 11389)
El puerto 11389 / tcp se encontró abierto

172.20.22.243 (tcp / 12489)
El puerto 12489 / tcp se encontró abierto

172.20.22.243 (tcp / 18081)
El puerto 18081 / tcp se encontró abierto

172.20.22.243 (tcp / 47001)
El puerto 47001 / tcp se encontró abierto

172.20.22.243 (tcp / 49152)
El puerto 49152 / tcp se encontró abierto

172.20.22.243 (tcp / 49153)
El puerto 49153 / tcp se encontró abierto

172.20.22.243 (tcp / 49154)
El puerto 49154 / tcp se encontró abierto

172.20.22.243 (tcp / 49155)
El puerto 49155 / tcp se encontró abierto

172.20.22.243 (tcp / 49167)
El puerto 49167 / tcp se encontró abierto

172.20.22.243 (tcp / 49181)

El puerto 49181 / tcp se encontró abierto

172.20.22.243 (tcp / 62671)
El puerto 62671 / tcp se encontró abierto

172.20.22.243 (tcp / 64869)
El puerto 64869 / tcp se encontró abierto

172.20.22.243 (tcp / 64871)
El puerto 64871 / tcp se encontró abierto

56979 (1) - Detección de Oracle WebLogic (combinada)

Sinopsis
Oracle WebLogic se ejecuta en el servidor web remoto.

Descripción
Oracle (anteriormente BEA) WebLogic, un servidor de aplicaciones Java EE, se ejecuta en el servidor web remoto.
Ver también
http://www.nessus.org/u?99924a19

Solución
n / A

Factor de riesgo
Ninguno

Información del complemento:
Publicado: 30/11/2011, modificado: 2018/05/03

Salida de plugin
172.20.22.243 (tcp / 7001)
Versión: 12.1.3.0.0
Fuente: www
Puerto: 7001
Protocolos: www t3

109553 (1) - Detección HTTP de Oracle WebLogic

Sinopsis
El servidor HTTP de Oracle WebLogic se ejecuta en el servidor web remoto.

Descripción

Oracle (anteriormente BEA) WebLogic, un servidor de aplicaciones Java EE, se ejecuta en el servidor web remoto.
Ver también
http://www.nessus.org/u?99924a19

Solución
n / A

Factor de riesgo
Ninguno

Información del complemento:
Publicado: 2018/05/03, modificado: 2018/05/03

Salida de plugin
172.20.22.243 (tcp / 7001)
URL: http://172.20.22.243:7001/console/login/LoginForm.jsp
Versión: 12.1.3.0.0

1. **Falta el encabezado de tipo de contenido**

Sinopsis
En esta categoría se encuentran 897 vulnerabilidades que indican que el encabezado del tipo de contenido está ausente ó vacío.

Descripción
Corresponde a falta de control de contenido del software que permite que se deje el campo vacío, no es obligatoria su captura o este presentando un fallo. La verificación de los datos es insuficiente.

El código relacionado con la vulnerabilidad es: CWE-345 [35] Verificación insuficiente de la autenticidad de los datos

Solución
Se debe asegurar que cada página establezca el valor de tipo de contenido especifico y apropiado para el contenido entregado.

2. **Inclusión de archivos de código Javascript de dominios cruzados**

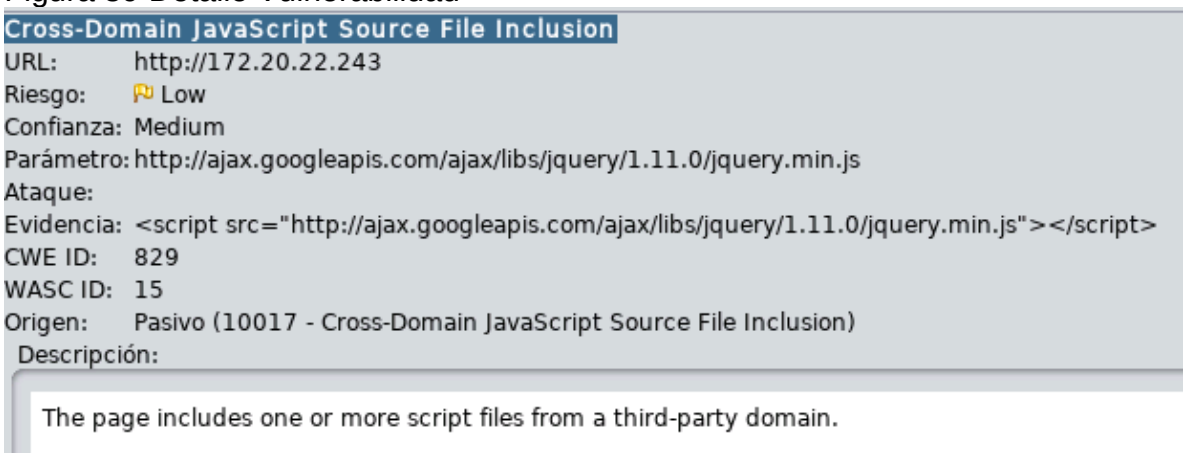
Sinopsis

35 Common Weakness Enumeration, Octubre 2018, Disponible en https://cwe.mitre.org/data/definitions/345.html

En esta categoría se encuentran 1.728 vulnerabilidades que indican que la pagina contiene script de un dominio de terceros, lo que permite ejecutar elementos no seguros o que su fuente es externa, por tanto, se salen del perímetro seguro.

Descripción
La amenaza se relaciona con la incorrecta configuración de aplicación y se explotan deficiencias de configuración de la plataforma WEB.

Figura 39 Detalle Vulnerabilidad



Fuente: El autor

El código relacionado con la vulnerabilidad es: CWE-15 Configuración incorrecta de la aplicación

Solución
Se debe asegurar que los javascript fuentes usados solo se carguen de fuentes confiables y que los orígenes de datos no puedan ser controlados por los usuarios finales de las aplicaciones.
No se debe dejar configurado con opciones predeterminadas los accesos y usuarios de la plataforma a fin de evitar un ataque de suplantación que use esos parámetros por defecto.

Como conclusión de los resultados recopilados se identifican fallos que están catalogados dentro de los siguientes ítems del top 10 de Owasp 2017:
A4:2017 - Entidades Externas XML (XXE)
A5:2017 – Pérdida de Control de Acceso:
A6:2017 - Configuración de Seguridad Incorrecta
A7:2017 - Cross-Site Scripting (XSS)

4.3 CONTROLES

Teniendo en cuenta que existen muchas vulnerabilidades listadas y que algunas pueden tener mayor gravedad que otras, es necesario que se realice una actualización del gestor de contenido Liferay Portal 7 a su versión actualizada y estable disponible, a fin de disminuir o mitigar las vulnerabilidades identificadas que de acuerdo con la versión se listan 6 fallos de seguridad relacionados con ***Cross-Site Scripting (XSS)***, para aquellas que no representan un riesgo alto los controles y recomendaciones que deben aplicarse inician con revisión de procesos o procedimientos, revisión de plataforma para garantizar que no se presenten afectaciones o se mitiguen los fallos.

- En primer lugar, se deben restringir los accesos a servicios que no son requeridos, así mismo, se deben restringir los accesos administrativos al grupo de usuarios encargados de esta tarea.
- Continuar con los procesos de pruebas y evaluación de código fuente para disminuir el riesgo ante posibles fallas que el software tenga y que no se han identificado.
- Revisar y ajustar la matriz de riesgo de la plataforma para validar que no hay cambios de estos.
- Continuar con la documentación o actualización de la existente para facilitar auditorias.

Para los fallos identificados se resume lo siguiente:
A4:2017 - Entidades Externas XML (XXE)[36]

La evaluación del código y el entrenamiento del desarrollador es esencial para identificar y mitigar defectos de XXE. Aparte de esto, prevenir XXE requiere:

- De ser posible, utilice formatos de datos menos complejos como JSON y evite la serialización de datos confidenciales.
- Actualice los procesadores y bibliotecas XML que utilice la aplicación o el sistema subyacente. Utilice validadores de dependencias. Actualice SOAP a la versión 1.2 o superior.
- Deshabilite las entidades externas de XML y procesamiento DTD en todos los analizadores sintácticos XML en su aplicación, según se indica en la hoja de trucos para prevención de XXE de OWASP.
- Implemente validación de entrada positiva en el servidor (“lista blanca”), filtrado y sanitización para prevenir el ingreso de datos dañinos dentro de documentos, cabeceras y nodos XML.

---

[36] OWASP, HERRAMIENTAS, Herramientas OWASP [Disponible en] https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf, pág. 10.

- Verifique que la funcionalidad de carga de archivos XML o XSL valide el XML entrante, usando validación XSD o similar.
- Las herramientas SAST pueden ayudar a detectar XXE en el código fuente, aunque la revisión manual de código es la mejor alternativa en aplicaciones grandes y complejas.
- Si estos controles no son posibles, considere usar parcheo virtual, gateways de seguridad de API, o Firewalls de Aplicaciones Web (WAFs) para detectar, monitorear y bloquear ataques XXE.

A5:2017 – Pérdida de Control de Acceso[37]:
El control de acceso sólo es efectivo si es aplicado del lado del servidor o en Server-less API, donde el atacante no puede modificar la verificación de control de acceso o los metadatos.

- Con la excepción de los recursos públicos, la política debe ser denegar de forma predeterminada.
- Implemente los mecanismos de control de acceso una vez y reutilícelo en toda la aplicación, incluyendo minimizar el control de acceso HTTP (CORS).
- Los controles de acceso al modelo deben imponer la propiedad (dueño) de los registros, en lugar de aceptar que el usuario puede crear, leer, actualizar o eliminar cualquier registro.
- Los modelos de dominio deben hacer cumplir los requisitos exclusivos de los límites de negocio de las aplicaciones.
- Deshabilite el listado de directorios del servidor web y asegúrese que los metadatos/fuentes de archivos (por ejemplo de GIT) y copia de seguridad no estén presentes en las carpetas públicas.
- Registre errores de control de acceso y alerte a los administradores cuando corresponda (por ej. fallas reiteradas).
- Limite la tasa de acceso a las APIs para minimizar el daño de herramientas de ataque automatizadas.
- Los tokens JWT deben ser invalidados luego de la finalización de la sesión por parte del usuario.
- Los desarrolladores y el personal de QA deben incluir pruebas de control de acceso en sus pruebas unitarias y de integración.

---

[37] OWASP, HERRAMIENTAS, Herramientas OWASP [Disponible en] https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf, pág. 11.

A6:2017 - Configuración de Seguridad Incorrecta[38]

Deben implementarse procesos seguros de instalación, incluyendo:

- Proceso de fortalecimiento reproducible que agilice y facilite la implementación de otro entorno asegurado. Los entornos de desarrollo, de control de calidad (QA) y de Producción deben configurarse de manera idéntica y con diferentes credenciales para cada entorno. Este proceso puede automatizarse para minimizar el esfuerzo requerido para configurar cada nuevo entorno seguro.
- Use una plataforma minimalista sin funcionalidades innecesarias, componentes, documentación o ejemplos. Elimine o no instale frameworks y funcionalidades no utilizadas.
- Siga un proceso para revisar y actualizar las configuraciones apropiadas de acuerdo con las advertencias de seguridad y siga un proceso de gestión de parches. En particular, revise los permisos de almacenamiento en la nube (por ejemplo, los permisos de buckets S3).
- La aplicación debe tener una arquitectura segmentada que proporcione una separación efectiva y segura entre componentes y acceso a terceros, contenedores o grupos de seguridad en la nube (ACLs).
- Envíe directivas de seguridad a los clientes (por ej. cabeceras de seguridad).
- Utilice un proceso automatizado para verificar la efectividad de los ajustes y configuraciones en todos los ambientes.

A7:2017 - Cross-Site Scripting (XSS)[39]

Prevenir XSS requiere mantener los datos no confiables separados del contenido activo del navegador.

- Utilizar frameworks seguros que, por diseño, automáticamente codifican el contenido para prevenir XSS, como en Ruby 3.0 o React JS.
- Codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML (cuerpo, atributos, JavaScript, CSS, o URL) resuelve los XSS Reflejado y XSS Almacenado. La hoja de trucos OWASP para evitar XSS tiene detalles de las técnicas de codificación de datos requeridas.
- Aplicar codificación sensitiva al contexto, cuando se modifica el documento en el navegador del cliente, ayuda a prevenir DOM XSS. Cuando esta técnica

---

[38] OWASP, HERRAMIENTAS, Herramientas OWASP [Disponible en] https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf, pág. 12.

[39] OWASP, HERRAMIENTAS, Herramientas OWASP [Disponible en] https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf, pág. 13.

no se puede aplicar, se pueden usar técnicas similares de codificación, como se explica en la hoja de trucos OWASP para evitar XSS DOM.

- Habilitar una Política de Seguridad de Contenido (CSP) es una defensa profunda para la mitigación de vulnerabilidades XSS, asumiendo que no hay otras vulnerabilidades que permitan colocar código malicioso vía inclusión de archivos locales, bibliotecas vulnerables en fuentes conocidas almacenadas en Redes de Distribución de Contenidos (CDN) o localmente.

5 CONCLUSIONES

Como resultado del trabajo se puede concluir:

- Que se obtuvo el objetivo planteado de evaluar la seguridad del sitio web mediante pruebas de pentesting e identificar las vulnerabilidades que estaban expuesta por la plataforma.
- Dentro del proceso de pentesting no solo se evidenció que hay vulnerabilidades que pueden ser explotadas por un atacante, sino que también se pueden entregar controles para aplicar a fin de minimizar el riesgo de ataque.
- Se puede concluir que, para efectuar pruebas de este tipo, se requiere una inversión baja dado que puede ser usado software libre, puede ser medido y evaluado el impacto de una afectación de seguridad.
- Que es posible definir un procedimiento que ayude a auditar, evaluar y entregar recomendaciones o controles para las vulnerabilidades de aplicaciones Web de una empresa.
- Se puede concluir que debe planearse una evaluación de seguridad y listar unos objetivos para el test a realizar a fin de enfocarse en buscar esos posibles fallos.

6 RECOMENDACIONES

Para poder dar solución a las vulnerabilidades encontradas y prevenir la aparición de agujero o fallos de seguridad se recomienda:

- Dado que no se evidencia vulnerabilidades críticas en las pruebas, pero si algunas que para la entidad no son valoradas de impacto alto, es necesario que se continúen con las auditorias periódicas, a fin de cumplir con el numeral 12.6.1 Gestión de las vulnerabilidades técnicas, para esto se debe revisar las pruebas aplicadas y riesgos de manera periódica a fin de identificar nuevas amenazas.
- Para garantizar el numera 17.1.3 “Verificación, revisión y evaluación de la continuidad de la seguridad de la información”. Se recomienda que los planes de contingencia que se tengan se actualicen o diseñen nuevamente para permitir restaurar los ambientes afectados por un ataque, de esta manera se puede garantizar la disponibilidad y continuidad de la plataforma.
- Se recomienda implementar certificados y mecanismos que permitan asegurar la comunicación y los datos que se trasmiten, habilitar https para la página web.
- Dentro de las recomendaciones que deben aplicarse esta el revisar la configuración, parches de seguridad y realizar auditorías periódicas que permitan identificar nuevos fallos de seguridad de la plataforma, donde igualmente se actualice la documentación permitiendo la continuidad y rápida recuperación ante un incidente.
- Por último, una inscripción en boletines de seguridad para atender recomendaciones de vulnerabilidades que son detectadas por especialistas agiliza la aplicación de correctivos de software que deban ser aplicados sobre la infraestructura del sitio web.
- Teniendo en cuenta la ISO 27000 se debe evaluar la política de seguridad y validar si la misma se esta cumpliendo o debe ajustarse.

7 BIBLIOGRAFÍA

ALDEGANI, G. M. (1997). *Seguridad Informática.* ARGENTINA: MP EDICIONES. Recuperado el Noviembre de 2018

Alvarez, M. A. (abril de 2017). *DesarrolloWeb.* Obtenido de DesarrolloWeb: https://desarrolloweb.com/articulos/que-es-html.html

Ascencio Mendoza, M., & Moreno Patiño, P. J. (2011). *Repositorio Universidad Tecnologica de Pereira.* Recuperado el 18 de Octubre de 2016, de Universidad Tecnologica de Pereira: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf?sequence=1

ASCENCIO MENDOZA, M., & MORENO PATIÑO, P. J. (s.f.). *http://repositorio.utp.edu.co/.* Obtenido de http://repositorio.utp.edu.co/: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf

Benítez Andrades, J. A. (8 de Agosto de 2013). *http://www.jabenitez.com/#home*. Obtenido de http://www.jabenitez.com/#home: http://www.jabenitez.com/2013/08/08/joomla-hackeado-exploit-del-plugin-jce-editor/

Common Vulnerabilities and Exposures. (23 de Diciembre de 2011). Obtenido de Common Vulnerabilities and Exposures: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4908

CVE Details. (20 de Mayo de 2009). Obtenido de CVE Details: https://www.cvedetails.com/cve/CVE-2009-1499

Foundation, O. (2017). *https://www.owasp.org.* Recuperado el Noviembre de 2018, de https://www.owasp.org: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

GONZÁLEZ GÓMEZ, D. (1 de Mayo de 2016). *www.criptored.upm.es.* Obtenido de www.criptored.upm.es: http://www.criptored.upm.es/guiateoria/gt_m481a.htm

HERZOG, P. (Marzo de 2016). *http://www.isecom.org.* Recuperado el Marzo de 2016, de http://www.isecom.org: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

https://www.auditool.org/. (5 de Junio de 2015). Obtenido de https://www.auditool.org/: https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque

https://www.incibe.es/. (1 de Mayo de 2016). Obtenido de https://www.incibe.es/: https://www.incibe.es/CERT/guias_estudios/guias//guia_information_gathering

https://www.microsoft.com. (1 de Mayo de 2016). Obtenido de https://www.microsoft.com: https://www.microsoft.com/latam/technet/seguridad/boletines/rating.mspx

HUERTA, A. V. (Septiembre de 2004). *http://www.criptored.upm.es/.* Recuperado el Marzo de 2016, de http://www.criptored.upm.es/: http://www.criptored.upm.es/descarga/ISO17799avh.zip

Instituto Nacional de Ciberseguridad. (20 de Febrero de 2017). Obtenido de Incibe: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

joomla Developer Network. (17 de Octubre de 2015). Obtenido de joomla Developer Network: https://developer.joomla.org/security/news/301-20090722-core-file-upload.html

Martí Talón, R. M. (20 de Septiembre de 2016). *RuiNet.* Recuperado el 17 de Noviembre de 2016, de Repositorio Institucional UPV: https://riunet.upv.es/handle/10251/70164

MCCLURE, S. S. (s.f.). *Hackers, Secretos y soluciones para seguridad de redes.* Mexico D.F.: McGraw-Hill.

Morales, R. (1 de Septimbre de 2014). *Colombia Digital*. Obtenido de Colombia Digital: https://colombiadigital.net/actualidad/articulos-informativos/item/7669-lenguajes-de-programacion-que-son-y-para-que-sirven.html

Openwebinars. (18 de Febrero de 2016). Recuperado el 18 de Febrero de 2016, de Openwebinars: https://openwebinars.net/que-es-el-pentesting/

PHP. (enero de 2017). Obtenido de php.net: http://php.net/manual/es/intro-whatis.php

RAE. (2005). Obtenido de RAE: http://lema.rae.es/dpd/srv/search?id=HTm1EjFzPD6zs66ao6

Ronderos, M. F. (Legislación informática y protección de datos en Colombia, comparada con otros países de Legislación informática y protección de datos en Colombia, comparada con otros países de 2014). *Legislación informática y protección de datos en Colombia, comparada con otros países*. Recuperado el 3 de 2 de 2018, de Legislación informática y protección de datos en Colombia, comparada con otros países: http://biblioteca.uniminuto.edu/ojs/index.php/inventum/article/view/1014

securitybydefault.com. (Febrero de 2016). Recuperado el 19 de Febrero de 2016, de securitybydefault.com: http://www.securitybydefault.com/2011/11/uso-de-burp-intruder-para-ataques-de.html

Seifreed. (Noviembre de 2016). *http://www.dragonjar.org/joomscan-analizando-joomla.xhtml.* Obtenido de http://www.dragonjar.org/joomscan-analizando-joomla.xhtml: http://www.dragonjar.org/joomscan-analizando-joomla.xhtml

Universidad Internacional de Valencia. (9 de Setiembre de 2016). Obtenido de Universidad Internacional de Valencia: http://www.viu.es/la-seguridad-informatica-puede-ayudarme/

ww.elempleo.com. (1 de Mayo de 2016). Obtenido de El empleo: ww.elempleo.com

www.isaca.org. (15 de Marzo de 2016). Recuperado el 15 de Marzo de 2016, de www.isaca.org: http://www.isaca.org/chapters8/Montevideo/Events/Documents/penetration%20testing%20-%20conceptos%20generales%20y%20situacin%20actual.pdf

Yánez Cedeño, E. (26 de Mayo de 2016). *Universidad Politécnica de Madrid.* Recuperado el 20 de Septiembre de 2016, de Departamento de Ingeniería de Sistemas Telemáticos - ETSIT - UPM:

http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf