UNIDAD ACADÉMICA

OFICINA DE INVESTIGACIÓN Y POSTGRADOS

TEMA:

ESTRATEGIA PARA LA DETECCIÓN DE VULNERABILIDADES EN LA APLICACIÓN WEB DE LA AGENCIA NACIONAL DE TRÁNSITO COMO HERRAMIENTA PARA LA TOMA DE DECISIONES

Proyecto de Investigación y Desarrollo previo a la obtención del título de:

Magister en Gerencia Informática

Línea de Investigación, Innovación y Desarrollo:

Ingeniería de Software y/o Plataformas Educativas

Caracterización técnica del trabajo:

Desarrollo

Autor:

Raúl Alfredo Panchi Herrera

Director:

Ricardo Patricio Medina Chicaiza; Ing. Mg.

Ambato - Ecuador

Agosto 2017

Estrategia para la detección de vulnerabilidades la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones

Informe de Trabajo de Titulación

presentado ante la

Pontificia Universidad Católica del Ecuador

Sede Ambato

por:

Raúl Alfredo Panchi Herrera

En cumplimiento parcial de

los requisitos para el Grado de

Magister en Gerencia Informática

Oficina de Investigación y Postgrados

Agosto 2017

Estrategia para la detección de vulnerabilidades en la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones

Aprobado por:

Diego Armando Jiménez Bósquez, Mg.
Presidente del comité calificador
Coordinador de la oficina de Investigación y Postgrados

Elsa Pilar Urrutia Urrutia, Mg.
Miembro Calificador

Ricardo Patricio Medina Chicaiza, Mg.
Miembro Calificador
Director de Proyecto

Hugo Rogelio Altamirano Villarroel, Dr.
Secretario General

José Marcelo Balseca Manzano, Mg.
Miembro Calificador

Fecha de aprobación:
Agosto, 2017

Ficha Técnica

Programa: Maestría en Gerencia Informática

Tema: Estrategia para la detección de vulnerabilidades en la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones

Tipo de trabajo: Proyecto

Clasificación técnica del trabajo: Desarrollo

Autor: Raúl Alfredo Panchi Herrera

Director: Ing. Ricardo Patricio Medina Chicaiza Mg.

Línea de Investigación, Innovación y Desarrollo:

Principal: Ingeniería de Software y/o Plataformas Educativas

Secundaria: Redes y aplicaciones.

Resumen Ejecutivo

Para mejorar los mecanismos de seguridad y optimizar los servicios que proveen los aplicativos web, tanto de entidades públicas es imperiosamente necesario efectuar detección de vulnerabilidades y posteriormente pruebas de penetración, las cuales hagan posible la toma de decisiones en pos de implementar procedimientos de seguridad y estar un paso delante de cualquier potencial ataque por parte de hackers.

El presente documento plasma una revisión documental de conceptos esenciales sobre aplicaciones web, su infraestructura, vulnerabilidades, así como pone en evidencia algunas técnicas, procedimientos, herramientas, metodología, para efectuar detección de vulnerabilidades a los aplicativos web, las cuales son utilizadas por delincuentes cibernéticos para vulnerarlas y cometer delitos enmarcados en el ámbito informático.

Como objetivo de análisis se tomó al aplicativo web de la Agencia Nacional de Tránsito del Ecuador, cuya infraestructura fue violentada a inicios de año, el resultado de la presente propuesta fue evidenciar las vulnerabilidades encontradas mediante el formato de "Informe Técnico Pericial", usado por parte de Peritos del Consejo de la Judicatura, para reportar las conclusiones llegadas, luego de la aplicación de un procedimiento técnico el cual es el soporte para una decisión al momento de impartir justicia, para el caso servirá como una herramienta documental para tomar decisiones en el aspecto de seguridad al aplicativo web analizado.

Declaración de Originalidad y Responsabilidad

Yo, Raúl Alfredo Panchi Herrera, portador de la cédula de ciudadanía Nº 0502521032, declaro que los resultados obtenidos en el proyecto de titulación y presentados en el informe final, previo a la obtención del título de Magister en Gerencia Informática; son absolutamente originales y personales. En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

Raúl Alfredo Panchi Herrera

C.I. 0502521032

Dedicatoria

El presente trabajo lo dedico al afecto y calor del seno familiar.

A mi Hija Emilia Augusta,

A mi Esposa Martha Verónica,

A mis Padres Angelita y César.

A mi Hermano César Augusto.

A Dios por cobijarnos con su bendición, en los momentos difíciles encontrados en el sendero de la vida, y por esa fortaleza brindada para superarlos.

Raúl

Reconocimiento

Mi reconocimiento y agradecimiento a la Pontificia Universidad Católica del Ecuador Sede Ambato, en su nombre al personal docente, quienes supieron impartir una formación académica de calidad, con deferencia especial al Ing. Patricio Medina, director, por su apoyo y aliento para la consecución del presente proyecto.

A la Agencia Nacional de Tránsito del Ecuador, institución que me permitió brindar mis servicios profesionales y abrió las puertas para el desarrollo del objetivo de evaluación.

Al Consejo de la Judicatura, entidad que me permitió adquirir experiencia en el mundo de la investigación tecnológica en calidad de Perito Judicial Informático.

A la Secretaría de Educación Superior, Ciencia Tecnología e Innovación, entidad en la cual actualmente brindo mi contingente en pos de la formación técnica y tecnológica del país.

Raúl

Resumen

Para mejorar la seguridad de las aplicaciones web, es pertinente detectar vulnerabilidades, resultados que permitan implementar procedimientos de seguridad, para prevenir potenciales ataques. Por ello, el objetivo del presente trabajo es desarrollar una estrategia para detectar vulnerabilidades en la aplicación web de la Agencia Nacional de Tránsito. La investigación se basa en un marco metodológico mixto, empleando técnicas, procedimientos y herramientas, para descubrir potenciales vulnerabilidades en el objetivo de evaluación, además la investigación documental, abordando referentes teóricos como el proyecto OWASP[1], y artículos relacionados a delitos informáticos referidos en el COIP[2], también la investigación de campo, evidenciando una problemática de intrusión real y alteración de datos de licencias de conducir, denunciada ante organismos de justicia, y difundida por medios de comunicación, adicionalmente la investigación explicativa, determinando las causas que originan el problema. En la práctica empleado la técnica Black box hacking, y la metodología OWASP[3], abordando las fases de reconocimiento, mapeo y descubrimiento, con perspectiva de hacking ético. Los resultados de vulnerabilidades, obtenidos, y las recomendaciones, se describe en un modelo de "Informe Pericial", usado por Peritos del Consejo de la Judicatura, para reportar conclusiones, producto de aplicar procedimientos técnicos, siendo el soporte decisivo para impartir justicia, para el caso se entrega un documento para tomar decisiones en cuanto a seguridad del aplicativo web analizado.

Palabras clave: Aplicaciones web, Pruebas de penetración, Vulnerabilidades, Hacking ético.

[1] Open Web Application Security Project (Proyecto abierto de seguridad en aplicaciones web)
[2] Código Orgánico Integral Penal del Ecuador
[3] Metodología para pruebas de penetración abarca las fases de reconocimiento, mapeo, descubrimiento y explotación.

Abstract

To improve security of web applications, it is necessary to detect vulnerabilities. This facilitates implementation of security procedures which prevent potential attacks. To this end, the objective of this project is to develop a strategy to detect of vulnerabilities on the web application of Ecuador's National Transit Agency (Agencia Nacional de Tránsito). A mixed methodology was adopted for research, using different techniques, procedures and tools in order to detect potential vulnerabilities in the application under evaluation. Further to this, documentary research was carried out, addressing theoretical references such as the Open Web Application Security Project (OWASP) and articles related to computer-related crime as described in Ecuador's Organic Penal Code (Código Orgánico Integral Penal del Ecuador). Field research highlighted a problem of intrusion and tampering with drivers' licence data, which has been reported to criminal justice agencies and published by the media. In addition, explanatory research was used to determine the causative factors of the issue under research. In practice, the Black Box hacking technique is often employed, which uses an OWASP methodology, which is made up of recognition, mapping and discovery phases, and using an ethical hacking perspective. The results obtained concerning vulnerabilities were sufficient to make recommendations, which are described in a forensic report, as used by experts at the Judiciary Council. The conclusions of this product were reached following technical processes, which are sufficient evidence to impart justice. In each case, a document is presented to aid in decision taking regarding the security of the web application under analysis.

Keywords: web applications, penetration test, vulnerabilities, ethical hacking.

Tabla de Contenidos

Lista de Tablas

Lista de Figuras

Capítulo 1

Introducción

El trabajo de investigación de tipo desarrollo titulado "Estrategia para la detección de vulnerabilidades en la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones", aborda aspectos relacionados con el hacking ético, vulnerabilidades en aplicaciones web, así como aspectos legales relacionados con los delitos informáticos en el Ecuador, concomitante con lo que se desarrolla una estrategia, la cual empleando una metodología, herramientas y procedimientos tecnológicos, se delinean procedimientos para evidenciar potenciales vulnerabilidades que se puedan localizar en el aplicativo web de la entidad considerada objetivo de evaluación.

En el aspecto legal se aborda artículos del Código Orgánico Integral Penal, los cuales refieren a los delitos informáticos establecidos y tipificados en el Ecuador, así como se aborda el Esquema Gubernamental de Seguridad de la Información, vigente en el país, para las entidades públicas, del cual se refiere aspectos relacionados con la factibilidad de aplicar y desarrollar proyectos enfocados a contribuir con procesos que coadyuven el aseguramiento de la información hacia entidades del sector público, por parte de entes o profesionales, mediante la contribución desde una perspectiva externa, para brindar lineamientos que puedan ser tomados en consideración para prevenir ataques especialmente hacia los aplicativos web por parte de hackers.

Aspecto importante, es indicar que el proceso investigativo se lo desarrolla desde una perspectiva del hacking ético, ya que el alcance presentado hacia la entidad objetico de evaluación, determina la ejecución de las etapas de reconocimiento, mapeo, y descubrimiento de posibles vulnerabilidades en el aplicativo web de la entidad evaluada, más se aclara la no realización de la etapa de explotación, ya que el proyecto al ser de índole académica, no se orienta a causar daños o detener el normal funcionamiento de la infraestructura tecnológica del estamento público evaluado.

1.1. Presentación del trabajo

La presente propuesta proyecta evidenciar algunas vulnerabilidades encontradas en el aplicativo web de la Agencia Nacional de Tránsito del Ecuador, luego de aplicar una metodología utilizada para detección de vulnerabilidades y posteriores pruebas de penetración hacia aplicativos web, en la cual se cumplirán las etapas de Reconocimiento, Mapeo y Descubrimiento, con excepción de la fase de Explotación, esto debido a que el enfoque del desarrollo de las actividades se las hace desde la perspectiva de hacking ético, mas no es el afán violentar y poner en riesgo la integridad y normal funcionamiento de servicios que brinda el aplicativo.

En el proceso investigativo documental se referirá a terminología y conceptos sobre aplicaciones web, seguridad de las mismas, hacking ético, riesgos de seguridad según OWASP (Open Web Application Security Project), pruebas de penetración y sus tipos, arquitectura de servidores web y sus tipos, legislación ecuatoriana sobre delitos informáticos, y aspectos sobre vulnerabilidades, recogidos en el Esquema Gubernamental de Seguridad de la Información (EGSI).

La plataforma seleccionada para llevar a efecto la detección de vulnerabilidades y que posibilita la ejecución de pruebas de penetración hacia el aplicativo web objetivo de evaluación es Samurai Web Testing Framework en su versión 3.0, ya que dicha plataforma es de código abierto y contiene herramientas gratuitas que se enmarcan en evaluar la seguridad y en auditar los perfiles de seguridad de sitios y aplicaciones web.

La metodología utilizada es OWASP, la cual consiste en ejecutar de forma secuencial las fases de Reconocimiento, Mapeo, Descubrimiento y Explotación, de las vulnerabilidades localizadas en el objetivo de evaluación, pero para el caso no se llevará a efecto la fase de Explotación por estar fuera del alcance de la propuesta al enmarcarse en el ámbito del Hacking ético.

Una vez aplicadas las herramientas, de la mano de procedimientos, los resultados de las vulnerabilidades detectadas, se los condensará utilizando el modelo de un “Informé Pericial”, el cual servirá como herramienta para la toma de decisiones en el marco de seguridad del aplicativo web, por parte del personal encargado de TI (Tecnologías de la Información) del a entidad objetivo de análisis.

1.2. Descripción del Documento

El presente trabajo está dividido en capítulos, mismos que abarcan aspectos como: en el Capítulo 2 se hace referencia a la propuesta del trabajo, mientras que en el Capítulo 3 se enuncia el Marco Teórico, abordando definiciones y conceptos esenciales sobre la temática en la Sección 3.1, en tanto que en la Sección 3.2 se establece el Estado del Arte, posteriormente en el Capítulo 4 se muestra la Metodología con la etapa de Diagnóstico en la Sección 4.1, la metodología específica utilizada en la propuesta en la Sección 4.2, para en la sección 4.3 mencionar los Materiales y Herramientas utilizados, en el Capítulo 5 se enfoca la Presentación y Análisis de los Resultados de la propuesta, y finalmente en el Capítulo 6 se establecen las Conclusiones y Recomendaciones, además se muestran documentos como la solicitud para la autorización a llevar a efecto la detección de vulnerabilidades y sugerir la ejecución de posteriores pruebas de penetración dirigida a la Agencia Nacional de Tránsito, así como también el formulario de encuesta aplicado al personal del departamento de TI de la entidad, y finalmente se muestra el formato del informe pericial documento guía para la presentación de informes de Consejo de la Judicatura.

Capítulo 2

Planteamiento de la Propuesta de Trabajo

2.1. Información técnica básica

Programa: Maestría en Gerencia Informática.

Tema: "Estrategia para la detección de vulnerabilidades en la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones"

Tipo de trabajo: Proyecto

Caracterización técnica del trabajo: Desarrollo

Línea de Investigación, Innovación y Desarrollo:

Principal: Ingeniería de Software y/o Plataformas Educativas

Secundaria: Redes y aplicaciones

Autor: Raúl Alfredo Panchi Herrera.

Director: Ing. Ricardo Patricio Medina Chicaiza Mg.

2.2. Descripción del problema

Al ser "el ciberespacio un ámbito virtual en el que, desde hace algunos años, gran parte de la población está expuesta", al (Medina & Molist, 2015), no fuera de tono es la preocupación de los usuarios respecto a la privacidad de la información que es gestionada en los diferentes aplicativos web (Mateu, 2004) de entidades especialmente del sector público, estando sin excepción alguna

expuestos a sufrir incidencias de seguridad, con graves consecuencias como daños económicos, morales, robo de información privada, retraso en la gestión de procesos, entre otros.

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP "Open Web Application Security Project") en (OWASP, OWASP Top 10 - 2013, 2013) , refiere encabezando el listado de riesgos a las fallas de inyección al ser enviados datos no confiables a un intérprete como una instrucción o consulta, en cuarto lugar la referencia directa insegura a objetos, cuando un desarrollador expone la referencia a un objeto de implementación interno, como fichero, directorio, o base de datos, en quinto lugar la configuración de seguridad incorrecta, al no definir una buena configuración de seguridad para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma, en séptimo lugar se describe la ausencia de control de acceso a funciones, cuando no se verifican las solicitudes de acceso, pudiendo atacar mediante peticiones sin la autorización apropiada, en noveno lugar la utilización de componentes con vulnerabilidades conocidas en donde componentes como las librerías, framework y otros módulos casi siempre requieren privilegios totales para funcionar, facilitando la intrusión en el servidor; aspectos de seguridad que serán abordados en el proyecto.

En consecuencia mientras más se conecta el mundo, para gestionar transacciones a través de la web es necesario e importante verificar qué tan seguros son dichos aplicativos, más aun poniéndose literalmente en "los zapatos" de atacantes mediante el uso de técnicas, procedimientos y herramientas de su uso, conocimiento y dominio para vulnerar aplicativos y cometer actos delictivos a nivel informático, para prevenirlos evidenciándolos y poniendo en conocimiento de las instituciones evaluadas dirigido como herramienta para la toma de decisiones al personal encargado del desarrollo de aplicativos.

Por la experiencia laboral en la Agencia Nacional de Tránsito (ANT), se conoce que dicha entidad dispone de un aplicativo web el cual permite realizar transacciones en línea sean éstas consultas de multas, turnos para obtener licencias, validación de certificados de conductor, estado de licencia, entre otras, que son factibles de realizar por parte de los usuarios a través de internet, evidencian además que dicho aplicativo web interactúa con equipos servidores y acceso a bases de datos los mismos que almacenan información vital de usuarios y distintos procesos, información que es apetecida por Hackers, quienes cuentan con conocimientos en técnicas, herramientas y procedimientos para vulnerar aplicativos web con la finalidad de robar información, causar daños tecnológicos, dañar la imagen de personas o instituciones y el principal obtener réditos económicos, evidencia de ello es la desarticulación de una red de hackers como se

publica en (Policía Nacional del Ecuador, 2016), quienes consiguieron vulnerar aplicativos web de algunas entidades públicas de Ecuador como la ANT y la Secretaría de Educación Superior, Ciencia Tecnología e Innovación (SENESCYT), haciendo uso de técnicas descritas en (Rando & Alonso, 2014), en las que como consecuencia se concretaron delitos informáticos al registrar licencias de conducir y títulos profesionales especialmente de tercero y cuarto nivel de forma fraudulenta respectivamente en cada uno de los casos, incurriendo en el cometimiento de un delito informático como lo refiere en (Fiscalía General del Estado, 2015), que de acuerdo al Artículo 190 del (Ministerio de Justicia Derechos Humanos y Cultos, 2014), Apropiación fraudulenta por medios electrónicos, establece pena privativa de la libertad de uno a tres años.

2.3. Preguntas básicas

¿Cómo aparece el problema que se pretende solucionar?

Al detectar registros inconsistentes en la base de datos, los cuales no tienen respaldo documental.

¿Por qué se origina?

Por la falta de implementación de políticas de seguridad en aplicaciones web

¿Qué lo origina?

Las violaciones de seguridad concretadas por delincuentes informáticos en el aplicativo web de la Agencia Nacional de Tránsito, habiendo alterado datos de licencias y valores de multas.

¿Cuándo se origina?

Al haber ingresado a la base de datos y alterado los campos de valores por concepto de multas e ingresando datos para la generación de licencias.

¿Dónde se origina?

En la base de datos de la Agencia Nacional de Tránsito.

¿Dónde se detecta?

En la comparación de los backups de las bases de datos.

2.4. Formulación de meta

Desarrollar una estrategia para la detección de vulnerabilidades en el aplicativo web de la Agencia Nacional de Tránsito como una herramienta para la toma de decisiones.

2.5. Objetivos

2.5.1. Objetivo general

Desarrollo de una estrategia para la detección de vulnerabilidades en el aplicativo web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones.

2.5.2. Objetivos específicos

- Fundamentar teórica y metodológicamente sobre vulnerabilidades en aplicaciones web.
- Diagnosticar la situación actual de uso de procedimientos para la detección de vulnerabilidades en el aplicativo web de la Agencia Nacional de Tránsito.
- Utilizar procedimientos, técnicas y herramientas, empleados para vulnerar aplicativos web, en el aplicativo de la Agencia Nacional de Tránsito.
- Utilizar el formato de un informe pericial del Consejo de la Judicatura para difundir los resultados obtenidos.

2.6. Delimitación funcional

2.6.1. ¿Qué será capaz de hacer el producto final del proyecto de titulación?

- En el proceso de documentación se podrán identificar las modalidades de Hacking.

- Evidenciará metodologías para reconocimiento o Footprinting.
- Evidenciará técnicas utilizadas para escaneo y enumeración.
- Empleará un framework de escaneo y explotación además de mecanismos de ataques.

2.6.2. ¿Qué no será capaz de hacer el producto final del proyecto de titulación?

- La estrategia establecida no corregirá automáticamente errores de programación detectados en la fase de análisis y escaneo de vulnerabilidades.
- No generará código de programación para implementación de aspectos de seguridad en los aplicativos analizados.
- No se explotará la vulnerabilidad analizada y detectada, por ser un aspecto de Hacking Ético.

Capítulo 3

Marco Teórico

3.1. Aplicaciones web

En sus inicios las aplicaciones web se basaban en una estructura cliente–servidor, conformándose por un programa cliente más una interfaz de usuario, los que debían ser instalados en cada una de las estaciones de trabajo desde donde se accedería a la aplicación, generando costos de servicio técnico, más en la actualidad las aplicaciones web generan de forma dinámica una serie de páginas que constituyen la aplicación cliente y sus interfaz que son soportadas por navegadores web mediante lenguaje HTML[4], teniendo como ventaja el ahorro en el coste de servicio técnico al no requerir de instalación de clientes específicos para los diversos sistemas operativos, se escribe la aplicación una sola vez y puede ser mostrada en cualquier navegador a su vez en cualquier sistema operativo. (Vértice, 2010)

Se establecen varias definiciones de Aplicaciones Web dadas por diferentes autores (Ver tabla 1). Partiendo del análisis de estas definiciones el autor señala que reciben ese nombre porque se ejecutan a través de internet, a las cuales se accede mediante un navegador y se basan en una arquitectura cliente- servidor, y proveen de información y gestión de servicios a usuarios desde cualquier parte del mundo.

Tabla 1: Definiciones de Aplicaciones Web según autores.

Autor	Año	Concepto
Aumaille	2002	"Una aplicación Web es un conjunto de recursos Web que participan en el funcionamiento de la propia aplicación Web"
Miño	2010	"Las aplicaciones web son aplicaciones a las que se accede mediante un navegador y están alojadas en servidores dentro de una intranet o en internet."

[4] HyperText Markup Language: Lenguaje de marcado para la elaboración de páginas web.

Lujan	2012	"Una aplicación web es un tipo especial de aplicación cliente/servidor, donde tanto el cliente (el navegador, explorador o visualizador) como el servidor (el servidor web) y el protocolo mediante el que se comunican (HTTP) están estandarizados y no han de ser creados por el programador de aplicaciones." (Lujan, 2012)
Berzal, Cortijo & Cubero	2013	"…las aplicaciones web nos permiten ofrecer la información más actual de la que disponemos al poder acceder directamente a las bases de datos que contienen los datos operativos de una empresa." (Berzal, Cortijo, & Cubero, 2013)

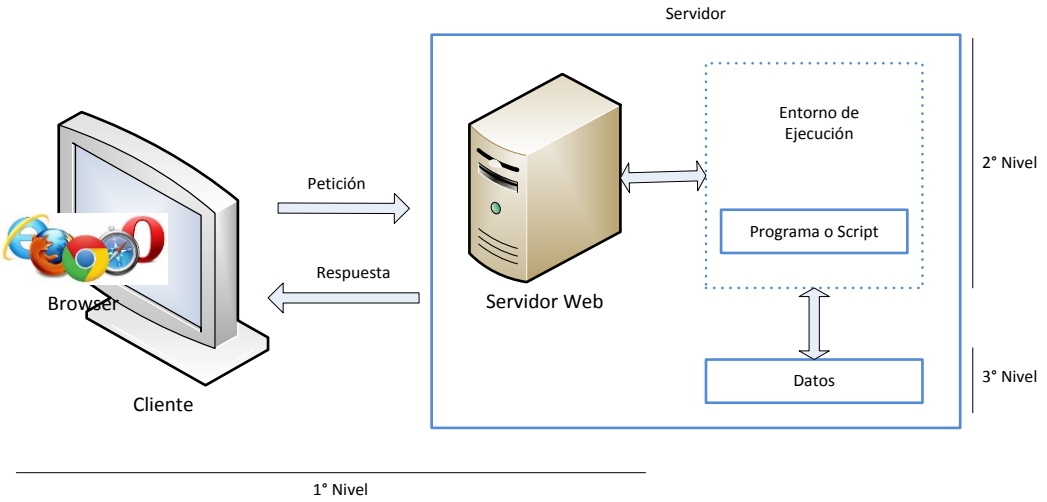
Fuente: elaboración propia

3.2. Niveles de una aplicación web

Desde la creación de la web en 1989 por Tim Berners Lee, época en la cual se la consideraba como una "*forma de organizar la información*" (Ramos, 2011), con la intervención de internet como medio físico de comunicación y el protocolo HTTP[5], usado por los navegadores para efectuar peticiones al servidor web y a su vez recibir la respuesta, y gracias a la difusión de internet, en la actualidad los aplicativos web permiten a los usuarios interactuar directamente para efectuar una tarea específica, lo que los ha masificado y diversificado, a la vez derivando en que sean apetecidos y buscados para ser explotados o violentados, esto debido a su amplia funcionalidad e incrementando aún su interés y valor de ataque por el al alto valor de los datos accedidos, ya que dichos aplicativos se han orientado a almacenar, gestionar, acceder a datos financieros sensibles o información personal, convirtiéndose en cierto grado en vitales para la funcionalidad de personas u organizaciones públicas o privadas sea cual fuere su enfoque o razón de ser.

[5] Hypertext Transfer Protocol: Protocolo de comunicación que permite la transferencia de información en la World Wide Web.

Figura 1: Niveles de una aplicación web.



Fuente: Elaboración propia.

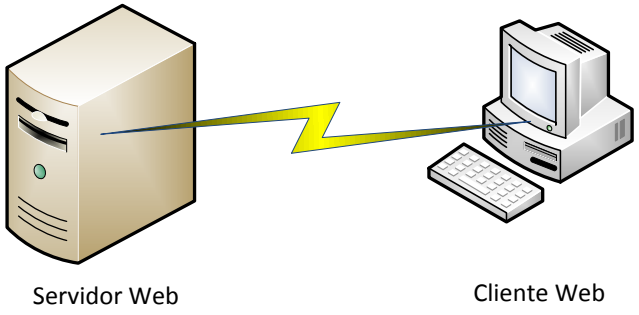
3.2.1. Arquitectura de servidores web

Un servidor web es un programa que con la implementación del protocolo HTTP (HyperText Transfer Protocol), el cual tiene por objetivo transferir páginas HTML (HyperText Markup Language), acorde a las peticiones que realicen los clientes desde los navegadores (Miño, Servidores de aplicaciones web, 2011).

Ejemplos de servidores web se mencionan IIS (Internet Information Services) o Apache, cada uno desde su perspectiva para entorno Windows o Linux respectivamente.

Un servidor web en su modelo clásico proporciona contenido estático para sus clientes.

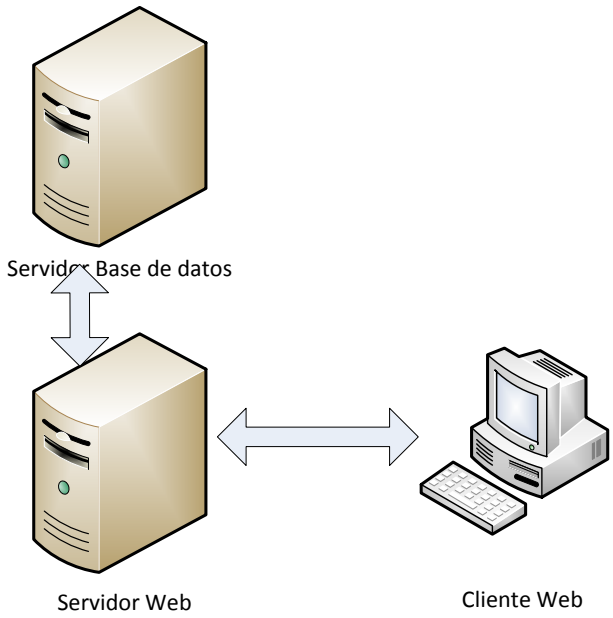
Figura 2: Esquema clásico de comunicación Cliente - Servidor



Fuente: Elaboración propia.

Servidor Hibrido se considera aquel que va más allá de mostrar página estáticas, proporcionando contenido activo extraído de un almacenamiento de datos o llamado Backend pudiendo ser una Base de datos, o un Servidor de archivos, entre otros.

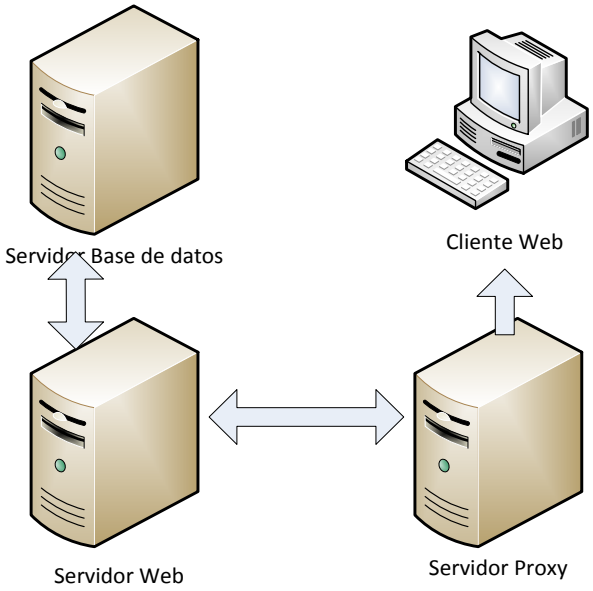
Figura 3: Esquema de servidor híbrido



Fuente: Elaboración propia.

Servidor Proxy cumplen la función de manejar tráfico web, permiten limpiar las entrada del usuario previas a enviarlas al servidor de aplicación, además almacenan en “caché” los resultados de las peticiones del usuario.

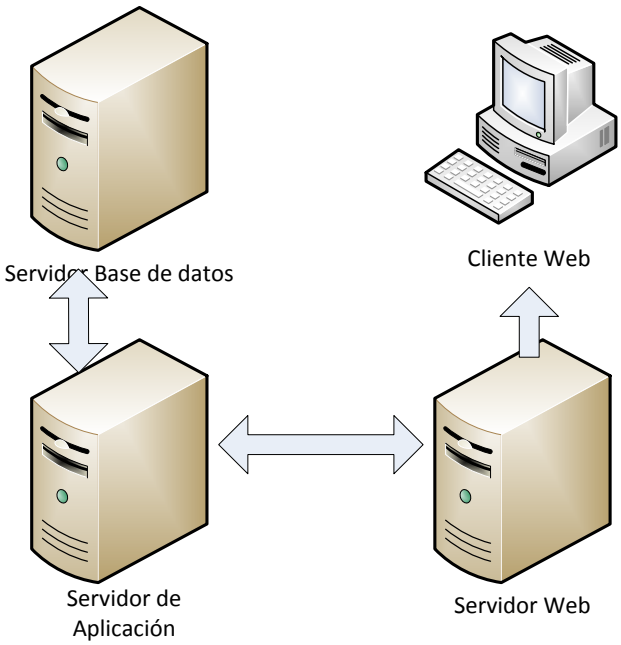
Figura 4: Esquema de servidor Proxy



Fuente: Elaboración propia.

Servidor de Aplicación es el encargado del procesamiento de la lógica de la aplicación, se localiza entre el Servidor Web o Servidor Proxy y el Servidor de Base de Datos.

Figura 5: Esquema de un Servidor de Aplicación



Fuente: Elaboración propia.

3.2.2. Interfaces Arquitectura Cliente – Servidor

Definiéndose como interface a la superficie de contacto que se muestra luego de establecer conexión entre dos sistema o dispositivos.

Según indica (Estrada, 2011), toda aplicación web que posea un cierto tipo de interacción con el cliente debe acceder a las funciones del servidor. Actualmente se definen dos interfaces que son las más difundidas en el mercado Common Gateway Interface (CGI) e Internet Server Application Programming Interface (ISAPI).

CGI es un método estándar de escribir programas para que funcionen en los servidores web, a estos programas se los suele llamar "Scripts CGI", los cuales por lo general toman sus datos de entrada de forma HTML que les permiten luego ejecutar tareas específicas. Estos programas ofrecen una gran facilidad de desarrollo y como la interfaz con el usuario es HTML, se pueden acceder desde cualesquier navegador. Cada llamada a ejecución de un script consume tiempo de CPU y recursos del servidor, por esta razón se debe prestar especial atención a la simultaneidad de las mismas.

Otra de las interfaces es ISAPI, siendo una buena alternativa de empleo de esta interfaz en los casos donde prime la eficiencia, ya que a diferencia de CGI, las aplicaciones que emplean ISAPI, se compilan dentro de archivos DLL[6] del servidor, siendo más eficientes. Estos archivos son el método nativo del ambiente Windows. La desventaja aquí es que un colapso de DLL puede provocar serios problemas en el servidor, existe una versión desarrollada por Netscape que se denomina NSAPI**,** la cual también trabaja con sistemas Unix, que soportan objetos compartidos.

Dentro de las interfaces encontramos los servlets**,** tratándose de componentes del lado del servidor, que son independientes de las plataformas pues se ejecutan en una máquina virtual Java (JVM). Por ejecutarse dentro del servidor, no necesitan una interfaz gráfica de usuario, permitiendo una interacción completa entre los mismos (usuario y servidor). En el caso de los servlets[7] Java, ofrecen una solución para generar contenido dinámico, son objetos de programa que pueden cargarse dinámicamente en los servidores Web, ampliando su funcionalidad,

[6] Biblioteca de enlace dinámico (sigla en inglés de *dynamic-link library*)
[7] Clase en el lenguaje de programación Java, utilizada para ampliar las capacidades de un servidor

desempeñándose mejor que las CGI, a su vez son muy seguros y pueden emplearse sobre protocolos de seguridad SSL[8].

3.2.3. Seguridad en aplicaciones web

La seguridad en todo ámbito es algo que preocupa y amerita sea analizado en pos de búsqueda de mecanismos que permitan hacer frente ante posibles violaciones a la seguridad. Más aún en la perspectiva web es muy necesario evaluar aspectos de seguridad en los aplicativos web, ya que por su importancia se han convertido en una herramienta indispensable para gestión e interacción de transacciones acorde a la orientación o razón de ser de las entidades.

Un alto porcentaje de las organizaciones centran sus esfuerzos en realizar pruebas sobre la funcionalidad de las aplicaciones web desarrolladas para su necesidad, pero muy escasamente se enfocan en realizar pruebas de seguridad como lo menciona (Aviles, 2015), por lo que diariamente y a nivel mundial se reportan gran cantidad de incidentes relacionados a aplicativos web que han sido vulnerados como lo indica en (OWASP, OWASP Top 10 - 2013, 2013), comunidad abierta y libre que tiene como objetivo mejorar la seguridad en aplicativos web, la cual evidencia el listado de las diez principales amenazas en la que se puede ver que la inyección es la más común.

Acorde el criterio del autor (Lenin, 2014), indica que el éxito de las aplicaciones web se debe a dos pilares fundamentales: el protocolo HTTP y el lenguaje HTML. El primero permite una implementación simple y sencilla de un sistema de comunicaciones facilitando el envío de cualquier tipo de ficheros de una forma fácil, simplificando el funcionamiento del servidor y permitiendo que servidores con características poco potentes atiendan varias peticiones y reduzcan los costes de despliegue, mientras que HTML proporciona un mecanismo de composición de páginas enlazadas simple y fácil, altamente eficiente y de uso muy sencillo. En sus albores la web era simplemente una colección de páginas estáticas, documentos, etc., los que podían consultarse o descargarse. A través del tiempo evolucionó a métodos más complejos con capacidad de desarrollar páginas dinámicas. La compatibilidad multiplataforma, el acceso de múltiples usuarios de forma concurrente, la información en línea, facilidad de actualización, entre otras se constituyen en factores de ventaja. Al ser internet el medio de interacción para las aplicaciones web, se ciernen sobre ellas diversas amenazas que provienen de diferentes orígenes; es por eso

[8] "Secure Sockets Layer", protocolo diseñado para transmitir información en aplicativos web.

que hablar de aplicaciones web se encuentra ligado incondicionalmente al tema seguridad. Los ataques a nivel de aplicación son una amenaza en constante crecimiento contra la seguridad web. Para esto se utilizan una gran variedad de medios disponibles para violentar seguridades de un sitio web, acciones que desembocan en la pérdida de rendimiento de un aplicativo hasta el robo de datos y la desprotección de la infraestructura tecnológica.

3.2.4. Hacker

Lastimosamente éste término se ha masificado, pero de una manera peyorativa, al relacionarlo a una persona cuando comete un delito en el ámbito informático, todo esto de manera errónea, ya que por el contrario se constituye la persona o conglomerado quienes en base a sus conocimientos exploran, analizan, emplean técnicas, herramientas, para determinar errores, vulnerabilidades, y exponer mecanismos de corrección.

El autor (Arellano, 2015), indica que la palabra Hacker deriva del término inglés para hacer alusión a una persona o a una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo, y se los denomina también "*piratas informáticos*".

Como tal, la comunidad de los hackers, tienen como función explotar a fondo el funcionamiento de los diferentes sistemas informáticos con la finalidad de encontrar errores, corregirlos y solucionar los mismos.

Los autores (De Miguel Molina & Oltra Gutiérrez, 2007), consideran Hacker a una persona entusiasta, con un gran interés en aprender acerca de los sistemas informáticos y de cómo usar los mismos de formas innovadoras. Este afán les lleva a buscar métodos para penetrar sistemas, generalmente a través de Internet, en busca de esa información que los lleve acrecentar aún más sus conocimientos. Una vez dentro de un sistema, se limitan a dejar su marca de presencia. Su actuación viene determinada por alguna versión de la ética del hacker, código que no les permite buscar vulnerabilidades de forma maliciosa y que además refleja una fuerte repulsión contra el vandalismo de los crackers. Suelen ser personas inteligentes. Aunque su actuación dista mucho de los crackers, en la práctica un hacker auténtico ha jugado con algún tipo de "crackeo" y conoce muchas de las técnicas básicas. Se caracterizan por ser personas que disfrutan investigando al detalle los sistemas y cómo aprovecharlos; diferenciándose de la mayoría de los usuarios, quienes únicamente aprenden lo imprescindible. Disfrutan del reto intelectual de superar o rodear las

limitaciones de forma creativa. Su accionar se basa en el gusto por la programación de forma entusiasta (incluso obsesiva), son sociales, en contra de la opinión generalizada, pues se reconocen los méritos entre sí mismos.

3.2.5. Crackers

En éste contexto si se enmarcan las personas o comunidades, que emplean los conocimientos, técnicas, herramientas, para acceder a sistemas informáticos, pero su finalidad es hacerse de algún tipo de provecho o beneficio, pudiendo ser económico, dañar, o destruir los entornos a los que acceden.

El autor (Gómez H. R., 2007) , define como cracker a una persona que intenta acceder a un sistema informático sin autorización, con el fin de obtener ficheros del sistema o sabotear el mismo. Estas personas tienen a menudo malas intenciones en contraste con los hackers, y suelen disponer de muchos medios para introducirse en un sistema.

Según lo indica en (Benchimol, 2011), el término Crack desprende del vocablo inglés crack cuyo significado es romper, siendo aplicado para describir una persona que violenta la seguridad de un determinado sistema informático utilizando su inteligencia de forma eficaz.

3.2.6. Hacking

Toda vez que se ha visto el concepto de Hacker, es evidente enunciar como definición de hacking a la interacción, proceso o actividades que desarrollan personas o comunidades, enfocadas a la búsqueda de fallas, o debilidades en los aplicativos para proponer soluciones.

Según lo describe en (Benchimol, 2011), el término Hacking fue creado por *The Tech Model Railroad Club* (TMRC) perteneciente al Instituto Tecnológico de Massachusetts (MIT), por la década de los años 50, para describir el proceso que efectúa una persona que mediante su ingenio obtiene rápida y efectivamente alguna solución a un problema, derivándose en el uso erróneo como sinónimo de “delincuente informático”.

Para los autores (De Miguel Molina & Oltra Gutiérrez, 2007), el hacking se define como un conjunto de técnicas para acceder a un sistema informático sin autorización. Es un término

estrechamente ligado a la libertad de información de Internet. Entre sus medios destacan los sniffers o escaneadores de puertos, programas que buscan claves, passwords y puertos abiertos.

Un concepto más global lo describe (Alegsa, 2010) al definir al hacking como técnicas y procedimientos utilizados por un hacker para cumplir un determinado objetivo. Suele asociarse esta palabra a procedimientos ilegales o malignos.

3.2.7. Hacking Ético

Desde el punto de vista estrictamente de la comunidad informática, la experimentación e investigación, el "hackeo" está bien visto, siempre y cuando la actividad este enmarcada dentro del respeto de la ética del hacker.

La ética hacker se basa en estos principios, introducidos por (Levy, 2001)en 1984. "El acceso a las computadoras y cualquier cosa que pueda enseñarle algo acerca de cómo funciona el mundo debería ser ilimitado y total. Siempre ríndase al imperativo de "¡Manos a la obra!"".

De acuerdo como lo menciona en (Benchimol, 2011), hacker ético hace referencia a profesionales relacionados a las tecnologías y seguridad de la información, que usan conocimientos de hacking para dar oportuno aviso de las fallas de seguridad que sean encontradas en los aplicativos web a ser analizados, dando la pauta de prevención antes de que crackers entren en operación.

Definiéndose como metodología es la que ayuda a solventar problemas relacionados a la seguridad en las aplicaciones, ya que emplea procedimientos, técnicas y herramientas desde el punto de vista defensivo.

3.2.8. Tipos de Hacking

Al aplicar un procedimiento de hacking ético, es menester definir el alcance de la evaluación, para lo cual se debe establecer el tipo de hacking que se va a efectuar, la modalidad a emplear y los servicios adicionales.

Desde el lugar que se ejecuten las técnicas, metodologías y herramientas para la detección de vulnerabilidades, puede considerarse hacking ético externo, cuando se lo realiza utilizando la infraestructura de la red pública respecto a la organización objetivo de análisis como: enrutador, firewall, servidor web, servidor de correo, servidor DNS, entre otros.

Mientras que hacking ético interno, se lo efectúa desde la red interna de la organización objetivo de evaluación, desde una perspectiva como empleado con acceso a la red organizacional (Astudillo, 2013).

Según indica (Moral, 2014), la infraestructura tecnológica de una organización puede ser probada, analizada, y atacada en varias maneras, seguidamente hace una descripción de algunos de los más comunes modos de hacking ético:

Ataque local, siendo una prueba simula asignada a una persona autorizada la cual tiene una conexión legítima a la red de la organización. Las defensas primarias que deben ser derrotadas son: firewalls de la intranet, servidores Web internos, y medidas de seguridad del servidor.

Ataque remoto, ésta prueba simula un ataque realizado por un intruso externo por medio del Internet, sus posibles objetivos son: Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Structured Query Language (SQL), o cualquier otro servicio disponible. Para cumplir su cometido el ataque remoto, debe vulnerar dispositivos como: firewall externo, enrutadores que filtran paquetes, entre otros.

Ataques con equipo robado, en los cuales frecuentemente computadoras portátiles son sustraídas, con el objetivo de evaluar la forma en cómo los usuarios protegen la información. Por ejemplo, si una computadora portátil robada tiene almacenada información confidencialmente crítica que puede ser fácilmente vulnerada, puede constituirse en una amenaza de seguridad para la organización. Los atacantes podrían usar diferentes métodos, conectarse remotamente a los servidores de la empresa con autenticaciones verdaderas.

Ataques a entradas físicas de la organización, cuando se busca poner a prueba los procedimientos de control físico en la organización, tales como puertas, salidas, seguridades, circuito cerrado de televisión. Para lograr este cometido, el atacante deberá intentar ingresar al edificio de la organización, las defensas primarias en este caso es una política de seguridad bien implementada, guardias de seguridad, controles de acceso y monitoreo.

Ataques por medio de equipos sin autenticación, ésta simulación está pensada para buscar puntos de acceso inalámbricos y módems, para validar la seguridad de los dispositivos determinando que posean los debidos controles para autenticación necesarios.

Ataques con ingeniería social, ésta prueba no se enfoca en sistemas técnicos o acceso físico, por el contrario, busca evaluar la integridad y el compromiso del personal de la organización, en ellos normalmente se busca manipular a los empleados para obtener información privilegiada como: controles existentes, políticas de seguridad, procedimientos internos de la organización y rutinas del resto del personal, entre ellos los administradores de tecnologías.

3.2.9. Técnicas de Hacking (Tipos de pruebas de penetración)

Las técnicas de hacking son tres como lo muestra en (Astudillo, 2013) , Black box hacking (Hacking de caja negra), relacionado a pruebas de intrusión externas, en la que únicamente se conocerá el nombre de la empresa objetivo, teniéndose escaso o nulo conocimiento de la infraestructura por parte del consultor. La segunda modalidad es Gray box hacking (Hacking de caja gris), siendo las pruebas que se las realiza desde el interior de la organización en donde se conoce información limitada sobre los equipos, direcciones IP (Internet Protocol), tipo de función de equipos como router, web server, firewall, entre otros; y finalmente se cuenta con las pruebas llamadas White box hacking (Hacking de caja blanca), o también denominadas trasparentes, se la aplica únicamente a las pruebas internas, ya que el cliente provee al auditor información completa de las redes y sistemas objetivo de la evaluación.

3.2.10. Vulnerabilidades

En forma general se entiende por vulnerabilidades a determinadas debilidades que se localizan en un entorno o escenario, la cuales pueden ser aprovechadas para la consecución de intereses negativos. Enmarcado en el aspecto de aplicativos web según refiere (Medina J. , 2014), se considera a cualquier falla relacionada al diseño, configuración o implementación, la misma que puede llevar a ser comprometida la seguridad de dicho aplicativo web. Las vulnerabilidades enfocan las debilidades y los métodos más comunes utilizados para realizar ataques a la seguridad de un sistema.

Ente las vulnerabilidades o fallas que pueden comprometer la seguridad de un aplicativo web se destacan:

Fallas de fuga de información, mismas que permiten descubrir información sobre la configuración y el estado de la aplicación, pudiendo ser utilizada para efectuar ataques muy dañinos.

Fallas de configuración, relacionadas a la configuración del servidor web, o el sistema operativo sobre el cual se levanta el aplicativo, pueden permitir explotar el sistema sin importar la seguridad del aplicativo web.

Fallas de Bypass, permiten al atacante evadir controles, pudiendo acceder y modificar archivos sobre el servidor.

Fallas de inyección, cuando existe demasiada confianza en el cliente para aceptar entradas de filtros inadecuados, siendo comunes mediante Inyecciones SQL o Cross Site Scripting (XSS) (Aviles, 2015).

El autor (Moral, 2014), refiere que vulnerabilidad es cualesquier tipo de falla inherente en el diseño, configuración o implementación de un sistema o una red que pueda generar un evento que comprometa la seguridad. Las vulnerabilidades describen las debilidades y los métodos más comunes que se utilizan para realizar ataques a la seguridad de un sistema, en donde hay que definir las prioridades en los elementos a proteger, de acuerdo al valor que representan para la organización y de esta forma poder prevenir los diferentes tipos de ataques que pueden sufrir, detectando las vulnerabilidades que presentan estos elementos.

3.2.11. Ataques

Se define como el proceso de enviar código, sustraer información de forma no autorizada, causando daños en la infraestructura de la aplicación.

Los autores (Jara & Pacheco, 2012), definen el término ataque en el aspecto informático, el violentar la seguridad de un sistema o aplicativo, producto de una planificación, con el uso de técnicas y herramientas cada vez más sofisticadas por su capacidad de afectación.

Se diferencian dos tipos de ataques: Ataques Activos y Ataques Pasivos.

Los ataques activos se consideran los que tienen la firma intención de causar daños en el aplicativo, obviamente con afectaciones o graves perjuicios a la organización, su detección se lo hace toda vez que existe una afectación en cuanto a fallas de funcionamiento en la disponibilidad, integridad o autenticidad del objetivo atacado, un ejemplo de peste tipo de ataque es el denominado DoS (Denial of Sevice) (Balado, 2005).

Los ataques pasivos por su parte son aquellos que vulneran la seguridad del aplicativo sin afectar el estado del mismo, más su visión es determinar vulnerabilidades con el objetivo de tomar los correctivos a tiempo (Balado, 2005).

En referencia a ataques informáticos, el autor (Gaibor, 2007), considera un ataque a cualquier acción que intenta violar la seguridad del sistema. Las técnicas que se utilizan cada vez son más sofisticadas, y a la vez difíciles de prevenir y su capacidad potencial de hacer daño es mucho mayor, debido a que atacan vulnerabilidades en el diseño, configuración y operación.

Existe dos tipos de ataques, pasivos y activos, ésta clasificación se basa en los objetivos y efectos que puede tener un determinado ataque.

Ataques pasivos, se consideran aquellos que violan la confidencialidad sin afectar el estado del sistema, su función en la mayoría de casos es el aprendizaje de la estructura de una red; este tipo de ataque, se utiliza para determinar zonas vulnerables del sistema. Un ejemplo de un ataque pasivo es interferir en las transmisiones electrónicas ya sea para dejar mensajes o para obtener contraseñas inseguras. En este tipo de ataques la confidencialidad juega un papel muy importante para prevenir el descubrimiento de información por parte de personal no autorizado.

Ataques activos, se realizan con la intención real de producir daños en un sistema o con la finalidad de extraer información confidencial. Este tipo de ataque provoca mayores perjuicios; generalmente son más fáciles de detectar debido a que se registra fallas en el funcionamiento del sistema atacado. Un ejemplo de ataque en esta categoría es un ataque en la disponibilidad del sistema o servicio, llamado DoS (Denial of Service). Los ataques activos pueden afectar factores como la disponibilidad, integridad y autenticidad de un sistema.

En resumen, la diferencia radica en que mientras un ataque activo intenta alterar los recursos del sistema o afectar su operación, un ataque pasivo está orientado al aprendizaje sin afectación del recurso.

3.2.12. Clasificación de los delitos informáticos

De acuerdo a (Consejo de Europa, 2001), suscrito por el Consejo de Europa, clasifica los delitos informáticos de la siguiente manera:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. -

Acceso ilícito al acceso deliberado e ilegítimo a parte o a la totalidad de un sistema informático.

Interceptación ilícita cuando por medio tecnológicos se intercepte ilegítima y deliberadamente datos comunicados de forma confidencial.

Interferencia en los datos a la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

Interferencia en el sistema a la obstaculización del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de datos, borrado, deterioro, alteración o supresión de datos informáticos.

Abusos de los dispositivos a la producción, venta, obtención para uso, importación, difusión u cualquier forma de puesta a disposición de un dispositivo o programa informático diseñado para el cometimiento de un delito informático, similar si se trata de contraseñas o códigos de acceso a datos o parte de modular de un sistema informático.

Delitos informáticos. -

Falsificación informática a través de la introducción, borrado o supresión de datos informáticos, resultando en datos no auténticos intencionalmente usados como verídicos con repercusiones legales.

Fraude informático a la actuación deliberada e ilegítima causante de perjuicio patrimonial a un individuo en beneficio económico del cibercriminal o de una tercera persona, mediante la introducción, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el normal funcionamiento de determinado sistema informático.

Delitos relacionados con el contenido. -

Pornografía infantil a la producción, oferta, difusión, adquisición de contenidos con pornografía infantil, a través de un sistema informático, o a su vez poseer dichos contenidos en un sistema informático o medio de almacenamiento de datos.

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. -

La producción, distribución y reproducción de software legalmente prohibido y que cuenta con derechos de autor y/o propiedad intelectual, los cuales cuenten con licencias para su uso.

3.2.13. Tipos de delitos informáticos

Toda vez analizadas la clasificación de los delitos informáticos, es pertinente sintetizar dicha clasificación en los tipos de delitos informáticos, así lo sintetiza el Dr. Santiago Acurio del Pino en su obra digital: "*Delitos Informáticos*" (Acurio), considerándose como tales a los fraudes, el sabotaje informático, el espionaje informático y el robo o hurto de software, el robo de servicios, y el acceso no autorizado a servicios informáticos.

3.2.14. Legislación ecuatoriana sobre delitos informáticos

En el Ecuador se cuenta con el COIP[9] promulgado por (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), para la administración de justicia en los casos los cuales exista el cometimiento de delitos.

En cuanto a delitos informáticos específicamente el documento citado anteriormente hace referencia en algunos articulados como los siguientes a las penas que serán impuestas a quienes cometan dichos delitos.

Artículo 190.- Apropiación fraudulenta por medios electrónicos. -

"*La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de ésta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistema informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionado con pena privativa de la libertad de uno a tres años.*"

En la sección tercera, (Ministerio de Justicia, Derechos Humanos y Cultos, 2014) expone sobre los delitos contra la seguridad de los activos de los sistemas de información y comunicación, que rezan los siguientes artículos:

Artículo 229.-Revelación ilegal de base de datos. -

"*La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.*"

Artículo 230.- Interceptación ilegal de datos. -

La sanción será pena privativa de la libertad de tres a cinco años para quienes:

[9] Código Orgánico Integral Penal

1. "*La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.*"

2. "*La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder."*

3. "*La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.*"

4. "*La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.*"

Artículo 231.- Transferencia electrónica de activo patrimonial. -

Será sancionada con pena privativa de libertad de tres a cinco años: "*La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero*"

Artículo 232.- Ataque a la integridad de sistemas informáticos. -

"*La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.*"

Con la misma sanción se aplica para quienes:

1. "*Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo."*

2. *"Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general."*

"Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad."

Artículo 233.- Delitos contra la información pública reservada legalmente. -

"La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años."

"La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años."

"Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad."

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. -

"La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años."

3.2.15. Pruebas de Penetración en Aplicaciones Web (Pentesting)

Para efectuar detección de vulnerabilidades y posteriores pruebas de penetración o Pentesting con resultados satisfactorios, se requiere de conocimientos relacionados a las tecnologías web más allá del nivel de un usuario normal, siendo vital el entendimiento de la estructura y funcionamiento de aplicaciones web desde la óptica de un desarrollador o administrador (Benchimol, 2011).

Además los profesionales de ésta área deben literalmente adoptar "la mente maliciosa" de los hackers al imaginar las formas de cómo pasar las restricciones, analizar los errores de la etapa de desarrollo que puedan ser aprovechados, y muchas interrogantes todas desde una estricta perspectiva ética y profesional, ya que consistirá en atacar a un sistema informático con el objetivo de encontrar debilidades de seguridad que permitan acceder a su funcionalidad, datos, archivos o cualquier información importante.

Para efectuar una buena prueba de penetración es importante seguir una metodología aprobada, repetible y explicable, asociado a éste aspecto es fundamental conocer las herramientas y sus múltiples opciones que dispongan.

Otro aspecto vital a tomar en cuenta es el contar con el permiso de la organización para la realización de las pruebas, esto debido a la existencia de legislaciones sobre hacking, aunque en la constitución del Ecuador *"…ni siquiera considera la posibilidad de que alguien use las herramientas diseñadas en gran porcentaje, para explotar las vulnerabilidades, en beneficio de los sistemas de destino, convirtiendo las mismas herramientas en parte de la solución y no del problema*" (Rojas, 2014)

3.2.16. Metodologías de una Prueba de Penetración

Constituyen una guía para alcanzar un objetivo al realizar una prueba de penetración de una manera organizada para obtener mejores resultados.

A continuación, se destacan tres metodologías utilizadas para la aplicación de pruebas de penetración:

Inicio citando la metodología Open Source Security Testing Metohodology (OSSTMM), la cual constituye en un manual de metodología abierta que contempla grana parte de los aspectos que se deben tomar en cuenta al realizar pruebas de seguridad, con la finalidad de organizar su contenido se divide en fases, siendo la fase A Seguridad de la información, fase B Seguridad de los procesos, fase C Seguridad en las tecnologías de internet, fase D Seguridad en las comunicaciones, fase E Seguridad inalámbrica, fase F Seguridad Física. (Benchimol, 2011).

De acuerdo al autor (Jake Kouns, 2011), en referencia a ésta metodología dice: que busca establecer un método científico para el análisis de seguridad, evitando el basarse en la experiencia del analista, se enfoca a la medición del estado de seguridad de un ambiente operativo, tomando en cuenta medidas de seguridad en las interacciones, menciona que con OSSTMM, se mide cada característica funcional del aplicativo y que actualmente está en vías de considerarse al estándar como un nuevo ISO.

Figura 6: Logotipo OSSTMM

Fuente: página web del proyecto OSSTMM

En segunda instancia cito la metodología Information System Security Assessment Framework (ISSAF), constituye un marco de trabajo detallado respecto a las prácticas y conceptos relacionados a cada actividad que se debe realizar durante el testeo de seguridad, dicha información se la ha centrado bajo la denominación de "criterios de evaluación", mismos que han sido escritos y revisados por parte de expertos en cada una de las áreas de aplicación, mismos que se componen en los ítems: Descripción del criterio de evaluación, Puntos y objetivos para cubrir, Prerrequisitos para conducir la evaluación, Proceso mismo de evaluación, Informe de los resultados esperados, Contramedidas y recomendaciones, Referencias y documentación externa. (Benchimol, 2011)

En tanto que el autor (Wilhelm, 2013), define a ISSAF como una metodología estructurada de análisis de seguridad en varios dominios y detalles específicos de test o pruebas para cada uno de

estos. Tiene como objetivo proporcionar procedimientos muy detallados para el "testing" de sistemas de información que reflejan situaciones reales, es utilizado en su mayoría para cumplir con los requisitos de evaluación de las organizaciones y puede utilizarse además como referencia para nuevas implementaciones relacionadas con la seguridad de la información.

Figura 7: Logotipo ISSAF

Fuente: página web del proyecto OISSG

Finalmente, la metodología Open Web Application Security Project (OWASP), la cual específicamente es un proyecto que se enfoca en la seguridad de aplicaciones web, lo constituye una comunidad abierta y libre cuyo objetivo el visibilizar y concientizar la seguridad en aplicaciones, para que las organizaciones tomen las mejores decisiones sobre riesgos de seguridad. Los proyectos que dispone se dividen en dos categorías, por una parte los proyectos de documentación siendo: Guía de desarrollo, Guía de pruebas, Top 10, Legal, y App Sec FAQ; mientras que entre los proyectos de desarrollo se denotan: WebScarab siendo una aplicación para efectuar pruebas de seguridad en aplicaciones y servicios web, de la mano de WebGoat, el cual es un entorno de entrenamiento para usuarios enfocado al aprendizaje con enfoque seguro u legal hacia el aprendizaje de la seguridad en aplicaciones web.

De acuerdo al autor te. (Michael E. Whitman, 2015), indica que OWASP es un proyecto exitoso y está conformado por una serie de guías y proyectos relacionados con la implementación de la seguridad en desarrollos principalmente web. Su comunidad está conformada por varias empresas, organizaciones educativas y particulares alrededor de todo el mundo, constituyéndose en una comunidad de seguridad informática que trabaja en la creación de artículos, metodologías, documentación, herramientas y tecnologías que se liberan de forma gratuita. Una ventaja excepcional de esta comunidad es que no tiene fines de lucro y por ende no depende de presiones corporativas, factor que facilita se proporcione información imparcial, práctica y que pueda ser aprovechada de forma productiva.

Las pruebas en éste método se dividen en: Obtención de información, Pruebas de reglas del negocio, Pruebas de autenticación, Pruebas de manejo de sesión, Pruebas de validación de datos, Pruebas de denegación de servicio, Pruebas en servicios web, Pruebas en Ajax (Benchimol, 2011).

Figura 8: Logotipo OWASP

Fuente: página web del proyecto OWASP

3.2.17. Escanners de vulnerabilidades para aplicativos web

Su espectro de acción es evaluar los riesgos en los aplicativos web, con el propósito de evitar ataques posteriores, se los puede utilizar durante la fase de desarrollo de la aplicación web, ayudando a encontrar errores en la programación (Huércano Ruiz & Villar Cueli, 2015).

Los escanners de vulnerabilidades de aplicativos web son algo diferentes a los escanners de vulnerabilidades tradicionales o de redes, por ejemplo, ya que los plugins cambian la petición realizada en base a cómo el escanner ha visto la aplicación web, por ejemplo, tomará en consideración si el formulario web envía diferentes parámetros y si define varias cookies.

Seguidamente se muestra una lista de herramientas para escaneo de vulnerabilidades en aplicaciones web, la cual está disponible en el contenido de OWASP (OWASP, Vulnerability Scanning Tools, 2016).

Según refiere el autor (Gómez V. , 2015), en su artículo hace referencia a los ocho mejores escanners de vulnerabilidades web, iniciando con Grabber, el cual es capaz de detectar vulnerabilidades relacionadas a Cross site scripting, Inyección SQL, Pruebas de Ajax, La inclusión de archivos, JS analizador de código fuente, Comprobación del archivo de copia de seguridad, como características indica que no es rápido, pero es simple y portátil, no ofrece interfaz gráfica, tampoco crea informes en formato .pdf.

Luego menciona Vega, el cual es de código abierto, está desarrollado en Java y ofrece un entorno basado en GUI, su disponibilidad es para Linux y Windows. Se puede encontrar inyección SQL, inyección de cabecera, listado de directorios, inyección cáscara, cross site scripting, la inclusión de archivos y otras vulnerabilidades.

Posteriormente refiere a Zed Atack Proxy, también llamado ZAP, es de código abierto y está desarrollado por AWASP. Está disponible para las plataformas de Windows, Unix / Linux y Macintosh. Se puede encontrar una amplia gama de vulnerabilidades en aplicaciones web, como herramienta es muy simple y fácil de usar, sus funciones principales son scanner automático, Fuzzer, Socket Web, lug-n-hack.

Luego hace mención a Wapiti, el cual permite auditar la seguridad de las aplicaciones web. Efectúa pruebas de caja negra al escanear páginas web e inyecciones de datos. Puede detectar vulnerabilidades como: Exposición de archivos, Cross Site Scripting (XSS), Ejecución de comandos, CRLF Inyección, SEL Inyección y Xpath Injection, Configuración de .htaccess, crear backups y muchos otros.

Continua con W3af, el mismo que tiene como objetivo proporcionar una plataforma de pruebas de penetración de aplicaciones web, su desarrollo se basa en Python, permite identificar más de 200 tipos de vulnerabilidades, incluyendo la inyección SQL, cross-site scripting y muchos otros, dispone de una interfaz gráfica y consola.

Luego refiere a WebScarab, es basado en Java, para el análisis de aplicaciones web usa HTTP o HTTPS, dispone de plugins, también funciona como proxy de interceptación.

Continúa citando a Skipfish, el cual es una herramienta de seguridad de aplicaciones web agradable, comprueba cada página para diversas amenazas a la seguridad y al final permite genera informes.

Finalmente hace mención a Ratproxy, el cual es una herramienta abierta de auditoría de seguridad de aplicaciones web, soporta Linux, FreeBSD, MacOS X, y (Cygwin) entornos Windows. Es capaz de distinguir entre las hojas de estilo CSS y códigos de JavaScript, también es compatible con SS. Puede tomar el control de la solicitud y la respuesta mediante el uso de plugins disponibles. Sus módulos pueden detectar vulnerabilidades más comunes, como la inyección SQL, XSS <CRLF y muchas otras.

En tanto que (OWASP, Vulnerability Scanning Tools, 2016), hace referencia a una tabla conteniendo un listado de herramientas, de las cuales se mencionan algunas acorde a su nombre, propietario, licencia y plataformas soportadas.

Tabla 2: Algunas herramientas de escaneo de vulnerabilidades.

Nombre	Propietario	Licencia	Plataformas
Acunetix WVS	Acunetix	Commercial / Free (Limited Capability)	Windows
Burp Suite	PortSwiger	Commercial / Free (Limited Capability)	Most platforms supported
Grabber	Romain Gaucher	Open Source	Python 2.4, BeautifulSoup and PyXML
GoLismero	GoLismero Team	GPLv2.0	Windows, Linux and Macintosh
Nexpose	Rapid7	Commercial / Free (Limited Capability)	Windows/Linux
Nikto	CIRT	Open Source	Unix/Linux
Proxy.app	Websecurify	Commercial	Macintosh
Retina	BeyondTrust	Commercial	Windows
Securus	Orvant, Inc	Commercial	N/A
Sentinel	WhiteHat Security	Commercial	N/A
Vega	Subgraph	Open Source	Windows, Linux and Macintosh
Wapiti	Informática Gesfor	Open Source	Windows, Unix/Linux and Macintosh
WebApp360	TripWire	Commercial	Windows
Wikto	Sensepost	Open Source	Windows
w3af	w3af.org	GPLv2.0	Linux and Mac

Zed Attack Proxy	OWASP	Open Source	Windows, Unix/Linux and Macintosh

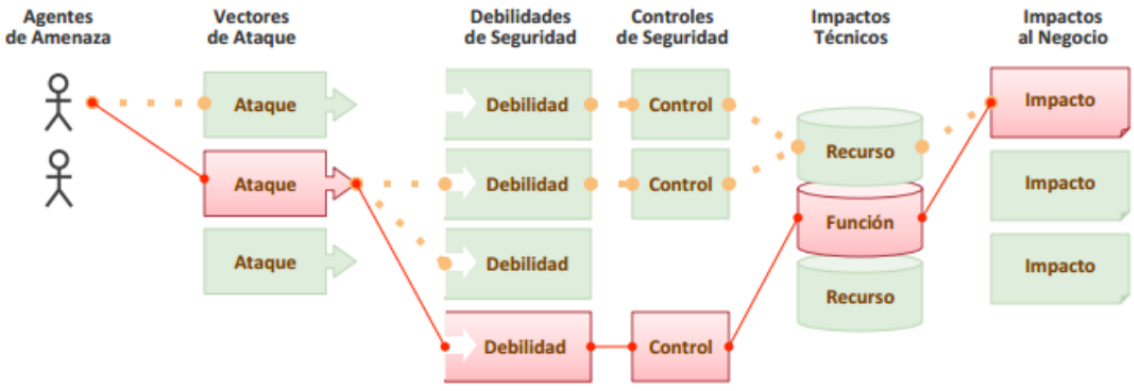
Fuente: página web del proyecto OWASP

3.2.18. Vulnerabilidades o riesgos de seguridad en aplicaciones web

Las aplicaciones web pueden presentar diversas vulnerabilidades, las cuales ocurren acorde al tipo de servicio que prestan, lo indica el autor (Aumaille, J2EE Desarrollo de aplicaciones web, 2002). De acuerdo con el criterio de (Palmer, 2011), el Open Web Application Security Project (OWASP), recoge y difunde las vulnerabilidades en aplicaciones web que más han prevalecido catalogándolas en su Top Ten que se publica cada tres años.

Un atacante puede utilizar diversas rutas a través de la aplicación para maximizar el daño a la organización, cada una de dichas rutas puede ser potencialmente un riesgo, el cual requiere de la atención debida. Para analizar el riesgo que puede tener la organización es pertinente evaluar de manera asociada la probabilidad de cada agente de amenaza, vector de ataque, debilidades de seguridad, impacto técnico y de negocio como lo menciona en (OWASP, OWASP Top 10 - 2013, 2013).

Figura 9: Evaluación de riesgos de seguridad en una organización.



Fuente: Top 10 -2013 del proyecto OWASP

Siendo el objetivo principal de OWASP, la educación dirigida a desarrolladores, diseñadores, arquitectos, gerentes de organizaciones, en torno a las consecuencias que pueden existir en el caso de vulnerar los aplicativos de las organizaciones, provee el TOP 10 de vulnerabilidades, que actualmente dispone de la versión 2013, el cual "*se basa en 8 conjuntos de datos de 7 firmas*

especializadas en seguridad de aplicaciones" (OWASP, OWASP Top 10 - 2013, 2013), para seleccionarlas y priorizarlas en base a dichos datos conjuntamente con estimaciones de explotación, su detección e impacto.

Seguidamente se muestra el TOP 10 de riesgos de seguridad en aplicaciones.

En lo relacionado a las referencias sobre los riesgos más comunes reportados a la seguridad en cuanto a aplicativos web, se ha considerado el Top Ten de la organización Open Web Aplication Security Project (OWASP), en su última versión la cual es del año 2013 el mismo que se muestra en el Apéndice A, esto debido a que es una guía que reporta los 10 riesgos de seguridad de mayor importancia para aplicativos web.

En primer lugar, reporta A1 - Inyección, siendo las fallas de inyección, como SQL, sucediendo cuando datos no confiables se envían hacia un intérprete como parte de un comando o consulta, en tanto que los datos hostiles del atacante pueden engañar al intérprete ejecutando comandos no intencionados, accediendo a datos no autorizados.

En segundo lugar, establece A2 – Pérdida de autenticación y gestión de sesiones, cuando las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, pudiendo los atacantes comprometer contraseñas, claves, token de sesión, o explotar fallas de implementación asumiendo la identidad de otros usuarios.

En tercer lugar, menciona A3 – Secuencia de comandos en sitios cruzados (XSS), siendo fallas que suceden cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación adecuada, lo que permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima, consiguiendo secuestrar sesión del usuario, destruir sitios web, o dirigir al usuario a sitios maliciosos.

En cuarto lugar, asevera A4 – Referencia directa insegura a objetos, ocurriendo cuando el desarrollador expone una referencia hacia un objeto de implementación interno, como fichero, directorio, o base de datos, sin un control de chequeo de acceso u otra protección, pudiendo el atacante manipular dichas referencias para el acceso a datos no autorizados.

En quinto lugar, refiere A5 – Configuración de seguridad incorrecta, cuando no se dispone de una buena implementación de configuración de seguridad tanto para la aplicación, marcos de

trabajo, servidor de aplicación, servidor web, base de datos y plataforma. Debiendo ser definidas, implementadas y mantenidas, puesto que no son seguras por defecto, superando mediante actualizaciones de software y librerías de código.

Ocupando el sexto lugar, postula A6 – Exposición de datos sensibles, cuando determinadas aplicaciones web no protegen datos sensibles como números de tarjetas de crédito, credenciales de autentificación, con lo que los atacantes pueden robar o manipular dichos datos para cometer fraudes, robos de identidad u otros delitos. Para su corrección se requiere métodos de protección como cifrado de datos, y precauciones en el intercambio de datos con el navegador.

En el séptimo lugar, se enmarca A7 – Ausencia de control de accesos a funciones, sucediendo cuando la aplicación web no verifica los derechos de acceso a nivel de función antes de hacer visible en la misma interfaz de usuario, al no ser verificadas dichas solicitudes el atacante puede realizar peticiones sin la autorización adecuada.

En el octavo lugar, enlista A8 – Falsificación de peticiones en sitios cruzados (CSRF), cuando obliga al navegador de una víctima autenticada al envío de una petición HTTP falsa, incluyendo la sesión de usuario e información de autenticación, permitiendo al atacante forzar al navegador de la víctima a que genere peticiones que la aplicación vulnerable piensa son legítimas.

En noveno casillero, enumera A9 – Utilización de componentes con vulnerabilidades conocidas, sucediendo cuando al usar componentes como librerías, frameworks y otros módulos de software los que casi siempre funcionan con todos los privilegios, tienen vulnerabilidades conocidas, lo cual facilita la intrusión en el servidor, ya que hacen débiles las defensas de la aplicación y amplían el rango de ataques por ende el riesgo es alto.

Finalmente, en el décimo casillero, cita A10 – Redirecciones y reenvíos no validados, cuando los aplicativos web redirigen y reenvían a los usuarios hacia otras páginas o sitios web, empleando datos no confiables para la determinación de la página de destino. Sin una validación apropiada, el atacante puede redirigir a las víctimas a sitios de "phishing[10]" o malware, o también utilizar reenvíos para el acceso a páginas no autorizadas.

[10] Suplantación de identidad

En referencia a los diez riesgos citados por (OWASP, OWASP Top 10 - 2013, 2013), al final de la aplicación de la fase de descubrimiento se efectuarán las observaciones correspondientes en base a los resultados obtenidos, plasmándolos en el formato de informe pericial, el cual se muestra en el Apéndice B, mismo que es el producto final del presente trabajo.

3.2.19. Comparativo de riesgos de seguridad en aplicaciones entre 2010 y 2013

Los riesgos en la seguridad hacia los aplicativos web han evolucionado acorde a grado de interés y a la importancia e integración de gestiones que permiten efectuar dichos aplicativos.

Es así que según (OWASP, OWASP Top 10 - 2013, 2013), y efectuando una comparativa entre los años 2010 y 2013, se ve la permanencia de los ataques de inyección en primer lugar, así como en segundo lugar se mantiene también la pérdida de autenticación y gestión de sesiones, continua el tercer lugar y el cuarto en la misma posición o "ranking", pero se muestra que el quinto lugar se ha modificado, ya que en 2010 se tenía a la defectuosa configuración de seguridad, y para el 2013 se indica que el riesgo es la configuración de seguridad incorrecta, evidenciando que entre esos años se avanzó en los intentos de mejorar las configuraciones de seguridad pero siguen siendo muy riesgosas.

Tabla 3: OWASP Top 10 -2013 Comparativo de riesgos de seguridad en aplicaciones web entre 2010 y 2013.

OWASP Top 10 – 2010 (Previo)	OWASP Top 10 – 2013 (Nuevo)
A1 – Inyección	A1 – Inyección
A3 – Pérdida de autenticación y gestión de sesiones	A2 – Pérdida de autenticación y gestión de sesiones
A2 – Secuencia de comandos en sitios cruzados (XSS)	A3 – Secuencia de comandos en sitos cruzados (XSS)
A4 – Referencia directa insegura a objetos	A4 – Referencia directa insegura a objetos
A6 – Defectuosa configuración de seguridad	A5 – Configuración de seguridad incorrecta
A7 – Almacenamiento criptográfico inseguro	A6 – Exposición de datos sensibles
A8 – Falla de restricción de acceso a URL	A7 – Ausencia de control de acceso a las funciones
A5 – Falsificación de peticiones en sitios cruzados (CSRF)	A8 – Falsificación de peticiones en sitios cruzados (CSRF)
<dentro de A6: – Defectuosa configuración de seguridad>	A9 – Uso de componentes con vulnerabilidades conocidas

A10 – Redirecciones y reenvíos no validados	A10 – Redirecciones y reenvíos no validados
A9 – Protección insuficiente en la capa de transporte	Fusionada con 2010-A7 en la nueva 2013-A6

Fuente: página web del proyecto OWASP

3.3. Estado del Arte

Según Hermosa (2013) en su artículo: "Seguridad en aplicativos web", pone en consideración la existencia de varias herramientas enfocadas a la evaluación de seguridad web, algunas de las cuales evidencian inconvenientes, muchas por su antigüedad y caducidad al no disponer de actualizaciones, y otras por ser de código cerrado o comerciales, siendo además sus costos elevados, también hace referencia a dos herramientas que presentan características similares y pueden ser consideradas para realizar evaluaciones de seguridad hacia aplicativos web, las cuales son por una parte Burp Suite con disponibilidad bajo licencia comercial pero no excesivamente cara y muy potente, y por otra parte menciona a Zed Attack Proxy o también conocida como ZAP, con licencia libre y de código abierto, herramienta desarrollada por el OWASP[11], la cual se constituye de una comunidad abierta orientada a la habilitación de las organizaciones a desarrollar, comprar, y mantener aplicaciones confiables, misma que desde al año 2003 hace la publicación: OWASP Top Ten, siendo hasta el momento de la versión más actual del año 2013 titulada. "Los diez riesgos más críticos en aplicaciones web", en ella se muestra encabezando los tres primeros lugares de los riesgos de seguridad hacia loa aplicativos web a las fallas de inyección como SQL[12], ocurriendo cuando datos no confiables son enviados hacia un intérprete como parte de una consulta, en segundo lugar menciona a la pérdida de autenticación y gestión de sesiones, al ser implementadas de forma incorrecta pudiendo comprometer contraseñas, y tokens de sesión, en tercer lugar de la lista se muestra a la secuencia de comandos en sitios cruzados (XSS), ocurriendo cuando una aplicación toma datos no confiables y envía al navegador web sin una validación y codificación adecuada, y continúa el listado definiendo las siete amenazas, en resumen el enfoque planteado por la comunidad es brindar una guía sobre las vulnerabilidades de seguridad en aplicaciones web más relevantes y sus consecuencias, esto función a la recolección de ocho conjuntos de datos de siete firmas especializadas en seguridad de aplicaciones en las que destacan cuatro empresas consultoras y tres proveedoras de herramientas SaaS (Software as a Service). OWASP es referido por estándares como SAMM (Modelo de madurez para el aseguramiento del software), libros como Hacking de aplicaciones web SQL Injection, herramientas como Samurai

[11] Open Web Application Security Project: proyecto abierto en seguridad de aplicaciones web.
[12] Inyección SQL: método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos

Web Testing Framework, organizaciones como MITRE[13], PCI[14] DSS[15], y más recursos dedicados a la seguridad en aplicativos web.

El presente proyecto mantiene afinidad de criterios en cuanto al uso del criterio de OWASP como guía de referencia de vulnerabilidades, basándose en el Top Ten del año 2013 para efectuar una concordancia con el objetivo de evaluación, además se toma como referencia el uso de herramientas de software libre en cada una de las fases o etapas de la prueba de penetración a desarrollarse, específicamente planteándose el uso de ZAP en la fase de descubrimiento apegándose y compartiendo el criterio con el referido autor.

Con relación a componentes de seguridad, Pérez Jenny; Parco Gustavo, 2013, pertenecientes a la Escuela Superior Politécnica de Chimborazo, exponen el proyecto titulado: "Análisis de componentes de seguridad a nivel de interfaz de usuario en jsf primemobile para desarrollo de aplicaciones móviles", cuyo resultado final es determinar el nivel de seguridad del aplicativo web móvil para el Departamento Financiero, utilizando JSF+ PrimeMobile y componentes personalizados de seguridad.

Relacionado al proyecto mencionado se evidencia la sustentación teórica sobre el entorno de OWASP, así también describe algunas de las vulnerabilidades más comunes de acuerdo a la referida metodología, como: fallas de inyección, cross site scripting (XSS), falsificación de peticiones en sitios cruzados, exposición de datos sensibles, lo cual guarda relación a las referencias teóricas sobre fallas de seguridad descritas en el presente proyecto.

En torno a la temática de la seguridad de aplicaciones web, se evidencia por parte de Bermejo Juan, 2014, perteneciente a la Universidad Nacional de Educación a Distancia de España, el desarrollo del proyecto titulado: "Metodología de evaluación de herramientas de análisis automático de seguridad de aplicaciones web para su adaptación en el ciclo de vida de desarrollo", cuyo resultado final es la creación de un modelo de ciclo de vida de desarrollo seguro de software, aplicando en cada fase los tipos de herramientas de análisis automáticas de caja blanca, dinámico de caja negra, en tiempo real. La metodología de evaluación de las herramientas se basa en ejecutar

[13] Organización sin fines de lucro, opera centros de investigación y desarrollo patrocinados por el gobierno federal de Estados Unidos.
[14] Empresa mexicana orientada a servicios de Estudios, Desarrollo de Proyectos de Ingeniería, Arquitectura, Vialidad, Arquitectura del Paisaje, Gerencia de Proyectos y de Obra, Supervisión, Auditoria Técnica, Evaluación y Elaboración de Concursos y Licitaciones de Obra Pública y de Servicios.
[15] Defense Security Service del Departamento de defensa de los Estados Unidos.

cada una de ellas contra aplicaciones benchmark[16], las cuales contienen vulnerabilidades conocidas.

Del proyecto referido se toma como punto de partida y comparte el criterio para el enfoque de la técnica a utilizarse en el presente trabajo, la cual es Black box hacking, por tratarse de una actividad externa a la organización.

Respecto a la seguridad de la información, la situación actual que presentan tanto organizaciones públicas como privadas, el autor Ardita (2016), presenta su ponencia: "Los desafíos de la ciberseguridad y la ciberdefensa", desarrollada en la conferencia Segurinfo Argentina 2016, en la cual enuncia la inexistencia de regulaciones y procedimientos referentes a la seguridad de la información y de los sistemas. Referente a incidentes de seguridad el mismo autor referido (2014), en su artículo: "Estado del arte de la seguridad de la información", enlista los fraudes, amenazas, sabotaje, robo de información, pishing[17], y ataques DoS[18], como los efectuados tanto a entidades públicas como privadas, además hace referencia al número de incidentes de seguridad manejados por CYBSEC (empresa especializada en seguridad informática que opera desde 1996 con un área de cobertura de servicio en Latinoamérica desde Paraguay y Ecuador, Panamá y España) en el año 2014 siendo un número de doce incidentes reportados.

A nivel de Latinoamérica lastimosamente aún no se ha dado la verdadera importancia a las posibles debilidades que pueden existir a nivel de aplicativos web, centrando el enfoque en el Ecuador, especialmente a nivel de las entidades u organismos gubernamentales o pertenecientes al sector público no cuentan con medidas de previsión ante un potencial ataque como lo muestra en la página de noticias de la (Policía Nacional del Ecuador, 2016) y lo corrobora (Ortiz, 2016), en un espacio noticioso del periódico "El Comercio".

Con relación a componentes de seguridad, Pérez Jenny; Parco Gustavo, 2013, pertenecientes a la Escuela Superior Politécnica de Chimborazo, exponen el proyecto titulado: "Análisis de componentes de seguridad a nivel de interfaz de usuario en jsf primemobile para desarrollo de aplicaciones móviles", cuyo resultado final es determinar el nivel de seguridad del aplicativo web

[16] Técnica utilizada para medir el rendimiento de un sistema o componente del mismo.
[17] Suplantación de identidad mediante ingeniería social.
[18] Denial of services: ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

móvil para el departamento financiero de la entidad de educación superior, utilizando JSF+ PrimeMobile y componentes personalizados de seguridad.

Relacionado al proyecto mencionado enuncia las protecciones correspondientes a cada una de las vulnerabilidades analizadas en la fase teórica, en torno a la aplicación web que permite realizar gestiones de pagos y transacciones mediante dispositivos móviles en el departamento financiero, para lo que referencia a Enterprise Security API (OWASP ESAPI), la cual es una colección de métodos de seguridad para aplicaciones web, de código abierto y gratuita, la cual facilita a desarrolladores la creación de aplicaciones con menor riesgo de vulnerabilidad, teniendo relación con las referencias teóricas sobre fallas de seguridad más comunes como: fallas de inyección, cross site scripting (XSS), falsificación de peticiones en sitios cruzados, exposición de datos sensibles.

Respecto a analizar los riesgos de las aplicaciones web, Salgado Álvaro, 2014, perteneciente a la Escuela Superior Politécnica del Ejército, realiza el proyecto titulado: "Análisis de las aplicaciones web de la Superintendencia de Bancos y Seguros", entidad la cual dispone de sus aplicativos desarrollados usando la plataforma (JEE) Java Enterprise Edition, como parte de software libre, el resultado final del proyecto es emitir propuestas de buenas prácticas para el aseguramiento de las aplicaciones, con el empleo de las recomendaciones de OWASP Top 10 -2010 para el descubrimiento de las vulnerabilidades existentes en el desarrollo y su respectiva estimación de riesgos para la entidad.

En referencia al proyecto es compartido el criterio con el autor la referencia a OWASP ESAPI, en razón de las recomendaciones de seguridad para aplicaciones web, que se abordan en las recomendaciones del presente proyecto.

Capítulo 4

Metodología

La presente investigación se basa en un enfoque mixto, con el que se busca desarrollar una estrategia en base al empleo de técnicas, metodología y herramientas, aplicadas en el objetivo de evaluación, el cual es el aplicativo web de la Agencia Nacional de Tránsito, para determinar posibles vulnerabilidades y emitir recomendaciones acordes a las mismas, plasmando los resultados en el formato de un informe pericial.

La metodología a emplearse en el desarrollo del proyecto es OWASP, basada en las fases de: Reconocimiento, Mapeo, Descubrimiento y Explotación, como se muestra con más detalle en (4.3).

4.1. Diagnóstico

Para el sustento documental del presente proyecto se recolectó información de libros, artículos de periódicos y entidades de control, así como noticias emitidas por medios de comunicación, en las que abordan aspectos conceptuales, clasificación, sucesos reportados, metodología y herramientas, relacionadas a la vulneración de aplicativos web.

Se apoyó en la investigación de campo puesto que se efectuaron observaciones, así como se entrevistó al Director de Tecnologías, y al personal del departamento de tecnologías de la Agencia Nacional de Tránsito, como se indica en el Apéndice C, quienes brindaron su aporte para el desarrollo de la propuesta, ya que se evidenció la existencia de acceso y alteración de datos no autorizado al interior del sistema informático de la entidad objetivo de evaluación, difundida inclusive a través de diferentes medios de comunicación.

También se hizo uso de la investigación descriptiva debido a que en ella se describen sucesos reportados ante organismos de control, relacionados a delitos informáticos los que refieran a la temática abordada.

Otro referente tomado es la investigación explicativa, en la que se combinan los métodos analítico y sintético con los cuales se ha podido determinar conclusiones fruto de la ejecución de la fase de descubrimiento.

Se emplea también los métodos deductivo e inductivo en donde se analizan las vulnerabilidades más frecuentes hacia los aplicativos web, de la mano del método histórico - lógico en donde se evidencio la categorización de vulnerabilidades acorde al tiempo, para emplear el método sistémico - instrumental con el cual se referencia a documentos legales en los que se abordan temática sobre delitos informáticos comprendidos en la vulneración de aplicaciones, así como el uso de un documento técnico para reportar los resultados obtenidos.

4.2. Métodos aplicados

Para el desarrollo del trabajo primeramente se definió la técnica relacionada a pruebas de penetración a utilizarse siendo Black box hacking (Hacking de caja negra) como se refirió en la sección (3.1.6), debido a que la actividad se enmarca en la aplicación de algunas fases de una prueba de penetración externa con una perspectiva ética, hacia el objetivo de evaluación, entidad de la cual solamente se conoce el nombre.

En tanto que, para el desarrollo del producto final se establece el empleo de la metodología OWASP, misma que es utilizada para la realización de pruebas de penetración de forma muy específica y exclusiva, la cual abarca las fases de reconocimiento, mapeo, descubrimiento y explotación, mismas que comprenden los siguientes aspectos:

Reconocimiento, es la fase inicial en la que se plantean las bases para ejecutar la detección de vulnerabilidades para una futura ejecución de una prueba de penetración en todas sus fases, las cuales tengan resultados satisfactorios con efectividad, para lo que se definirá el objetivo de análisis, el alcance y los objetivos de la detección de vulnerabilidades propuesta. Adicionalmente se plantea el acercamiento hacia el personal que dirige la entidad conjuntamente con quienes conforman el área o departamento de Tecnologías de la Información (TI), a fin de solicitar la autorización correspondiente en la que conste el alcance que tendrá la detección de vulnerabilidades, y la aplicación de la encuesta para recolección de datos sobre eventos ocurridos y reportados en el aplicativo web de la entidad.

Para el cumplimiento de ésta fase se han empleado algunas herramientas como la consola de Samurai Web Testing Framework, específicamente el comando Who is, así como la consulta Who is, a través de la página de IANA, procedimiento que permite determinar el servidor de nombre del dominio (DNS), esto con la intervención del comando nslookup, conocer cuáles son los servidores de intercambio de correo mediante el comando dig, además efectuar búsquedas de referencias e información personal e institucional de los funcionarios relacionados al campo de TI de la entidad, mediante fuentes de información externa como redes sociales y búsquedas avanzadas en bases de datos como google hacking, finalmente se cierra la fase con el empleo de la interfaz de Netcraft, misma que permite la detección del tipo de servidor web y de sistema operativo del objetivo de evaluación.

En la fase de mapeo se plantea efectuar diferentes tareas o actividades, incluyendo realizar un spidering mediante un programa que explora el aplicativo web y sus enlaces, o descargar el sitio web completo, siendo posible trazar el flujo de la aplicación y analizar la relación entre las páginas, para luego identificar las máquinas que se utilizan dentro de la aplicación las cuales son visibles para los clientes, para lo que se efectuarán actividades de escaneo de puertos Transmission Control Protocol (TCP) y User Datagram Protocol (UPD), escaneo de versiones y reconocimiento del sistema operativo, y obtención de información de configuración del software.

Dentro de esta fase en la actividad de escaneo de puertos se busca capturar información sobre los puertos abiertos, sistema operativo y versión del servicio, para lo cual se prevé la intervención de herramientas activas y pasivas, en el caso de las activas enviando tráfico hacia el objetivo de evaluación, para ser analizadas las respuestas devueltas, empleándose para ello Nmap, mientras que por parte de las herramientas pasivas permitirá capturar y analizar sin enviar tráfico al objetivo, para lo cual se establece el uso de pOf3.

En la fase de descubrimiento se dará inicio a la exploración de forma más profunda en la aplicación web, encontrándose ya los resultados de posibles vulnerabilidades e información para la fase de explotación o ataque. Para el desarrollo de ésta fase se ha propuesto el empleo de herramientas como: Zed Attack Proxy (ZAP).

Finalmente se expone la fase de explotación, fase en la cual se unifica toda la información recolectada en cada fase anterior para efectuar los ataques al aplicativo web. Cabe indicar que ésta fase no se la contempla dentro del alcance del proyecto por estar al margen del concepto de hacking ético, pero se deja sentado las bases para una ejecución controlada de ésta fase y por

tratarse de un proyecto el cual tiene por objetivo evidenciar las vulnerabilidades detectadas mas no el efectuar o concretar el ataque.

Como herramientas útiles para aplicar en el proceso de explotación se puede emplear BeEF, AJAXShell, con las cuales es factible realizar la intromisión y al aplicativo web, siempre y cuando el alcance lo permita y lo más importante exista la respectiva autorización para su ejecución por parte de la entidad objetivo de evaluación.

Toda vez que se han aplicado las técnicas, metodología y herramientas en cada una de las fases establecidas, se propone plasmar la estrategia y los resultados obtenidos mediante el uso del formato de informe pericial, el cual sea considerado como un instrumento para la toma de decisiones en aspectos de seguridad a ser tomado en consideración por parte del personal de TI de la entidad objetivo de evaluación.

4.3. Materiales y herramientas

A continuación, se describen las herramientas tanto de hardware como de software que se han utilizado en el proyecto.

Se ha empleado una laptop la cual cuenta con las siguientes características básicas:

Tabla 4: Características del computador utilizado.

PROCESADOR	MEMORIA	DISCO DURO	TARJETA DE ALÁMBRICA	TARJETA DE INALÁMBRICA
Core ™ i7-4710HQ CPU 2.50 GHz	RAM 16.0 GB	1024 GB	Realtek PCIe GBE Family Controller	Intel ® Dual Band Wireless-AC 3160

Fuente: elaboración propia.

VMWare 12 Player como software de virtualización.

Samurai Web Testing Framework versión 3.0 como entorno de trabajo para pruebas de penetración.

Consola de Samurai Web Testing Framework

Buscador Google

Red social Facebook

Red profesional LinkedIn

Herramienta Nslookup

Herramienta dig

Página web de ARIN

Página web de IANA.

Página web de NIC.EC

Página web de Netcraft

Maltego

Nmap

Netcat

Herramienta OpenSSL

Buscador bing

Nikto

Wget

Zed Attack Proxy (ZAP)

w3af

Capítulo 5

Resultados

5.1. Producto final del proyecto de titulación

En el producto final del proyecto se estableció en uno de los objetivos específicos el utilizar el formato de un informe pericial del Consejo de la Judicatura para escribir los resultados obtenidos producto de la estrategia, la cual emplea una técnica, metodología y herramientas, aplicadas en el objetivo de evaluación, es por ello que seguidamente se sigue el formato y en cada uno de los ítems contenidos en él se irán desarrollando las actividades requeridas para alcanzar los resultados propuestos.

FORMATO DEL "INFORME PERICIAL"

5.1.1. Datos generales del proceso de indagación previa

Tabla 5: Datos generales del informe pericial.

TRIBUNAL/JUZGADO/FISCALÍA	
No. de Proceso/No. de Indagación Previa o Instrucción Fiscal	
Nombre y Apellido del Perito/a	Raúl Alfredo Panchi Herrera
Profesión, Oficio, Arte, o Actividad calificada	Ingeniería Informática
No. de Calificación y Acreditación	5000008
Fecha de terminación de la calificación y acreditación	
Dirección de contacto	Provincia: Cotopaxi, Cantón: Latacunga, Parroquia Juan Montalvo, Barrio San Martin Isimbo II, calles Tomebamba y Cicalpas vía a San José
Teléfono fijo de contacto	(03)2104008/2104047
Teléfono celular de contacto	0984523738
Correo electrónico de contacto	raulalfredoph@gmail.com

Fuente: elaboración propia en base al formato de un informe pericial del Consejo de la Judicatura.

5.1.2. Antecedentes

En mi calidad de Perito de la Función Judicial de Cotopaxi, especialidad de Ingeniería en Informática, yo Ing. Raúl Alfredo Panchi Herrera, emito el presente INFORME TÉCNICO PERICIAL, empleando como ejemplo de su estructura, el formato utilizado por peritos judiciales ante una disposición o petición efectuada por alguna autoridad, pudiendo ser un juez/a o fiscal de determinada Unidad Judicial del país, que para el ejemplo se asume la disposición de: "Efectuar la experticia técnica al aplicativo web de la Agencia Nacional de Tránsito a fin de determinar la existencia o no de vulnerabilidades", esto en el marco del desarrollo del proyecto de titulación como procedimiento académico, previo a la obtención del título de Magister en Gerencia Informática por parte del postulante.

5.1.2.1. Datos de la entidad objetivo de evaluación

Misión: Planificar, regular y controlar la gestión del Transporte Terrestre, Tránsito y Seguridad Vial en el territorio nacional, a fin de garantizar la libre y segura movilidad terrestre, prestando servicios de calidad que satisfagan la demanda ciudadana; coadyuvando a la preservación del medio ambiente y contribuyendo al desarrollo del País, en el ámbito de su competencia.

Visión: Ser la entidad líder que regule y controle el ejercicio de las competencias de transporte terrestre, tránsito y seguridad vial, basados en la transparencia y calidad de servicio que garanticen a la sociedad ecuatoriana una regulación eficaz mediante la planificación y control del transporte terrestre, tránsito y seguridad vial.

Objetivos

Incrementar la calidad y cobertura del servicio de transporte terrestre.
Incrementar la calidad del Tránsito en la Red Vial Estatal.
Incrementar la eficiencia operacional.
Incrementar el desarrollo del talento humano.
Incrementar el uso eficiente del presupuesto.
Incrementar el nivel de seguridad vial.

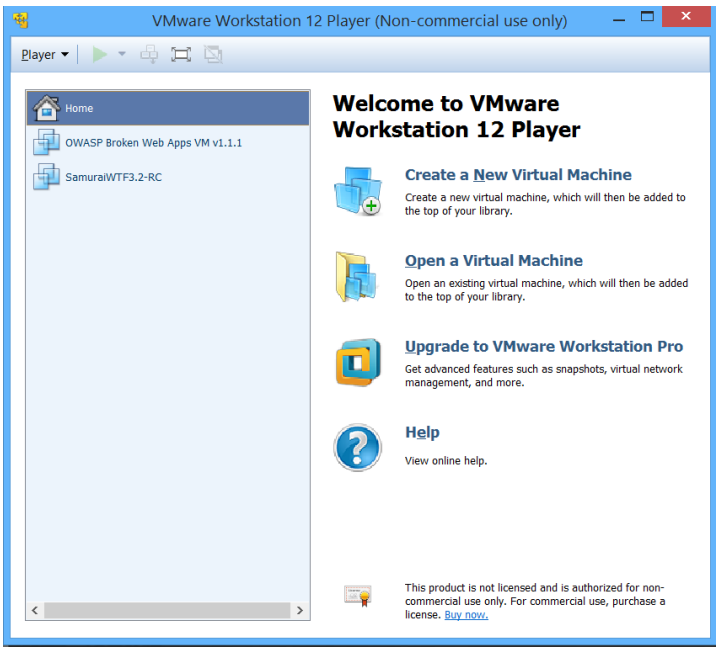
5.1.3. Consideraciones técnicas o metodología a aplicarse

En la presente simulación de actuación pericial se emplea la técnica denominada Black Box Hacking orientada a pruebas de penetración.

La metodología OWASP, con la intervención de sus fases correspondientes, es empleada para evaluar el aplicativo web de la entidad objetivo de evaluación, seguidamente se enfocan las fases desarrolladas y las actividades efectuadas en las mismas.

En cuanto al software utilizado para la implementación de la máquina virtual es VMware Workstation 12 Player, esto debido a que es una aplicación optimizada para virtualizar en un mismo computador varios sistemas operativos acorde a la necesidad, adicionalmente la versión Player es completamente gratuita.

Figura 10: Software para virtualización VMWare 12Player.



Fuente: manual de instalación de VMware Workstation.

En lo que respecta al software que se ha definido para el marco de trabajado del proyecto se ha seleccionado la plataforma Samurai Web Testing Framework en su versión 3.0, esto debido a que es un entorno basado en GNU/Linux Ubuntu, previamente configurado y de forma específica funciona como un entorno de pruebas de penetración hacia aplicaciones web, además es de código abierto e integra herramientas gratuitas usadas en cada una de las fases.

Figura 11: Entorno de trabajo de Samurai Web Testing Framework.

Fuente: interface del sistema operativo Samurai Web Testing Framework

5.1.3.1. Fase de Reconocimiento

Es la fase inicial de una prueba de penetración por ende es muy importante abordarla, esto debido a que muchas personas que desconocen o cuentan con poca experiencia en el ramo, la omiten sin considerar la importancia que tiene, ya que permite formular el ataque de manera informada elevando las posibilidades de éxito en la consecución de información.

Aspecto importante para el desarrollo del proyecto, es considerar y aplicar como base documental legal, para tomar procedimiento, el Esquema Gubernamental de Seguridad de la Información (EGSI), el cual entró en vigencia mediante Acuerdo Ministerial 166, publicado en el Registro Oficial Suplemento 88 de 25-sept-2013, por parte de la Secretaría Nacional de la Administración Pública del Ecuador, del cual seguidamente se refieren en el presente proyecto, aspectos inherentes a las vulnerabilidades en los sistemas de información, en el siguiente detalle:

En el título 2. Organización de la Seguridad de la Información, subtítulo 2.2. Coordinación de la Gestión de la Seguridad de la Información, acápite cuarto refiere a la "aprobación de las principales iniciativas para incrementar la seguridad de la información."

En el subtítulo 2.4. Procesos de autorización de nuevos servicios de procesamiento de la información, literal e) refiere a "implementar los controles necesarios para el uso de nuevos servicios para procesar información de la institución sean personales o de terceros para evitar nuevas vulnerabilidades."

En el subtítulo 2.7. Contactos con grupos de interés especiales, literal a) cita: "Mantener contacto apropiados con organizaciones públicas y privadas, asociaciones profesionales y grupos de interés especializados en seguridad de la información para mejorar el conocimiento sobre mejores prácticas y estar actualizado con información pertinente a gestión de la seguridad."; y el literal b) menciona: "recibir reportes advertencias oportunas de alertas, avisos y parches relacionados con ataques y gestión de la seguridad de la información."

El subtítulo 2.9. Identificación de los riesgos relacionados con las partes externas, literal c), refiere a "registrar y mantener las terceras partes vinculadas a la entidad…", en consideración de algunos tipos, como: asesores y auditores externos, personal temporal (estudiantes, pasantes, funcionarios públicos externos), ciudadanos o clientes, que para el caso se considera desarrollar el procedimiento desde la perspectiva académica.

En el título 6. Gestión de Comunicaciones y Operaciones, subtítulo 6.23. Sistemas de Información del Negocio, literal a), menciona "proteger o tener en cuenta las vulnerabilidades conocidas en los sistemas administrativos, financieros, y demás sistemas informáticos donde la información es compartida."

En el título 8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, subtítulo 8.16. Control de las vulnerabilidades técnicas, literal f) refiere a "identificar los riesgos asociados a una vulnerabilidad potencial y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y/o la aplicación de otros controles."; en el literal l) menciona sobre "aumentar el monitoreo para detectar o prevenir los ataques reales"; y en el literal o) hace referencia a "monitorear y evaluar a intervalos regulares las vulnerabilidades técnicas, para garantizar eficacia y eficiencia."

En el título 9. Gestión de los Incidentes de la Seguridad de la Información, subtítulo 9.2. Reporte sobre las debilidades en la seguridad, literal a), enmarca "Todos los empleados,

contratistas y usuarios de terceras partes deberían informar sobre éstos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberán ser fáciles, accesibles y disponibles. Se les debe informar a ellos que en ninguna circunstancia deberán intentar probar una debilidad sospechada", aspecto a destacar, ya que, en la aplicación de la metodología, se establecen cuatro fases, de las cuales no se aplicará la cuarta que comprende a la explotación misma de las vulnerabilidades, manteniéndose dentro de una perspectiva de hacking ético.

Finalmente, en el título 11. Cumplimiento, subtítulo 11.8. Verificación del cumplimiento técnico, literal e), establece "ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes…"

5.1.3.1.1. Alcance del proyecto

El primer paso dentro de ésta etapa es definir el alcance de la prueba constituyendo el objetivo general del presente trabajo, el desarrollar una estrategia para la detección de vulnerabilidades en el aplicativo web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones, con el empleo de la metodología OWASP en sus fases, a excepción de la última fase que es la de explotación, en la que se dejará sentado la base informativa del procedimiento, así también las herramientas que pueden ser empleadas para efectuar una prueba de penetración de forma integral, pudiéndose posteriormente llegar a la explotación o vulneración misma del objetivo de evaluación, esto debido a que el marco legal y ético del trabajo se enfoca en esencia desde una perspectiva académica y de hacking ético, a fin de brindar a la entidad, un sustento procedimental que puede ser aplicado, para tomar decisión y acción frente a potenciales vulnerabilidades detectadas, y evitar ataques reales al aplicativo web.

No se establece el acceso, obtención o manipulación de datos e información de usuarios contenidas en bases de datos, a través del procedimiento, ya que el aspecto central es detectar posibles vulnerabilidades en el aplicativo web.

Al tratarse de un proyecto académico de titulación, los resultados obtenidos, mismos que arrojen información considerada confidencial, así como datos de configuración y los resultados de vulnerabilidades encontradas, serán protegidos para su visualización en el documento entregable mediante pixelado o desenfoque en partes o en la totalidad de las imágenes, más en el documento entregable hacia la entidad objetivo de evaluación si se visualizarán en detalle.

Además, se establece la elaboración de una carta compromiso por parte del autor en mantener la confidencialidad de la información de vulnerabilidades que se obtenga.

5.1.3.1.2. Acercamiento al aplicativo a evaluar

Para el desarrollo de la primera fase, existen varias herramientas que pueden ser empleadas, las mismas que utilizadas de una manera combinada permitirán obtener mejores resultados, mismos que en el caso de evitar la presente fase no se podrían localizar, y es así que se consideran las herramientas:

El primer acercamiento se efectúa ingresando al aplicativo web del objetivo de evaluación, a través de un navegador web.

Figura 12: Página web de la entidad objetivo de evaluación.

Fuente: sitio web de la Agencia Nacional de Tránsito (objetivo de evaluación)

5.1.3.1.3. Capturando información sobre el personal de TI

Inicialmente se hace uso de fuentes de información externa en donde se puede obtener algún tipo de información sin la interacción directa con el objetivo de evaluación, para lo cual se utilizan buscadores como Google Groups, redes profesionales o sociales como LinkedIn, Google+, Twitter, Facebook, páginas de anuncios y bolsas de trabajo entre otros, en los cuales se puede encontrar buena cantidad de información personal de quienes laboran de cerca en el entorno del objetivo de evaluación, especialmente se puede encontrar información de perfiles de formación y capacidades profesionales, tecnologías en las que se desempeñan, experiencia, aptitudes, capacitación, campo de desempeño, plataformas de manejo, actividad de los empleados, correos electrónicos, y perfeccionamiento en determinadas tecnologías, inclusive fotografías del entorno laboral en el que se desenvuelven las cuales pueden revelar aspectos relacionados a la infraestructura tecnológica de la entidad, constituyéndose en información de gran utilidad para las etapas siguientes. Específicamente en el caso se efectúa una búsqueda en la red profesional LinkedIn a fin de recabar información del Director de Tecnologías de la entidad evaluada.

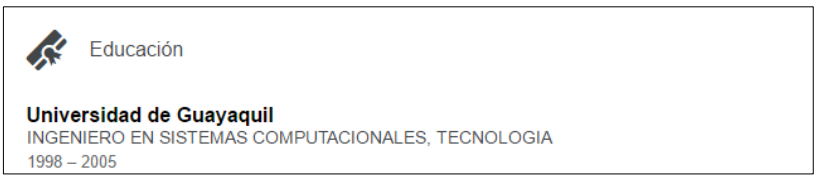
Figura 13: Información básica del ex-Director de Tecnologías de la entidad objetivo de evaluación.

Fuente: sitio web de la red profesional LinkedIn

Figura 14: Información de experiencia del ex-Director de Tecnologías de la entidad objetivo de evaluación.

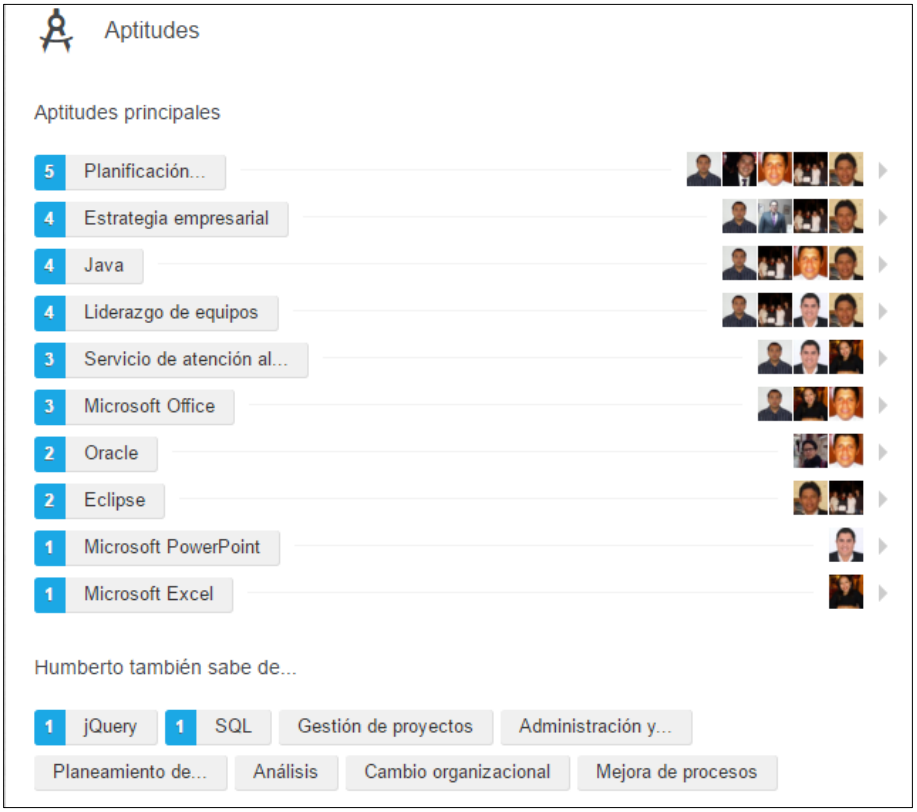
Fuente: sitio web de la red profesional LinkedIn

Figura 15: Información educativa del ex-Director de Tecnologías de la entidad objetivo de evaluación.



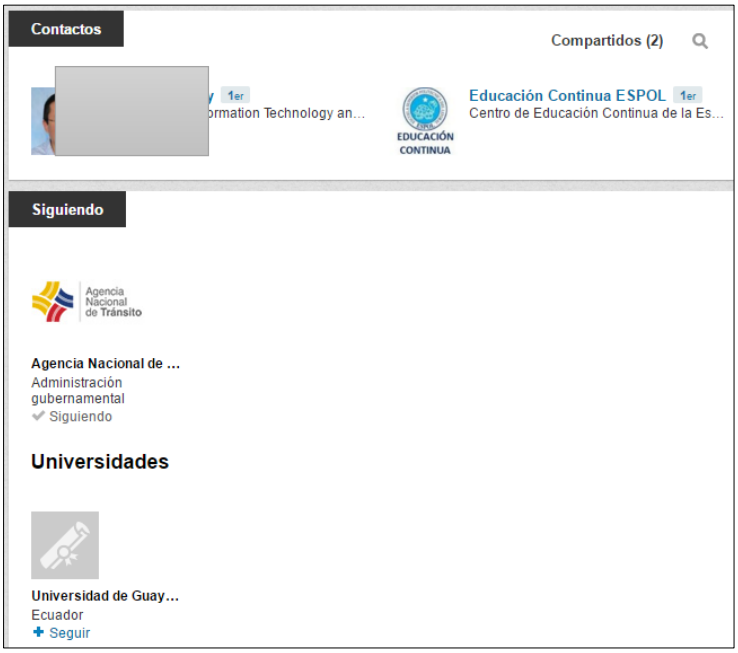
Fuente: sitio web de la red profesional LinkedIn

Figura 16: Información de aptitudes del ex-Director de Tecnologías de la entidad objetivo de evaluación.



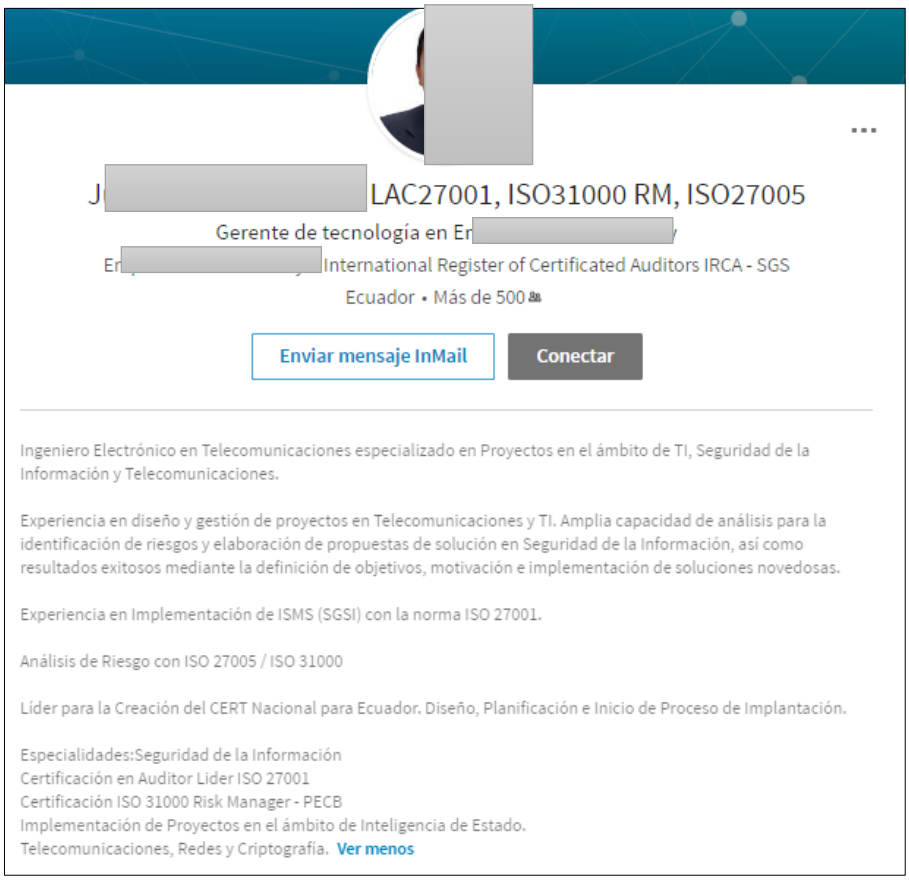
Fuente: sitio web de la red profesional LinkedIn

Figura 17: Información de contactos del ex-Director de Tecnologías de la entidad objetivo de evaluación.



Fuente: sitio web de la red profesional LinkedIn

Figura 18: Información del Director de Tecnologías de la entidad objetivo de evaluación.



Fuente: sitio web de la red profesional LinkedIn

Como se muestra en las imágenes que anteceden, con el empleo de la red profesional LinkedIn, se ha localizado información del Director de TI de la entidad considerada objetivo de evaluación, información como experiencia profesional, formación educativa, aptitudes, en donde se dispone de un probable perfil de manejo y dominio de tecnologías, herramientas y procesos, que pueden ser un indicio de implementación en la entidad objetivo.

5.1.3.1.4. Capturando información sobre el dominio

Para ésta gestión se emplea el protocolo Whois, el mismo que permite capturar información relacionada a un dominio o dirección IP objetivo de evaluación, pudiendo ser información de contacto, nombre de propietario, servidores de nombres autorizados por el dominio. El paso inicial es desplegar la consola de comandos de Samurai Web Testing Framework (SWTF), en la que se ingresa la instrucción: whois dominio

Figura 19: Información obtenida mediante protocolo Whois.

```
samurai@samuraiwtf:~$ whois ant.gob.ec


Los datos detallados a continuación por NIC.EC es información pública cuyo propósito es
únicamente informativo que sirve para la obtención de la información acerca de o
relacionado con los registros de un Nombre de Dominio. Los datos se muestran de acuerdo
a los datos de NIC.EC en la última actualización de su base de datos. Al realizar una
búsqueda de WHOIS de un dominio, usted declara y acepta que los datos serán utilizados
solo para fines legales y que no utilizara los datos para envíos masivos no solicitados
de correo electrónico o para publicidad o fines comerciales no solicitados.


Domain Information
Query: ant.gob.ec
Status: Delegated
Created: 07 Apr 2011
Modified: 22 Apr 2017
Expires: 07 Apr 2021
Name Servers:
    p
    t

Registrar Information
Registrar Name: LogicBoxes
Country: IN
Phone: 1 832 2951535



Registrant:
Email Address: j
Phone Number: +0

Local Name: J
Local Organisation: Agencia Nacional de Regulación y Control del Transporte TerrestreTránsito y Seguridad Vial
Local Address:
        Av.Mariscal Sucre SN y Jóse Sánchez
        Quito, Pichincha EC170528
        EC
```

```
Admin Contact:
Email Address: l                .ec
Phone Number: +0

Local Name: L
Local Organisation: Agencia Nacional de Regulación y Control del Transporte TerrestreTránsito y Seguridad Vial
Local Address:
        Av.Mariscal Sucre SN y Jóse Sánchez
        Quito, Pichincha EC170528
        EC



Technical Contact:
Email Address: a                .ec
Phone Number: +0

Local Name: A
Local Organisation: Agencia Nacional de Regulación y Control del Transporte TerrestreTránsito y Seguridad Vial
Local Address:
        Av.Mariscal Sucre SN y Jóse Sánchez
        Quito, Pichincha EC170528
        EC



Billing Contact:
Email Address: l                .ec
Phone Number: +0

Local Name: L
Local Organisation: Agencia Nacional de Regulación y Control del Transporte TerrestreTránsito y Seguridad Vial
Local Address:
        Av.Mariscal Sucre SN y Jóse Sánchez
        Quito, Pichincha EC170528
        EC
```

Fuente: elaboración propia, consulta whois en consola de SWTF.

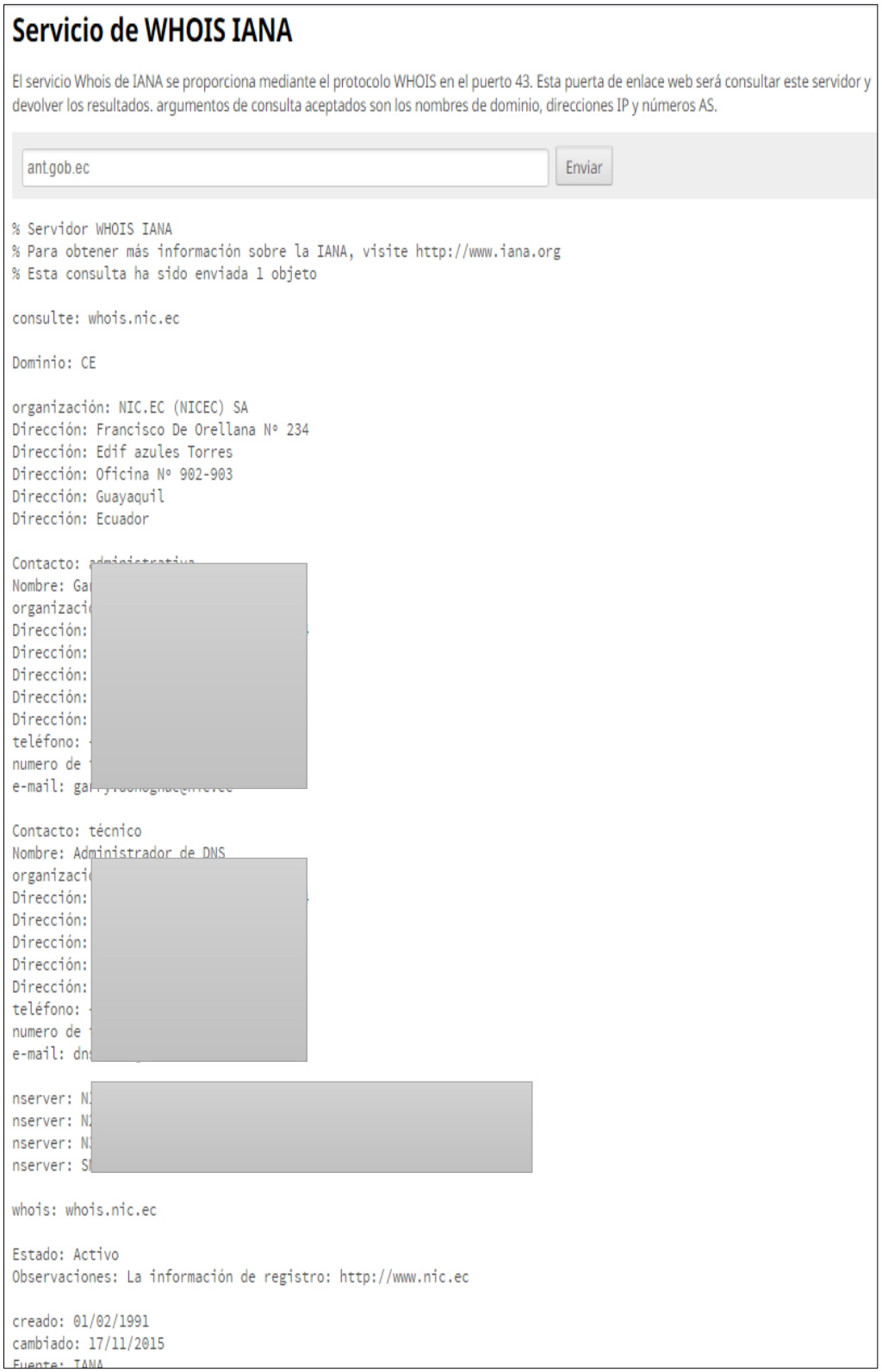
Como se muestra en la Figura 19, se ha logrado obtener información como: servidores de nombre del dominio, fecha de creación, modificación y expiración, información del registrador, del contacto administrativo, del contacto técnico; sus nombres, teléfonos, correos y dirección organizacional, respectivamente, información útil para la realización de ataques de ingeniería social, o enviar archivos, código a los correos, toda vez que se conoce la estructura o formato de nombres de usuario, siendo útiles para probar con posibles nombres de usuario para autenticación, siendo lo más importante de ésta acción los servidores de nombre.

Este proceso también se lo puede efectuar empleando una interfaz visual proporcionada por la *Internet Assigned Numbers Authority* (IANA) que es la Autoridad de Internet para la asignación de números, lo que se puede evidenciar en la Figura: 20. El acceso es mediante la página: www.iana,org/whois, en donde se coloca el nombre del dominio.

También puede ser empleado dicho protocolo mediante consulta en la página de NIC.EC, que es el administrador de dominios para Ecuador, el resultado se muestra en la Figura: 21. De similar forma para el caso se lo efectúa a través de la página: www.whois.com/whois/nic.ec, colocándose el nombre del dominio.

Como se evidencia en las Figuras. 20 y 21, respectivamente, se ha logrado mostrar información similar que con la consulta who is efectuada mediante el terminal de SWTF.

Figura 20: Consulta Whois mediante la interfaz gráfica de IANA.



Servicio de WHOIS IANA

El servicio Whois de IANA se proporciona mediante el protocolo WHOIS en el puerto 43. Esta puerta de enlace web será consultar este servidor y devolver los resultados. argumentos de consulta aceptados son los nombres de dominio, direcciones IP y números AS.

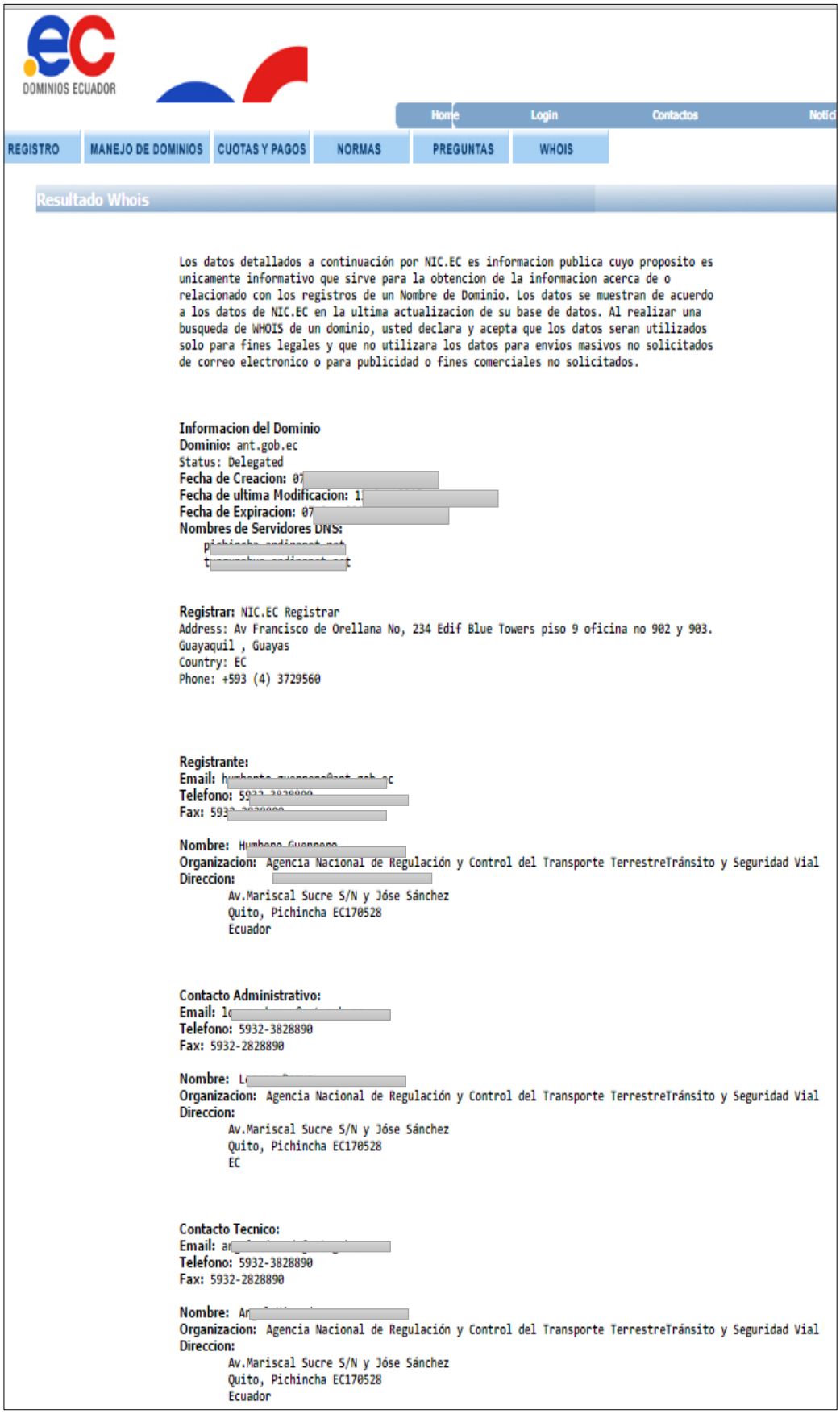
ant.gob.ec

Enviar

```
% Servidor WHOIS IANA
% Para obtener más información sobre la IANA, visite http://www.iana.org
% Esta consulta ha sido enviada 1 objeto

consulte: whois.nic.ec

Dominio: CE

organización: NIC.EC (NICEC) SA
Dirección: Francisco De Orellana Nº 234
Dirección: Edif azules Torres
Dirección: Oficina Nº 902-903
Dirección: Guayaquil
Dirección: Ecuador

Contacto: administrativa
Nombre: Ga
organizaci
Dirección:
Dirección:
Dirección:
Dirección:
Dirección:
teléfono:
numero de
e-mail: ga

Contacto: técnico
Nombre: Administrador de DNS
organizaci
Dirección:
Dirección:
Dirección:
Dirección:
Dirección:
teléfono:
numero de
e-mail: dn

nserver: N
nserver: N
nserver: N
nserver: S

whois: whois.nic.ec

Estado: Activo
Observaciones: La información de registro: http://www.nic.ec

creado: 01/02/1991
cambiado: 17/11/2015
Fuente: IANA
```

Fuente: sitio web de IANA

Figura 21: Consulta Whois mediante la interfaz gráfica en NIC EC.



Fuente: sitio web de NIC EC

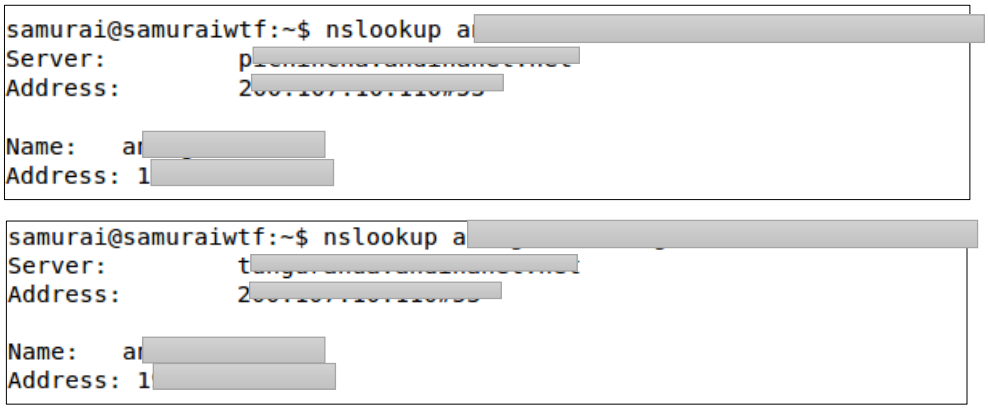
5.1.3.1.5. Consultando la dirección IP a la cual resuelve el nombre de dominio.

Este proceso permite conocer cuál es la dirección IP a la cual resuelve el nombre de dominio.

Se debe ejecutar la consola de SWTF, en ella el comando nslookup, seguido del dominio y luego el servidor de nombre, quedando la instrucción así:

nslookup dominio servidor de nombre.

Figura 22: Consulta de la dirección IP a la cual resuelve el nombre de dominio mediante nslookup.



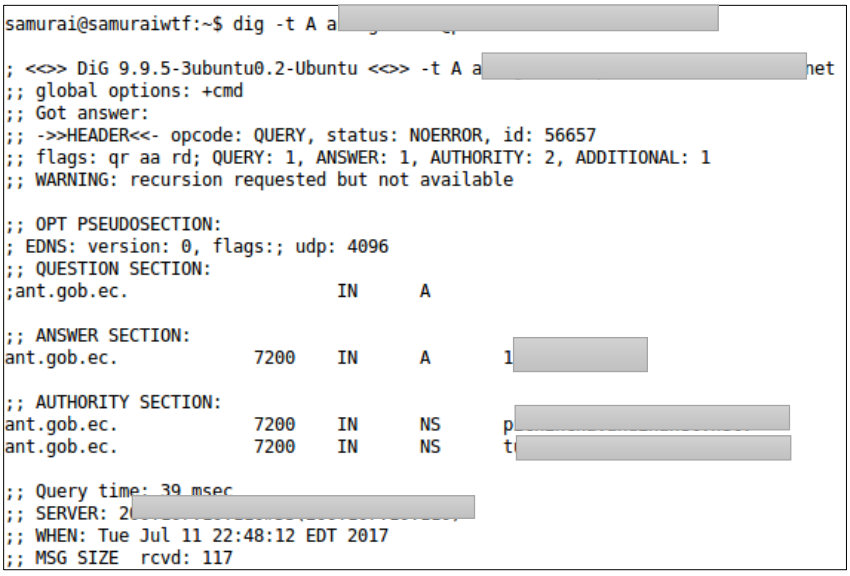
Fuente: elaboración propia, consulta nslookup en la consola de SWTF.

Para el caso se ha consultado a los dos servidores de nombre localizados y se ha obtenido la dirección IP a la cual resuelve el nombre de dominio.

Para consultar registros específicos definidos en la zona para ese dominio, se emplea el comando dig, seguido de las letras –t A, las cuales definen el tipo de consulta, seguido del dominio, y luego el servidor de nombre antecedido del símbolo @. La instrucción se establece:

dig –t A dominio @servidor de nombre

Figura 23: Consultar si existen registros específicos definidos en la zona para el dominio.



Fuente: elaboración propia, comando dig en la consola de SWTF.

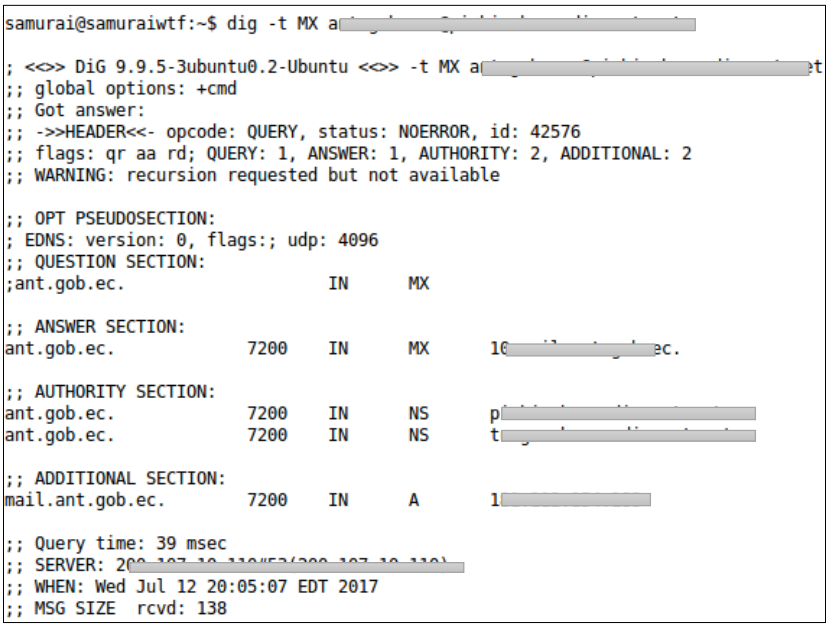
En la Figura: 23, en el campo ANSWER SECTION, se muestra la respuesta, la cual es la misma que en el caso del resultado obtenido mediante la consulta efectuada con el comando nslookup, mostrado en la Figura: 22.

5.1.3.1.6. Consultando cuales son los servidores de intercambio de correo.

Los servidores de intercambio de correo, son los encargados de enviar o recibir correo desde un dominio específico. Para conocer los mismos, se puede emplear el comando dig, seguid de –t MX, luego el dominio y luego el servidor de nombre antecedido del símbolo @, quedando la instrucción así:

dig –t MX dominio @servidor de nombre.

Figura 24: Consultar cuales son los servidores de intercambio de correo.



Fuente: elaboración propia, comando dig –t MX en la consola de SWTF.

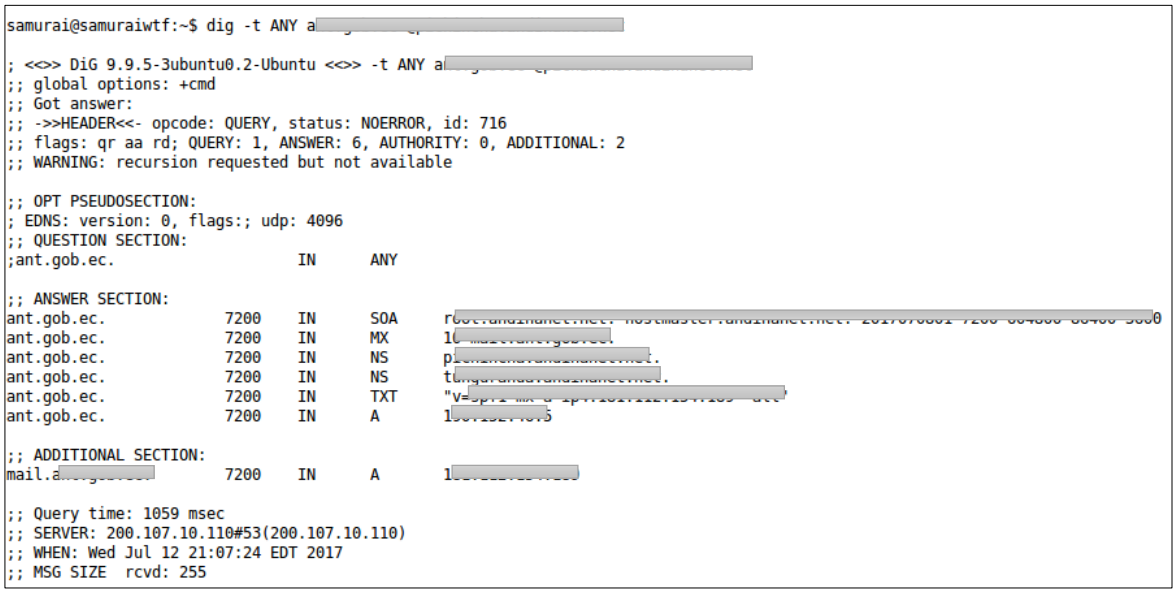
En la Figura: 24, en el campo ADDITIONAL SECTION, se muestra la respuesta, relacionada a la dirección IP del servidor de intercambio de correo.

5.1.3.1.7. Mostrando todos los registros definidos para el dominio.

Para mostrar todos los registros definidos para el dominio establecido, se usa el comando dig –t ANY, seguido del dominio y luego el servidor de nombre antecedido del símbolo @, quedando la instrucción así:

dig –t ANY dominio @servidor de nombre.

Figura 25: Consultando todos los registros definidos para el dominio.



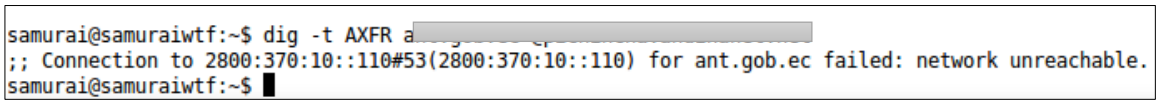
Fuente: elaboración propia, comando dig –t ANY en la consola de SWTF.

5.1.3.1.8. Comprobando la configuración de servidores principal y secundario mediante transferencia de zona.

Si el servidor principal o secundario, disponen de una configuración inadecuada, mediante la transferencia de zona, se puede ver información mucho más sensible e interna de la organización, como subdominios, IP, números de teléfono, información de usuarios, la que no debe ser permitida, todo esto sin haber tenido el impedimento de atravesar firewall o haber explotado alguna vulnerabilidad, todo debido a configuraciones inadecuadas de los servidores DNS. Para comprobar éste concepto, se emplea el comando dig, -t AXFR, seguido del dominio y luego el servidor de nombre antecedido del símbolo @, quedando la instrucción así:

dig –t AXFR dominio @servidor de nombre.

Figura 26: Comprobando la configuración de servidores principal y secundario mediante transferencia de zona.



Fuente: elaboración propia, comando dig –t AXFR en la consola de SWTF.

Como se muestra en la Figura: 26, no permite visualizar información alguna, toda vez aplicada la instrucción, lo que indica que las configuraciones de los servidores son adecuadas para el nivel de seguridad que se ha evaluado.

5.1.3.1.9. Consultando en fuentes de información externa.

Para proceder con la búsqueda de información sin interactuar con el objetivo de evaluación, se puede recurrir a fuentes de información externa, siendo estas: bases de datos de terceros como Who is, DNS, sitios en los que se almacena o "cachea" información, motores de búsqueda, grupos de noticias, grupos de google, listas de correo electrónico, foros web, redes sociales como Facebook, LinkedIn, Twitter, Google+, entre otras fuentes que pueden proporcionar información tanto personal como institucional, que conlleve o sea útil para un proceso ingeniería social y posterior vulneración.

Para el caso del objetivo de evaluación se emplea la directiva site: desde el buscador google más la red social en la que se realice la búsqueda y una expresión asociada a la entidad objetivo, para el ejemplo de trata de localizar a personas que tengan el perfil de director de la entidad.

Figura 27: Búsqueda de información personal en Google, mediante la directiva site:

Fuente: elaboración propia, búsqueda en Google mediante la directiva site.

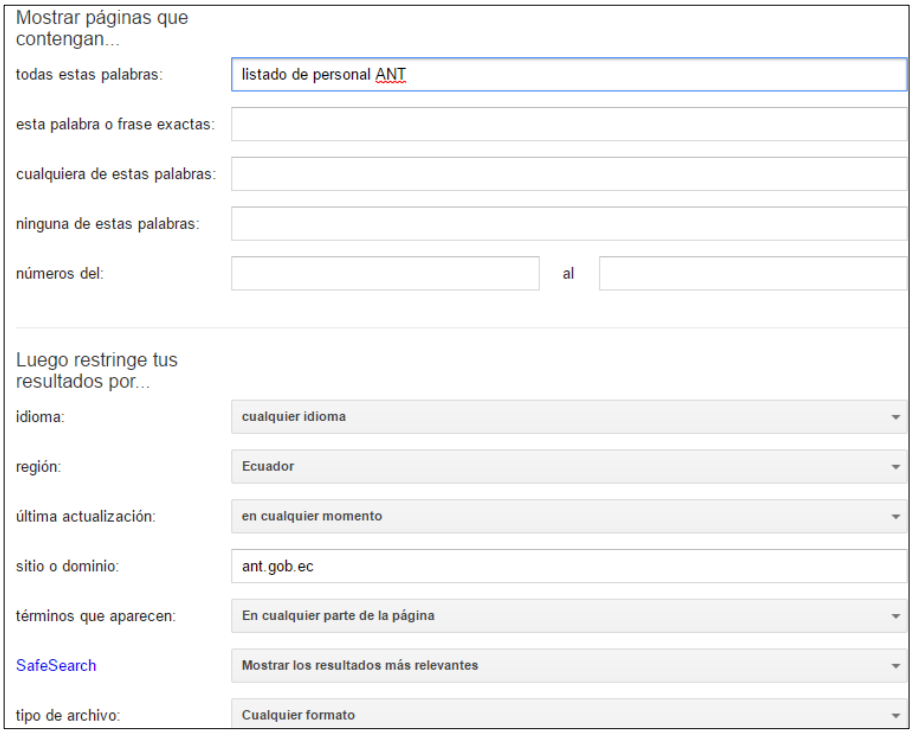
Con éste proceso se ha obtenido perfiles de personas que forman parte de la entidad, y al interior de los mismos se puede extraer información como hoja de vida, experiencia, áreas de dominio, las cuales pueden ser relevantes en un

contexto de averiguar las tecnologías utilizadas y aspectos de seguridad empleados en la entidad evaluada.

Otras fuentes de información que serán útiles para fortalecer ésta fase puede ser Google Hacking, mediante la utilización de las directivas avanzadas del motor de búsqueda como: site, inurl, intitle, link, filetype, asociadas a la base de datos de Google Hacking la cual contiene una lista de consultas relacionadas a archivos conteniendo nombres de usuario o contraseñas, directorios sensibles, archivos y servidores vulnerables, mensajes de error, entre otros.

Se procede mediante búsquedas avanzadas, de los listados del personal, así como también de algún archivo que contenga el directorio telefónico según dependencias o funcionarios, mostrado en las Figuras: 28 y Figura: 29, respectivamente.

Figura 28: Búsqueda avanzada por listado de personal del objetivo de evaluación.



Fuente: página web del buscador Google

Figura 29: Búsqueda avanzada del directorio telefónico de la entidad objetivo de evaluación.

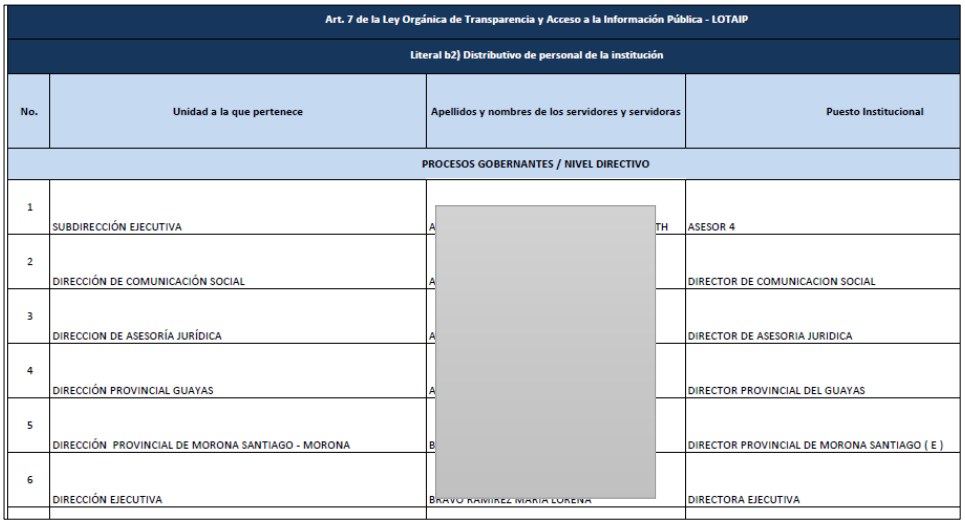
Fuente: página web del buscador google

Como resultado de la búsqueda avanzada relacionada a listados del personal (Figura: 30), se evidencia la disponibilidad de un archivo de los años 2014 y 2015 respectivamente, en formato .pdf (Figura: 31), en el cual se puede obtener información de: unidad a la que pertenece, apellidos y nombres, y puesto institucional de los servidores de la entidad. Se encuentra también archivos con nóminas de años anteriores en formato .xlsx (Figura: 32), en donde se muestra detalles de provincia, cantón, dependencia, unidad, cédula, cargo público, apellidos y nombres de funcionarios, lo cual puede constituir un aspecto de inseguridad al poderse contactar con ex funcionarios de la entidad y recabar información.

Figura 30: Resultados de la búsqueda avanzada por listado de personal de la entidad evaluada.

Fuente: página web del buscador Google

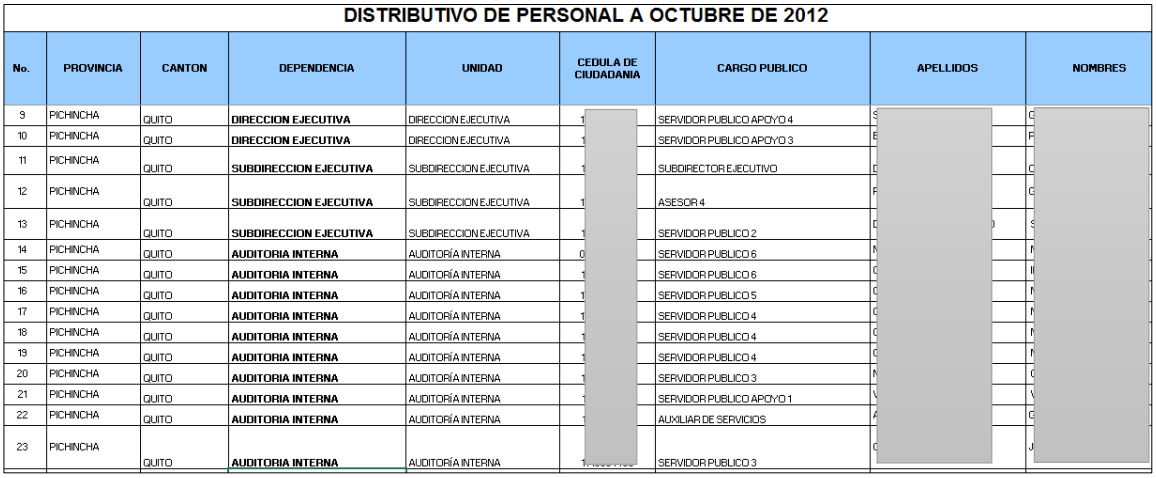
Figura 31: Archivo en formato .pdf conteniendo el listado del personal de la entidad evaluada.



Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP			
Literal b2) Distributivo de personal de la institución			
No.	Unidad a la que pertenece	Apellidos y nombres de los servidores y servidoras	Puesto Institucional
PROCESOS GOBERNANTES / NIVEL DIRECTIVO			
1	SUBDIRECCIÓN EJECUTIVA	A [redacted] TH	ASESOR 4
2	DIRECCIÓN DE COMUNICACIÓN SOCIAL	A	DIRECTOR DE COMUNICACION SOCIAL
3	DIRECCION DE ASESORÍA JURÍDICA	A	DIRECTOR DE ASESORIA JURIDICA
4	DIRECCIÓN PROVINCIAL GUAYAS	A	DIRECTOR PROVINCIAL DEL GUAYAS
5	DIRECCIÓN PROVINCIAL DE MORONA SANTIAGO - MORONA	B	DIRECTOR PROVINCIAL DE MORONA SANTIAGO (E)
6	DIRECCIÓN EJECUTIVA	BRAVO RAMIREZ MARIA LORENA	DIRECTORA EJECUTIVA

Fuente: archivo en formato pdf, localizado en la página web del objetivo de evaluación.

Figura 32: Listado del personal del objetivo de evaluación localizado en formato .xlsx.

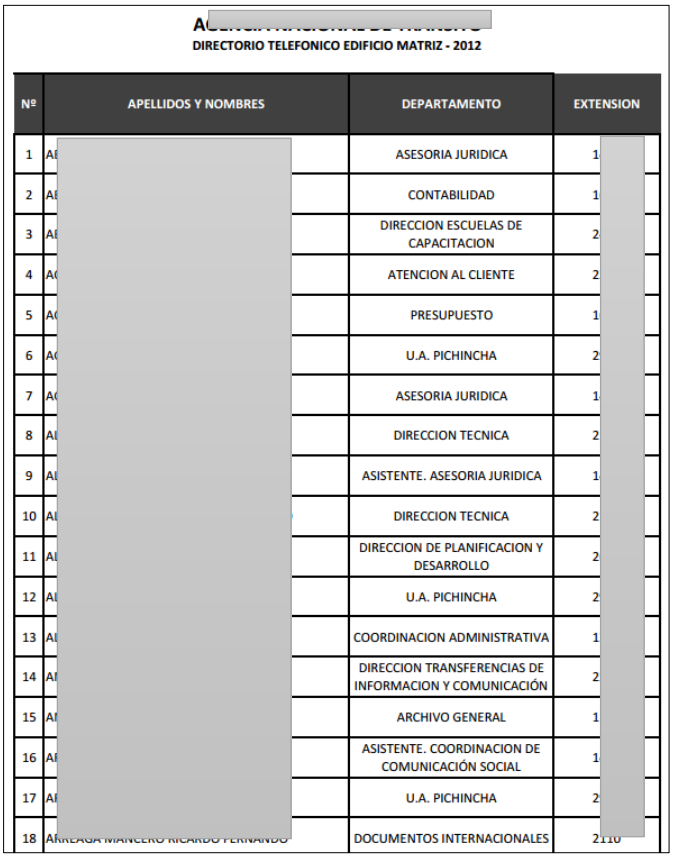


DISTRIBUTIVO DE PERSONAL A OCTUBRE DE 2012								
No.	PROVINCIA	CANTON	DEPENDENCIA	UNIDAD	CEDULA DE CIUDADANIA	CARGO PUBLICO	APELLIDOS	NOMBRES
9	PICHINCHA	QUITO	DIRECCION EJECUTIVA	DIRECCION EJECUTIVA	1	SERVIDOR PUBLICO APOYO 4	S	C
10	PICHINCHA	QUITO	DIRECCION EJECUTIVA	DIRECCION EJECUTIVA	1	SERVIDOR PUBLICO APOYO 3	B	F
11	PICHINCHA	QUITO	SUBDIRECCION EJECUTIVA	SUBDIRECCION EJECUTIVA	1	SUBDIRECTOR EJECUTIVO	D	C
12	PICHINCHA	QUITO	SUBDIRECCION EJECUTIVA	SUBDIRECCION EJECUTIVA	1	ASESOR 4	P	G
13	PICHINCHA	QUITO	SUBDIRECCION EJECUTIVA	SUBDIRECCION EJECUTIVA	1	SERVIDOR PUBLICO 2	D	) S
14	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	0	SERVIDOR PUBLICO 6	N	N
15	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO 6	C	I
16	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO 5	C	M
17	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO 4	C	M
18	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO 4	C	M
19	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO 4	C	M
20	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO 3	M	C
21	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO APOYO 1	V	V
22	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	AUXILIAR DE SERVICIOS	A	G
23	PICHINCHA	QUITO	AUDITORIA INTERNA	AUDITORÍA INTERNA	1	SERVIDOR PUBLICO 3	C	J

Fuente: archivo en formato .xls, localizado en la página web del objetivo de evaluación.

En cuanto a la búsqueda de algún archivo que contenga el directorio telefónico, se ha localizado un archivo del año 2012, en formato .pdf (Figura: 33), mismo que contiene el listado del personal por apellidos y nombres, departamento y extensión.

Figura 33: Directorio telefónico encontrado de la entidad objetivo de evaluación.



DIRECTORIO TELEFONICO EDIFICIO MATRIZ - 2012

Nº	APELLIDOS Y NOMBRES	DEPARTAMENTO	EXTENSION
1	[redacted]	ASESORIA JURIDICA	1
2		CONTABILIDAD	1
3		DIRECCION ESCUELAS DE CAPACITACION	2
4		ATENCION AL CLIENTE	2
5		PRESUPUESTO	1
6		U.A. PICHINCHA	2
7		ASESORIA JURIDICA	1
8		DIRECCION TECNICA	2
9		ASISTENTE. ASESORIA JURIDICA	1
10		DIRECCION TECNICA	2
11		DIRECCION DE PLANIFICACION Y DESARROLLO	2
12		U.A. PICHINCHA	2
13		COORDINACION ADMINISTRATIVA	1
14		DIRECCION TRANSFERENCIAS DE INFORMACION Y COMUNICACIÓN	2
15		ARCHIVO GENERAL	1
16		ASISTENTE. COORDINACION DE COMUNICACIÓN SOCIAL	1
17		U.A. PICHINCHA	2
18	[redacted]	DOCUMENTOS INTERNACIONALES	2110

Fuente: archivo en formato pdf, localizado en la página web del objetivo de evaluación.

Empleando directivas adicionales del buscador Google, se puede indagar por ejemplo la infraestructura de la página web, para el caso se coloca en el buscador Google la siguiente instrucción: site:dominio intext:"Joomla"

Obteniéndose como resultado el enlace de acceso a la administración de Joomla, mostrado en la Figura: 34.

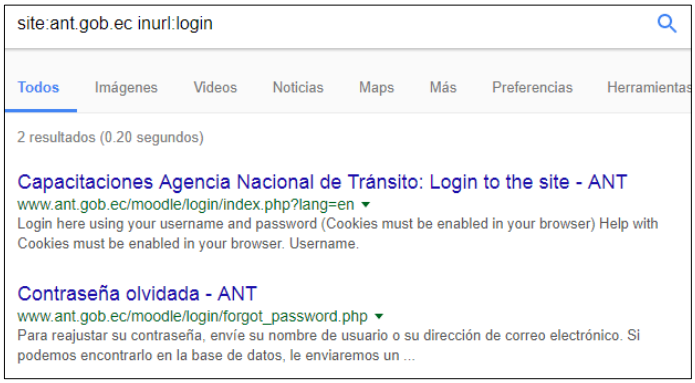
Figura 34: Resultado de la búsqueda de la posible infraestructura de la página web de la entidad objetivo.

Fuente: enlace de la página web del objetivo de evaluación.

También se busca en el sitio objetivo, palabras contenidas dentro de la página, mediante la instrucción: site:dominio inurl:login

Obteniéndose, dos resultados los cuales contienen enlaces a páginas que cuentan con formularios de login, mostrado en la Figura: 35.

Figura 35: Búsqueda de formularios de login en el objetivo de evaluación.



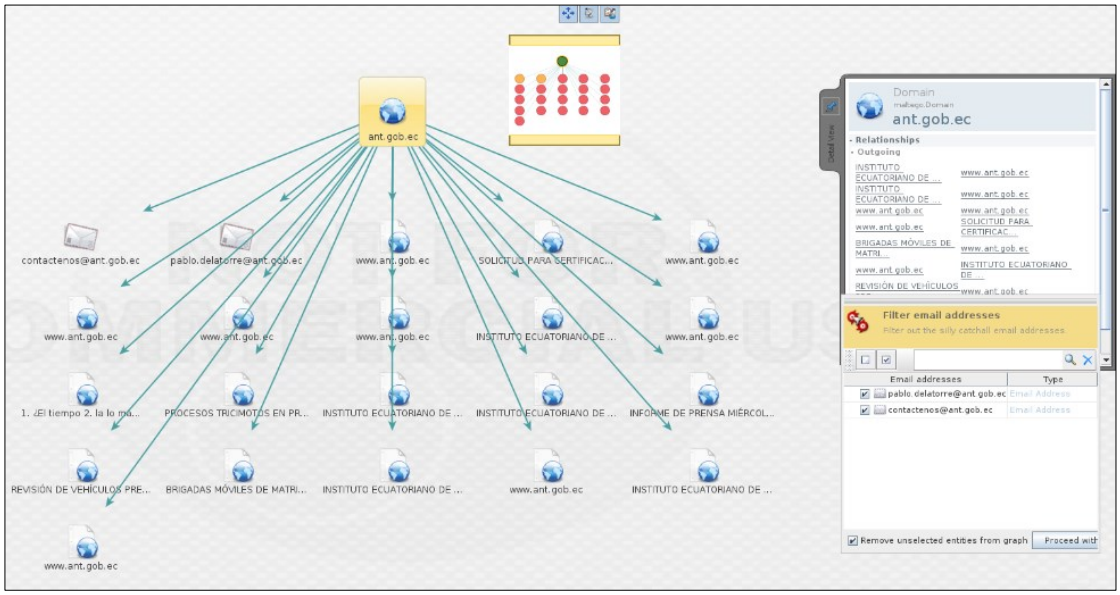
Fuente: Buscador Google, directiva site y inurl.

5.1.3.1.10. Detección de información, correos asociados y servidores DNS, de forma gráfica mediante Maltego.

Para finalizar la fase de reconocimiento se utilizará Maltego, ya que es una herramienta que posibilita recolectar datos del objetivo de evaluación, con el uso de objetos gráficos y menús contextuales, aplicando "transformaciones" en los objetos de acuerdo al nivel y profundidad de información que se desee obtener. Los objetos pueden ser dispositivos, elementos de infraestructura como nombres de dominio, direcciones IP, entradas DNS, ubicaciones como sitios físicos, ciudades, oficinas; pruebas de intrusión, elementos personales y sociales como nombres de personas, documentos, imágenes, correos, números de teléfono, en tanto que los dispositivos pueden ser teléfonos, cámaras, los objetos tipo pruebas dan la posibilidad de encontrar información sobre las tecnologías utilizadas.

Existe la versión gratuita del software la cual permite instalar una vez descargada desde la página de Paterva, y luego registrarse. Una vez instalado seleccionando la opción Company Stalker, permite recolectar los correos de una organización según el dominio requerido.

Figura 36: Detectando correos asociados al dominio objetivo de evaluación mediante Maltego.

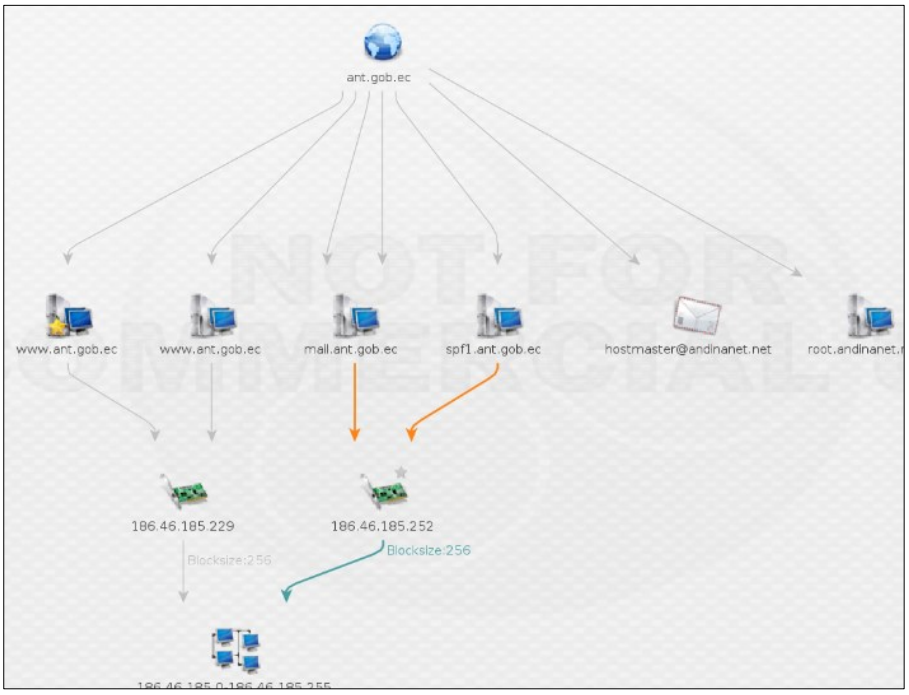


Fuente: interfaz de la herramienta Maltego

De la operación se visualizan correos asociados al dominio evaluado.

La opción Footprint L1, permite recolectar información básica del dominio analizado.

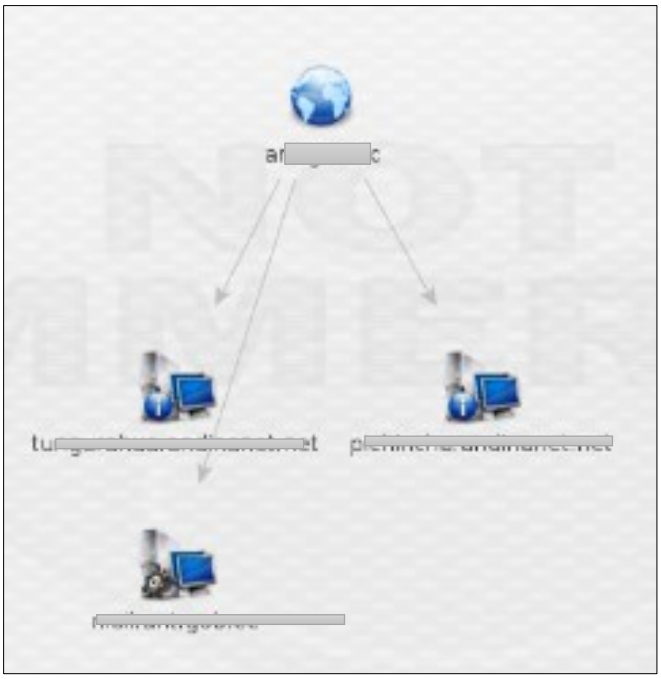
Figura 37: Detectando IP del dominio objetivo de evaluación mediante Maltego.



Fuente: interfaz de la herramienta Maltego

La opción Footprint L2, permite recolectar información media del dominio analizado.

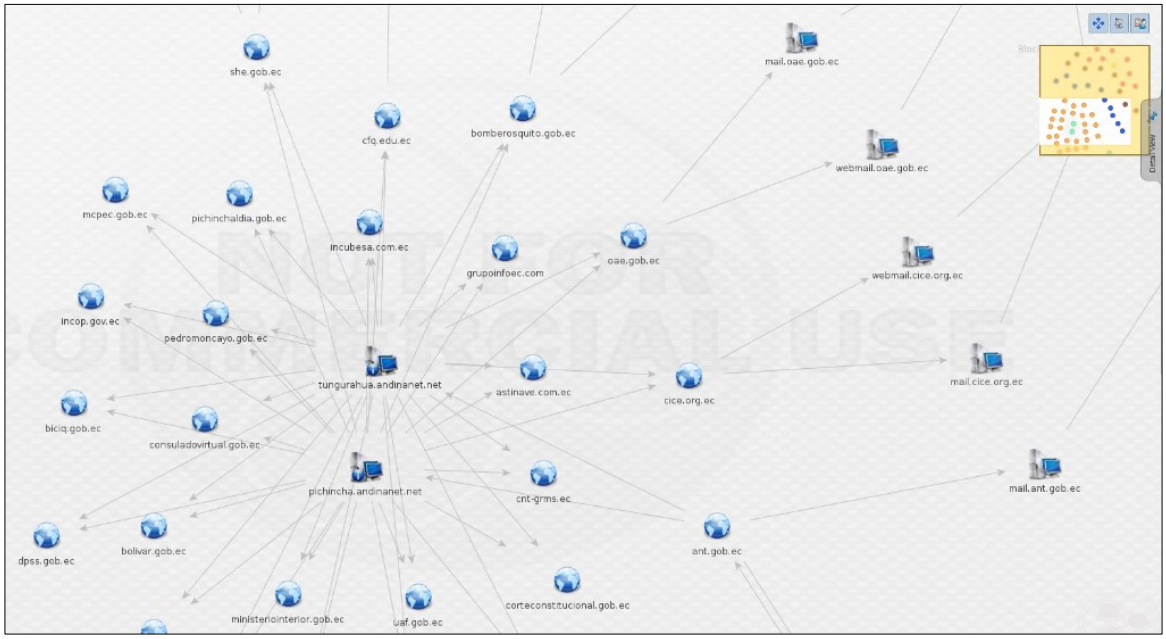
Figura 38: Detectando servidores DNS del dominio objetivo de evaluación mediante Maltego.



Fuente: interfaz de la herramienta Maltego

La opción Footprint L3, permite recolectar información avanzada del dominio analizado.

Figura 39: Detectando sitios asociados a los servidores DNS del dominio objetivo de evaluación mediante Maltego.



Fuente: interfaz de la herramienta Maltego

5.1.3.2. Fase de Mapeo

En la fase de mapeo se pueden abordar diferentes tipos de tareas como la realización de un "spidering", proceso que comprende en visitar los enlaces y si los tuviere otros enlaces dentro de los principales, esto mediante un programa que explora el aplicativo web y sus enlaces, o descargar el sitio web completo, siendo posible trazar el flujo de la aplicación y analizar la relación entre las páginas.

Otra actividad a efectuar es identificar las máquinas que se utilizan dentro de la aplicación, aquellas que sean visibles para los clientes, conjuntamente con un escaneo del sistema operativo y la versión del servicio.

También se efectuarán actividades de escaneo de puertos en busca de información sobre los puertos abierto.

5.1.3.2.1. Escaneo de puertos y sistema operativo.

La intención es capturar información sobre los puertos abiertos, sistema operativo, y versión del servicio.

Para éstas actividades, se prevé la intervención de herramientas activas y pasivas, en el caso de las activas son las que envían tráfico hacia el objetivo de evaluación, para ser analizadas las respuestas devueltas, empleándose para ello Nmap, mientras que por parte de las herramientas pasivas se propone pOf3, la cual permitirá capturar y analizar sin enviar tráfico al objetivo de evaluación.

Entonces se da inicio al escaneo de puertos del objetivo de evaluación, interactuando con Nmap desde la consola de comandos de Samurai Web Testing Framework.

La instrucción utilizada en la consola es: sudo nmap –n –Pn –O dirección web, o a su vez se puede colocar la dirección IP del objetivo de evaluación. En la instrucción se hace la petición de escaneo de puertos, con la opción –n indica no realizar consultas al DNS para saber cuál es el nombre de dominio asociado a la dirección ip, con -Pn no realizar procedimientos para comprobar si el sistema operativo está o no en funcionamiento, mientras que la opción –O indica realizar un escaneo para identificar el sistema operativo.

Figura 40: Escaneo de puertos y sistema operativo con NMap.

Fuente: consola de comandos de Samurai Web Testing Framework herramienta nmap

En la Figura anterior, se evidencian los puertos abiertos, así también en la respuesta OS CPE, se visualiza la familia del sistema operativo y kernel del mismo.

5.1.3.2.2. Escaneo de versiones.

Adicionalmente al escaneo de puertos, se puede efectuar un escaneo más detallado, en el que se visualizaría de forma más detallada el servicio que atiende en determinado puerto.

Para escanear las versiones del sistema operativo se emplea la instrucción:

sudo nmap –n –Pn –sV –O dirección web, en donde –sV hace referencia a la petición.

Figura 41: Escaneo de versiones con Nmap.

Fuente: consola de comandos de Samurai Web Testing Framework herramienta nmap

Como respuesta al escaneo de versiones, se muestra en la columna VERSION, la información correspondiente.

5.1.3.2.3. Escaneo de versiones desde fuentes externas (Netcraft).

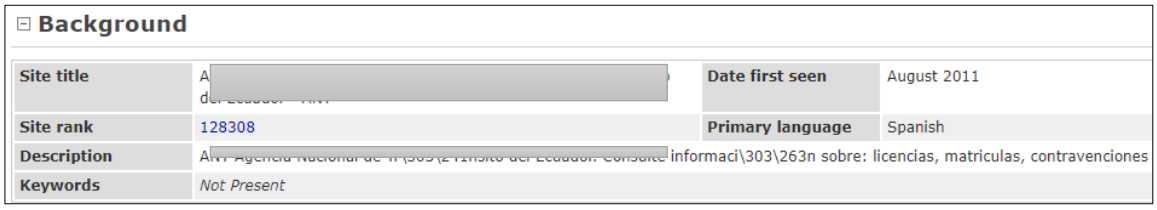
Para escanear versiones desde una fuente externa y en modo visual se puede emplear Netcraft, el cual permite conocer el software en funcionamiento en un sitio web evaluado. La dirección para su acceso es www.netcraft.com, e ingresar el dominio en el sitio que indica: averigüe qué tecnologías están potenciando cualquier sitio web, para el caso del objetivo de evaluación.

Figura 42: Búsqueda de las tecnologías en Netcraft.

Fuente: página web de Netcraft

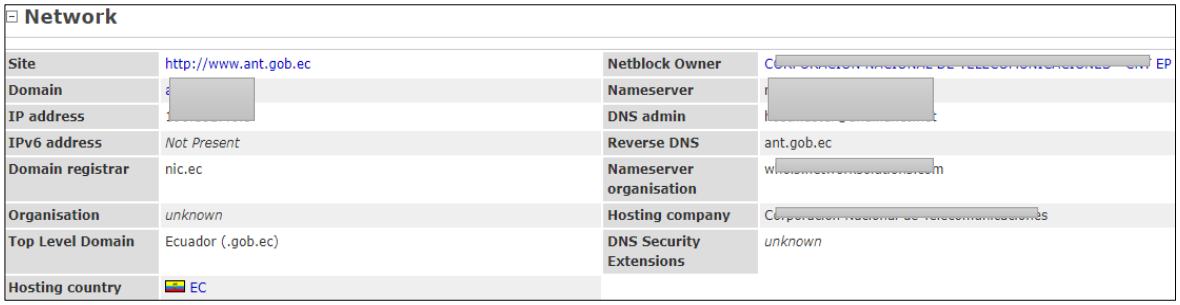
Para obtener mayor información del sitio, se debe dar clic en la columna Site Report, obteniéndose información como: la dirección IP, información del DNS, la compañía la cual proporciona los servicios de acceso, un historial de cómo ha evolucionado a través del tiempo, direcciones IP asignadas al dominio evaluado, el sistema operativo sobre los cuales funcionaba y funciona por fechas, entre otra información que puede ser importante para el proceso.

Figura 43: Información de fondo del objetivo de evaluación.



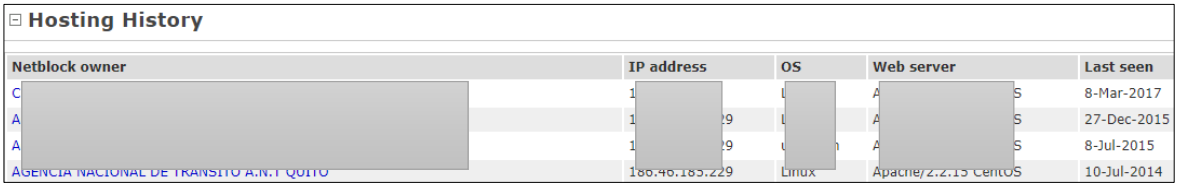
Fuente: página web de NETCRAFT

Figura 44: Información de IP, DNS, compañía prestadora de servicio de acceso para la entidad objetivo de evaluación.



Fuente: página web de NETCRAFT

Figura 45: Información del historial, IP y sistema operativo utilizado en el tiempo por la entidad evaluada.

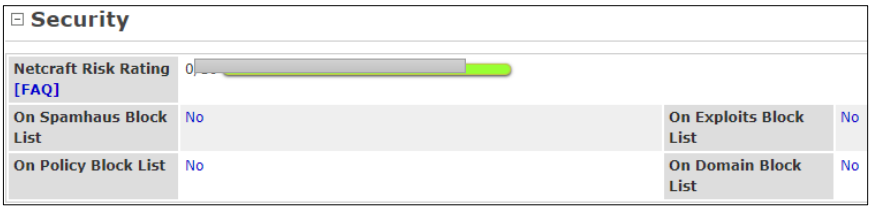


Hosting History

Netblock owner	IP address	OS	Web server	Last seen
C	1	L	A S	8-Mar-2017
A	1 :9	L	A S	27-Dec-2015
A	1 :9	u n	A S	8-Jul-2015
AGENCIA NACIONAL DE TRANSITO A.N.T QUITO	186.46.185.229	Linux	Apache/2.2.15 CentOS	10-Jul-2014

Fuente: página web de NETCRAFT

Figura 46: Clasificación de riesgos según Netcraft para el sitio evaluado.



Security

Netcraft Risk Rating [FAQ]	0		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

Fuente: página web de NETCRAFT

La clasificación de riesgo que indica la extensión de Netcraft, ofrece un nivel de protección adicional hacia sitios nuevos que aún no constan en la base de datos de Netcraft. Una calificación de riesgo menor es mejor, ya que asocia menor riesgo.

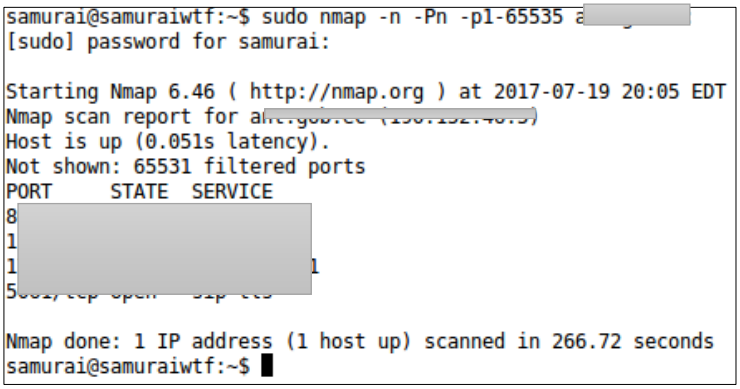
Para garantizar que el tráfico cifrado previamente grabado, no sea descifrado con facilidad, es pertinente configurar la propiedad PFS (Perfect Forward Secrecy), de una conexión SSL (Secure Sockets Layer).

5.1.3.2.4. Escaneo de puertos con Nmap.

Para escanear los 65535 puertos posibles del Protocolo de Control de transmisión (TCP), se emplea Nmap, la cual es una herramienta para exploración de redes y auditoría de seguridad de código abierto, por medio de la consola de comandos se emplea la siguiente instrucción:

```
sudo nmap –n –Pn –p1-65535 dominio
```

Figura 47: Escaneo de los 65535 puertos posibles del objetivo de evaluación mediante nmap.



Fuente: consola de comandos de Samurai Web Testing Framework herramienta nmap

Posterior al escaneo de puertos, se determina lo siguiente:

Se encuentra abierto el puerto 80 sobre el cual funciona el servicio http, lo cual es

Espacio oculto para proteger datos evidenciados.

aplicaciones encriptada, mediante sip, siendo similar al puerto HTTP.

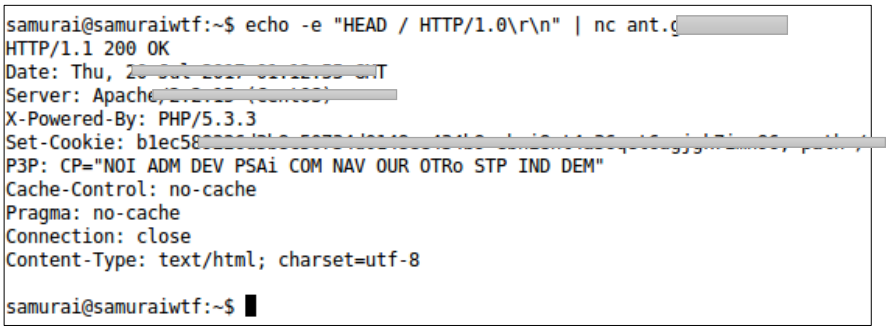
5.1.3.2.5. Obteniendo más información del servidor web con NETCAT.

Adicionalmente para obtener más información del servidor web, se puede emplear la herramienta Netcat, siendo una herramienta que establece conexión con el servidor en modo escucha para obtener la información de los mismos e inclusive forzando a su apertura, la instrucción usada es:

echo –e “HEAD / HTTP/1.0\r\n” | dominio 80

*(80 puerto HTTP)

Figura 48: Información de la versión del servidor objetivo de evaluación con NETCAT.



Fuente: consola de comandos de Samurai Web Testing Framework herramienta netcat

De la acción se muestra el tipo, la versión, y el tipo de contenido del servidor web.

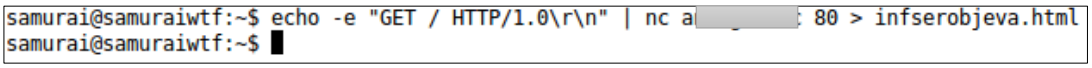
5.1.3.2.6. Obteniendo información de respuesta del contenido de la cabecera y cuerpo de la página web objetivo de evaluación.

Para obtener información de respuesta del contenido de la cabecera y cuerpo de la página web, se guarda la instrucción realizada en Netcat en un archivo html, para posteriormente abrirlo y analizarlo. La instrucción usada para guardar el archivo es:

echo –e “GET / HTTP/1.0\r\n” | dominio 80 > infserobjeva.html

Con GET obtiene información tanto de la cabecera, como del cuerpo de la página web evaluada.

Figura 49: Guardando la respuesta de cabecera y cuerpo de la página web del objetivo de evaluación con NETCAT.



Fuente: consola de comandos de Samurai Web Testing Framework herramienta netcat

Una vez guardado el archivo que para el caso es infserobjeva.html, se puede analizar el contenido tanto de la cabecera como del cuerpo de la página, en donde se puede encontrar información de etiquetas, y estructura de la página, lo cual se define como capturar de forma manual la información del servidor web usando Netcat, proceso el cual se puede ver con más detalle en el archivo referido en el Apéndice D.

Figura 50: Apertura del archivo guardado, conteniendo información de la cabecera y cuerpo de la página web objetivo de evaluación.

```
HTTP/1.1 200 OK
Date: [redacted]
Server: [redacted]
X-Powered-By: [redacted]
Set-Cookie: [redacted]
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="es-es" lang="es-es" >
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8" />  <meta
description+xml" />  <link rel="stylesheet" href="/plugins/content/phocadownlo
{color:#ffffff;}UL#aext59700f29438d3 LI A:hover,UL#aext59700f29438d3 LI A:focu
js" type="text/javascript"></script>  <script type="text/javascript">window.ad
```

Fuente: archivo guardado con la respuesta de la cabecera y cuerpo de la página web con la herramienta netcat

5.1.3.2.7. Consultando directorios y subdirectorios no deseados para su visualización.

Mediante la ejecución de un NSC (nmap scrpt engine), el cual es un motor de scripting para Nmap, permite consultar por ejemplo al archivo (robots), pudiendo hacer un mapeo de los directorios y subdirectorios no deseados que sean indexados por los buscadores. La instrucción usada es:

sudo nmap –n –Pn –p80 –script http-robots.txt dominio

Figura 51: Consulta de directorios y subdirectorios sensibles a ser indexados por los buscadores.

```
samurai@samuraiwtf:~$ sudo nmap -n -Pn -p80 --script http-robots.txt a[redacted]
[sudo] password for samurai:

Starting Nmap 6.46 ( http://nmap.org ) at 2017-07-19 23:14 EDT
Nmap scan report for a[redacted])
Host is up (0.036s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-robots.txt: 16 disallowed entries (15 shown)
| /[redacted]
| /[redacted]
|_/[redacted]

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
samurai@samuraiwtf:~$
```

Fuente: consola de comandos de Samurai Web Testing Framework herramienta nmap

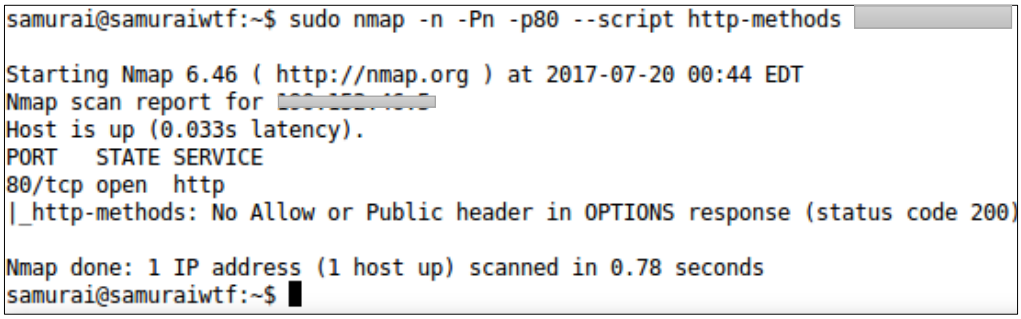
Gracias a éste procedimiento, se ha evidenciado directorios y subdirectorios, sensibles a ser indexados por cualquier buscador en un número de dieciséis entradas no permitidas.

5.1.3.2.8. Conociendo la existencia de métodos riesgosos existentes en el servidor web.

Mediante la ejecución del script methods, se puede evidenciar los métodos soportados por el servidor web objetivo de evaluación y los riesgosos. Mediante la instrucción:

sudo nmap -n -Pn -p80 --script http-methods dominio

Figura 52: Comprobación de métodos riesgosos en el servidor evaluado.



Fuente: consola de comandos de Samurai Web Testing Framework, comando Nmap.

Se ha observado que no existen permisos para visualizar públicamente la respuesta OPTIONS. Además, indica código de estado 200, el cual representa a una respuesta estándar para peticiones correctas, por lo que no existen métodos riesgosos visualizados.

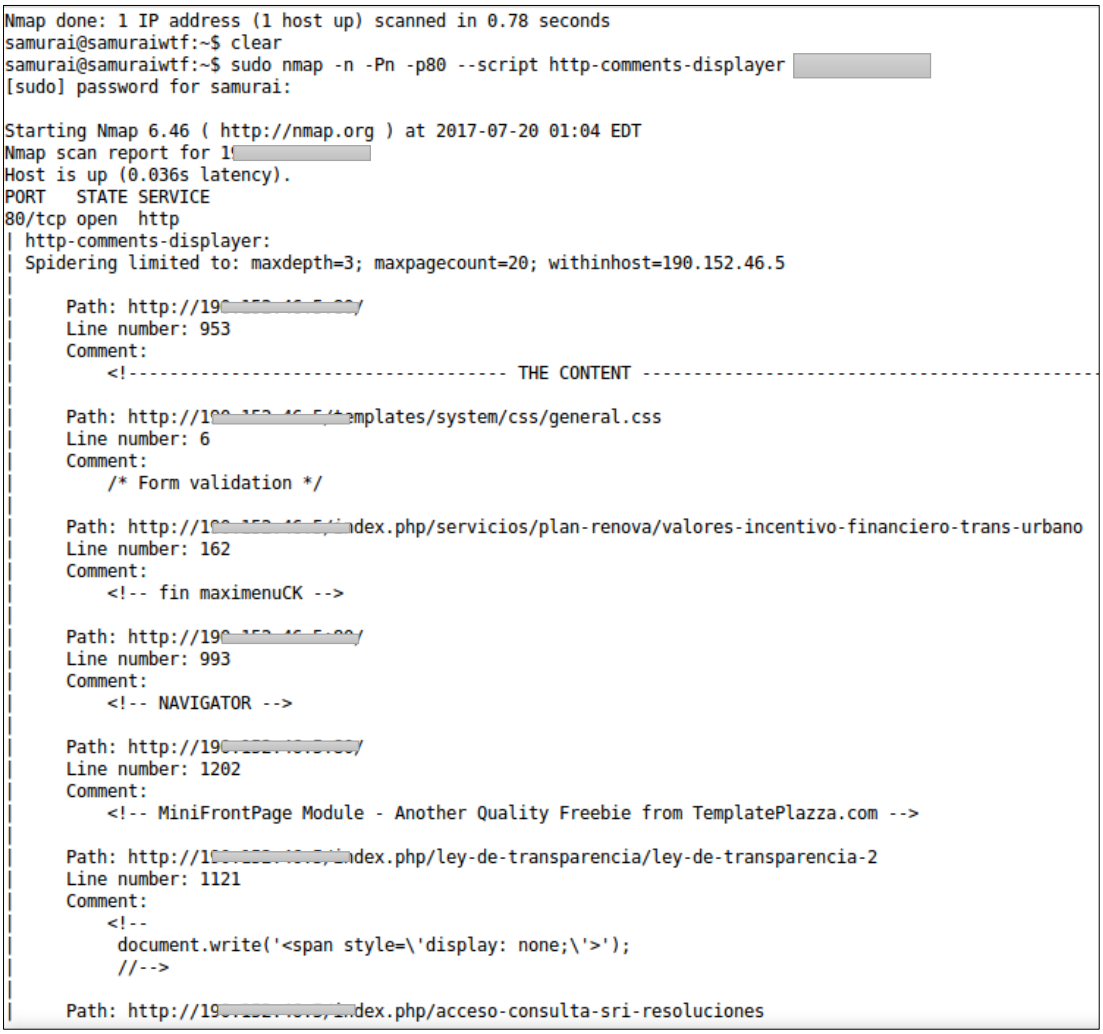
5.1.3.2.9. Identificando la existencia de comentarios dentro del aplicativo web.

Mediante la ejecución del script comments, se puede identificar los comentarios existentes dentro de la respuesta emitida por el objetivo de evaluación, se emplea la herramienta Nmap, mediante la instrucción:

sudo nmap -n -Pn -p80 --script http-comments-displayer dominio

El resultado de forma completa se lo muestra en el informe que se entregará a la entidad objetivo de evaluación, adjunto en el Apéndice E.

Figura 53: Identificando comentarios dentro de la respuesta del objetivo de evaluación.



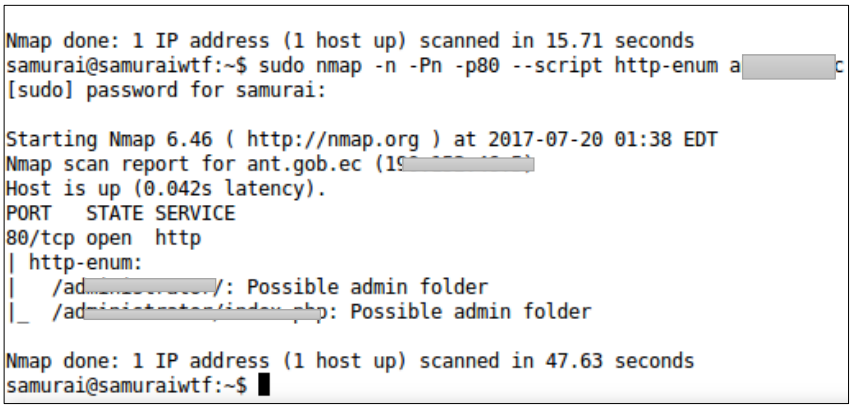
Fuente: consola de comandos de Samurai Web Testing Framework, comando Nmap.

5.1.3.2.10. Buscando directorios, dentro de la respuesta emitida por el servidor.

En cuanto a la búsqueda de directorios dentro de la respuesta emitida por el objetivo de evaluación, se emplea la herramienta Nmap, mediante la instrucción:

sudo nmap -n -Pn -p80 --script http-enum dominio

Figura 54: Búsqueda de directorios dentro de la respuesta del objetivo de evaluación con NMAP.



Fuente: consola de comandos de Samurai Web Testing Framework, comendo nmap.

Se determina la visualización de potenciales directorios de interés para ser vulnerados posteriormente.

Como ayuda o referencia técnica sobre los scripts, que se pueden ejecutar hacia el objetivo de evaluación es menester referirse a la página web de Nmap: https://nmap.org/nsedoc/index.html

Figura 55: Referencia técnica sobre scripts en Nmap.

Guiones	
acarsd-info	Recupera información de un demonio de escucha acarsd. Acarsd decodifica ACARS (Aircraft Communication Direccionamiento y Reporting System) de datos en tiempo real. La información recuperada por este script incluye la versión del demonio, versión de la API, administrador de la dirección de correo electrónico y la frecuencia de escucha.
Dirección-info	Muestra información adicional acerca de las direcciones IPv6, como las direcciones MAC o IPv4 embebidas cuando esté disponible.
AFP-bruta	Realiza adivinar la contraseña contra el protocolo de archivos de Apple (AFP).
AFP-ls	Los intentos de obtener información útil acerca de los archivos de volúmenes AFP. La salida está destinada a asemejarse a la salida de `ls` .
AFP-path-VULN	Detecta la vulnerabilidad de recorrido de directorio Mac OS X AFP, CVE-2010-0533.
AFP-info_servidor	Muestra información del servidor AFP. Esta información incluye el nombre del servidor, las direcciones IPv4 e IPv6, y el tipo de hardware (por ejemplo `MacMini` o `MacBookPro`).
AFP-showmount	Muestra acciones de AFP y ACL.
AJP-auth	Recupera el esquema de autenticación y el reino de un servicio de AJP (Protocolo JServ Apache) que requiere autenticación.
AJP-bruta	Realiza bruta auditoría contraseñas de fuerza contra el protocolo de Apache JServ. El Protocolo JServ Apache es comúnmente utilizado por los servidores web para comunicarse con los contenedores de servidor de aplicaciones Java de back-end.
AJP-headers	Realiza una cabeza o petición GET contra el directorio raíz o cualquier directorio opcional de un servidor de Protocolo de JServ Apache y devuelve las cabeceras de respuesta del servidor.
AJP-methods	Descubre qué opciones están soportadas por el servidor AJP (Apache Protocolo JServ) mediante el envío de una solicitud y listas de opciones potencialmente métodos riesgosos.
AJP-petición	Pide un URI sobre el Protocolo JServ Apache y muestra el resultado (o lo almacena en un archivo). Diferentes métodos de AJP, tales como; GET, HEAD, TRACE, PUT o DELETE se pueden utilizar.
allseeingeye-info	Detecta el servicio de ojo que todo lo ve. Proporcionada por algunos servidores de juegos para consultar el estado del servidor.

Fuente: página web de Nmap

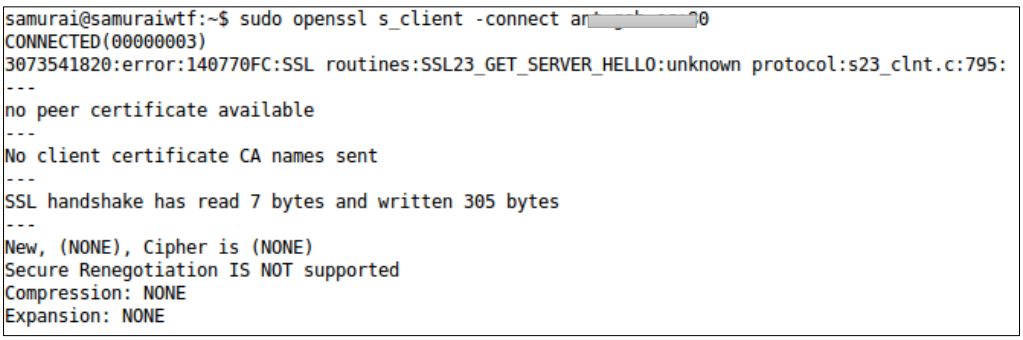
5.1.3.2.11. Evaluando SSL.

Para evaluar la disponibilidad de (SSL) Secure Sockets Layer, siendo un protocolo criptográfico que permite implementar seguridad en la comunicación sobre internet, brindando confidencialidad en el envío y recepción de mensajes y

datos, garantizando integridad y autenticación, constituye una herramienta útil para implementar seguridad, para ello se emplea la herramienta openssl, la cual simula ser un cliente al conectarse desde un navegador con la opción s_client. Para la obtención de información se escribe la instrucción:

sudo openssl s_client -connect dominio:80 (puerto http)

Figura 56: Evaluando SSL en el objetivo.



Fuente: consola de comandos de Samurai Web Testing Framework, comando openssl.

Del procedimiento, se visualiza que no existen disponibles certificados SSL, por lo que es importante considerar la implementación de los mismos.

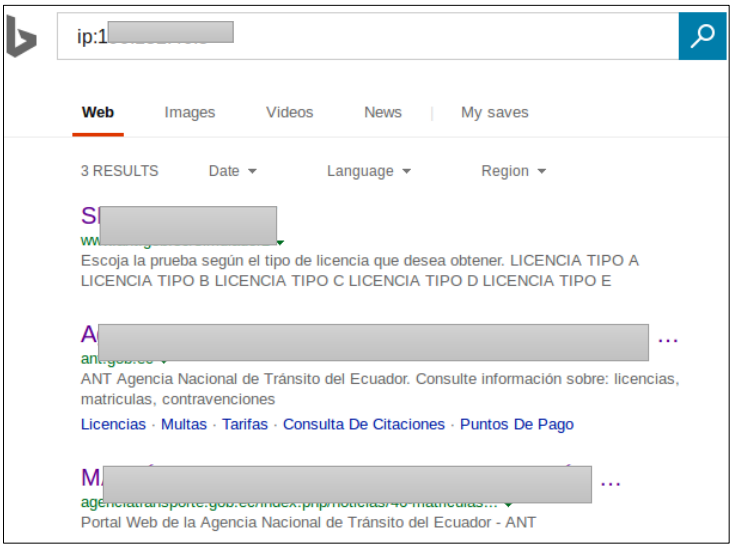
5.1.3.2.12. Evaluando estructuras intermedias (Servidores virtuales).

Aspecto muy importante a evaluar en ésta fase, es la existencia de infraestructura intermedia, la cual está por delante de la aplicación web y puede influir en las pruebas, entre ellos pueden estar los servidores virtuales, balanceadores de carga, proxies, y firewall de aplicación.

Para evaluar la existencia de servidores virtuales o compartidos, que constituyen una gran cantidad de servidores funcionando en diferentes direcciones IP, puede señalar la existencia de una sola máquina con varias direcciones IP virtuales o un hosting compartido. Para la evaluación de éste aspecto se puede emplear el buscador Bing de Microsoft con la directiva IP, en el cual se coloca la siguiente instrucción en la barra de búsqueda:

IP: (Dirección IP del objetivo de evaluación).

Figura 57: Evaluando la existencia de servidores compartidos.

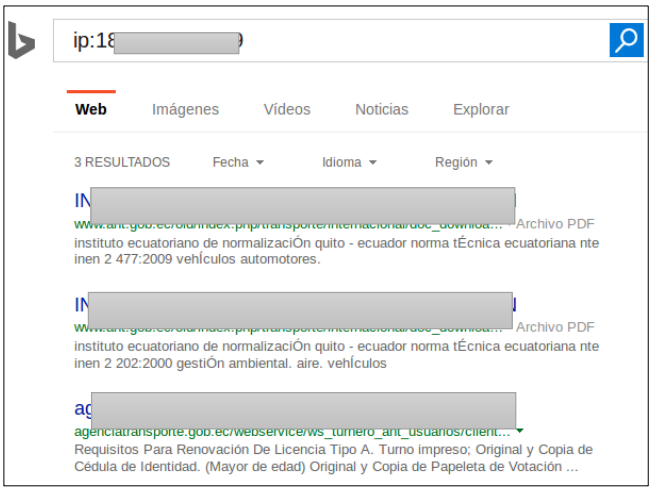


Fuente: buscador bing

De la evaluación se desprende, la existencia de tres dominios con sus aplicaciones, los que comparten la dirección IP del objetivo de evaluación.

Aspecto a considerar, es que, en una evaluación en meses posteriores, se determinó inclusive la existencia de aplicativos de una entidad pública ajena a la entidad evaluada.

Figura 58: Evaluación la existencia de servidores compartidos (meses anteriores).



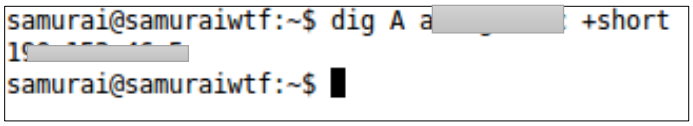
Fuente: buscador bing

5.1.3.2.13. Evaluando estructuras intermedias (Balanceadores de carga).

Para analizar los balanceadores de carga, considerados elementos tanto de hardware como de software, los cuales permiten se reparta la carga de peticiones entre diferentes servidores web. Para éste proceso se emplea el comando dig, seguido de la letra A que indica la consulta por el registro, dominio +short, obteniendo la instrucción:

dig A dominio +short

Figura 59: Búsqueda de balanceadores de carga en el objetivo de evaluación.



Fuente: consola de comandos de Samurai Web Testing Framework, comando dig.

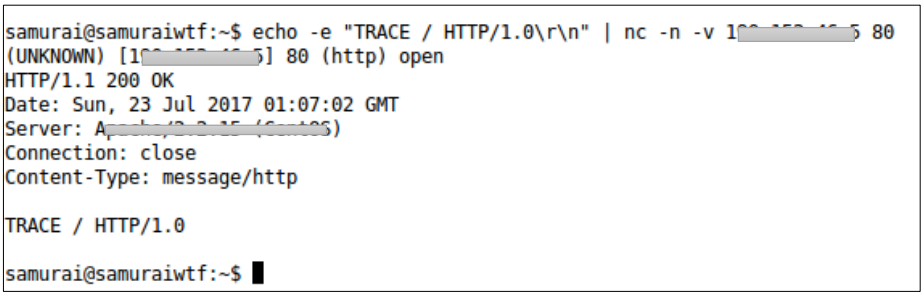
Como resultado de la búsqueda, se determina la inexistencia de balanceadores de carga en el objetivo de evaluación.

5.1.3.2.14. Evaluando estructuras intermedias (Proxies).

Para evaluar la existencia de un proxy, se emplea la herramienta Netcat, con el comando echo -e, el cual permite la escritura de un parámetro como respuesta ante una petición, que para el caso es TRACE, seguido del recurso http, y la dirección IP del objetivo de evaluación, añadiendo al final el puerto HTTP.

echo -e "TRACE / HTTP/1.0\r\n" | nc -n -v (ip del objetivo) 80 (puerto http).

Figura 60: Evidenciando la existencia de proxies en el objetivo de evaluación.



Fuente: consola de comandos de Samurai Web Testing Framework, comando echo con Netcat.

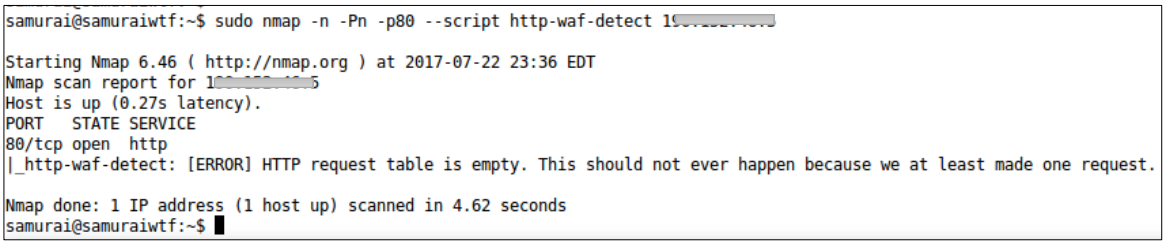
En éste procedimiento, se ha identificado la existencia de un servidor proxie, con la versión y el tipo.

5.1.3.2.15. Evaluando estructuras intermedias (Firewall de aplicación).

Para identificar la existencia de un firewall a nivel de aplicación, el cual la proteja, se emplea la herramienta Nmap, con el comando sudo nmap -n -Pn -p80, y utilizando el --script http-waf-detect (IP objetivo de evaluación), quedando la instrucción:

sudo nmap –n –Pn –p80 –script http-waf-detect IP

Figura 61: Detectando Firewall a nivel de aplicación en el objetivo de evaluación.



Fuente: consola de comandos de Samurai Web Testing Framework, herramienta nmap, y script http-waf-detect.

Del procedimiento efectuado, r en el objetivo de evaluación.

5.1.3.2.16. Escaneo de la configuración del software con Nikto2.

Posteriormente es necesario conocer el software y la configuración, ya que será determinante al momento de efectuar un ataque al objetivo de evaluación. Aquí se evidenciarán los métodos de petición soportados por el objetivo, a más de los comunes GET y HEAD, como los métodos OPTIONS, el cual muestra los métodos soportados, el método TRACE, el cual muestra las peticiones como si fuesen receptadas por el servidor, el método CONECT, el cual crea un túnel TCP mediante un servidor proxy, lo cual conducirá ya a evidenciar vulnerabilidades.

Para éste proceso se emplea la herramienta llamada Nikto2, la cual es un escaner Open Sorce, misma que permite efectuar pruebas muy completas hacia servidores web, incluyendo más de 6700 archivos CGI (Common Gateway Interface) peligrosos, los cuales en la práctica deben proveer interactividad a las páginas web, se puede verificar versiones no actualizadas de aproximadamente 1250 tipos de servidores, problemas específicos en al menos 270 servidores,

verifica problemas de configuración como la existencia de archivos índice, opciones HTTP del servidor, e identificar los servidores web y software instalado, sus plugins con actualizados con frecuencia y pueden ser instalados automáticamente. Al realizar las pruebas contra el servidor web, deja rastros en los archivos de registro del objetivo de evaluación.

La herramienta empleada es NIKTO, hacia el host y la IP del objetivo de evaluación, establecido en la siguiente instrucción:

nikto –host (IP objetivo)

Figura 62: Escaneo de la configuración del software con Nikto.

Fuente: consola de comandos de Samurai Web Testing Framework, herramienta Nikto.

Del procedimiento efectuado, se obtiene como resultado, el evidenciar datos del servidor como la versión, detección de algunos directorios, obtención de la versión del PHP, inclusive en el resultado del escaneo ya se evidencian algunas posibles vulnerabilidades hacia el aplicativo como indica en el encabezado X-Frame-Options de anti-clickjacking no está presente, mencionada cabecera, sirve para prevenir que la página pueda ser abierta en un frame, o iframe. De tal forma que se prevenga ataques de clickjacking, una forma de prevenir ante dichos ataques es configurando mediante tres posibles valores para el encabezado; el primero, mediante DENY, evitando que cualquier dominio enmarque el contenido, en segunda instancia, se recomienda SAMEORIGIN, que sólo permite que el sitio actual enmarque el contenido, y en tercera opción ALLOW-FROM uri , la cual permite que el "uri" (Uniform Resource Identifier, sirve para identificar recursos en Internet), especificado enmarque esta página.

Espacio oculto para protección de datos evidenciados.

Otra consideración a efectuarse es la indicación que el encabezado X-XSS-Protection no está definido. (Cross Site Scripting) es un tipo de agujero de se na in or el no o da cargarse o modificar propiedades del documento desde un "origen" diferente. La recomendación es agregar el fragmento apropiado al archivo de configuración, como para el caso de Apache es:

Espacio oculto para protección de datos evidenciados.

Header set X-XSS-Protection: 1; mode=block;

Otro aspecto a considerar es la descripción que indica que el encabezado X-Content-Type-Options no está establecido, lo cual hace que los navegadores que soportan esta cabecera (IE y chrome), no carguen las hojas de estilos, tampoco los scripts (Javascript), cuyo Mume type no sea el apropiado. Como sugerencia es añadir a la cabecera de los archivos functions,php, las siguientes líneas de código:

Espacio oculto para protección de datos evidenciados.

```
add_action( 'send_headers', 'add_header_xcontenttype' );
function add_header_xcontenttype() {
header( 'X-Content-Type-Options: nosniff' );
```

}

U otra forma es implementar la cabecera en un servidor web Apache, usando el fichero .htaccess, añadiendo el código:

Header set X-Content-Type-Options nosniff

Otra consideración es la que refiere a que el servidor pierde inodes vía ETags, cabecera encontrada con el archivo /robots.txt, el cual se encuentra en el directorio raíz de un sitio, e indica a qué partes se desea que accedan y a qué partes no se desea que accedan los buscadores. La sugerencia es implementar métodos de bloqueo, como proteger los archivos privados en el servidor mediante contraseñas.

Finalmente existe una consideración sobre la indicación que el método HTTP TRACE está activo, sugiriendo que el host es vulnerable a XST (Cross Site Tracing explota controles ActiveX, Flash, Java y otros que permiten la ejecución de una llamada HTTP TRACE). Como sugerencia es vital que los métodos PUT, DELETE, CONNECT y TRACE estén deshabilitados, y de ser requeridos por algunos servicios, se considere la verificación de uso se limitado y en condiciones seguras a usuarios confiables.

5.1.3.2.17. "Spidering" del sitio web objetivo de evaluación con Wget.

Luego de las actividades descritas, se establece la realización de un "spidering" o también conocido como "crawling", que es el proceso de rastrear o seguir todos los enlaces del sitio web y descargar cada página encontrada, obteniendo una copia local del sitio web completo, lo cual es muy útil para analizar el código fuente en busca de potenciales debilidades de seguridad, pudiendo también con la ayuda de otras herramientas crear listas de palabras claves o diccionarios en base al sitio descargado que pueden ser útiles para determinar contraseñas, información como direcciones de correo electrónico, nombres, números de teléfono, y cualquier dato útil para efectuar ataques de ingeniería social o de fuerza bruta.

Se puede efectuar dos tipos de "spidering", uno manual o dirigido, el cual es controlado por el usuario, siendo éste quien transita por todas las funcionalidades

de la aplicación web empleando un navegador común, el tráfico que se genera transita por una herramienta que combina un proxy de interceptación y un spider, obteniendo como resultado un mapa de la aplicación con todas los identificadores de recursos uniformes (URLs), por los que se haya navegado.

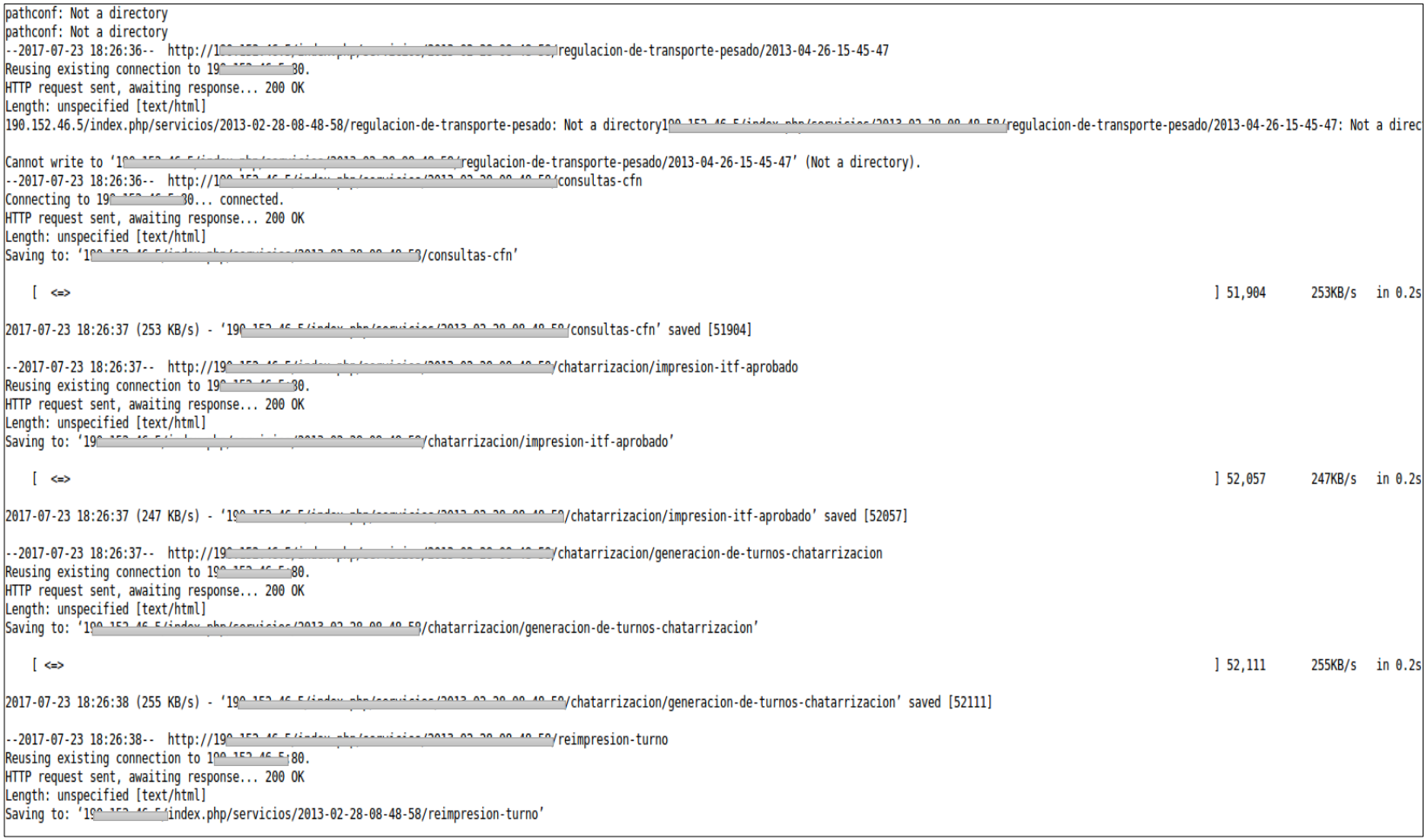
Por otro lado, existe el "spidering" automático, el cual solicita una página web e interpreta en búsqueda de enlaces y demás contenidos, actuando de forma recursiva hasta que no exista contenido nuevo que descubrir, de la misma manera, el resultado es la construcción de un mapa de la aplicación con todas las URLs obtenidas por la herramienta.

Como resultados de la realización del "spidering" se espera visualizar algunos cometarios, los cuales pueden incluir usuarios, contraseñas y algunos datos de la aplicación web, también se espera encontrar códigos o enlaces comentados los que pueden dirigir a páginas con privilegios, y el mismo código que puede ser analizado en búsqueda de debilidades en su implementación, además se puede tener acceso al archivo robots.txt el cual se utiliza para permitir a los administradores de un sitio web indicar el listado de directorios y páginas las cuales no deben ser capturadas ya que no se desean que no sean accedidos por los robots, siendo evidenciados para alguna tarea específica.

Para éste proceso se puede emplear herramientas como Wget, cuRL, CeWL, por lo que para el caso de análisis se emplea Wget, la cual es una herramienta libre que soporta descargas de sitios web mediante los protocolos HTTP, HTTPS y FTP. El procedimiento es ingresando a un directorio temporal, seguido colocar la instrucción con la opción –r para efectuar un procedimiento recursivo, seguido de la dirección IP objetivo de evaluación, disponiendo de la instrucción:

```
cd/tmp/
wget –r  (IP objetivo)
```

Figura 63: "Spidering" del sitio web objetivo de evaluación.

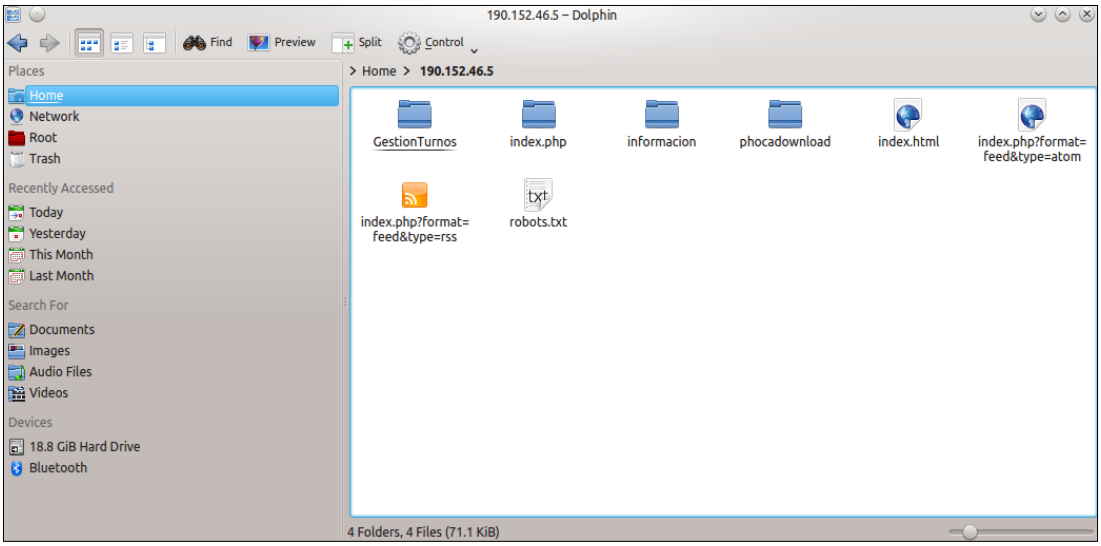


```
pathconf: Not a directory
pathconf: Not a directory
--2017-07-23 18:26:36--  http://1[redacted]regulacion-de-transporte-pesado/2013-04-26-15-45-47
Reusing existing connection to 19[redacted]30.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
190.152.46.5/index.php/servicios/2013-02-28-08-48-58/regulacion-de-transporte-pesado: Not a directory1[redacted]regulacion-de-transporte-pesado/2013-04-26-15-45-47: Not a direc

Cannot write to '1[redacted]regulacion-de-transporte-pesado/2013-04-26-15-45-47' (Not a directory).
--2017-07-23 18:26:36--  http://1[redacted]consultas-cfn
Connecting to 19[redacted]30... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: '1[redacted]/consultas-cfn'

    [  <=>                                                                                                                                  ] 51,904       253KB/s   in 0.2s

2017-07-23 18:26:37 (253 KB/s) - '19[redacted]/consultas-cfn' saved [51904]

--2017-07-23 18:26:37--  http://19[redacted]/chatarrizacion/impresion-itf-aprobado
Reusing existing connection to 19[redacted]30.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: '19[redacted]/chatarrizacion/impresion-itf-aprobado'

    [  <=>                                                                                                                                  ] 52,057       247KB/s   in 0.2s

2017-07-23 18:26:37 (247 KB/s) - '1[redacted]/chatarrizacion/impresion-itf-aprobado' saved [52057]

--2017-07-23 18:26:37--  http://19[redacted]/chatarrizacion/generacion-de-turnos-chatarrizacion
Reusing existing connection to 19[redacted]80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: '1[redacted]/chatarrizacion/generacion-de-turnos-chatarrizacion'

    [ <=>                                                                                                                                   ] 52,111       255KB/s   in 0.2s

2017-07-23 18:26:38 (255 KB/s) - '19[redacted]/chatarrizacion/generacion-de-turnos-chatarrizacion' saved [52111]

--2017-07-23 18:26:38--  http://19[redacted]/reimpresion-turno
Reusing existing connection to 1[redacted]80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: '1[redacted]index.php/servicios/2013-02-28-08-48-58/reimpresion-turno'
```

Fuente: consola de comandos de Samurai Web Testing Framework, herramienta Wget

El resultado del “spidering”, se puede evidenciar accediendo al directorio en donde fue guardado, disponiendo del archivo robots.txt, en donde se parametriza módulos o sitios a los que no se quiere que el “spider” acceda a la captura de información.

Figura 64: Visualizando el resultado del "Spidering" al objetivo de evaluación.



Fuente: explorador de archivos Dolphin de Samurai Web Testing Framework

5.1.3.3. Fase de Descubrimiento

En la fase de descubrimiento se da inicio a la exploración de forma más profunda en la aplicación web, encontrándose ya los resultados de posibles vulnerabilidades e información para la fase de explotación o ataque. Para el desarrollo de ésta fase se ha propuesto el empleo de herramientas como: Zed Attack Proxy (ZAP), la cual es una herramienta de código abierto, integrada en Samurai Web Testing Framework, y que es parte del proyecto OWASP, orientada específicamente a pruebas de penetración para encontrar vulnerabilidades en aplicaciones web.

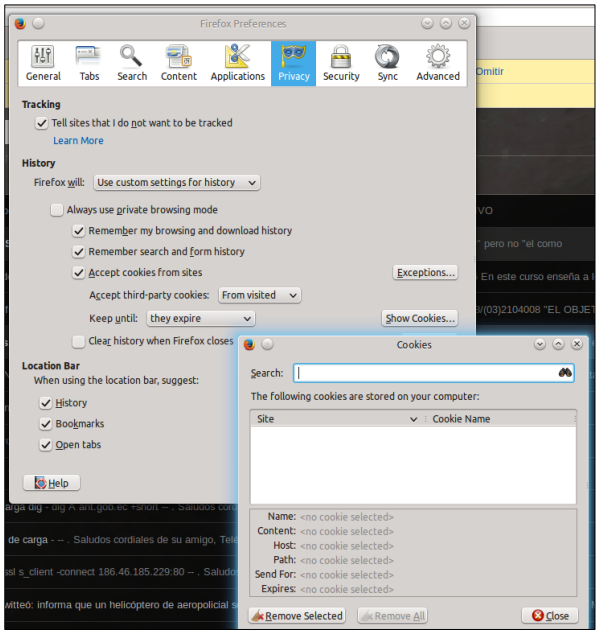
Para éste proceso primeramente se inicia ZAP, mediante la consola de comandos de Samurai Web Testing Framework (SWTF), con la instrucción: zap

Figura 65: Iniciando ZAP.

Fuente: consola de comandos de Samurai Web Testing Framework herramienta ZAP

Posteriormente se debe configurar el navegador web, eliminando el cache de datos y el historial de navegación.

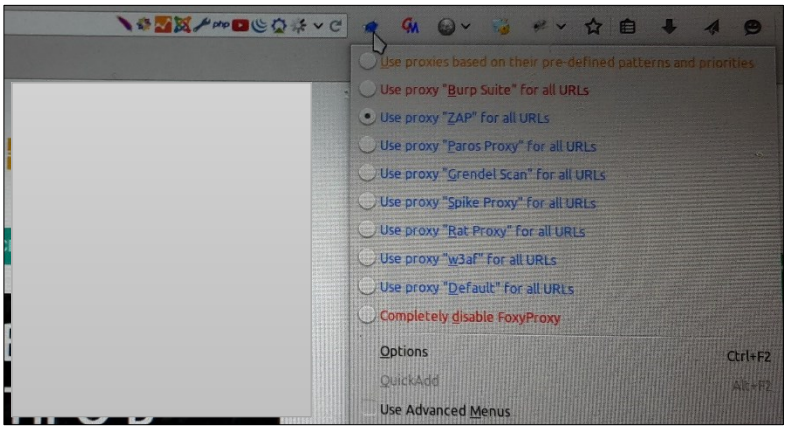
Figura 66: Eliminación de cache de datos e historial de navegación.



Fuente: navegador Mozilla Firefox en Samurai Web Testing Framework

Para paso seguido configurar el navegador para que utilice ZAP, como proxy de interceptación.

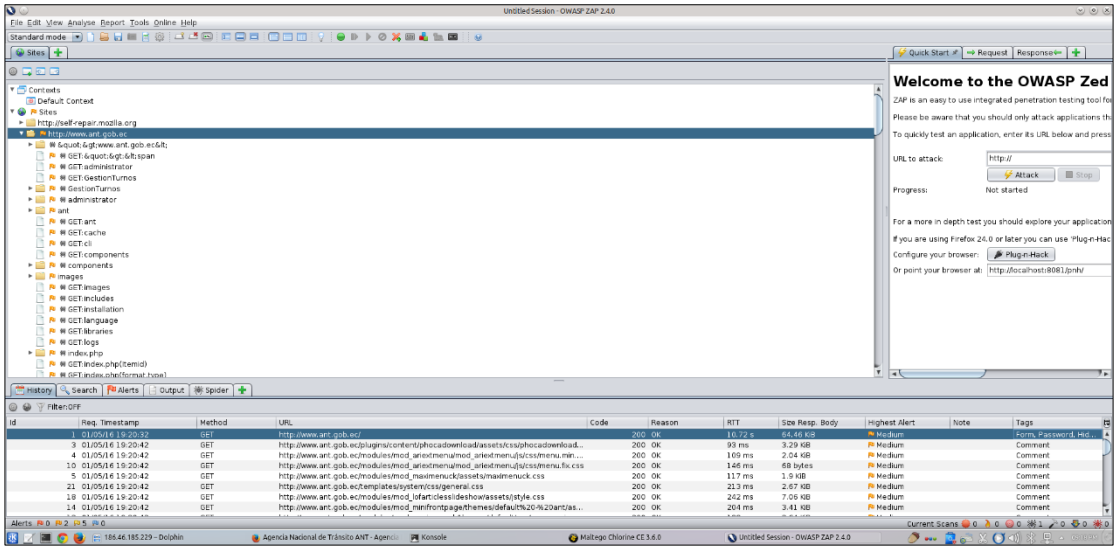
Figura 67: Configuración de ZAP en el navegador Mozilla Firefox.



Fuente: navegador Mozilla Firefox en Samurai Web Testing Framework

Finalmente se obtiene los resultados producto de la realización del "spidering" con ZAP, evidenciando en la columna TAGS de la herramienta recursos relacionados a comentarios, formularios, scripts, password, los que se hayan encontrado en el objetivo de evaluación.

Figura 68: "Spidering" del objetivo de evaluación.



Fuente: interfaz de la herramienta ZAP

En éste punto de la fase, es pertinente indicar que se han efectuado las solicitudes respectivas a la entidad objetivo de evaluación, para la aplicación de la fase de descubrimiento, por ya tratarse de un procedimiento de interacción directa con el aplicativo web evaluado, de la cual no se ha obtenido respuesta de ningún tipo, inclusive se ha presentado la propuesta del proyecto en la que se incluye el alcance, la aprobación del tema por parte de la Pontificia Universidad Católica del Ecuador sede

Ambato, así como una carta con el acuerdo de confidencialidad por parte del autor, así como la ruta de las peticiones efectuadas a través del Sistema de Gestión Documental Quipux, documentos que se adjuntan en el Anexo F, y razón por la cual, el presente proyecto cumple hasta ésta etapa con su cometido de abordar una estrategia para la detección de vulnerabilidades en un determinado objetivo de evaluación de una forma externa y con el empleo de herramientas pasivas, estando enmarcado dentro del alcance efectuado en la propuesta, indicando además que no se ejecuta la herramienta ZAP, hacia el aplicativo web de la entidad, por lo que no se presenta el informe de dicha actividad, ya que ello si conllevaría el uso de herramientas activas hacia el aplicativo , más se establece el proceso a ser desarrollado al memento de contar con la respectiva autorización.

5.1.3.4. Fase de Explotación

Finalmente se expone la fase de explotación, fase en la cual se unifica toda la información recolectada en cada fase anterior para efectuar los ataques al aplicativo web. Cabe indicar que ésta fase no se la contempla dentro del alcance del proyecto por estar al margen del concepto de hacking ético, pero se deja sentado las bases para una ejecución controlada de ésta fase y por tratarse de un proyecto el cual tiene por objetivo evidenciar una estrategia para detectar vulnerabilidades en el aplicativo web de la entidad objetivo de evaluación, más no contempla el efectuar o concretar el ataque.

Como herramientas útiles para aplicar en el proceso de explotación se puede emplear BeEF (Browser Exploitation Framework), la cual es una herramienta de pruebas de penetración, o también las herramientas AJAXShell o SQLBrute, con las cuales es factible realizar la intromisión al aplicativo web, siempre y cuando el alcance lo permita y lo más importante exista la respectiva autorización para su ejecución por parte de la entidad objetivo de evaluación.

5.1.4. Conclusiones

En la fase de reconocimiento se encontraron datos relacionados a la trayectoria laboral, experiencia, trayectoria académica formación, aptitudes y contactos del director del área de tecnologías de la entidad objetivo de evaluación, información que puede ser empleada para efectuar ataques de ingeniería social, así también se ha determinado la dirección IP, se han

encontrado los host asociados al DNS del objetivo, se ha obtenido información del dominio del objetivo evaluado, hallándose información de registrante, nombre de servidor DNS, contacto administrativo, contacto técnico, ubicación geográfica, se obtuvo información del directorio telefónico del personal de la entidad. Se detectó también información del servidor web y sistema operativo, finalmente se pudo recolectar de forma gráfica datos del objetivo de evaluación, obteniéndose información del dominio, direcciones de correo electrónico, host compartidos, direcciones IP del servidor web y de correo, se localizaron los servidores DNS, y los sitios asociados a los servidores DNS en donde reside el dominio del objetivo.

En la fase de mapeo, se ha evidenciarse el puerto, el estado y el servicio, así como el sistema operativo y la versión soportada. En el escaneo de versiones se obtuvieron datos como nombre del sitio, dominio, dirección IP, nombre del servidor, DNS del administrador, e inclusive un rango de riesgos catalogado por netcraft, además el historial del host, las direcciones IP, sistemas operativos y versiones soportadas en épocas anteriores. Se encontraron los puertos abiertos. Se han comprobado la implementación de métodos riesgosos en el servidor, así también se han localizado comentarios en el código del aplicativo, se determina la no existencia de protocolo criptográfico, se detectó la presencia de servidores compartidos, se determinó la presencia de equipo balanceador de carga, se evidencia un servidor proxy, no se determina la existencia de un firewall de aplicación, también se detectó deficiencia en configuraciones, se logró realizar un "spidering" del sitio web, y finalmente en la etapa de mapeo, se encontraron comentarios, formularios, y password de sesión.

En la fase de descubrimiento se han encontrado posibles vulnerabilidades.

En la fase de explotación se han abordado sobre las herramientas que pueden emplearse, más no se las ha aplicado por estar fuera del alcance de la propuesta y estar al margen del hacking ético.

5.1.5. Inclusión de documentos de respaldo, anexos, o explicación de criterio técnico

Como documentos de respaldo se remiten a los Anexos respectivos referidos en cada aspecto, además de los documentos de acercamiento y gestión para la consecución del permiso por parte de la entidad objetivo de evaluación para la aplicación de la estrategia, enfocada al aplicativo web de la misma.

5.1.6. Otros requisitos

No existe información adicional a ser considerada en el presente informe.

5.1.7. Información adicional

No existe información adicional a ser considerada en el presente informe.

5.1.8. Declaración juramentada

En calidad de Perito de la Función Judicial de Cotopaxi, yo Ing. Raúl Alfredo Panchi Herrera, declaro bajo juramento que el presente Informe Técnico Pericial, las actividades efectuadas, información, resultados obtenidos y planteados, así como las conclusiones emitidas, están enmarcados en la veracidad, independencia, ética y convicción profesional.

Es cuanto puedo informar para los fines pertinentes,

5.1.9. Firma y rúbrica

Atentamente,

Ing. Raúl Alfredo Panchi Herrera.

C.I.:0502521032

N° Calificación: 5000008

Ex Perito Informático

Ambato, agosto 2017.

5.2. Evaluación Preliminar

Con la finalidad de conocer el impacto del proyecto se procedió a realizar una encuesta dirigida al personal de TI de la ANT, conformado por el Director, cinco programadores, dos analistas, tres administradores de base de datos y un diseñador gráfico web. Seguidamente se presentan los resultados obtenidos.

ENCUESTA SOBRE PRUEBA DE PENETRACIÓN EN EL APLICATIVO WEB DE LA AGENCIA NACIONA DE TRÁNSITO

Estimados profesionales del área de tecnologías de la Agencia Nacional de Tránsito, toda vez que se ha entregado el documento que recoge los resultados de la aplicación del proyecto: "ESTRATEGIA PARA LA DETECCIÓN DE VULNERABILIDADES EN LA APLICACIÓN WEB DE LA AGENCIA NACIONAL DE TRÁNSITO COMO HERREMIENTA PARA LA TOMA DE DESICIONES", me permito aplicar éste instrumento evaluativo a fin de determinar su evaluación preliminar..

Considera que el proyecto desarrollado traerá beneficios desde el aspecto tecnológico para la institución?

Si ☐ No ☐ Desconozco ☐

Los reportes de vulnerabilidades encontradas son considerados importantes en una escala de valores:

Bajo ☐ Medio ☐ Alto ☐

Estima que con la ayuda de la solución y en base a los resultados obtenidos en la misma, se tomarán decisiones a un plazo:

Corto ☐ Mediano ☐ Largo ☐

Qué tipo de recursos considera se puede optimizar con la aplicación de la solución propuesta.

Tecnológicos ☐ Económicos ☐ Humanos ☐ Tiempo ☐

Contar con reportes de vulnerabilidades detectadas, será funcional para el proceso de desarrollo en un porcentaje de:

5% ☐ 25% ☐ 50% ☐ 75% ☐ 95% ☐ Otro ☐

Las herramientas descritas y utilizadas en el desarrollo del proyecto, considera que son:

Poco útiles. ☐ Medianamente útiles. ☐ Muy útiles ☐

El impacto que tendrá el proyecto realizado en la toma de decisiones por parte del personal de Tecnologías de la ANT será:

Irrelevante ☐ Poco importante ☐ Muy importante ☐

En base a los resultados de la prueba de penetración entregados, se considera que se tomaran acciones:

Correctivas ☐ Preventivas ☐

Qué valoración le daría de 0 a 5, donde 0 es nada y cinco muy fiable, los resultados del proyecto desarrollado.

0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

De la encuesta se determina que el proyecto de titulación efectuado tiene un impacto muy importante, ya que un 91,6% de encuestados afirma aquella definición, lo cual se refleja en que para el caso específico para la realización de pruebas de penetración y análisis de vulnerabilidades se ha requerido la subcontratación de empresas especializadas en el ramo para efectuar el requerimiento, y generalmente se lo hace toda vez que se ha detectado algún tipo de intrusión en el sistema.

Por parte del Director de TI a nivel nacional de la entidad evaluada, se ha mostrado interés en el resultado del proyecto, ya que indicó haber sido ya objeto de intrusiones en meses pasados, y el

documento entregado ayudará y dará una perspectiva externa y complementaria a un proceso de análisis desarrollado por una empresa que se contrató para la detección de vulnerabilidades.

En la encuesta participaron 12 personas relacionadas al área de TI de la entidad evaluada, de los cuales el 83.33 % indica que el reporte si traerá beneficios en la parte tecnológica, ya que se puede hacer comparativas con proyectos presentados por una empresa evaluadora de vulnerabilidades, evaluando los resultados a fin de determinar acciones específicas y oportunas.

Respecto a la importancia de las vulnerabilidades reportadas en el informe, existen dos criterios de valoración siendo el 75% de encuestados que indican un valor alto, mientras que el 25% un valor medio, de lo que se determina que el parámetro de importancia está por arriba del 75%.

En cuanto a la consideración del tiempo en el cual se tomará decisiones, en función de los resultados reportados, un 91.6% de encuestados indica que las acciones a tomarse deben ser o corto plazo, y un 8.4%, indica que se tomarán a mediano plazo, de lo que se evidencia que las acciones a tomar serán determinantes en función de los resultados emanados.

Sobre la optimización de recursos que arrojará el trabajo presentado, un 83,33% de encuestados indica que inferirá en el recurso tecnológico, mientras que un 16,7% menciona que los recursos económicos serán los optimizados, de los resultados se avizora que de forma específica el recurso que se fortalecerá es el tecnológico al disponer de una alerta sobre debilidades detectadas en su aplicación.

La funcionalidad que dará el proyecto en la fase de desarrollo, indican en un 66,66%, indican que será de un 75%, mientras que un 16,66% se inclina por un 50%, y finalmente un 16,66% de encuestados se menciona por un 25%, de lo cual se infiere que en definitiva si es pertinente y será de referencia el resultado del trabajo para la fase de desarrollo de nuevas aplicaciones y funcionalidades.

En referencia a las herramientas que se han utilizado y con las cuales se han determinado los resultados, un 75% de encuestados se inclina por el criterio que son muy útiles, versus un 25% que indican ser medianamente útiles, lo cual confirma que las herramientas propuestas y empleadas están dentro de las adecuadas para el proceso.

En cuanto a las medidas a tomar en relación al aplicativo web, un 83,33% indica que deben ser de carácter preventivo, y un 16,67% indica que las medidas a tomar deben ser correctivas.

Finalmente, respecto a los resultados plasmados en el informe, consideran que la fiabilidad de los resultados es en la escala de 5 o muy fiable se inclina por un 33,33%, en tanto que por la escala de 4 se manifiesta un 50%, y por una valoración de 3 se apega un 16,66%, lo que indica que la credibilidad en los resultados plasmados está por encima del 83,33%.

5.3. Análisis de resultados

El objetivo principal del presente proyecto era el de desarrollar una estrategia para la detección de vulnerabilidades en la aplicación web de la Agencia Nacional de Tránsito, utilizando técnicas, conocimientos, metodología y herramientas las cuales son usadas por parte de Hackers para evidenciar debilidades en los aplicativos web con la finalidad de alertar a sus encargados y tomar acciones preventivas, y así miso usadas también por Crackers, quienes persiguen interés económicos o destructivos en su accionar.

En el proceso mismo han convergido todas las actividades referidas, y se ha evidenciado información de diferente índole a medida que se ha ido adentrando en la ejecución de cada una de las fases establecidas como fueron reconocimiento, mapeo, descubrimiento y explotación, las cuales se describió en la metodología y un poco más específica en el desarrollo mismo de la propuesta.

Inicialmente dentro de la fase de reconocimiento se empleó el buscador Google Groups y Google Site, así como redes sociales y profesionales como Facebook y LinkedIn, con las que se encontraron datos relacionados a la trayectoria laboral, experiencia, trayectoria académica formación, aptitudes y contactos, para el caso del director del área de tecnologías de la entidad objetivo de evaluación, información que puede ser empleada para efectuar ataques de ingeniería social.

Ya adentrados en el uso de herramientas se ha determinado la dirección IP del objetivo de evaluación, con el uso de nslookup, así como se han encontrado los hosts asociados al DNS del objetivo mediante la herramienta dig. Adicionalmente se ha empleado el recurso Whois tanto de las páginas de ARIN, IANA, NIC.EC, para obtener información del dominio del objetivo evaluado, hallándose información de registrante, nombre de servidor DNS, contacto administrativo, contacto técnico, ubicación geográfica, entre otros datos.

Mediante Google Site, se obtuvo información del directorio telefónico del personal de la entidad evaluada.

Para la detección de información del servidor web y sistema operativo, se recurrió a la página de Netcraft, obteniendo los resultados requeridos.

Finalmente, dentro de la fase de reconocimiento, se usó la herramienta Maltego para recolectar de forma gráfica datos del objetivo de evaluación, obteniéndose información del dominio, direcciones de correo electrónico, host compartidos, direcciones IP del servidor web y de correo, se localizaron los servidores DNS, y los sitios asociados a los servidores DNS en donde reside el dominio del objetivo.

Para el cumplimiento de la fase de mapeo, se ha recurrido a nmap, para escanear los puertos y el sistema operativo, pudiendo evidenciarse el puerto, el estado y el servicio, así como el sistema operativo y la versión soportada.

Para el escaneo de versiones de forma visual, se empleó la interfaz de netcraft, en donde se obtuvieron datos como nombre del sitio, dominio, dirección IP, nombre del servidor, DNS del administrador, e inclusive un rango de riesgos catalogado por netcraft, además el historial del host, las direcciones IP, sistemas operativos y versiones soportadas en épocas anteriores.

Se ha confirmado los puertos abiertos con nmap, con un rango de búsqueda desde el puerto 1 hasta el 65535 encontrándose resultados limitados.

Con netcat se ha verificado la versión del servidor web. En cuanto a interacción con el servidor se ha guardado respuestas tanto de cabecera y cuerpo de la página web.

Se han comprobado la implementación de métodos riesgosos en el servidor con nmap, no existiendo información al respecto.

Se han localizado comentarios en el código del aplicativo, pesto con nmap, así como con la misma herramienta se localiza directorios.

Se determina la no existencia de Secure Socket Layer o protocolo criptográfico, con la intervención de la herramenta openssl.

Se detectó la presencia de servidores compartidos mediante el buscador bing, se determinó la presencia de equipo balanceador de carga, con la ayuda del comando dig.

Se evidencia un servidor proxy mediante netcat.

No se determina la existencia de un firewall de aplicación, con la herramienta nmap.

Mientras que con Nikto se detectó deficiencia en configuraciones.

Se logró realizar un "spidering" del sitio web, con la herramienta wget.

Finalmente, en la etapa de mapeo, se recurrió a Zed Attack Proxy, con lo que se encontraron comentarios, formularios, y password de sesión intersectados por la herramienta actuando como proxy de interceptación.

En lo que respecta a la fase de descubrimiento se han encontrado posibles vulnerabilidades, esto con la intervención de la herramienta Zed Attack Proxy (ZAP) y w3af.

Sobre la última fase de explotación no se la establece información, ya que el alcance del proyecto no es explotar o atacar el objetico de evaluación, por ser actividades fuera del marco legal y ético de la detección de vulnerabilidades.

Capítulo 6

Conclusiones y recomendaciones

6.1. Conclusiones

- Se fundamentó teóricamente y metodológicamente sobre vulnerabilidades en aplicaciones web, mediante referencias metodológicas de los diferentes proyectos existentes para la realización de pruebas de penetración en aplicativos web como son la metodología Open Source Security Testing Metohodology (OSSTMM), por otra parte la metodología Information System Security Assessment Framework (ISSAF) y una tercera metodología Open Web Application Security Project (OWASP), de la cual se han tomado las herramientas para la implementación del producto de titulación.

- De manera técnica se desarrolló la estrategia, con la intervención de herramientas, que permitieron establecer las bases desde el ámbito académico, para ser producto de implementación en el ámbito laboral, de procedimientos para detectar potenciales vulnerabilidades en aplicativos web.

- Durante el desarrollo de la propuesta se emplearon técnicas, metodología y herramientas para efectuar un proceso de búsqueda, tal es el caso que como técnica se definió black box hackin, con una perspectiva externa a la entidad, en cuanto a la metodología de pruebas de penetración apunto a OWASP, efectuando procesos dentro para el caso de cada fase abarcando desde el reconocimiento, el mapeo, el descubrimiento, y la explotación, claro está que se exceptúa la última fase por haberse definido en el alcance la no realización de ésta fase y más aún al tratarse de una perspectiva ética y no de comprometer la infraestructura de la entidad evaluada.

- En el producto final del proyecto se estableció en uno de los objetivos específicos el utilizar el formato del informe pericial para plasmar los resultados obtenidos, lo cual se lo ha efectuado siguiendo los acápites contenidos en dicho cuerpo, al ser un documento referenciado por parte de peritos judiciales, para exponer los resultados de un procedimiento técnico efectuado.

6.2. Recomendaciones

- Se recomienda considerar el procedimiento desarrollado, para su implementación en la fase de desarrollo de aplicaciones, a fin de evaluar de forma interna al aplicativo ante posibles vulnerabilidades a las que puede estar expuesto.

- Es recomendable, desarrollar el procedimiento, desde una perspectiva de la ética, puesto que, al obtener datos sensibles, se puede exponer a la entidad ante potenciales ataques.

- A nivel académico, es recomendable exponer éste tipo de procedimientos, como proceso formativo, a fin de cimentar en los alumnos, los conocimientos sobre el ámbito de las vulnerabilidades web, a ser considerado en el campo profesional.

- En base a los resultados evidenciados, se recomienda efectuar de manera interna un procedimiento complementario a fin de obtener comparativos entre informes en determinados rangos de tiempo.

- Es vital recomendar que dentro de la planificación que disponga el área de tecnologías de la entidad, se considere la realización de pruebas de penetración para evaluar los niveles de seguridad implementados en su aplicativo de forma periódica.

- En base a los resultados específicos de vulnerabilidades evidenciados, adoptar medidas acordes, a fin de evitar posibles intromisiones en la infraestructura tecnológica.

APÉNDICES

Apéndice A. Top Ten del Proyecto OWASP – 2013 (fragmento)

O Acerca de OWASP

Prefacio

El software inseguro está debilitando las finanzas, salud, defensa, energía, y otras infraestructuras críticas. A medida que la infraestructura digital se hace cada vez más compleja e interconectada, la dificultad de lograr la seguridad en aplicaciones aumenta exponencialmente. No se puede dar el lujo de tolerar problemas de seguridad relativamente sencillos, como los que se presentan en este OWASP Top 10.

El objetivo del proyecto Top 10 es crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. El proyecto Top 10 es referenciado por muchos estándares, libros, herramientas, y organizaciones, incluyendo MITRE, PCI DSS, DISA, FCT, y muchos más . Esta versión de OWASP Top 10 marca el aniversario número diez de este proyecto, de concientización sobre la importancia de los riesgos de seguridad en aplicaciones. OWASP Top 10 fue lanzado por primera vez en 2003, con actualizaciones menores en 2004 y 2007. La versión 2010 fue renovada para dar prioridad al riesgo, no sólo a la prevalencia. La edición 2013 sigue el mismo enfoque.

Lo invitamos a que utilice el Top 10 para hacer que su organización se inicie en la temática sobre seguridad en aplicaciones. Los desarrolladores pueden aprender de los errores de otras organizaciones. Los ejecutivos deben comenzar a pensar como gestionar el riesgo que las aplicaciones de software crean en sus empresas.

A largo plazo, le recomendamos que cree un programa de seguridad en aplicaciones que sea compatible con su cultura y su tecnología. Estos programas vienen en todas las formas y tamaños, y debe evitar tratar de hacer todo lo prescrito por algún modelo de procesos. En cambio, debe de aprovechar las fortalezas existentes en su organización para hacer y medir lo que le funcione a usted.
Esperamos que OWASP Top 10 sea útil para sus esfuerzos de seguridad en aplicaciones. Por favor no dude en ponerse en contacto con OWASP para sus dudas, comentarios, e ideas, ya sea públicamente a owasp-topten@lists.owasp.org o en privado a dave.wichers@owasp.org.

Acerca de OWASP

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones que pueden ser confiables. En OWASP encontrará gratuitas y abiertas ...

- Herramientas y estándares de seguridad en aplicaciones
- Libros completos de revisiones de seguridad en aplicaciones, desarrollo de código fuente seguro, y revisiones de seguridad en código fuente
- Controles de seguridad estándar y librerías
- Capítulos locales en todo el mundo
- Investigaciones de vanguardia
- Extensas conferencias alrededor del mundo
- Listas de correo

Aprenda más en: https://www.owasp.org

Todas las herramientas de OWASP, documentos, foros, y capítulos son gratuitas y abiertas a cualquiera interesado en mejorar la seguridad en aplicaciones. Abogamos por resolver la seguridad en aplicaciones como un problema de personas, procesos y tecnología, ya que los enfoques más efectivos para la seguridad en aplicaciones requieren mejoras en todas estas áreas.

OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva. OWASP no está afiliada con ninguna compañía de tecnología, aunque apoyamos el uso instruido de tecnologías de seguridad comercial. Al igual que muchos otros proyectos de software de código abierto, OWASP produce muchos tipos de materiales en una manera abierta y colaborativa.

La fundación OWASP es una entidad sin ánimo de lucro para asegurar el éxito a largo plazo del proyecto. Casi todos los asociados con OWASP son voluntarios, incluyendo la junta directiva de OWASP, comités globales, líderes de capítulos, los líderes y miembros de proyectos. Apoyamos la investigación innovadora sobre seguridad a través de becas e infraestructura.

¡Únase a nosotros!

Derechos de Autor y Licencia


T10
OWASP Top 10 de Riesgos de Seguridad en Aplicaciones
A1- Inyección
Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.
A2 – Pérdida de Autenticación y Gestión de Sesiones
Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)
Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la victima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.
A4 – Referencia Directa Insegura a Objetos
Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.
A5 – Configuración de Seguridad Incorrecta
Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.
A6 – Exposición de datos sensibles
Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito o credenciales de autenticación. Los atacantes pueden robar o modificar tales datos para llevar a cabo fraudes, robos de identidad u otros delitos. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador.
A7 – Ausencia de Control de Acceso a Funciones
La mayoría de aplicaciones web verifican los derechos de acceso a nivel de función antes de hacer visible en la misma interfaz de usuario. A pesar de esto, las aplicaciones necesitan verificar el control de acceso en el servidor cuando se accede a cada función. Si las solicitudes de acceso no se verifican, los atacantes podrán realizar peticiones sin la autorización apropiada.
A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF)
Un ataque CSRF obliga al navegador de una victima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la victima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la victima.
A9 – Utilización de componentes con vulnerabilidades conocidas
Algunos componentes tales como las librerías, los frameworks y otros módulos de software casi siempre funcionan con todos los privilegios. Si se ataca un componente vulnerable esto podría facilitar la intrusión en el servidor o una perdida seria de datos. Las aplicaciones que utilicen componentes con vulnerabilidades conocidas debilitan las defensas de la aplicación y permiten ampliar el rango de posibles ataques e impactos.
A10 – Redirecciones y reenvios no validados
Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

Apéndice B. Formato de Informe Pericial

FORMATO DE INFORME PERICIAL

Las peritas y peritos presentarán su informe de conformidad con lo establecido en los artículos 19 y 20 del REGLAMENTO QUE REGULA EL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL. Por lo tanto, el **presente formato es de uso obligatorio para la presentación de los informes periciales**, sin perjuicio de lo establecido en normas legales específicas.

"INFORME PERICIAL

1. **DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA**

TRIBUNAL/JUZGADO/FISCALÍA	
No. de Proceso/No. de Indagación Previa o Instrucción Fiscal	
Nombre y Apellido del Perito/a	
Profesión, Oficio, Arte, o Actividad calificada	
No. de Calificación y Acreditación	
Fecha de terminación de la calificación y acreditación	
Dirección de contacto	
Teléfono fijo de contacto	
Teléfono celular de contacto	
Correo electrónico de contacto	

2. **PARTE DE ANTECEDENTES**, en donde se debe delimitar claramente el encargo realizado, esto es, se tiene que especificar claramente el tema sobre el que informará en base a lo ordenado por el juez, el fiscal y/o lo solicitado por las partes procesales.

3. **PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE**, en donde se debe explicar claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. El perito/a deberá relacionar los contenidos de sus conocimientos especializados con el objeto de la pericia encargada. Analizará si son pertinentes o no la aplicación de sus conocimientos especializados al caso concreto materia de su informe.

4. **PARTE DE CONCLUSIONES**, luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. Se prohíbe todo tipo de juicios de valor sobre la actuación de las partes en el informe

técnico. El informe solamente versará sobre los hechos consultados y ordenados, establecidos en los antecedentes, y nada dirá sobre el accionar de las partes procesales en el caso en particular. Las conclusiones solamente se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Cualquier otro criterio adicional a la delimitación de la pericia no será tomado en cuenta al momento de resolver, y será tomado en consideración para la evaluación del perito/a.

5. **PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO,** deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, copias certificadas de documentos, grabaciones, etc.); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas del perito/a para llegar a la conclusión correspondiente. No se cumplirá con este requisito si no se sustenta la conclusión con documentos, objetos, o con la explicación técnica y científica exigida en este numeral. El perito/a deberá razonar y motivar diáfanamente la razón de sus dichos, esto es, justificar desde todo punto de vista las conclusiones que incluya en el informe. En caso de que no fundamente sus conclusiones y esto sea informado por el juez, la jueza, o el/la fiscal, será considerado al momento de la evaluación del perito.

6. **OTROS REQUISITOS,** si la ley procesal correspondiente determina la inclusión de requisitos adicionales a los establecidos por el reglamento, la perita y el perito debe hacerlo constar necesariamente en su informe pericial de conformidad con dicha exigencia legal.

7. **INFORMACIÓN ADICIONAL,** el perito o la perita podrá incluir cualquier otro tipo de información adicional a los numerales anteriores, siempre y cuando la misma ayude a clarificar sus explicaciones y/o conclusiones; y, siempre y cuando esta información se encuentre dentro de los límites del objeto de la pericia.

8. **DECLARACIÓN JURAMENTADA,** el perito o la perita deberá en la parte final del informe, declarar bajo juramento que su informe es independiente y corresponde a su real convicción profesional, así como también, que toda la información que ha proporcionado es verdadera.

9. **FIRMA Y RÚBRICA,** al final del informe se deberá hacer constar la firma y rúbrica del perito o perita, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial."

Apéndice C. Encuesta al personal de TI del objetivo de evaluación

ENCUESTA SOBRE PRUEBA DE PENETRACIÓN EN EL APLICATIVO WEB DE LA AGENCIA NACIONA DE TRÁNSITO

Estimados profesionales del área de tecnologías de la Agencia Nacional de Tránsito, toda vez que se ha entregado el documento que recoge los resultados de la aplicación del proyecto: "ESTRATEGIA PARA LA DETECCIÓN DE VULNERABILIDADES EN LA APLICACIÓN WEB DE LA AGENCIA NACIONAL DE TRÁNSITO COMO HERREMIENTA PARA LA TOMA DE DESICIONES", me permito aplicar éste instrumento evaluativo a fin de determinar su evaluación preliminar..

Considera que el proyecto desarrollado traerá beneficios desde el aspecto tecnológico para la institución?

Si☐ No☐ Desconozco☐

Los reportes de vulnerabilidades encontradas son considerados importantes en una escala de valores:

Bajo☐ Medio☐ Alto☐

Estima que con la ayuda de la solución y en base a los resultados obtenidos en la misma, se tomarán decisiones a un plazo:

Corto☐ Mediano☐ Largo☐

Qué tipo de recursos considera se puede optimizar con la aplicación de la solución propuesta.

Tecnológicos☐ Económicos☐ Humanos☐ Tiempo☐

Contar con reportes de vulnerabilidades detectadas, será funcional para el proceso de desarrollo en un porcentaje de:

5%☐ 25%☐ 50%☐ 75%☐ 95%☐ Otro☐

Las herramientas descritas y utilizadas en el desarrollo del proyecto, considera que son:

Poco útiles.☐ Medianamente útiles.☐ Muy útiles☐

El impacto que tendrá el proyecto realizado en la toma de decisiones por parte del personal de Tecnologías de la ANT será:

Irrelevante☐ Poco importante☐ Muy importante☐

En base a los resultados de la prueba de penetración entregados, se considera que se tomaran acciones:

Correctivas☐ Preventivas☐

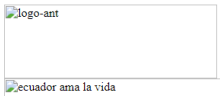
Qué valoración le daría de 0 a 5, donde 0 es nada y cinco muy fiable, los resultados del proyecto desarrollado.

0☐ 1☐ 2☐ 3☐ 4☐ 5☐

Apéndice D. Información de la respuesta del contenido de la cabecera y cuerpo de la página web del objetico de evaluación.

HTTP/1.1 200 OK Date: Thu, 20 Jul 2017 02:02:17 GMT Server: Apache/2.2.15 (CentOS) X-Powered-By: PHP/5.3.3 Set-Cookie: b1ec589226d3b8c50734d0148ee434b9=het5bug5buvtd93mknunh08484; path=/ P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Cache-Control: no-cache Pragma: no-cache Connection: close Content-Type: text/html; charset=utf-8

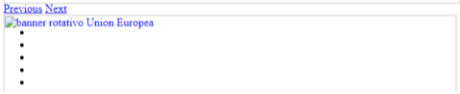
- A+ A-



- Inicio
- ANT
  - Visión, Misión y Objetivos
  - Base Legal
    - Ley Orgánica Reformatoria a la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial
    - Reglamento General para la Aplicación de la LOTTTSV
    - Código Orgánico Integral Penal
  - Contratación Pública
    - Resoluciones Modificatorias al PAC
      - 2012
      - 2013
      - 2014
    - 2015
    - 2016
    - 2017
    - TDR Contratación Especialista Financiero
  - Proyectos
  - Metodología GPR
  - Autoridades
    - Director Ejecutivo
    - Vocales del Directorio
- Programas/Servicios
  - Trámites en Línea
    - Turno para Obtener tu Licencia
    - Consulta tus Multas
    - Regulación de Transporte Pesado
      - Seguimiento de Solicitud
      - Registro de Operador
      - Registro de Factura
    - Validación de Certificado
    - Consultas CPN
    - Chatarrización
      - Impresión FIT Aprobado
      - Generación de Turnos Chatarrización
    - Reimpresion Turno
    - Banco de Preguntas Licencias
  - Puntos de Pago
  - Homologación Vehicular
    - Que es la Homologación Vehicular
    - Documentos del Proceso
    - Formularios
  - Homologación de Dispositivos de Control
    - Resolución No. 20-DIR-2011-ANT
    - Empresas distribuidoras de Dispositivos Contro autorizadas por la ANT
    - PROCEDIMIENTOS PARA LA HOMOLOGACION DE TAXIMETROS
    - Listado de Dispositivos de control homologados
  - Plan Renova
    - Descarga de Formularios
    - Que es Plan Renova
    - Base Legal
    - Requisitos para Acceder
- Obtén tu Turno para Licencias
- Consulta de Citaciones
- Banco de preguntas Licencia
- Pago con dinero electrónico
- Proceso de multas y citaciones
- Consulta de Valor de Matrículas
- Licencias
- 

Concursos de Méritos y Oposición
- Rendición de Cuentas 2015
- Rendición de Cuentas 2016

Previous Next



twitter facebook youtube flickr
Tu Gobierno
Búsqueda

Campaña Respeto al Peaton

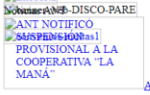
Campaña #DiscoPare

Volcan Cotopaxi
Pablo Andres Calle

Servicios

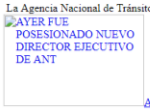
- Proceso para el trámite de devolución a terceros
- Taximetros y GPS homologados
- Listado de Homologación Vehicular
- Descargables
- Taxis Ejecutivos
- Facilidad de Pago para Cancelar Multas de Tránsito
- Licencias conductores
- Tarifas
- Remate de Vehículos
- Consulte el valor a pagar de la matrícula
- Unidades Administrativas y Agencias
- Las tarifas de nuestros servicios
- GPR
- INCOP
- Quipux
- Viajes
- Tramites Ciudadanos
- CEGE

Encuesta
Noticias ANT- DISCO-PARE



ANT NOTIFICÓ SUSPENSIÓN PROVISIONAL A LA COOPERATIVA "LA MANÁ"

La Agencia Nacional de Tránsito (ANT), notificó hoy la suspensión provisional a la Cooperativa de Transporte Interprovincial de Pasajeros "LA MANÁ", tr [...]



AYER FUE POSESIONADO NUEVO DIRECTOR EJECUTIVO DE ANT

Ayer, miércoles 5 de julio de 2017, Pablo Andrés Calle Figueroa, fue posesionado como DirectorEjecutivo de la Agencia Nacional de Tránsito (ANT), como parte&nbs [...]

- 30 Jun 15:45 ANT ADOPTARÁ MEDIDAS A OPERADORAS DE TRANSPORTE INVOLUCRADAS EN LOS ÚLTIMOS SIN...
- 27 Jun 12:22 CÁMARAS DE TRANSPORTE SEGURO FACILITARON LA ATENCIÓN A MUJER EN LABOR DE PARTO E...

- Inicio
- Intranet
- Formularios Plan Renova
- Acceso Consulta SRI Resoluciones
- Videos Quipux
- Instalador SITCON
- Formulario Homologación chasis
- SITOP-ANT

Usuario
Contraseña
Recuérdeme
Identificarse

- ¿Recordar contraseña?
- ¿Recordar usuario?

- Av Antonio José de Sucre y José Sánchez
- contactenos@ant.gob.ec
- PBX (593) Pichincha (02) 3-828-890
- Mapa del Sitio
- |
- Webmail
- |
- Rol de pagos
- ANT

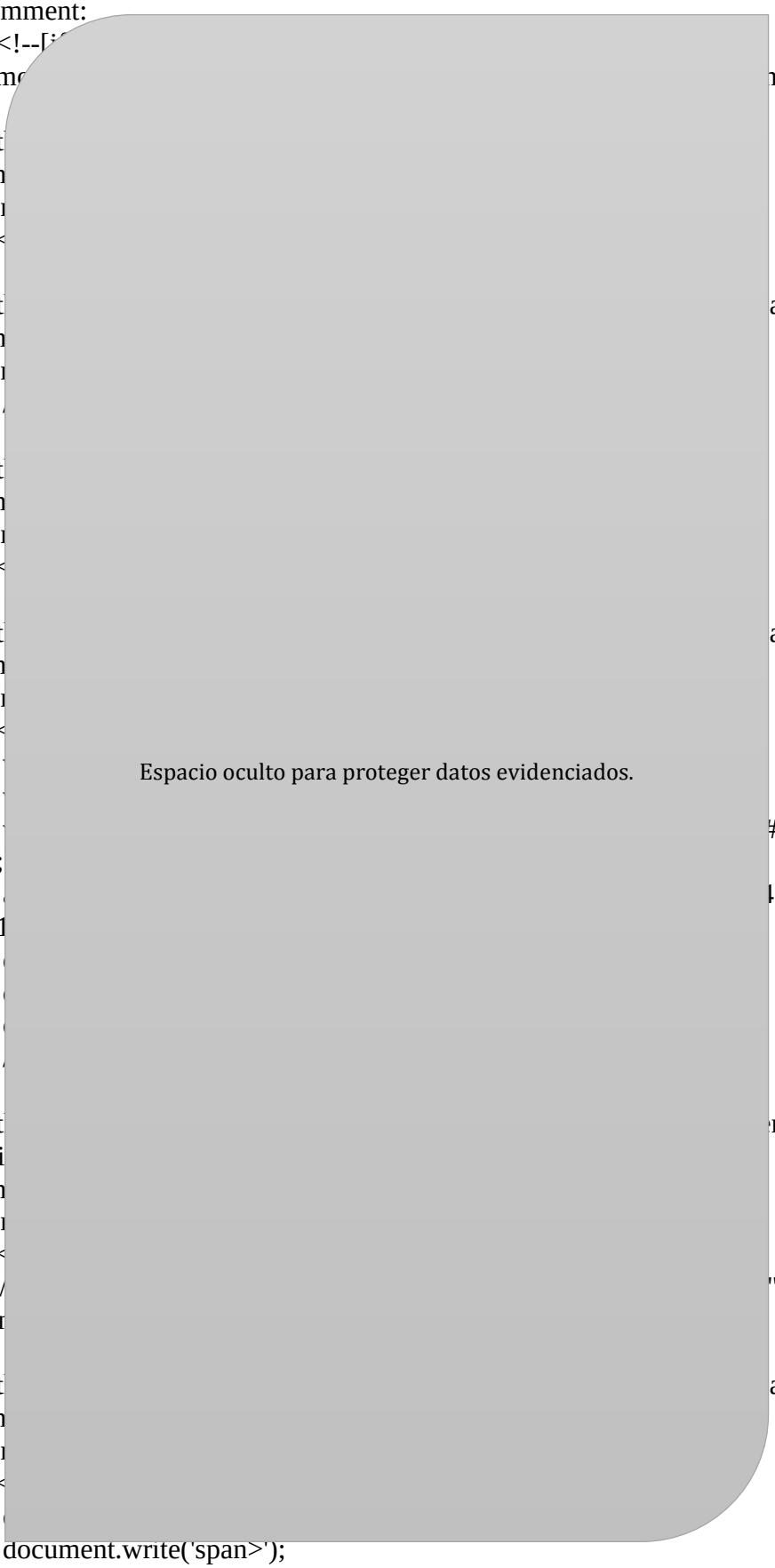
Apéndice E. Identificación de comentarios en la página web del objetico de evaluación.

samurai@samuraiwtf:~$ sudo nmap -n -Pn -p80 --script http-comments-displayer
190.1
[sudo

Start
Nma
Host
POR
80/tc
| http
| Spi 6.5
|
| P
| L
| Comment:
| <!---------- THE CONTENT ----------
---------->
|
| P
| L
| C
|
|
| P o-
finan
| L
| C
|
|
| P
| L
| C
|
|
| P
| L
| C
|
Temp
|
| P cia-2
| L
| C
|
| document.write('<span style=\'display: none;\'>');
| //-->

| Path: http://190.152.46.5/index.php/acceso_consulta_sri_resoluciones
| Li
| C
|
|
| Pa centivo-
finan
| Li
| C
|
|
| Pa
| Li
| C
|
|
| Pa parencia-2
| Li
| C
|
|
| Pa
| Li
| Comment:
| <!-- MAIN CONTENT -->
|
| Pa
| Li
| C
|
|
| Pa
| Li
| C
|
|
| Pa
| Li
| C
|
|
| Pa centivo-
finan
| Li
| C
| ack.fr -->
|
| Path: http://190.152.46.5/templates/system/css/general.css
| Line number: 156

| Comment:
| /* Calendar */
|
| Pat
| Li
| Co
|
|
| Pa res-incentivo-
financ
| Li
| Co
|
|
| Pa
| Li
| Co
|
| ters, Inc. All rights
reserv
| r later; see
LICE
|
|
| Pa e-
taxim ara-empresas-
distrib
| Li
| Co
|
|
| Pa
| Li
| Co
|
|
| Pa
| Li
| Co
|
|
| Pa res-incentivo-
financ
| Li
| Co
|
|
| Path: http://190.152.46.5/index.php/servicios/plan-renova/valores-incentivo-financiero-trans-urbano
| Line number: 47


Espacio oculto para proteger datos evidenciados.

| Path: http://[redacted]atoria-a-la-ley-organic
| Line [redacted]
| Com[redacted]
| <![redacted]
|
| Path[redacted]ntivo-financier
| Line [redacted]
| Com[redacted]
| <![redacted]
| <l[redacted]" />
| <![redacted]
|
| Path[redacted]
| Line [redacted]
| Com[redacted]
| <![redacted]
|
| Path[redacted]rencia-2016/en
| Line [redacted]
| Com[redacted]
| <![redacted]
|
| Path[redacted]ntivo-financier
| Line [redacted]
| Com[redacted]
| <![redacted]
| [redacted]oad", function
|
| documer[redacted]");
|
|
|
|
|
|
|
| [redacted]new RegExp
|
|
|
|
|
| Path: http://[redacted]/index.php/servicios/normas-y-reglamentos-inen/regulacion

Espacio oculto para proteger datos evidenciados.

| Line number: 162
| Comment:
| <!-- /index.php/servicios/normas -->
|
| Pa
| Li
| Co
|_

Espacio oculto para proteger datos evidenciados.

Nmap done: 1 IP address (1 host up) scanned in 15.71 seconds

Apéndice F. Propuesta y gestión documental presentada a la entidad objetivo de evaluación.

ANT-AC-2017-18021
Sistemas

Quito, 10 de julio de 2017

Ingeniero.
Juan Carlos Gómez Paspuel.
Director de Tecnologías de la Información y Comunicaciones de la Agencia Nacional de Tránsito.
Presente. -

De mi consideración:

Por medio de la presente reciba un cordial saludo de Raúl Alfredo Panchi Herrera, portador de la cédula de ciudadanía N°0502521032, me dirijo a usted muy respetuosamente en calidad de alumno del programa de maestría en Gerencia Informática de la Pontifica Universidad Católica del Ecuador Sede Ambato (PUCESA). Agradeciendo por la apertura en semanas pasadas, en la que en diálogo se me recomendó articular el alcance del proyecto propuesto por mi persona, titulado: "Estrategia para la detección de vulnerabilidades la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones", al Esquema Gubernamental de Seguridad de la Información. En ésta oportunidad presento a usted en detalle el alcance del mismo, así también adjunto la certificación que describe que el tema referido, fue aprobado por la Dirección del Departamento de Investigación y Postgrados de la entidad educativa, así también reportes de prensa, en los que se recoge noticias sobre vulneración de sistemas informáticos de algunas entidades públicas, problemática real, que da origen al desarrollo del proyecto referido.

Descripción del proyecto:

La presente propuesta proyecta evidenciar algunas vulnerabilidades encontradas en el aplicativo web de la Agencia Nacional de Tránsito del Ecuador, luego de aplicar una metodología utilizada para detección de vulnerabilidades y posteriores pruebas de penetración hacia aplicativos web, en la cual se cumplirán las etapas de Reconocimiento, Mapeo y Descubrimiento, con excepción de la fase de Explotación, esto debido a que el enfoque del desarrollo de las actividades se las hace desde la perspectiva académica y de hacking ético, mas no es el afán violentar y poner en riesgo la integridad y normal funcionamiento de servicios que brinda el aplicativo.

En el proceso investigativo documental se referirá a terminología y conceptos sobre aplicaciones web, seguridad de las mismas, hacking ético, riesgos de seguridad según OWASP (Open Web Application Security Project), pruebas de penetración y sus tipos, arquitectura de servidores web y sus tipos, legislación ecuatoriana sobre delitos informáticos, y aspectos sobre vulnerabilidades, recogidos en el Esquema Gubernamental de Seguridad de la Información (EGSI).

La plataforma seleccionada para llevar a efecto la detección de vulnerabilidades y que posibilita la ejecución de pruebas de penetración hacia el aplicativo web objetivo de evaluación es Samurai Web Testing Framework en su versión 3.0, ya que dicha plataforma es de código abierto y contiene herramientas gratuitas que se enmarcan en evaluar la seguridad y en auditar los perfiles de seguridad de sitios y aplicaciones web.

La metodología utilizada es OWASP, la cual consiste en ejecutar de forma secuencial las fases de Reconocimiento, Mapeo, Descubrimiento y Explotación, de las vulnerabilidades localizadas en el objetivo de evaluación, pero para el caso no se llevará a efecto la fase de Explotación por estar fuera del alcance de la propuesta al enmarcarse en el ámbito del hacking ético.

Una vez aplicadas las herramientas, de la mano de procedimientos, los resultados de las vulnerabilidades detectadas, se los condensará utilizando el modelo de un "Informé Pericial", el cual servirá como herramienta para la toma de decisiones en el marco de seguridad del aplicativo web, por parte del personal encargado de TI (Tecnologías de la Información) del a entidad objetivo de análisis.

Alcance del proyecto:

Es el primer paso dentro de la fase de reconocimiento es justamente definir el alcance del proyecto, constituyendo el objetivo general del presente trabajo, el cual es desarrollar una estrategia para la detección de vulnerabilidades en el aplicativo web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones, con el empleo de la metodología OWASP en sus fases, a excepción de la última fase que es la de explotación, en la que se dejará sentado la base informativa del procedimiento, así también las herramientas que pueden ser empleadas para efectuar una prueba de penetración de forma integral, pudiéndose posteriormente llegar a la explotación o vulneración misma del objetivo de evaluación, esto debido a que el marco legal y ético del trabajo se enfoca en esencia desde una perspectiva académica y de hacking ético, a fin de brindar a la entidad, un sustento procedimental que puede ser aplicado, para tomar decisión y acción frente a potenciales vulnerabilidades detectadas, y evitar ataques reales al aplicativo web.

No se establece el acceso, obtención o manipulación de datos e información de usuarios contenidas en bases de datos, a través del procedimiento, ya que el aspecto central es detectar posibles vulnerabilidades en el aplicativo web.

Como documento entregable a la entidad, se define un informe conteniendo el procedimiento aplicado, así como las vulnerabilidades obtenidas y recomendaciones hacia las mismas.

Metodología y etapas:

La metodología propuesta para el desarrollo del proyecto es OWASP (Open Web Application Security Project), orientada a la realización de pruebas de penetración y consiste en ejecutar de forma secuencial las fases de Reconocimiento, Mapeo, Descubrimiento y Explotación de las vulnerabilidades en un objetivo de evaluación, enfatizando que para el presente caso no se efectuará la fase de Explotación por estar fuera del alcance de la propuesta, misma que se enmarca desde la perspectiva del hacking ético.

En la fase de Reconocimiento se plantean las bases para ejecutar la detección de vulnerabilidades, en ésta se reconocerá el objetivo de evaluación, los objetivos y el alcance, adicionalmente se establece el acercamiento hacia el personal que dirige administrativa y tecnológicamente la entidad, a fin de solicitar la autorización correspondiente para la realización del proyecto. Para el cumplimiento de ésta fase se plantea el uso de algunas herramientas como Samurai Web Testing Framework, en base a su consola de comandos, instrucciones como Who is, así como dicha consulta a través de la página de IANA, procedimiento que permitirá determinar el servidor de nombre del dominio (DNS), además buscar referencias del personal de TI mediante fuentes de información externa como redes sociales y búsquedas avanzadas en bases de datos como google hacking, para finalizar la fase con el empleo de la interfaz de Netcraft, misma que permitirá la detección del tipo de servidor web y de sistema operativo del objetivo de evaluación.

En la fase de mapeo se plantea efectuar diferentes tareas o actividades, entre las cuales se establece un spidering mediante un programa que explora el aplicativo web y sus enlaces, trazar el flujo de la aplicación y analizar la relación entre las páginas, para luego identificar las máquinas que se utilizan dentro de la aplicación las cuales son visibles para los clientes, para lo que se efectuarán actividades de escaneo de puertos, escaneo de versiones, reconocimiento del sistema operativo, y obtención de

información de configuración del software. En el escaneo de puertos se busca capturar información sobre los puertos abiertos, sistema operativo y versión del servicio, para lo cual se prevé la intervención de herramientas activas y pasivas, en el caso de las activas enviando tráfico hacia el objetivo de evaluación, para ser analizadas las respuestas devueltas, empleándose para ello Nmap, mientras que por parte de las herramientas pasivas permitirá capturar y analizar sin enviar tráfico al objetivo, para lo cual se establece el uso de pOf3.

En la fase de descubrimiento se dará inicio a la exploración de forma más profunda en la aplicación web, encontrándose ya los resultados de posibles vulnerabilidades, información requerida para la fase de explotación. Para el desarrollo de ésta fase se ha propuesto el empleo de herramientas como: Zed Attack Proxy (ZAP).

Finalmente, la metodología expone la fase de explotación, consistiendo en efectuar el ataque al aplicativo web. Cabe indicar que ésta fase no se la contempla dentro del alcance del proyecto por estar dentro del concepto de hacking ético, más en su lugar y en base a las vulnerabilidades evidenciadas, se efectuarán recomendaciones para evitar ataques reales no autorizados al aplicativo web, los mismos que serán expuestos mediante el uso del formato de informe pericial, el cual sea considerado como un instrumento para la toma de decisiones en aspectos de seguridad por parte del personal de TI de la entidad objetivo de evaluación.

Importancia e impacto del proyecto:

En cuanto al impacto y la importancia que tiene el proyecto radica en que se dispondrá de una estrategia, la cual se puede emplear en el aplicativo web, de manera controlada y dentro de los procedimientos legales, con la finalidad de evaluar la existencia de potenciales vulnerabilidades, orientando o siendo una herramienta con la que el personal de TI de la entidad, puede tomar decisiones en pos de acciones preventivas o correctivas para mitigar sucesos ante posibles ataques hacia la infraestructura web institucional, por parte de piratas informáticos para el cometimiento de delitos enmarcados en el ámbito informático.

Inclusive, desde una perspectiva global, se puede tomar como base procedimental, para su aplicación en otros objetivos de evaluación especialmente enfocados a entidades del sector público, por la importancia de la gestión que permiten actualmente realizar a través de sus aplicaciones web, permitiendo disponer de un mecanismo evaluativo ante potenciales vulnerabilidades.

Base legal:

El marco legal tomado en consideración para el desarrollo del proyecto es la legislación ecuatoriana que expresa sobre delitos informáticos, considerando:

En el Ecuador se cuenta con el Código Orgánico Integral Penal (COIP) promulgado por (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), para la administración de justicia en los casos los cuales exista el cometimiento de delitos.

En cuanto a delitos informáticos específicamente el documento citado anteriormente hace referencia en algunos articulados como los siguientes a las penas que serán impuestas a quienes cometan dichos delitos.

Artículo 190.- Apropiación fraudulenta por medios electrónicos. -

"La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de ésta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistema informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionado con pena privativa de la libertad de uno a tres años."

En la sección tercera, (Ministerio de Justicia, Derechos Humanos y Cultos, 2014) expone sobre los delitos contra la seguridad de los activos de los sistemas de información y comunicación, que rezan los siguientes artículos:

Artículo 229.-Revelación ilegal de base de datos. -

"La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años."

Artículo 230.- Interceptación ilegal de datos. -

La sanción será pena privativa de la libertad de tres a cinco años para quienes:

1. "La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible."

2. "La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder."

3. "La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares."

4. "La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior."

Artículo 231.- Transferencia electrónica de activo patrimonial. -

Será sancionada con pena privativa de libertad de tres a cinco años: "La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero"

Artículo 232.- Ataque a la integridad de sistemas informáticos. -

"La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años."

Con la misma sanción se aplica para quienes:

1. "Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo."

2. "Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general."

"Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad."

Artículo 233.- Delitos contra la información pública reservada legalmente. -

"La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años."

"La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años."

"Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad."

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. -

"La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años."

Aspecto importante para el desarrollo del proyecto, es considerar y aplicar como base documental legal, para tomar procedimiento, el Esquema Gubernamental de Seguridad de la Información (EGSI), el cual entró en vigencia mediante Acuerdo Ministerial 166, publicado en el Registro Oficial Suplemento 88 de 25-sept-2013, por parte de la Secretaría Nacional de la Administración Pública del Ecuador, del cual seguidamente se refieren en el presente proyecto, aspectos inherentes a las vulnerabilidades en los sistemas de información, en el siguiente detalle:

En el título 2. Organización de la Seguridad de la Información, subtítulo 2.2. Coordinación de la Gestión de la Seguridad de la Información, acápite cuarto refiere a la "aprobación de las principales iniciativas para incrementar la seguridad de la información."

En el subtítulo 2.4. Procesos de autorización de nuevos servicios de procesamiento de la información, literal e) refiere a "implementar los controles necesarios para el uso de nuevos servicios para procesar información de la institución sean personales o de terceros para evitar nuevas vulnerabilidades."

En el subtítulo 2.7. Contactos con grupos de interés especiales, literal a) cita: "Mantener contacto apropiados con organizaciones públicas y privadas, asociaciones profesionales y grupos de interés especializados en seguridad de la información para mejorar el conocimiento sobre mejores prácticas y estar actualizado con información pertinente a gestión de la seguridad."; y el literal b) menciona: "recibir reportes advertencias oportunas de alertas, avisos y parches relacionados con ataques y gestión de la seguridad de la información."

El subtítulo 2.9. Identificación de los riesgos relacionados con las partes externas, literal c), refiere a "registrar y mantener las terceras partes vinculadas a la entidad...", en consideración de algunos tipos, como: asesores y auditores externos, personal temporal (estudiantes, pasantes, funcionarios públicos externos), ciudadanos o clientes, que para el caso se considera desarrollar el procedimiento desde la perspectiva académica.

En el título 6. Gestión de Comunicaciones y Operaciones, subtítulo 6.23. Sistemas de Información del Negocio, literal a), menciona "proteger o tener en cuenta las vulnerabilidades conocidas en los sistemas administrativos, financieros, y demás sistemas informáticos donde la información es compartida."

En el título 8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, subtítulo 8.16. Control de las vulnerabilidades técnicas, literal f) refiere a "identificar los riesgos asociados a una vulnerabilidad potencial y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y/o la aplicación de otros controles."; en el literal l) menciona sobre "aumentar el monitoreo para detectar o prevenir los ataques reales"; y en el literal o) hace referencia a "monitorear y evaluar a intervalos regulares las vulnerabilidades técnicas, para garantizar eficacia y eficiencia."

En el título 9. Gestión de los Incidentes de la Seguridad de la Información, subtítulo 9.2. Reporte sobre las debilidades en la seguridad, literal a), enmarca "Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre éstos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberán ser fáciles, accesibles y disponibles. Se les debe informar a ellos que en ninguna circunstancia deberán intentar probar una debilidad sospechada", aspecto a destacar, ya que, en la aplicación de la metodología, se establecen cuatro fases, de las cuales no se aplicará la cuarta que comprende a la explotación misma de las vulnerabilidades, manteniéndose dentro de una perspectiva de hacking ético.

Finalmente, en el título 11. Cumplimiento, subtítulo 11.8. Verificación del cumplimiento técnico, literal e), establece "ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes..."

Talento Humano:

Al tratarse de un proyecto de titulación, el autor del mismo, es considerado como actor principal, con la participación del director del proyecto, en la revisión y asesoría para el desarrollo del documento

entregable. Adicionalmente de la designación de un contacto, quine sea un funcionario de la entidad, para establecer comunicación de procedimientos a desarrollar.

Materiales y herramientas:

A continuación, se describen las herramientas tanto de hardware como de software que se han utilizado en el proyecto.

Se ha empleado una laptop la cual cuenta con las siguientes características básicas:

Tabla 1: Características del computador utilizado.

PROCESADOR	MEMORIA	DISCO DURO	TARJETA DE ALÁMBRICA	TARJETA DE INALÁMBRICA
Core ™ i7-4710HQ CPU 2.50 GHz	RAM 16.0 GB	1024 GB	Realtek PCIe GBE Family Controller	Intel ® Dual Band Wireless-AC 3160

Fuente: elaboración propia.

VMWare 12 Player como software de virtualización.
Samurai Web Testing Framework versión 3.0 como entorno de trabajo para pruebas de penetración.
Consola de Samurai Web Testing Framework
Buscador Google
Red social Facebook
Red profesional LinkedIn
Herramienta Nslookup
Herramienta dig
Página web de ARIN
Página web de IANA.
Página web de NIC.EC
Página web de Netcraft
Maltego
Nmap
Netcat
Herramienta OpenSSL
Buscador bing
Nikto
Wget
Zed Attack Proxy (ZAP)
w3af

Cronograma de trabajo:

Respecto al cronograma de trabajo propuesto se detalla, una duración del proyecto de nueve semanas, en las que desarrollarán cada una de las fases, como se muestra seguidamente:

ACTIVIDAD	SEMANAS								
	1	2	3	4	5	6	7	8	9
Gestiones para obtener la autorización para la ejecución del proyecto en el aplicativo web de la Agencia Nacional de Tránsito del Ecuador.	X	X							
Aplicación de la fase de Reconocimiento en el aplicativo web de la entidad objetivo de evaluación.			X	X					
Documentación de los resultados obtenidos en la fase de Reconocimiento.				X					
Exploración del aplicativo web y sus enlaces dentro de la fase de Mapeo.					X	X			
Documentación de los resultados obtenidos en la fase de Mapeo.						X			
Localización de posibles vulnerabilidades aplicando la fase de Descubrimiento.							X	X	
Documentación de los resultados obtenidos en la fase de Descubrimiento.								X	
Establecimiento de Conclusiones y Recomendaciones.								X	X
Redacción del documento entregable en base al formato del informe parcial con los resultados obtenidos.			X	X	X	X	X	X	X

Costos:

Respecto a los costos, no se establece valor alguno, ya que se trata de una intervención desde al ambiente académico, para brindar de una herramienta procedimental factible de aplicar.

Políticas de confidencialidad de la información:

Al tratarse de un proyecto académico de titulación, los resultados obtenidos, mismos que arrojen información considerada confidencial, así como datos de configuración y los resultados de vulnerabilidades encontradas, serán protegidos para su visualización en el documento entregable mediante pixelado o desenfoque en partes o en la totalidad de las imágenes, más en el documento entregable hacia la entidad objetivo de evaluación si se visualizarán en detalle.

Además, se establece la elaboración de una carta compromiso por parte del autor en mantener la confidencialidad de la información de vulnerabilidades que se obtenga.

En cuanto a la interacción con el aplicativo para el desarrollo de cada una de las fases, se establecerá contacto vía telefónica y correo electrónico, con personal de la entidad para informar del procedimiento a efectuar, manteniendo comunicación constante de la gestión, para lo que solicito también datos de contacto de la persona que se designe por parte de la entidad.

Finalmente, mantengo que mi compromiso con la realización del proyecto, no es causar inconvenientes, ni mucho menos poner en riesgo la seguridad del aplicativo web de la ANT, por el contrario, es brindar desde mi perspectiva personal y profesional un aporte a la entidad para determinar posibles vulnerabilidades, permitiendo tomar acciones preventivas o correctivas ante posibles ataques informáticos.

Con lo descrito, me dirijo a usted con la finalidad de solicitarle muy comedidamente, se digne expresar por escrito la autorización o negativa, en detalle, de ser el caso respectivo, para la realización y ejecución del proyecto de titulación mencionado en la aplicación web de la Agencia Nacional de Tránsito, documento que servirá como sustento académico y base habilitante o limitante, para el desarrollo del proyecto propuesto en sus diferentes fases.

Por la gentil y favorable atención que se digne dar a mi petición, anticipo y reitero mis agradecimientos.

Atentamente,

Ing. Raúl Alfredo Panchi Herrera.
C.I.:0502521032

Teléfonos de contacto: 0984523738 / (03)2104008
Correo electrónico: raulalfredoph@gmail.com
Dirección laboral: CENESCYT, Cotopaxi, Latacunga, Tanicuchí, panamericana norte kilómetro 12 vía a Quito, Instituto Superior Tecnológico Cotopaxi.
Dirección domiciliaria: Cotopaxi, Latacunga, Juan Montalvo, San Martín – Isimbo, calles Tomebamba y Cicalpas vía a San José.

Documentos adjuntos:
Documentos personales del autor del proyecto.
Certificación de aprobación del tema del proyecto.
Carta de compromiso de confidencialidad de la información.
Reportes de prensa sobre vulnerabilidades en entidades públicas.


REPUBLICA DEL ECUADOR
CIUDADANIA
0502521032-2
PANCHI HERRERA RAUL ALFREDO
COTOPAXI/LATACUNGA/JUAN MONTALVO (SN.SEBAS
06 OCTUBRE 1979
003- 0186 01964 M
COTOPAXI/ LATACUNGA
LA MATRIZ
1979
ECUATORIANA*****
E444314222
CASADO
YUBCHA VILEMA MARTHA VERONICA
SUPERIOR
ING SIST/INFO/COMPUT
CESAR AUBUSTO PANCHI
ANGELA HERRERA
LATACUNGA
11/01/2010
11/01/2022
REN 2220555


CERTIFICADO DE VOTACIÓN
ELECCIONES GENERALES 2017
2 DE ABRIL 2017
CNE
013
JUNTA No
013 - 328
NÚMERO
0502521032
CÉDULA
PANCHI HERRERA RAUL ALFREDO
APELLIDOS Y NOMBRES
COTOPAXI
PROVINCIA
CIRCUNSCRIPCIÓN
LATACUNGA
CANTÓN
ZONA
JUAN MONTALVO
PARROQUIA

OFICINA DE INVESTIGACIÓN Y POSTGRADOS. SECRETARIA.- Ambato, julio 03 del 2017.- Presentada en esta fecha. Certifico

Lic. Doris Rosales Vacas
SECRETARIA OIP

Pontificia Universidad Católica del Ecuador
SECRETARÍA DE LA OFICINA DE INVESTIGACIÓN Y POSGRADOS

OFICINA DE INVESTIGACIÓN Y POSTGRADOS Ambato, julio 03 del 2017. Vista la solicitud que antecede, sea la Secretaria de la OIP dé el trámite pertinente.

Pfr. Diego Jiménez Bósquez
COODINADOR DE LA OFICINA DE INVESTIGACIÓN y POSTGRADOS

Pontificia Universidad Católica del Ecuador
OFICINA DE INVESTIGACIÓN Y POSGRADOS

OFICINA DE INVESTIGACIÓN Y POSTGRADOS. SECRETARIA.- Ambato, julio 04 del 2017. Revisado el kardex # MGI-076, perteneciente a **RAÚL ALFREDO PANCHI HERRERA. CERTIFICO** que, el Proyecto de Investigación que debe realizar el mencionado estudiante previo a la obtención del título de Magister en Gerencia Informática, fue aprobado con el tema, **"ESTRATEGIA PARA LA DETECCIÓN DE VULNERABILIDADES EN LA APLICACIÓN WEB DE LA AGENCIA NACIONAL DE TRÁNSITO COMO HERRAMIENTA PARA LA TOMA DE DECISIONES"**, por la Dirección del Departamento de Investigación y Postgrados con fecha 12 de enero de 2016.

Dr. Hugo Altamirano Villarroel
SECRETARIO GENERAL PUCESA

CARTA DE COMPROMISO DE CONFIDENCIALIDAD DE LA INFORMACIÓN

Quito, 10 de julio de 2017

Ingeniero.
Juan Carlos Gómez Paspuel.
Director de Tecnologías de la Información y Comunicaciones de la Agencia Nacional de Tránsito.
Presente. -

Por medio de la siguiente carta, yo Raúl Alfredo Panchi Herrera, portador de la cédula de identidad N°0502521032, en calidad de alumno del programa de maestría en Gerencia Informática de la Pontifica Universidad Católica del Ecuador Sede Ambato (PUCESA), y proponente del proyecto titulado: "Estrategia para la detección de vulnerabilidades la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones", para el desarrollo del mismo me obligo y comprometo a los siguientes aspectos:

- No divulgar a terceras personas, el contenido, datos o información confidencial, obtenida producto de la aplicación del proyecto de titulación planteado.
- No revelar públicamente detalles sobre las vulnerabilidades encontradas.
- No ejecutar procedimientos que lleven a la explotación o alteración de datos al interior del aplicativo web de la entidad.
- Mantener los procedimientos técnicos en apego a las leyes y reglamentos vigentes.
- Entregar un documento que contenga el procedimiento y los resultados a la entidad.
- El procedimiento será únicamente desde la perspectiva investigativa - académica, dentro del proceso de titulación.

Atentamente,

Ing. Raúl Alfredo Panchi Herrera.
C.I.:0502521032

Teléfonos de contacto: 0984523738 / (03)2104008

EL COMERCIO

Actualidad - SEGURIDAD

18 de enero de 2016 (0:0)

Bandas de 'hackers' intensificaron sus operaciones en 2015

Fernando Medina
seguridadec@elcomercio.com

Los 'hackers' operaban en el país desde hace 18 meses. En ese tiempo movieron **USD 1 millón en sus cuentas bancarias de Ecuador y Colombia**.

Ese dinero era producto de los cobros que realizaban por registrar ilegalmente **títulos profesionales falsos en la Senescyt** y **licencias de conducción en la Agencia Nacional de Tránsito** (ANT). Para toda esta operación, 10 personas atacaban los portales digitales de las instituciones públicas.

Según investigadores de la Policía, lo piratas cibernéticos lograron incluir **366 títulos falsos** en la base de datos de la Senescyt y **600 permisos de conducir falsos** en la Agencia de Tránsito.

Esos detalles se revelaron por completo el pasado viernes (16 de enero del 2016). Pero este es solo uno de los casos más recientes. De hecho, datos de la Fiscalía indican que solo en ocho meses del año anterior se registraron 1 026 denuncias por delitos informáticos en el país.

Aquí están, por ejemplo, ataques de ciberpiratas a empresas públicas y privadas. En el 2014, durante ese mismo período, se reportaron 877. Es decir, hubo para el 2015 un incremento de 16,9% en los ataques.Pero, ¿cómo operan estas cibermafias?

Agentes de unidades especiales de la Policía y de la Fiscalía saben cómo han evolucionado las maniobras de estas bandas: antes, los ataques se realizaban principalmente desde el extranjero, por lo que la tarea para capturar a los implicados se tornaba imposible.

En el último año, esta actividad se realiza dentro de Ecuador; se ha detectado a expertos en computación que vulneran las seguridades de sitios web a cambio de fuertes sumas de dinero. Por ejemplo, se conoció que la organización que **registraba los títulos falsos cobraba desde USD 1 000 hasta USD 10 000**.

De igual forma, en la Internet existe una amplia 'oferta' de 'hackers' que aseguran pueden conseguir las claves de accesos de cuentas bancarias o de correos electrónicos. Por esa tarea, los montos que piden fluctúan entre USD 150 y USD 600. Precisamente, descifrar las claves es uno de los tres tipos de 'hackeos' que más se producen en el país.

La Fiscalía señala que entre enero y agosto del 2015 se iniciaron procesos por violentar las contraseñas o encriptarlas. Así como también por la apropiación fraudulenta por medios electrónicos. Por último, está "el acceso no consentido a un sistema informático, telemático o de telecomunicación".
El **Código Integral Penal** sanciona hasta con cinco años de cárcel a quien acceda, intervenga, divulgue información personal, destruya o modifique base de datos. Precisamente, esa sería la pena que podrían enfrentar los 10 involucrados en los fraudes de títulos del último caso.

Además, en ese hecho **quienes pagaron o se beneficiaron de los 'hackeos' también pudieran enfrentar juicios**, cuyas penas ascienden a seis meses o hasta dos años de cárcel . Esto, por ejercer una profesión de forma ilegal en el país.

Pero los 'hackeos' no solo se han dado en el sector público o a personas naturales. Las empresas privadas también han sido víctimas de las cibermafias, que exactamente hace un año hicieron su primera aparición a escalana nacional.

El 19 de enero, cuando la Fiscalía reportó el primer ataque masivo de los 'hackers' en el país, en total 17 empresas resultaron afectadas. Lo que los desconocidos hicieron fue entrar a las bases de información de las empresas y bloquearlas. Luego pedían una alta suma de dinero para liberar los datos o, caso contrario, la información era eliminada en su totalidad.

Este es uno de los casos con los que se confirmó la falta de seguridad informática en el país. La compañía **Kaspersky**, una empresa que da seguridad a las megaplataformas digitales, en su informe del 2014 colocó al Ecuador en el octavo puesto en Latinoamérica con más ataques informáticos.
En su reciente informe, de noviembre pasado, señala que durante este 2016 se incrementarán y diversificarán los ataques a dispositivos mó-viles, principal herramienta para conectarse a Internet.

Las empresas deben tener especial cuidado con su seguridad informática, ya que se han incrementado no solo los 'malware' (virus) sino los ataques híbridos. Esto quiere decir, ataques informáticos con la complicidad de personal de empresas que ayudan al vulnerar los sistemas de seguridad digital.

Esta anomalía también se detectó en la red de los 10 detenidos, pues según agentes de la Policía, al menos un funcionario habría colaborado en la falsificación de las 600 licencias de la ANT.

En cuanto a los títulos universitarios, el proceso de investigación continúa y ya se tiene previsto que la **Secretaría Nacional de la Administración Pública** (SNAP) se pronuncie sobre este caso. La Fiscalía también espera esa información para iniciar procesos legales a quienes pagaron.

Fuente: Fernando Medina Diario "El Comercio", 18 de enero de 2016, recuperado electrónicamente de: http://www.elcomercio.com/actualidad/bandas-hackers-titulos-licencias-falsas.html

EL COMERCIO

Actualidad - SEGURIDAD

9 de enero de 2016 09:41

Hackers registraron 366 títulos universitarios en la Senescyt y entregaron 600 licencias de conducir

El ministro del Interior, José Serrano, explicó los detalles de cómo operaba la banda de hackers que falsificaba títulos universitarios y doctorados, para registrarlos en la Senescyt.
Foto: Vicente Costales/ EL COMERCIO

Sara Ortiz

Un **PhD** era el **más caro**, costaba hasta USD 10 000. Por **licenciaturas** e **ingenierías** los precios iniciaban desde los **USD 1 000**. Una supuesta **banda de** hackers o **delincuentes cibernéticos** habría cobrado estos precios por **registrar un título falso** en el sistema informático de la **Secretaría Nacional de Educación Superior** (Senescyt).

Abogados, médicos, ingenieros, administradores de empresas, maestrías y hasta doctorados. La Policía y la Fiscalía descubrieron que 366 **títulos en el país eran** falsos y que una banda estaba detrás de esto.

La misma red también habría atacado los sistemas informáticos de la **Agencia Nacional de Tránsito** (ANT), del **Banco Central del Ecuador** y otras entidades financieras. En 18 meses que los supuestos hackers operaron se calcula que **movieron USD 1 millón** a cuentas bancarias en el país y también **derivaron el dinero a Colombia**.

Estos detalles los dio a conocer el **ministro del Interior, José Serrano**, en una rueda de prensa sobre la desarticulación de la presunta organización. El operativo se realizó en la mañana de este viernes 8 de enero del 2016 y fue denominado 'Impacto inicial'.

Fuente: Sara Ortiz, Diario "El Comercio", 9 de enero de 2016, recuperado electrónicamente de: http://www.elcomercio.com/actualidad/hackers-registraron-titulos-universitarios-falsos.html

EL COMERCIO

Actualidad > JUSTICIA

10 de diciembre de 2014 15:02

Cinco personas detenidas por vulnerar los sistemas informáticos del Sercop

Un servidor, una laptop y documentos fueron las evidencias encontradas en el operativo. Foto: Cortesía Ministerio de Interior.

Redacción Quito (i)

Tras dos meses de investigación la **Policía Judicial** logró **desarticular una banda** conformada por cinco personas que vulneraron la integridad de los sistemas informáticos del Servicio Nacional de Contratación Pública (Sercop).

Los detenidos usaban un **software para "adulterar todo el sistema** en beneficio de empresas, microempresas o personas naturales, quienes pagaban fuertes sumas de dinero para salir favorecidas con los contratos", esto explicó el coronel **Ramiro Ortega**, director de la Policía Judicial en rueda de prensa realizada hoy, miércoles 10 de diciembre, a las 11:30.

Ortega explicó que el **operativo se denominó Tempestad** y contó con la participación del **Grupo de Intervención y Rescate (GIR)** y el apoyo técnico del Departamento Criminalístico.

Los detenidos son **cuatro hombres y una mujer**. Las aprehensiones se llevaron a cabo ayer, martes 9 de diciembre, y se allanó a cuatro inmuebles en el norte y en el sur de la ciudad.

Entre las evidencias encontradas están **11 teléfonos celulares, un CPU, un ruteador, dos módems**, cuatro tarjetas de memoria, cinco chequeras, seis discos duros externos, cinco discos duros internos, una **computadora y varios documentos**.

Fuente: Redacción, Diario "El Comercio", 10 de diciembre de 2014, recuperado electrónicamente de: http://www.elcomercio.com/actualidad/sercop-hackers-detenidos-informatica-evidencias.html

Quito, 03 de abril de 2017

Ingeniero.
John Hill Peña.
DIRECTOR EJECUTIVO DE LA AGENCIA NACIONAL DE TRÁNSITO.
Presente. -

ANT-A-2017-10723
Sistemas

De mi consideración:

Por medio de la presente reciba un cordial saludo de Raúl Alfredo Panchi Herrera, portador de la cédula de ciudadania N°0502521032, me dirijo a usted muy respetuosamente en calidad de alumno del programa de maestría en Gerencia Informática de la Pontifica Universidad Católica del Ecuador Sede Ambato (PUCESA). En anterior ocasión me dirigí a usted con la finalidad de solicitar la autorización respectiva para el desarrollo del proyecto titulado: "Estrategia para la detección de vulnerabilidades la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones", ésta vez me permito a través de la presente y en atención al Oficio Nro. ANT-ANT.-2017-2223, suscrito por el Señor Ingeniero Juan Carlos Gómez Paspuel, Director de Tecnologías de la Información y Comunicaciones de la ANT, emitir el detalle de la metodología RMDE, el impacto que tendría, así como el cronograma de trabajo planteado para el desarrollo del proyecto.

La metodología propuesta para el desarrollo del proyecto es RMDE, orientada a la realización de pruebas de penetración y consiste en ejecutar de forma secuencial las fases de Reconocimiento, Mapeo, Descubrimiento y Explotación de las vulnerabilidades en un objetivo de evaluación, enfatizando que para el presente caso no se efectuará la fase de Explotación por estar fuera del alcance de la propuesta, misma que se enmarca desde la perspectiva del hacking ético.

En la fase de Reconocimiento se plantean las bases para ejecutar la detección de vulnerabilidades, en ésta se reconocerá el objetivo de evaluación, los objetivos y el alcance, adicionalmente se establece el acercamiento hacia el personal que dirige administrativa y tecnológicamente la entidad, a fin de solicitar la autorización correspondiente para la realización del proyecto. Para el cumplimiento de ésta fase se plantea el uso de algunas herramientas como Samurai Web Testing Framework, en base a su consola de comandos, instrucciones como Who is, así como dicha consulta a través de la página de IANA, procedimiento que permitirá determinar el servidor de nombre del dominio (DNS), además buscar referencias del personal de TI mediante fuentes de información externa como redes sociales y búsquedas avanzadas en bases de datos como google hacking, para finalizar la fase con el empleo de la interfaz de Netcraft, misma que permitirá la detección del tipo de servidor web y de sistema operativo del objetivo de evaluación.

En la fase de mapeo se plantea efectuar diferentes tareas o actividades, entre las cuales se establece un spidering mediante un programa que explora el aplicativo web y sus enlaces, trazar el flujo de la aplicación y analizar la relación entre las páginas, para luego identificar las máquinas que se utilizan dentro de la aplicación las cuales son visibles para los clientes, para lo que se efectuarán actividades de escaneo de puertos, escaneo de versiones, reconocimiento del sistema operativo, y obtención de información de configuración del software. En el escaneo de puertos se busca capturar información sobre los puertos abiertos, sistema operativo y versión del servicio, para lo cual se prevé la intervención de herramientas activas y pasivas, en el caso de las activas enviando tráfico hacia el objetivo de evaluación, para ser analizadas las respuestas devueltas, empleándose para ello Nmap, mientras que por parte de las herramientas pasivas permitirá capturar y analizar sin enviar tráfico al objetivo, para lo cual se establece el uso de pOf3.

Quito, 11 de enero de 2017

Ingeniero.
John Hill Peña.
DIRECTOR EJECUTIVO DE LA AGENCIA NACIONAL DE TRÁNSITO (e).
Presente.-

De mi consideración:

Por medio de la presente reciba un cordial saludo de Raúl Alfredo Panchi Herrera, portador de la cédula de ciudadanía N°0502521032, me dirijo a usted muy respetuosamente en calidad de alumno del programa de maestría en Gerencia Informática de la Pontifica Universidad Católica del Ecuador Sede Ambato (PUCESA), con el propósito de relatarle lo siguiente: dentro de la planificación académica de las entidades de educación superior se establece la realización o desarrollo de proyectos con la finalidad de obtener la titulación, por lo cual en la entidad educativa mencionada he propuesto la realización del proyecto con el tema: "Estrategia para la detección de vulnerabilidades en la aplicación web de la Agencia Nacional de Tránsito como herramienta para la toma de decisiones."; proyecto el cual ha sido referido como factible, teniendo la finalidad de brindar un aporte desde la perspectiva académica y de las tecnologías informáticas, a instituciones del estado como es la ANT, sobre posibles vulnerabilidades detectadas en su aplicativo, a fin de disponer de una herramienta que permita tomar decisiones en cuanto a procedimientos de seguridad a implementar para evitar ser objeto de accesos no autorizados hacia referida herramienta tecnológica de la entidad que usted la dirige.

Para el desarrollo del proyecto se plantea su ejecución desde el marco del Hacking ético, por lo que la metodología a emplearse es RMDE, la cual comprende las fases de reconocimiento, mapeo, descubrimiento y explotación, claro está que, al enmarcarse dentro de la ética profesional, no se ejecutará la fase de explotación, ya que la intención del proyecto es evidenciar posibles vulnerabilidades en el aplicativo web de la entidad, mas no es causar daños o inconvenientes a su normal funcionamiento.

Se propone emplear técnicas, herramientas, así como procedimientos para la obtención de resultados, los cuales serán evidenciados en un documento tomando como referencia la estructura de un modelo de informe pericial, empleado por peritos del Consejo de la Judicatura, ante la ejecución de un proceso técnico, documento que lo conozco de cerca ya que desempeñé la actividad en calidad de Perito Informático del Consejo de la Judicatura de Cotopaxi.

En cuanto a costos no se establecen para la entidad, por ser un proyecto eminentemente académico para un proceso de titulación, en lo referente a funcionalidad o espacio no se requiere interrumpir las actividades normales de la entidad o de su personal, ya que se realizará de forma externa.

En cuanto a la interacción con el aplicativo web, se establecerá contacto con el personal de tecnologías de la ANT, a fin de comunicar los espacios de tiempo en los cuales se efectuará las intervenciones y toma de resultados.

De lo referido, se destaca que el alcance del proyecto es entregar a la ANT, un documento en base a la estructura del informe pericial, el mismo que plasmará la descripción de las herramientas, técnicas, proceso y resultados obtenidos fruto de la aplicación de las fases de reconocimiento, mapeo, descubrimiento, con excepción de la fase de explotación, por el contrario, como aspecto final se abordarán recomendaciones inherentes a los resultados obtenidos en la fase de descubrimiento,

Agencia Nacional de Tránsito

Documento Nº : ANT-AC-2017-0882
Fecha : 2017-01-11 08:58:49 GMT -05
Recibido por : Angela Victoria Torres Moreno
Para verificar el estado de su documento ingrese a https://www.gestiondocumental.gob.ec con el usuario: "0502521032"

Dirección Ejecutiva

ANT-AC-2017-0882

disponiendo de una herramienta la cual puede ser de ayuda para el departamento de tecnologías en la toma de decisiones en cuanto al aplicativo web.

Debo indicar que al tratarse de un proyecto de titulación, los resultados obtenidos, mismos que arrojen información considerada confidencial, así como datos de configuración y los resultados de vulnerabilidades encontradas, no serán descritos de forma directa tanto en el informe del proyecto de titulación como en la respectiva sustentación, más se emplearán mecanismos para ocultar dichos datos al público, siendo entregados los resultados visible únicamente a la ANT en calidad de entidad de aplicación de dicho proyecto.

Por lo detallado, me dirijo hacia usted con la finalidad de solicitarle muy comedidamente, se digne autorizar la realización y ejecución del proyecto de titulación mencionado en la aplicación web de la Agencia Nacional de Tránsito.

Por la gentil y favorable atención que se digne dar a mi petición, anticipo y reitero mis agradecimientos.

Atentamente,

Ing. Raúl Alfredo Panchi Herrera.
C.I.:0502521032

Celular de contacto: 0984523738
Correo electrónico: raulalfredoph@gmail.com

Hoja de Ruta

Fecha y hora generación: 2017-07-23 23:23:10 (GMT-5)

Generado por: Raul Alfredo Panchi Herrera

Información del Documento			
No. Documento:	ANT-AC-2017-0882	**Doc. Referencia:**	S/N
De:	Ing. Raul Alfredo Panchi Herrera, Docente, SENECYT	**Para:**	Sr. Ing. John Charles Hill Peña, MBA, Director Ejecutivo (E), Agencia Nacional de Regulación y Control de Transporte Terrestre, Tránsito y Seguridad Vial
Asunto:	SOLICITA AUTORIZACION PARA REALIZACION Y EJECUCION DE PROYECTO DE TITULACION	**Descripción Anexos:**	--
Fecha Documento:	2017-01-11 (GMT-5)	**Fecha Registro:**	2017-01-11 (GMT-5)

Ruta del documento

Área	De	Fecha/Hora	Acción	Para	No. Días
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Maria Elizabeth Aguay Guaman (ANT)	2017-03-02 16:37:45 (GMT-5)	Archivar		50
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Maria Elizabeth Aguay Guaman (ANT)	2017-02-15 11:18:01 (GMT-5)	Responder a Todos		35
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Juan Carlos Gómez Paspuel (ANT)	2017-01-13 09:59:44 (GMT-5)	Reasignar	Maria Elizabeth Aguay Guaman (ANT)	2
DIRECCIÓN EJECUTIVA	John Charles Hill Peña, MBA (ANT)	2017-01-12 08:45:18 (GMT-5)	Reasignar	Juan Carlos Gómez Paspuel (ANT)	1
DIRECCIÓN EJECUTIVA	Denisse Lissette Peñafiel Medina (ANT)	2017-01-11 11:40:59 (GMT-5)	Reasignar	John Charles Hill Peña, MBA (ANT)	0
DIRECCIÓN EJECUTIVA	Denisse Lissette Peñafiel Medina (ANT)	2017-01-11 11:40:56 (GMT-5)	Asignación Carpeta Virtual		0
DIRECCIÓN EJECUTIVA	John Charles Hill Peña, MBA (ANT)	2017-01-11 09:28:26 (GMT-5)	Reasignar	Denisse Lissette Peñafiel Medina (ANT)	0
Atención al Cliente	Angela Victoria Torres Moreno (ANT)	2017-01-11 09:01:52 (GMT-5)	Envío Electrónico del Documento	John Charles Hill Peña, MBA (ANT)	0
Atención al Cliente	Angela Victoria Torres Moreno (ANT)	2017-01-11 09:01:52 (GMT-5)	Registro	John Charles Hill Peña, MBA (ANT)	0

Hoja de Ruta

Fecha y hora generación: 2017-07-23 23:24:55 (GMT-5)

Generado por: Raul Alfredo Panchi Herrera

Información del Documento			
No. Documento:	ANT-AC-2017-10723	**Doc. Referencia:**	S/N
De:	Ing. Raul Alfredo Panchi Herrera, Docente, SENECYT	**Para:**	Sr. Ing. Juan Carlos Gómez Paspuel, Director Tecnologías de la Información y Comunicaciones, Agencia Nacional de Regulación y Control de Transporte Terrestre, Tránsito y Seguridad Vial
Asunto:	EN ATENCION A OFICIO ANT-ANT.-2017-2223	**Descripción Anexos:**	--
Fecha Documento:	2017-04-03 (GMT-5)	**Fecha Registro:**	2017-04-03 (GMT-5)

Ruta del documento

Área	De	Fecha/Hora	Acción	Para	No. Días
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Juan Carlos Gómez Paspuel (ANT)	2017-05-17 22:39:18 (GMT-5)	Reasignar	Karla Candelaria Villalobos Lozano (ANT)	44
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Luis Anibal Untuña Palomo (ANT)	2017-05-17 11:24:10 (GMT-5)	Reasignar	Juan Carlos Gómez Paspuel (ANT)	44
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Juan Carlos Gómez Paspuel (ANT)	2017-05-08 17:16:43 (GMT-5)	Reasignar	Luis Anibal Untuña Palomo (ANT)	35
Atención al Cliente	Eduardo Xavier Mateus Callejas (ANT)	2017-05-05 09:18:15 (GMT-5)	Reasignar	Juan Carlos Gómez Paspuel (ANT)	32
Atención al Cliente	Estefany Carolina Murillo Flores (ANT)	2017-05-04 15:54:29 (GMT-5)	Reasignar	Eduardo Xavier Mateus Callejas (ANT)	31
Atención al Cliente	Estefany Carolina Murillo Flores (ANT)	2017-04-04 09:58:44 (GMT-5)	Informar	Luis Anibal Untuña Palomo (ANT)	1
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Juan Carlos Gómez Paspuel (ANT)	2017-04-04 09:26:44 (GMT-5)	Reasignar	Estefany Carolina Murillo Flores (ANT)	1
Atención al Cliente	Angela Victoria Torres Moreno (ANT)	2017-04-03 14:47:57 (GMT-5)	Envío Electrónico del Documento	Juan Carlos Gómez Paspuel (ANT)	0
Atención al Cliente	Angela Victoria Torres Moreno (ANT)	2017-04-03 14:47:57 (GMT-5)	Registro	Juan Carlos Gómez Paspuel (ANT)	0

Hoja de Ruta

Fecha y hora generación: 2017-07-23 23:26:37 (GMT-5)

Generado por: Raul Alfredo Panchi Herrera

Información del Documento			
No. Documento:	ANT-AC-2017-18021	**Doc. Referencia:**	S/N
De:	Ing. Raul Alfredo Panchi Herrera, Docente, SENECYT	**Para:**	Sr. Ing. Juan Carlos Gómez Paspuel, Director Tecnologías de la Información y Comunicaciones, Agencia Nacional de Regulación y Control de Transporte Terrestre, Tránsito y Seguridad Vial
Asunto:	SOLICITA AUTORIZACION PARA REALIZACION Y EJECUCION DE PROYECTO DE TITULACION	**Descripción Anexos:**	--
Fecha Documento:	2017-07-10 (GMT-5)	**Fecha Registro:**	2017-07-10 (GMT-5)

Ruta del documento

Área	De	Fecha/Hora	Acción	Para	No. Días
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Juan Carlos Gómez Paspuel (ANT)	2017-07-11 14:32:35 (GMT-5)	Reasignar	Christian Geovanny Soliz Sacaquirin (ANT)	1
Atención al Cliente	Angela Victoria Torres Moreno (ANT)	2017-07-10 09:42:38 (GMT-5)	Envio Electrónico del Documento	Juan Carlos Gómez Paspuel (ANT)	0
Atención al Cliente	Angela Victoria Torres Moreno (ANT)	2017-07-10 09:42:38 (GMT-5)	Registro	Juan Carlos Gómez Paspuel (ANT)	0

REFERENCIAS

Acurio, S. (s.f.). *OAS ORG.* Recuperado el 19 de Febrero de 2016, de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alegsa, L. (12 de 05 de 2010). *http://www.alegsa.com.ar/Dic/hacking.php*.

Arellano, D. (11 de 11 de 2015). *Tareas De Tics*. Obtenido de http://daniiela1234.blogspot.com/

Astudillo, K. (2013). *Hacking Ético 101.* Guayaquil: Seguridadinformáticafacil.

Aumaille, B. (2002). *J2EE Desarrollo de aplicaciones web.* Barcelona: ENI.

Aumaille, B. (202). *J2EE: Desarrollo de aplicaciones Web.* Madrid: Ediciones ENI.

Aviles, G. G. (2015). *SEGURIDAD EN BASES DE DATOS Y APLICACIONES WEB.* Madrid: Autor - Editor.

Balado, E. S. (2005). *Estrategias para la implmentación de nuevas tecnologías en PYMES.* Vigo: Ideas Propias.

Benchimol, D. (2011). *Hacking.* Buenos Aires: Desde Cero.

Berzal, F., Cortijo, F., & Cubero, J. (2013). *Desarrollo profesional de aplicaciones web con ASP.NET.* Alicante: Club Universitario.

Cardador, A. (2014). *Desarrollo de aplicaciones web distribuidas.* Málaga: IC Editorial.

Consejo de Europa. (2001). *Agencia Española de Protección de Datos.* Recuperado el 19 de Febrero de 2016, de www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/

De Miguel Molina, M. d., & Oltra Gutiérrez, J. V. (2007). *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia: Universidad Politécnica de Valencia, Escuela Técnica Superior de Informática.

Estrada, A. C. (2011). *Seguridad por niveles.* Madrid: DarFE Learning & Consulting S.L.

Fiscalía General del Estado. (13 de Junio de 2015). *Fiscalía General del Estado.* Recuperado el 14 de Enero de 2016, de Los delitos informáticos van desde el fraude hasta el espionaje: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Gaibor, A. (2007). *REPOSITORIO DIGITAL EPN.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

Gómez, H. R. (2007). *El periodista digital Mexicano: hacia su definición.* Obtenido de https://books.google.com.ec/books?id=Ze6Ua6CRoLIC&printsec=frontcover&hl=es#v=onepage&q&f=false

Gómez, V. (04 de Abril de 2015). *Desarrollo Geek*. Obtenido de https://desarrollo-geek.net/sistemas-operativos/linux/soft-linux/los-mejores-8-scanners-de-vulnerabilidades-web/

Huércano Ruiz, F., & Villar Cueli, J. (2015). *Desarrollo de componentes software para servicios de comunicaciones.* Málaga: IC.

Jake Kouns, D. M. (2011). *Information Technology Risk Management in Enterprise Environments.* Nueva York: John Wiley & Sons.

Jara, H., & Pacheco, F. (2012). *Ethical hacking 2.0.* Buenos Aires: Fox Andina.

Lenin, S. Y. (03 de 2014). *http://repositorio.espe.edu.ec/handle/21000/8246.*

Levy, S. (2001). *Hackers: Heroes of the Computer Revolution.* Pensilvania: Penguin Books, 2001.

Lujan, S. (2012). *Programación de aplicaciones web: historia, principios básicos y clientes web.* Alicante: Club Universitario.

María del Rosario de Miguel Molina, J. V. (2007). *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia: Universidad Politécnica de Valencia, Escuela Técnica Superior de Informática.

Mateu, C. (2004). *Desarrollo de aplicaciones web.* Catalunya: Universidad de Catalunya.

Medina, J. (2014). *Evaluación de vulnerabilidades TIC.* Murcia: Laderas del Campillo.

Medina, M., & Molist, M. (2015). *Cibercrimen.* Catalunya: Tibidabo.

Michael E. Whitman, H. J. (2015). *Guide to Network Security.* Boston: Cengage Learning.

Ministerio de Justicia Derechos Humanos y Cultos. (2014). *justicia.gob.ec.* Recuperado el 15 de Enero de 2016, de Código Orgánico Integral Penal: http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Ministerio de Justicia, Derechos Humanos y Cultos. (2014). *Código Orgánico Integral Penal.* Recuperado el 19 de Febrero de 2016, de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Miño, J. (2010). *Aplicaciones web.* Barcelona: Editex.

Miño, J. (2011). *Servidores de aplicaciones web.* Madrid: Editex. Recuperado el 19 de Febrero de 2016

Moral, L. G. (2014). *Curso de Ciberseguridad y Hacking Ético 2013.* Sevilla: Punto Rojo Libros, S.L.

Ortiz, S. (9 de Enero de 2016). *El Comercio*. Obtenido de http://www.elcomercio.com/actualidad/hackers-registraron-titulos-universitarios-falsos.html

OWASP. (2013). *OWASP Top 10 - 2013.* Recuperado el 10 de Enero de 2016, de Los diez riesgos más críticos en aplicaciones web: https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

OWASP. (22 de Febrero de 2016). *Vulnerability Scanning Tools*. (OWASP) Recuperado el 25 de Febrero de 2016, de https://www.owasp.org/index.php?title=Category:Vulnerability_Scanning_Tools&setlang=es

Palmer, S. (2011). *Web Application Vulnerabilities: Detect, Exploit, Prevent.* Massachusett: Syngress.

Policía Nacional del Ecuador. (8 de Enero de 2016). *Policía Nacional del Ecuador.* Recuperado el 10 de Enero de 2016, de Desarticulada red de hackers que vulneraba sistemas de entidades bancarias y públicas: http://www.policiaecuador.gob.ec/desarticulada-red-de-hackers-que-vulneraba-sistemas-de-entidades-bancarias-y-publicas/

Ramos, A. (2011). *Aplicaciones Web.* Madrid: S.A. EDICIONES PARANINFO. Recuperado el 16 de Enero de 2016, de https://books.google.com.ec/books?id=LXs3YlMoeNgC&printsec=frontcover&dq=aplicaciones+web&hl=es-419&sa=X&ved=0ahUKEwiY0cb1rbfLAhXD7SYKHQB6BaEQ6AEIIDAB#v=onepage&q=aplicaciones%20web&f=false

Rando, E., & Alonso, C. (2014). *Hacking de Aplicaciones Web: SQL Injection.* Barcelona: Informática64.

Razo, C. M. (2012). *Auditoría en sistemas computacionales.* Naucalpan de Juárez: Pearson Educación de México, S. A.

Rojas, D. (2014). *Academia edu.* Recuperado el 18 de Febrero de 2016, de https://www.academia.edu/6761612/HACKEO_ETICO_EN_EL_ECUADOR

Varon, R., Ángel, A., Muñoz, B., Sánchez, R., & García, Á. (2013). *HACKING Y SEGURIDAD DE PÁGINAS WEB.* Barcelona: RA-MA.

Vértice, P. (2010). *Técnicas avanzadas de diseño web.* Málaga: Vértice S.L.

Wilhelm, T. (2013). *Professional Penetration Testing.* Newnes: Syngress.