Análisis de vulnerabilidades mediante pruebas de penetración avanzada *pentesting* al sitio web oficial de la alcaldía del municipio de Quibdó – Chocó

Presentado por:

Ing. Carlos Andrés Cautín García

Universidad Nacional Abierta y a Distancia

"UNAD"

Escuela de Ciencias Básicas Tecnología e Ingenierías

ECBTI

Especialización en Seguridad Informática

Quibdó-Chocó

2019

Análisis de vulnerabilidades mediante pruebas de penetración avanzada *pentesting* al sitio web oficial de la alcaldía del municipio de Quibdó – Chocó

Presentado por:

ING. Carlos Andrés Cautín García

Trabajo de Grado para optar el Título de Especialista en seguridad Informática

Director: Ing. Jorge Enrique Ramírez Montanez

Universidad Nacional Abierta y a Distancia

“UNAD”

Escuela de Ciencias Básicas Tecnología e Ingenierías

ECBTI

Especialización en Seguridad Informática

Quibdó-Chocó

2019

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

Introducción

Actualmente la información es el mayor activo para las instituciones, en especial para las instituciones estatales en las que la imagen y el prestigio son recursos intangibles, que, al ser afectados, se pierde la reputación y la confianza de los usuarios, generando descontento en los diferentes niveles de la organización, autoridades superiores del Gobierno y los propios funcionarios y usuarios de los servicios. Según la estrategia de gobierno en línea 3.1 2012 – 2017:

> La implementación de la estrategia gobierno en línea en Colombia por el conjunto de entidades públicas ha generado logros muy importantes, tales como el incremento en la provisión de trámites y servicios por medios electrónicos, la mejora en la calidad de la información de las entidades públicas en sus sitios web y la apertura de espacios de participación, entre otros. Gracias al Gobierno en línea, los colombianos tienen acceso a la información pública en los sitios web del Estado, lo cual incluye a entidades de todas las ramas del poder público del orden nacional y al 100% de los municipios y departamentos de Colombia. Asimismo, el país ha mejorado en las mediciones internacionales, relacionadas con la implementación de servicios en línea y en participación electrónica. (p. 15).

La alta importancia de la información de las entidades y empresas, sean públicas o privadas, genera gran interés para cometer delitos informáticos por parte de los diferentes intrusos expertos en informática y comunicaciones, Por lo cual, los administradores de red deben mitigar al máximo los riesgos mediante la implementación de técnicas que permitan la detección de vulnerabilidades de la infraestructura de red y los diferentes servicios tecnológicos.

En el presente trabajo se realizara un diagnóstico de alto nivel sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó www.quibdomia.com se ejecutaran unas pruebas de penetración de caja negra bajo una metodología que define un conjunto de reglas, prácticas, procedimientos y métodos utilizando las

herramientas que contiene la distribución de software libre Kali Linux, es necesario tener en cuenta que inicialmente no se tiene conocimiento sobre la infraestructura de red de la organización, por lo tanto se realizaran pruebas externas a nivel web solo con el detalle de la URL e intentando interrumpir en el sitio web o red de la organización simulando ataques externos realizados por un atacante malicioso.

Para realizar el diagnóstico y las pruebas de penetración, el administrador de red requiere aplicar conocimientos avanzados en infraestructura de redes, seguridad informática, protocolos TCP / IP y habilidades razonables en uso de sistemas operativos Linux derivados de Debían.

CAPÍTULO 1

1. PROBLEMA DE INVESTIGACIÓN

En este capítulo se presenta el problema de investigación, sus antecedentes sus objetivos y por último su justificación.

1.1. Antecedentes del problema

El municipio de Quibdó es la capital del departamento del Chocó y una de las poblaciones más importantes de la región del pacífico colombiano. La ciudad está ubicada en una de las zonas más forestales del país, lindante de grandes reservas ecológicas e indígenas. La alcaldía del municipio de Quibdó es una entidad de orden territorial que presta sus servicios públicos en favor de la comunidad, como institución autónoma se encarga de diseñar, promover y ejecutar actividades políticas, recreacionales, sociales, culturales y económicas plasmadas en su plan de desarrollo para satisfacer las necesidades de sus ciudadanos.

La institución en medio de la implementación de la estrategia gobierno en línea ha logrado implementar algunos trámites, servicios y espacios de participación por medio de su sitio web, permitiendo a sus ciudadanos tener facilidades de acceso a la información de interés general. La importancia de la información que reposa en el sitio, los continuos ataques informáticos que se realizan a los diferentes sitios estatales, la continua actualización de técnicas para realizar ataques, la debilidad en la infraestructura tecnológica de la alcaldía, la deficiente política de seguridad

informática y la falta de implementación del sistema de seguridad de la información, generan la necesidad de utilizar herramientas y estrategias que permitan incrementar los niveles de confidencialidad, integridad y disponibilidad de la información.

Según el espectador en la sección de Tecnología, publicado el 20 Oct 2014, manifiesta que:

> Colombia lidera la lista de ataques informáticos en países de habla hispana, en el informe anual realizado por Digiware, primer integrador de seguridad informática de Latinoamérica se reveló que Colombia es el país de habla hispana que genera más ataques informáticos en Latinoamérica, luego siguen Argentina, Perú, México y Chile. El informe muestra que los sectores más atacados en términos generales son: el Gobierno, los bancos y las empresas de comunicaciones. Además se explica que hay tres factores principales para que Colombia concentre una alta cifra de generación de ataques, al ser colombianos tendemos a tener una gran capacidad de creatividad, el segundo tema tiene que ver con capacidades técnicas que tiene el personal para desarrollar ataques y el uso de inglés. (Redacción Tecnología)

1.2. **Descripción del problema’**

Un ataque informático al sitio web de la alcaldía puede implicar pérdida o alteración de información, denegación de servicios, sabotajes, lentitud o intermitencia en la navegación del sitio, suplantación de identidad de funcionarios, phishing y otras situaciones que impedirían el correcto funcionamiento del sitio y los servicios en línea prestados por la entidad. Fue así como le sucedió a la Asociación Civil Convite (Venezuela) que el pasado 12 de agosto de 2018, denunció que su página web fue víctima de un ataque informático:

> Lamentamos informar que nuestra página web del Directorio de Entidades de Atención de Personas Mayores sufrió un cuarto ataque informático y esta vez fue exitoso, lograron borrar TODA la información, sin embargo contamos con respaldo, tocara volver a hacer la página NO NOS RENDIMOS1. — Convite A.C (@conviteac)

De no realizarse un diagnóstico de alto nivel sobre el estado actual de seguridad del sitio web y unas pruebas de penetración de caja negra, la alcaldía de Quibdó no podría identificar y caracterizar los diferentes ataques a los que está expuesto y no podrá implementar controles que reduzcan las vulnerabilidades de la información almacenada en su sitio web, ante un posible ataque se podría afectar la imagen y credibilidad de la institución.

1.3. **Planteamiento del problema**

¿Cómo se puede realizar una medición de los niveles de seguridad y caracterización de los posibles ataques informáticos, a los que está expuesta la información publicada en el sitio web de la alcaldía del municipio de Quibdó?

1.4. **Objetivos**

1.4.1. **General**

Realizar un análisis de vulnerabilidades mediante pruebas de penetración avanzada *pentesting* al sitio web oficial de la alcaldía del municipio de Quibdó – Chocó.

1.4.2. **Específico**

- Realizar un diagnóstico de alto nivel sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó.

- Ejecutar pruebas de penetración de caja negra al sitio web de la alcaldía de Quibdó utilizando las herramientas que contiene la distribución de software libre Kali Linux.
- Generar un informe de seguridad informática donde se Identifican los diferentes ataques a los que está expuesto el sitio web y los servicios en línea que presta la alcaldía de Quibdó.
- Proponer controles que reduzcan las vulnerabilidades del sitio web de la alcaldía de Quibdó.

1.5. **Justificación del problema**

El desarrollo de este proyecto de grado le permitirá a la Alcaldía del Municipio de Quibdó, contar con un sitio web y servicios en línea seguros, garantizando que su información permanezca confiable, íntegra y disponible para los usuarios internos y externos.

El diagnóstico de alto nivel sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó www.quibdomia.com permitirá tener una bitácora de datos con aspectos tanto internos como externos de la página que abarcan situaciones técnicas y legales. Toda esta información será de gran utilidad para los administradores de red de la institución para mejorar tiempos de respuestas en los momentos de ejecutar procesos de respaldo o restauración ante fallos en la plataforma.

Los análisis de vulnerabilidades determinaran la seguridad con la que cuenta el sitio web y el servidor de alojamiento “Hosting” donde se encuentra hospedado, se utilizaran pruebas de caja negra con herramientas de Kali Linux con las que se ejecutaran los distintos tipos de ataques informáticos que realizaría en su actualidad un intruso del tipo hacker o cracker con solo conocer su dirección web e IP, pero sin arriesgar la integridad de la información y la disponibilidad de la plataforma, esto se realiza con el fin de encontrar las posibles vulnerabilidades a las que está expuesto el sitio web antes de que las descubra un atacante real.

Durante la ejecución del análisis de vulnerabilidades se ejecutarán procesos para intentar acceder a la administración del sitio web y obtener el control total de todos los servicios activos. Mantener seguro el sitio web de la alcaldía de Quibdó, facilitara el cumplimiento de las metas establecidas por la estrategia gobierno en línea en Colombia, se podrán garantizar la disponibilidad de la información, el acceso a los trámites y servicios en línea ofrecidos por la entidad.

Los informes generados por este proyecto servirán como insumo para la implementación de políticas de seguridad informática y la aplicación del sistema de gestión de seguridad de la información bajo la norma ISO 27001.

Identificadas las posibles vulnerabilidades del sitio web, el administrador de red podrá aplicar una serie de controles que le permitirán mitigar los riesgos y poder prevenir posibles ataques informáticos, además de capacitar a los funcionarios que tienen cuentas de usuario para administrar el portal en temas de seguridad

informática. Finalmente, se generará confianza en el personal interno y externo a la alcaldía por que se garantizará la integridad de la información que se encuentra publicada en el sitio web.

CAPÍTULO 2

2. MARCO REFERENCIAL

A continuación, se expondrán los componentes teóricos que permitieron realizar un análisis de vulnerabilidad mediante pruebas de penetración avanzada *pentesting* al sitio web oficial de la alcaldía del municipio de Quibdó, a fin de fundamentar adecuadamente la investigación.

2.1. Marco contextual

El Departamento de Chocó está situado en el Noroccidente de Colombia, en la región del Pacífico; Políticamente dividido en 30 municipios, cuenta con una población aproximada de 500.093 habitantes distribuidos porcentualmente en: afrodescendientes 82,1%, Mestizos 5,2%, indígenas: 12,7% (DANE, 2015).

Su capital es el municipio de Quibdó, la cual tiene una superficie de 3.338 km2 y una población de 126.384 habitantes, la cual representa el 32% del total del departamento. El 65% se encuentran en el área urbana y el 35% en área rural.

Mena, Bejarano, & Palacios, (2013), se tiene que, según registros de la Secretaría de Planeación Municipal, el Municipio de Quibdó posee en el casco urbano un perímetro aproximado de 425 hectáreas, delimitada por una longitud calculada en 11 km. Distribuida inicialmente mediante Acuerdo No. 014 del 6 de diciembre de 1979, en 28 barrios, posteriormente, mediante acuerdo 26 de 1987,

considerando el crecimiento de la ciudad y el aumento de las viviendas, se anexaron 6 barrios más.

Quibdó posee un índice de ruralidad de 47.34%, ocupando el puesto 2 dentro del departamento y está constituido por 28 corregimientos, 14 veredas, 13 resguardos indígenas, 6 comunas urbanas y 74 barrios en la zona urbana.

Las actividades económicas predominantes en el municipio están ligadas principalmente al sector terciario (servicio y comercio y recientemente la construcción) para la zona urbana, y al sector primario (agricultura, pesca, ganadería, actividad forestal y minería) en el área rural.

2.2. **Marco teórico**

- **Red de ordenadores**

Según el Diccionario de Informática y Tecnología, Alegsa, (1998) la red de ordenadores es: “Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico. La red de computadoras más grande y difundida en la actualidad es Internet. Para comunicarse entre sí en una red el sistema de red utiliza protocolos de red. Los dispositivos de una red de computadoras que: originan, enrutan o reciben los datos, son llamados nodos. Cada nodo puede incluir hosts como computadoras personales, teléfonos, servidores y dispositivos de hardware de red”.

En la actualidad una red de ordenadores puede clasificarse de la siguiente manera:

De acuerdo con la extensión:

- LAN: red de área local
- MAN: red de área metropolitana
- WAN: red de área amplia
- PAN: red de área personal
- SPL: red de área simple
- SAN: red de área de almacenamiento
- NANORED: Red a nano escala
- CAN: red de área de campus
- GAN: red de área global

De acuerdo con la función de los nodos:

- Red Cliente/Servidor
- Redes de igual a igual P2P (peer to peer)

De acuerdo con la topología:

- Malla
- Estrella

- Bus
- Anillo
- Árbol

De acuerdo con el medio de transmisión:

- Red cableada: conectadas con cables eléctricos, cable coaxial, par trenzado, línea telefónica y líneas de energía y fibra óptica.
- Red Inalámbrica: conectadas por ondas de radio, microondas terrestres, comunicaciones satelitales, celulares, comunicaciones ópticas por espacio libre.

- **Internet**

El concepto de internet es conocido como red de redes, puesta que es la red de ordenadores más grande del mundo y se encarga de interconectar la mayoría de los dispositivos utilizando el protocolo TCP/P independientemente de los medios de conexión, con el objeto de compartir una infinidad de recursos.

Para acceder a los servicios de internet los usuarios deben adquirir el servicio mediante una compañía proveedora de servicios de Internet ISP, la cual suministrará mediante sus diferentes dispositivos de Red los servicios de enrutamiento y configuración TCP/IP para comunicar el dispositivo con los diferentes servicios que ofrece internet.

Para acceder a un sitio web, es necesario digitar en un navegador web la dirección IP del sitio o el nombre de dominio para que un servidor DNS la traduzca y la localice, una vez realizado este proceso totalmente transparente para el usuario, el mismo podrá visualizar el contenido en su dispositivo.

En la actualidad los principales servidores de internet están en las universidades, empresas, instituciones públicas y Hosting de pago o gratuitos, aunque realizar la configuración como servidor es tan sencilla que cualquier persona puede realizar el proceso y compartir información en la web desde su propio dispositivo.

Teniendo en cuenta que en internet circula información tanto privada como pública, es necesario utilizar diferentes métodos de seguridad para evitar que la información caiga en destinatarios no deseados que la puedan utilizar para actividades ilícitas. Se pueden utilizar tecnologías para encriptamiento de la información, firewall, UTM, VPN, entre otros.

El internet se caracteriza por estar casi por todo el planeta, es fácil de usar, variedad de contenido, económico, útil, libre, anónima, autorregulada, sin verificar, segura, con crecimiento vertiginoso, funciona como motor de cambios

- **Sitio web**

Un sitio web es un conjunto o directorio de sitios web enlazados entre sí y alojados en un servidor configurado como hosting e identificado con un nombre de

dominio, que tienen como objetivo publicar información o realizar trámites, transacciones y procedimientos desde cualquier sitio remoto.

Hoy en día un sitio web no es una moda, teniendo en cuenta la evolución tecnológica, se ha convertido en una necesidad para cualquier institución, empresa y hasta personas tener un sitio web propio, que permita mostrar información, productos o servicios a usuarios, clientes y proveedores en cualquier parte del mundo sin importar horarios ni fechas.

Para el funcionamiento de un sitio web es necesario contar con un servidor de nombres de dominios DNS que permita resolver los nombres de dominios e indicando la ubicación de estos.

De acuerdo con los servicios contratados con el Hosting donde se aloja el sitio web, así será el rendimiento y prestaciones del sitio ante las visitas de los usuarios.

Cada sitio web publicado en internet posee un nombre de dominio único, que lo identificara cada vez que sea digitado en un navegador web y así poder desplegar la información alojada en el sitio. Por ejemplo, el dominio del sitio web de la universidad nacional abierta y a distancia UNAD es www.unad.edu.co.

Otra forma de acceder a contenidos publicados en internet es mediante el protocolo de transferencia de Ficheros FTP, el cual permite cargar o descargar los ficheros del sitio Web en el hosting.

- **Servidor web**

Un servidor web es un programa que permite administrar las aplicaciones alojadas en el servidor para dar respuesta a las peticiones realizadas por el cliente, el código enviado por el cliente al servidor es interpretado, compilado y ejecutado desde un navegador o visor web mediante el protocolo HTTP. Por ejemplo, el cliente podría realizar peticiones mediante un gestor de correo electrónico como thunderbird o Microsoft Outlook y, el servidor devuelve los datos en forma de correos electrónicos respondiendo a la solicitud.

El principal servidor web o el más utilizado es el software libre APACHE y puede ser instalado en cualquier equipo y proveer servicios web con tan solo estar conectado a la red.

Cuando se administra un sitio web se sugiere tener configurado el sitio en un servidor local que permita comprobar las actualizaciones de diseños o bases de datos antes de cargarlas al servidor web remoto, de tal manera que evitemos errores que afecten los servicios ofrecidos en el sitio web, nos permite tener un Backus o copia de seguridad del sitio y nos facilita el proceso de carga y actualización al hosting.

Un Servidor de Aplicaciones es un servidor web de alto rendimiento orientado a servir a sitios web con grandes requerimientos, cantidad de conexiones, consultas a bases de datos, transferencias, cargas y descargas de información.

Cuando hablamos de servidores web es necesario aclarar los servicios de las aplicaciones del lado del servidor, las cuales son algoritmos o programas desarrollados para procesar o realizar alguna acción. Estas aplicaciones están escritas mediante lenguajes de programación como PHP, ASP, Perl, Python, Ruby, entre otros.

- **Servidores más usados**

A continuación, se muestra un listado de los servidores web más utilizados actualmente:

Apache. Es una aplicación desarrollado por la comunidad del software y se ha diseñado para ser un servidor web potente, flexible y multiplataforma gracias a su diseño modular. Estas características, hacen que frecuentemente sean necesarias diferentes características o funcionalidades. El software Apache es totalmente parametrizable por el administrador de red, permitiendo habilitar o deshabilitar funcionalidades de acuerdo con las necesidades del sitio, también permite realizar una selección, revisión, modificación de sus módulos para posteriormente compilarlo y/o ejecutarlo, por estas razones es el servidor más utilizado en la actualidad en la Internet. Por el hecho de ser software libre y gratuito, ha permitido que desarrolladores de todo el mundo puedan colaborar y dar soporte para actualizaciones permanentes, lo que ha logrado que sea multiplataforma, multilenguaje y con múltiples comunidades para términos de soporte.

Microsoft IIS. IIS (*Internet Information Server*), es el servidor web que ofrece la compañía Microsoft a modo profesional, En él es posible programar en el lenguaje ASP (Active Server Pages, Páginas de Servidor Activo) las cuales son algo similares a las generadas mediante el lenguaje libre PHP, este servidor cuenta con componentes programables desde ASP si se accede a los módulos para funciones específicas. Una de las principales limitantes de este servidor web es que solo puede ser instalado en sistemas operativos de Microsoft.

Sun Java System Web Server. El servidor *Sun Java System Web Server* es de alto rendimiento, escalable y seguro, ofrece contenido dinámico y estático. Cuenta con características de virtualización de dominio, variabilidad de configuración y seguridad robusta, brindando una mejor calidad de servicio.

- **Seguridad informática**

De acuerdo con los avances tecnológicos actuales y el uso masivo del internet, ha sido necesario que tanto socios, proveedores, empleados y clientes puedan interactuar con los recursos de la compañía por medios remotos como el internet, por tal motivo ha sido necesario aplicar una serie de controles para el acceso a los sistemas de información que permitan que los datos se mantengan confiables, íntegros y disponibles en tiempo real.

Teniendo en cuenta tendencias como el teletrabajo y factores como los estilos de vida nómada, problemas de movilidad y trabajos necesarios casi de manera instantánea ha sido necesaria la implementación de estrategias y herramientas que

permitan a los empleados acceder a partes de los sistemas de información fuera de la infraestructura física de las compañías, generando riesgos que de no controlarse colocan en riesgo la seguridad de la información.

En términos de seguridad, los riesgos se caracterizan por lo general utilizando la siguiente ecuación.

$$Riesgo = \frac{Amenaza\ x\ Vulnerabilidad}{Contramedida}$$

En el contexto de seguridad informática, una amenaza es cualquier tipo de acción que puede generar daños, una vulnerabilidad es el nivel de exposición a las amenazas en un contexto particular; una contramedida son los controles implementados previniendo las amenazas, los cuales deben ser implementados con soluciones técnicas y con capacitación y sensibilización a los usuarios de los sistemas.

Para catalogar un sistema como seguro, se deben identificar las posibles amenazas, conocer y prever las posibles acciones de un intruso. Por tanto, es necesario estar al tanto de las posibles motivaciones de los atacantes, categorizarlas, y estudiar su funcionamiento para conocer la mejor forma de mitigar el riesgo de intrusiones.

- **Objetivos de la seguridad informática**

Normalmente, los sistemas de información incluyen los datos de la compañía y también se encuentran en los materiales y recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Por lo tanto, estos sistemas de información son fundamentales y deben ser protegidos y usados únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume generalmente en tres objetivos principales:

Integridad. Garantizar que los datos sean los que se supone que son.

Confidencialidad. Asegura que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.

Disponibilidad. Garantizar el correcto funcionamiento de los sistemas de información

- **Cómo implementar una política de seguridad**

Las seguridades de los sistemas informáticos concentran gran parte de sus actividades en garantizar el correcto acceso a datos y recursos de sistemas por medio de controles de autenticación de los usuarios con sus respectivos roles y permisos. Por esta razón, uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

- Identificación de las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía y sus posibles consecuencias.
- Proporcionar una perspectiva general de las reglas y los protocolos que deben implementarse para mitigar los riesgos.
- Controlar y detectar las vulnerabilidades del sistema de información.
- Definir las acciones a realizar y las personas a contactar en caso de amenazas.

Una verdadera política de seguridad informática debe ser liderada principalmente por la dirección general de las instituciones o empresas, no se debe dejar toda la responsabilidad en los administradores de sistemas, puesto que están capacitados técnicamente, pero a la hora de la toma de decisiones e implementación de estrategias deben estar acompañadas por las políticas definidas por la organización.

La correcta implementación de la seguridad informática y la seguridad de la información de una compañía en gran parte depende de que los usuarios tengan conocimiento de las reglas a través de sesiones de capacitación y sensibilización que cubran las áreas de:

- Seguridad física y lógica de la información de la organización.
- Procesos y procedimientos para las actualizaciones.
- Estrategia de copias de seguridad (backup).
- Plan de recuperación de desastres.

- Sistemas de información documentados y actualizados.

2.3. **Marco histórico**

Para realizar pruebas de penetración *pentesting* se necesita conocer una serie de procedimientos para ejecutar actividades que identifican las vulnerabilidades que se pueden explotar y los daños que se podrían ocasionar en una infraestructura objetivo. Es necesario realizar un proceso de Hacking ético para caracterizar las posibles incidencias antes que sucedan y luego reparar o mejorar los sistemas y su infraestructura para evitar los ataques. Las siguientes son otros trabajos de investigación relacionados con el tema que fueron revisados previamente a este documento:

REFERENCIA BIBLIOGRÁFICA	
Título:	PRUEBAS DE PENETRACIÓN O PENT TEST
Autor:	RAMOS RAMOS, Jorge Luis.
Temas:	Ethical Hacker, test de penetración, Black-box, White-box, Gray-box
En:	Revista de Información, Tecnología y Sociedad, 2013, n.8, pp. 31-33. ISSN 1997-4044 http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100014&script=sci_abstract

Descripción:	En este artículo se pudo evidenciar que los ethical hackers son personas, dispositivos o redes de computadoras dedicadas a detectar debilidades o vulnerabilidades de sistemas informáticos, para luego atacarlos con la autorización de sus propietarios, para así poder encontrar alguna falla que los verdaderos atacantes puedan utilizarlos, es por lo que surge la necesidad de desarrollar esto que se conoce como pruebas de penetración o Pent Test.

REFERENCIA BIBLIOGRÁFICA	
Título:	Laboratorio Virtualizado de Seguridad Informática con Kali Linux
Autor:	Gutiérrez Benito, Fernando
Temas:	Kali Linux; Proxmox; investigación, pruebas y documentación de Ettercap, Zaproxy, Hydra y Maltego
En:	Biblioteca universitaria UVa, 2014, Trabajos Fin de Grado Uva: http://uvadoc.uva.es/handle/10324/5792

Descripción:	Este proyecto construyo un laboratorio de seguridad informática virtualizado con el software libre PROXMOX, los alumnos conocieron la importancia de la seguridad y la capacidad de administrar las aplicaciones, redes y sistemas de la forma más segura posible.

REFERENCIA BIBLIOGRÁFICA	
Título:	Explotación de vulnerabilidades web a través de DVWA
Autor:	Novella Román, José Carlos
Temas:	Web; SQL injection; DVWA; WegGoat; Pen-Testing
En:	Biblioteca digital universidad de Alcalá, 2015, p.154, http://dspace.uah.es/dspace/handle/10017/23220
Descripción:	Este proyecto realizo una descripción detallada de las herramientas usadas para análisis de seguridad, usando herramientas de vulnerabilidades web, entre las que destacan DVWA y WebGoat. Ambas herramientas son aplicaciones inseguras, diseñadas para que los usuarios pudieran practicar las diferentes vulnerabilidades que

	pueden darse en las páginas web. El objetivo final de este proyecto fue dar a conocer algunas vulnerabilidades, para así crear páginas web seguras.

REFERENCIA BIBLIOGRÁFICA	
Título:	Desarrollo e implementación práctica de un PENTEST
Autor:	Martí Talón, Rafael Manuel
Temas:	Seguridad informática; Auditoría; Penetration test; Máquinas virtuales; Hacking; Security.
En:	Repositorio Universidad Politécnica de Valencia, 2016, p.51, http://hdl.handle.net/10251/70164
Descripción:	Con este proyecto se buscó mostrar una visión muy general de las etapas que se ejecutan en una auditoria de seguridad informática profesional, enumerando las herramientas más utilizadas por cada fase. Se comenzó con la ejecución de pruebas de penetración estándar utilizando herramientas actualizadas, además se incluyó una sección con los lugares desde donde se practica el *pentest* de manera gratuita y otra fase donde se pone a

	prueba la metodología utilizando maquias virtuales vulnerables que se encuentran disponibles en internet.

2.4. **Marco normativo**

Para la implementación de este proyecto se debe obligatoriamente cumplir con las leyes, normas y decretos que sean aplicables en el desarrollo de las actividades. En lo referente específicamente a Seguridad informática, estas son las Leyes nacionales e internacionales vigentes a la fecha:

2.4.1. **Normatividad Internacional**

Estándar ISO/IEC 17799

“Debido a la necesidad de hacer segura la información que poseen las organizaciones era necesaria la existencia de alguna normativa o estándar que acogiera todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudieran afectarla, por esta necesidad apareció el BS 7799, o estándar para la gestión de la seguridad de la información, el cual es un estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la organización. Esta normativa británica acabó desembocando en la actual

ISO/IEC 17799:2000 – Code of Practice Information Security Management" (Jolman 2012)

ISO/IEC 17799 (también ISO 27002) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization For Standardization y por la Comisión International Electrotechnical Commission en el año 2000 y con el título de Information Technology - Security Techniques - Code of Practice For Information Security management. La actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

Estándar ISO/IEC 27001

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Los activos de información pueden impulsar o destruir una institución o empresa. Si se gestionan correctamente se genera un ambiente de confianza al trabajar. Una buena administración de la seguridad de la información ofrece posibilidades de

crecer, innovar y ampliar la base de clientes y usuarios sabiendo que toda su información continuara siendo confidencial, integra y se encontrara disponible.

La implementación de un Sistema de Gestión de Seguridad de la Información SGSI es la forma más eficaz de minimizar los riesgos, puesto que nos aseguramos de q identificar y valorar los activos y sus riesgos, determinando el impacto para la organización, por lo tanto, se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de la institución o empresa.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Estándar ISO/IEC 27000:2009

El estándar ISO/IEC 27000:2009 hace parte de una familia en crecimiento de Estándares para Sistemas de Administración de Seguridad de la información (ISMS), las series ISO/IEC 27000.

ISO/IEC 27000, es un estándar internacional titulado “Tecnología de la Información – Técnicas de Seguridad – Sistemas de Administración de la Seguridad de la Información – Visión general y Vocabulario”.

El estándar fue desarrollado por el sub-comité 27 (SC27) del primer Comité Técnico Conjunto (JTC1), de la ISO (International Organization for Standardization) y el IEC (International Electrotechnical Commission).

ISO/IEC 27000 provee:

- Una vista general a la introducción de los estándares de la familia ISO/IEC 27000
- Un glosario de términos usados a lo largo de toda la familia ISO/IEC 27000

“La Seguridad de la Información, como muchos otros temas técnicos, está desarrollando una compleja red de terminología. Relativamente pocos autores se toman el trabajo de definir con precisión lo que ellos quieren decir, un enfoque que es inaceptable en el campo de los estándares, porque puede potencialmente llevar a la confusión y a la devaluación de la evaluación formal y la certificación.” (Seguridad Informática 2014).

El alcance de ISO/IEC 27000 es especificar los principios fundamentales, conceptos y vocabulario para la serie de documentos ISO/IEC 27000.

ISO/IEC 27000 contiene:

- Una vista general de los estándares ISO/IEC 27000, mostrando cómo son usados complementariamente para planear, implementar, certificar, y operar un Sistema de Gestión de Seguridad de la información, con una introducción básica a la Seguridad de la Información, administración de riesgos, y sistemas de gestión.

- Definiciones para temas relacionados con seguridad de la información.

- ISO/IEC 27000 es similar a otros vocabularios y definiciones y con suerte se convertirá en una referencia generalmente aceptada para términos relacionados con seguridad de la información entre esta profesión.

2.4.2. **Normatividad Nacional**

Ley 1273 del 2009 Delitos Informáticos

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.” (Secretaria general de la Alcaldía Mayor de Bogotá 2009) Dicha ley decreta:

Capítulo I:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático.

- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático.

- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.

- Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos.

- Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile,

sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

Es de tener en cuenta que el artículo 269H incluye que los delitos anteriores pueden ser agravados y generan un aumento de la pena entre la mitad y tres cuartas partes si se comenten las siguientes acciones:

- Sistemas de información y/o redes estatales u oficiales o del sector financiero, con cobertura nacional o internacional.

- Un servidor público en ejercicio de sus funciones

- Abuso de confianza como poseedor de la información o con vínculo contractual con el mismo.

- Revelar datos o contenido de la información en perjuicio de otro.

- Obteniendo provecho propio o para un tercero.

- Información utilizada con fines terroristas o poniendo en peligro la seguridad nacional.

- Asaltando en su buena fe a un tercero.

- Si el responsable de la administración, manejo o control de la información es quien incurre en la conducta, también se le incrementara hasta por 3 años la pena de inhabilidad para ejercer la profesión relacionada con sistemas de información.

Capitulo II:

De los atentados informáticos y otras infracciones:

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante.

- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.

CAPÍTULO 3

3. DISEÑO METODOLÓGICO

En el presente capítulo se presenta la forma de cómo fue abordada la investigación metodológicamente, las fases de la investigación y la aplicación de las técnicas e instrumentos para llegar a conclusiones más elaboradas.

3.1. Tipo de investigación

Este proyecto de grado se desarrollará de acuerdo con los elementos o fases de la investigación cualitativa. Determinando un alcance de procedimientos exploratorios, y teniendo en cuenta los diferentes métodos y técnicas propias de cada una de las etapas que se abordaran en el estudio, incluyendo los procedimientos, recolección, procesamiento y análisis de la información, además del seguimiento al cronograma de actividades.

Se comenzará con la formulación de preguntas al administrador de red y administrador del sitio web de la alcaldía de Quibdó, además de la aplicación de un *pentesting* “Prueba de Penetración” para la identificación de vulnerabilidades del sitio web de la entidad y los servicios en línea prestados por la alcaldía de Quibdó.

3.2. Fases del proyecto

La investigación se llevará a cabo en las siguientes fases:

- **Fase I.** Identificación de fuentes de información que permitirán ampliar la perspectiva del conocimiento a aplicar.
- **Fase II.** Análisis y clasificación de la información según su género, origen y categoría.
- **Fase III.** Selección y aplicación de las herramientas de *pentesting* “Prueba de Penetración” para determinar las vulnerabilidades del sitio web y sus servicios.
- **Fase IV.** Análisis de resultados obtenidos del sitio web y sus servicios e identificación de las vulnerabilidades.
- **Fase V.** Aplicación de medidas correctivas y sugerencias para mitigar las vulnerabilidades del sitio web y sus servicios.
- **Fase VI.** Conclusiones y elaboración de un Documento final.

3.3. **Técnicas e instrumentos de recolección de información**

Se emplearán técnicas de recolección de la información cuantitativas y cualitativas, tales como: La observación, la entrevista no estructurada y la encuesta, al grupo de administración de la red, la administración web y los funcionarios de la alcaldía municipal con la finalidad de obtener los resultados más exactos con respecto a los problemas que se generan a través de las vulnerabilidades del sistema.

- **Fuentes primarias:**

Las principales fuentes de información serán unas encuestas directas para recolectar los datos necesarios con el fin de identificar el centro del problema y

escoger la solución; que es la aplicación de las herramientas de *Pentesting* “Prueba de Penetración” para determinar las vulnerabilidades del sitio web y sus servicios, dichas encuestas se le realizan a los Administradores de la red, administrador web y funcionarios de la Alcaldía de Quibdó. Las pruebas de penetración incluyen los siguientes testeos de seguridad informática del sitio web en Internet utilizando las herramientas descritas:

Métodos de análisis del sitio web utilizando Kali Linux

- Mapeo de red – Network mapping: Ping y Nmap.
- Recopilación de información - Information Gathering: Dmitry y Maltego.
- Identificación del CMS: BlindElephant y WhatWeb.
- Detección de IDS/IPS: Waffit.
- Análisis de código abierto - Open Source Analysis: Httrack.
- Rastreadores Web - Web Crawlers: Dirb.
- Evaluación y Explotación de la Vulnerabilidad - Vulnerability Assessment and Exploitation: SqlMap, Uniscan y Nikto.

Estructura del informe técnico final del *pentesting*:

El informe técnico se centrará en el detalle en profundidad de las vulnerabilidades detectadas y contendrá los siguientes apartados:

- Introducción: se describirá el objetivo perseguido con el servicio de *pentesting* y una introducción al formato del *pentesting* realizado.

- Alcance: se definirá el alcance de la auditoria enumerando aquellos activos sobre los que se ejecutará el servicio de *pentesting*. Por ejemplo: sitio web corporativo www.quibdomia.com.

- Resumen ejecutivo: Se resumirá los resultados obtenidos con el servicio de *pentesting*.

- Ventanas de actuación: En este apartado reflejaremos las fechas y horas concretas en las que se ha llevado a cabo el *pentesting*, de tal forma que quede constancia.

- Descripción detallada del proceso de *pentesting*: Se definirá el tipo de metodología utilizada, como se han llevado a cabo cada una de las fases del *pentesting* y que técnicas/herramientas se han utilizado en cada una de las fases.

- Vulnerabilidades detectadas: Se realizará una descripción técnica detallada de las vulnerabilidades encontradas en los activos definidos en el alcance del servicio. Se definirá: como se han encontrado, como se han explotado, si ha existido escalada de privilegios, recomendaciones de mitigación.

- Anexos: Haremos referencia y describiremos las metodologías en las que nos hemos apoyado a la hora de ejecutar el servicio: metodologías y referencias.

- **Fuentes secundarias:**

Con el fin de complementar la información requerida y recolectada es necesario tomar fuentes externas de información como la investigación en internet, material multimedia, libros o textos que tengan relación con el tema y el problema planteado y todo el material que direccione como fuente de solución al cumplimiento del objetivo.

3.4. **Tipo de análisis**

El tipo de análisis que se aplica en este proyecto se determinó por las técnicas cualitativas y cuantitativas, dado que los datos se requieren de manera gráfica o numérica.

CAPÍTULO 4

4. RESULTADOS Y ANÁLISIS

En el presente capítulo se presentan los resultados de la investigación conforme se plantearon en los objetivos específicos.

4.1. Diagnóstico sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó

En el presente informe se presenta un diagnóstico sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó www.quibdomia.com, se ejecutaron pruebas de penetración de caja negra bajo una metodología que definía un conjunto de reglas, prácticas, procedimientos y métodos utilizando las herramientas que contiene la distribución de software libre Kali Linux, inicialmente no se tenía conocimiento sobre la infraestructura de red de la organización ni del hosting, por lo tanto se realizaron pruebas externas a nivel web solo con el detalle de la URL e intentando interrumpir en el sitio web o red de la organización simulando ataques externos realizados por un atacante malicioso.

Para realizar el diagnóstico y las pruebas de penetración, se aplicaron conocimientos avanzados en infraestructura de redes, seguridad informática, protocolos TCP / IP y habilidades razonables en uso de sistemas operativos Linux derivados de Debían. Luego de realizar el análisis y levantamiento de información disponible como vulnerabilidades del sitio web Quibdomia.com se detectaron los siguientes datos a utilizar para posibles ataques:

- Dirección IP del servidor: 104.131.21.200.
- Puertos abiertos: SSH:22 y HTTP:80.
- Nombre del dominio: quibdomia.com.
- Nombre Hosting: http://www.iana.org.
- Nombre de usuario administrador: admin-c: IANA1-RIPE.
- Directorio con contenido de admin: http://quibdomia.com/admin/.
- Sistema Operativo del servidor: Ubuntu.
- Servidor de dominio: godaddy.com.
- URL servidor de dominio: http://www.godaddy.com.
- Nombres de servidores: ns1.digitalocean.com, ns2.digitalocean.com, ns3.digitalocean.com.
- Fecha de última actualización del sitio: 30-nov-2016.
- Fecha de creación del sitio: 19-nov-2015.
- Estructura de enlaces del sitio.
- Gestor de contenidos CMS: Drupal.
- 16 plugins drupal instalados.
- Cookies: San_Pacho_Session.
- correos electrónicos del sitio: prensa@quibdo-choco.gov.co.
- Campo de usuario y contraseña dentro de código jQuery para el login.
- El servidor no cuenta con un firewall que lo proteja.
- Se pudo descargar el código Fuente y subdirectorios del sitio web.
- listado de palabras claves del sitio.

- listado de 6 correos electrónicos externos registrados en plataforma.

4.2. **Identificación de vulnerabilidades del sitio web de la alcaldía de Quibdó**

En este capítulo se busca realizar la identificación de vulnerabilidades para realizar un diagnóstico de alto nivel sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó utilizando las diferentes herramientas de Kali Linux, una distribución GNU/Linux diseñada para la realización de auditoria de seguridad e instalada en una máquina virtual Oracle Sun VirtualBox.

Se ejecutarán unas pruebas de penetración de caja negra bajo una metodología que define un conjunto de reglas, prácticas, procedimientos y métodos utilizando las herramientas que contiene la distribución, es necesario tener en cuenta que inicialmente no se tiene conocimiento sobre la infraestructura de red de la organización, por lo tanto, se realizan pruebas externas a nivel web solo con el detalle de la URL e intentando interrumpir en el sitio web o red de la organización simulando ataques externos realizados por un atacante malicioso.

4.2.1. **Mapeo de Red – Network Mapping**

Un mapeo de red es el análisis y estudio de la conectividad física de redes y busca identificar los diferentes servidores y sistemas operativos que se ejecutan en una red. El mapeo se realiza mediante procesos complejos de escaneo de puertos acompañados de unos correctos fundamentos de ley y valores éticos. Estos

métodos pueden ser detectados por los seres humanos o sistemas automatizados, y se presenta como un acto malicioso de no conocerse previamente la ejecución de estos.

En la suite de Kali Linux se incluye los programas PING y NMAP, herramientas muy potentes y eficaces a la hora que realiza sus trabajos, las cuales sirven para llevar a cabo la Auditoria Web.

- **Ping**

Se utilizó esta herramienta para identificar la dirección IP del sitio web quibdomia.com arrojándonos la dirección IP del servidor 104.131.21.200, para las diferentes pruebas que se ejecutan en adelante se pueden realizar con el nombre del dominio o la dirección IP arrojada.

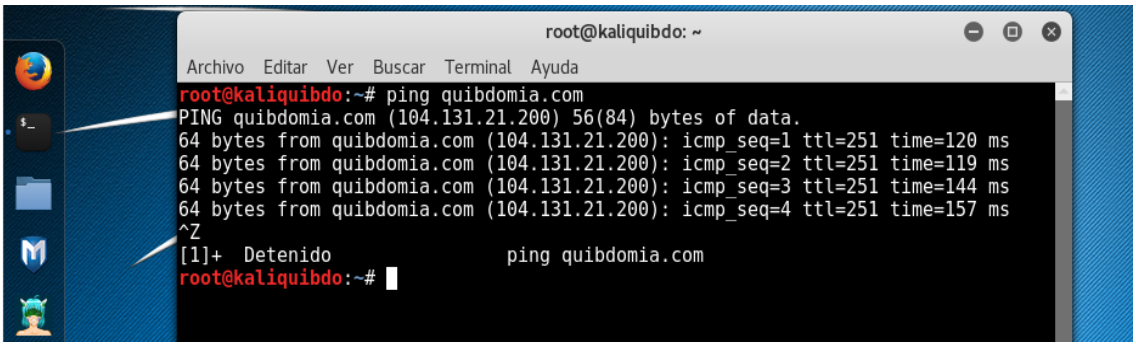


Figura 1. Ejecución programa Ping
Fuente: Autor de la investigación

- **Nmap:**

La herramienta Nmap es un mapeadores de redes de código abierto que permite la exploración de red y auditorías de seguridad. Utiliza paquetes IP para identificar

los diferentes equipos que se encuentran disponibles en una red, los servicios que ofrece cada equipo, los sistemas operativos que ejecutan, los sistemas para filtros de paquetes o cortafuegos que utilizan, entre otras características.

Se ejecuta el comando nmap quibdomia.com y arroja que el servidor tan solo tiene abiertos los puertos SSH para conexión mediante consola remota y HTTP para la navegación en el sitio web mediante los diferentes navegadores.

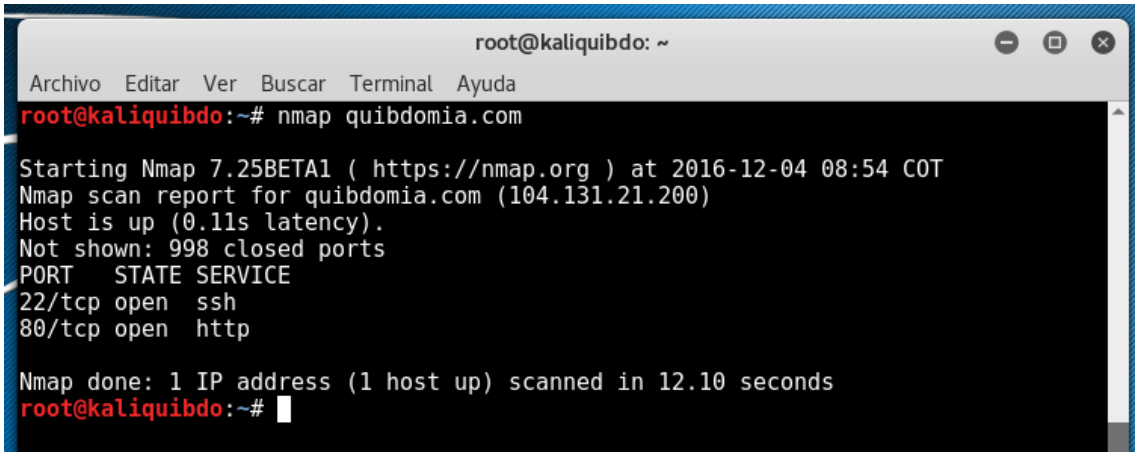


Figura 2. Ejecución comando Nmap
Fuente: Autor de la investigación

4.2.2. **Recopilación de Información - *Information Gathering***

Luego de realizar el mapeo de la Red con Ping y Nmap procedemos a realizar la primera fase de evaluación de la seguridad, recopilando toda la información posible acerca del sitio web de la alcaldía. En este crítico paso de las pruebas de seguridad, se usan motores de búsqueda, escáner de red, envío aleatorio de peticiones HTTP, posibilitando forzar al sitio web a suministrar información, por ejemplo, mostrar

mensajes de errores o las versiones de paquetes de software y las tecnologías utilizadas.

Se recoge la información activa el sitio web, haciendo contacto directo con el objetivo y tratando de reunir los datos con las herramientas dmitry y Maltego.

- **Dmitry**

La herramienta Dmitry permite obtener casi toda la información sustraible sobre un host. Se puede utilizar para realizar búsquedas en Internet, obtener el nombre de la máquina Hostname, recuperar la hora del sistema y los datos del servidor. Tiene capacidad de realizar búsquedas de subdominios y exploración de los puertos TCP para identificar cuales están abiertos o cerrados.

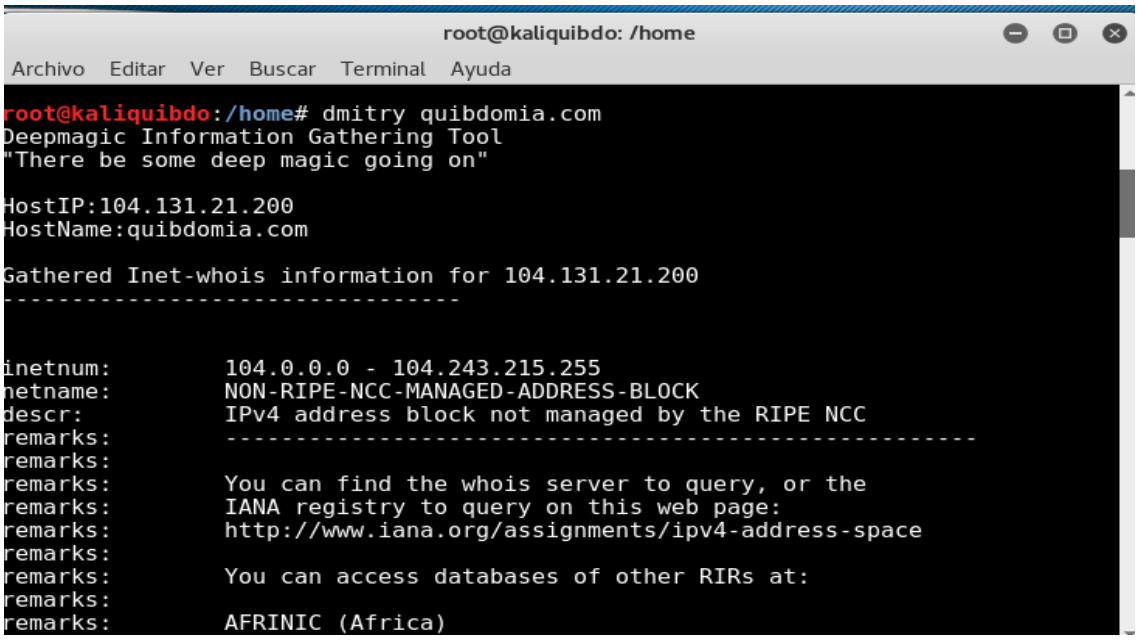


Figura 3. Ejecución programa Dmitry
Fuente: Autor de la investigación

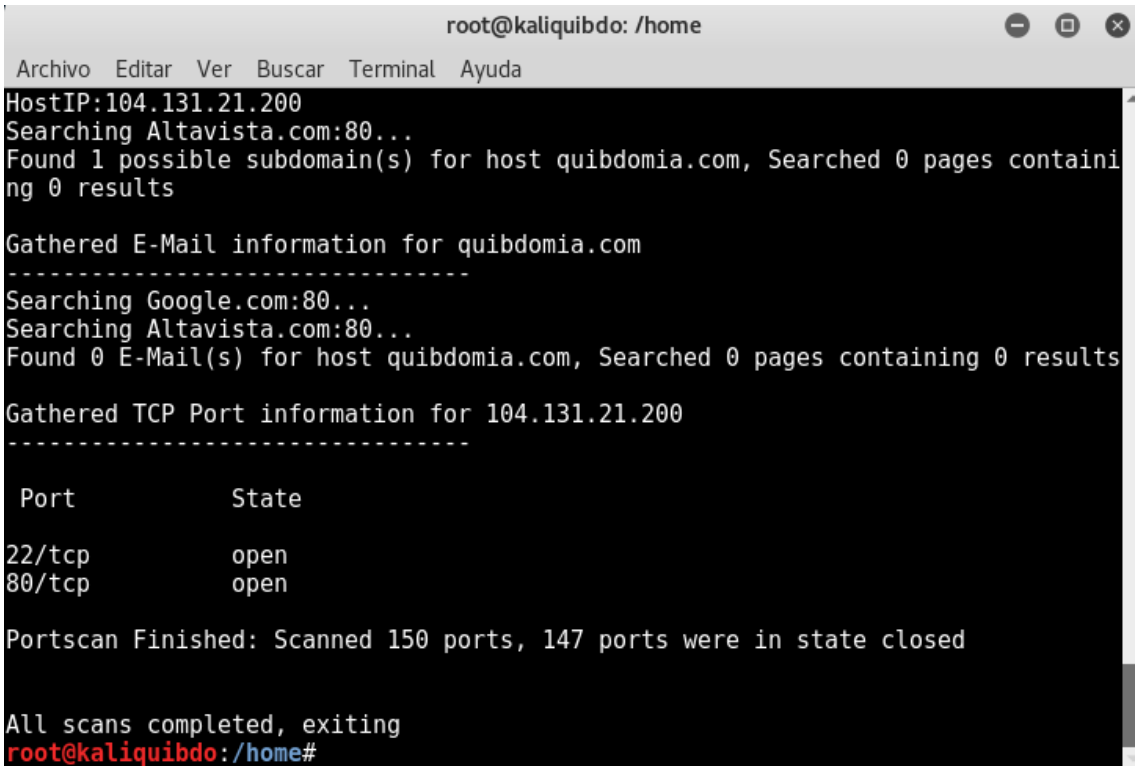


Figura 4. Ejecución programa Dmitry
Fuente: Autor de la investigación

En la Tabla 1, se encuentra el archivo dmitry.txt, donde se encuentra el log completo de la información arrojada, del cual se destacan los siguientes datos:

Tabla 1. Resultados del archivo dmitry.txt

HostIP:	104.131.21.200
HostName:	quibdomia.com
role:	Internet Assigned Numbers Authority
address:	see http://www.iana.org.
admin-c:	IANA1-RIPE
Domain Name:	QUIBDOMIA.COM
Registrar:	GODADDY.COM, LLC
Whois Server:	whois.godaddy.com
Referral URL:	http://www.godaddy.com
Name Server:	NS1.DIGITALOCEAN.COM
Name Server:	NS2.DIGITALOCEAN.COM
Name Server:	NS3.DIGITALOCEAN.COM

Status:	clientDeleteProhibited
	https://icann.org/epp#clientUpdateProhibited
Updated Date:	30-nov-16
Creation Date:	19-nov-15
Expiration Date:	19-nov-17
Searching Google.com:80...	
Searching Altavista.com:80...	
Found 0 E-Mail(s) for host quibdomia.com, Searched 0 pages containing 0 results.	
Gathered TCP Port information for 104.131.21.200.	
Port:	State
22/tcp:	open
80/tcp:	open
Portscan Finished: Scanned 150 ports, 147 ports were in state closed	

Nota. Fuente: Autor de la investigación con datos del archivo dmitry.txt

- **Maltego**

Maltego es una aplicación forense que muestra cómo está conectado el sitio con otros por medio de su infraestructura de red, las empresas se relacionan con la información recopilada y con sus sitios web.

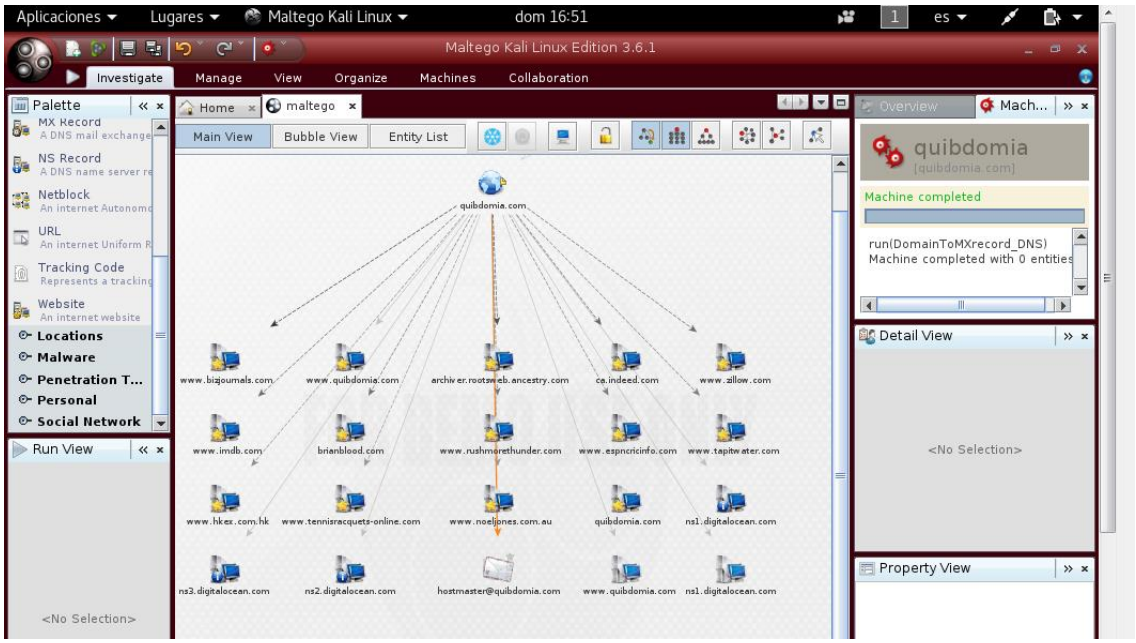


Figura 5. Ejecución programa Maltego
Fuente: Autor de la investigación

4.2.3. **Identificación del CMS**

En esta etapa del proyecto utilizamos herramientas para identificar el sistema de gestión de contenidos CMS usado por el sitio web, conocer esta información permitirá tener conocimientos sobre las vulnerabilidades ya conocidas de los mismos.

- **BlindElephant**

Es una herramienta que se utiliza para realizar *Fingerprinting* en Aplicaciones Web. La herramienta es rápida, tiene poco ancho de banda y está altamente automatizada.

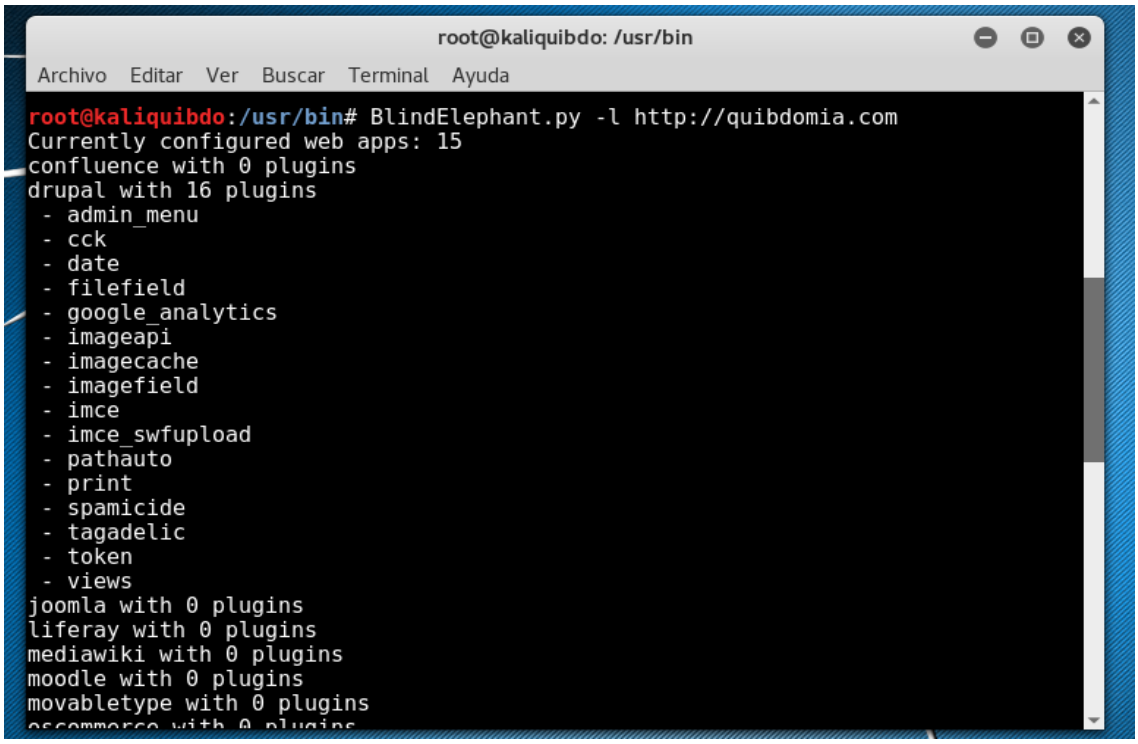


Figura 6. Ejecución programa BlindElephant
Fuente: Autor de la investigación

Ejecutando la herramienta detectamos que el sitio web está instalado bajo el CMS drupal y contiene 16 plugins instalados, Ver anexo BlindElephant.txt.

- **WhatWeb**

El paquete WhatWeb es utilizado para identificar el tipo de sistemas de gestión de contenidos CMS, plataforma de blogs, estadísticas, bibliotecas Javascript y servidores utilizados en un sitio web. Esta herramienta cuenta con más de 900 Plugins para realizar análisis web y permite complementar la información obtenida con la herramienta BlindElephant.

Primero ejecutamos la herramienta solo informando sobre el sitio web para que nos devuelva información general así:

whatweb http://quibdomia.com/

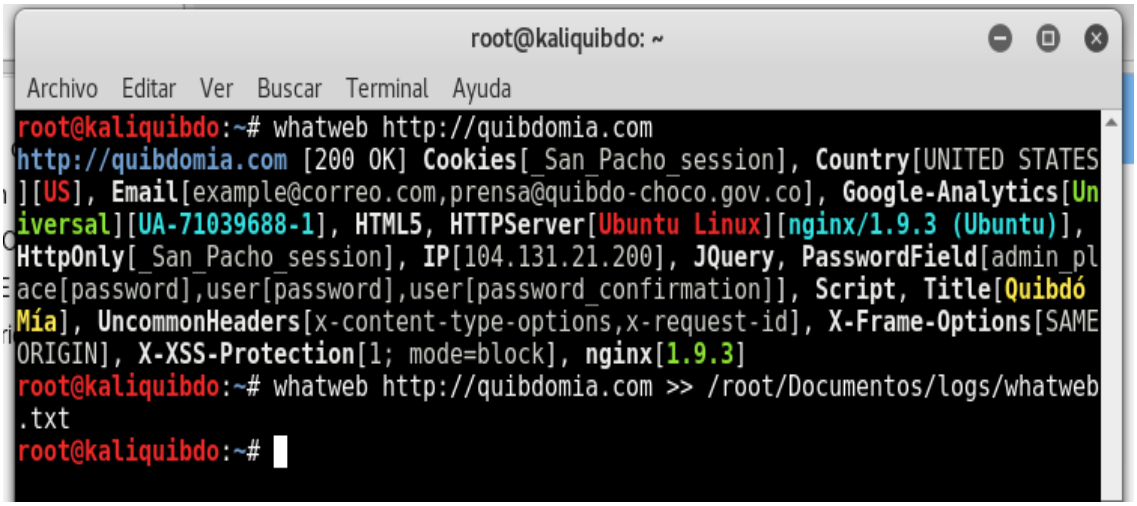


Figura 7. Ejecución programa whatweb
Fuente: Autor de la investigación

Con esta primera ejecución se pudo detectar información valiosa como las cookies habilitadas, el correo electrónico, la versión de HTML utilizada, el servidor web y su sistema operativo, la dirección IP del sitio, el uso de JQuery para el login entre otros datos.

Luego ejecutamos el comando whatweb –v http://quibdomia.com/ arrojándonos información más detallada del sitio:

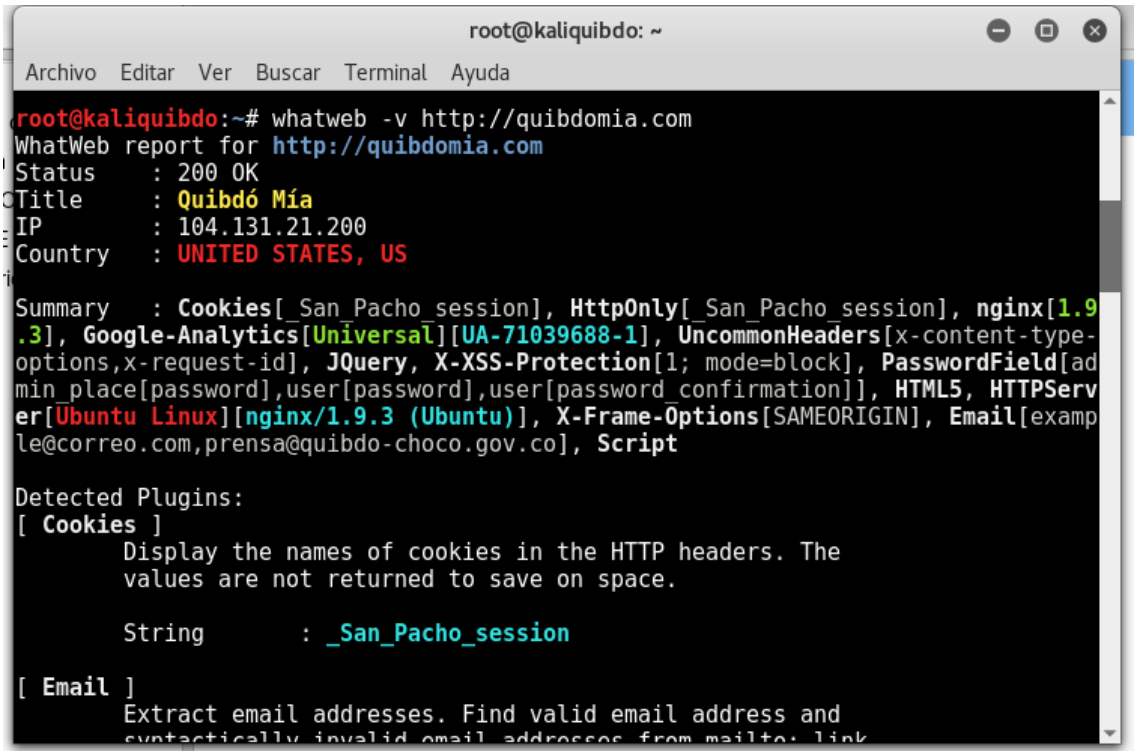


Figura 8. Ejecución comando whatweb –v
Fuente: Autor de la investigación

Los resultados completos de los comandos se pueden verificar en los archivos whatweb.txt y whatwebv.txt.

4.2.4. **Detección de IDS/IPS**

Los sistemas de Detección de Intrusos IDS y los sistemas de Protección de Intrusos IPS en ocasiones están instalados y activados para detener distintos tipos de ataques y amenazas contra el hosting y el dominio donde se encuentra alojado el sitio web. También es común encontrar WAF (Web Aplication Firewall) que sirven para mitigar vulnerabilidades de las aplicaciones web y los distintos servidos de red.

Algunos firewalls se pueden detectar muy fácilmente porque la mayoría usan la firma con métodos de detección, de tal manera que el intruso puede encriptar o codificar los parámetros del ataque y *bypassear* las reglas y políticas de filtrado configuradas en el firewall.

- **Waffit**

Waffit es una herramienta que detecta los posibles Firewall que puede tener el servidor web detrás del dominio, esta información es muy importante para las pruebas de penetración.

Al ejecutar el programa Wafw00f se pudo verificar mediante 13 peticiones que el servidor no cuenta con un firewall que lo proteja.

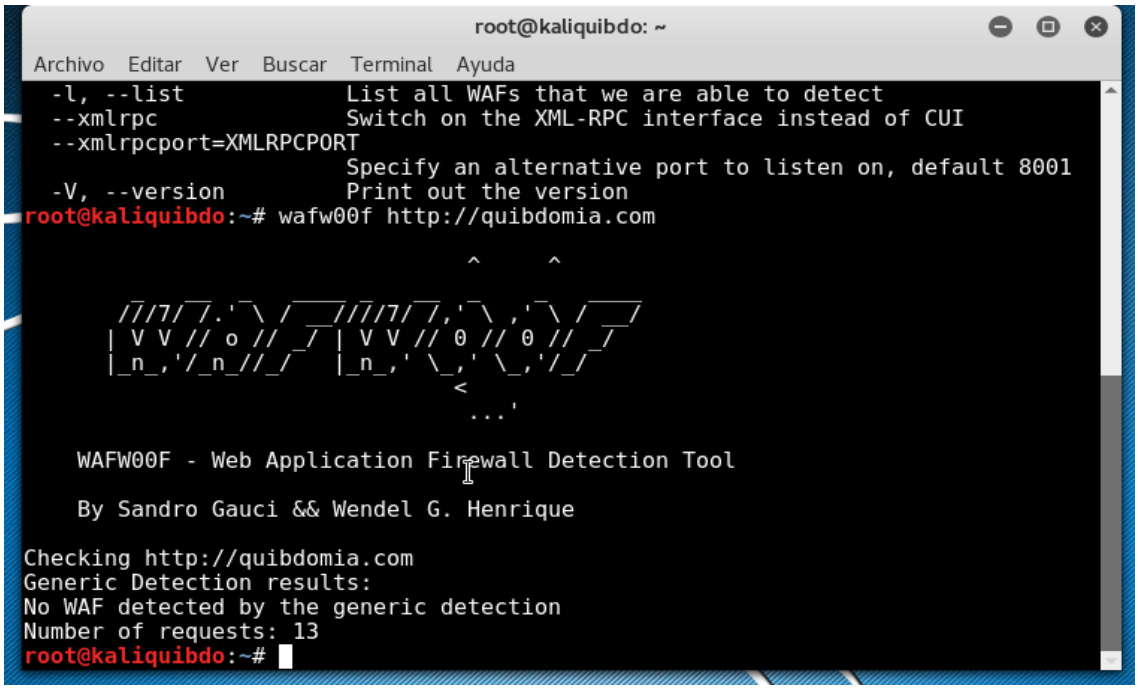


Figura 9. Ejecución programa Wafw00f
Fuente: Autor de la investigación

4.2.5. **Análisis de Código Abierto - *Open Source Analysis***

Se realiza un análisis de código abierto utilizando herramientas como Httrack para verificar las posibles vulnerabilidades permitidas por el código fuente de la aplicación o sitio web.

- **Httrack**

Httrack es una herramienta facilitada por la comunidad de software libre bajo licencia GPL, la cual tiene versiones multiplataforma y multilenguaje adaptándose a cualquier tipo de usuario, esta herramienta permite la captura y descarga parcial o total de un sitio web para su posterior análisis offline de su contenido y código fuente.

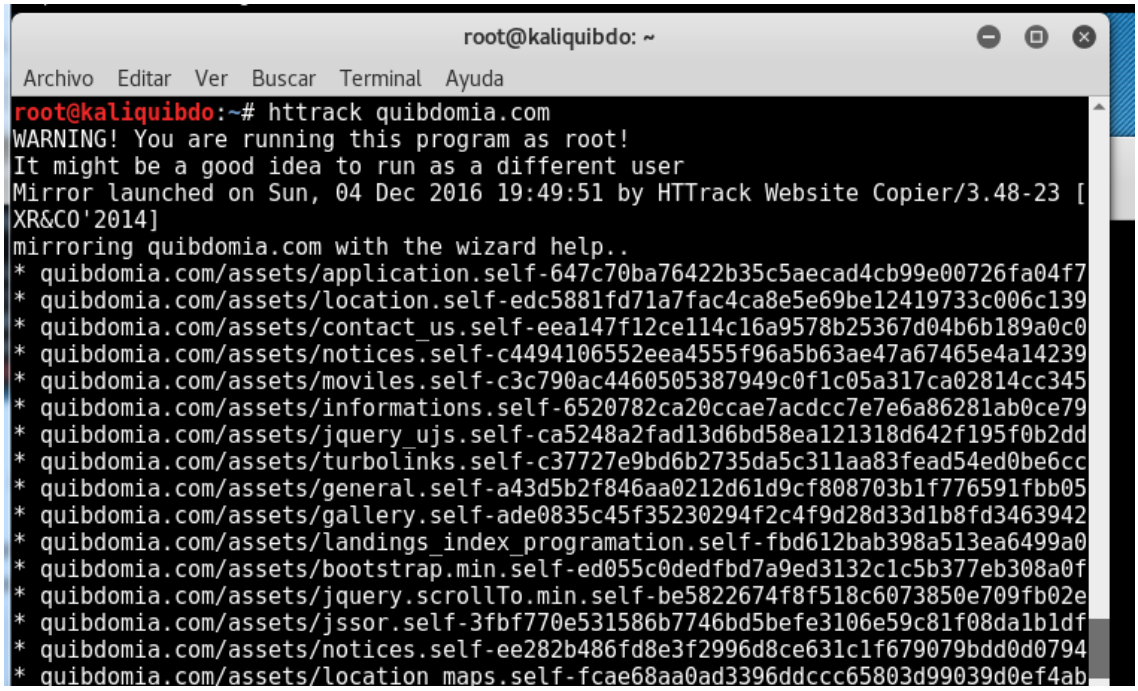


Figura 10. Ejecución comando httrack
Fuente: Autor de la investigación

Para revisar detalladamente el código Fuente del sitio web se pudo descargar el directorio completo del sitio.

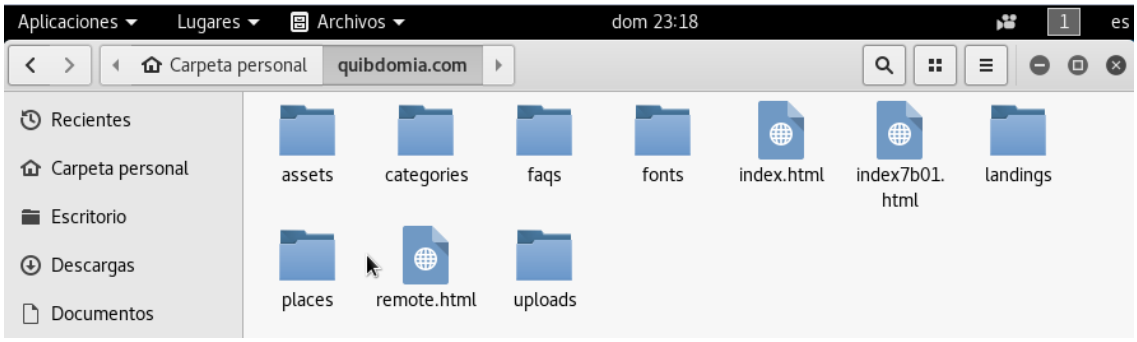


Figura 11. Directorio web ejecución comando httrack
Fuente: Autor de la investigación

4.2.6. **Rastreadores Web - *Web Crawlers***

En esta fase del proyecto utilizamos los Crawlers, que ayudaran mucho a enumerar los archivos y carpetas "escondidos" dentro de un servidor web. Para lo cual utilizamos las siguientes herramientas:

- **Dirb**

DIRB es un escáner de contenido web que busca los objetos Web existentes así estén ocultos. Con estos objetos podemos entrar a revisar posibles usuarios y contraseñas no encriptadas si están en ficheros de texto, configuraciones de acceso a bases de datos, transacciones, entre otra información confidencial.

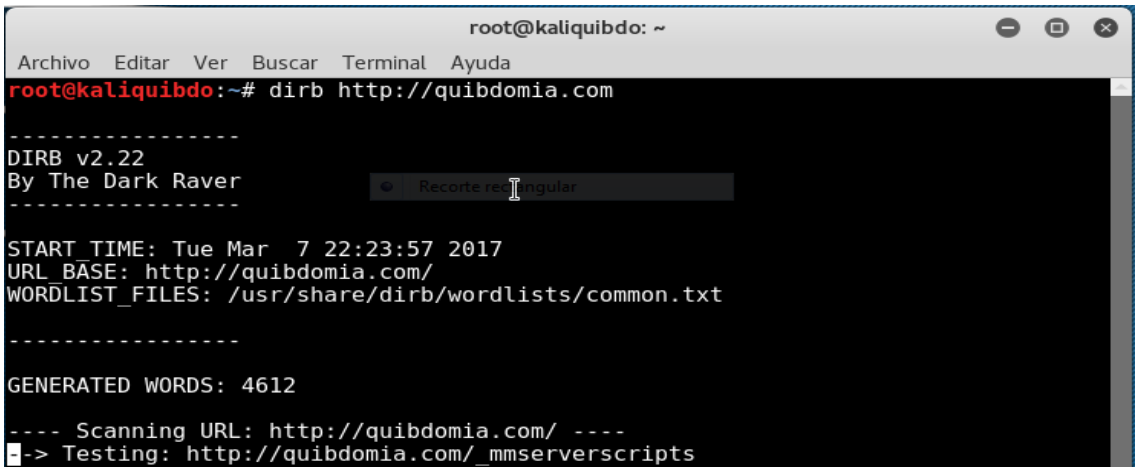


Figura 12. Ejecución comando dirb
Fuente: Autor de la investigación

Los resultados de este escaneo se pueden revisar detalladamente los ficheros dirb.txt y los ficheros en common.txt.

4.2.7. **Evaluación y Explotación de la Vulnerabilidad - *Vulnerability Assessment and Exploitation***

En esta etapa se explora el objetivo de buscar los errores, antes de hacer una evaluación de la vulnerabilidad, la recopilación de información de las etapas anteriores ha sido de mucha utilidad, en el anterior escaneo se encontró la versión del CMS instalado con el sitio web. Ahora, en la etapa de evaluación de la vulnerabilidad, se utilizan herramientas que ayudan mucho a encontrar respectivas vulnerabilidades en ese servidor web específico.

- **SqlMap**

Con SqlMap intentamos detectar vulnerabilidades de inyección SQL, conectándonos directamente a la base de datos del sitio web. Al ejecutar el

comando nos sugiere una serie de palabras extraídas del sitio que se pueden utilizar para intentar ingresar a la base de datos.

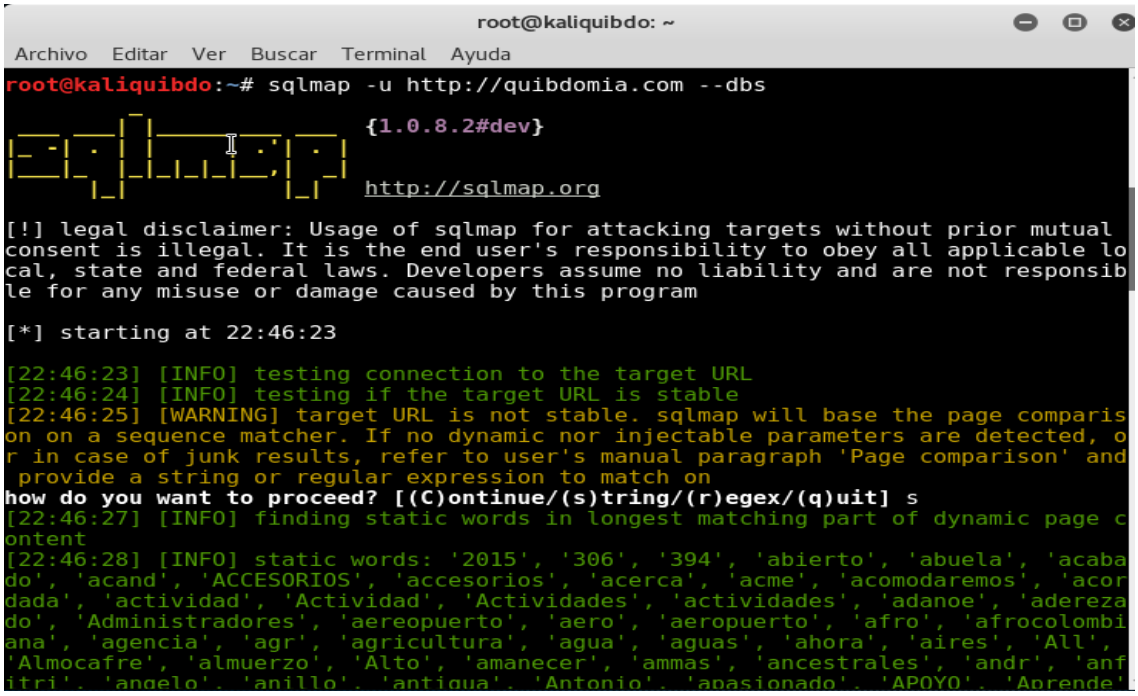


Figura 13. Ejecución programa sqlmap
Fuente: Autor de la investigación

- **Uniscan**

El paquete Uniscan fue desarrollado en el lenguaje PERT, liberado bajo licencia GPL y contiene funcionalidades de escáner de vulnerabilidades de sitios Web, es de fácil uso y administración por la línea de comandos utilizando expresiones regulares y multihilos. Entre sus principales características se encuentran: identificación de páginas del sistema, identificación de páginas mediante método GET, pruebas de sitios por método POST, soporte a peticiones SSL y HTTPS, soporte a servidores proxy, generación de listados de sitios mediante buscadores Google y Bing, interfaz gráfica para el usuario.

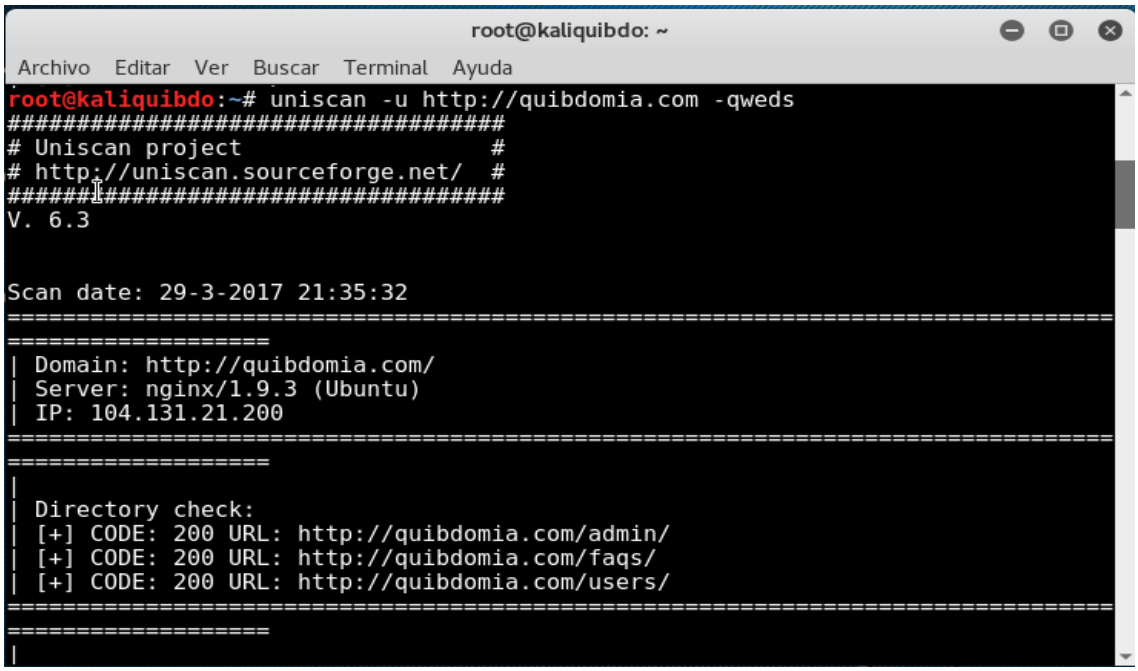


Figura 14. Ejecución programa Uniscan
Fuente: Autor de la investigación

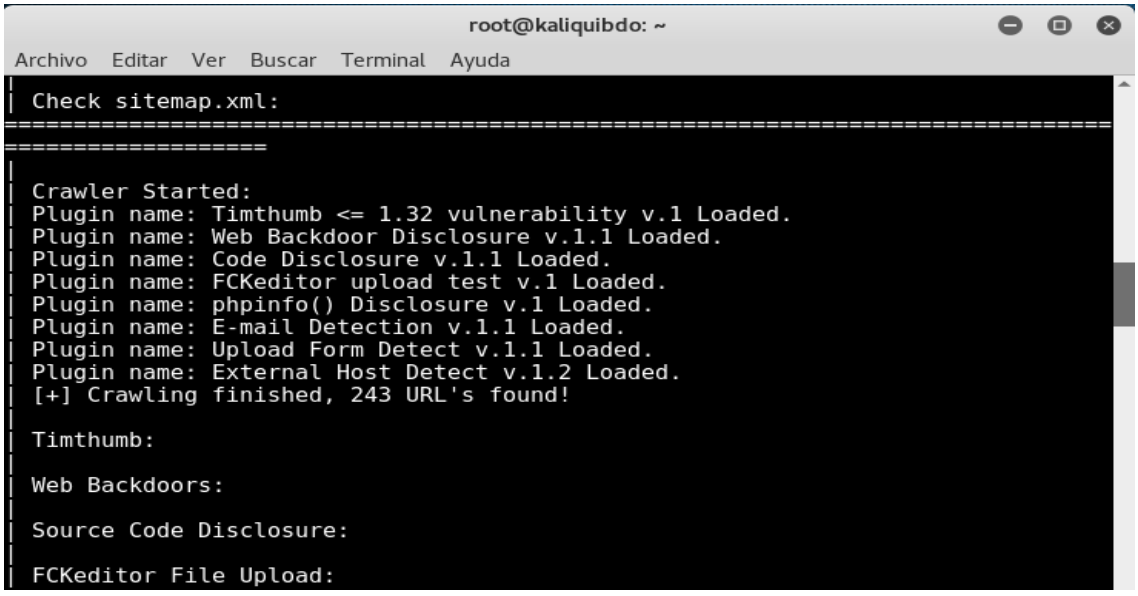


Figura 15. Ejecución programa Uniscan – Plugins Crawler cargados
Fuente: Autor de la investigación

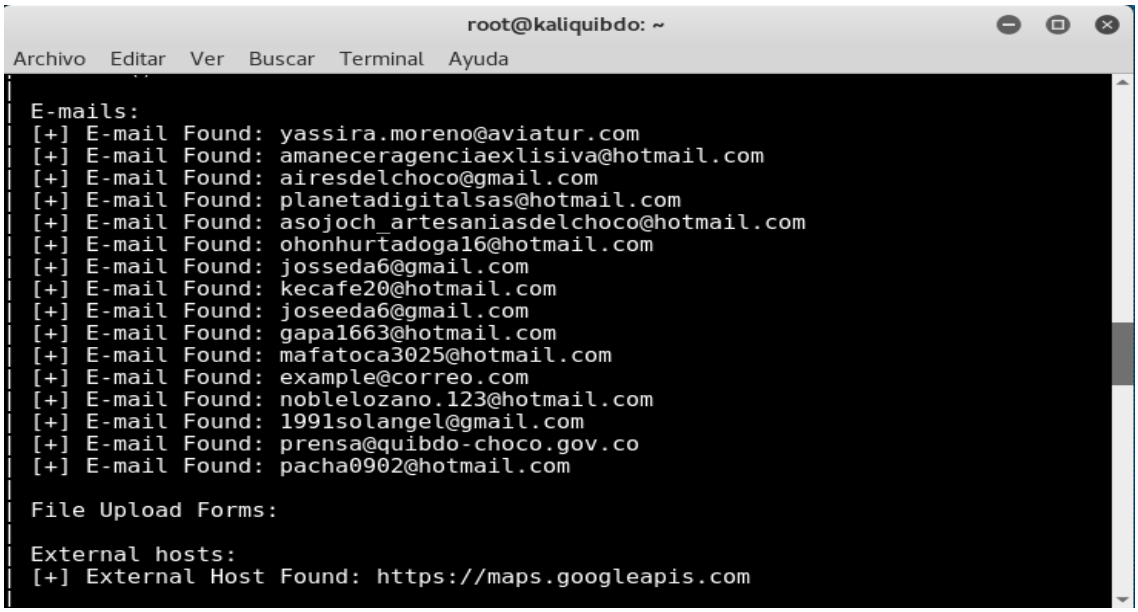


Figura 16. Ejecución programa Uniscan - Correos encontrados
Fuente: Autor de la investigación

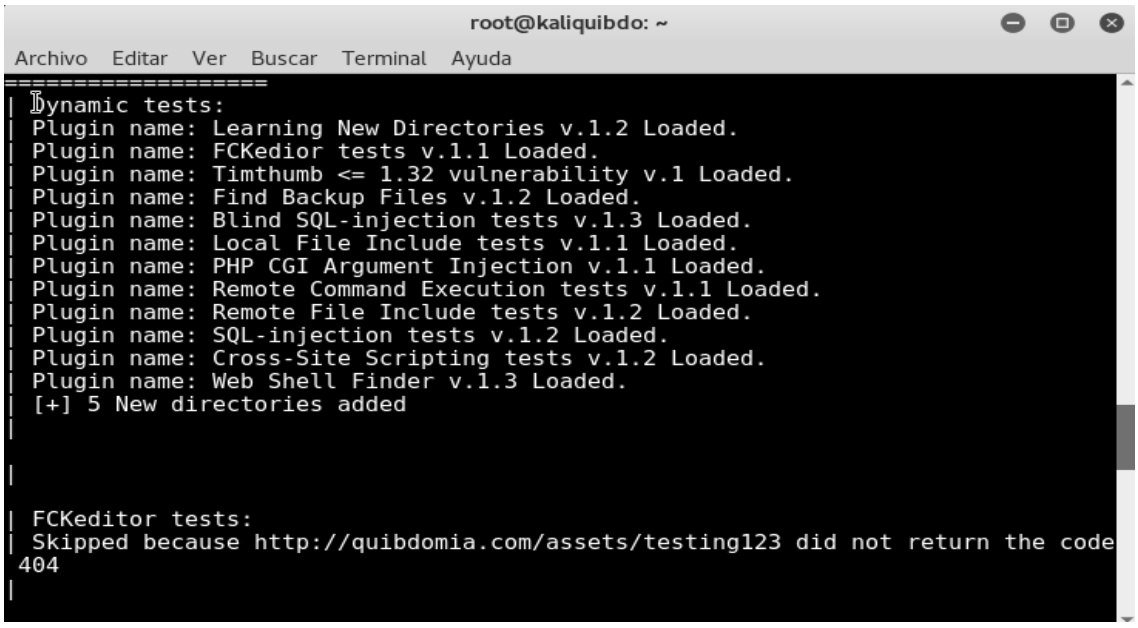


Figura 17. Ejecución programa Uniscan - Plugins test dinámicos
Fuente: Autor de la investigación

Como se evidencia en los pantallazos anteriores, no se logró detectar una vulnerabilidad utilizando los diferentes *plugins* que contiene la herramienta *Uniscan*.

- **Nikto**

El paquete de software Nikto permite escanear completamente servidores web, escaneando más de 6500 ficheros potencialmente dañinos, revisa las versiones instaladas en los servidores y los problemas ya caracterizados de más de 270 servidores. Adicionalmente permite comprobar la configuración del servidor y la presencia de archivos índex y opciones HTTP del servidor.

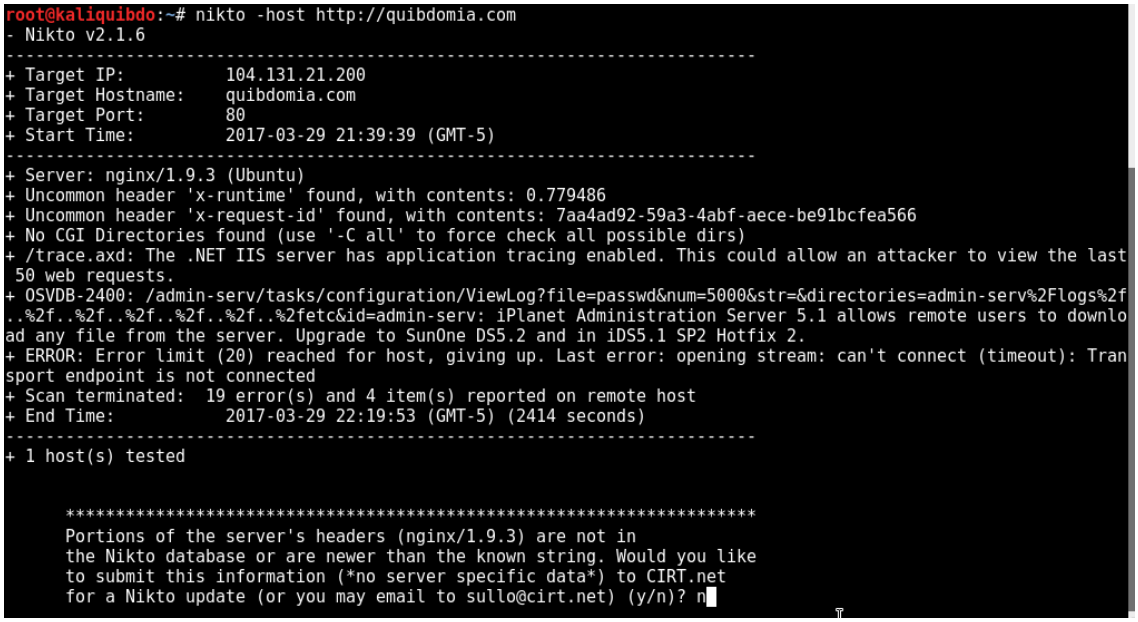


Figura 18. Ejecución programa Nikto
Fuente: Autor de la investigación

Luego del escaneo con la herramienta *nikto* se pudo evidenciar que el servidor no presento vulnerabilidades detectadas por esta herramienta.

4.3. **Pruebas de penetración de caja negra al sitio web de la alcaldía de Quibdó**

Con la información diagnosticada en el capítulo anterior, enunciamos un listado de los posibles ataques a los que puede estar expuesto el sitio web y servicios en línea de Quibdomia.com.

4.3.1. **Ataques de Inyección de Ficheros**

Con el ataque "*Remote file inclusión*" se podría ejecutar código remoto dentro de la aplicación web vulnerable. Basándose en que, si es posible cargar un fichero local para su inclusión dentro de un sitio, también se puede cargar uno remoto que contenga código malicioso.

Otro tipo de ataque de inyección de ficheros es el "Local file inclusión" que, a diferencia del remoto, afecta lenguajes compilados e interpretados y busca incluir dentro del sitio un fichero local del usuario con el que se ejecuta el servidor de aplicaciones web que tenga permisos de lectura.

4.3.2. **Denegación de Servicio – DOS**

Un ataque de denegación de servicios puede ser utilizado contra cualquier servidor web, dificultando el uso autorizado del sitio y los servicios en línea prestados, debido al agotamiento de los recursos. Generalmente estos ataques están dirigidos a los servidores de una organización con el objetivo de imposibilitar el acceso de los usuarios.

4.3.3. **Denegación de Servicio Distribuido – DDOS**

Este ataque es una variante del ataque DoS pero utiliza varios equipos distribuidos como zombies para realizar el ataque.

4.3.4. **Phishing**

Con este tipo de ataque que se lleva a cabo a base de ingeniería social con el objetivo de intentar conseguir información confidencial de forma fraudulenta, se puede explotar utilizando las palabras claves sugeridas por la aplicación SQLMAP. El intruso o phisher, se hace pasar por una de las cuentas de correos electrónicos registradas en el sistema en una aparente comunicación oficial electrónica y puede obtener información del portal.

4.3.5. **Bomba Lógica**

En caso de éxito del tipo de ataque anterior Phishing, una vez se tenga acceso al servidor se puede colocar intencionalmente un pedazo de código de programación dañino dentro del código fuente de del sitio web. El objetivo de este ataque es ejecutar una función, procedimiento o código malicioso al momento que se produzcan ciertas condiciones determinadas.

4.3.6. **SQL Injection**

Si el phishing funciona, al igual que la bomba lógica se puede realizar el ataque *SQL Injection*, que consiste en la inserción de código malicioso en la aplicación web

con el objetivo de obtener acceso no autorizado a información confidencial de la base de datos.

4.3.7. **Fuerza Bruta**

Los ataques de fuerza bruta crean procesos automatizados que realizan pruebas para detectar errores generando usuarios y contraseñas al azar para así acceder a los sistemas de información que requieren de un login, como es el caso del sitio Quibdomia.com. El cual no cuenta con técnicas para evitar este tipo de ataques a pesar de la gran variedad de técnicas disponibles en el mercado.

4.3.8. **Predicción del Identificador de Sesión**

Algunas aplicaciones Web gestionan sus métodos de autentificación usando valores de identificación de sesión (SESSION ID). Cuando el identificador de sesión es predecible, un intruso puede obtener un número de sesión válido y obtener acceso no autorizado a la aplicación, sustituyendo a un usuario previamente autentificado, en el caso de Quibdomia se podría utilizar la cookie identificada como San_Pacho_Session.

4.3.9. **Autenticación Incompleta y Débil Validación**

Es un tipo de ataque en el cual un intruso accede alguna funcionalidad de la aplicación sin tener que autenticarse. En este ataque un individuo puede descubrir la URL específica de la funcionalidad sensible través de pruebas de fuerza bruta sobre directorios comunes de ficheros de administración. Normalmente sucede

cuando los datos de validación de la identidad de los usuarios son predecibles o puedan ser falsificadas.

4.3.10. **Autorización Insuficiente**

Se presenta cuando un usuario tiene acceso a los partes sensibles de la aplicación o sitio web que deberían estar protegidas por controles para restringir el acceso. Si no se cuenta con algunas medidas de seguridad para las aplicaciones, este ataque podría ser muy dañino, ya que el intruso autenticado podría controlar toda la aplicación y el contenido del sitio.

4.3.11. **Path Traversal**

En estos ataques los individuos acceden a los archivos, directorios y comandos que se encuentran fuera del *path* de administración *Root* del sitio web, accediendo a los archivos ejecutables para realizar la funcionalidad de la aplicación web e información confidencial de usuarios.

Los anteriores son algunos de los tipos de ataques que tienen como objetivo vulnerar la confiabilidad, integridad y disponibilidad de la información y servicios en línea publicados por la alcaldía de Quibdó en el portal quibdomia.com.

4.4. **Controles para reducir las vulnerabilidades del sitio web de la alcaldía de Quibdó**

Al contener los posibles ataques a los cuales está expuesto Quibdomia.com se proponen una serie de controles que mejoraran la seguridad informática de la entidad y así, poder disminuir el riesgo de afectación de la disponibilidad, confiabilidad e integridad de este sitio web:

4.4.1. **Drush**

Descargar e instalar el módulo drush de Drupal y aplicarlo en el código manualmente para realizar actualizaciones del sitio web usando los comandos de Drush. El cual es una interfaz de scripting de Unix para Drupal y contiene una serie de comandos útiles para interactuar con módulos, temas y perfiles de drupal. También permite ejecutar el fichero update.php, realizar consultas SQL, migraciones de bases de datos y utilizar cron o limpiar caché.

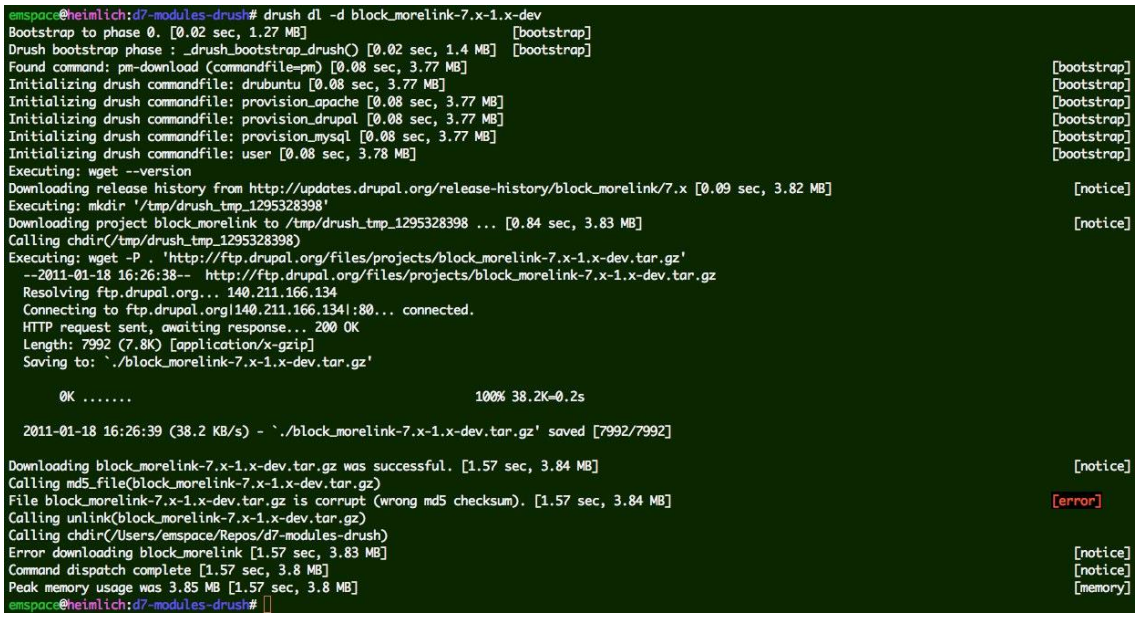


Figura 19. Ejecución comando drush para bloquear un módulo drupal
Fuente: Sitio web https://www.drupal.org/node/499884

4.4.2. **Comprobar Informe de Actualizaciones**

Realizar la comprobación periódica del informe de actualizaciones de Drupal, el cual avisa sobre cuestiones de seguridad en el sitio web, como un núcleo caducado, módulos o bases de datos que necesitan ser actualizados o instalados. Esta tarea no hay que descuidarla para mantener nuestro sitio web drupal lo más protegido y libre de errores posibles, el proceso, aunque requiere unos cuantos pasos, es bastante sencillo y no suele traer problemas.

Figura 20. Informe de actualizaciones drupal
Fuente: http://www.dataprix.com/blog-it/cms/como-hacer-actualizacion-o-update-drupal

4.4.3. **Actualizar Core de Drupal**

Para la administración del sitio web Quibdomia.com que está desarrollado bajo el CMS Drupal es muy importante mantener el Core y los módulos actualizados. Debido a que las nuevas versiones son solo publicadas cuando se han eliminado los errores o vulnerabilidades detectadas. Cada vez que una nueva versión de Drupal es lanzada, las vulnerabilidades de la versión anterior se hacen públicas y los hackers pueden entrar en el sitio si este desactualizado.

4.4.4. **Usar Captcha**

CAPTCHA es un mecanismo para diferenciar entre usuarios humanos y bots. Para ello se muestra una mezcla aleatoria de caracteres alfanuméricos para que sean copiados por los usuarios. De esta forma, los administradores web lo utilizan para bloquear los bots de spam.

Instalar y configurar captcha en el servidor es muy sencillo y además se cuenta con la seguridad de disponer de una captcha en continua revisión y actualización, tan solo es cuestión de realizar tres pasos: Registrarse en reCAPTCHA http://recaptcha.net/, Incluir el captcha 'recaptchalib.php' en el formulario. Por ejemplo, recaptcha_get_html($captcha_publickey, $error_captcha); finalmente toca validar el captcha utilizando la función llamada recaptcha_check_answer().

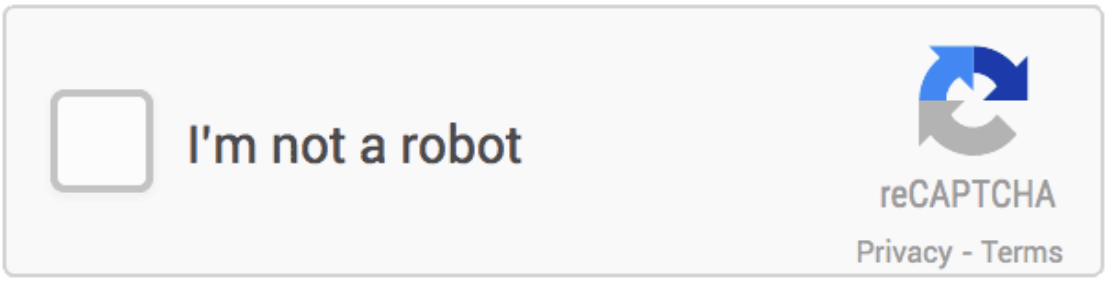


Figura 21. Utilizar captcha en el sitio web
Fuente: Sitio web http://www.apañados.es/tenemos-que-apanar/internet-tutoriales-y-trucos/1061-implementacion-de-no-captcha-el-nuevo-recaptcha-mas-facil-de-usar.html

4.4.5. **Módulos de Seguridad**

EL Gestor de contenidos Drupal tiene disponibles muchos módulos que pueden ser usados para mejorar la seguridad de los sitios web. Las categorías más comunes de seguridad son User Access, Spam Prevention y Security. Por tal motivo

se sugiere meterse en Drupal.org para descargar e instalar los módulos necesarios para el sitio.

Se recomienda utilizar el módulo SecKit, el cual proporciona varias opciones de seguridad y permite mitigar los riesgos de la explotación de diferentes vulnerabilidades de la aplicación web.

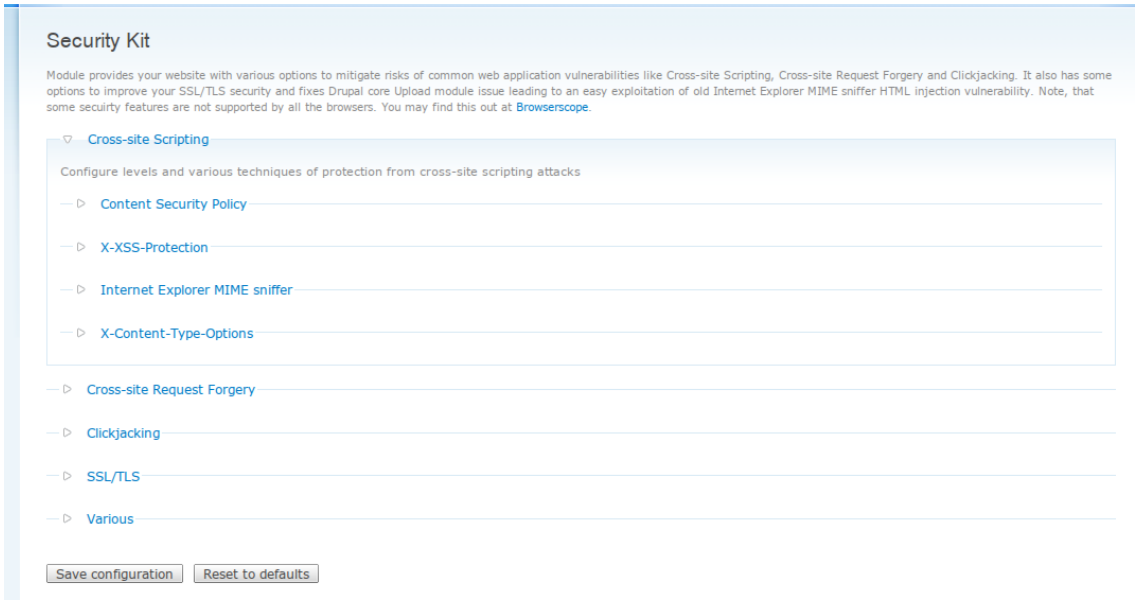


Figura 22. Instalación módulo securty kit de drupal
Fuente: Sitio web https://www.drupal.org/project/security_review

4.4.6. **Obstaculizar el Acceso a tus Ficheros Importantes**

Se recomienda bloquear el acceso a algunos archivos importantes como upgrade.php, install.php o authorize.php, mediante la configuración del fichero .htaccess dentro del sitio web.

4.4.7. **Login Seguro**

Los administradores web deben asegurar las operaciones de inicio de sesión en el sitio. Se debe configurar el máximo de intentos de login inválidos y asegurarse que las direcciones IPs que sean detectadas intentando hackear las contraseñas queden baneadas temporal o permanentemente. Se recomienda usar el módulo Login Security que es una herramienta muy efectiva que no solo controla y restringe el acceso, sino que tiene notificaciones mediante correo electrónico.

Este módulo de seguridad de inicio de sesión mejora las opciones de seguridad en la operación de inicio de sesión del sitio de Drupal. Por defecto, Drupal introduce sólo el control de acceso básico que deniega el acceso IP al contenido completo del sitio. Con este módulo el administrador del sitio puede proteger y restringir el acceso añadiendo funciones de control de acceso a los formularios de inicio de sesión como: limitar el número de intentos de inicio de sesión no válidos antes de bloquear cuentas o denegar el acceso por dirección IP, temporal o permanentemente.

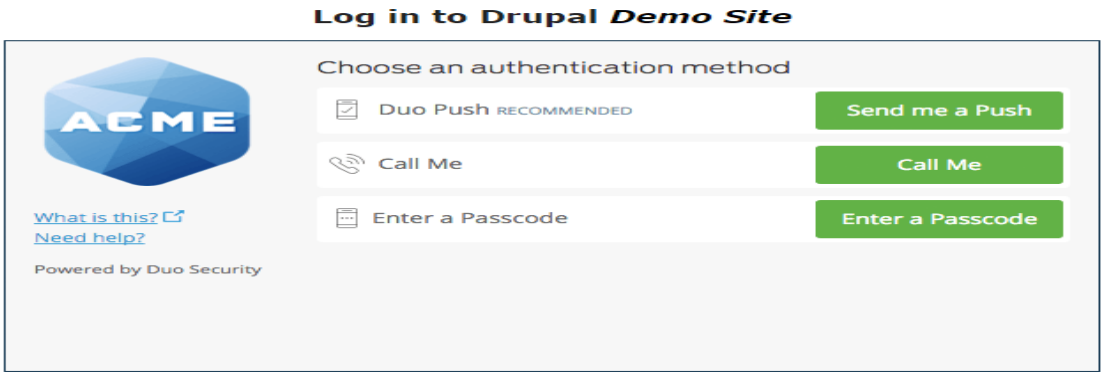


Figura 23. Algunas opciones de seguridad para el login de drupal
Fuente: Sitio web https://duo.com/docs/drupal

4.4.8. **Backups**

El administrador web debe realizar copias de seguridad del sitio web regularmente, estas pueden ser programadas automáticamente desde el hosting o realizarlas manualmente. Independientemente de que el sitio haya sido hackeado, se puede restaurar muy fácilmente. Tanto el contenido del sitio como el contenido de la base de datos MySQL. La copia de seguridad soporta compresión en formatos gzip, bzip y zip.

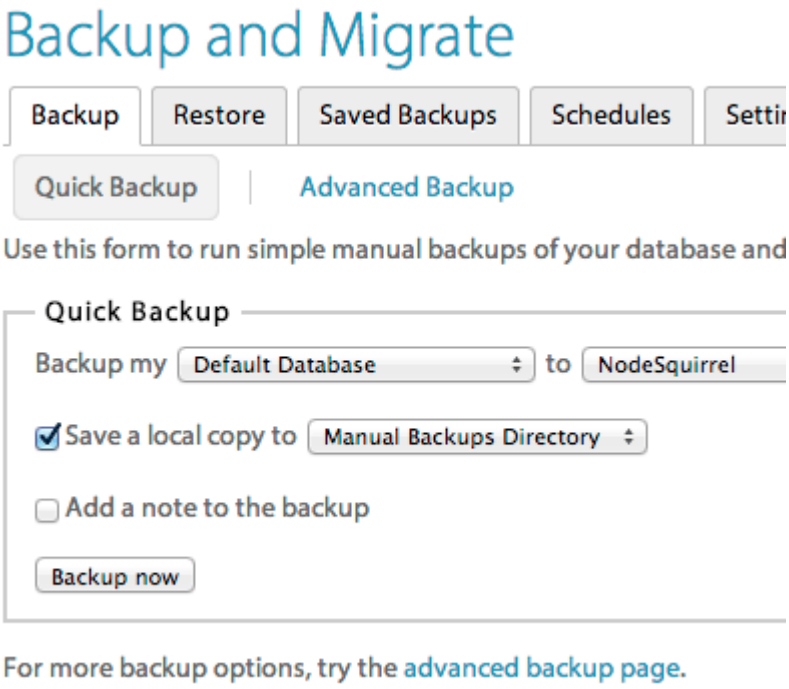


Figura 24. Módulo backup and migrate de drupal
Fuente: Sitio web https://www.drupal.org/project/backup_migrate

4.4.9. **Firewall**

Se recomienda la instalación y configuración de un servidor Firewall que permita filtrar los contenidos con origen y destino al servidor que aloja el sitio web. Formando una DMZ que permita asegurar el acceso correcto al servidor web donde está alojado el sitio. Actualmente se encuentran muchas distribuciones Linux libres que facilitan la configuración de firewalls de manera rápida y sencilla, además de asegurar nuestros recursos de red, en este caso se recomienda utilizar la distribución pfsense.

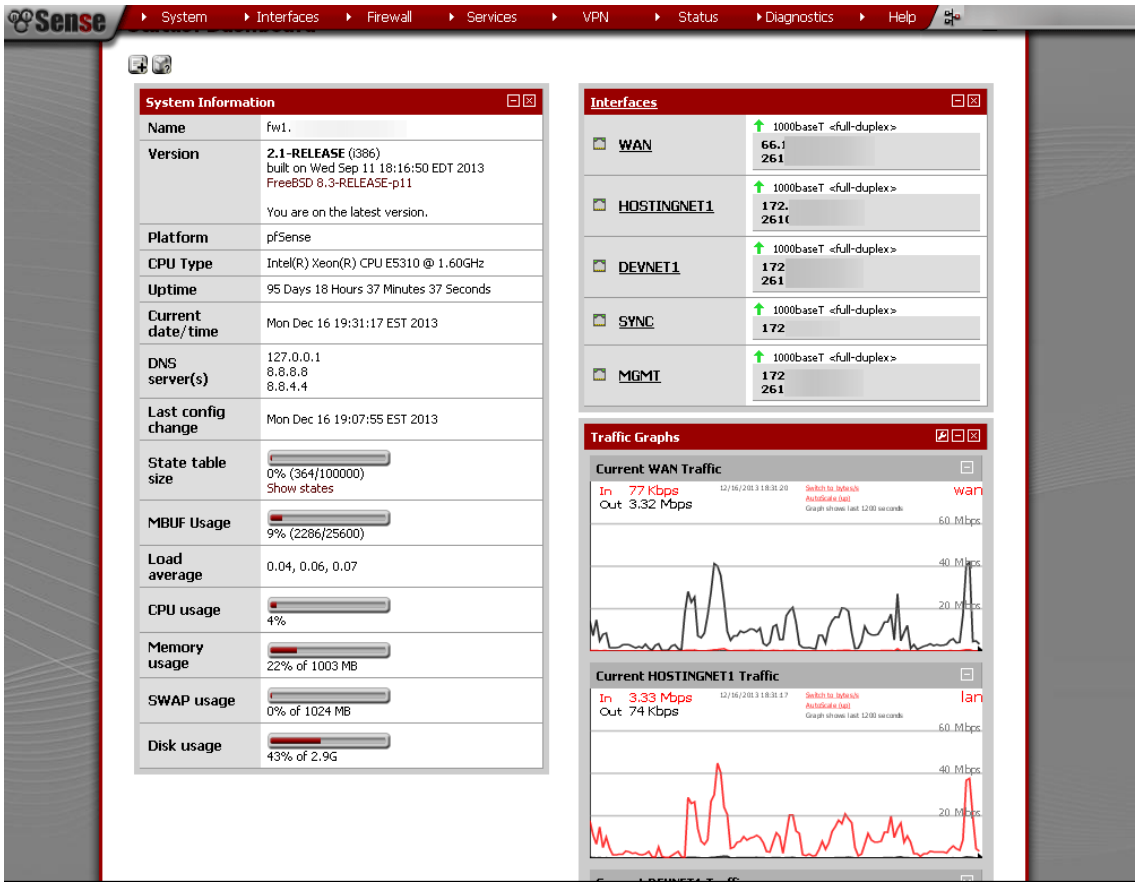


Figura 25. interfaz firewall pfsense
Fuente: Sitio web http://blog.elhacker.net/2015/06/disponible-distribucion-pfsense-2-2-3-orientada-firewall-routeo.html

4.4.10. **Comprobar Permisos de Ficheros y Directorios**

Se recomienda chequear que los permisos de los ficheros y directorios del sitio web son los correctos, No se deben dar permisos totales a carpetas que no los necesiten para no facilitar la inserción de ficheros maliciosos y hay que administrar correctamente los roles y permisos asignados a cada usuario.

4.4.11. **Bloquear la actividad sospechosa a través de los archivos de configuración distribuida**

Se recomienda personalizar determinadas líneas en los archivos de configuración, según se desee restringir el acceso a directorios, ISP, IPs, etc. También se deben gestionar errores del servidor, controlar la caché, etc.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

Realizada la investigación, en este aparte, se presentan las conclusiones y recomendaciones teniendo en cuenta los hallazgos y el análisis de la información.

5.1. Conclusiones

Del diagnóstico sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó www.quibdomia.com se determinó que el administrador de la red se ha encargado de asegurar correctamente el sitio y la información disponible es la que debe estar en esa condición de acuerdo con las herramientas utilizadas.

Se logró Identificar los diferentes ataques a los que está expuesto el sitio web y los servicios en línea que presta la alcaldía de Quibdó. Se realizaron ataques con:

- Paquete Uniscan. No se logró detectar una vulnerabilidad utilizando los diferentes plugins que contiene la herramienta.
- Paquete de Software Nikto. Se pudo evidenciar que el servidor no presento vulnerabilidades detectadas por esta herramienta

Se ejecutaron pruebas de penetración de caja negra al sitio web de la alcaldía de Quibdó utilizando las herramientas que contiene la distribución de software libre Kali Linux y no fue posible bloquear o denegar la vulnerar la confiabilidad, integridad y disponibilidad de la información y servicios en línea publicados por la alcaldía de Quibdó en el portal quibdomia.com.

Se realizó la propuesta de controles que reducen las vulnerabilidades del sitio web de la alcaldía de Quibdó, para ello fue necesario utilizar DRUPAL que es un CMS de código abierto, con el cual, el administrador del sitio puede proteger y restringir el acceso añadiendo funciones de control de acceso a los formularios de inicio de sesión como: limitar el número de intentos de inicio de sesión no válidos antes de bloquear cuentas o denegar el acceso por dirección IP, temporal o permanentemente.

La seguridad de un sitio web está asociada directamente con el desarrollador del sitio, el administrador web y los usuarios, pero también se presentan muchos casos en los que los defectos del servidor o las tecnologías utilizadas permiten que los intrusos puedan afectar la confiabilidad, integridad y disponibilidad de la información.

Se debe actualizar permanentemente el núcleo y los módulos del sitio web www.quibdomia.com que está desarrollado bajo el CMS Drupal, de tal manera que se disminuya el riesgo de ataque informático de hackers que conocen los errores de las versiones anteriores.

El gestor de contenidos Drupal tiene disponibles módulos (Plugins) que deben ser usados para fortalecer la seguridad del sitio web. Las categorías mas comunes de seguridad son Accesos de usuarios y prevención de Spam

5.2. **Recomendación**

Debido a que la información institucional se ha convertido en el activo más valioso que poseen las empresas, es por lo que se le recomienda a la Alcaldía del Municipio de Quibdó, que se hace necesario realizar inversiones en seguridad informática a fin de mantener la disponibilidad, integridad y confiabilidad de esta siguiendo los estándares para la seguridad de la información conforme lo establece la Norma ISO 27002:2013.

Referencias bibliográficas

Alegsa, L. (1998). Diccionario de informática y tecnología. Recuperado el 12 de abril de 2019. Tomado de http://www.alegsa.com.ar/Dic/red_de_computadoras.php

BSI (British Standards Institution 2012). Seguridad de la Información ISO/IEC 27001. Tomado de: http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/.

Catorira, Fernando (24 de Julio de 2012). Penetration Test, ¿En qué consiste? Obtenido del sitio web de we live security: http://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

El espectador – tecnología - Colombia lidera lista de ataques informáticos en países de habla hispana. Tomado de: http://www.elespectador.com/tecnologia/colombia-lidera-lista-de-ataques-informaticos-paises-de-articulo-523201

El espectador, Colombia lidera lista de ataques informáticos en países de habla hispana (2014). Recuperado de: http://www.elespectador.com/tecnologia/colombia-lidera-lista-de-ataques-informaticos-paises-de-articulo-523201

Estrategia gobierno en línea 3.1 2012 - 2017. Manual 3.1 para la Implementación de la Estrategia de Gobierno en línea para entidades del Orden Nacional.

Consultado el 2 de abril de 2019. Tomado de: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

ISO (International Organization Of Estandardization). ISO/IEC 27001:2005. (28 de Febrero de 2012) Tomado de: http://www.iso.org/iso/catalogue_detail?csnumber=42103

Jolman, A. (2012) Seguridad Informática. Tomado de: http://jrobledoherrera.blogspot.com/2009/02/seguridad- informatica.html.

Mahecha Rivera, M. (2016-04-16). Identificación de los ataques más realizados en un sitio concurrido por personas que utilizan sus dispositivos móviles y determinación de las vulnerabilidades más comunes en el sistema operativo Android. Recuperado de http://hdl.handle.net/10596/6337

Martí Talón, RM. (2016). Desarrollo e implementación práctica de un PENTEST. Recuperado de: http://hdl.handle.net/10251/70164.

Mena, M. H., Bejarano, C. K. J. & Palacios, C. J. E. (2013). Estudio del perfil productivo urbano y rural para el municipio de Quibdó. Programa de las Naciones Unidas para el Desarrollo PNUD. Disponible en http://www.redormet.org/documento/perfil-productivo-quibdo/

Ministerio de Tecnologías de la información y las comunicaciones, estrategia gobierno en línea 3.1 (2012 – 2017) Manual de implementación GEL,

Recuperado de: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

Secretaria general de la Alcaldía Mayor de Bogotá (2009). Ley 1273 de 2009. Tomado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Seguridad Informática (2014). Tomado de: https://seguridadinformaticaufps.wikispaces.com/Normatividad+en+la+Seguridad+Inform%C3%A1tica

Serrano, M. (2011) Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala. Recuperado de Universidad Javeriana: http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

ANEXOS

Anexo A. Resumen RAE

1. Información General	
Tipo de Documento:	Trabajo de Grado
Acceso al documento:	Universidad Nacional Abierta y a Distancia UNAD
Título del documento:	Análisis de vulnerabilidades mediante pruebas de penetración avanzada *pentesting* al sitio web oficial de la alcaldía del municipio de Quibdó – Chocó
Autor:	Carlos Andrés Cautín García
Director:	Jorge Enrique Ramírez Montanez
Unidad Patrocinante:	Universidad Nacional Abierta y a Distancia UNAD (Bogotá, Colombia), Ciencias Básicas, Tecnología e Ingeniería, Facultad de Ingeniería de Sistemas.
Palabras Claves:	Seguridad Informática; Sitio Web; Alcaldía de Quibdó; Análisis de Vulnerabilidad.
2. Descripción	
Este documento busca realizar un diagnóstico sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó www.quibdomia.com, durante la investigación se ejecutaron pruebas de penetración utilizando las herramientas que contiene la distribución de software libre Kali Linux, Inicialmente no se tenía conocimiento sobre la infraestructura de red de la organización, de tal manera que realizaron las pruebas a nivel web solo con el detalle de la URL e intentando interrumpir en el sitio web simulando ataques externos realizados por un atacante malicioso. Para realizar este diagnóstico y las pruebas de penetración, el administrador de red debió aplicar conocimientos avanzados en infraestructura de redes, seguridad informática, protocolos TCP / IP y habilidades razonables en uso de sistemas operativos Linux derivados de Debían.	
3. Fuentes	
Los escritos en este documento son el resultado de una investigación aplicada realizada por el investigador, en esta investigación fue necesario revisar otras fuentes bibliográficas que fueron citadas en el documento de acuerdo con el uso de estas, las imágenes que se encuentran en el documento son imágenes propias, tomadas a manera de pantallazo durante la ejecución de las herramientas.	
4. Contenidos	
Este documento inicia con la información básica e introductoria como cualquier proyecto, luego se realiza la etapa de marco referencial, en la cual se detalla toda la parte normativa, teórico y los antecedentes; a continuación, se realiza el diseño	

metodológico del proyecto en el cual queda plasmado como se va a desarrollar el proyecto con sus respectivas fases, cronogramas y presupuestos.

Una vez contextualizados con el proyecto se ejecutan una serie de herramientas libres de la distribución Kali Linux, con las cuales se logra extraer información muy valiosa para identificar las posibles vulnerabilidades con las que cuenta el sitio web a la fecha, con base a toda esta información se desarrolla un capítulo que muestra un diagnóstico de seguridad del sitio web y los posibles ataques a los que está expuesto según la información sustraída con las herramientas.

Finalmente se proponen una serie de controles que permiten mitigar el riesgo de pérdida de la información publicada en el sitio.

5. Metodología

Este trabajo de grado se desarrolló de acuerdo con los elementos o fases de la investigación cualitativa. Determinando un alcance de procedimientos exploratorios, y teniendo en cuenta los diferentes métodos y técnicas propias de cada una de las etapas que se abordaran en el estudio, incluyendo los procedimientos, recolección, procesamiento y análisis de la información, además del seguimiento al cronograma de actividades.

Se comenzó con la formulación de preguntas al administrador de red y administrador del sitio web de la alcaldía de Quibdó, además de la aplicación de un *pentesting* "Prueba de Penetración" para la identificación de vulnerabilidades del sitio web de la entidad y los servicios en línea prestados por la alcaldía de Quibdó.

6. Conclusiones

Se realizó un diagnóstico de alto nivel sobre el estado actual de seguridad del sitio web de la alcaldía de Quibdó, en el cual se establece que el administrador de la red se ha encargado de asegurar correctamente el sitio y la información disponible es la que debe estar en esa condición de acuerdo con las herramientas utilizadas.

Se ejecutaron pruebas de penetración de caja negra al sitio web de la alcaldía de Quibdó utilizando las herramientas que contiene la distribución de software libre Kali Linux y no fue posible bloquear o denegar los servicios prestados por el sitio web.

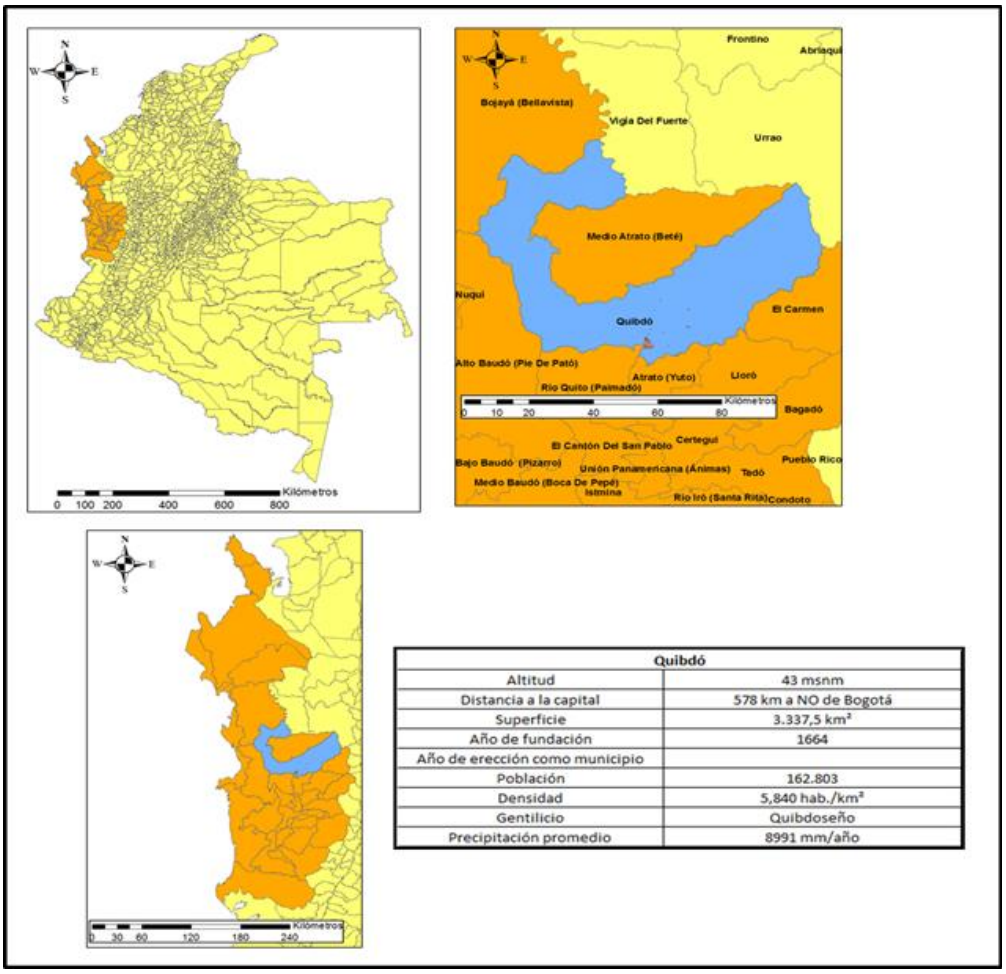
Se logró Identificar los diferentes ataques a los que está expuesto el sitio web y los servicios en línea que presta la alcaldía de Quibdó.

La información institucional se ha convertido en el activo más valioso que poseen las empresas, por tal motivo es necesario realizar inversiones que permitan mantener la disponibilidad, integridad y confiabilidad de esta.

La seguridad de los sitios Web involucra principalmente al desarrollador, al administrador web y a los usuarios, aunque con gran frecuencia se encuentran defectos

que pueden ser aprovechados por atacantes en las tecnologías en que se basan los sistemas web.				
Elaborado por:	Carlos Andrés Cautín García			
Fecha de elaboración del Resumen:		12	04	2019

Anexo B. Ubicación geográfica del Municipio de Quibdó



Quibdó	
Altitud	43 msnm
Distancia a la capital	578 km a NO de Bogotá
Superficie	3.337,5 km²
Año de fundación	1664
Año de erección como municipio	
Población	162.803
Densidad	5,840 hab./km²
Gentilicio	Quibdoseño
Precipitación promedio	8991 mm/año

Fuente: Instituto Geográfico Agustín Codazzi (IGAC)

Anexo C. Ubicación institucional donde se realizó la investigación