UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN

CARRERA: ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES

TEMA: Implementación de hacking ético para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red de la empresa Construlec Cía. Ltda., en Quito-Ecuador.

AUTOR: Flavio Javier Quisaguano Belduma

TUTORA: Ing. Tannia Mayorga Jácome Mg.

2015

APROBACIÓN DEL TUTOR

En mi calidad del Tutora del Trabajo de Titulación certifico:

Que el Trabajo de Titulación “IMPLEMENTACIÓN DE HACKING ÉTICO PARA EL ANÁLISIS DE VULNERABILIDADES, MÉTODOS DE PREVENCIÓN Y PROTECCIÓN APLICADOS A LA INFRAESTRUCTURA DE RED DE LA EMPRESA CONSTRULEC CÍA. LTDA., EN QUITO-ECUADOR”, presentado por el señor Flavio Javier Quisaguano Belduma, estudiante de la carrera de Electrónica Digital y Telecomunicaciones, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D.M., 2015

TUTORA

……

Ing. Tannia Mayorga Jácome Mg.

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORÍA DE PROYECTO DE TITULACIÓN

El abajo firmante, en calidad de estudiante de la carrera de Electrónica Digital y Telecomunicaciones, declaro que los contenidos de este Trabajo de Titulación requisito previo a la obtención del Grado de Ingeniería en Electrónica Digital y Telecomunicaciones, son absolutamente originales, auténticos y de exclusiva responsabilidad legal y académica del autor.

Quito D.M., 2015

……

Flavio Javier Quisaguano Belduma.

CI: 171720224-4

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de Grado, aprueban el Trabajo de Titulación para graduación de acuerdo con las disposiciones reglamentarias emitidas por la Universidad Tecnológica Israel para títulos de pregrado.

Quito D.M., 2015

Para constancia firman:

TRIBUNAL DE GRADO

……

PRESIDENTE

…… ……

MIEMBRO 1 MIEMBRO 2

AGRADECIMIENTO

Agradezco especialmente a Dios por regalarme el aliento de vida cada mañana para poder así entregar lucha, fortaleza y paciencia por cumplir mis sueños.

Gracias de todo corazón a mi querida Universidad Israel por brindarme la oportunidad de continuar con este sueño, a mis distinguidos docentes por su entrega cada día en el aula de clase, a mí estimada tutora que con sus conocimientos y ánimos supo guiar mis pensamientos.

Agradezco sin duda a cada una de esas personas innombradas que creyeron en mí aun cuando el camino se tornaba turbio, a mi familia y amigos, en especial a mi Eloy, mi padre, mi orgullo, por elegir quedarse conmigo ante todas las adversidades, también agradezco sus valores, consejos, paciencia, sonrisa y regaños, que permiten cuidar y guiar mí vida.

Un agradecimiento muy grande a mis amigos de carrera y sobre todo a mis compañeros Daniel y Freddy, ya que juntos empezamos y nos mantuvimos en pie de lucha, brindándonos apoyo y fortaleza cada día, siendo así un orgullo culminar con ellos esta meta.

Agradezco fraternalmente a la empresa Construlec Cía. Ltda., al Ing. Jaime Franco, al Ing. Jaime Franco Jr., y a cada uno de mis compañeros y compañeras de oficina por brindarme sus consejos y apoyo incondicional.

Flavio Javier Quisaguano Belduma

DEDICATORIA

Este trabajo está dedicado con mucho cariño y amor a mi mamita Irmi que como la luna protege mis sueños, a mi súper papá Eloy que como el viento a un ave le brinda fortaleza a mi vida, a mi mami Racke que como el agua le da salud a mi cuerpo, a mi LizZ que como el sol ilumina mi alma, a mis hermanos y hermanas Christian, Ricky, Paul, Daniel, Carly, Gaby y Rocío que llenan éste loco corazón de alegrías.

Flavio Javier Quisaguano Belduma

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Antecedentes

En Ecuador Provincia de Pichincha ciudad de Quito se encuentra CONSTRULEC Cía. Ltda., es una compañía dedicada a la construcción, instalación y montaje de sistemas eléctricos, electrónicos, electromecánicos y electromagnéticos.

CONSTRULEC Cía. Ltda., inició sus operaciones en el año 1970, como el departamento de construcciones de INELIN CIA. LTDA., habiéndose constituido legalmente, en el año 1980. Ha ejecutado con sus ingenieros y técnicos obras de mucha importancia para la Empresa Eléctrica, ex-INECEL, para la empresa de telecomunicaciones ex- ANDINATEL S.A., para la industria, para la Construcción y otras áreas de desarrollo del País.

En general donde se requiere instalaciones eléctricas, electrónicas, electromecánicas y de control, CONSTRULEC Cía. Ltda., ha demostrado su experiencia y la capacidad de sus técnicos.

Para el diseño de proyectos la empresa cuenta con un sistema informático actualizado, además de equipos como un Plotter, Digitalizador de Planos y toda la biblioteca completa de literatura técnica.

Para la ejecución del diseño de proyectos y para la implementación en construcción cuenta con las siguientes áreas de trabajo.

El área de gerencia de proyectos, que es la instancia responsable de la administración de proyectos y es una parte de la estructura funcional de la empresa identificando los proyectos que serán desarrollados de acuerdo con la planificación institucional y presupuestal, además genera, emite y coordina las licitaciones de proyectos, conjuntamente establece las bases de diseño o bases de licitación del proyecto.

El área administrativa, encargada de cubrir las necesidades y usos de fondos de la empresa, obteniendo recursos financieros y usándolos para fines rentables, además, en su función está encargada de la gestión contable y de sistemas por sus aportes de herramientas para controles de auditorías administrativas y financieras, y con la facultad de supervisión del área de recursos humanos integrándola a un proceso de cambio organizacional.

El área de dirección de construcción, que es la encargada de la coordinación y ejecución técnica de los procesos de construcción estableciendo procesos y sistemas de trabajo con los estándares de calidad de acuerdo a las especificaciones técnicas y normas organizacionales y gubernamentales.

El área de proyectos, dedicada al diseño, planeación, dirección, organización, integración, implantación y control de los proyectos constructivos de los sistemas electrónicos y eléctricos de medio y bajo voltaje.

El área de sistemas, responsable de ofrecer soporte técnico y tecnológico de la empresa. Sin embargo los datos son un bien invaluable de las empresas e instituciones para lo cual el administrador de la red, debe identificar mecanismos y herramientas que le permita trasportar los datos de una manera segura.

La seguridad es el aspecto más importante dentro de la empresa CONSTRULEC Cía. Ltda., ya que la información que posee constituye el activo más importante para el desarrollo de sus actividades, por lo que se deben tomar todas las medidas necesarias para precautelar esta información y no ser víctimas de intrusos o delincuentes informáticos.

Además, necesita brindar una transmisión de información ágil y segura tratando en lo posible de mantener los datos en forma confidencial aplicando nuevas tecnologías que no representen gastos económicos si no que ayuden a lograr una máxima seguridad beneficiando así a la empresa y a sus empleados.

A nivel mundial las instituciones tanto públicas como privadas poseen intranets para transmitir su información sea de menor o mayor volumen, el creciente desarrollo de las tecnologías de la información, hace que las empresas, públicas o privadas estén ansiosas de ser parte de esta evolución, pero en los últimos años se ha registrado un creciente número de ataques por parte de crackers hacia los usuarios de Internet, Extranet e Intranet.

En el Ecuador, las instituciones son cada vez más dependientes de sus redes informáticas, un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes especialmente en los servicios de red es un problema que está en crecimiento. Cada vez es mayor el número de atacantes considerando que estos están más organizados, y van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

Problema Investigado

La empresa Construlec Cía. Ltda., posee una infraestructura de red, la cual no ha sido sometida a una detección de vulnerabilidades, tampoco se ha usado métodos de prevención y protección que utilicen aplicaciones tecnológicas usadas a nivel mundial, las mismas que puedan alertar al administrador de red antes de un posible ataque.

Por consiguiente, se requiere construir una propuesta de un plan de seguridad de la información que permita disminuir las amenazas y vulnerabilidades de la red de la empresa mediante mecanismos de protección.

Objetivos

Objetivo General

Implementar el hacking ético para el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la red de la empresa CONSTRULEC Cía. Ltda., ubicada en la ciudad de Quito-Ecuador.

Objetivos Específicos

- Investigar la metodología de hacking ético que proporciona una guía sistemática de cómo realizar ataques a la integridad de la red.

- Analizar las herramientas que provee Kali Linux para realizar el Test de penetración de la red, basado en el método de hacking ético.

- Desarrollar ataques controlados en la red de la empresa CONSTRULEC Cía. Ltda., con las herramientas que posee Kali Linux.

- Establecer una propuesta de seguridad que permita disminuir las amenazas y vulnerabilidades de la red de información de la empresa CONSTRULEC Cía. Ltda.

CAPÍTULO I
FUNDAMENTACIÓN TEÓRICA

1.1. PREÁMBULO

En un mundo en el que se mueven millones de datos y personas, es de vital importancia que las empresas inviertan en seguridad de la información, ya que los datos se han convertido en un bien invaluable para las empresas e instituciones, para lo cual el administrador de la red, debe identificar mecanismos y herramientas que le permita transportarlos de una manera segura.

Hoy en día cualquier persona u empleado puede conectarse a los sistemas de información casi desde cualquier lugar, permitiendo que los empleados porten consigo parte del sistema de información fuera de la infraestructura segura de la compañía.

Por tanto, es de suma importancia el saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del mismo. Este mismo procedimiento se aplica cuando se permite el acceso a la compañía a través de Internet.

La seguridad informática ha adquirido una gran importancia dentro de una empresa, puesto que la información electrónica que posee es uno de sus activos más importantes por lo que se deben tomar medidas necesarias para precautelar esta información y no ser víctimas de intrusos o delincuentes informáticos.

Alcanzar un buen nivel de seguridad para una organización depende de un sistema el cual involucre el concienciar de las amenazas a las que se está expuesto, desde las autoridades de dicha organización, hasta alcanzar a todo el personal.

El sistema debe de proveer seguridad desde el punto de vista de la seguridad informática tanto en lo personal, operaciones cruciales de la organización, ambiente físico, integridad de la red y al acceso de la información.

1.2. SEGURIDAD INFORMÁTICA

En la seguridad Informática es necesario tener en cuenta dos aspectos de protección, la seguridad de la Información y la protección de datos.

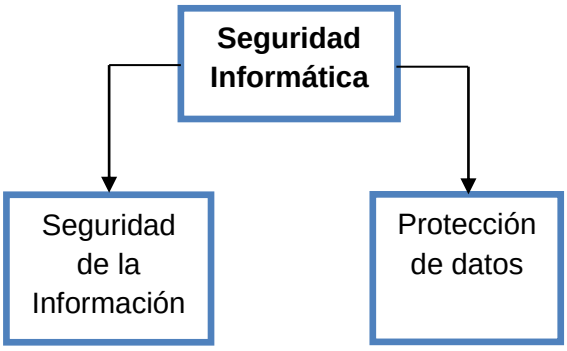


Figura 1.1.- Seguridad Informática

Fuente:(Investigador)

El objetivo de la seguridad de la información según la norma es “preservación de la confidencialidad, la integridad y la disponibilidad de la información, además también pueden estar implicados otras propiedades como la autenticidad, la responsabilidad, el no repudio, y la fiabilidad” (ISO/IEC27000, 2014, pág. 4).

En la protección de datos el objetivo es proteger la integridad de la información de cada persona para poder evitar el abuso de esta, garantizando la confidencialidad, y disponibilidad de los datos.

Es necesario el tratamiento conceptual de ciertos términos con el objetivo de dar unidad, coherencia y consistencia a los postulados.

1.2.1. Activo

Es el recurso primordial en un sistema de información dentro de una organización, según la norma “se denomina activo a cualquier cosa que tenga valor para la organización” (ISO/IEC27001, 2013, pág. 9).

1.2.2. Amenaza

Según la norma ISO/IEC27000, la define como “la causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización” (ISO/IEC27000, 2014, pág. 11).

1.2.3 Ataque

Según la norma ISO/IEC27000, ataque “es aquel evento que intente destruir, exponer, alterar, inutilizar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo” (ISO/IEC27000, 2014, pág. 1).

1.2.4 Autenticidad

Según la norma ISO/IEC27000, “es la propiedad de que una entidad es lo que afirma ser” (ISO/IEC27000, 2014, pág. 2).

1.2.5 Confidencialidad

Según la norma ISO/IEC27000, establece que “es la propiedad de que la información no esté disponible o se revelará a personas no autorizadas, entidades o procesos” (ISO/IEC27000, 2014, pág. 2).

1.2.6 Contramedida

Según el autor “son mecanismos o procesos diseñados para disminuir los efectos subsiguientes a una amenaza, o amenazas, que ya ha(n) tenido lugar. Así pues, a diferencia de las medidas preventivas, las contramedidas son instaladas una vez que la amenaza se ha cumplido” (Calle Guglieri, 2012, pág. 75).

1.2.7 Disponibilidad

Según la norma ISO/IEC27001, se establece que “la disponibilidad es la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada” (ISO/IEC27001, 2013, pág. 9).

1.2.8 Integridad

Según la norma ISO/IEC27001, “es la propiedad de salvaguardar la exactitud e integridad de los activos” (ISO/IEC27001, 2013, pág. 10).

1.2.9 Medida

Según la norma ISO/IEC27000, “es la variable a la que se asigna un valor como el resultado de la medición” (ISO/IEC27000, 2014, pág. 6).

1.2.10 No Repudio

Significa el no-rechazo a las reglas planteadas por el administrador del sistema, según la norma ISO/IEC27000, “es la capacidad de probar la ocurrencia de un evento o una acción reivindicada y sus entidades originarias” (ISO/IEC27000, 2014, pág. 7).

1.2.11 Riesgo

Se considera un riesgo a la posibilidad de que se produzca un ataque determinado a un activo, siendo esta en un usuario o en toda la organización. Según la norma ISO/IEC27000, establece que “el riesgo es el efecto de la incertidumbre en los objetivos” (ISO/IEC27000, 2014, pág. 8).

1.2.12 Vulnerabilidad

Según la norma ISO/IEC27000, “es la debilidad de un activo o de control que puede ser explotado por una o más amenazas” (ISO/IEC27000, 2014, pág. 12).

1.3 ATAQUES Y VULNERABILIDADES

Las redes de información de una organización a menudo son víctimas de atacantes utilizando diferentes técnicas para quebrantar la seguridad de las mismas, entre estos los ataques más comunes son:

1.3.1 Denegación de Servicio

Es un tipo de ataque en el cual la meta se convierte en negarle el acceso a un servicio o de un recurso a la víctima, estos pueden dejar inoperativa una computadora o a la red misma de la empresa. Según el autor “denegación de servicio es la forma de ataque informático, que sin afectar a la información de un sistema, le impide prestar el servicio por saturación o bloqueo” (Gonzáles Ruz, de la Mata Barranco, Morón Lema, Mata, Moreno, & Morales , 2012, pág. 398).

1.3.2 Password Cracking

Se lo llama a aquella acción que busca descifrar las contraseñas de determinadas aplicaciones elegidas por el atacante (Kaufmann, 2011, pág. 283).

1.3.3 E-mail Bombing y Spamming

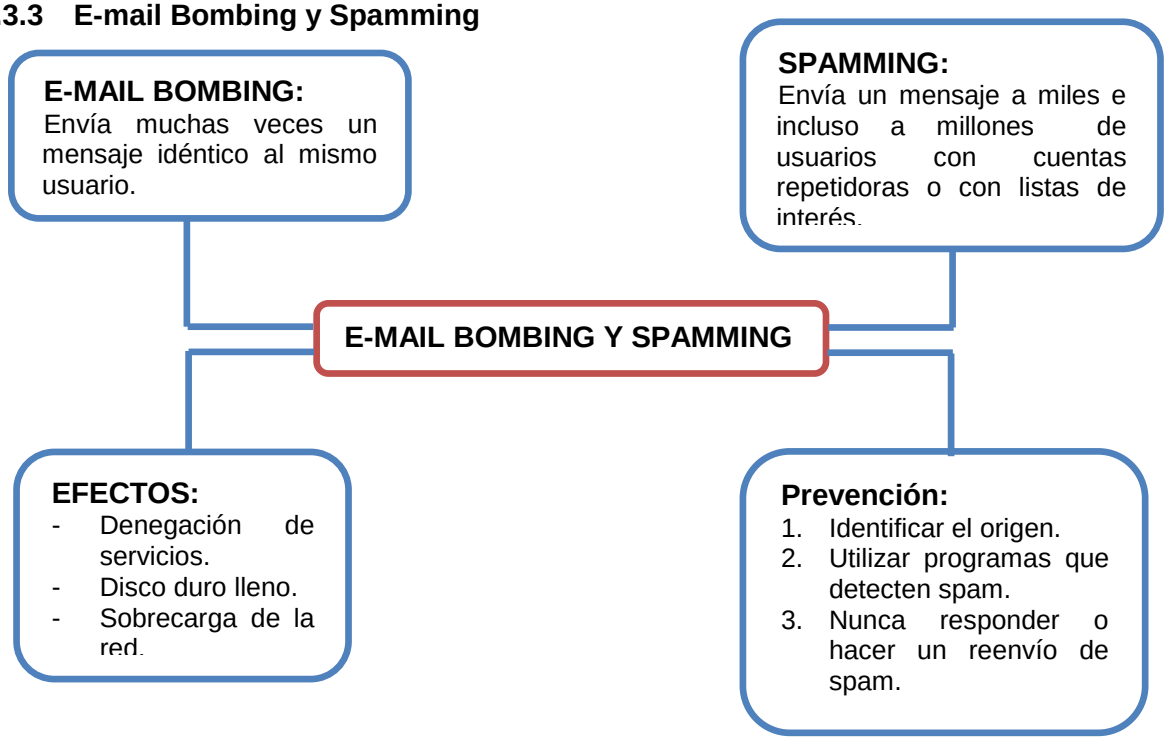


Figura 1.2.- E-mail Bombing y Spamming

Fuente:(Investigador)

1.4 POLÍTICAS DE SEGURIDAD INFORMÁTICA

Una política de seguridad es aquel compromiso descrito en un documento para establecer reglas claras para una mejor defensa de la red, es por ello que los usuarios deben firmar un documento y a su vez ser capacitados con la forma en que se debe manejar la información, conociendo así lo que se puede hacer o no en el sistema (ISO/IEC27002, 2013, pág. 2).

Una política de seguridad está comprometida a prestar una mejor defensa a los empleados de acciones perjudiciales por parte de intrusos internos o externos.

Para que una política de seguridad sea efectiva se debe trabajar en conjunto con todo el personal permitiendo que el compromiso de seguridad se lo tome responsablemente. El reglamento define la protección del empleado y de la empresa en caso de alguna mala acción en contra de la integridad de la red, a su vez el detalle de las actividades prohibidas, excepciones a ciertas prohibiciones de acuerdo a la naturaleza del cargo a asumir del empleado.

Las políticas no siempre deben ser un documento de muchas hojas sino simplemente las necesarias, en las que se formulen políticas específicas como: de correo electrónico, de contraseñas, de emisión de cuentas de usuario, entre otras.

Existen razones para tener políticas de seguridad, entre estas se tienen a:

1. Para cumplir con regulaciones establecidas en conjunto con la gerencia.
2. Para permitir unificar la forma de trabajo a los empleados que tienen cargos similares.
3. Para permitir encontrar las mejores prácticas laborales.

Finalmente una política de seguridad establece que bienes deben ser protegidos y dar pautas sobre cómo hacerlo, determinando herramientas de seguridad y estrategias que deben ser implementadas en la red.

1.5 HACKING ÉTICO

Un Hacker Ético es la persona que usa sus conocimientos de informática para realizar las diferentes pruebas en las redes de una empresa utilizando herramientas de software para poder encontrar sus debilidades de seguridad, con ello encontrar una forma de defensa y protección hacia intrusos de una forma legal (Corletti Estrada, 2011, pág. 505).

1.6 TÉRMINOS Y DEFINICIONES

A los efectos de este documento es necesario definir los términos más importantes.

1.6.1 Amenaza

Se conceptualiza en este documento en el enunciado 1.2.2.

1.6.2 Ataque

Se conceptualiza en este documento en el enunciado 1.2.3. los ataques muchas veces son ocasionados a través de un exploit.

1.6.3 Vulnerabilidad

Como se lo menciono antes es una debilidad del sistema comprometiendo al activo y se las puede encontrar en algunos aspectos como tales como:

En el diseño: Es aquella debilidad que se transmite en el diseño de protocolos utilizados en la red de la compañía.

En la Implementación: Se manifiestan a través de los errores de programación, existencias de puertas traseras en el sistema informático.

En el Uso: Puede darse por un desconocimiento y falta de compromiso por parte de los usuarios y del responsable de informática, también porque se puede tener una disponibilidad de herramientas que puedan facilitar los ataques.

1.6.4 Virus

Los virus son malwares o programas maliciosos destinados con el fin de dañar o modificar archivos del sistema informático, pueden propagarse a través de software y pueden tomar el control del sistema operativo (Pardo, 2010, pág. 157).

1.6.5 Spoofs

Los Spoofs es una técnica que prioriza la suplantación de identidad para poder obtener un acceso ilegitimo al sistema informático (Gonzáles Ruz, de la Mata Barranco, Morón Lema, Mata, Moreno, & Morales , 2012, pág. 408).

1.6.6 Port Scanning

El port scanning o escaneo de puertos consiste en determinar características de una máquina conectada a una red o sistema remoto, identificando así sus puertos abiertos o cerrados y también se puede detectar si esta protegidos por un cortafuegos (Zhenyu, 2012, pág. 33).

1.6.7 Exploits

Exploits es un software dedicado a aprovechar las vulnerabilidades que se puedan dar en la red de información y así romper su seguridad, llevándola a perder su integridad tomando ventajas de ellas (Serrano, 2010, pág. 130).
Existen diferentes tipos de exploits y estos pueden ser:

- ***Exploit remoto*:** es aquel que necesita una red de comunicaciones para acceder a la máquina o con el sistema victima siendo esta una red interna o aquella del internet.
- ***Exploit local*:** es aquel que para ejecutarlo necesita tener acceso al sistema de datos.
- ***Exploit ClientSide*:** este tipo de exploit aprovecha la vulnerabilidad de las aplicaciones sensibles que están instaladas en las estaciones de trabajo de la compañía, estas necesitan que el usuario abra un archivo o que de un click en algún enlace.

1.7 CLASIFICACIÓN DEL HACKER

Los hackers pueden ser divididos en cuatro principales grupos los cuales están descritos a continuación:

1.7.1 Black Hats

Un Black hats o hacker de sombrero negro es considerado a toda aquella persona que busca a través de sus conocimientos penetrar en un sistema informático de una forma ilegal buscando así un bien económico o simplemente el gusto por lograr romper una defensa, sea ésta a computadoras, colapsando servidores o también deleitándose entrando a zonas restringidas, creando así muchos daños incuantificables y a su vez grandes problemas inmanejables, siendo de esta manera un gran dolor de cabeza para el profesional de sistemas (Graves, 2012, pág. 12).

1.7.2 White Hats

Se dice White hats o hacker de sombrero blanco a toda aquella persona con conocimiento de penetración en un sistema pero con el objetivo de utilizar sus herramientas profesionales para encontrar vulnerabilidades en el sistema informático y fortalecerlo a través de contramedidas, estos hacker de sombrero blanco se caracterizan por tener el respaldo de un permiso del titular de datos de la compañía, diferenciándolo así de un hacker malicioso (Graves, 2012, pág. 12).

1.7.3 Gray Hats

Gray Hats o Hackers de Sombreros grises son considerados así a toda persona que juega el papel de ética ambigua, es decir que usa todos sus conocimientos informáticos bajo el concepto de hacker de sombrero negro para poder romper la defensa de un sistema, para luego ofrecer sus servicios como hacker de sombrero blanco, pero esta vez bajo un contrato (Graves, 2012, pág. 12).

1.7.4 Cracker

Es considerado un cracker a toda persona natural que utiliza sus conocimientos y herramientas informáticas para diseñar programas que puedan romper seguridades de software, también este tipo de hacker puede ampliar funcionabilidades de software o del mismo hardware a través de los conocidos cracks, key generators, entre otros (Gonzáles Ruz, de la Mata Barranco, Morón Lema, Mata, Moreno, & Morales , 2012, pág. 397).

Este tipo de hacker también posee el poder de entrar en sistemas vulnerables y dañarlos, ya sea dejando algún virus o robando información, adicionalmente estos hackers crean puertas traseras para poder ingresar nuevamente al sistema de información.

1.8 TEST DE PENETRACIÓN

Test de Penetración o Pruebas de penetración es denominado así al conjunto de técnicas utilizadas para el análisis y evaluación de la seguridad del sistema informático (Corletti Estrada, 2011, pág. 505).

Esta técnica o dicha así metodología no es un trabajo fácil de realizar y requiere de los suficientes conocimientos de las tecnologías involucradas en el sistema como lo es las aplicaciones y servicios, permitiendo de esta manera obtener un documento donde se

ofrece la información del sistema, por estas obvias razones es necesario definir un plan de trabajo para evaluar correctamente al sistema de seguridad.

Las razones por las que se puede realizar un test de penetración pueden ser la determinación de la viabilidad de un ataque sea este externo o interno, la evaluación del impacto de un ataque permite identificar la magnitud y el grado de vulnerabilidad de la defensa de un sistema informático, proporcionando así evidencia para mejorar el control de la defensa del sistema de información, siendo necesario realizar un test de penetración anualmente o de forma permanente de acuerdo a los diferentes cambios del sistema en sí, brindando de esta manera una solución antes de que el cyber-delincuente aproveche alguna debilidad.

Para la persona que lleva a cabo la auditoria está encargado de dar a conocer las deficiencias de la seguridad, para posteriormente mejorar los niveles de seguridad por ello sus objetivos deben ser:

- Evaluación de un sistema.
- Mejora continua de seguridad.
- Conocer la situación real de la compañía.
- Medir y obtener una valoración objetiva del nivel de seguridad de la compañía.

Los resultados obtenidos de la prueba de penetración contienen un informe detallado dividido en secciones frente a las debilidades encontradas en el estado actual del sistema informático, incluyendo también las contramedidas y sus recomendaciones.

1.8.1 Tipos de Test de Penetración

Los cyber-delincuentes pueden realizar ataques en forma externa o interna en la red de comunicación, siendo así que los ataques externos son más fáciles de detectar y repeler que los mismos ataques internos ya que los ataques del mismo poseen libre acceso a toda la red incluyendo el servidor (EC-Council, 2010, pág. 6).

Este test de penetración puede tener un alcance muy amplio o puede también ser focalizado a determinados equipos concretados así en reuniones previas con el administrador del sistema definiendo a su vez los tiempos de ejecución que reflejen el estado de la seguridad informática de la compañía, por lo general no suelen demorar más de un mes.

1.8.1.1 Test de Penetración Externo

Se lo considera de esta forma a las pruebas de seguridad informática que simulan una intrusión desde fuera de la instalación realizando así actividades como el barrido de líneas telefónicas, un análisis del sistema de accesos remoto, pruebas de intrusión en la conexión a internet, la comunicación con otras redes y además en las aplicaciones web (EC-Council, 2010, pág. 7).

1.8.1.2 Test de Penetración interno

Conocido así porque las pruebas de seguridad informática se las realizas desde dentro de la instalación de la compañía permitiendo realizar pruebas en la seguridad informática en los dispositivos de red internos, servidores, estaciones de trabajo, base de datos e incluso redes inalámbricas (EC-Council, 2010, pág. 10).

1.8.2 Metodologías de Hacking Ético

Para realizar una prueba de penetración en alguna red de información existen 3 tipos de metodologías en hacking ético.

1.8.2.1 Test de Caja Blanca

En este tipo de prueba se simula un ataque real al sistema de red del objetivo planteado conociendo de antemano gran parte información de la red evitando de esta manera la fase de recolección de Información.

1.8.2.2 Test de Caja Negra

En este tipo de prueba se simula un ataque real al sistema de red del objetivo planteado sin disponer de la información de la red, lo que obliga a realizar análisis muy meticulosos del objetivo.

1.8.2.3 Test de Caja Gris

En este tipo de prueba se simula un ataque real al sistema de red del objetivo planteado conociendo parte de la información técnica de la red y desconociendo a su vez ciertos detalles de la misma lo que obliga a realizar una prueba un poco más meticulosa que la de un Test de caja Blanca, por ello a este tipo de prueba se la conoce como mezcla entre un Test de caja Blanca y un Test de caja Negra.

CAPÍTULO II
DIAGNÓSTICO DEL PROBLEMA Y BREVE DESCRIPCIÓN DEL PROCESO INVESTIGATIVO

2.1 PROBLEMA PRINCIPAL

La seguridad es el aspecto más importante dentro de la empresa CONSTRULEC Cía. Ltda., ya que la información que posee constituye el activo más importante para el desarrollo de sus actividades, por lo que se deben tomar todas las medidas necesarias para precautelar esta información y no ser víctimas de intrusos o delincuentes informáticos.

Además, necesita brindar una transmisión de información ágil y segura tratando en lo posible de mantener los datos en forma confidencial aplicando nuevas tecnologías que no representen gastos económicos si no que ayuden a lograr una máxima seguridad beneficiando así a la empresa y a sus empleados.

La empresa CONSTRULEC Cía. Ltda., posee una infraestructura de red, la cual no ha sido sometida a una detección de vulnerabilidades, tampoco se ha usado métodos de prevención y protección que utilicen aplicaciones tecnológicas usadas a nivel mundial que permitan alertar al administrador de red antes de un posible ataque.

Las instituciones a nivel mundial tanto públicas como privadas poseen intranets para transmitir su información, sea de menor o mayor volumen, el creciente desarrollo de las tecnologías de la información, hace que las empresas, públicas o privadas estén ansiosas de ser parte de esta evolución, pero en los últimos años se ha registrado un creciente número de ataques por parte de crackers hacia los usuarios de Internet, Extranet e Intranet.

En el Ecuador, las instituciones son cada vez más dependientes de sus redes informáticas, un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes especialmente en los servicios de red es un problema que está en crecimiento. Cada vez es mayor el número de atacantes considerando que estos están más organizados, y van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

2.2 EXPLICACIÓN DEL POR QUÉ Y PARA QUÉ DE LOS OBJETIVOS

2.2.1 Objetivo General

Implementar el hacking ético para el análisis de vulnerabilidades en la red de información de la empresa Construlec Cía. Ltda., es esencial para poder establecer métodos de prevención y protección a la red de la misma, ya que ayudará a construir una propuesta de seguridad de la información que permita disminuir las amenazas y vulnerabilidades de la red de la empresa mediante mecanismos de protección.

2.2.2 Objetivos Específicos

- Investigar la metodología de hacking ético proporcionará una guía sistemática de cómo realizar ataques a la integridad de la red.

- Analizar las herramientas que provee Kali Linux permitirá realizar un prueba de penetración basada en el método de hacking ético a la red de la empresa Construlec Cía. Ltda.,

- Desarrollar ataques controlados en la red de la empresa CONSTRULEC Cía. Ltda., con las herramientas que posee Kali Linux, permitirá tener una mejor visión de la seguridad que posea la infraestructura de red de la empresa.

- Establecer una propuesta de seguridad permitirá disminuir las amenazas y vulnerabilidades de la red de información de la empresa CONSTRULEC Cía. Ltda.

2.3 HIPÓTESIS

El análisis de vulnerabilidades mediante la aplicación de Hacking ético permitirá conocer las deficiencias en materia de seguridad que existan en la infraestructura de red de la empresa Construlec Cía. Ltda., a la vez se podrá generar una propuesta que dote de un mayor nivel de seguridad, para disminuir las amenazas y vulnerabilidades de la red de información de la empresa Construlec Cía. Ltda.

2.4 NORMATIVA

Para la ejecución del presente trabajo de titulación se tomo como guía y referencia las normas de la familia ISO/IEC 27000 publicadas por la Organización Internacional para la estandarización y la Comisión Electrotécnica Internacional, las cuales permiten coordinar y organizar esfuerzos e ideas para la obtención, aplicación y gestión de un plan de seguridad.

La normativa ISO/IEC 27000 Sin duda proporciona una visión general de la familia, puesto que maneja un glosario general, para de ésta manera poder entender cada extracto de la norma.

La normativa ISO/ 27001 especifica una serie de requisitos que permiten implantar un Sistema de Gestión de Seguridad de la Información, además proporciona un enfoque de gestión de riesgos y promueve la mejora continua de los procesos para poder obtener un plan de seguridad eficiente (ISO/IEC27001, 2013, pág. 5).

La normativa ISO/ 27002 publicada en el año 2013 está diseñada para la selección de los controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información o como un documento de orientación para las organizaciones ejecutoras de controles de seguridad de la información (ISO/IEC27002, 2013, pág. 5).

2.5 METODOLOGÍA

Para elaboración del presente trabajo se utilizo una técnica de investigación a través de la entrevista al Señor Jordán Vinueza, Administrador de red de la empresa Construlec Cía. Ltda., en la cual corrobora la necesidad de realizar una prueba de penetración en la infraestructura de red de la empresa para poder generar una propuesta de seguridad de la información para la empresa; misma que se encuentra adjunta como Anexo 39.

La ejecución del proyecto se la realizó en cuatro etapas, cada una de ellas utilizando un método de investigación detallado a continuación:

En la primera etapa, para la de investigación se manejará el método de análisis y síntesis, para realizar la correcta recopilación de información necesaria.

En la segunda etapa se usará el método analítico para realizar de forma adecuada el test de penetración de la red, utilizando las herramientas que prevé Kali Linux.

En la tercera etapa de elaboración se utilizará el método experimental, para realizar las diferentes pruebas de ataques controlados basándose en el método de hacking ético.

En la cuarta etapa se aplicará el método inductivo el cual permitirá analizar casos particulares permitiendo extraer conclusiones de carácter general.

2.6 RESULTADOS ESPERADOS

Una vez investigada la metodología de hacking ético, se espera obtener una guía sistemática de cómo realizar ataques a la integridad de la red de la empresa, para así poder aplicar las herramientas que provee Kali Linux en una prueba de penetración basada en el método de hacking ético. Además con la realización de ataques controlados en la red de la empresa con las herramientas que posee Kali Linux, se espera obtener una propuesta de seguridad que ayudará a disminuir las amenazas y vulnerabilidades de la red de información de la empresa CONSTRULEC Cía. Ltda.

CAPÍTULO III
PRESENTACIÓN DE RESULTADOS

3.1 ANÁLISIS DE SEGURIDAD

Entendiendo que la explotación de las vulnerabilidades informáticas puede ser muy perjudicial para uno de sus activos más preciados como lo es los datos de información en una compañía, se debe implementar una arquitectura de seguridad con la finalidad de preservar la integridad y la disponibilidad de los recursos.

Por ello el método escogido para el análisis de seguridad es el de un profesional de hacking ético, siendo así puntualizado a continuación.

3.2 HERRAMIENTAS DE HACKING ÉTICO

Existen varias herramientas que permiten realizar pruebas de penetración a fines de prevenir, monitorear y mejorar la seguridad de un sistema informático, los cuales se encuentran disponibles en LiveCD por lo que permiten rápidamente probarlos y usarlos sin tener que alterar el sistema operativo instalado, entre los cuales se destacan WIFislax, WIFIway, S-T-D, Pentoo y Kali Linux. A continuación se puede observar una tabla comparativa de estas herramientas calificándolas con una escala valorativa que va de 1 a 5 donde 5 es el valor equivalente a la mejor calificación.

Herramienta	Ventajas	Desventaja	Calificación
WIFIway	Utilizada en redes WiFi, Bluetooth y RFID Se la puede encontrar en idioma español.	Solo sirve para redes inalámbricas.	1
WIFislax	Se usa para efectuar operaciones de auditoría de seguridad WiFi en toda clase de entornos.	Las versiones de wifislax no son actualizables, siempre hay que formatear e instalar una nueva.	2
S-T-D	Diseñado para profesionales que se sienten cómodos trabajando con comandos.	Asume que conoce los conceptos básicos de Linux como la mayor parte de su trabajo se realizará desde la línea de comandos.	3

Pentoo	Herramientas diversas para el Pentest sobre la red de información y se lo puede utilizar en redes alámbricas e inalámbricas	Es un software experimental y disponible sólo para sistemas de 64 bits.	4
Kali Linux	Evolución de BackTrack con más de 300 herramientas para el proceso del test de penetración, fácil de utilizarla, se la puede utilizar en redes alámbricas e inalámbricas, sistemas de 32 y 64 bits, versiones actualizables sin necesidad de reinstalar.	Aunque cuenta con más de 300 herramientas de pentest, muchas de las que son nuevas para BackTrack no siempre se incluyen todos los drivers, aunque se ha avanzado mucho al respecto.	5

Tabla 3.1.- Herramientas de Hacking ético

Fuente:(Wifiway, 2014), (Wifislax, 2014). (S-T-D, 2014). (Pentoo, 2014), (KaliLinux, 2014), (Investigador).

3.2.1 KALI LINUX

BackTrack es sin duda una herramienta muy popular y la más acogida por parte del profesional de seguridad de la información ya que posee un conjunto de aplicaciones para llevar a cabo las diferentes pruebas de penetración en el sistema informático de una compañía, sin embargo evoluciona a una herramienta mucho más fuerte en todas sus aplicaciones, llamada Kali Linux (KaliLinux, 2014).

Figura 3.1.- Logo BackTrack

Fuente: (debianArt, 2014)

Kali-Linux derivada de BackTrack deja a un lado sus raíces de LiveCD y se convierte en un sistema operativo avanzado para el Pentest y se adhiere a los estándares de Debian dándole así su principal diferencia ante BackTrack ya que éste usa como base a Ubuntu, sin embargo se lo puede obtener en LiveCD o LiveUSB (KaliLinux, 2014).

Figura 3.2.- Logo Kali Linux

Fuente: (KaliLinux, 2014)

Kali Linux dispone de un abanico de herramientas todas ellas destinadas a realizar pruebas, diagnósticos y comprobaciones de aspectos importantes para evaluar la seguridad informática de los equipos destinados (KaliLinux, 2014).

Para que Kali Linux ocupe la preferencia de un Software de seguridad se debe a que es fácil de usar y a la vez es superior ante otras herramientas ofertadas en el mercado poseyendo varias herramientas de trabajo entre las que se puede clasificar por su funcionabilidad:

- ***Enumeration***: Se puede obtener información acertada sobre el equipo analizado como el kernel, sistema operativo, entre otros (KaliLinux, 2014).
- ***Exploit Archives***: En esta rama se encuentran todos los exploits (KaliLinux, 2014).
- ***Fuzzers***: Justamente aquí se puede encontrar herramientas que sirven para buscar fallos en un protocolo (KaliLinux, 2014).
- ***Spoofing***: En esta sección se recogen técnicas de suplantación de identidad como por ejemplo cambios de IP, falsificación de tabla ARP, etc (KaliLinux, 2014).
- ***Tunneling***: Con ella se puede básicamente implementar un protocolo de red sobre otro (KaliLinux, 2014).
- ***Forensic Tools***: Con este componente se puede realizar un análisis completo a aquellos sistemas que han sufrido algún tipo de ataque, permitiendo arreglarlos y ser prevenidos para el futuro (KaliLinux, 2014).

3.3 FASES DE PENETRACIÓN DE UN SISTEMA

Las fases de Ethical Hacking tienen diversas variantes pero en general un hacker ético debe seguir un proceso para obtener y poder mantener la entrada en un sistema informático, estos pasos pueden tener similitudes a los que da un atacante malicioso,

de los cuales se pueden mencionar a continuación 5 fases para la intrusión en un sistema de información (Benchimol, 2011, pág. 138).

3.3.1 Fase de Reconocimiento

Es necesario antes de empezar una intrusión el mantener un reconocimiento y recopilación de toda la información posible del objetivo preestablecido, es así que se establece la primera fase también conocida como FootPrinting o huella.

El footprinting es vital para poder desarrollar una técnica de intrusión al medio, a su vez debe ejecutarse de una manera organizada ya que la información puede llegar de varias capas de red y pueden ser utilizadas a lo largo de las posteriores fases (Benchimol, 2011, pág. 141).

La información encontrada gracias a FootPrinting puede abarcar direcciones de correo electrónico, información personal de los empleados, topología de red, direcciones IP, servicios de red y sus aplicaciones, entre otros (Benchimol, 2011, pág. 142).

Existen métodos que pueden ayudar a cumplir el objetivo y uno de estos es la ***Búsqueda Online***, la cual permite buscar la información mediante el internet, para ello se puede respaldar de Google Hacking, herramienta que permite utilizar funciones de búsquedas avanzadas. ***Búsqueda Offline****,* permite realizar los diversos procesos de búsqueda mediante software como por ejemplo Kali Linux (Benchimol, 2011, pág. 143).

3.3.2 Fase de Exploración

Para desarrollar la fase de exploración se debe partir de la recolección de la información previa y de este modo poder detectar un método de ataque en la infraestructura de red de la compañía (Benchimol, 2011, pág. 144).

Para que una exploración de resultados se debe seguir estos pasos:

Paso 1:

Escaneo de Puertos.- Implica la determinación de puertos abiertos para poder asociarlo a un servicio y además permite determinar que host está activo (Benchimol, 2011, pág. 145).

Paso 2:

Determinación del Sistema Operativo.- En ella se puede determinar el sistema operativo del host a partir de las respuestas que el mismo brinde frente a

determinados paquetes, siendo estos interpretados por alguna aplicación dada (Benchimol, 2011, pág. 146).

Paso 3:

Identificación de Servicios.- Se puede llegar a una determinación de servicios a través de los banner predeterminados siendo ellos las leyendas que traen las aplicaciones como puede ser su versión, su arquitectura, entre otras. También se puede identificar un servicio mediante la asociación de sus puertos abiertos (Benchimol, 2011, pág. 147).

Paso 4:

Identificación de Vulnerabilidades.- En ésta se puede encontrar las diversas vulnerabilidades de los equipos del usuario dependiendo de los servicios prestados en ese instante, estos pueden ser los servicios web, E-mail, entre otros. Se puede partir además del sistema operativo sea éste Windows. Linux. Mac OSX, e incluso se puede determinar ciertas vulnerabilidades conocidas a través de aplicaciones dadas, como por ejemplo Apache (Benchimol, 2011, pág. 147).

Paso 5:

Planificación de la intrusión.- En este último paso se prioriza llevar a cabo el proceso de anonimización de la intrusión ya que es necesario no dejar rastros de lo que se está haciendo o de lo que se hizo en procesos anteriores (Benchimol, 2011, pág. 147).

3.3.3 Fase de Enumeración

Para entrar a esta etapa es necesario partir de un buen proceso de footprinting ya que así se puede obtener nombres y cuentas de usuario, grupos de trabajo, recursos compartidos, recursos de NetBios, nombres de máquinas y los diferentes servicios de la intranet del objetivo, para de esta forma obtener resultados óptimos en la penetración del sistema (Benchimol, 2011, pág. 148).

Un profesional de seguridad debe tener en cuenta actividades que le permitan desarrollar una buena etapa de enumeración y estas son:

Extracción de nombres de usuario en Windows.

Extracción de nombres de usuario usando SNMP.

Extracción de nombres de usuario de las IDs de E-mail.

Extracción de información utilizando Password por defecto.

3.3.4 Fase de Análisis de Vulnerabilidades

Esta fase tiene como objetivo primordial el identificar si un sistema es débil o susceptible de ser afectado o atacado de alguna manera utilizando métodos qué permitan describir las respectivas debilidades del sistema de información (Benchimol, 2011, pág. 149).

En esta fase se debe enfatizar las prioridades de los elementos a proteger respetando el valor que representa en la empresa para poder así prevenir una degradación de la seguridad del sistema de información, para ello se tiene que:

- Identificar vulnerabilidades en sistemas operativos.
- Identificar vulnerabilidades en aplicaciones.
- Identificar vulnerabilidades en configuraciones por defecto.
- Identificar las vulnerabilidades locales o remotas.

3.3.5 Fase de Explotación

Explotación es la fase en que un profesional de seguridad pone a prueba todas las destrezas y conocimientos para poder explotar todas las vulnerabilidades posibles encontradas en fases anteriores, permitiendo escalar privilegios, aprovechar debilidades a través de exploits, denegar servicios y mantener el acceso (Benchimol, 2011, pág. 149).

Un profesional en seguridad de la información debe tomar el control sobre el sistema para detectar las vulnerabilidades y así poder dar soluciones a las mismas, de ello dependerá mucho la arquitectura y la configuración del sistema de información encontrado (Benchimol, 2011, pág. 150).

Así también ésta fase es muy importante ya que a través de ella se permite extraer resultados del test de penetración para poder así detallarlos en un informe final que se lo presentará con total confidencialidad a la organización recurrente.

3.4 ANÁLISIS DE VULNERABILIDADES A TRAVÉS DE LA IMPLEMENTACIÓN DE HACKING ÉTICO

El análisis de vulnerabilidades de la infraestructura de la red de información en la empresa Construlec Cía. Ltda., se lo realizará a través de la implementación de hacking ético con la ayuda del software libre Kali Linux en su versión LiveCD,

siguiendo cinco principales fases mencionadas anteriormente en este documento y de las cuales se detallará su proceso.

3.4.1 Fase1 Reconocimiento

Como se lo puntualizo anteriormente, antes de planificar o analizar un posible ataque a un sistema o red de información, es conocer el objetivo, es decir conocer su huella identificativa o footprinting – el arte de extraer toda la información posible del objetivo.

3.4.1.1 Objetivos de la Fase de Reconocimiento

- Extraer información de la topología de la red de la empresa para obtener el esquema de cableado estructurado
- Descubrir la dirección ip del servidor de datos.
- Descubrir en que host se encuentra albergado el dominio y su respectiva ip.

Análisis del Cableado Estructurado de la empresa y su Topología

El cableado estructurado de la empresa Construlec Cía. Ltda., ha sufrido varios cambios, siendo éste el más importante a partir de febrero del presente año.

Se remodelo el diseño de interiores del departamento de proyectos como se lo puede apreciar en el anexo 1.

La remodelación del diseño de interiores recurrió en la actualización de su infraestructura de cableado estructurado y contempla los puntos de datos en cada una de las áreas que requieren este servicio como se muestra en el anexo 2.

El cableado de la red horizontal va desde el rack comunicaciones ubicado en el cuarto de data center hasta la toma de cada usuario, está construido en cable UTP categoría 5e con los respectivos face place y conectores, conducidos mediante canaleta instalada a lo largo de la planta siguiendo las normas de la construcción establecidas por TIA, ANSI, EIA, ISO, IEEE,

- ANSI/TIA/EIA-568-B: “Cableado de Telecomunicaciones en Edificios Comerciales sobre como instalar el Cableado” (Unitel, 2014).
- ANSI/TIA/EIA-569-A: “Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado” (Unitel, 2014).

Se debe indicar que el sistema consta un rack de pared tipo gabinete de 12 Unidades con todas sus partes pasivas, un switch de tipo Core perimetral de 24 puertos que sirve de núcleo de la topología en estrella de la red en conjunto con el servidor de datos tipo torre, también se enlaza al sistema un switch de 8 puertos de tipo perimetral ubicado en la bodega 2 que permite la conexión al sistema de los departamentos de Gerencia General, Técnica y Secretaria,

En los Anexos 2 y 3 se presentan los diseños del sistema de cableado estructurado, el diseño del rack de comunicaciones instalado y además las ubicaciones de cada uno de los puntos de datos.

Ejecución del comando Ping al sitio www.construlec.com.ec

En este punto se realizó un ping al nombre del dominio para poder conseguir información útil, analizar la dirección IP del host y las peticiones DNS que en este momento están respondiendo correctamente.

Figura 3.3.- Ping al dominio Construlec.com.ec

Fuente:(Investigador) (Kali Linux)

Adicionalmente el comando Traceroute permite conocer todos los sistemas existentes en un camino entre dos host, además permite conocer la ruta que toman los paquetes en la red de información y así poder obtener una lista de los elementos de red recorridos desde el computador de origen a un host de destino a través de internet, el comando Traceroute envía paquetes a la red de formas TTL=1, TTL=2, hasta llegar a su destino, envía de regreso la dirección IP de cada salto hacia el destino establecido.

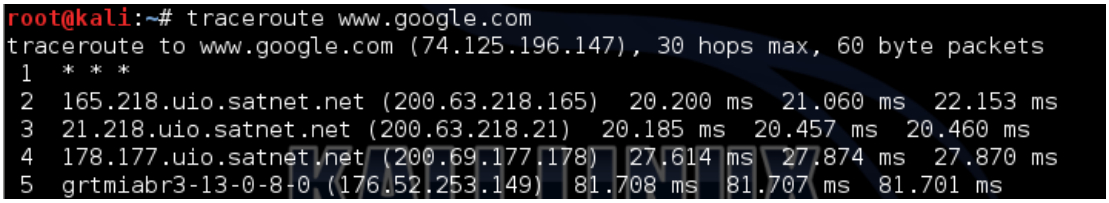


Figura 3.4.- Traceroute a www.google.com

Fuente:(Investigador) (Kali Linux)

A continuación se procede a identificar los Servidor DNS y a intentar encontrar la dirección IP del Servidor de datos de la empresa CONSTRULEC CÍA. LTDA.

Figura 3.5.- Identificación de los Servidores DNS

Fuente:(Investigador) (Kali Linux)

3.4.1.2 Resultado de la Fase 1

- La topología de la infraestructura de la red analizada es de forma estrella extendida lo que permite una buena administración de los host, en la inspección física realizada se observa que el sistema no cuenta con un respaldo de emergencia UPS en el cuarto de comunicaciones, tampoco cuenta con la correcta etiquetación del sistema de cableado estructurado incluyendo el rack de comunicaciones.
- Con la ejecución de los comandos ping y traceroute a las direcciones www.google.com y www.construlec.com.ec, no se pudo obtener la dirección IP del servidor, sin embargo con el comando cat /etc/resolv.conf si se pudo obtener la dirección IP del servidor que es 192.168.0.1, la cual va ayudar mucho a las fases posteriores.
- En esta fase se pudo establecer que el dominio se encuentra albergado en un hosting por lo que se asume que no existe un servidor DNS en la empresa CONSTRULEC CÍA. LTDA.

3.4.2 Fase 2 Exploración

El paso siguiente que se debe dar después de conocer el objetivo es el escaneo de las características de la red, permitiendo identificar los equipos disponibles, así también los servicios que ofrecen cada uno. Se procede al escaneo de red en forma activa para lo cual se empleó las herramientas otorgadas por Kali linux las cuales permiten escanear host activos con su respectiva ip, MAC Address, nombre de la pc y hasta el grupo al que pertenece dentro de la intranet, presentando sus resultados en modo gráfico.

3.4.2.1 Objetivos de la Fase de Exploración

- Descubrir host activos dentro de la subred local 192.168.0.255 mediante la utilización de la herramienta Angry IP Scanner y Nmap de Kali Linux.
- Ejecutar un escaneo de puertos para detectar puertos abiertos en el servidor proxy y datos, routers, incluyendo además los servicios que los mismos puedan prestar.
- Conocer el sistema operativo que existe en el servidor y en los Pc´s conectados en la red de la empresa.
- Buscar carpetas compartidas y archivos confidenciales.

Escaneo de Host Activos

Para cumplir con este objetivo se tomó la ayuda de Angry IP Scanner, el mismo que permite realizar un escaneo de las direcciones ip de toda la red estudiada, seleccionando la máscara se puede obtener los host activos a la infraestructura de red, sus hostnames, los puertos abiertos de un pc.

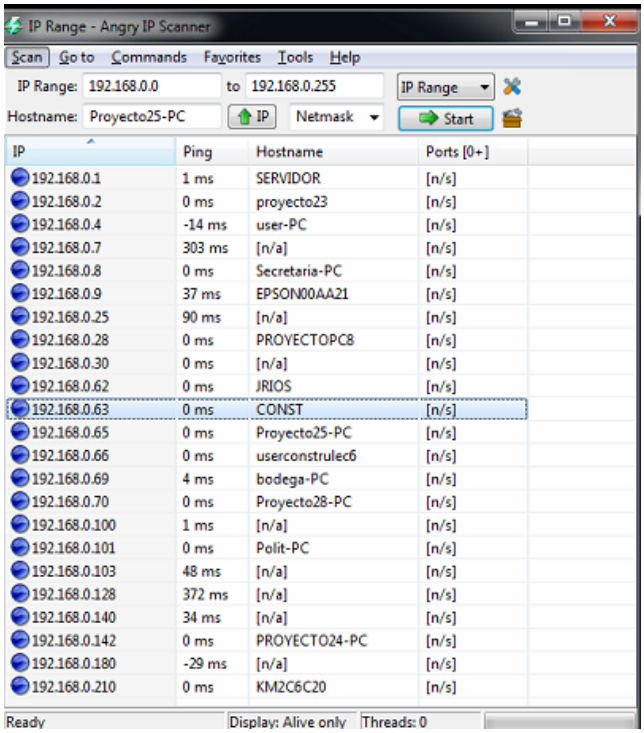


Figura 3.6.- Escaneo de host activos con Angry IP Scanner

Fuente:(Investigador) (Kali Linux)

Para una mejor visión de esta fase se puede utilizar nmap como el ejemplo mostrado en la figura 3.7.

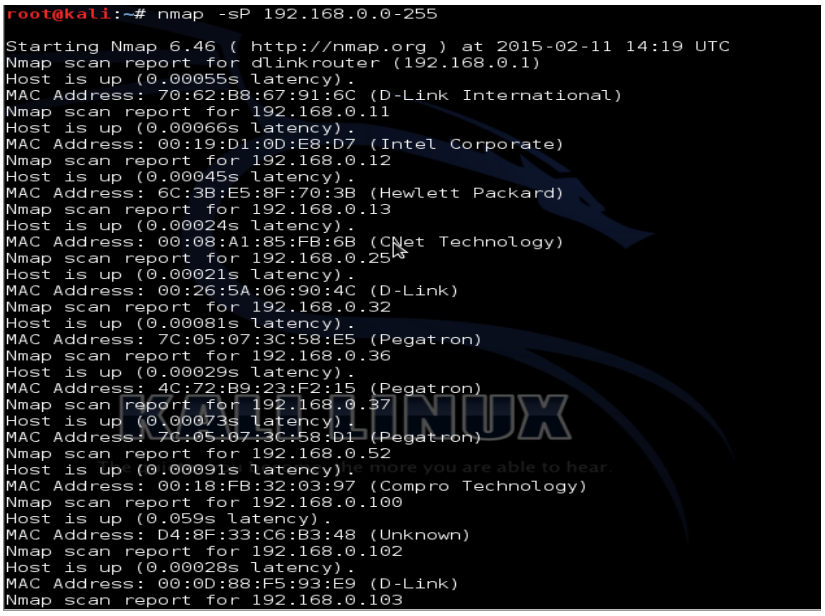


Figura 3.7.- Escaneo de host activos con nmap

Fuente:(Investigador) (Kali Linux)

Escaneo de Puertos

Luego de la obtención de dispositivos activos en la red y sus respectivas ip´s. Es necesario proseguir al escaneo de puertos tomando en cuenta la herramienta zenmap, la cual permite verificar el estado de los puertos del servidor, de esta manera poder encontrar vulnerabilidades a respuestas obtenidas en test anteriores, así también se puede obtener información muy valiosa de cada uno de los pc´s enlazados a la red de información estudiada.

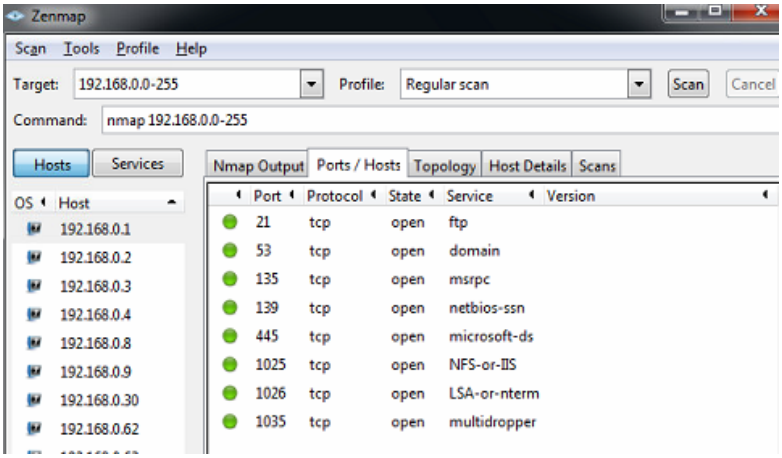


Figura 3.8.- Escaneo de Puertos con Zenmap

Fuente:(Investigador) (Kali Linux)

Identificación del Sistema

Con la herramienta zenmap también se puede extraer la información del sistema operativo del servidor y la dirección MAC de los PC´s conectados a la red de información.

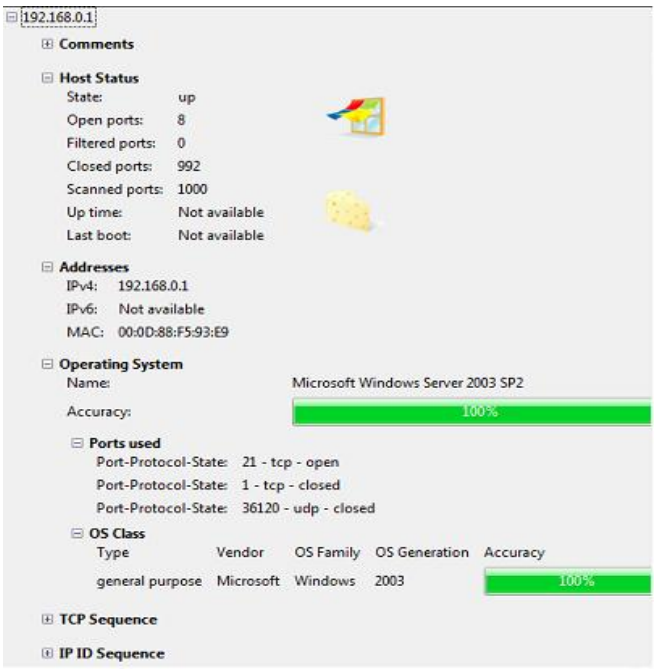


Figura 3.9.- Información del Sistema Operativo con Zenmap

Fuente:(Investigador) (Kali Linux)

Identificación de Vulnerabilidades

En este punto se toma la ayuda que zenmap ya que permite obtener detalladamente los host que son vulnerables desde su herramienta Host Viewer, marcando de color rojo los Host Vulnerables.

Se puede examinar uno por uno si necesario y muestra la cantidad de puertos abiertos como se muestra en la Figura 3.10, en él se puede observar que el servidor con dirección ip 192.168.0.1 es vulnerable.

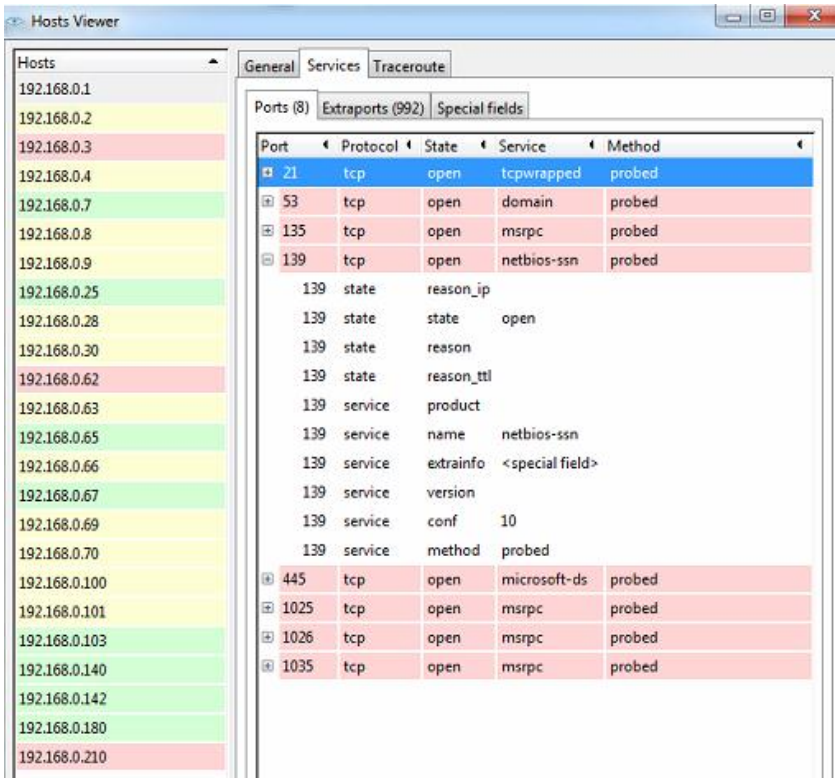


Figura 3.10.- Identificación de Vulnerabilidades con Zenmap

Fuente:(Investigador) (Kali Linux)

Identificación Carpetas compartidas por los usuarios

Luego de haber obtenido la información del sistema operativo de los diferentes host, se puede proceder a identificar carpetas compartidas de los dispositivos de la red y así también buscar la información de dichas carpetas para ello se utiliza la herramienta nbtscan y SoftPerfect Network Scanner, mediante las cuales también se puede conocer la ip, el nombre de la Pc y la Mac Address.

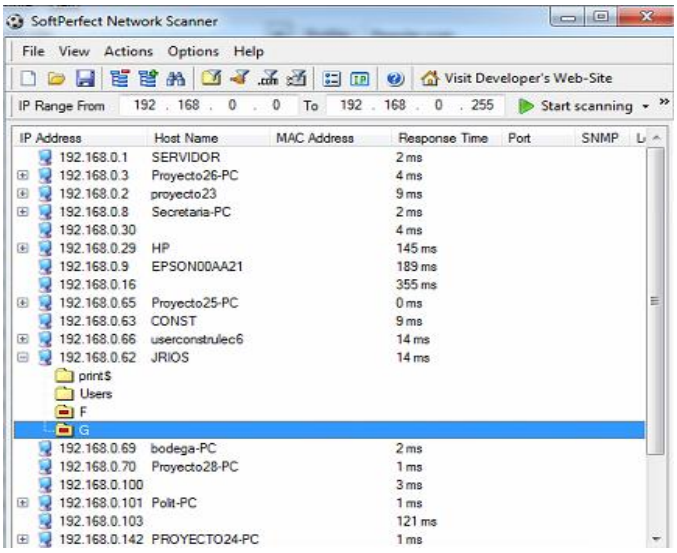


Figura 3.11.- Escaneo de Carpetas compartidas con SoftPerfect Network Scanner

Fuente:(Investigador) (Kali Linux)

Para el software SoftPerfect Network Scanner si se tiene el icono + junto a la ip, se puede decir que existe una carpeta compartida en la red, además con esta herramienta se puede establecer si existe algún disco duro compartido.

Se puede ingresar a los documentos compartidos con tan solo hacer doble click sobre ellos, como se lo puede observar en la Figura 3.12.

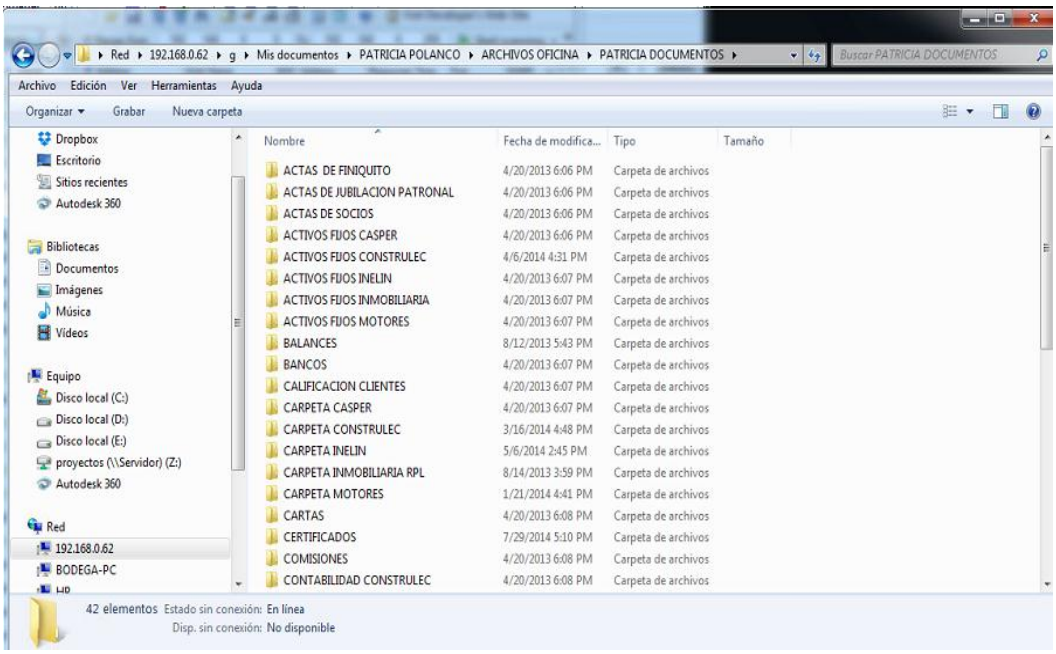


Figura 3.12.- Documentos Compartidos de un Estación de Trabajo

Fuente:(Investigador)

3.4.2.2 Resultados de la Fase 2

- Se pudo conocer los host activos y sus hostname a través de la utilización de la herramienta Angry IP Scanner y nmap de Kali Linux., se lo puede apreciar en el anexo 4.
- Se pudo conocer los puertos abiertos en el servidor, incluyendo además los servicios que los mismos puedan prestar, se lo puede constatar en el anexo 5.
- Se pudo conocer el sistema operativo que presenta el servidor y algunos de los Pc´s conectados en la red de la empresa, se lo puede apreciar en el anexo 6.
- Se pudo ingresar a carpetas compartidas y archivos confidenciales del departamento de contabilidad como ejemplo se muestra el archivo encontrado en el anexo 7, siendo esta una alta vulnerabilidad de intrusión ya que el intruso puede extraer cualquier documento de confidencialidad alta para la empresa.

3.4.3 Fase 3 Enumeración

Partiendo de un buen proceso de reconocimiento y exploración se puede obtener una buena etapa de enumeración ya que significa poder obtener nombres y cuentas de usuario, grupos de trabajo, recursos compartidos, recursos de NetBios, nombres de máquinas y los diferentes servicios de la intranet del objetivo.

3.4.3.1 Objetivo de la Fase de Enumeración

- Realizar una tabla informativa que contenga la dirección ip, nombre de los equipos NetBIOS y la dirección MAC de las maquinas correspondientes a los usuarios.

Entrando por NetBIOS

Utilizando la herramienta nbtscan de Kali Linux se puede obtener la tabla informativa que se requiere para cumplir con el objetivo y que permite realizarlo con la única digitalización de un comando operando en un rango de direcciones ip establecidas.

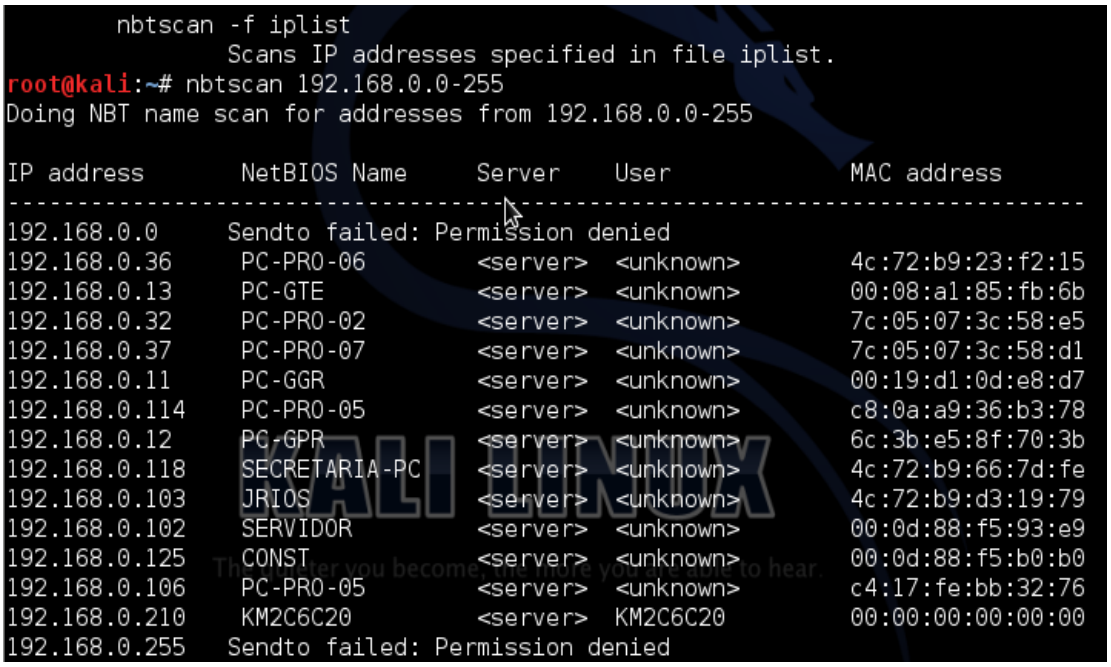


Figura 3.13.- Proceso de nbtscan

Fuente:(Investigador) (Kali Linux)

La tabla informativa de NetBIOS se la puede apreciar a detalle en el Anexo 8

3.4.3.2 Resultado de la Fase 3

- Mediante esta fase se pudo obtener las direcciones MAC ingresando por el puerto 139 (NetBIOS) década host de la red de información, además se pudo conocer a que grupo pertenecen.

3.4.4 Fase 4 búsqueda de vulnerabilidades

En esta fase se analiza las vulnerabilidades a nivel de puerto, con la ayuda de Nessus 5.0 en su versión Home el cual fue instalada en Kali Linux, se determinaran vulnerabilidades del servidor de datos e internet.

3.4.4.1 Objetivo de la búsqueda de vulnerabilidades

- Escanear el servidor para obtener vulnerabilidades dependiendo de los puertos abiertos y niveles de severidad de cada una.

Escaneo de Vulnerabilidades al Servidor

Para el escaneo de vulnerabilidades se utiliza la herramienta Nessus que opera en diversos sistemas operativos. Nessus comienza escaneando puertos abiertos con su propio escáner, luego prueba varios exploits para un posible ataque y mostrarlo en una interfaz gráfica (NESSUS, 2014).

Se puede escanear el servidor un vez que se añada políticas de seguridad, para su uso se toma políticas por default de nessus, después se procede añadir un escaneo desde la pestaña Scans, seguidamente se digita el nombre del escaneo, en Police escogeremos la política que añadimos y en Scan Target se digita la ip del servidor de la empresa en este caso 192.168.0.1.

En Nessus se muestra los resultados de los reportes en formatos como texto plano, XML, HTML, y LaTeX, además se puede guardar los diferentes escaneos en una base de datos para referencia de futuros escaneos de vulnerabilidades (NESSUS, 2014).

Plugin ID	Count	Severity	Name	Family
45004	2	Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
57603	2	Critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers
33822	2	High	XAMPP Example Pages Detection	CGI abuses
41014	2	High	PHP < 5.2.11 Multiple Vulnerabilities	CGI abuses
42052	2	High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
48244	2	High	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses
57537	2	High	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses
10862	1	High	Microsoft SQL Server Default Credentials	Databases
11213	2	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
39480	2	Medium	PHP < 5.2.10 Multiple Vulnerabilities	CGI abuses
40467	2	Medium	Apache 2.x < 2.2.12 Multiple Vulnerabilities	Web Servers
43351	2	Medium	PHP < 5.2.12 Multiple Vulnerabilities	CGI abuses
44921	2	Medium	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CGI abuses
48205	2	Medium	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Web Servers
50070	2	Medium	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers
51139	2	Medium	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	CGI abuses
51439	2	Medium	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CGI abuses
53896	2	Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Web Servers

Figura 3.14.- Análisis de vulnerabilidad en el servidor de datos con Nessus

Fuente:(Investigador) (Kali Linux)

3.4.4.2 Resultado de la Fase 4

- Mediante la ayuda de Nessus y de Znmap de Kali Linux, se puede apreciar que el servidor es altamente vulnerable, ya que se puede ingresar a él sin mayor esfuerzo.

3.4.5 Fase 5 penetración del sistema

Después de haber pasado por las cuatro fases anteriores de donde se pudo extraer valiosa información como la visualización de host activos, puertos abiertos, ip´s, direcciones MAC, Hostname y grupo de trabajo de cada hosts, se procede a explotar las vulnerabilidades

3.4.5.1 Objetivo de la penetración al sistema

- Realizar ataques de hombre en el medio para lograr conseguir conversaciones, contraseñas de ingresos a sistemas o correos electrónicos.

Ejecución del Ataque Hombre en el Medio

Luego de haber cumplido con los procedimientos de las anteriores fases a continuación se procede a realizar un ataque de tipo “hombre en el Medio” con ARP-Spoof encargado de encontrar la dirección hardware o la Ethernet MAC correspondiente a un IP determinada, traduciendo así las direcciones IP a direcciones MAC, el funcionamiento de la solicitud ARP se lo puede observar en la Figura 3.15 y la tabla de solicitud ARP se lo puede apreciar en la Figura 3.16.

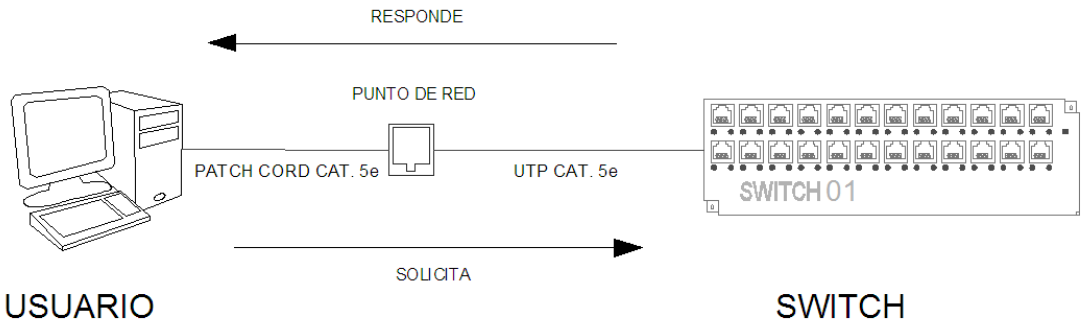


Figura 3.15.- Forma de solicitud ARP

Fuente:(Investigador) (AutoCAD 2014)

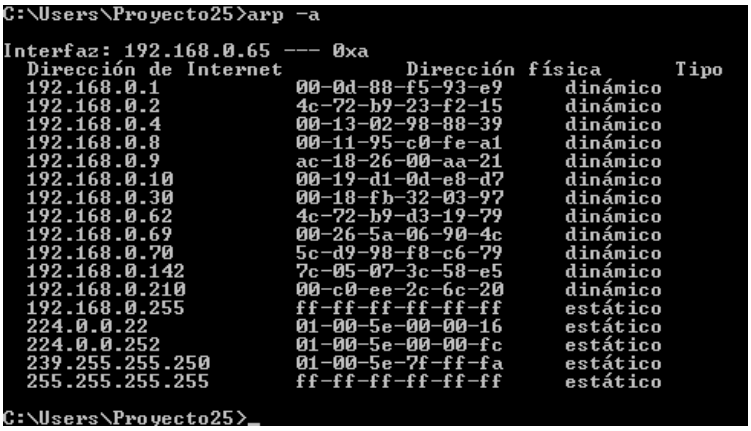


Figura 3.16.- Solicitud de la Tabla ARP desde el Host del Atacante

Fuente:(Investigador) (Windows cmd)

Los ataques de tipo “hombre en el Medio” permiten al atacante hacerse pasar como usuario o como Gateway al mismo tiempo en una infraestructura de red, para este objetivo se utiliza la herramienta ARP-Spoofing, la cual consiste en enviar mensajes ARP falsos en la red de información con el propósito de asociar la dirección MAC del atacante con la dirección IP del atacado y de este modo establecer la infiltración en medio de las comunicaciones entre host víctima y la puerta de enlace.

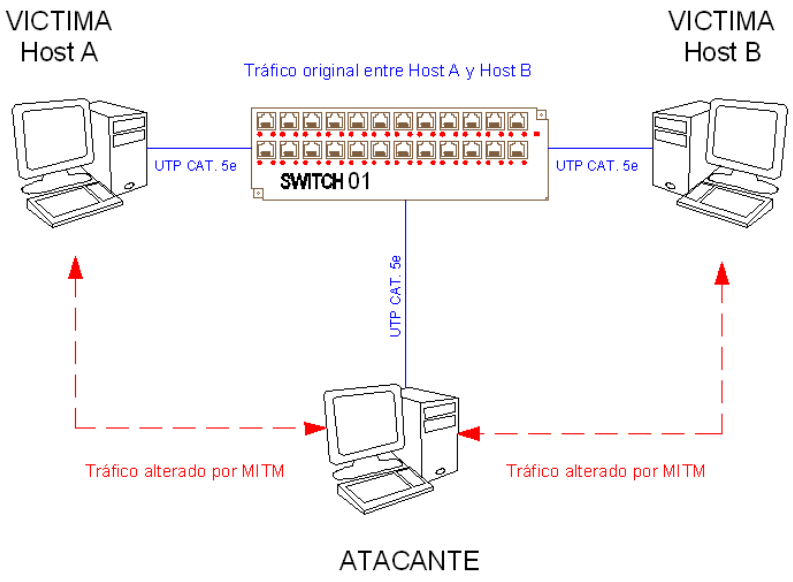


Figura 3.17.- Diagrama de ataque MITM (Hombre en el medio)

Fuente:(Investigador) (AutoCAD 2014)

Intrusión en el Objetivo

Ettercap es una herramienta que permite realizar ARP-Spoofing la cual es muy usada gracias a su modo grafico en Kali Linux a través del comando **root@bt:-# ettercap –G.**

Una vez ingresado a la versión gráfica Ettercap se procede a seguir los siguientes pasos:

- **Paso 1:** Acudir a *Sniff>Unified Sniffing* una herramienta que permite analizar el objetivo deseado para luego buscar los host dentro de la LAN utilizando *Hosts>Scan for hosts* que es una de las aplicaciones de Ettercap, para luego poder visualizarlos mediante *Hosts>Host list* que a su vez permite identificar los objetivos en targets o destinatarios Ideales.
- **Paso 2:** Seguidamente se establece como TARGET1 la dirección del Gateway 192.168.0.1 correspondiente al servidor de datos y en TARGET2 192.168.0.32 la dirección de una PC de un usuario dentro de la LAN.
- **Paso 3:** Posteriormente se puede empezar con un ataque gracias a la herramienta conocida como *Mitm>ARP poisoning* provista por Ettercap, permitiendo escoger el parámetro Sniff remote connections, el mismo que ayudara a envenenar las conexiones elegidas.

En la figura 3.18 se puede constatar que el ataque se lo realizó con gran éxito ya que existen direcciones MAC duplicadas en direcciones IP diferentes.

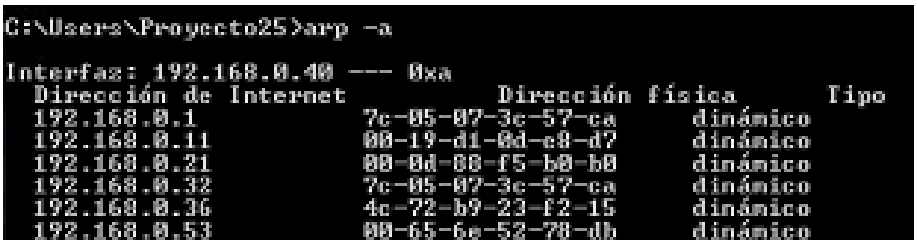


Figura 3.18.- Dirección MAC duplicadas

Fuente:(Investigador) (Windows cmd)

El detalle de este ataque se lo puede apreciar en el anexo 9 presentado en este documento.

Este sin duda es un ejemplo de los muchos ataques que se pueden realizar, se puede también obtener conversaciones de los usuarios de una misma red LAN, para el cual se siguen los siguientes pasos desde la aplicación Ettercap de Kali Linux.

- **Paso 1:** Se deben repetir los paso 1, 2 y 3 de la forma de ataque vista anteriormente teniendo en cuenta que se debe establecer como TARGET1 la dirección del Gateway 192.168.0.1 correspondiente a la puerta de enlace y en TARGET2 el objetivo de intrusión 192.168.0.39 la dirección de una PC usuario dentro de la LAN.
- **Paso 2:** Seguidamente se elige *Start Sniffing* desde el menú *Start* para finalmente poder utilizar *View>Connections* la cual permitirá obtener datos que pueden contener mensajería instantánea y además se podrá obtener contraseñas de correos escritos por otros usuarios, en esta etapa se pondrá a prueba la paciencia del atacante.

El detalle y el resultado de este ataque se lo aprecia en el anexo 10 presentado en este documento.

3.4.5.2 Resultado de la fase 5

Los ataques de hombre en el medio fueron exitosos, los mismos que permitieron conseguir conversaciones, contraseñas de ingresos a sistemas o correos electrónicos, permitiendo así concluir que no se están acatando ciertas sugerencias por parte del administrador de red ya que en la red de la empresa no se debe tener acceso a páginas de redes sociales, sin embargo no se mostraran a detalle el procedimiento de ataque ni el resultado obtenido de cada usuario porque es deber de un profesional de seguridad de la información velar y proteger la privacidad de los usuarios.

3.5 REPORTE DE LAS PRUEBAS DE PENETRACIÓN EN LA RED

3.5.1 Informe General

El presente trabajo investigativo se origina por la necesidad de mostrar las diferentes vulnerabilidades que posee la red de información de la Empresa CONSTRULEC. CIA. LTDA., para este caso de estudio se adoptó realizarlo desde el interior de la intranet.

3.5.1.1 Resumen Ejecutivo

a. Antecedentes

La gran mayoría de fraudes cometidos a entidades públicas o privadas son desarrollados desde el interior de la misma, por lo que conlleva a que las intranets sean vulnerables a los ataques informáticos.

Para poder establecer las fallas de seguridades en la red de la empresa Construlec Cía. Ltda. Se toma la metodología de un Hacker ético para poder desarrollar las diferentes pruebas de penetración o pentest, la cual consiste en realizar un análisis de vulnerabilidades a través de la realización de ataques controlados a los equipos y dispositivos de la red, determinando así las diferentes deficiencias de seguridad de la misma, las cuales permitan emitir correcciones pertinentes que ayuden a disminuir las probabilidades de sufrir algún ataque informático.

b. Objetivo del Pentest

El objetivo principal al realizar ésta prueba de penetración es ayudar con el fortalecimiento de seguridad en la red de área local de la compañía, usando a su vez las herramientas que posee Kali Linux, permitiendo así demostrar las diferentes vulnerabilidades que posee la red de la empresa Construlec Cía. Ltda.

3.5.1.2 Informe Técnico

Para el presente proyecto de investigación es necesario realizar un informe de evaluación técnica, el mismo que debe ser comprendido por los técnicos, manejando a su vez las diferentes características de seguridad adoptadas en el sistema, teniéndolas también en cuenta a la hora de diseñar e implementar la red.

a. Objetivo de la prueba

Realizar un análisis intensivo de las vulnerabilidades en la red de información de la empresa Construlec Cía. Ltda., utilizando el método de hacking ético.

b. Alcance de la prueba

Revelar las diferentes vulnerabilidades e identificar su nivel de peligrosidad al ser explotadas en la red de la empresa CONSTRULEC CIA. LTDA.

c. Fuerza de la prueba

Explotar las diferentes vulnerabilidades críticas en la red de información de la empresa CONSTRULEC CIA. LTDA., en un entorno controlado.

d. Enfoque

Demostrar la importancia de un análisis de pentest a la empresa Construlec Cía. Ltda.

e. Recopilación de Información

La recopilación y evaluación de la información es la base de una correcta prueba de penetración en la red de información.

f. Inteligencia pasiva.

Para recolectar la información se utilizó herramientas de footprinting con la ayuda de Kali Linux en especial con su herramienta Angry IP Scanner, las misma que permitió recoger información muy valiosa siendo ésta mostrada en las figuras anteriores de footprinting en este documento y se la pudo detallar en términos de:

- Arquitectura del sistema
- Nombres de usuarios
- Direcciones IP específicas
- Nombres de Dominios
- Estado de host
- Servicios de red

g. Inteligencia activa.

Muestra los métodos y los diferentes resultados obtenidos de tareas como el escaneo de puertos, mapeo de infraestructura y la evaluación de la arquitectura.
Gracias a herramientas como Zenmap, Nmap y ntbscan de Kali Linux se pudo obtener la siguiente información:

Sistema Operativo en servicio.
Dirección MAC.
Puertos Abiertos, protocolo que utiliza, estado y el servicio que ejecuta.
Direcciones IP y servicios activos (netbios,etc).
Topología de la Red.

3.5.1.3 Evaluación de Vulnerabilidades.

Significa identificar, evaluar y clasificar las posibles amenazas que dan como resultado de una prueba de penetración en la red de la empresa Construlec Cía. Ltda.

a. Niveles de Vulnerabilidad

- ***De severidad baja*:** Está dada así a un tipo de acción no perjudicial en el sistema, siendo identificada por Nessus de color Verde.
- ***De severidad media*:** Está relacionado con un nivel medio de gravedad en la que se podría tomar precauciones, en Nessus se la identifica con el color amarillo.
- ***De alta severidad*:** A éste nivel de vulnerabilidad que por lo general Nessus lo identifica de color tomate se lo debe poner cierto grado de precaución.
- ***De severidad crítica*:** Mostrado así como un nivel crítico de vulnerabilidad al que se debe poner mucha atención al que por lo general Nessus lo identifica de color rojo.

b. Mapa de Vulnerabilidades

Se realizó el análisis de vulnerabilidades anteriormente al servidor de la empresa como se lo puede constatar en la fase 4 de este documento, sin embargo es necesario establecer el análisis a toda la infraestructura de red de la empresa con ayuda de la aplicación Nessus, para ello se utilizó su versión Home y se ejecutó esta prueba al menos cinco veces, permitiendo tener una mejor visión de la misma y en todos los casos se reveló el mismo nivel de riesgo a sus respectivas IP como se lo puede apreciar en la Figura 3.19.

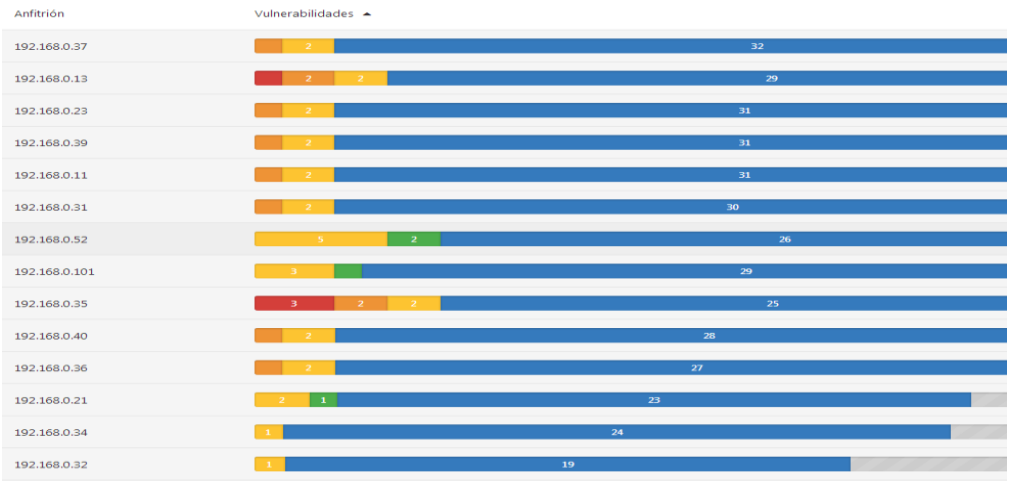
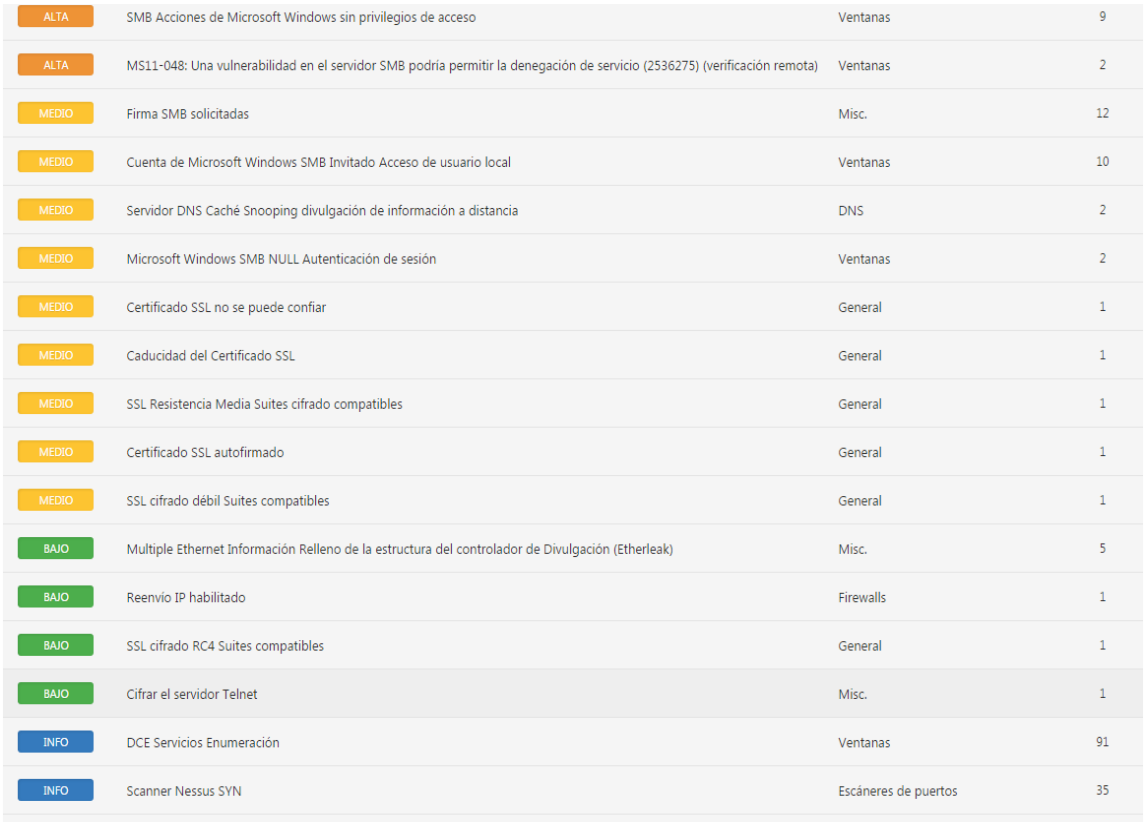


Figura 3.19.- Reporte HTML del Análisis de vulnerabilidades con Nessus

Fuente:(Investigador) (Kali Linux)

Para una mejor visión, la aplicación Nessus muestra las características de vulnerabilidades y su nivel de riesgo por cada host como se lo observa en la Figura 3.20.



ALTA	SMB Acciones de Microsoft Windows sin privilegios de acceso	Ventanas	9
ALTA	MS11-048: Una vulnerabilidad en el servidor SMB podría permitir la denegación de servicio (2536275) (verificación remota)	Ventanas	2
MEDIO	Firma SMB solicitadas	Misc.	12
MEDIO	Cuenta de Microsoft Windows SMB Invitado Acceso de usuario local	Ventanas	10
MEDIO	Servidor DNS Caché Snooping divulgación de información a distancia	DNS	2
MEDIO	Microsoft Windows SMB NULL Autenticación de sesión	Ventanas	2
MEDIO	Certificado SSL no se puede confiar	General	1
MEDIO	Caducidad del Certificado SSL	General	1
MEDIO	SSL Resistencia Media Suites cifrado compatibles	General	1
MEDIO	Certificado SSL autofirmado	General	1
MEDIO	SSL cifrado débil Suites compatibles	General	1
BAJO	Multiple Ethernet Información Relleno de la estructura del controlador de Divulgación (Etherleak)	Misc.	5
BAJO	Reenvío IP habilitado	Firewalls	1
BAJO	SSL cifrado RC4 Suites compatibles	General	1
BAJO	Cifrar el servidor Telnet	Misc.	1
INFO	DCE Servicios Enumeración	Ventanas	91
INFO	Scanner Nessus SYN	Escáneres de puertos	35

Figura 3.20.- Descripción de vulnerabilidades del reporte HTML con Nessus

Fuente:(Investigador) (Kali Linux)

3.5.1.4 Presentación de Resultados

Se obtuvo el permiso correspondiente a la empresa para poder realizar los diferentes ataques a la infraestructura de red, de los cuales se pudo obtener un resumen de ataques realizados con éxito, mostrados en la tabla 3.2.

ATAQUES	HERRAMIENTAS	NUMERO DE VECES
Escaneo de Host Activos	Angry IP Scanner	10
Escaneo de Puertos	Zenmap	15
Identificación del Sistema Operativo	Zenmap	7
Scaneo y recolección de archivos Compartidos	SoftPerfect Network Scanner	5
Sniffing	Wireshark, Ettercap	15
ARP Spoofing	Ettercap	17
Hombre en el medio	ARP Apoof	23
Denegación de Servicio	Ettercap	6

Tabla 3.2.- Resumen de ataques realizados con éxito

Fuente:(Investigador)

La tabla 3.2 es una cuantificación de ciertos ataques realizados, pero no se muestra a detalle cada uno de ellos ya que el fin de este trabajo de investigación es mostrar las vulnerabilidades halladas, mas no es una guía de intrusión en la red por lo que el resto de ataques no se muestran en este documento.

En el Anexo 11 del presente documento muestra la tabla informativa de las vulnerabilidades y el grado de severidad encontrada en la infraestructura de la red de información de la empresa Construlec Cía. Ltda.

El resumen de la tabla informativa de las vulnerabilidades y el grado de severidad encontrada en la infraestructura de la red de información de la empresa Construlec Cía. Ltda., se lo puede apreciar en la figura 3.21.

Figura 3.21.- Resumen de vulnerabilidades encontradas en la red de la empresa Construlec Cía. Ltda., con Nessus

Fuente:(Investigador) (Kali Linux)

El cuadro informativo del proceso de las pruebas de penetración se lo puede observar en el anexo 12 del presente documento, el cual a su vez permitió generar un cuadro de recomendación para la asignación de direcciones IP, grupos y hostnames para la empresa y se lo puede apreciar en el anexo 13.

3.6 PLAN DE SEGURIDAD

Luego de cumplir con las etapas de una prueba de penetración siguiendo los procesos de hacking ético descritos en los anteriores enunciados, es necesario preservar el activo de información estableciendo acciones que doten de excelentes resultados al sistema de seguridad de la información en la infraestructura de red de la empresa Construlec Cía. Ltda., siendo ésta razón necesaria para aplicar un plan de seguridad de la información ya que en la actualidad no se ha prestado la atención debida al tema, para lo cual se siguen algunas recomendaciones dadas por la norma ISO/IEC 27002 e ISO/27001 del año 2013,

Datos del caso de Estudio	
Empresa	Construlec Cía. Ltda.
Dirección	Av. 6 de Diciembre y Av. Gaspar de Villarroel 1179, Edif. Paris.
Facilitador	Ing. Jaime Franco Miranda

Tabla 3.3.- Datos del caso de estudio

Fuente:(Investigador)

3.6.1 Aplicación del Plan de Seguridad

Previo a la aplicación del plan de seguridad es necesario realizar un análisis del sistema de gestión de la red de la empresa, teniendo como puntos un análisis de la infraestructura y un análisis de la situación previa de la seguridad de información.

3.6.2 Análisis de la Infraestructura

La empresa Construlec Cía. Ltda., presenta una estructura jerárquica, la misma que no cuenta con el departamento de Sistemas y se la puede apreciar en el anexo 14. Se recomienda crear el departamento de sistemas respaldado con la dirección de seguridad informática como se lo observa en el anexo 15.

La red de datos de la empresa Construlec Cía. Ltda., en su sistema de cableado estructurado presenta un diseño jerárquico en cada uno de sus departamentos como se muestra en el anexo 3.

La ubicación de los puntos de datos, se encuentran distribuidos según los puestos de trabajo y se lo puede observar en el anexo 2.

La distribución del diseño del rack de comunicaciones se lo puede apreciar en el anexo 3.

Previo a la inspección física realizada, se puede determinar que es necesario realizar un correcto etiquetado del sistema de cableado estructurado de la empresa Construlec Cía. Ltda., ya que en el presente momento no se encuentra bien etiquetado, por ello se sugiere seguir la norma ANSI/TIA-606-A, la cual contempla la administración del sistema de cableado estructurado. El documento guía para el etiquetado del sistema de cableado estructurado de la empresa Construlec Cía. Ltda., se lo puede observar en el Anexo 32.

3.6.3 Análisis de la situación previa de la seguridad de la información

En la actualidad la empresa Construlec Cía. Ltda., no cuenta con el departamento de sistemas en su organigrama jerárquico ni tampoco cuenta con lineamientos de seguridad de la información, sin embargo cuenta con una persona encargada como administrador de red, razón por la cual se requiere que la información y la seguridad sean tratadas de una forma organizada.

Para realizar este análisis se evaluaron los siguientes aspectos:

- Evaluación de la seguridad lógica
- Evaluación de la seguridad de las comunicaciones
- Evaluación de seguridad en las aplicaciones
- Evaluación de seguridad física
- Administración del cuarto de equipos

La tabla 3.4., muestra a detalle los aspectos evaluados, cuyos valores obtenidos se basan en la escala de Likert, donde 1 representa un significado de muy bajo, 2 bajo, 3 medio, 4 alto y 5 muy alto.

Aspectos Evaluados		Nivel de Seguridad
Evaluación de Seguridad Lógica	Contraseñas	3
	Inactividad	2
	Asignación de Funciones	1
Evaluación de Seguridad de las Comunicaciones	Topología de Red	3
	Conexiones Externas	3
	Configuración lógica de Red	1
	Mail	2
	Antivirus	2
	Firewall	1
Evaluación de Seguridad en las Aplicaciones	Control de Aplicaciones en pc´s	2
Evaluación de Seguridad Física	Equipamiento	2
	Control de Accesos a equipos	2
	Dispositivos de Soporte	3
	Cableado Estructurado	2
Administración del cuarto de Equipos	Administración del cuarto de equipos	1
	Capacitación	1
	Backup	2
	Documentación	1

Tabla 3.4.- Situación Previa de la Seguridad de la Información

Fuente:(Investigador) (Chamorro, V., 2013, pág. 78)

3.6.4 Establecimiento del plan de seguridad de la información

Con el análisis de la situación previa de la seguridad de la información descrita en el capitulo anterior, se pudo determinar que políticas son necesarias establecer.

3.6.4.1 Alcance del plan de seguridad de la información

El alcance del presente plan de seguridad de la información abarca al departamento de sistemas de la empresa Construlec Cía. Ltda.

3.6.4.2 Políticas del plan de seguridad

Partiendo del análisis realizado en el test de penetración presentado en el presente documento, en el segundo capítulo, se realiza la recomendación de la implementación de un conjunto de políticas de seguridad, las mismas que ayudarán a disminuir las posibilidades de riesgo e intrusión informática y en caso de presentarse, ayudarán a disminuir el impacto en la organización, se toma además la ayuda de la norma ISO/IEC 27002 para poder generarlas.

La norma, recomienda que las políticas de seguridad se puedan emitir en un solo documento, política de seguridad de la información (ISO/IEC27002, 2013).

Las políticas de la seguridad de la información presentadas en el Anexo 22 han sido divididas en cuatro grupos los cuales son: seguridad organizacional, seguridad a nivel Lógico, seguridad a nivel físico y seguridad a nivel legal. La norma recomienda partir del objetivo de "proporcionar la dirección de gestión y apoyo a la seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes" (ISO/IEC27002, 2013, pág. 2).

Para garantizar un perfecto control de las políticas adjuntas se sigue los lineamientos que por norma establece. Según la norma, el control de las políticas de seguridad a implementarse deben de "ser definidas, aprobado por la administración, publicado y comunicado a los empleados y colaboradores externos" (ISO/IEC27002, 2013, pág. 2).

3.6.4.3 Aspectos para efectuar el análisis de riesgos

Para el desarrollo del análisis y evaluación del riesgo se requieren de los siguientes aspectos.

- Identificación de Activos
- Identificación de requerimientos legales y comerciales
- Tasación de activos
- Identificación de amenazas, vulnerabilidades y probabilidad de ocurrencia
- Análisis del riesgo y su evaluación
- Aspectos a contemplar al efectuar la evaluación del riesgo

3.6.4.3.1 Identificación de activos

En el departamento de sistemas de la empresa se identifican los activos y se los muestra en la tabla 3.5.

Ítem	Activos de Información	Propietarios
1	Adquisiciones	Administración
2	Asistente	Administración
3	Base de Datos	Administración
4	Central Telefónica	Administración

5	Contador	Administración
6	Correo	Administración
7	Gerencia	Administración
8	Información de clientes y proveedores	Administración
9	Backup	Desarrollo
10	Help Desk	Desarrollo
11	Manuales	Desarrollo
12	Reposito de Software	Desarrollo
13	Administrador de Red	Sistemas
14	Conexión a Internet	Sistemas
15	Equipo de Trabajo	Sistemas
16	Técnico	Sistemas

Tabla 3.5.- Identificación de Activos

Fuente:(Investigador) (Chamorro, V., 2013, pág. 81)

3.6.4.3.2 Identificación de Requerimientos legales y Comerciales

Los equipos que se encuentran el departamento de sistemas, todos son propiedad única de la empresa Construlec Cía. Ltda., por tanto no deben cumplir ningún cumplimiento legal.

En la empresa Construlec Cía. Ltda., no existen equipos a la venta por lo que no se tiene el requerimiento comercial de la misma.

3.6.4.3.3 Tasación de Activos

La tasación de activos se la puede medir mediante la escala de Likert, donde 1 representa un significado de muy bajo, 2 bajo, 3 medio, 4 alto y 5 muy alto.

Para realizar la tasación de activos es necesario hacerse la pregunta ¿Cómo una pérdida o falla de un activo afecta la confidencialidad, la integridad y la disponibilidad? (Chamorro, V., 2013, pág. 82).

En el anexo 16 se puede observar la tabla correspondiente a la Tasación de Activos.

Para el proceso del plan solo se toman en cuenta los activos de información que conllevan al área de Sistemas de la empresa, estos son Administrador de Red, Conexión a Internet, Equipo de Trabajo y Técnico.

3.6.4.3.4 Identificación de Vulnerabilidades

En esta parte del proceso es necesario identificar las amenazas, vulnerabilidades y la probabilidad de Vulnerabilidad al activo de Información.

Para el proceso, se toman en cuenta los activos de información que conllevan al área de Sistemas de la empresa, estos son Administrador de Red, Conexión a Internet, Equipo de Trabajo y Técnico. En el anexo 17 se observan las vulnerabilidades y la posibilidad de amenaza encontradas en el área de sistemas de la empresa Construlec Cía. Ltda.

3.6.4.3.5 Evaluación del riesgo

Es necesario realizar la evaluación del riesgo determinando las amenazas cuyos riesgos son los más relevantes y para ello se utiliza la escala de Likert y criterios como el impacto económico del riesgo, el tiempo de recuperación de la empresa, la probabilidad real de ocurrencia del riesgo y la probabilidad de interrumpir las actividades de la empresa (Chamorro, V., 2013, pág. 88).
La evaluación del riesgo se lo puede observar en el anexo 18.

3.6.4.3.6 Tratamiento del riesgo y el proceso de toma de decisión gerencial

Para poder realizar un correcto tratamiento del riesgo es necesario manejar un correcto criterio para su tratamiento, para ello se parte de la tabla 3.6., de esta manera se puede analizar los controles y cuales son aplicables.

Criterio	Tratamiento del Riesgo
De 4 a 7	Aceptar
De 8 a 12	Reducir
De 13 en Adelante	Transferir
No existen niveles para evitar el riesgo	Evitar

Tabla 3.6.- Tratamiento del Riesgo

Fuente: (Investigador) (Chamorro, V., 2013, pág. 91)

Según el autor, “Cuando se ha calculado el riesgo, se debe iniciar un proceso de toma de decisiones para determinar que va a ocurrir con el riesgo” (Chamorro, V., 2013, pág. 91).

Es necesario partir de dos factores; El posible impacto si el riesgo se pone de manifiesto y Que tan frecuente puede vulnerar" (Chamorro, V., 2013, pág. 91).

En el Anexo 19 se puede observar la tabla relacionada a la toma de decisiones de acuerdo al tratamiento del riesgo y se manejaran criterios que para el tratamiento del riesgo aceptado debe ser aprobado por la gerencia, para el tratamiento del riesgo reducido es necesario establecer en conjunto con la gerencia y el encargado del departamento de Sistemas la metodología a implementarse a su tratamiento, para el riesgo transferido se recomienda contratar un seguro que proteja a los activos y finalmente todos los activos son indispensables y es por ello que no existen activos con la estrategia Evitar (Chamorro, V., 2013, pág. 92).

3.6.4.3.7 Riesgo Residual

No se pude eliminar todas las vulnerabilidades, es así que se deja un riesgo remanente (Chamorro, V., 2013, pág. 93).
Según la norma, "El riesgo remanente existe después de que se hayan tomado las medidas de seguridad" (ISO/IEC27001, 2013, pág. 15).
Se determinan además los controles que pueden ser implementados en la empresa, para poder determinar objetivos de control y controles a implementarse (Chamorro, V., 2013, pág. 93).

Es necesario establecer una declaración de aplicabilidad para asegurar a la empresa que no ha omitido algún error, igualmente se debe incluir los objetivos de control y controles que serán excluidos (Chamorro, V., 2013, pág. 93)
En el Anexo 20 se puede observar la tabla referente a la declaración de aplicabilidad.

3.7 PROPUESTA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

Según la norma, la propuesta del plan de seguridad de la información debe ser apoyada por las políticas sobre temas específicos, los cuales exigen aún más la aplicación de los controles de seguridad de la información y por lo general están estructurados para atender las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas (ISO/IEC27002, 2013, pág. 3).
Partiendo de la recomendación que da la norma ISO/IEC 27002 las políticas presentadas en este documento incluyen temas de:

a) El control de acceso (véase en el Anexo 22, numeral 3.2.1.)

b) La clasificación de la información (véase en el Anexo 22, numeral 3.1.3.)

c) La seguridad física y ambiental (véase en el Anexo 22, numeral 3.3.1.)

d) De usuario final temas orientados tales como:

1) el uso aceptable de los activos (véase en el Anexo 22, numeral 3.2.)

2) escritorio limpio y claro de la pantalla (véase en el Anexo 22, numeral 3.2.)

3) la transferencia de información (véase en el Anexo 22, numeral 3.2.6.)

4) Las restricciones a las instalaciones de software y su uso (véase en el Anexo 22, el numeral 3.2.4.)

e) Copia de seguridad (véase en el Anexo 22, numeral 3.2.6.)

f) La transferencia de información (véase en el Anexo 22, numeral 3.2.6.)

g) La protección contra el malware (véase en el Anexo 22, numeral 3.2.5.)

h) La gestión de vulnerabilidades técnicas (véase en el Anexo 22, numeral 3.1.4.)

i) Controles criptográficos (véase en el Anexo 22, numeral 3.2.1.)

j) Las comunicaciones de seguridad (véase en el Anexo 22, numeral 3.2.3.)

k) La intimidad y la protección de la información personal identificable (véase en el Anexo 22, numeral 3.1.5.)

La implementación del plan de seguridad de la información genera los siguientes documentos:

- Documento No. 1: Acuerdo de confidencialidad (véase el anexo 21).
- Documento No. 2: Políticas de seguridad informática (véase el anexo 22).
- Documento No. 3: Asignación de responsabilidades (véase el anexo 23).
- Documento No. 4: Uso aceptable de los activos de información (véase el anexo 24).
- Documento No. 5: Instructivo para nombrar respaldos (véase el anexo 25).
- Documento No. 6: Inventario de activos (véase el anexo 26).
    - Formato para solicitar salida de equipos fuera de Construlec Cía. Ltda. (Véase el anexo 27).
    - Formato de entrega de equipos (Véase el anexo 28).
    - Formato de solicitud de acceso a sitios web (Véase el anexo 29).
- Documento No. 7: Instructivo para etiquetado y manejo de la información (Véase el anexo 30).
- Documento No. 8: Instructivo para segregación de la Red (Véase el anexo 31).
- Documento No. 9: Instructivo para la etiquetación de la Infraestructura de Red (Véase el anexo 32).
- Documento No. 10: Instructivo para el revisión de las políticas de seguridad informática (Véase el anexo 33).

- Documento No. 11: Registro de compromiso de la dirección con la seguridad informática (Véase el anexo 34).
- Documento No. 12: Registro de contacto con grupos de seguridad informática. (Véase el anexo 35).
- Documento No. 13: Registro de contacto con las autoridades (véase el anexo 36).
- Documento No. 14: Registro de revisión independiente de la seguridad informática (véase el anexo 37).
- Documento No. 15: Registro de seguimiento de las políticas de seguridad informática (véase el anexo 38).

3.8 ANÁLISIS DE COSTOS

En la tabla 3.7., se puede observar el presupuesto tomado en cuenta para poder realizar la Implementación de hacking ético en el análisis de vulnerabilidades, métodos de prevención y protección aplicados a la infraestructura de red de la empresa Construlec Cía. Ltda.,

MATERIALES			
	CANTIDAD	**V. UNITARIO**	**TOTAL**
Norma ISO/IEC 27002	1	$ 220.00	$ 220.00
Dvd´s en blanco Matrix Torre 50 Unidades	1	$ 14.48	$ 14.48
Flash Memory Memoria Usb, tipo Pen Drive Hp Mini 8gb V165w	1	$ 18.56	$ 18.56
TOTAL DE COSTOS MATERIALES			$ 253.04

OTROS GASTOS		
Capacitación y Consultoría	GLB	$ 405.00
Transporte	GLB	$ 180.00
Impresión y Otros	GLB	$ 120.00
Servicio de Ingeniería	GLB	$ 600.00
TOTAL DE OTROS COSTOS		$ 1,305.00

COSTO DEL PROYECTO	$ 1,558.04

Tabla 3.7.- Análisis de Costos

Fuente: (Investigador)

CONCLUSIONES Y RECOMENDACIONES

3.9 CONCLUSIONES

- Un Test de caja gris es una metodología de hacking ético que proporcionó una guía sistemática basada en valores, permitiendo realizar ataques controlados a la integridad de la red, para poder posteriormente analizar y mejorar la seguridad de la red de información.

- Kali Linux en conjunto con métodos de hacking ético forman un poderoso instrumento para realizar una prueba de intrusión, analizando la red con su abanico de herramientas destinadas para ello, permitiendo evaluar el sistema, conocer la situación real de la empresa y de esta forma conllevar a una mejora continua de su seguridad.

- Se desarrolló ataques controlados en la red de la empresa Construlec Cía. Ltda., con las herramientas que posee Kali Linux las cuales permitieron conocer las vulnerabilidades y el nivel de riesgo que puedan presentarse y así se pudo tener una mejor visión de la seguridad para lo posterior tomar decisiones que mejoren la seguridad de la información.

- Tras las intrusiones dadas en la red de la empresa Construlec Cía. Ltda., se pudo obtener un plan de seguridad de la información aplicada a la empresa siguiendo lineamientos y recomendaciones de normas como ISO/IEC 27000, ISO/IEC 27001 e ISO/IEC 27002, para poder así de ésta manera intentar reducir el índice de vulnerabilidades que pueda darse a la misma.

3.10 RECOMENDACIONES

- Se recomienda realizar pruebas de penetración internas, planificadas por el administrador, en la red de la empresa Construlec Cía. Ltda., siguiendo una metodología de hacking ético.

- Para poder realizar una prueba de seguridad informática en los equipos de una red se recomienda utilizar el software Kali Linux ya que es de fácil uso y a su vez es superior a otros porque posee un abanico de herramientas todas ellas destinadas a realizar pruebas, diagnósticos y comprobaciones de aspectos importantes para evaluar la seguridad informática de los equipos destinados.

- Se debe tener una visión muy responsable para usar Kali Linux ya que posee un potencial muy grande gracias a sus más de 300 herramientas actualizadas, con una configuración automatizada y enfocada al Pentest y algunas de éstas herramientas pueden vulnerar la legalidad.

- Se recomienda a la empresa Construlec Cía. Ltda. Seguir un plan de seguridad que permita disminuir las amenazas y vulnerabilidades de la red de información con el compromiso tanto de autoridades como de empleados de la empresa para cumplir y hacer cumplir las políticas de seguridad planteadas.

- El plan de seguridad de la Información de una empresa o institución es propia de cada una, ya que parte del análisis del riesgo aplicado a la misma y no pueden ser copiada de otra empresa, por eso se recomienda aplicar y seguir los lineamientos y recomendaciones de normas como ISO/IEC 27000, ISO/IEC 27001 e ISO/IEC 27002, según la actividad de la empresa, para poder así de ésta manera intentar reducir el índice de vulnerabilidades que pueda darse a la misma.

BIBLIOGRAFÍA

- Areitio Bertolín, J. (21010). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Paraninfo.
- Benchimol, D. (2011). *Hacking desde Cero.* Buenos Aires: Fox Andina.
- Calle Guglieri, J. (2012). *Reingeniería y Seguridad en el Ciberespacio.* Madrid: Díaz de Santos S.A.
- Chamorro, V. (2013). *Plan de Seguridad de la Información basado en el estandar ISO 13335 aplicado a un caso de estudio.* Quito, Pichincha, Ecuador: Escuela Politécnica Nacional.
- Corletti Estrada, A. (2011). *Seguridad por Niveles.* Madrid: DarFE.
- debianArt. (15 de Mayo de 2014). *debianArt*. Recuperado el 15 de Mayo de 2014, de debianArt: http://www.deviantart.com/morelikethis/collections/269847846
- EC-Council. (2010). *Ethical Hacking and Countermeasures: Attack Phases.* New York: Cengage Learning.
- Gonzáles Ruz, J., de la Mata Barranco, N., Morón Lema, E., Mata, R., Moreno, J., & Morales , F. (2012). Delito e Iformática: Algunos Aspectos. En J. Gonzáles Ruz, N. de la Mata Barranco, E. Morón Lema, R. Mata, J. Moreno, & F. Morales, *Delito e Iformática: Algunos Aspectos* (pág. 398). Madrid: Deusto.
- Graves, K. (2012). *Certified Ethical Hacker.* Barcelona: Sybex.
- ISO/IEC27000. (15 de Enero de 2014). Información General y Vocabulario. *ISO/IEC 27000*. Ginebra, Suiza.
- ISO/IEC27000. (15 de Enero de 2014). Sistemas de Gestión de Seguridad de la Información - Información General y Vocabulario. *ISO/IEC 27000*. Ginebra, Suiza.
- ISO/IEC27001. (28 de noviembre de 2013). Sistemas de Gestión de Seguridad de la Información - Requisitos. *ISO/IEC 27001*. Ginebra, Suiza.
- ISO/IEC27002. (1 de Octubre de 2013). Código de buenas prácticas para los controles de seguridad de la información. *ISO/IEC 27002*. Ginebra, Suiza.

- KaliLinux. (30 de Julio de 2014). *Kali Linux*. Recuperado el 30 de Julio de 2014, de Kali Linux: http://www.kali.org/
- Kaufmann, M. (2011). *Web Server Technology: The Advanced Guide for World Wide Web Information Providers.* San Francisco: Morgan Kaufmann .
- NESSUS. (5 de Julio de 2014). *NESSUS*. Recuperado el 5 de Julio de 2014, de NESSUS: http://www.nessus.com/
- Pardo, E. (2010). *Microinformática de Gestion.* Oviedo: Publicaciones Oviedo.
- Pentoo. (1 de Mayo de 2014). *Pentoo*. Recuperado el 1 de Mayo de 2014, de Pentoo: http://www.pentoo.ch/
- Serrano, K. (2010). *Conceptos fundamentales en la Planificación Estratégica de las Relaciones Públicas.* Barcelona: UOC.
- S-T-D. (1 de Mayo de 2014). *STD 0.1 Security Tools Distribution*. Recuperado el 1 de Mayo de 2014, de STD 0.1 Security Tools Distribution: http://s-t-d.org/
- Unitel. (8 de Junio de 2014). *Normas sobre Cableado Estructurado*. Recuperado el 8 de Junio de 2014, de Normas sobre Cableado Estructurado: http://www.unitel-tc.com/normas-sobre-cableado-estructurado/
- Wifislax. (1 de Mayo de 2014). *LiveWifislax*. Recuperado el 1 de Mayo de 2014, de LiveWifislax: http://www.wifislax.com/
- Wifiway. (1 de Mayo de 2014). *Wifiway 3.5*. Recuperado el 1 de Mayo de 2014, de Wifiway 3.5: http://www.wifiway.org/
- Zhenyu, D. (2012). *Proceedings of the 2012 International Conference of Modern Computer Science and Applications.* Wuhan: Springer.

ANEXOS