

**UNIVERSIDAD TECNOLÓGICA DE SANTIAGO  
UTESA**

Área de Arquitectura e Ingeniería  
Carrera de Informática



**IMPACTO DE LAS PRUEBAS DE PENETRACIÓN EN LA  
EMPRESA CENTRO LEÓN EN SANTIAGO DURANTE EL  
PERÍODO 2010-2011**

Monografía para optar por el título  
de Ingeniero en Informática

**PRESENTADA POR:**  
ANTHUAN VÁSQUEZ  
RAMÓN MARZÁN

**ASESORES:**  
ING. RAMÓN MARTÍNEZ MOTA, M.S.  
LIC. LUCILO TORRES, MA

Santiago de los Caballeros  
República Dominicana  
Abril, 2012

**UNIVERSIDAD TECNOLÓGICA DE SANTIAGO  
UTESA**

Área de Arquitectura e Ingeniería  
Carrera de Informática

**IMPACTO DE LAS PRUEBAS DE PENETRACIÓN EN LA  
EMPRESA CENTRO LEÓN EN SANTIAGO DURANTE EL  
PERÍODO 2010-2011**

Monografía para optar por el título  
de Ingeniero en Informática

**PRESENTADA POR:**

ANTHUAN VÁSQUEZ 1-05-3693  
RAMÓN MARZÁN 1-05-3652

**ASESORES:**

ING. RAMÓN MARTÍNEZ MOTA, M.S  
LIC. LUCILO TORRES, MA

Santiago de los Caballeros  
República Dominicana  
Abril, 2012

**IMPACTO DE LAS PRUEBAS DE PENETRACION EN LA  
EMPRESA CENTRO LEON EN SANTIAGO DURANTE EL  
PERIODO 2010-2011**

# INDICE

|   |    |
|---|----|
| <b>Dedicatorias</b>   | vi |
| <b>Agradecimientos</b>  | ix |
| <b>Resumen</b>  | xi |
| <b>Introducción</b>   | xv |
| <br>  |    |
| <b>1. Capítulo I: Seguridad Informática</b>   |    |
| 1.1. Antecedentes   | 2  |
| 1.2. ¿Qué es Seguridad Informática?   | 4  |
| 1.3. Función de la Seguridad Informática  | 5  |
| 1.4. Conceptos Básicos de Seguridad Informática   | 8  |
| 1.5. Mecanismos de Protección   | 11 |
| 1.6. Seguridad en República Dominicana  | 16 |
| <br>  |    |
| <b>2. Capítulo II: Pruebas de Penetración</b>   |    |
| 2.1. ¿Qué son Pruebas de Penetración?   | 20 |
| 2.2. Tipos de Pruebas de Penetración  | 24 |
| 2.2.1. Prueba de Caja Negra   | 25 |
| 2.2.2. Prueba de Caja Blanca  | 26 |
| 2.3. Evaluación de Vulnerabilidades frente a las Pruebas de Penetración   | 27 |
| 2.4. Hacking Ético  | 30 |
| <br>  |    |
| <b>3. Capítulo III: Pruebas de Penetración: Técnicas y Herramientas</b>   |    |
| 3.1. Etapas   | 34 |
| 3.2. Herramientas de Auditoria de Seguridad   | 40 |
| 3.3. Herramientas de Vulnerabilidades Web   | 41 |
| 3.4. Herramientas de Capturación de Tráfico de Red  | 42 |
| 3.5. Herramientas de Detección de Intrusos  | 44 |
| 3.6. Sistemas Operativos Orientados a Seguridad   | 45 |
| <br>  |    |
| <b>4. Capítulo IV: Impacto de las Pruebas de Penetración en la Empresa Centro León en Santiago, en el período 2010-2011</b> |    |
| 4.1. Descripción de la empresa Centro León Jimenes  | 48 |
| 4.1.1. Misión   | 49 |
| 4.1.2. Visión   | 50 |

|  |           |
|--|-----------|
| 4.1.3. Descripción de la Red en la empresa Centro León | 51        |
| 4.2. Objetivo de la investigación de campo             | 52        |
| 4.3. Metodología de la investigación                   | 52        |
| 4.4. Análisis de los resultados                        | 53        |
| <b>Conclusiones</b>                                    | <b>56</b> |
| <b>Recomendaciones</b>                                 | <b>58</b> |
| <b>Bibliografía</b>                                    | <b>59</b> |

## **DEDICATORIAS**

A mi Padre, el Dr. Fausto Rafael Vásquez Santos, por ser el mejor padre del mundo y ser mi soporte económico para mis estudios en la universidad, por darme consejos para que siga hacia delante.

A mi Madre, Eridania del Rosario Morel, por apoyarme en todo, por cuidarme y darme cariño siempre en todo momento y por ser una buena madre.

A mis Hermanos, Perla Marina Vásquez Morel y Magno Rafael Vásquez Morel, por siempre estar ahí cuando más los necesitaba.

**Anthuan**

A mi padre y a mi madre, Ramón T. Marzan, Belkis Valenzuela, por todo lo que soy hoy, por el apoyo brindado durante el proceso universitario, por su seguimiento y buenas orientaciones.

A Dios, por darme la fuerza necesaria que me mantuvo perseverante, responsable con mis deberes y con toda la fe posible de que si podía lograr mis metas.

**Ramón**

## **AGRADECIMIENTOS**

A los profesores, Cesar Rodríguez, Luis Santana y Gioberty Tineo por compartir sus experiencias como profesionales, por preocuparse siempre por sus estudiantes y hacer la mejor labor como lo es enseñar.

A mis amigos, Alvaro Hilario y Maxuel Jeréz, porque con su apoyo sin importar el momento ni las horas muchas cosas fueron logradas a lo largo de la carrera.

**Anthuan**

A la universidad Tecnológica de Santiago, por brindarnos la oportunidad de realizar y completar nuestros estudios.

Al ayuntamiento de Santiago, por haberme proporcionado una ayuda parcial económica hasta la finalización de mis estudios.

A mis compañeros de trabajo, Dionedi García y José R. Francisco, por todas las veces que me tendieron la mano de forma incondicional.

**Ramón**

## **RESUMEN**

El tema del cual es objeto la presente investigación es el Impacto de las Pruebas de Penetración en la empresa Centro León en el período 2010-2011, en la ciudad de Santiago De Los Caballeros, República Dominicana.

Las Pruebas de Penetración son métodos y técnicas que se utilizan para evaluar, detectar y solucionar vulnerabilidades en las distintas áreas de una infraestructura tecnológica, como servidores web, firewalls, sistemas operativos, base de datos entre otros. Las pruebas de penetración son importantes porque permiten a las empresas conocer las fallas de seguridad que pueden causar en un tiempo determinado daños invaluable dependiendo al área comercial que esta pertenezca y así obtener los parches de actualizaciones que solucionen las brechas de seguridad.

Esta investigación tiene como objetivo general evaluar las vulnerabilidades que se presentan en la infraestructura tecnológica en el Centro León Jimenes en la ciudad de Santiago de los Caballeros, República Dominicana.

Las metodologías que se utilizaron en esta investigación son: bibliográficas, ya que se consulta material de libros, artículos de Internet, revistas y otro tipo de fuentes para obtener información relevante. De campo, porque se hace uso de herramientas y técnicas para determinar las

vulnerabilidades de seguridad dentro de la infraestructura de TI. Descriptiva, porque se evalúan las fallas de seguridad de la infraestructura de TI de la empresa respondiendo a preguntas ¿cómo estaba la seguridad antes de evaluar el área? ¿Cuántas áreas fueron evaluadas? y Prospectiva, porque se toma en cuenta un período determinado dentro del cual se evalúa la empresa.

Los puntos más relevantes de la investigación se basan en las diferentes técnicas y métodos que envuelven el proceso de las pruebas de penetración, así como también, los diferentes pasos secuenciales que se utilizan en dichos métodos. Cabe destacar que cuando se evalúa algún recurso tecnológico específico, esto conlleva al uso de las herramientas destinadas para detectar los diferentes tipos de vulnerabilidades que pueda contener la estructura del servidor web.

Al finalizar la investigación sobre el impacto de las pruebas de penetración en la empresa Centro León en la ciudad de Santiago durante el período 2010-2011, se ha llegado a la conclusión de que:

Mediante la evaluación del servidor web y las pruebas hechas para detectar vulnerabilidades, se obtuvieron resultados que a pesar de no tener

un alto riesgo para el funcionamiento de la página, si comprometen la integridad de los datos que se almacenan en dicho servidor.

Se recomienda la descarga e instalación de parches de seguridad o actualización que permitan cubrir la más mínima brecha de seguridad en la estructura del servidor web para evitar intrusiones futuras no deseadas.

## **INTRODUCCION**

Esta investigación evalúa el impacto que tienen las Pruebas de Penetración en la empresa Centro León Jiménez, en la ciudad de Santiago de los Caballeros, República Dominicana.

En las empresas del país los profesionales del área no conocen de manera amplia lo que son las pruebas de penetración y no cuentan con la preparación necesaria para realizarlas y es por eso que el trabajo de esta investigación busca centrar los aspectos específicos para que sirvan de guía.

A través de los años en la ciudad de Santiago las empresas que cuentan con servidores instalados y sistemas en funcionamiento, es muy poco probable que ejecuten pruebas de penetración para evaluar las fallas de seguridad, estas solo recurren a estas técnicas cuando se encuentran en un estado crítico donde su seguridad ya ha sido violada.

Esta investigación tiene como objetivo general: evaluar las vulnerabilidades que se presentan en la infraestructura tecnológica en el Centro León Jimenes y como objetivos específicos:

- Determinar los métodos y herramientas que se usan en las pruebas de penetración.

- Evaluar los servidores y aplicaciones de la empresa para ofrecer reportes de resultados.
- Analizar la información resultante y que esta sirva de ayuda para optimizar los mecanismos de defensa de la infraestructura.

Este trabajo de investigación ha sido delimitado a impacto de las pruebas de penetración en la empresa Centro León Jimenes, en la ciudad de Santiago en el periodo 2010-2011.

Las metodologías utilizadas en esta investigación son las siguientes: bibliográfica, ya que se consulta material de libros, artículos de Internet, revistas y otro tipo de fuentes para obtener información relevante. De campo, porque se hace uso de herramientas y técnicas para determinar las vulnerabilidades de seguridad dentro de la infraestructura de TI. Descriptiva, porque se evalúan las fallas de seguridad de la infraestructura de TI de la empresa respondiendo a preguntas ¿cómo estaba la seguridad antes de evaluar el área? ¿Cuántas áreas fueron evaluadas? y Prospectiva, porque se toma en cuenta un período determinado dentro del cual se evalúa la empresa.

Se tomará como universo dos servidores web de los cuales uno de ellos servirá como muestra para la evaluación de la infraestructura tecnológica de la empresa, es decir, todo lo concerniente a la página web y como está estructurada.

Las pruebas se harán utilizando la metodología de black box o caja negra, la cual consiste en evaluar la seguridad de la Infraestructura Tecnológica de la empresa sin conocimiento general del entorno, ni cómo operan, ya que esta hace más referencia a lo que es un ataque real.

El Primer Capítulo trata sobre Seguridad Informática de una forma en general, viendo los acontecimientos que han transcurrido durante un periodo de tiempo, se refiere a los conceptos básicos que se suelen usar en seguridad informática.

El Segundo Capítulo trata sobre las Pruebas de Penetración, que son realmente las pruebas, los métodos más utilizados, quienes practican estas pruebas y como lo hacen.

El Tercer Capítulo trata sobre las técnicas y herramientas que se utilizan para realizar las pruebas de penetración, los pasos que hay que

realizar con cada una de ellas para encontrar vulnerabilidades en la infraestructura de TI.

El Cuarto Capitulo trata sobre la empresa Centro León Jimenes, una breve historia de esta, como está configurada el área de TI de la empresa y los resultados sobre el impacto que obtuvo las pruebas de penetración en la infraestructura de TI.

**CAPITULO I**  
**SEGURIDAD INFORMATICA**

De forma general la Seguridad Informática juega un papel muy importante en las organizaciones, ya que abarca todos los aspectos que conciernen a la protección de la infraestructura de Tecnología de información, a medida que surgen nuevos avances tecnológicos las empresas al igual que los empleados se deben acoplar a los nuevos tiempos porque de esta forma se mantienen a la vanguardia y al más alto nivel de competitividad entre las demás empresas a lo que seguridad se refiere.

## **1.1 Antecedentes**

En 1960, el Ministerio de Defensa de los Estados Unidos dio inicio al desarrollo de una red experimental de computadoras para aplicaciones e investigaciones de tipo militar, la cual fue llamada Advanced Research Projects Agency Network por sus siglas en inglés (ARPANET).

Las principales aplicaciones de la red ARPANET permitieron a los usuarios intercambiar información a lo largo de todo el país, en 1970 se formó un grupo de manera informal para trabajar en el proyecto Transmission Control Protocol/Internet Protocol por sus siglas en inglés TCP/IP.

En 1983 se comenzaron a implementar estos protocolos y la red que en ese entonces se conocía como ARPANET fue dividida en dos partes: MILNET, la cual fue utilizada para aplicaciones militares e INTERNET, por otra parte siguió siendo objeto de investigación y se convirtió en lo que se conoce como la red de computadoras más grande del mundo.

Internet iba creciendo en forma considerable ya que se le fueron sumando un sin número de redes y aun así esto no evitó que se le restara importancia a lo que era la seguridad informática en ese entonces.

El 2 de noviembre del año 1988 ocurrió el primer ataque a la red de Internet causado por un Gusano, desarrollado por Robert T. Morris, en el cual se vieron afectados equipos de instituciones como bancos, universidades y organizaciones del gobierno de los Estados Unidos.

La finalidad de este ataque era señalar las fallas de seguridad de otras redes informáticas, pero el Gusano se replicó más rápido de lo esperado y causó pérdidas millonarias de dólares debido a la sobrecarga de los sistemas hasta el punto que se convierten en no funcionales. Este acontecimiento logró concientizar en cuanto a la seguridad informática ya que llevó a la creación del Computer Emergency Reponse Team por sus siglas en inglés CERT.

## 1.2 ¿Qué es Seguridad Informática?

Muchas veces se confunde el término de Seguridad Informática con Seguridad de la Información, cuando en realidad estos son distintos, la seguridad informática es una especialidad que conlleva el uso de diferentes técnicas, softwares y hardwares que se encargan de asegurar una infraestructura de red de una empresa, a diferencia del término de seguridad de la información que está más vinculado con lo que es la protección y la privacidad de los datos.

En el ámbito de seguridad informática no existen sistemas impenetrables, ya que siempre habrá un método por el cual se logrará detectar una vulnerabilidad de seguridad que posee la infraestructura tecnológica a la cual se desea penetrar, lo fundamental en la mayoría de las empresas es documentar a los usuarios acerca de cómo protegerse de las amenazas y a cómo utilizar los recursos para prevenir ataques. Podemos decir que la seguridad informática trata de asegurar los recursos de las empresas para que estos no sean objetos de intrusión.

“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas

medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores”. (Mitnik, 2003, p. 12)

De lo precedentemente citado se entiende que las empresas usualmente no invierten de forma correcta el dinero, al no darse cuenta que la capacitación de los usuarios es primordial para el manejo de los equipos y a su vez mantener la debida seguridad de estos.

Es razonable aclarar que no todas las empresas manejan sus recursos económicos de la misma forma, ya que algunas en muchos casos al área de tecnología de la información no le dan la importancia que requiere dentro de la organización y por consiguiente suelen ocurrir problemas al no contar con la con la tecnología adecuada.

La seguridad informática se fundamenta en tres principios básicos que deben cumplir los sistemas informáticos para lograr sus objetivos, los cuales son:

- **Disponibilidad:** los sistemas siempre deben estar en funcionamiento continuo para que los usuarios accedan a los datos con la frecuencia que requieran y ofrecer un servicio permanente.

- **Confidencialidad:** los sistemas solo deben permitir acceso a las personas que estén autorizadas para mantener la privacidad de los datos.
- **Integridad:** los sistemas deben evitar la duplicidad o la redundancia de información en su base de datos, esto se logra obteniendo una buena actualización y sincronización de los datos.

### 1.3 Función de la Seguridad Informática

Dentro de las funciones que debe desempeñar un departamento de seguridad informática en una organización es un cuanto complicado, ya que toda organización es distinta y cada una de ellas se rige por políticas y procedimientos diferentes, es oportuno mostrar que un departamento de seguridad informática hay varias funciones que se pueden desempeñar.

Existen posiciones dentro del departamento de seguridad informática tales como: Gerente de Tecnología de la Información, Encargado de Infraestructura, Encargado de Sistemas, los cuales desempeñan funciones específicas con un objetivo común.

**Funciones del Gerente de Tecnología de la Información:**

- Administración del presupuesto de seguridad informática.
- Administración de las personas de su equipo.
- Definición de la estrategia de seguridad informática y los objetivos.
- Administración de proyectos.
- Detección de necesidades y vulnerabilidades de seguridad desde el punto de vista del negocio y su solución.

**Funciones del Encargado de Infraestructura:**

- Configuración y operación de los controles de seguridad informática.
- Monitoreo de indicadores de controles de seguridad de los equipos.
- Modificación de accesos a sistemas y aplicaciones.

**Funciones del Encargado de Sistemas:**

- Evaluación de efectividad de los sistemas.
- Analista de los Sistemas.
- Administrador de Base de Datos.
- Auditor de los Sistemas de Información.

## 1.4 Conceptos Básicos de Seguridad Informática

Dentro de los conceptos más comunes que se pueden encontrar en seguridad informática están:

**Amenaza:** podemos entender este término como un posible peligro para la infraestructura de redes o del sistema de información, el cual puede ser una persona o un programa, no es más que un elemento que compromete al sistema.

**Vulnerabilidad:** son las fallas que se suelen encontrar en los sistemas de información o la infraestructura de red, estas son consideradas como debilidades dentro del sistema las cuales pueden ser atacadas para afectar el funcionamiento de estos.

**Virus:** son programas que contienen un código malicioso capaz de infectar otros programas, haciendo que estos disminuyan su rendimiento y causen fallas de seguridad, pueden existir diferentes tipos de virus como: gusanos, caballos de Troya y bombas lógicas.

**Hacker:** es una persona con elevados conocimientos en informática que busca reconocimiento por eludir la seguridad de un sistema si hacer daño.

**Cracker:** es una persona con elevado conocimientos en informática que quiere demostrar sus habilidades de forma equivocada, haciendo daño solo por diversión.

**Phreaker:** es la persona que se asiste de herramientas hardware y software para engañar las compañías telefónicas y evitar el cobro de llamadas.

**Pirata Informático:** es la persona que vende software que está protegido bajo las leyes de copyright.

**Insider:** es la persona que es considerado una amenaza de cualquier forma para el sistema de la empresa.

**SDI:** es un programa el cual está destinado a encontrar intrusos que hayan accedido a un red.

**SPI:** es una extensión de los SDI que previene el acceso no autorizado de un atacante.

**Botnet:** son de robots informáticos que se ejecutan de manera automática y de forma remota para controlar un conjunto de computadoras infectadas.

**Zombie Host:** es un software o un conjunto de computadoras que simula vulnerabilidad para atraer atacantes para saber los métodos y técnicas con las cuales ellos operan.

**Encriptación:** es un proceso que se utiliza para volver de manera ilegible información que se considera importante.

**Spam:** son mensajes masivos no deseados, usualmente publicitarios que perjudican a quien lo recibe.

**Spyware:** es un programa espía que recopila información de un computador y la transmite sin el consentimiento del propietario del mismo.

## 1.5 Mecanismo de Protección

Cuando ya se conocen las fallas de seguridad a las que está expuesta un sistema, se deben tener los mecanismos de defensa apropiados para contrarrestar estas brechas de seguridad, aunque las empresas cuentan con los equipos necesarios para proteger la información y la infraestructura, pocas veces utilizan las técnicas o métodos internamente para determinar el nivel de protección que poseen.

A continuación se especifica algunas herramientas de tipo hardware y software que pueden reducir el nivel de riesgo de ser atacados:

**Firewall:** es un sistema que está destinado a bloquear todo tipo de tráfico que no esté autorizado, permitiendo solo las comunicaciones que estén autorizadas en la infraestructura de red de una empresa, este está basado en políticas de seguridad establecida haciendo que la red sea confiable, los objetivos que debe cumplir un firewall son:

- Todo el tráfico que venga del exterior debe pasar a través de él, así como todo el tráfico del vaya desde el interior hacia el exterior.

- Solo el tráfico que se ha establecido en la política de seguridad es el que se permite.

Es preciso señalar que los firewall no detienen los ataques, tampoco protegen el sistema una vez que se hayan penetrado las políticas de seguridad, sino que estos ayudan a elevar el sistema de seguridad en una organización.

**Lista de Control de Acceso:** es una lista que permite definir los permisos y accesos que son concedidos a los usuarios, así también como limitarlos en ciertas características de la red como el ancho de banda, el tráfico con el uso de ftp.

**Wrapper:** son mecanismos de suplantación de identidad de programas en específico para cambiar el comportamiento de los sistemas operativos sin alterar su funcionamiento original.

**DMZ:** significa zona desmilitarizada es un tipo de configuración que se utiliza para limitar, dividir el acceso a la red desde fuera de una institución, esta solo permite a los usuarios internos tener facilidad para usar los recursos y compartir información.

**Proxy Server:** el servidor Proxy filtra, controla los accesos a páginas Web, limita el uso del Internet en diferentes horarios, las empresas lo usan para tener un mejor control de las operaciones que realizan sus empleados en la Web.

**Sistemas Anti-Sniffer:** este método provee de información al usuario para detectar cuando se está comprometiendo la red, es decir, cuando la placa de red está siendo atacada.

**Gestión de Claves Seguras:** utilizar una clave de 8 caracteres, le permite al usuario o administrador de sistemas de seguridad, mantener la integridad de los datos o el área donde se aplique, ya que con esta combinación pueden tardarse varios años en poder descifrarla.

**SDI:** significa Sistema de Detección de Intrusos es un programa el cual está destinado a encontrar intrusos que hayan penetrado en una red. El objetivo de estos es encontrar cualquier anomalía en las actividades del sistema que venga desde el exterior hacia el interior, de acuerdo al comportamiento y la función que se requiera, estos se clasifican de la siguiente manera:

- **Host-Based IDS:** estos detectan actividades maliciosas que operen en el mismo host donde se encuentre.

- **Network-Based IDS:** se basan en el intercambio de información que se realice en la red.
- **Knowledge-Based IDS:** estos se basan en conocimiento.
- **Behavior-Based IDS:** estos se basan en el comportamiento del usuario.

**SPI:** significa Sistemas de Prevención de Intrusos, es una extensión de los SDI que previene el acceso no autorizado de un atacante, este está basado en políticas de seguridad al igual que los firewalls, dependiendo en la forma en que detectan el tráfico, estos se clasifican de la siguiente manera:

- **Detección Basada en Firmas:** se basa en reconocer una cadena de bytes para hacer la alerta.
- **Detección Basada en Políticas:** se basa en reconocer todo el tráfico que esté fuera de las políticas establecidas.
- **Detección Basada en Anomalías:** se basa en reconocer cuando el tráfico no está dentro de lo normal.
- **Detección Honey Pot:** se basa en usar un señuelo para que los atacantes no puedan llegar al sistema original.

**Criptografía:** estos son métodos que se utilizan para el ocultamiento de información con el objetivo de que dicha información no sea entendible

para aquellas personas que no estén autorizadas. Esta es importante porque hace cumplir los objetivos de la seguridad informática, los cuales son; mantener la privacidad, la integridad y autenticidad de los datos.

**Anti-Virus:** son programas que están destinados con el objetivo de detectar programas que contengan código malicioso o como solemos llamarlos, virus informático. Para estos poder detectar virus deben actualizarse frecuentemente a una base de datos de forma remota, ya que cada día que pasa el número de virus en internet se va incrementando.

“Alcanzar el nivel de seguridad necesario para un organismo financiero representa un ejercicio más difícil”. (Royer, 2004, p.11)

Del escrito anterior se desprende la idea de que las empresas, para poder adoptar un alto nivel de seguridad deben estar siempre a la vanguardia con los últimos avances tecnológicos, esto resulta un tanto difícil ya que se debe tener un buen soporte económico y una buena capacitación en los empleados que son quienes estarán trabajando con estas tecnologías.

Es significativo evidenciar que cuando se trata de un organismo financiero, los procesos que conlleva la seguridad informática dentro del

área de TI son más rigurosos, debido a que todas las operaciones que se realizan dentro de la empresa giran en torno a dinero, por esta razón la seguridad informática debe conservar más sus principios como la confidencialidad, disponibilidad e integridad de los datos.

## **1.6 Seguridad en República Dominicana**

En República Dominicana no se cuenta con los mejores avances tecnológicos, es preocupante y alarmante la forma en que se manejan los centros de cómputos que están encargados de salvaguardar toda la información de la nación, aunque cabe destacar que posee profesionales con altos conocimientos capaces de competir ante escenarios internacionales, aunque la razón por la cual no se están tan protegidos en este país es por la falta de inversión de las empresas multimillonarias e instituciones Bancarias que en ciertos casos suelen ser víctimas de ataques a sus infraestructuras tecnológicas.

Se debe tomar en cuenta que la inversión que se hace en el área de tecnológica da beneficios a largo plazo, proteger la información que es primordial para las instituciones gubernamentales del país es primordial y no se considera un juego, la república dominicana ha sido víctima en varias ocasiones de fraudes y daños a varias de las instituciones que residen en

ella y que forman parte del desarrollo cotidiano y funcionamiento del engranaje que mueve la nación.

Las leyes del país penalizan los delitos informáticos que ocurren, se tiene como ejemplo el de robo de identidad que se contempla en la ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, en su artículo 17 esta legislación establece que el hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con penas de tres meses a siete años de prisión y multa de dos a doscientas veces el salario mínimo.

Dentro de las organizaciones que trabajan y persiguen los delitos informáticos está el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología de la Policía Nacional que tiene como función:

- Investigar todas las denuncias de crímenes o delitos considerados de alta tecnología.
- Responder con capacidad investigativa a todas las amenazas y ataques a la infraestructura crítica nacional.
- Desarrollar análisis estratégicos de amenazas informáticas.
- Desarrollar inteligencia.

Definitivamente se debe tomar más en serio la inversión en la Seguridad Informática por parte de las empresas, instituciones privadas y públicas de lo contrario la república dominicana seguirá modernizándose y al mismo tiempo exponiéndose a crímenes informáticos. En República Dominicana las universidades deben crear nuevas formas que permitan a los estudiantes tener más preparación en el área de seguridad Informática porque sería más factible para los profesionales nativos hacer maestrías en el campo de la informática localmente que salir e invertir grandes cantidades de dinero en el exterior.

Las empresas en el país deben estar muy preocupadas y siempre estar en expectativa ya que lo primordial deben ser sus datos y siempre preguntarse qué tan seguras están, pero al mismo tiempo saber que quienes deberían estar mejor preparados son sus empleados ya que son los que manejan y controlan todo lo que tiene que ver con los sistemas e infraestructura tecnológica.

**CAPITULO II**  
**PRUEBAS DE PENETRACION**

Para detener a un intruso informático se debe de pensar como tal, existen procedimientos que se deben realizar en una empresa para determinar el nivel de seguridad de la misma, llamadas Pruebas de Penetración, estas se ejecutan por personas que tienen la preparación y los conocimientos adecuados en el área de seguridad de informática.

## **2.1 ¿Que son Pruebas de Penetración?**

Con los grandes fallos de seguridad que se presentan constantemente, las empresas han tenido que recurrir a diferentes métodos y pruebas para proteger su infraestructura tecnológica de atacantes que buscan tener acceso a los sistemas, ya sea para afectar el funcionamiento de estos, robar o modificar información de importancia para la empresa. Estas pruebas llevan a las empresas a disminuir los riesgos de seguridad y tener un entorno más seguro dentro de la infraestructura informática.

Las Pruebas de Penetración se definen como un procedimiento que involucra métodos y técnicas para inspeccionar la infraestructura tecnológica de una institución en busca de fallas de seguridad que afectan la, integridad, confidencialidad y disponibilidad de los datos.

Las Pruebas de Penetración no son técnicas ilegales, ya que antes de realizar estas pruebas la institución tiene que facilitar una autorización por escrito, dando el permiso a la persona o a la institución que va a efectuar las pruebas haciendo que todo se conleve dentro de un ámbito profesional.

Opina **Whittaker (2008)** que “Las pruebas de penetración son muy distintas de las pruebas funcionales tradicionales; no sólo carecen los evaluadores de penetración de la documentación apropiada sino que, además, éstos deben pensar como usuarios que tienen la intención de hacer daño”.

“Las pruebas de penetración pueden llevarse a cabo de forma independiente o como parte de los riesgos de seguridad de gestión de procesos que se pueden incorporar en un desarrollo de ciclo de vida regular.” (Ali y Heriyanto, 2011, p.38)

Del escrito anterior se desprende la idea que las pruebas de penetración aparte de que se realizan por personas con conocimientos básicos en el área y desempeñan tareas por cuenta propia, pueden ser integradas en las políticas y procedimientos de una organización con lo cual se puede asegurar durante cada período correspondiente la forma en que se mantiene asegurada la infraestructura tecnológica de dicha empresa.

Es significativo evidenciar que las pruebas de penetración conllevan un procedimiento dentro de la institución que se evaluará, los cuales deben estar bien acoplados a las técnicas y métodos que se usaran para la evaluación de la seguridad de los diferentes equipos que se encuentran en el área de tecnología de la información, para asegurar que las pruebas fueron exitosas.

Cuando se realizan pruebas de penetración el principal objetivo es encontrar vulnerabilidades en la infraestructura tecnológica de una institución, dentro de las cuales podemos destacar las más comunes:

- **Identificación de vulnerabilidades de alto riesgo:** este tipo de vulnerabilidad ponen en riesgo la infraestructura tecnológica de la institución.
- **Identificación de vulnerabilidades de bajo riesgo:** este tipo de vulnerabilidad contienen informaciones de menor riesgo, pero aun así son importantes.
- **Determinar los puntos clave donde se pueden realizar diferentes tipos de ataques:** esto verifica todas las áreas dentro de la infraestructura de red de la institución donde pueda haber un acceso, así como los routers y puntos de acceso que sirven como medio para la conexión de dispositivos.

- **Evaluar el impacto de los ataques exitosos:** también se debe evaluar que tan exitoso fue un ataque determinado en los diferentes puntos clave para solucionar las fallas de seguridad.

“La mayoría de los atacantes ponen a prueba algunas formas muy evidentes para lograr entrar en los ordenadores, y si no lo hacen, van a pasar a la máquina siguiente. Puede decir algo el hecho que se les llaman script kiddies” (Small, 2011, p.4)

De la cita presentada en el texto anterior se puede decir que los Script Kiddies son atacantes que carecen de conocimientos sobre lo que están haciendo y suelen emplear herramientas que no conocen muy bien por ende cuando no logran penetrar en una computadora específica lo que hacen es rendirse e intentar con otra herramienta y computadora en la cual piensan tendrán éxito al tratar de lograr sus objetivos.

Es razonable aclarar que las pruebas de penetración se consideran por algunos dentro del marco informático como un arte y por otros como ciencia, las técnicas y procedimientos utilizados se practican por los profesionales de TI porque estos se certifican y acreditan para realizarlas.

## 2.2 Tipos de Pruebas de Penetración

En el capítulo anterior se explican algunos conceptos relacionados con la seguridad informática, en este se tratan expresiones técnicas sobre las pruebas de penetración como son caja negra y caja blanca, los cuales son términos que representan metodologías en esta rama de la seguridad informática e identifica a los profesionales involucrados en lo que se conoce como Ethical Hacking, que no es más que el uso adecuado de las técnicas y metodologías de forma eficiente para detectar vulnerabilidades dentro de un sistema para proveer reportes de resultados concernientes a estas fallas de seguridad.

Los procedimientos que se emplean en estos dos tipos de metodologías dotan de información necesaria a quien los requiere sobre el estado de la infraestructura, también cabe destacar que cada uno de ellos tiene sus ventajas y desventajas en cuanto a su uso, así como también que están destinados a detectar vulnerabilidades específicas y depende de lo que se quiera lograr. Los hackers éticos que utilizan estas metodologías con propósitos benignos tardan años en aprender y adquirir toda la experiencia necesaria para brindar sus servicios así como redactar documentos que sirven de fuentes para futuras investigaciones y orientaciones.

### **2.2.1 Prueba de Caja Negra**

Se conoce como Caja Negra o Black Box a la metodología de prueba que se realiza desde el exterior de la institución sin tener ningún tipo de conocimiento de la infraestructura que se va a evaluar, haciendo una simulación de un ataque real hacia el sistema, antes de comenzar las pruebas, las personas que practican esta metodología primero deben detectar la localización y la extensión del sistema a analizar, esta es importante porque determina el impacto que tendría un ataque desde el exterior. Las pruebas de penetración de caja negra son actividades intensas que requieren de experiencia para reducir al mínimo el riesgo que podrían correr los sistemas de que se analizan.

#### **Ventajas de las Pruebas de Caja Negra:**

- Provee información cercana a la realidad sobre las amenazas.
- Obtiene resultados a partir del entorno donde se localiza el sistema.
- No necesita información proveniente de los propietarios o de los encargados de la infraestructura de red.

### **Desventajas de las Pruebas de Caja Negra:**

- No consta con información específica sobre el entorno.
- Pasa por desapercibido detalles de seguridad.

#### **2.2.2 Prueba de Caja Blanca**

Se conoce como Caja Blanca o White Box a la metodología de prueba que se realiza cuando se tiene conocimiento total de la infraestructura tecnológica con la que se está trabajando a diferencia de la metodología de caja negra. El objetivo de esta es comprobar errores de código y verificar configuraciones de software y hardware, centrándose más en los procesos principales del sistema.

Se puede referir a la prueba de caja blanca como Prueba Interna. La persona involucrada en este tipo de prueba de penetración debe estar al tanto de todas las tecnologías fundamentales utilizadas internamente en el entorno objetivo, por consiguiente esto ofrece al auditor la posibilidad de evaluar las vulnerabilidades de seguridad con el más mínimo esfuerzo requerido durante el transcurso de las operaciones que se tienen en planificación para llevarse a cabo. Comparativamente se requiere de menos tiempo y dinero para encontrar y resolver fallas de seguridad que con el enfoque de caja negra.

**Ventajas de las Pruebas de Caja Blanca:**

- Permite ejecutar los procedimientos de forma cautelosa.
- Consta con información específica sobre el entorno.
- Se identifican todas las posibles amenazas y las fallas de configuración.

**Desventajas de las Pruebas de Caja Blanca:**

- Simulaciones en busca de vulnerabilidades son lejanas de la realidad.
- Los propietarios del sistema necesitan proveer mucha información.

**2.3 Evaluación de Vulnerabilidades frente a las Pruebas de Penetración**

Debido al crecimiento de la industria de seguridad de tecnología de la información resulta difícil entender y practicar la correcta terminología utilizada para referirse a evaluación de la seguridad. Por esto a continuación se detalla la descripción de lo que es Evaluación de la seguridad y también diferenciarlo de lo que se conoce como pruebas de penetración.

**Evaluación de Vulnerabilidad:** es un proceso que consiste en acceder los controles de seguridad **internos** y **externos**, identificando las amenazas que exponen los recursos de la institución u organización. La evaluación que se realiza en la infraestructura de red o sistema de la empresa no solo da a conocer los riesgos en los mecanismos de defensa existentes, sino que también recomienda y prioriza las estrategias adecuadas para corregir las fallas o brechas de seguridad que fueron encontradas durante dicha evaluación.

Se evalúan las vulnerabilidades internas en una empresa para garantizar la seguridad del sistema interno, mientras que la evaluación de vulnerabilidades externas puede proveer información crucial sobre la seguridad de los mecanismos de defensa con los cuales se cuenta. Dependiendo del tipo de evaluación que se vaya a realizar se sigue un patrón de pruebas, herramientas, y técnicas utilizadas para detectar estas vulnerabilidades en los recursos tecnológicos de información de forma automatizada.

Lo antes mencionado se puede lograr mediante una plataforma integrada administradora de vulnerabilidad, la cual mantiene una base de datos de vulnerabilidades actualizadas capaz de probar diferentes tipos de

equipos en una red y a su vez mantener la integridad de los cambios que se realicen en la configuración de dichos equipos.

La diferencia que se puede explicar entre estos dos términos es que una Prueba de Penetración va más allá de lo que es identificar vulnerabilidades y se apega a lo que es el proceso de exploración, obtención de privilegio, aseguramiento de acceso en el sistema que se evalúa, por otro lado la Evaluación de Vulnerabilidades da una vista general de cualquier brecha o falla de seguridad en la infraestructura sin medir el impacto que pueden tener en esta.

Otra diferencia que se puede denotar es que en las pruebas de penetración se trabaja de forma más agresiva ya que se busca la forma de hacer el papel de un posible intruso por lo cual utiliza y aplica todos los métodos y técnicas necesarias en un ambiente de trabajo constante, mientras que la Evaluación de Vulnerabilidades como se realiza un proceso cuidadoso este identifica y cuantifica todas las posibles amenazas de una forma procedimental y muy tranquila.

## 2.4 Hacking Ético

Todo profesional en su área de desarrollo tiene un código por el cual rige su conducta así como los procedimientos que ejecuta al momento de realizar alguna tarea específica, en el área de seguridad informática se les denomina Hackers Éticos a los profesionales que con técnicas y procedimientos logran obtener resultados producto de evaluaciones e investigaciones rigurosas sobre algún tipo de problema que se presenta en la infraestructura tecnológica de una empresa.

¿Porque utilizar el término Ético en esta área de seguridad? Cuando se pretende emular la metodología de ataque de un Cracker y no se es, tiene que existir ética de por medio, esto quiere decir que todas las operaciones que realice el Hacker Ético no deben comprometer de ninguna forma la información con la cual la empresa cuenta, ya que este es su activo más valioso para la realización de sus operaciones internas y externas.

Dentro de los daños que se pueden presentar en la empresa si no se trabaja con ética y profesionalismo están los siguientes: Modificación de registros, Borrado de Datos, Alteración de Configuraciones de Equipos, proveer información a Terceros, Guardar Información en Memorias USB entre otros que comprometen normas de confidencialidad.

A lo largo del tiempo el término de Hacking se mal interpreta y se asocia a personas con mala reputación que buscan hacer daño solo por diversión, así como ingresar a sistemas y redes informáticas sin ningún tipo de autorización para probar de lo que son capaces. A continuación se presentan una lista de conductas que deben de existir en el profesional ético de la Seguridad Informática:

- Hacer su trabajo de la mejor manera posible
- Hacer un buen reporte de trabajo.
- Acordar un precio justo.
- Respetar el secreto.
- No hablar mal de ningún administrador ni equipo de trabajo.
- No aceptar sobornos.
- No alterar o manipular resultados o análisis.
- Delegar tareas específicas en alguien más capacitado.
- No prometer algo imposible de cumplir.
- Ser responsable en su rol y función.
- Manejar los recursos de forma eficiente.

El Hacker Ético de la Seguridad cuando evalúa una red informática como parte de las actividades que realiza necesita ser perseverante ya que

en ciertos casos se puede presentar la tarea de mantenerse por largos periodos ejecutando procesos hasta lograr su objetivo, y todo esto sin valerse del uso de técnicas y herramientas específicas.

Para esto se deben emplear todos los recursos de inteligencia al alcance, utilizar al extremo los conocimientos que se tengan, poder de análisis, deducción y razonamiento para así determinar que se puede intentar, cómo, dónde y con qué. Un Hacker Ético debe cumplir con las siguientes aptitudes como:

- Saber cómo definir patrones de conducta y acción.
- Hacer relevamientos pasivos de información.
- Interpretar, generar código y cifrado de datos.
- Descubrir vulnerabilidades presentes de todo el escenario técnico.
- Buscar lógica e ilógicamente.
- Proyectarse sobre la marcha en modo abstracto, táctica y estratégicamente.
- Ser ético por sobre todas las cosas.

## **CAPITULO III**

### **PRUEBAS DE PENETRACION: TECNICAS Y HERRAMIENTAS**

Mostrar las metodologías específicas y el uso de herramientas de las pruebas de penetración es una forma de incentivar y también fomentar el desarrollo intelectual de personas que desean incursionar en el área del Pentest. Ocultar este tipo de recursos no es la solución para que los intrusos declinen de hacer daño a Sistemas Informáticos sino que mostrarlas puede ayudar a que se de el uso correcto y se descubra la magnitud de sus resultados.

### **3.1 Etapas**

Es preciso que al momento de hacer las pruebas, el especialista realice una lista de los requerimientos del cliente para hacer las evaluaciones de seguridad en la infraestructura de red de la empresa. Dentro de los pasos o procedimientos que hay que realizar para obtener los resultados esperados de las pruebas, se pueden destacar: Recolección de información, detección de vulnerabilidades, escalamiento de privilegios, limpieza de evidencias y mantenimiento de acceso. Cada uno de estos procedimientos se realiza con un objetivo común, y con herramientas específicas para cada etapa.

Cada uno de estos niveles posee vital importancia para lograr los objetivos que se plantean al inicio de las pruebas, trabajan de forma

secuencial, por consiguiente el nivel de experiencia y profesionalismo que se requiere en el área debe ser alto. Cuando una prueba usando la técnica de Black Box se ejecuta hay que tener en cuenta, primero que la empresa a la cual se le realiza corre riesgos con sus equipos de hardware, ya que esta trabaja de forma paralela, es decir, mientras se realiza la evaluación la empresa opera y realiza sus funciones normales bajo este ámbito de riesgos.

### **Recolección de Información:**

Siendo la primera etapa del proceso de evaluación de seguridad, básicamente consiste en recolectar la mayor cantidad de información sobre el objetivo a ser evaluado, esta etapa busca contar con todos los detalles necesarios e información que ayuden a facilitar hacker ético conocer el entorno en el que trabajara, sin revelar la presencia de este ni las intenciones, analizando así la forma en que la institución opera y determinando la mejor ruta para hacerlo. La recolección de información requiere de paciencia, mucha investigación y sobre todo pensar como el atacante.

La mayoría de los profesionales sabe que los detalles de la investigación o recolección pueden significar la diferencia entre el éxito y

el fracaso de la prueba de penetración. La recolección de información se conoce como la etapa de mayor importancia ya que prevé todas las bases para la continuidad de los demás niveles. La inteligencia abierta es una forma utilizada para recabar, seleccionar información disponible, también existe la forma pasiva que permite identificar los límites de una red, los sistemas operativos y los servidores Web en dicho objetivo.

### **Detección de vulnerabilidades:**

Determinar la vulnerabilidad que existe en los sistemas es el siguiente paso luego de reunir toda la información relevante sobre el objetivo. Con este propósito un hacker ético debe tener a su disposición un conjunto de exploits y vulnerabilidades, el conocimiento del profesional es parte vital también en este proceso ya que pone a prueba toda su experiencia, se realiza un análisis de toda la información recolectada para determinar la vulnerabilidad lo cual se le llama escaneo manual de vulnerabilidad mientras que la detección de vulnerabilidad se hace manual.

Cuando se finaliza la detección de vulnerabilidades se produce una lista definitiva de brechas sobre el objetivo para investigar a profundidad, esta lista se utiliza en la siguiente etapa. Luego se realiza un intento de intrusión en estas brechas las cuales ya fueron definidas previamente.

## **Escalamiento de Privilegios:**

Esta etapa se enfoca en hacer pruebas de seguridad con la información previamente recolectada para la explotación de las vulnerabilidades encontradas en la infraestructura de red. Se utilizan todos los conocimientos que se tenga sobre los sistemas para probar todas las alternativas necesarias que se puedan, para introducirse al sistema. En esta es donde se refleja la profesionalidad y el conocimiento que posee el especialista que realiza las pruebas, la organización donde se realizan estas pruebas debe de estar informada de cualquier actividad que pueda ocasionar problemas al funcionamiento del sistema, de modo que pueda planificarse en una fecha donde se realicen sin inconvenientes.

Cuando se trata de acceder al sistema esto nunca se logra a la primera, primero hay que hacer explotar varias vulnerabilidades del sistema para conseguir un acceso de diferentes niveles en la plataforma que se esté trabajando, no suele pasar de inmediato, hay que hacer uso de varias técnicas y herramientas para conseguir un acceso total y hacerse del control del sistemas. Esta tiene como objetivo comprobar si un atacante puede tener privilegios en el sistema para obtener datos que estén restringidos y ocasionar daños a la infraestructura del sistema. En esta etapa es donde se

requiere el uso de técnicas de programación o exploit para explotar los niveles de seguridad que se encuentren en el sistema.

### **Limpieza de Evidencias:**

Esta se enfoca en comprobar todo tipo de información que pueda detectar que se hayan introducido al sistema, los atacantes una vez que logran acceder a un sistema de una organización van eliminando todo tipo de rastros dejado como la eliminación de logs para no ser detectados por algún tipo de sistema de prevención de intrusos. Esto lo hacen para que cuando se haga una auditoria de seguridad en la infraestructura de red no quede ningún registro existen del ataque al sistema.

Cuando se está en esta etapa se toman todas las precauciones posibles para eliminar los registros dejados luego de acceder al sistema, todo esto dependerá de la plataforma en la que se esté trabajando, ya que dependiendo el sistema operativo al que se acceda cada uno de ellos maneja de forma diferente el registro de los logs de la acciones que realizan los usuarios, si se borra por completo un log esto encendería una alerta en el sistema lo que puede ocasionar que detecten si hay un intruso en el sistema, por lo que hay que recurrir a modificar y suplantar la información que contenga el log. Todo se realiza para no ser descubierto por los

administradores del sistema y hacer que el análisis de los registros sea más difícil cuando se audite la seguridad en la empresa.

### **Mantenimiento de Acceso:**

Después de la intrusión en el sistema objetivo se debe mantener el acceso a este y aún más, expandirlo. Un profesional puede decidir entre atacar el sistema el cual ha estado evaluando o mantenerse al margen para desde dentro ingresar a los demás sistemas de la empresa y explotarlos, en ambas situaciones la empresa es vulnerable. Se suele utilizar kits de acceso con los cuales se obtiene acceso a nivel de sistema operativo mientras que con los troyanos el acceso se da a nivel de aplicaciones, con este último se pueden obtener las contraseñas, usuarios entre otros y se pueden integrar en el sistema operativo como servicios del sistema.

Dentro de esta etapa se destaca el hecho de que un hacker ético puede plantar un acceso de Puerta Trasera el cual puede utilizar para tener acceso a un sistema cuando le plazca, aunque en muchos casos esto puede tener consecuencias graves, también podría ser beneficioso para los sistemas si se contempla con tiempo para cuando se presente una situación de emergencia se tenga acceso de esta forma como segunda opción.

### 3.2 Herramientas de Auditoria de Seguridad

Existe un conjunto extenso de herramientas para la evaluación de seguridad de la infraestructura de red de una empresa, con las cuales se pueden obtener diferentes resultados en diferentes ámbitos, es decir, muestran resultados asociados a la categoría que pertenecen. Para hacer un buen uso de las herramientas se debe tener un conocimiento previo.

“La emoción para la mayoría de las personas viene de la explotación de los sistemas obteniendo los privilegio de administrador, pero se necesita caminar antes de correr”. (Kennedy, D., O’Gorman, J., Kearns, D. y Aharony, M., 2011, p. 16)

De la cita presentada en el texto anterior se asocia a que las personas o conjunto de ellas dedicadas a la auditoria de seguridad, deben contar con los conocimientos o capacitaciones adecuadas para poder obtener información de calidad en el filtrado de vulnerabilidades en la organización.

Es conveniente destacar que las personas que practican las pruebas de penetración deben tener los conocimientos o capacidades necesarias para solucionar cualquier falla de seguridad encontrada en la infraestructura de TI de la empresa.

### 3.3 Herramientas de Vulnerabilidades WEB

Dentro de las diferentes herramientas que pueden utilizarse para la evaluación de seguridad de ambientes web podemos destacar:

**Burp Suite:** es un conjunto de herramientas con varias interfaces que permite atacar aplicaciones web, su diseño facilita e incrementa el proceso de ataque. Todas las herramientas contenidas en este paquete comparte el mismo framework para manejar autenticación, proxys, alertas y extensibilidad. Esta es compatible con los sistemas operativos Linux, Mac y Windows.

**Nickto:** es una aplicación de código abierto que descubre las vulnerabilidades de los servidores web, tiene la capacidad de analizar la configuración de los servidores tales como la presencia de múltiples archivos indexados, opciones de http y también identifica los web servers y software instalados en el servidor. Esta es compatible con los sistemas operativos Linux, Mac y Windows.

**Paros Proxy:** es un web proxy basado en Java para acceder a las vulnerabilidades de las aplicaciones que permite editar y ver mensajes de tipo http/https para cambiar los cookies y los campos de formularios de

dichas páginas, también escanea ataques de Inyección SQL las cuales pueden modificar registros en la base de datos.

**Dirbuster:** busca directorios y páginas ocultas en un servidor web, ya que en algunas ocasiones las páginas se dejan de formas accesibles pero no enlazadas. El objetivo de esta herramienta es encontrar estas vulnerabilidades potenciales. Esta está desarrollada en Java por lo que es multiplataforma.

### 3.4 Herramientas de Capturación de Trafico de Red

**Wireshark:** es una aplicación para analizar protocolos y solucionar problemas en redes de comunicaciones, que permite examinar información de la red en ambiente real y capturarla en un archivo para almacenarlas en el disco duro. Esta aplicación permite filtrar y detallar los paquetes capturados que se desean y también es utilizada con fines educativos.

**Netstumbler:** es la mejor herramienta utilizada en la plataforma de Windows para encontrar puntos de accesos inalámbricos abiertos que verifica la configuración de una red, detecta las redes que causan interferencias a otras, así como también la intensidad de la señal de dichas redes.

**POF:** esta herramienta es capaz de identificar el sistema operativo de un objetivo simplemente examinando los paquetes capturados, aun cuando el dispositivo que se analiza está detrás de un corta fuegos de paquetes. Esta herramienta no genera ningún tráfico adicional de red. Puede detectar la presencia de un firewall así como también el uso del NAT.

**Cisco Global Exploiter:** es una herramienta de hackeo utilizada para encontrar vulnerabilidades de explotación en los sistemas de redes de Cisco. La herramienta combina catorce vulnerabilidades que aplican a un conjunto específico de dispositivos Cisco de Telnet, HTTP y el protocolo UDP.

**Ettercap:** es un paquete para ataques a redes LAN que contiene monitoreo de conexiones en tiempo real. Soporta protocolos SSH y HTTPS y hace posible la inyección de datos en una conexión establecida e intercepta tráfico remoto mediante un túnel llamado Encapsulación Genérica de Enrutamiento por sus siglas en ingles GRE.

**NMap:** es una utilidad para la exploración de redes o auditoria de seguridad. Muchos administradores la utilizan porque permite inventariar redes, administrar servicios y monitorear equipos clientes. Permite determinar que tipo de filtro de paquetes, sistemas operativos, nombre de

aplicaciones, están siendo utilizadas por el equipo cliente. Es multiplataforma y posee una interfaz gráfica avanzada.

### **3.5 Herramientas de Detección de Intrusos**

**Snort:** es una herramienta para analizar el tráfico y paquetes de la red a través de protocolos y búsqueda de contenido. Detecta gran variedad de Gusanos así como intentos de intrusión y cualquier otro tipo de comportamiento sospechoso, posee un motor de detección que permite o rechaza el tráfico que circula en la red.

**Ossec Hids:** esta herramienta realiza análisis de logs, detecta intrusos al sistema raíz. Es comúnmente utilizada en por las universidades, ISP y Data Centers, para monitorear sus sistemas de firewalls.

**Honeyd:** esta aplicación crea clientes virtuales en una red, los clientes pueden ser configurados para ejecutar servicios de forma arbitraria. Puede habilitar un solo cliente para que simule múltiples direcciones en una red LAN. Es posible hacer ping desde las máquinas virtuales así como también simular cualquier tipo de servicio de acuerdo a un sencillo archivo de configuración.

### 3.6 Sistemas Operativos Orientados a Seguridad

**Backtrack:** es una distribución de Linux que contiene una gran variedad de herramientas de seguridad y provee un buen entorno de desarrollo. Es una de las herramientas más utilizadas para la realización de pruebas de penetración por los Hackers Éticos.

**Knoppix:** es una representación colectiva de GNU Linux capaz de detectar el hardware de un equipo automáticamente. Soporta diferentes tarjetas gráficas, sonido y dispositivos de almacenamiento entre otros periféricos.

**SELinux:** es una distribución dedicada a la mejora de seguridad para implementar comandos de control de acceso. Los usuarios y los procesos se les garantizan el más mínimo privilegio requerido de una forma más fácil que la tradicional. Se pueden definir políticas para prevenir los navegadores de tener acceso a llaves de tipo SSH.

**Blackbuntu:** es una distribución Linux que está diseñada especialmente para pruebas de seguridad, orientada a estudiantes que se forman en el área de seguridad informática y para profesionales que practican el Ethical Hacking.

“La desventaja de utilizar herramientas comerciales es que debido a su automatización, el usuario no aprende a realizar los mismos procesos de forma independiente”. (Maynor, D., Mookhey, K., Cervini, J. y Rosean F., 2007, p.231)

De la cita anterior se determina que simplemente este tipo de herramientas comerciales no muestra en realidad la forma en que se realiza algún tipo de prueba, ya que con un simple clic para escanear o realizar otra función se puede resolver una parte de la prueba y volver en minutos después para seguir con la siguiente parte del proceso.

Se puede argumentar que utilizar un conjunto de herramientas de distribución abierta puede ser de gran ayuda, ya que proporciona de manera específica las que se utilizan para cada proceso y conllevan a que la persona que las utiliza tenga conocimientos sobre el sistema operativo donde se implementará, así como una lista de comandos secuenciales para su ejecución.

## **Capítulo IV**

### **Impacto de las Pruebas de Penetración en la Empresa**

**Centro León en Santiago de los Caballeros, en el**

**período 2010-2011**

En este capítulo se presenta una breve descripción de la empresa Centro León Jimenes, los objetivos de la investigación de campo, metodología de la investigación y los análisis de resultados de las pruebas de penetración.

#### **4.1 Descripción de la empresa Centro León Jimenes**

En 1964 se realizó el primer Concurso de Arte Eduardo León Jimenes con la doble intención de impulsar el desarrollo de las artes visuales y estimular la creatividad en las nuevas generaciones de artistas. En el discurso inaugural cuando Don Eduardo León Asensio anticipó que, al cabo de los años, se tendría una importante colección de artes visuales que iba a demandar la creación de una institución para exponerla de manera permanente.

Esta predicción se convirtió en realidad en 1999 cuando la Fundación Eduardo León Jimenes, presidida por Don José A. León Asensio, inició los trabajos preparatorios para la construcción del Centro Cultural Eduardo León Jimenes. Inmediatamente se comenzaron a recibir donaciones espontáneas, así como préstamos, cesiones y adquisiciones de importantes

colecciones artísticas, arqueológicas, etnológicas y bibliográficas, todas relacionadas con temas propios de la cultura dominicana.

Para organizar estas valiosas colecciones y sus formas de manejo y disposición al público, fueron contratados los servicios de Consultores y Asesores Profesionales (CAP), bajo la dirección de Rafael Emilio Yunén, y de Arquitectura del Sol, presidida por Pedro José Borrell. Junto a un equipo de especialistas en diversas áreas, ambas firmas propusieron una original visión institucional para integrar las colecciones a la documentación científica y a la producción de proyectos y servicios culturales.

#### **4.1.1 Misión**

El Centro León desarrolla la creatividad a través de la investigación, protección, exhibición y difusión de realizaciones artísticas y culturales dominicanas y de todo lo que contribuya a la conformación de una sociedad más sensible a los valores trascendentes, más orgullosa de sí misma y capaz de participar activamente en el mejoramiento de la calidad de vida de la nación dentro del contexto caribeño.

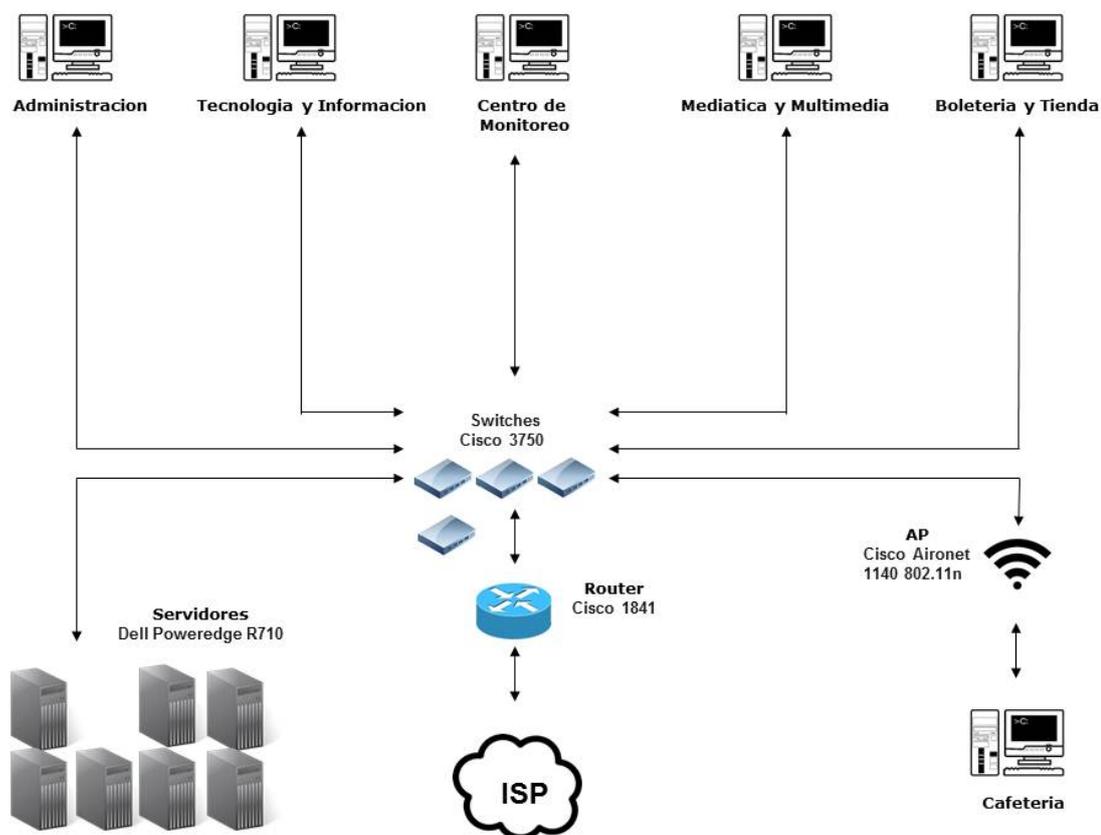
#### **4.1.2 Visión**

El Centro León trabaja para convertirse en uno de los centros culturales más completos en el Caribe y Latinoamérica en la documentación y realización de ofertas y productos culturales.

El Centro León busca favorecer el incremento del interés, los públicos y las instituciones especializadas en el campo cultural, al facilitar el reconocimiento cultural de comunidades, actores culturales, tradiciones y vanguardias, centrado en la calidad y diversidad de corrientes, concepciones y estilos artísticos, mediante la generación de dinámicas de aprendizaje, accesibilidad, participación y producción cultural fundamentadas en las tecnologías de información y comunicación.

### 4.1.3 Descripción de la Red en la empresa Centro León

Grafica No. 1 Descripción de la Red de la empresa Centro León,  
Santiago de los Caballeros, República Dominicana.



La Red de la empresa Centro León cuenta con los siguientes componentes: 7 Servidores Dell Poweredge R710 con los cuales se realizan todas las operaciones de la empresa, 4 Switches Cisco 3750 de 8 puertos que conectan cada uno de los departamentos, 1 Router Cisco 1841 que

conecta con la ISP, 1Access Point Cisco Aironet 1140 802.11n para dar servicios de Internet Wireless en la cafetería, Cat-5 es la categoría de cable UTP utilizado en la empresa, por ser el de más calidad y soporta frecuencias de 100MHZ.

## **4.2 Objetivo de la investigación de campo**

Dentro de los objetivos de campo de la investigación están:

- Detectar posibles vulnerabilidades en el servidor web.
- Presentar soluciones en las fallas de seguridad encontradas.

## **4.3 Metodología de la investigación**

Esta investigación se realizó utilizando la plataforma de Linux Backtrack 5 R1 que contiene un conjunto de herramientas destinadas a la evaluación de la seguridad de una infraestructura tecnológica en sus diversas áreas. Es preciso señalar que específicamente se utilizó la herramienta Websecurify Scanner, para analizar y encontrar brechas de seguridad en la estructura de la página web. Wapiti, fue otra de las herramientas utilizadas para el análisis de la página web.

Este tipo de herramientas son utilizadas para detección de errores en el contenido de los archivos de la página, inyecciones tipo SQL a la base de datos para probar su soporte, también inyecciones de tipo XSS.

#### 4.4 Análisis de los resultados

**Tabla No. 1 Vulnerabilidad de tipo Cross-site Scripting, Santiago de los Caballeros, Marzo 2012**

| URL  |          |
|--|----------|
| <i>http://www.centroleon.org.do/esp/n_lstnoticia.asp?index=916&amp;All=1&amp;month=1&amp;year=%22'%3Ctuf%3E</i>    |          |
| <i>http://www.centroleon.org.do/esp/n_lstnoticia.asp?index=922&amp;All=1&amp;year=2012&amp;month=%22'%3Ctuf%3E</i> |          |
| Nivel de Riesgo  | Cantidad |
| <b>Alto</b>  | 0        |
| <b>Medio</b>   | 0        |
| <b>Bajo</b>  | 2        |

| Leyenda |        |
|---------|--------|
| Alto    | 7 - 10 |
| Medio   | 4 - 6  |
| Bajo    | 1 - 3  |

La tabla No. 1 presenta las urls con sus respectivos parámetros, donde fue encontrada la vulnerabilidad de tipo cross-site scripting en toda de la página web.

**Tabla No. 2 Vulnerabilidad de tipo Directory Listing Enabled,  
Santiago de los Caballeros, Marzo 2012**

| URLs  |          |
|---|----------|
| <a href="http://www.centroleon.org.do/esp/Images/MIC4/gds/">http://www.centroleon.org.do/esp/Images/MIC4/gds/</a> |          |
| <a href="http://www.centroleon.org.do/esp/Images/MIC4/">http://www.centroleon.org.do/esp/Images/MIC4/</a>         |          |
| <a href="http://www.centroleon.org.do/esp/Images/">http://www.centroleon.org.do/esp/Images/</a>                   |          |
| <a href="http://www.centroleon.org.do/esp/Images/_notes/">http://www.centroleon.org.do/esp/Images/_notes/</a>     |          |
| Nivel de Riesgo   | Cantidad |
| <b>Alto</b>   | 0        |
| <b>Medio</b>  | 4        |
| <b>Bajo</b>   | 0        |

La tabla No. 2 muestra la vulnerabilidad de tipo Directory Listing Enabled en las urls mostradas anteriormente, lo cual permite a un atacante navegar entre los directorios de la página web.

**Tabla No. 3 Vulnerabilidad de tipo Banner Disclosure, Santiago de los Caballeros, Marzo 2012**

| URL   | Versión                     |
|---|-----------------------------|
| <a href="http://www.centroleon.org.do/">http://www.centroleon.org.do/</a>   | Server: Microsoft-IIS/7.5   |
| <a href="http://www.centroleon.org.do/">http://www.centroleon.org.do/</a>   | X-Powered-By: ASP.NET       |
| <a href="http://www.centroleon.org.do/esp/procesarform.aspx">http://www.centroleon.org.do/esp/procesarform.aspx</a> | X-AspNet-Version: 2.0.50727 |
| Nivel de Riesgo   | Cantidad                    |
| <b>Alto</b>   | 0                           |
| <b>Medio</b>  | 0                           |
| <b>Bajo</b>   | 3                           |

La tabla No. 3 muestra las vulnerabilidades de tipo Banner Disclosure en las URLs mostradas anteriormente, que permiten a un atacante saber mediante el tipo de servidor y su versión la debilidad de este.

## **CONCLUSIONES**

Al finalizar esta investigación sobre el impacto de las pruebas de penetración en la empresa Centro León en la ciudad de Santiago, en el periodo 2010-2011, se ha llegado a las siguientes conclusiones.

En las evaluaciones del servidor web de la empresa Centro León, mediante el uso de la herramienta Websecurify Scanner se obtuvieron los resultados del análisis a la página web realizados de forma directa, los cuales mostraron información relevante sobre la condición de la estructura y seguridad de dicha página.

Mediante el escaneo realizado se encontraron diferentes tipos de vulnerabilidades como: Cross-site Scripting, Listing Directory Enabled y Banner Disclosure las cuales pueden afectar la información contenida en la base de datos del servidor web de manera crucial.

Se logró determinar que estas vulnerabilidades facilitan el acceso de un atacante al servidor web para así poder alterar los datos y modificarlos a su antojo obteniendo así datos específicos de usuarios comprometiendo la confidencialidad y la integridad de estos.

## **RECOMENDACIONES**

A la empresa se le sugiere las siguientes recomendaciones o soluciones referentes a los tipos de vulnerabilidades encontradas:

Concerniente a la vulnerabilidad de tipo Cross-Site Scripting se recomienda que se filtre y se depure toda la información que el usuario maneje antes de utilizarla en la página para evitar las inyecciones de códigos maliciosos por los atacantes.

Para el caso de la vulnerabilidad de tipos Directory Listing Enabled se recomienda que el encargado de la administración del servidor web deshabilite la navegación de directorios, ya que no es factible que un usuario exterior conozca la estructura de cómo está formada la página.

No se recomienda que la empresa muestre los tipos y las versiones de los servidores web que utiliza para la administración de la página web, ya que esto da una idea general a un atacante de las posibles vulnerabilidades que presentan dicha aplicaciones web.

## **BIBLIOGRAFIA**

- Andreu, A. (2006). *Professional Pen Testing for Web Applications* United State Of America: Wrox.
- Ali, Heriyanto (2011). *BackTrack 4: Assuring Security by PenetrationTesting*. United State Of America.
- EC-Council, (Ed.) (2010). *Penetration Testing: Security Analysis (EC-Council Certified Security Analyst)*. United State Of America: Course Technology.
- EC-Council, (Ed.) (2010). *Penetration Testing: Procedures & Methodologies*. United State Of America: Course Technology.
- Engebretson, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series)*. United State Of America: Syngress.
- Firtman, S. (2005). *Seguridad Informática, Manuales USERS: Las amenazas y vulnerabilidades más peligrosas al desnudo*. United State Of America: M.P. Ediciones.
- Kennedy, D., O’Gorman, J., Kearns, D. y Aharoni, M. (2011). *The Penetration tester’s guide*. United State Of America.
- Maynor, D et al (2007). *Metasploit toolkit for peneration testing, exploit development, and vulnerability research*. United State Of America.
- Mitnick, K. y Simon, W. (2003). *The art of deception: controlling the human element of security*. United State Of America: Wiley.

Ramachandran, V. (2011). *BackTrack 5 Wireless Penetration Testing Beginner's Guide*. United State Of America: Packt Publishing.

Royer (2004). *Seguridad en la informática de empresa: Riesgos, amenazas, prevención y soluciones*. España: Editions ENI.

Small (2011). *Fixing the industry: penetration testing execution standar*. United State Of America.

Tori, C. (2008). *Hacking Ético*. Argentina: Rosario

Whitaker, A. y Newman, D. (2005). *Penetration Testing and Network Defense*. United State Of America: Cisco Press.

Wilhelm, T. (2009). *Professional penetration testing: Volume 1: Creating and learning in a hacking lab*. United State Of America: Syngress.

Wilhelm, T. (2010). *Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques*. United State Of America: Syngress.