

METODOLOGÍA PARA REALIZAR HACKING ÉTICO EN BASES DE DATOS
PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ

JORGE ALONSO FLOREZ ROJANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2017

METODOLOGÍA PARA REALIZAR HACKING ÉTICO EN BASES DE DATOS
PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ

JORGE ALONSO FLOREZ ROJANO

PROYECTO DE GRADO

Director

YINA ALEXANDRA GONZALEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ

2017

Nota de Aceptación:

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C. 30/11/2017

DEDICATORIA

El proyecto de grado lo dedico a mi esposa e hijos, quienes con su amor y apoyo me acompañan en todas las experiencias que adelanto. Sin ellos todo este esfuerzo no habría tenido significado

AGRADECIMIENTOS

A Dios por darme esta oportunidad luego de superar momentos difíciles y por permitirme alcanzar la meta, a mi familia, en especial a mis hermanos por su espera y paciencia, a compañeros de trabajo como Andrés Moncada y Eddi Romero quienes siempre brindaron el acompañamiento en la “última milla” y al Ing. Salomón García González por su guía y constante retroalimentación.

TABLA DE CONTENIDO

	Pag.
RESUMEN.....	10
INTRODUCCIÒN.....	12
1. TITULO	13
2. DEFINICIÒN DEL PROBLEMA.....	14
3. JUSTIFICACIÒN	16
4. OBJETIVOS	17
4.1 GENERAL.....	17
4.2 ESPECÍFICOS.....	17
5. MARCO REFERENCIAL.....	18
5.1 ANTECEDENTES.....	18
5.2 CONTEXTO.....	18
5.3 VICEPRESIDENCIA TECNOLOGÍAS INFORMACIÒN Y COMUNICACIONES	20
5.3.1 CARGOS Y FUNCIONES DE LA VICEPRESIDENCIA DE TIC	20
5.4 MARCO TEÓRICO	23
5.4.1 DESARROLLO DE LAS FASES DE IMPLEMENTACIÒN DEL HACKING ÉTICO.....	26
5.5 MARCO CONCEPTUAL.....	27

5.5.1 HACKER ÉTICO	27
5.5.2 METODOLOGÍA DE SEGURIDAD	27
5.5.3 HERRAMIENTAS DE TESTING A BASES DE DATOS	28
5.6 MARCO LEGAL	28
6. DISEÑO METODOLÓGICO	31
6.1 LÍNEA Y TIPO DE INVESTIGACIÓN	31
6.2 TIPO DE INVESTIGACIÓN	31
6.2.1 INVESTIGACIÓN EXPLORATORIA	31
6.2.2 INVESTIGACIÓN DESCRIPTIVA	31
6.3 AREA DE INVESTIGACIÓN	32
6.4 TECNICAS E INSTRUMENTOS DE RECOLECCION DE INFORMACIÓN ...	32
6.4.1 OBSERVACIÓN:.....	32
6.4.2 ENTREVISTA ESTRUCTURADA:.....	32
6.4.3 ENCUESTA:	33
6.5 POBLACIÓN Y MUESTRA	33
6.5.1 POBLACIÓN:.....	33
6.5.2 MUESTRA:	33
6.6 METODOLOGÍA DE DESARROLLO	33
6.6.1 DEFINICIÓN DE ACTIVIDADES	33
6.6.2. CONCATENACIÓN DE ACTIVIDADES	34

6.6.3. METODOLOGÍA DE ANÁLISIS DE SEGURIDAD	35
6.6.4. ESTIMACIÓN DE RECURSOS NECESARIOS PARA CADA ACTIVIDAD	35
6.6.5. ESTIMACIÓN DE LA DURACIÓN DE CADA ACTIVIDAD	36
6.6.6. GRUPOS DE PROCESOS Y ÁREAS DE CONOCIMIENTO:.....	36
7. ANALISIS SITUACIÓN ACTUAL DE LA CASA MATRIZ DE POSITIVA.....	38
7.1 FASE 1. DIAGNÓSTICO DE APLICATIVOS, SISTEMAS OPERATIVOS Y BASES DE DATOS.....	38
7.2 FASE 2. TIPOS DE PRUEBAS PARA VERIFICAR LA SEGURIDAD EN LA ORGANIZACIÓN	40
7.3 FASE 3. DEFINICIÓN DE LA METODOLOGÍA DE ANÁLISIS DE SEGURIDAD	42
7.4 FASE 4. ELABORACIÓN DEL INFORME EJECUTIVO	50
7.4.1 RECOMENDACIONES.....	56
8. METODOLOGIA DE DIAGNÓSTICO DE SEGURIDAD DE LAS BASES DE DATOS PARA POSITIVA COMPAÑÍA DE SEGUROS S.A.....	58
9. CONCLUSIONES.....	60
10. RESULTADOS.....	61
11. DIVULGACIÓN	63
BIBLIOGRAFÍA.....	64

TABLA DE ILUSTRACIONES

Pág.

Ilustración 1 Organigrama.....	19
Ilustración 2 Arquitectura TI	38
Ilustración 3 Objetivo estratégico TI.....	39
Ilustración 4 Metodología de Pruebas.....	43
Ilustración 5 Información Básica	45
Ilustración 6 Seleccionar Dispositivos Objetivo.....	45
Ilustración 7 Establecer opciones de escaneo	46
Ilustración 8 Registrar usuarios y permisos	46
Ilustración 9 Establecer parámetros por dispositivo	47
Ilustración 10 Programar ejecución del escaneo	47
Ilustración 11 Servidores por Severidad	48
Ilustración 12 Vulnerabilidades por clase.....	48
Ilustración 13 Resumen de vulnerabilidades por ocurrencia.....	49
Ilustración 14 Remediación.....	49
Ilustración 15 Gestión de Vulnerabilidades	51
Ilustración 16 Vulnerabilidades por componente	51
Ilustración 17 Gestión de vulnerabilidades AP	51
Ilustración 18 Gestión de vulnerabilidades Aplicaciones:	53
Ilustración 19 Gestión de vulnerabilidades Bases de Datos	53
Ilustración 20 Gestión de vulnerabilidades Server	55
Ilustración 21 Acceso a redes inalámbricas.....	61

RESUMEN

El Proyecto de grado corresponde al diseño de una metodología para la Casa Matriz de Positiva Compañía de Seguros S.A. que al final de las pruebas de Hacking ético a bases de datos le entrega el resultado con la lista detallada de las vulnerabilidades encontradas así como la lista de recomendaciones, que les permita entender los riesgos potenciales sobre su negocio, para que sean aplicadas por los responsables de seguridad en la organización.

Dicha metodología contempla las fases en que se debe abordar una tarea de Hacking ético a bases de datos en una organización, las pruebas de penetración que permitan la identificación de debilidades provocadas por una mala configuración de las aplicaciones, además de categorizar las debilidades con base al impacto potencial y la posibilidad que se convierta en realidad

La estructura del proyecto, está dada por secciones, la primera de ellas concierne al marco referencial el cual consta de marco de antecedentes, contextual, teórico, conceptual y legal que soportan la investigación a desarrollar; seguidamente se encuentra el aparte del diseño metodológico en el cual se describe los pasos a seguir a fin de recopilar información relevante, por ejemplo: línea y tipo de investigación, área de investigación, técnicas y herramientas de recolección de información.

La Metodología de desarrollo que por planteamiento relaciona, cuatro fases vitales, a saber:

Fase 1: Diagnostico de la situación actual teniendo en cuenta los aplicativos, sistemas operativos y motores de bases de datos en Casa Matriz, identificando los diferentes dispositivos pertenecientes a la infraestructura específica de la red informática.

Fase 2: Establecer los tipos de pruebas que se deben realizar con el objetivo de verificar la seguridad implantada en la organización

Fase 3: Definición de la Metodología de Análisis de seguridad contemplando aspectos como las tareas que se debe realizar al abordar un testeo de seguridad, la manera en la que los resultados de éste deben ser presentados, las normas éticas y legales que deben tenerse en cuenta al momento de concretar el test.

Fase 4: Elaboración del informe ejecutivo con la información del análisis de vulnerabilidad, pruebas de vulnerabilidad, Ethical Hacking realizado, con las conclusiones y recomendaciones

INTRODUCCIÓN

Como en todo sistema informático se deben tomar mecanismos y medidas de seguridad y de igual manera comprender los riesgos a los que se encuentra expuesta la información; las bases de datos son la primera elección para el almacenamiento estructurado de datos y es el primer objetivo de los atacantes

Un problema de seguridad común a todos los sistemas de cómputo es el de evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información o para efectuar cambios mal intencionados en una porción de la base de datos. El mecanismo de seguridad de un SGBD debe incluir formas de restringir el acceso al sistema como un todo

Para el desarrollo del proyecto se utilizan conceptos básicos de Ethical Hacking (técnica en la cual se realizan pruebas de penetración o de intrusión para detectar el nivel de seguridad interno y externo de los sistemas de información de una organización) determinando el grado de acceso que tendría un atacante con intenciones maliciosas a las bases de datos de los sistemas de información con información crítica.

Positiva Compañía de Seguros no es ajena al complejo panorama que representan los ataques informáticos, por tanto se ve en la necesidad de implementar una metodología que al final de las pruebas le entregue la lista detallada de las vulnerabilidades encontradas así como un documento con la lista de recomendaciones para que sean aplicadas por los responsables de seguridad en la organización, que le permita entender los riesgos potenciales sobre su negocio y fortalecer la confianza de sus grupos de interés

1. TITULO

METODOLOGÍA PARA REALIZAR HACKING ÉTICO EN BASES DE DATOS

2. DEFINICIÓN DEL PROBLEMA

El presente proyecto de investigación pretende establecer las fases en que se debe abordar una tarea de Hacking ético a bases de datos en una organización. Las pruebas de penetración permiten la identificación de debilidades provocadas por una mala configuración de las aplicaciones, además de categorizar las debilidades con base al impacto potencial y la posibilidad que se convierta en realidad

Las amenazas sobre los sistemas informáticos como la que representan usuarios que pueden usurpar la personalidad de usuarios autorizados para acceder y manipular indebidamente los datos de las empresas ha llevado que el tratamiento de los temas relacionados con la seguridad informática sea preponderante.

Positiva Compañía de Seguros S.A. es una Entidad de economía mixta, adscrita al Ministerio de Hacienda y Crédito Público. Cuenta con certificaciones otorgadas por ICONTEC (ISO 9001, ISO 14001, OSHAS 18001, NTC GP 1000) para la Gestión en el sector Público en Colombia, que han impactado positivamente en la imagen organizacional y han fortalecido la confianza a lo largo de la gestión pero que se han visto afectadas en el último año dada la falta de aplicación de un Hacking ético a bases de datos estructurado que le permita garantizar la confidencialidad, integridad y disponibilidad de los datos de sus clientes.

Los servicios de consultoría en Ethical Hacking consisten en realizar una evaluación en la seguridad de la infraestructura tecnológica a través pruebas de penetración interna y externa, buscando explotar las debilidades existentes, para obtener acceso a los sistemas, elevar privilegios de un usuario, todo de forma controlada sin afectación de ningún servicio de la compañía.

Dado lo anterior es necesario demostrar ¿Cómo el uso adecuado de una metodología para realizar Hacking Ético a sus bases de datos le proveerá a Positiva Compañía de Seguros S.A los mecanismos y lineamientos adecuados para proteger y garantizar la estabilidad, confiabilidad y seguridad de los datos?

3. JUSTIFICACIÓN

El proyecto que se pretende desarrollar es un proyecto de investigación donde se establecen las fases para realizar un Hacking ético a bases de datos para la Casa Matriz de Positiva Compañía de Seguros S.A. en la ciudad de Bogotá, teniendo en cuenta que al final de la prueba se le entrega un documento con la lista detallada de las vulnerabilidades encontradas así como una lista de recomendaciones para que sean aplicadas por los responsables de seguridad en la organización y para que puedan entender los riesgos potenciales sobre su negocio.

Durante la ejecución de la metodología propuesta se plantea la entrega de los siguientes criterios:

- Gestión de vulnerabilidades sobre la infraestructura de servidores y Aplicaciones objeto del servicio
- Cantidad ilimitada de escaneo de vulnerabilidades sobre la plataforma alcance del servicio.
- Ejecución de análisis bimensual de ethical hacking con su respectivo retest sobre los dispositivos que presenten un mayor factor de riesgo según las vulnerabilidades detectadas.
- Generación de informes gerenciales y técnicos de las pruebas de EH.
- Generación de informes mensuales del estado de la seguridad de la infraestructura analizada
- Seguimiento a la ejecución de las actividades de remediación definidas, para mitigar las vulnerabilidades detectadas
- Notificación oportuna a los administradores de las plataformas de las vulnerabilidades relevantes identificadas durante la ejecución de los escaneos programados.

El proceso de Hacking ético no contempla solucionar todas las vulnerabilidades descubiertas por lo tanto su compromiso será solucionar las vulnerabilidades de riesgo "Alto", dejando a consideración del cliente la opción de aceptar el riesgo en vez de mitigarlo, y que el cliente decida el tratamiento que dará sobre las de otros impacto (Medio, Bajo), acorde con los propósitos de su negocio

4. OBJETIVOS

4.1 GENERAL

Crear una metodología para realizar diagnósticos a bases de datos mediante técnicas de Ethical hacking.

4.2 ESPECÍFICOS

4.2.1 Levantar información de metodologías y procedimientos de Ethical hacking para bases de datos

4.2.2 Realizar la experimentación de pruebas de diagnóstico a las bases de datos para identificar y evaluar vulnerabilidades.

4.2.3 Diseñar la metodología de diagnóstico de seguridad de las bases de datos para la Casa Matriz de Positiva Compañía de Seguros S.A. en la ciudad de Bogotá.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Con el fin de enfocar la investigación sobre la implementación de un hacking ético en base de datos, fueron consultados los siguientes proyectos:

Artículo "Servicios de seguridad de la información - Servicio de HACKING ÉTICO" donde la empresa de consultoría IQ INFORMATION QUALITY presenta una propuesta de servicios para realizar pruebas de HACKING ÉTICO verificando los niveles de seguridad actuales y donde se utilizan metodologías de implementación como OSSTMM, OWASP e ISSAF que garantizan estándares de calidad para un correcto desarrollo del proyecto.

"Artículo La guía PMBOK" donde se desarrolla el tema Gestión del Alcance del Proyecto y se describen los procesos usados para gestionar el alcance del proyecto, así como las herramientas y técnicas asociadas que debe realizarse para entregar un producto o resultado con las características y funciones especificadas.

Artículo "Ethical hacking una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta kali-linux", donde se realizan pruebas de seguridad haciendo uso del Ethical Hacking como enfoque metodológico para determinar vulnerabilidades existentes en los sistemas operativos Windows y haciendo uso de herramientas del sistema operativo Kali Linux. Las pruebas de seguridad fueron realizadas en un entorno virtual controlado en la 1era Jornada Científico Estudiantil realizado dentro de las Instalaciones de la Universidad Técnica de Manabí

5.2 CONTEXTO

Positiva Compañía de Seguros S.A. es una Sociedad Anónima con Régimen de Empresa Industrial y Comercial del Estado, su organización, funcionamiento y en general el régimen jurídico de los actos, contratos, servidores y las relaciones con terceros es el previsto para las Empresas Industriales y Comerciales del Estado y

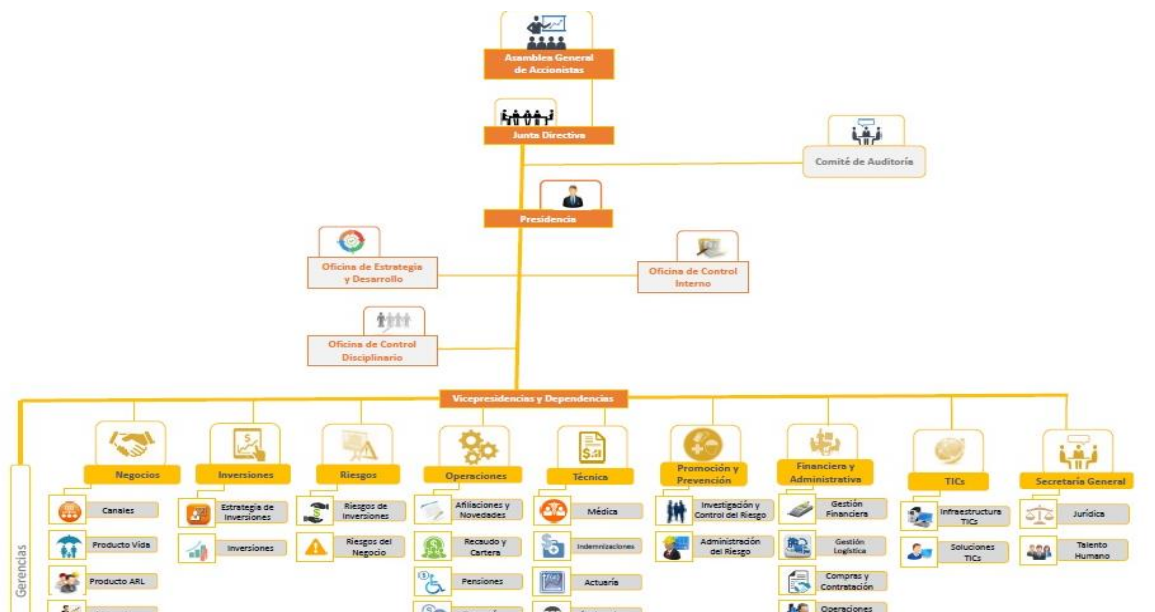
sus actividades de promoción, prevención y control de los factores de riesgo en las empresas a los cuales están expuestos sus trabajadores se desarrollan conforme a las reglas de derecho privado.

Los servicios ofertados por esta organización, están enmarcados en los ramos de ARL (Administradora de Riesgos Laborales), los ramos de Seguros de vida a saber:

- Accidentes personales
- Vida Grupo y Vida Individual
- Salud
- Exequias

Y los ramos de Seguros pensionales dentro de los cuales se cuenta con Rentas vitalicias y conmutación pensional

Ilustración 1 Organigrama



Fuente: Quiénes somos-estructura organizacional disponible en: www.positiva.gov.co

5.3 Vicepresidencia tecnologías información y comunicaciones

La vicepresidencia de TIC'S en Positiva Compañía de Seguros S.A, está conformada por la Gerencia de Infraestructura de TIC'S y la Gerencia de Soluciones TIC'S.

Esta vicepresidencia es responsable de elaborar, desarrollar y proponer la implementación de nuevas tecnologías y sistemas informáticos, planear actividades de mantenimiento preventivo y brindar soporte técnico a toda la compañía.

De acuerdo a la caracterización de cada proceso, la Vicepresidencia de TIC'S, tiene las siguientes funciones¹:

- Proponer y acompañar los Sistemas de Control Informáticos a ser implementados en las diferentes sucursales y regionales de la compañía.
- Gestionar la capacitación a los responsables operativos con el fin de garantizar la correcta implementación de los Sistemas Informáticos.
- Investigar, desarrollar e implantar tecnologías que soporten la operación de la entidad.
- Coordinar el análisis y desarrollo de los sistemas informáticos en conformidad con el plan estratégico 2015-2018.
- Impulsar el adecuado uso de los recursos informáticos al interior de la organización.
- Participar en los lineamientos generales y específicos para futuras adquisiciones de recursos informáticos.
- Velar y mantener en buen funcionamiento los recursos informáticos de la organización.

5.3.1 Cargos y Funciones de la Vicepresidencia de TIC

Positiva Compañía de Seguros cuenta con dos tipos de funcionarios, aquellos que son trabajadores oficiales (desde el cargo de profesional especializado grado 11

¹ POSITIVA COMPAÑÍA DE SEGUROS S.A. Caracterización Proceso Vicepresidencia TIC'S.: La entidad, 2012. 48 p.

hasta el asistente administrativo grado 2) y aquellos que son servidores públicos (desde el cargo de Vicepresidente hasta el Gerente Regional, sucursal y de área)².

El nivel directivo está encabezado por el:

- Vicepresidente Grado 8

Tiene como función principal el dirigir la formulación del plan estratégico de tecnologías de la información y comunicaciones de la compañía teniendo en cuenta las necesidades del negocio.

Igualmente debe coordinar el desarrollo de la arquitectura tecnológica de la compañía, de acuerdo a las mejores prácticas de tecnologías de la información y comunicaciones; también, le corresponde dirigir los procesos de investigación, implementación y evaluación de las diferentes tecnologías y servicios de la información, que requiera la compañía y finalmente debe garantizar el cumplimiento de normas, disposiciones, procedimientos y programas propios de la gestión de la vicepresidencia, para garantizar eficiencia y eficacia y oportunidad en las acciones institucionales, de acuerdo con los parámetros definidos.

- Gerente de área Grado 6

Por su parte, debe ser participe en la formulación del plan estratégico de tecnologías de la información y comunicaciones de la Compañía, igualmente es quien define y propone las especificaciones técnicas requeridas para la adquisición y contratación de bienes y servicios tecnológicos; a su vez, debe gestionar el seguimiento a los procesos a cargo de la Gerencia, obedeciendo a las metas e indicadores establecidos y es el encargado de preparar y presentar los informes que sean de su competencia y los requeridos por los entes de control con la oportunidad y periodicidad requerida.

- Profesional Especializado Grado 12 (Líder de proceso):

El líder de proceso es quien propone las estrategias de control y seguimiento para garantizar una adecuada evaluación a la gestión de la vicepresidencia y realiza las recomendaciones pertinentes. También es el encargado de formular proyectos de la Vicepresidencia y gestionar su registro en Casa Matriz, de acuerdo con los

² POSITIVA COMPAÑÍA DE SEGUROS. Manual de funciones para Empleados públicos y Trabajadores Oficiales. La entidad. 2011. 1092 p.

lineamientos establecidos, además, debe orientar a todas las dependencias de la compañía sobre los procedimientos y temas relativos a la misma.

- Profesional Especializado Grado 7

Este profesional es responsable de coordinar los servicios de recuperación de los elementos de tecnología informática y de implementar y manejar efectivamente las funciones y procedimientos de seguridad para cumplir con las necesidades de los propietarios de la Información.

Ejerce funciones como Oficial de Seguridad apoyando los procesos de Continuidad de Negocio.

- Técnico Administrativo Grado 3

Este es un cargo que realiza tareas como:

1. Llevar los registros documentales de los procesos de la Vicepresidencia de TIC`S de acuerdo a las políticas institucionales
2. Elaborar, mantener y realizar seguimiento a las bases de datos
3. Recopilar, clasificar y organizar información para la gestión de informes estadísticos
4. Apoyar la ejecución de las actividades para el desarrollo de los proceso de la Vicepresidencia.

- Asistente Administrativo Grado 2

Es el encargado de administrar el archivo y la correspondencia para facilitar la consulta de la documentación requerida, atiende a los usuarios internos y externos de la compañía dando la orientación e información propias de la dependencia; a su vez es quien efectúa las comunicaciones escritas y telefónicas obedeciendo las instrucciones demandas del superior inmediato o profesionales de la vicepresidencia.³

³ POSITIVA COMPAÑÍA DE SEGUROS. Manual de funciones para Empleados públicos y Trabajadores Oficiales. La entidad. 2011. 1093 p

5.4 MARCO TEÓRICO

Para hablar de hacking ético se hace necesario referirse a las herramientas de prevención y protección de datos. Lo que se pretende es estar adelante de quienes intentan agredir a una organización haciendo pruebas y ataques propios con la ayuda de expertos informáticos y con el uso de diferentes técnicas de ataque digital.

El hacking ético es la utilización de los conocimientos de seguridad en informática⁴ para realizar pruebas en sistemas, redes o dispositivos electrónicos, buscando vulnerabilidades que explotar, con el fin de reportarlas para tomar medidas sin poner en riesgo el sistema (Abraham, Security Solutions & Education (SSE), 2015, revista Enter)

Entendiendo el concepto de hacker ético como el de las personas que se encargan de penetrar la seguridad de las empresas para encontrar vulnerabilidades y así lograr prevenirlas. Por esta razón se realizan pruebas de penetración, buscando vulnerabilidades en el sistema, encontrar malas configuraciones y al final presentar un reporte para que se tomen medidas.

Para que este tipo de intervenciones surta efecto es necesario que haya conciencia empresarial de la importancia de la seguridad de la información, incorporando diferentes políticas de seguridad que permitan reducir el nivel de vulnerabilidad. Se puede decir entonces que lo que se busca en un proceso de hacking ético es tratar de encontrar vulnerabilidades y tomar las medidas necesarias antes de que suceda un incidente de seguridad

Los resultados de las vulnerabilidades encontradas tienen un manejo de total confidencialidad, los cuales son entregados y socializados con el personal de tecnología, oficial de seguridad, áreas de riesgos, o quienes defina la empresa contratante

Entendiendo el concepto Hardening como una estrategia defensiva⁵, que sirve para asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, que son innecesarios en el sistema, de igual manera se logra cerrando puertos que no se estén usando, removiendo servicios vulnerables e innecesarios, cerrando “huecos” de seguridad

⁴ Recuperado de: <http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html>

⁵ Recuperado de <http://www.ximark.com/EthicalHacking/HardeningdeSistemas.aspx>

y asegurando los controles de acceso, se incluye la evaluación de arquitectura de seguridad de una empresa y la auditoría de la configuración de sus sistemas con el fin de desarrollar e implementar procedimientos de consolidación para asegurar sus recursos críticos, estos procedimientos son personalizados para cada empresa

Una técnica de seguridad es el cifrado de datos, que sirven para proteger datos confidenciales que se transmiten por satélite o por algún otro tipo de red de comunicaciones. El cifrado puede proveer protección adicional a secciones confidenciales de una base de datos. Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado que tenga acceso a los datos codificados tendrá problemas para descifrarlos, pero un usuario autorizado contará con algoritmos (o claves) de codificación o descifrado para interpretarlos.⁶

No obstante que se cuente con bases de datos protegidas y con un Firewall encaminado a la seguridad de éstas y que se establezcan políticas de seguridad con las cuales se pueda controlar el acceso de usuarios a la información allí existente, el atacante ha logrado superar en muchos casos esta protección.

Para la realización de las pruebas se utilizan herramientas Open Source y licenciadas disponibles a cualquier persona que tenga acceso a internet. Las principales herramientas son:

- SQLMAP: Los administradores de red y webmaster tienen como prioridad proteger los datos alojados en una red o servidor. Algunas herramientas de pruebas de penetración le permiten automatizar el proceso de detectar errores como la inyección SQL como es SQLMAP, con la cual se minimiza el riesgo de intrusión y de acceso a información sensible para la compañía. Permite testear muchos motores de bases de datos para buscar vulnerabilidades y solucionar problemas, no para explotarlas maliciosamente. Soporta una gran variedad de motores de bases de datos como MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Sybase, SAP MaxDB y funciona sobre Sistemas Operativos Linux y en Sistema Operativo Windows.⁷

- IMPERVA: Monitoreo de Base de Datos y Auditoría (IMPERVA)

Actualmente los ataques contra aplicaciones web se han convertido en una de las amenazas más serias para las infraestructuras de seguridad al poner en peligro la información corporativa y los datos confidenciales de los

⁶ Recuperado de <http://eduteka.icesi.edu.co/gestorp/recUp/1275d0253997d62e90e9a7f6a5f107cc.pdf>

⁷ Recuperado de <http://sqlmap.org/>

clientes; si no se implantan medidas de seguridad a nivel de los flujos de transacciones HTTP, HTTPS y FTP, pueden llegar a convertirse en punto de entrada a las redes corporativas para robar información confidencial o atacar otros servidores internos.

Provee control sobre las bases de datos de negocio y las aplicaciones que las usan, para proteger contra robo de datos y vulnerabilidades, poner a salvo las aplicaciones y asegurar la confidencialidad de sus datos. Desde la consola SecureSphere se obtiene monitorización desde la base de datos hasta su uso aplicativo por usuarios⁸

- NMAP: Usado para pruebas de penetración con la cual los administradores de sistema pueden verificar la presencia de aplicaciones no autorizadas ejecutándose en el servidor; permite hacer el mantenimiento del inventario de computadores de una red. Se puede usar además para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte⁹
- SAINT: Herramienta de red integrada para el Administrador de Seguridad, A diferencia de las herramientas basadas en Windows, SAINT corre exclusivamente sobre sistemas operativos UNIX o SOLARIS y debe ser licenciada. Cuenta con una interfaz gráfica de usuario intuitiva y de fácil uso para explotar vulnerabilidades encontradas por el escaneo con la herramienta SAINT exploit¹⁰

La pérdida de información se presenta debido a esquemas poco eficientes de seguridad y al desconocimiento de políticas de seguridad que resguarden a los equipos informáticos de las actuales amenazas de hackers y procesos sin aseguramiento.

Un debido respaldo de la información y de los equipos donde se alojan es la mejor alternativa. Es importante conocer las vulnerabilidades que puedan presentar la base de datos y/o el servidor para poder proteger y garantizar la estabilidad, fiabilidad y seguridad de los datos presentes en esta.

Las pruebas de penetración se realizan para comprobar y clasificar vulnerabilidades, dejando al descubierto las vulnerabilidades que pudieran ser explotadas por personas no autorizadas, como: crackers, hackers, competidores,

⁸ Recuperado de <https://www.imperva.com/Products/WebApplicationFirewall-WAF>

⁹ Recuperado de <http://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/>

¹⁰ Recuperado de https://es.slideshare.net/gio_vani/scanners-29542462

etc. Están relacionadas con el tipo de información que cada organización maneja y de ahí se determina la estructura y las herramientas de seguridad requeridas.

La realización de las pruebas de penetración contempla las siguientes etapas:

- Recopilación de información
- Exploración de los sistemas
- Acceso no autorizado a información sensible o crítica
- Auditoría de las aplicaciones web
- Elaboración de informes

5.4.1 Desarrollo de las fases de implementación del Hacking Ético

- Fase de diagnóstico: Aquí se precisa la situación real de la entidad, identificando adecuadamente los sistemas informáticos que entrarán dentro del alcance del test.
- Fase de planificación de un Hacking Ético para la organización: Para esta etapa se determinan:

Grupos de trabajo

Establecer mesas de trabajo por cada aplicación misional involucrando los administradores de los equipos informáticos y los Líderes Técnicos que posean conocimiento de la organización y del proceso que gestionan.

Plan de trabajo

Se determina una metodología en la que se identifique claramente las actividades necesarias, el plazo pertinente para efectuar cada actividad, interrelación entre las mismas y finalmente se designa el personal o equipo para que lleve a cabo cada labor.

Asignación de responsabilidades

La especificación de los límites y compromisos permiten un adecuado monitoreo, por tanto es importante precisar que se espera de las personas que se asignen al proyecto.

Para el caso en particular se establece:

Tabla 1 Responsables del proyecto

Nombre Responsable	Papel y Función
Ing. Jorge Alonso Flórez Rojano	Ingeniero de Sistemas-Investigador del proyecto
Ing. Andrés Moncada	Oficial de Seguridad de TI - Monitoreo y evaluación del proyecto
Ing. Yina Alexandra González	Directora del proyecto

Fuente: El Autor

- Fase de implementación: Aquí debe reflejarse el cumplimiento de los objetivos previamente establecidos. Generalmente en esta fase se realiza un comparativo entre lo obtenido Vs lo planificado y así se establece las brechas existentes.
- Fase de evaluación y Monitoreo: El objetivo es evaluar los resultados obtenidos una vez fue implementado el Ethical Hacking.

5.5 MARCO CONCEPTUAL

5.5.1 Hacker Ético: Profesionales de la seguridad de la información que utilizan sus conocimientos de hacking con fines defensivos, cuya función es determinar lo que un intruso puede hacer sobre un sistema y la información, velando por su protección.

5.5.2 Metodología de Seguridad: ISSAF ¹¹(Information System Security Assessment Framework): En la traducción al español “Marco de Evaluación de Seguridad de Sistema de Información” es una metodología estructurada, detallada para realizar pruebas de penetración en diferentes dispositivos y escenarios

¹¹ Recuperado de https://www.linkedin.com/company/open-information-system-security-group?trk=company_logo

posibles dentro de la infraestructura tecnológica de una organización, esto con el propósito de evaluar la seguridad en los sistemas de información de la compañía.

5.5.3 Herramientas de Testing a Bases de Datos: Un problema de seguridad común a todos los sistemas de cómputo es el de evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información o para efectuar cambios mal intencionados en una porción de la base de datos. El mecanismo de seguridad de un SGBD debe incluir formas de restringir el acceso al sistema como un todo.¹²

5.6 MARCO LEGAL

La ley en Colombia en general es considerada una burla al pueblo y a la democracia, si los delitos son cometidos por personas del pueblo se aplica la mayor pena, pero si son realizados por gente de poder, la ley prácticamente no existe.

La legislación en materia informática presenta muchos vacíos y no hay integración de las diferentes partes que la componen como son la penal, comercial, administrativo, entre otros; se evidencian casos donde ciertos tipos de personas reciben el “castigo”, mientras que las personas detrás de toda la operación están libres continuando con su vida normal.

La legislación debe contemplar un castigo real, tanto para quien lo realiza como para quien lo induce o lo contrata, de igual forma. Es allí donde la legislación colombiana se debe plantear el comenzar por realizar un compendio de toda la normatividad, evitando los vacíos legales.

La problemática en Colombia es aún más grande, la incapacidad para tener presos (falta de cárceles), la existencia de un sistema penitenciario débil (formación, sueldos, educación, etc.) y la normatividad permisible, hacen que la aplicación de la ley sea muy difícil

Los delitos informáticos nacieron con la creación del computador y cada día son más frecuentes y destructivos; los daños causados se pueden medir en todos los aspectos, desde el psicológico hasta el monetario, en algunos casos hasta conducen al suicidio; pero lo más grave es que pueden ser realizados por

¹² Recuperado de <http://virtual.usalesiana.edu.bo/web/conte/archivos/2397.pdf>

personas de cualquier edad, y desde cualquier parte del mundo; a continuación, se presenta un cuadro con algunos de estos delitos que están causando estragos en el mundo entero

Tabla 2 Descripción de los delitos

#	DELITO	DESCRIPCIÓN
1	Hurto	Mediante dispositivos o software ingresan aun sistemas para extraer información de éste.
2	Sabotaje informático	Dañar o destruir o modificar información de carácter electrónico (virus, gusanos, bombas lógicas, bombas cronológicas)
3	Suplantación de identidad	Suplantación de personas, en redes sociales, páginas, correos electrónicos
4	Piratería	Libros, películas, canciones y otros son víctimas de esta modalidad.
5	Pornografía infantil	Actos de pornografía con menores de edad
6	Secuestro de información	Conocido como Ramsomware, secuestrar la información de los usuarios para pedir una cifra de dinero a cambio de una clave que permita liberar la información.
7	Espionaje	Robo de información a nivel industrial o país en el cual se sustraen datos de carácter vital.
8	Xenofobia	Acciones de rechazo hacia un grupo en particular a través de páginas, redes sociales u otros.
9	Fraude	Acciones de carácter engañoso por medios electrónicos destinadas a obtener un beneficio económico a expensas de la víctima por medio de la introducción, alteración, borrado, supresión de datos informáticos
10	Falsificación o Phising	Introducción, alteración, borrado o supresión de datos informáticos originando otros datos no auténticos, para ser utilizados como si fuesen auténticos,

Fuente: El autor

La ley 1273 ¹³de enero de 2009, en su primer capítulo, tipifica los delitos informáticos en Colombia contemplando penas a quienes cometan infracciones

¹³ DELTA. (2014). Ley de delitos informáticos en Colombia. (en línea). (2 de Septiembre de 2015). Disponible en: <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>

como romper la seguridad, acceso a datos o programas informáticos y/o mantenerse dentro contra la voluntad del legítimo propietario. La norma dicta medidas penales de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que las organizaciones estén preparadas legalmente para enfrentar los retos que plantea.

Entre los principales principios orientadores de la ley 1273 y que sirven de soporte para el uso e implementación del Hacking Ético se encuentran: Acceso abusivo a un sistema informático. El que sin autorización o por fuera de lo acordado, acceda en todo o en aparte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de 48 a 96 meses, y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2009)

Desde el punto de vista empresarial, las empresas aprovecharon la expedición de esta ley para realizar acuerdos de confidencialidad, crear puestos de trabajo que velan por la seguridad de los datos, lo que dio origen al llamado “Hacking ético” con lo cual se obtuvo una herramienta importante para denunciar los hechos delictivos a los que se puede ver afectada

La cifra de delitos informáticos en el país va en aumento. Tanto que Colombia es, actualmente, el tercer país en Latinoamérica donde más se cometen. Se calcula que 187 denuncias mensuales son interpuestas por fraude a diferentes bancos. Por ejemplo, en Cali la Unidad de Delitos Informáticos del CTI registra 4939 denuncias por estafas electrónicas y otros delitos relacionados; 823 al mes; 205 semanales; 27 cada día. Es el promedio. Un investigador del CTI asegura que, comparando las cifras del año anterior el 2014, en Cali y el resto del Valle del Cauca los delitos informáticos se han incrementado en un 100%. En Palmira, por ejemplo, se cuentan 249 denuncias en este 2015; en El Cerrito, 18; en Yumbo, 14. Pocos se salva, Lo que demuestra que los computadores cada vez son elementos que están siendo usados con más frecuencia para delinquir ¹⁴

¹⁴ E. Tiempo, «El Tiempo,» 2015. [En línea]. Available: <http://www.eltiempo.com/politica/justicia/estafas-en-las-que-usted-puede-caer/15593158> . [Último acceso: 2017].

6. DISEÑO METODOLÓGICO

6.1 LÍNEA Y TIPO DE INVESTIGACIÓN

La metodología de desarrollo del presente proyecto de grado, se basa en los planteamientos definidos en materia de Seguridad de la Información y Diagnósticos a bases de datos mediante técnicas de Ethical hacking.

La línea de investigación es del alcance profesional para la adquisición de nuevos conocimientos, hacia la resolución de un problema que responde a una demanda específica, donde se crea un proceso (Metodología) con una nueva forma de organizar el conocimiento alrededor de la solución de un problema planteado en el medio laboral y con incidencia en la formación profesional.

Principalmente se busca; realizar una metodología para hacer diagnósticos a bases de datos mediante técnicas de Ethical hacking con el fin de encontrar vulnerabilidades y tomar las medidas necesarias antes de que suceda un incidente de seguridad en los sistemas de información de las organizaciones.

6.2 TIPO DE INVESTIGACIÓN

6.2.1 Investigación Exploratoria: A través de la entrevista y observación se pretende levantar datos que permitan el diagnóstico inicial sobre la identificación de debilidades provocadas por una mala configuración de las aplicaciones y categorizar estas debilidades con base al impacto potencial y la posibilidad que se convierta en realidad. Relacionado con lo anterior, es importante conocer el grado de conciencia empresarial de la seguridad de la información para reducir el nivel de vulnerabilidad por la compañía.

6.2.2 Investigación Descriptiva: Este tipo de investigación permite la delimitación de los hechos que conforman el problema de investigación, como lo son:

- Establecer la Metodología de Análisis de Seguridad, para determinar aspectos como la forma en que el test debe ser desarrollado, la manera en

la que los resultados de éste deben ser presentados, los tiempos probables para cada una de las tareas.

- Identificar características técnicas de los equipos y aplicaciones de cómputo que se encuentran en el universo de investigación (sistemas operativos, motores de bases de datos, lenguajes de programación, etc.)
- Descubrir y comprobar la posible asociación de las variables de investigación

6.3 AREA DE INVESTIGACIÓN

La presente propuesta se enmarca dentro del área de conocimiento: Gestión de la Seguridad Informática, específicamente en, Sistema de Gestión de Seguridad de la Información "SGSI" basado en el estándar ISO/IEC 27001:2013 y de metodologías existente tales como OWASP e ISSAF.

6.4 TECNICAS E INSTRUMENTOS DE RECOLECCION DE INFORMACIÓN

Para este proyecto se hará uso de todas las fuentes bibliográficas posibles relacionadas con el Diseño e Implementación de una Metodología para realizar diagnósticos a bases de datos mediante técnicas de Ethical hacking, esto con el fin de establecer antecedentes que sustenten la investigación.

Las técnicas de recolección de datos elegidas para el desarrollo de esta investigación son: La observación, encuesta y entrevista.

6.4.1 Observación: Esta técnica permite entrar en contacto directo con los profesionales de informática encargados de la administración de las bases de datos y una investigación continua de los eventos de seguridad sucedidos en el sistema

6.4.2 Entrevista Estructurada: Mediante preguntas precisas es posible socializar la temática de investigación y conocer el punto de vista de las diferentes partes involucradas, además, permite registrar de forma estandarizada datos sobre seguridad informática y mecanismos de control implementados por la organización

6.4.3 Encuesta: Debido a su estructura con preguntas de múltiples opciones referentes a la seguridad informática es posible la identificación de debilidades en los sistemas de información provocadas por una mala configuración de las aplicaciones y el grado de acceso que tendría un atacante con intenciones maliciosas a las bases de datos de los sistemas de información con información crítica y también saber el grado de conocimiento de las mismas respecto a la temática tratada en esta investigación

Los instrumentos seleccionados para este proyecto son: Lista de cotejo, cuestionario y guía de entrevista.

6.5 POBLACIÓN Y MUESTRA

6.5.1 Población: El presente proyecto se realizará en la Casa Matriz de Positiva Compañía de Seguros ubicada en la ciudad de Bogotá, pues es aquí en donde se toman las decisiones y se realizan todas las actividades administrativas para el funcionamiento de la entidad

6.5.2 Muestra: Se estima que para el estudio en referencia, se involucrara cerca de 15 personas, profesionales del área de soluciones e infraestructura que actúan como administradores de los sistemas informáticos (bases de datos, equipos de cómputo, red local) y como Líderes Técnicos de los sistemas de información

6.6 METODOLOGÍA DE DESARROLLO

Con el fin de desarrollar satisfactoriamente la presente propuesta se ha contemplado adelantar las siguientes acciones: ¹⁵

6.6.1 Definición de actividades

¹⁵ Etapas del plan de gestión del tiempo en un proyecto Disponible en: <http://www.obs-edu.com/es/blog-project-management/planificacion-de-las-actividades-y-tiempo-de-un-proyecto/etapas-del-plan-de-gestion-del-tiempo-en-un-proyecto>

Identificar y documentar las acciones concretas que será necesario realizar para producir los entregables del proyecto. De este proceso se extraerán una lista de actividades, otra de hitos y un resumen que recoja las características y atributos de cada una de las actividades.

- Recopilación de información
- Descripción de la red
- Exploración de los sistemas
- Extracción de información
- Acceso no autorizado a información sensible o crítica
- Auditoría de las aplicaciones web
- Elaboración de informes
- Informe final

6.6.2. Concatenación de actividades

Establecer la secuencia lógica de trabajo que garantice la mayor eficiencia, teniendo en cuenta los diferentes dispositivos pertenecientes a la infraestructura específica del proyecto, con el objetivo de realizar pruebas de cumplimiento y verificaciones de la seguridad implantada en la organización

Se establecen los tipos de pruebas que se deben realizar según la siguiente lista:

16

- Pruebas de Ingeniería Social
- Pruebas de Análisis de Vulnerabilidades
- Pruebas de Intrusión (PenTest)
- Pruebas de Negación del Servicio
- Pruebas a Plataformas de Pagos

6.6.3. Metodología de Análisis de seguridad

Se determina a partir de las siguientes referencias metodológicas, cada una con su nivel de madurez propio: ¹⁷

- Open Source Security Testing Methodology Manual (OSSTMM): No solo abarca los ámbitos técnicos y de operación de seguridad tradicionales, sino que también se encarga de definir aspectos tales como las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado, la manera en la que los resultados de éste deben ser presentados, las normas éticas y legales que deben tenerse en cuenta al momento de concretar el test, los tiempos probables para cada una de las tareas¹⁸
- Information System Security Assessment Framework (ISSAF): Constituye un marco de trabajo detallado respecto de las prácticas y conceptos relacionados las tareas que se debe realizar al abordar un testeo de seguridad.¹⁹
- Open Web Application Security Project (OWASP): Centrado en la seguridad sobre aplicaciones web y cuya misión es hacer visible y consciente la seguridad en aplicaciones, de manera que las organizaciones puedan tomar mejores decisiones sobre sus riesgos de seguridad²⁰

6.6.4. Estimación de recursos necesarios para cada actividad

Hacer una aproximación del tipo y cantidad de recursos necesarios para llevar a cabo cada actividad.

De acuerdo a la cantidad y ubicación de los recursos informáticos de la organización se determinan las pruebas a realizar a:

- Sistema operativo
- Aplicaciones
- Errores en configuraciones

¹⁷ Hacking desde cero Disponible en <http://www.freelibros.org/manual/hacking-desde-cero-users.html>

¹⁸ Ethical hacking: Test de intrusion. Principales metodologías Disponible en <http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias2.shtml>

¹⁹ Seguridad Informática Disponible en <http://insecuredata.blogspot.com.co/2009/04/metodologia-de-test-de-intrusion-issaf.html>

²⁰ OWASP Disponible en https://www.owasp.org/index.php/Main_Page

- Errores en protocolos
- Evaluación de seguridad

6.6.5. Estimación de la duración de cada actividad

Se determina la cantidad de tiempo que cada actividad requiere para completarse.

6.6.6. Grupos de procesos y áreas de conocimiento:

- Inicio: En el grupo de procesos de inicio se establece los objetivos y expectativas del proyecto, así mismo el nombramiento de los Gerentes a cargo del proyecto.
- Planeación: Su objetivo es ejecutar las actividades necesarias para establecer el alcance total del esfuerzo, definir los objetivos y desarrollar la línea base de acción requerida para alcanzar dichos objetivos. Adicionalmente, realizar la definición y desarrollo del lanzamiento del proyecto ante los interesados del proyecto.
- Programación: En esta etapa el equipo de trabajo debe definir el plan detallado del proyecto donde se incluye las siguientes áreas:
 - Gestión de Integración del proyecto
 - Gestión del alcance
 - Gestión del tiempo
 - Gestión del costo
 - Gestión de la calidad del proyecto
 - Gestión de recursos humanos
 - Gestión de las comunicaciones
 - Gestión del riesgo
 - Gestión de las adquisiciones
 - Gestión de Interesados
- Ejecución: Su objetivo es ejecutar las actividades definidas en la etapa de planeación con el fin de cumplir con las especificaciones del proyecto, además de asegurar la calidad y veracidad de los entregables especificados.
- Seguimiento y Control: Evalúa el proyecto desde el inicio hasta el cierre, con el fin de identificar las posibles variaciones y tomar las acciones preventivas y correctivas necesarias para garantizar el cumplimiento de los objetivos propuestos.

- Cierre: Su objetivo es formalizar el cierre del proyecto; asegurando que los entregables satisfagan los requerimientos del proyecto

7. ANALISIS SITUACIÓN ACTUAL DE LA CASA MATRIZ DE POSITIVA

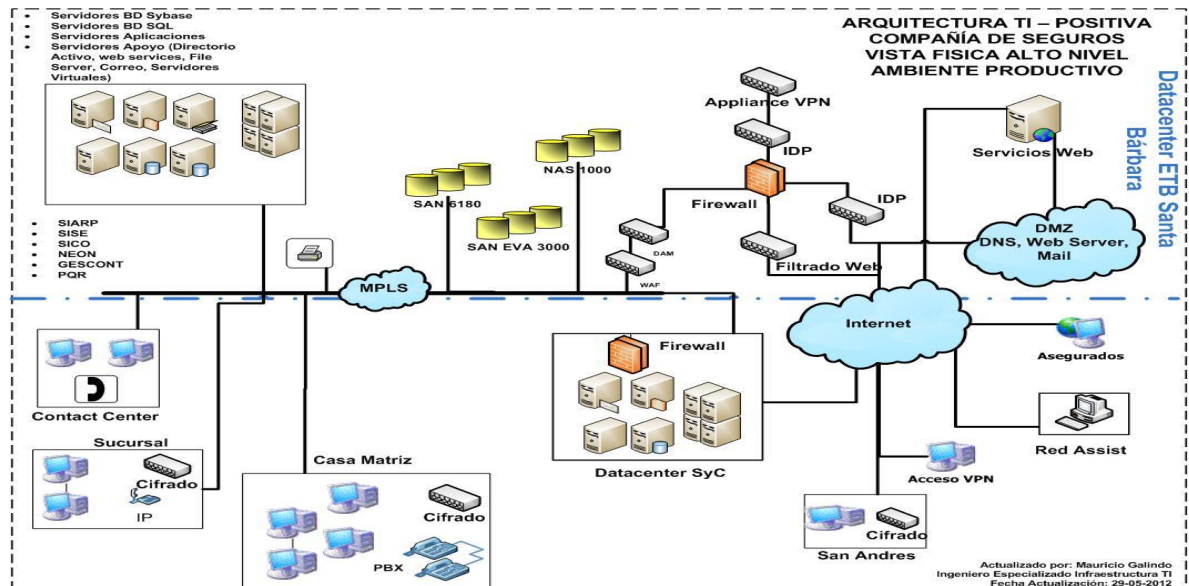
7.1 Fase 1. Diagnóstico de aplicativos, sistemas operativos y bases de datos

El concepto de seguridad informática, aquí tomado, es el de asegurar o blindar los datos de los clientes de Positiva SA, junto con sus movimientos realizados en la compañía. Garantizar que no van a ser tomados para hacer daño, es una de los objetivos que se pretende llegar.

Corresponde a la Vicepresidencia de TIC de Positiva Compañía de Seguros asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, además de proteger los recursos y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales.

El siguiente diagrama muestra la Arquitectura de TI en Positiva Compañía de Seguros:

Ilustración 2 Arquitectura TI



Fuente: El autor

El siguiente diagrama muestra el Objetivo Estratégico de la Tecnología Informática dentro de la organización de Positiva

Ilustración 3 Objetivo estratégico TI



Fuente: El autor

Los sistemas de información de Positiva Compañía de Seguros - Casa Matriz, son aquellos sistemas operativos, de infraestructura, aplicaciones de negocio y servicios de aplicación protegidos mediante la introducción de seguridad en todo el ciclo de vida del desarrollo, es decir que son definidos los controles en cada uno de los entornos y tecnologías empleadas. Antes del paso a producción, se desarrollan pruebas de seguridad de aplicación

Seguridad en las comunicaciones y red: De acuerdo a la interacción entre ambientes virtuales o físicos de las aplicaciones/componentes, estos son cifrados según la sensibilidad de la información transmitida.

En tanto a la red, está configurada de acuerdo a los requerimientos y necesidades de la entidad, esta es monitoreada para garantizar su disponibilidad, rendimiento y la gestión de incidentes oportunamente.

A continuación se describen los requisitos de seguridad:

- ✓ Las sesiones inactivas se cierran después de un periodo determinado de inactividad en los servidores.
- ✓ La red de Positiva Compañía de Seguros S.A. esta segmentada y protegida con dispositivos adicionales.

- ✓ Disposición de un entorno de Desarrollo, Pruebas y Producción en la Arquitectura de red.
- ✓ Los sistemas de información que provean servicios a los usuarios están ubicados en redes específicas de servidores, separadas de las redes de usuarios.
- ✓ Los sistemas y dispositivos de comunicaciones conectados a la red están correctamente bastionados

7.2 Fase 2. Tipos de pruebas para verificar la seguridad en la organización

Toda instalación inicial de sistema operacional se realiza dejando una instalación por defecto, esto significa que las consideraciones especiales sobre servicios, privilegios de acceso a directorios, etc., se dejan para una labor posterior del administrador del sistema. Sin embargo, en muy pocas ocasiones el administrador encontrará el tiempo requerido para realizar esta labor. Como consecuencia se pueden encontrar servicios no requeridos que están habilitados en cada servidor y esto termina produciendo brechas de seguridad que deberán ser cerrados

Existen varios niveles de seguridad posibles de aplicar sobre los sistemas Solaris, por lo cual es necesario personalizar el servicio con base en los requerimientos propios del área funcional; es necesario acercar al máximo el diseño final de seguridad a aplicar dentro del proceso de hardening, mediante el bloqueo de servicios específicos.

Se implementara un proceso de revisión y definición de servicios y privilegios de acceso en los servidores que se encuentran sobre plataformas Solaris y Windows.

Se establece la siguiente Escala de Valoración para identificar el grado de criticidad de la vulnerabilidad encontrada:

Tabla 3 Escala de valoración

1 – No Significativa	Los intrusos pueden recopilar información acerca del host (puertos abiertos, servicios, etc.) y pueden ser capaces de utilizar esta información para encontrar otras vulnerabilidades
2 - Baja	Los intrusos pueden ser capaces de obtener información sensible desde el host, cómo la versión exacta del software instalado. Con esta información, los intrusos pueden explorar vulnerabilidades

	conocidas específicas a las versiones del software
3 – Media	Los intrusos pueden ser capaces de acceder a la información específica almacenada en el servidor. Incluyendo la configuración de seguridad. Por ejemplo, las vulnerabilidades en este nivel pueden incluir la divulgación parcial de los contenidos del archivo, el acceso a ciertos archivos en el host, el examen de directorios la divulgación de las reglas del filtrado y mecanismo de seguridad, ataques de denegación de servicios y el uso no autorizado de los servicios, tales como correo de retransmisión
4 - Alta	Los intrusos posiblemente pueden obtener el control de la máquina, o puede existir la posibilidad de fugas de información altamente sensible. Por ejemplo, las vulnerabilidades en este nivel pueden incluir el acceso completo a los archivos, puertas traseras potenciales o un listado de todos los usuarios
5 – Crítica	Los intrusos pueden fácilmente obtener el control de la máquina, lo que puede llevar al compromiso de la seguridad de su red. Por ejemplo, las vulnerabilidades en este nivel pueden incluir lectura completa y escritura a los archivos, la ejecución remota de comandos y la presencia de puertas traseras. Ante la explotación de estas vulnerabilidades se pierde totalmente la confidencialidad, disponibilidad e integridad de la información

Fuente: El autor

Se determina realizar una (1) prueba de vulnerabilidades, cada prueba debe incluir un RETEST, con explotación controlada de las vulnerabilidades críticas, y deberá generar un (1) informe técnico y un (1) informe ejecutivo por cada prueba que detalle los hallazgos por tipo de dispositivo de la plataforma de TI; igualmente deberá determinar el riesgo asociado a cada vulnerabilidad usando para ello las mejores prácticas existentes en el mercado.

Las pruebas de vulnerabilidad se realizarán a los siguientes equipos:

- Servidores Datacenter Principal
- Equipos activos de red
- Appliance Juniper
- Aplicaciones web internas
- Portal en internet
- Bases de datos.

Las pruebas de penetración y explotación controlada de vulnerabilidades se harán a los componentes de la infraestructura de TI que resulten afectados con vulnerabilidades críticas o grado alto de vulnerabilidad.

Las pruebas de penetración internas serán del tipo caja blanca²¹ para los servidores, equipos de comunicaciones, aplicaciones, Servicios de Bases de Datos y los equipos PCs mencionados; y pruebas externas tipo caja gris para servidores expuestos en internet.

Para la realización de las pruebas se tomarán las direcciones IP y las URL entregadas y se realizará un escaneo para encontrar sus posibles vulnerabilidades basado en los servicios activos

En esta etapa se obtiene la mayor cantidad de información posible del objetivo: Que la IP fuera válida, host vivos, ruteo hasta el objetivo, información de DNS, información gathering, entre otras.

Para la realización de las pruebas se utilizarán herramientas Open Source y licenciadas disponibles a cualquier persona que tenga acceso a internet.

Las principales herramientas son:

- ✓ Acunetix Web Scanner
- ✓ Herramientas Libres contenidas en Kali Linux V. 1.08
- ✓ Nessus 5.0
- ✓ NMAP
- ✓ Herramientas básicas como ping, telnet y compiladores de C++ para la construcción de exploits.

7.3 Fase 3. Definición de la Metodología de Análisis de Seguridad

Para garantizar la seguridad informática se requiere de un método y el uso de herramientas destinadas a proteger la información; uno de esos servicios lo constituye el Ethical hacking, disciplina que se basa en el hecho de que para estar protegido se debe conocer cómo operan y qué herramientas usan los hackers. Un proceso de hacking ético contempla lo que se conoce como pruebas de

²¹ Hace referencia a que la organización expone de forma abierta la arquitectura tecnológica al analista e indica explícitamente los nombres y direcciones de los sistemas a evaluar

penetración, PEN-TEST, para la comprobación y clasificación de las vulnerabilidades (fallas de seguridad o riesgo para una organización).

Luego de analizar las necesidades de Positiva Compañía de Seguros se decide realizar el Test de intrusión sin objetivo, es decir, examinar la totalidad de los componentes en los sistemas informáticos presentes en la empresa, teniendo en cuenta que posee infraestructura de red propia con servicios accesibles desde el exterior (Aplicaciones en tres capas, aloja su propia página web y permite el acceso remoto a sus trabajadores por VPN).

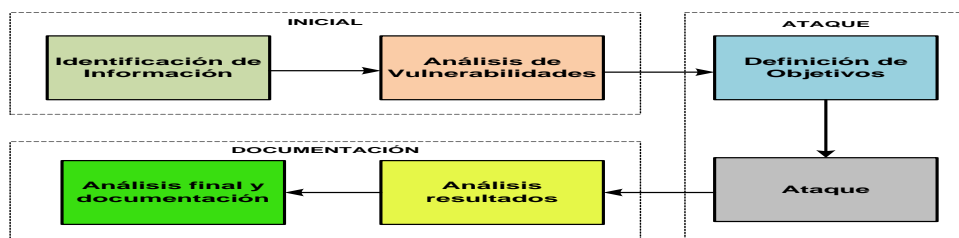
Las actividades realizadas se enmarcan dentro de la metodología para realización de pruebas de intrusión que incluye fases relacionadas en estándares libres como lo es OWASP, OSSTMM, ISSAF y comerciales como EC-Council.

Se lleva a cabo la reunión de Planeación Preliminar, donde se decide con el Oficial de Seguridad de TI los sistemas informáticos que entrarán dentro del alcance del test y se establece la siguiente lista de actividades:

1. Actividades Preliminares
- 2 Reunión de Planeación preliminar
- 3 Plan de Proyecto
- 4 Verificación preliminar de Equipos y Servicios
- 5 Reinicio de Servidores
- 6 Modificación de Script Principal de Hardening
7. Pruebas de Funcionalidad
- 8 Pruebas de Seguridad
9. Pruebas de Funcionalidad a largo plazo
10. Documentación Final del Proyecto

La siguiente figura muestra el Esquema de metodología de Pruebas de Intrusión acordado en la Planeación del proyecto

Ilustración 4 Metodología de Pruebas



Fuente: El autor

Al final de este ejercicio se entrega a la Vicepresidencia de TIC de Positiva esta metodología que le permitirá apoyar la prevención de incidentes de Seguridad de la Información a través de pruebas de vulnerabilidades, pruebas de intrusión (hacking ético) y aseguramiento de los sistemas de información y servicios tecnológicos con una periodicidad recomendada de mínimo cada 6 meses

Ejecución del escaneo

Se establece con el Oficial de Seguridad de POSITIVA realizar la prueba de escaneo con explotación local, es decir, se ejercen funciones como atacante, con acceso previo a los servidores residentes en su Casa Matriz, En este caso, la máquina asignada se utiliza como plataforma de lanzamiento para conectarse a otros objetivos vulnerables

Se establece que la herramienta integrada de pruebas de penetración - SAINT – será la elegida para realizar los escaneos principalmente por que los procesos CORE de Positiva están implementados con Bases de Datos presentadas en Servidores con Sistema Operativo SOLARIS, característica principal de SAINT que analiza cada sistema de una red para los servicios TCP y UDP, detectando lo que podría permitir a un atacante obtener acceso no autorizado, crear una denegación de servicio u obtener información confidencial sobre la red.

La herramienta SAINT utilizada permite identificar vulnerabilidades entre sistemas operativos, dispositivos de red, aplicaciones Web, bases de datos.

Se realiza este escaneo en cuatro etapas:

- Verifica en línea los servicios TCP y UDP de la red
- Analiza el tráfico para identificar intentos de acceso no autorizado, denegación de servicio u obtener información confidencial sobre la red de un atacante no identificado
- Comprueba las vulnerabilidades, categorizándolas de varias maneras, de acuerdo a estándares internacionales, según la gravedad o el tipo
- Describe la forma de corregir las vulnerabilidades, suministrando a veces los enlaces a nuevas versiones de software que eliminarán las vulnerabilidades detectadas.

La siguiente secuencia de ilustraciones muestra la forma como se configura la herramienta SAINT para realizar el escaneo de los diferentes componentes de las

Bases de Datos en la organización, ya sea para los Servidores de Bases de Datos (con sistemas operativos tales como Solaris, Unix), capa de comunicaciones (a nivel de firewall, inalámbricos) y de servidores de aplicaciones (Servidores Windows, Tomcat, LDAP)

- Se crea una actividad (job) y se asocia a un grupo de componentes (con características similares) donde se guarda la configuración y los binarios de las bases de datos.

Ilustración 5 Información Básica

Edit Job

1 Scan Info
Basic Setup

2 Targets
Select scan targets.

3 Scan Policy
Select a scan policy.

4 Authentication
Select credentials.

5 Advanced
Additional Options

6 Finish
Create schedules and select ticket rule set.

Step 1: Basic Information

Name & Description

Please enter a unique name for this job.
Solaris 2

Please enter a detailed description for this job. (Optional)
nuevo escaneo de vulnerabilidad de Solaris

Target Groups

A target group is a collection of pre-configured scan targets. Associating this job with a target group will import the targets for that group. You will still be able to select a scan policy and reporting options.

Please select a target group to associate with this job. (Optional)
Servidores Solaria or Create a new Target Group

Remove All

Fuente: El autor

- Se selecciona cada una de las direcciones IP de los servidores de las bases de datos.

Ilustración 6 Seleccionar Dispositivos Objetivo

1 Scan Info
Basic Setup

2 Targets
Select scan targets.

3 Scan Policy
Select a scan policy.

4 Authentication
Select credentials.

5 Advanced
Additional Options

6 Finish
Create schedules and select ticket rule set.

Step 2: Select Scan Targets

Enter Scan Targets

Local Node

Enter target(s) ?

More Options...

Node Information
Description: SAINT Built-In Scanner
Status: Active

Selected Target(s)

Remove All

Enter Target Restrictions

Enter target(s) ?

Target Restrictions(s)

Fuente: El autor

- Se establecen las políticas del escaneo y el grado de profundización que se va a realizar.

Ilustración 7 Establecer opciones de escaneo

1 Scan Info
Basic Setup

2 Targets
Select scan targets.

3 Scan Policy
Select a scan policy.

4 Authentication
Select credentials.

5 Advanced
Additional Options

6 Finish
Create schedules and select ticket rule set.

Step 3: Scan Options

Select a Scan Policy

Select Policy Category: Vulnerability

Select Policy: Heavy/Vulnerability Sca

The **Heavy/Vulnerability Scan** runs all available vulnerability checks against the selected targets.

Scan Policy Options

Exhaustive Scan ?

Allow Dangerous Tests ?

Fuente: El autor

- Se registran los usuarios y contraseñas, que previamente se acordaron con el oficial de seguridad, que poseen los privilegios (permisos) para analizar los directorios, objetos y diferentes componentes en el servidor (acorde al sistema operativo, el motor de base de datos y la capa de aplicaciones)

Ilustración 8 Registrar usuarios y permisos

1 Scan Info
Basic Setup

2 Targets
Select scan targets.

3 Scan Policy
Select a scan policy.

4 Authentication
Select credentials.

5 Advanced
Additional Options

6 Finish
Create schedules and select ticket rule set.

Step 4: Authentication and Credentials

Default Credentials

Enter default credentials for this scan. These credentials will be used on each host to attempt authenticated scans against certain services.

Microsoft Windows Domain (Admin):	+ Set	×	Oracle Server:	+ Set	×
Windows Domain (non-admin):	+ Set	×	Microsoft SQL Server:	+ Set	×
Unix, Linux, MacOS, etc.:	+ Set	×	MySQL Server:	+ Set	×
HTTP Basic:	+ Set	×	SNMP Version 3:	+ Set	×
Amazon Web Services (AWS):	+ Set	×	Web Application:	+ Set	×
Microsoft Azure:	+ Set	×			

Credentials Manager

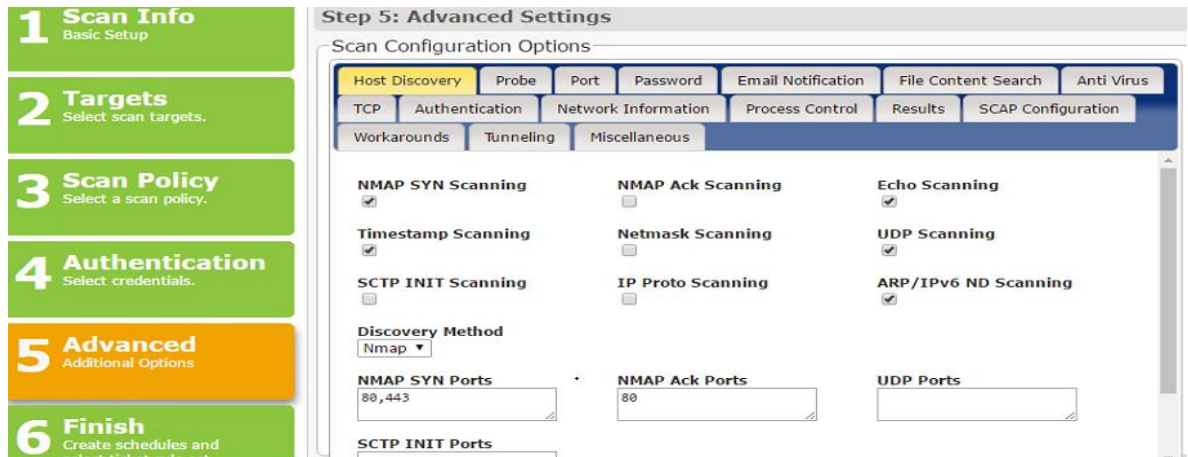
The credentials manager allows you to securely store credentials on a per-host basis. By default, these credentials will be used in place of any default credentials entered above when appropriate.

Use stored credentials if available

Fuente: El autor

- Se establecen las opciones avanzadas de configuración, parametrizando la herramienta con los diferentes utilitarios como NMAP que permiten identificar la presencia de aplicaciones no autorizadas ejecutándose en el servidor o la presencia de nuevos servidores que se conecten; se registran los puertos utilizados por las bases de datos (80, 443, etc)

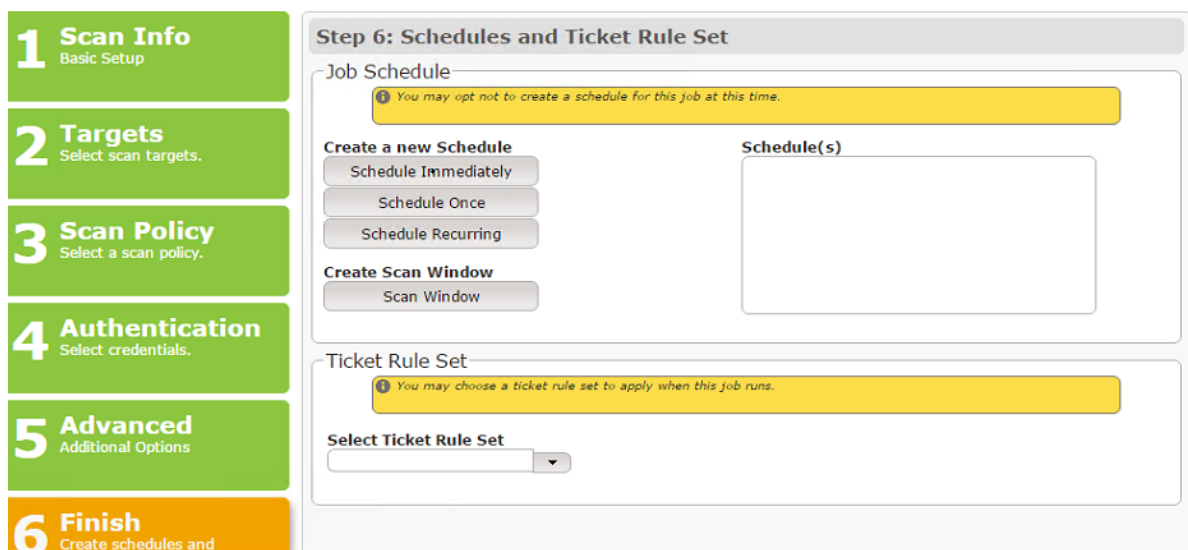
Ilustración 9 Establecer parámetros por dispositivo



Fuente: El autor

- Se programa la ejecución del trabajo (job) y se establecen unas reglas de notificación durante su ejecución

Ilustración 10 Programar ejecución del escaneo



Fuente: El autor

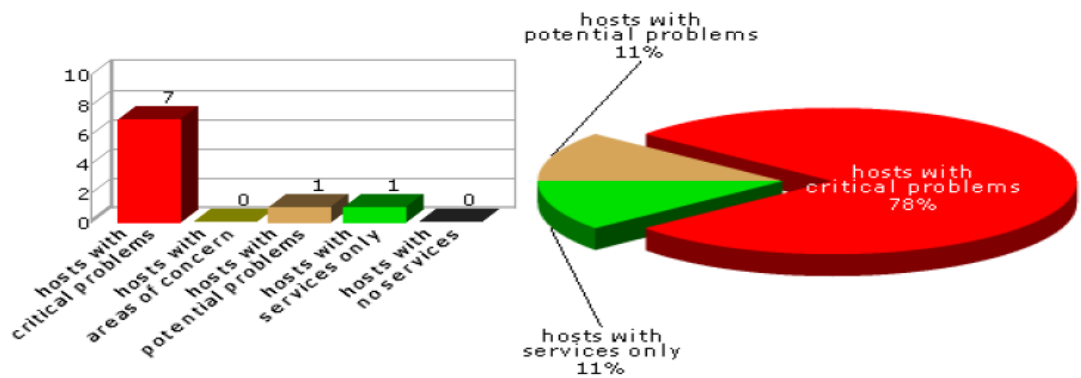
Al final del Test se recogen los archivos de salida y se procede a consolidar el informe final, teniendo en cuenta que se pretende mostrar al Oficial de Seguridad el detalle de servidores detectados en cada nivel de gravedad (Definido como el nivel de severidad de vulnerabilidad más alto detectado por servidor)

Gráficamente la herramienta genera análisis de esta manera:

Ilustración 11 Servidores por Severidad

2.2 Hosts by Severity

This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.



Fuente: El autor

Dónde:

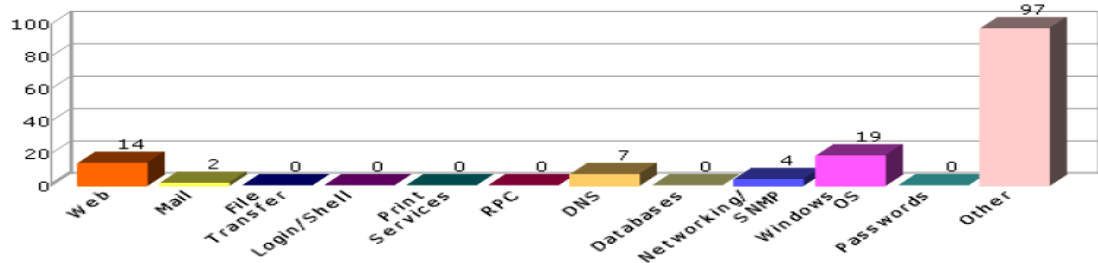
- 78% servidores con problemas críticos
- 11% servidores con problemas potenciales
- 11% servidores con servicios normales

Otros tipos de hallazgos de este escaneo organizado por clase son:

Ilustración 12 Vulnerabilidades por clase

2.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each vulnerability class.



Fuente: El autor

Donde se cuantifican por tipo de servicio o aplicativos residentes en el servidor

Otro tipo de información que ofrece la herramienta SAINT al finalizar el escaneo es la relacionada con un resumen de las vulnerabilidades y la cantidad de veces que se presentaron en la red

Ilustración 13 Resumen de vulnerabilidades por ocurrencia

3.2 Vulnerability Summary List

This table lists the number of times each vulnerability was detected on the network.

Vulnerability	Occurrences
ICMP netmask requests enabled	9
The sunrpc portmapper service is running	8
TCP timestamp requests enabled	8
rpc.statd is enabled and may be vulnerable	7
XDMCP protocol detected and may be vulnerable	7
tooltalk version may be vulnerable to buffer overflow	6
sunrpc services may be vulnerable	6
rshd receives cleartext passwords	6
rshd is enabled	6
rquotad may be vulnerable	6
rlogin receives cleartext passwords	6
rlogin is enabled	6
possible vulnerability in dtlogin	6
possible vulnerability in Solaris syslog	6
possible input validation error in tootalk	6
possible buffer overflow in dtspcd	6
Vulnerable Calendar Manager Service Solaris 9	6
SNMP to DMI mapper may be vulnerable	6
SNMP is enabled and may be vulnerable	6
Information from rusersd could help hacker	6
Information from rstatd could help hacker	6
IBM Lotus iNotes vulnerable version 9.	6

Fuente: El autor

Finalmente ofrece un detalle de la forma como puede ser resuelto o corregida la vulnerabilidad con información técnica de parches o versiones de software del producto

Ilustración 14 Remediación

Impact

A remote attacker could view directory listings, view source code of JSP files, view passwords, gain read access to files which are normally inaccessible, cause a denial of service, or possibly write files with the permissions of the user running the server.

Resolution

[Upgrade](#) Tomcat to version 9.0.0.M19 for 9.0.x, 8.5.13 for 8.5, or later 8.0.43 for 8.0, or later 7.0.77 for 7.0, or later 6.0.53 for 6.0, or later when available.

A mitigation is provided for the httpd CGI environment to avoid populating the "HTTP_PROXY" variable from a "Proxy:" header.

References

The 404 Error Page Cross Site Scripting vulnerability was reported in [Bugtraq ID 37149](#). The Security Bypass and Denial of Service vulnerabilities fixed in 6.0.36 were reported in [Secunia Advisory SA51138](#).

The Chunked Transfer Encoding denial of service was reported in [Fixed in Apache Tomcat 6.0.37](#), and [Fixed in Apache Tomcat 7.0.30](#).

Fuente: El autor

7.4 Fase 4. Elaboración del informe ejecutivo

Este informe contiene el resultado de la aplicación de las herramientas y metodología Hardening, la retroalimentación al cliente, el desempeño de los procesos, el estado de las acciones correctivas y preventivas, las acciones de seguimiento y revisión ejecutadas por el Oficial de seguridad de TI, los cambios que pueden afectar el sistema operacional, las recomendaciones para mejorar y los resultados de la gestión realizada sobre los riesgos identificados en Positiva Compañía de Seguros

De acuerdo al grado de madurez que se adquiera a través del tiempo se debe establecer una frecuencia de revisión por parte de la Vicepresidencia de Tecnología de Información, en concordancia con los objetivos y necesidades de Positiva Compañía de Seguros.

Este proceso de revisión, evidencia el compromiso asumido por esta entidad con el desarrollo, la implementación y mejora continua del Sistema de Gestión de la Información.

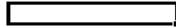
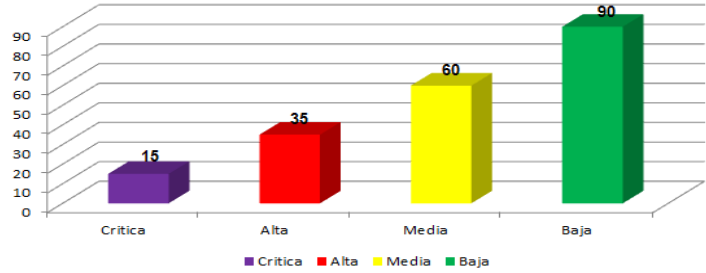
En esta Fase se requiere estructurar el documento que contenga el proceso de revisión de servicios y privilegios de acceso en los servidores, organizándolos en las diferentes plataformas que cuenta la Compañía, esto es, Solaris, Windows, etc.

Un primer análisis, luego de las pruebas realizadas, es presentar las vulnerabilidades identificadas en las categorías definidas anteriormente (Tabla 3 Escala de valoración) y luego discriminadas por cada componente de los sistemas de información.

Ilustración 15 Gestión de Vulnerabilidades

GESTIÓN DE VULNERABILIDADES INTERNAS

CONSOLIDADO VULNERABILIDADES	
RIESGO	VULNERABILIDAD
Critica	15
Alta	35
Media	60
Baja	90
TOTAL	200



Fuente: El autor

La gráfica anterior muestra el total de vulnerabilidades desagregado por nivel de criticidad sin especificar el componente en el cual se encuentran las bases de datos de la organización.

A continuación se debe mostrar el total de vulnerabilidades discriminadas por cada componente lógico, físico o de comunicaciones sobre los cuales están expuestas las bases de datos con su correspondiente nivel de criticidad.

Ilustración 16 Vulnerabilidades por componente

Access Point		APLICACIONES		BASES DE DATOS	
RIESGO	VULNERABILIDADES	RIESGO	VULNERABILIDADES	RIESGO	VULNERABILIDADES
Media	13	Critica	3	Critica	4
Baja	12	Alta	10	Alta	15
Total general	25	Media	18	Media	10
		Baja	21	Baja	20
		Total general	52	Total general	49
JUNIPER		SERVER		SWITCHS	
RIESGO	VULNERABILIDADES	RIESGO	VULNERABILIDADES	RIESGO	VULNERABILIDADES
Media	3	Critica	4	Alta	7
Baja	15	Alta	3	Media	10
Total general	18	Media	6	Baja	12
		Baja	10	Total general	29
		Total general	23		

Fuente: El autor

Luego se muestra el detalle de cada una de las acciones de remediación que se debe adelantar por cada componente al interior de la organización.

Ilustración 17 Gestión de vulnerabilidades AP

GESTIÓN DE VULNERABILIDADES AP

ID	Nombre de la Vulnerabilidad	Riesgo	Objetivo	Protocolo	Puerto	Descripción	Remediación por parte del Software
1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle	Media	18.0.0.94	tcp	3389	The remote version of the Remote Desktop Protocol Server is not supported, or/and	supported, or/and
2	SSL Certificate Cannot Be Trusted	Media	18.0.0.94	tcp	3389	The server's X.509 certificate does not have a signature from a trusted authority.	Purchase or generate a proper certificate for this service.
3	SSL Self-Signed Certificate	Media	18.0.0.94	tcp	3389	The X.509 certificate chain for this service is not signed by a trusted authority.	Purchase or generate a proper certificate for this service.
4	SMB Signing Required	Media	18.0.0.94	tcp	445	The remote host does not support SMB signing.	Windows,
5	Terminal Services Encryption Level is Medium or Low	Media	18.0.0.94	tcp	3389	The remote Terminal Services service is not configured to use Network Level Authentication (NLA).	server. This is
6	Terminal Services Doesn't Use Network Level Authentication (NLA)	Media	18.0.0.94	tcp	3389	The remote Terminal Services service is not configured to use Network Level Authentication (NLA).	server. This is
7	SSL Weak Cipher Suites Supported	Media	18.115.34.6	tcp	443	The remote host supports the use of SSL ciphers that offer only low or medium strength ciphers.	of
8	SSL Medium Strength Cipher Suites Supported	Media	18.115.34.6	tcp	443	The remote host supports the use of SSL ciphers that offer only medium strength ciphers.	medium strength ciphers.
9	SSL Certificate Cannot Be Trusted	Media	18.115.34.6	tcp	443	The server's X.509 certificate does not have a signature from a trusted authority.	Purchase or generate a proper certificate for this service.
10	SSL Self-Signed Certificate	Media	18.115.34.6	tcp	443	The X.509 certificate chain for this service is not signed by a trusted authority.	Purchase or generate a proper certificate for this service.
11	SSL Version 2 (v2) Protocol Detection	Media	18.115.45.5	tcp	443	The remote service accepts connections encrypted using SSL Version 2 (v2) protocol.	use
12	SSL Certificate Cannot Be Trusted	Media	18.115.45.5	tcp	443	The server's X.509 certificate does not have a signature from a trusted authority.	Purchase or generate a proper certificate for this service.
13	SSL Self-Signed Certificate	Media	18.115.45.5	tcp	443	The X.509 certificate chain for this service is not signed by a trusted authority.	Purchase or generate a proper certificate for this service.
14	Terminal Services Encryption Level is not FIPS-140 Compliant	Baja	18.0.0.94	tcp	3389	The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.	
15	SSL RC4 Cipher Suites Supported	Baja	18.115.34.6	tcp	443	The remote host supports the use of RC4 in one or more of its supported cipher suites.	RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites
16	Unencrypted Telnet Server	Baja	18.115.45.5	tcp	23	The remote host is running a Telnet server over an unencrypted connection.	Disable this service and use SSH instead.
17	SSL RC4 Cipher Suites Supported	Baja	18.115.45.5	tcp	443	The remote host supports the use of RC4 in one or more of its supported cipher suites.	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.
18	Unencrypted Telnet Server	Baja	18.214.158.1	tcp	23	The remote host is running a Telnet server over an unencrypted connection.	Disable this service and use SSH instead.

Fuente: El autor

En esta gráfica se recopila las salidas de la herramienta de escaneo (en este caso, Saint 8.7.6) utilizada para detectar las vulnerabilidades en el componente de Access Point (punto de acceso inalámbrico):

- Nombre de la vulnerabilidad: Descripción técnica de la vulnerabilidad donde se registra el componente, puerto o configuración que presenta fallas o debilidades que pueden ser explotadas por una atacante y que en muchos casos tienen asociado un código de error codificado por el fabricante del producto
- Riesgo: Corresponde al nivel de criticidad de la vulnerabilidad acorde a la Tabla 3 Escala de valoración
- Objetivo: Identifica el direccionamiento IP del equipo por donde se está identificando la vulnerabilidad.
- Protocolo: Protocolo de comunicación en la capa de red TCP/IP
- Puerto: La combinación de dirección IP + puerto es una dirección única en el socket; especifica la aplicación a la que se dirigen los datos
- Descripción: Describe en forma detallada el tipo de ataque recibido y las características de la vulnerabilidad
- Remediación por parte del Software: Sugiere algunas acciones y procesos con los cuales se puede mitigar la vulnerabilidad. Esta columna requiere un manejo cuidadoso dado que la solución no siempre se puede aplicar sin afectar el entorno del sistema de información

Este análisis se realiza para cada componente del Sistema de Información y debe realizarse de manera individual puesto que las bases de datos pueden ser atacadas o penetradas aún desde el componente físico (hardware).

Ilustración 18 Gestión de vulnerabilidades Aplicaciones:

GESTIÓN DE VULNERABILIDADES APLICACIONES

No.	Nombre de la Vulnerabilidad	Riesgo	Objetivo	Protocolo	Puerto	Descripción	Items Afectados
1	HP Data Protector < A.06.20 Multiple Vulnerabilities	Critica	18.114.158.33	tcp	5555	According to its version and build number, the remote instal	Installed version : A.06.11 Fixed version : A.06.2
2	HP Data Protector <= A.06.20 Multiple Vulnerabilities (uncredentialed c	Critica	18.114.158.34	tcp	5555	The version of HP Data Protector installed on the remote W	Installed version : A.06.11
3	Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Mar	Critica	18.114.158.34	tcp	8888	The 'EJBInvokerServlet' and 'JMXInvokerServlet' servlets	Nessus was able to verify the issue exists using the
4	PCI DSS compliance	Alta	18.114.158.106	tcp	0	The remote host is vulnerable to one or more conditions tha	
5	Microsoft Windows SMB Shares Unprivileged Access	Alta	18.114.158.106	tcp	445	The remote has one or more Windows shares that can be a	The following shares can be accessed as pruebas :
6	PCI DSS compliance	Alta	18.114.158.20	tcp	0	The remote host is vulnerable to one or more conditions tha	
7	Microsoft Windows SMB Shares Unprivileged Access	Alta	18.114.158.20	tcp	445	The remote has one or more Windows shares that can be a	The following shares can be accessed as pruebas :
8	PCI DSS compliance	Alta	18.114.158.33	tcp	0	The remote host is vulnerable to one or more conditions tha	
9	Microsoft Windows SMB Shares Unprivileged Access	Alta	18.114.158.33	tcp	445	The remote has one or more Windows shares that can be a	The following shares can be accessed as pruebas :
10	JBoss JMX Console Unrestricted Access	Alta	18.114.158.34	tcp	8888	The remote web server appears to be a version of JBoss th	The JMX Console can be accessed via the following
11	PCI DSS compliance	Alta	18.114.158.34	tcp	0	The remote host is vulnerable to one or more conditions tha	(XSS)
12	Microsoft Windows SMB Shares Unprivileged Access	Alta	18.114.158.34	tcp	445	The remote has one or more Windows shares that can be a	The following shares can be accessed as pruebas :
13	PCI DSS compliance	Alta	18.114.158.42	tcp	0	The remote host is vulnerable to one or more conditions tha	(XSS)
14	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle	Media	18.114.158.106	tcp	3389	The remote version of the Remote Desktop Protocol Server	n/a
15	Microsoft Windows SMB NULL Session Authentication	Media	18.114.158.106	tcp	445	The remote host is running Microsoft Windows. It is possible	It was possible to bind to the 'browser pipe
16	PCI DSS Compliance: Tests Requirements	Media	18.114.158.106	tcp	0	The scan settings did not fulfill the PCI DSS scan validation	#¿NOMBRE?
17	SMB Signing Required	Media	18.114.158.106	tcp	445	Signing is not required on the remote SMB server. This can	n/a
18	Terminal Services Encryption Level is Medium or Low	Media	18.114.158.106	tcp	3389	The remote Terminal Services service is not configured to u	The terminal services encryption level is set to :
19	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle	Media	18.114.158.20	tcp	3389	The remote version of the Remote Desktop Protocol Server	n/a
20	Sybase ASA Client Connection Broadcast Remote Information Disclosu	Media	18.114.158.20	udp	2638	The remote Sybase SQL Anywhere / Adaptive Server Any	Database name: slarp_sq12

Fuente: El autor

En esta gráfica se recopila las salidas de la herramienta de escaneo utilizada para detectar las vulnerabilidades, en este caso, Saint 8.7.6; se registra:

- Nombre de la vulnerabilidad: Descripción técnica de la vulnerabilidad donde se registra el componente, puerto o configuración que presenta fallas o debilidades que pueden ser explotadas por una atacante y que en muchos casos tienen asociado un código de error codificado por el fabricante del producto
- Riesgo: Corresponde al nivel de criticidad de la vulnerabilidad acorde a la Tabla 3 Escala de valoración
- Objetivo: Identifica el direccionamiento IP del equipo por donde se está identificando la vulnerabilidad.
- Protocolo: Protocolo de comunicación en la capa de red TCP/IP
- Puerto: La combinación de dirección IP + puerto es una dirección única en el socket; especifica la aplicación a la que se dirigen los datos
- Descripción: Describe en forma detallada el tipo de ataque recibido y las características de la vulnerabilidad
- Items afectados: Sugiere algunas acciones y procesos con los cuales se puede mitigar la vulnerabilidad. Esta columna requiere un manejo cuidadoso dado que la solución no siempre se puede aplicar sin afectar el entorno del sistema de información

Ilustración 19 Gestión de vulnerabilidades Bases de Datos

GESTIÓN DE VULNERABILIDADES BASES DE DATOS

No.	Nombre de la Vulnerabilidad	Riesgo	Objetivo	Protocolo	Puerto	Descripción	Items Afectados
1	HP Data Protector Remote Command Execution	Critica	18.114.158.14	tcp	5555	The remote HP Data Protector client or server service is aff	Nessus was able to exploit the vulnerability to execute
2	HP Data Protector < A.06.20 Multiple Vulnerabilities	Critica	18.114.158.14	tcp	5555	According to its version and build number, the remote instal	Installed version : A.06.11 Fixed version : A.06.2
3	HP Data Protector Remote Command Execution	Critica	18.114.158.16	tcp	5555	The remote HP Data Protector client or server service is aff	Nessus was able to exploit the vulnerability to
4	HP Data Protector < A.06.20 Multiple Vulnerabilities	Critica	18.114.158.16	tcp	5555	install of HP	Installed version : A.06.11
5	rlogin Service Detection	Alta	18.114.158.14	tcp	513	The remote host is running the 'rlogin' service. This service	n/a
6	NFS Share User Mountable	Alta	18.114.158.14	udp	2048	Some of the NFS shares exported by the remote server co	The following NFS shares could be mounted without.
7	PCI DSS compliance	Alta	18.114.158.14	tcp	0	The remote host is vulnerable to one or more conditions tha	
8	rlogin Service Detection	Alta	18.114.158.16	tcp	513	The remote host is running the 'rlogin' service. This service	n/a
9	NFS Share User Mountable	Alta	18.114.158.16	udp	2048	Some of the NFS shares exported by the remote server co	The following NFS shares could be mounted without.
10	PCI DSS compliance	Alta	18.114.158.16	tcp	0	The remote host is vulnerable to one or more conditions tha	+ 4 high risk flaws were found. See :
11	rlogin Service Detection	Alta	18.114.158.18	tcp	513	The remote host is running the 'rlogin' service. This service	n/a
12	NFS Share User Mountable	Alta	18.114.158.18	udp	2048	Some of the NFS shares exported by the remote server co	The following NFS shares could be mounted without.
13	PCI DSS compliance	Alta	18.114.158.18	tcp	0	The remote host is vulnerable to one or more conditions tha	
14	rlogin Service Detection	Alta	18.114.158.27	tcp	513	The remote host is running the 'rlogin' service. This service	n/a
15	PCI DSS compliance	Alta	18.114.158.27	tcp	0	The remote host is vulnerable to one or more conditions tha	
16	SNMP Agent Default Community Name (public)	Alta	18.114.158.27	udp	161	It is possible to obtain the default community name of the ren	The remote SNMP server replies to the following
17	Oracle TNS Listener Remote Poisoning	Alta	18.114.158.27	tcp	1521	The remote Oracle TNS listener allows service registration	The remote Oracle TNS listener returned the
18	PCI DSS compliance	Alta	18.114.158.29	tcp	0	The remote host is vulnerable to one or more conditions tha	
19	Microsoft Windows SMB Shares Unprivileged Access	Alta	18.114.158.29	tcp	445	The remote has one or more Windows shares that can be a	The following shares can be accessed as pruebas :
20	Finner Service Remote Information Disclosure	Media	18.114.158.14	tcp	79	The remote host is running the 'finner' service. The purp	

Fuente: El autor

En esta gráfica se registra:

- Nombre de la vulnerabilidad: Descripción técnica de la vulnerabilidad donde se registra el componente, puerto o configuración que presenta fallas o debilidades que pueden ser explotadas por una atacante y que en muchos casos tienen asociado un código de error codificado por el fabricante del producto.
Mensajes como “Exports /backups to unprivileged programs” (un atacante puede suplantar a un usuario de confianza en el sistema y ejecutar programas en un archivo del sistema) son detectados durante el escaneo.
- Riesgo: Corresponde al nivel de criticidad de la vulnerabilidad acorde a la Tabla 3 Escala de valoración
- Objetivo: Identifica el direccionamiento IP del equipo por donde se está identificando la vulnerabilidad.
- Protocolo: Protocolo de comunicación en la capa de red TCP/IP
- Puerto: La combinación de dirección IP + puerto es una dirección única en el socket; especifica la aplicación a la que se dirigen los datos
- Descripción: Describe en forma detallada el tipo de ataque recibido y las características de la vulnerabilidad
- Items afectados: Sugiere algunas acciones y procesos con los cuales se puede mitigar la vulnerabilidad. Esta columna requiere un manejo cuidadoso dado que la solución no siempre se puede aplicar sin afectar el entorno del sistema de información.

Por ejemplo, recomienda métodos generales para evitar y corregir las vulnerabilidades de NFS que se pueden encontrar en catálogos como CERT Advisory 94.15

Ilustración 20 Gestión de vulnerabilidades Server

GESTIÓN DE VULNERABILIDADES SERVER							
No.	Nombre de la Vulnerabilidad	Riesgo	Objetivo	Protocolo	Puerto	Descripción	Items Afectados
1	HP Data Protector Remote Command Execution	Critica	18.0.0.2	tcp	5555	The remote HP Data Protector client or server service is aff	Nessus was able to exploit the vulnerability to execute
2	HP Data Protector < A.06.20 Multiple Vulnerabilites	Critica	18.0.0.2	tcp	5555	According to its version and build number, the remote install	Installed version : A.06.11 Fixed version : A.06.2
3	HP Data Protector <= A.06.20 Multiple Vulnerabilites (uncredentialed c	Critica	18.0.0.2	tcp	5555	The version of HP Data Protector installed on the remote W	Installed version : A.06.11
4	HP System Management Homepage < 6.0.0.96 / 6.0.0-96 Multiple Vuln	Critica	18.0.1.38	tcp	2381	According to its self-reported version number, the HP Syst	Product : HP System Management
5	Microsoft Windows SMB Shares Unprivileged Access	Alta	18.0.1.2	tcp	445	The remote has one or more Windows shares that can be a	The following shares can be accessed as pruebas :
6	HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple V	Alta	18.0.1.38	tcp	2301	According to the web server banner, the version of HP Syst	Product : HP System Management
7	HP System Management Homepage < 6.2 Multiple Vulnerabilites	Alta	18.0.1.38	tcp	2301	According to its self-reported version number, the HP Syst	Product : HP System Management
8	DNS Server Cache Snooping Remote Information Disclosure	Media	18.0.0.2	udp	53	The remote DNS server responds to queries for third-party	Nessus sent a non-recursive query for example.com
9	SSL Weak Cipher Suites Supported	Media	18.0.0.2	tcp	1341	The remote host supports the use of SSL ciphers that offer	Here is the list of weak SSL ciphers supported by the
10	SSL Medium Strength Cipher Suites Supported	Media	18.0.0.2	tcp	1341	The remote host supports the use of SSL ciphers that offer	Here is the list of medium strength SSL ciphers
11	SSL Certificate Cannot Be Trusted	Media	18.0.0.2	tcp	1341	The server's X.509 certificate does not have a signature fro	The following certificate was at the top of the certificate
12	SMB Signing Required	Media	18.0.0.2	tcp	445	Signing is not required on the remote SMB server. This can	n/a
13	DNS Server Cache Snooping Remote Information Disclosure	Media	18.0.0.3	udp	53	The remote DNS server responds to queries for third-party	Nessus sent a non-recursive query for example.com
14	SSL RC4 Cipher Suites Supported	Baja	18.0.0.2	tcp	1341	The remote host supports the use of RC4 in one or more ci	Here is the list of RC4 cipher suites supported by the
15	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Baja	18.0.0.2	tcp	1341	At least one of the X.509 certificates sent by the remote host	The following certificates were part of the certificate
16	DHCP Server Detection	Baja	18.0.0.3	udp	67	This script contacts the remote DHCP server (if any) and at	Nessus gathered the following information from the
17	Terminal Services Encryption Level is not FIPS-140 Compliant	Baja	18.0.0.3	tcp	3389	The encryption setting used by the remote Terminal Servic	The terminal services encryption level is set to :
18	SSL RC4 Cipher Suites Supported	Baja	18.0.0.3	tcp	3269	The remote host supports the use of RC4 in one or more ci	Here is the list of RC4 cipher suites supported by the
19	Terminal Services Encryption Level is not FIPS-140 Compliant	Baja	18.0.1.2	tcp	3389	The encryption setting used by the remote Terminal Servic	The terminal services encryption level is set to :
20	SSL RC4 Cipher Suites Supported	Baja	18.0.1.2	tcp	3269	The remote host supports the use of RC4 in one or more ci	Here is the list of RC4 cipher suites supported by the

Fuente: El autor

En esta gráfica se registra:

- Nombre de la vulnerabilidad: Descripción técnica de la vulnerabilidad donde se registra el componente, puerto o configuración que presenta fallas o debilidades que pueden ser explotadas por una atacante y que en muchos casos tienen asociado un código de error codificado por el fabricante del producto.
Mensajes como “Possible Microsoft IIS ASP Remote Code Execution vulnerability” (Posible vulnerabilidad de ejecución remota de código de Microsoft IIS ASP) son detectados durante el escaneo.
- Riesgo: Corresponde al nivel de criticidad de la vulnerabilidad acorde a la Tabla 3 Escala de valoración
- Objetivo: Identifica el direccionamiento IP del equipo por donde se está identificando la vulnerabilidad.
- Protocolo: Protocolo de comunicación en la capa de red TCP/IP
- Puerto: La combinación de dirección IP + puerto es una dirección única en el socket; especifica la aplicación a la que se dirigen los datos
- Descripción: Describe en forma detallada el tipo de ataque recibido y las características de la vulnerabilidad
- Items afectados: Sugiere algunas acciones y procesos con los cuales se puede mitigar la vulnerabilidad. Esta columna requiere un manejo cuidadoso dado que

la solución no siempre se puede aplicar sin afectar el entorno del sistema de información.

Para el caso, recomienda instalar los parches referenciados en los boletines de seguridad de Microsoft

7.4.1 Recomendaciones:

Las siguientes configuraciones sugeridas buscan fortalecer las políticas de seguridad de la organización y dificultar el acceso a los atacantes:

- ✓ Firmware: Se sugiere mantener actualizado el Firmware de todos los equipos.
- ✓ Hardware: Se debe configurar el hardware para desactivar las interfaces físicas y los dispositivos de red que no estén siendo utilizados ni monitoreados. Se deben habilitar listas de acceso para direcciones reconocidas mediante la configuración de IP Tables.
- ✓ Software: El sistema operativo se debe instalar configurando dobles particiones, en cuyo esquema los documentos se almacenen en una partición y el sistema operativo en otra, lo cual aumenta la seguridad de la información.
- ✓ Red: Se debe evitar poner en riesgo la configuración de seguridad de la red de información, para ello se deben utilizar protocolos de cifrado en las tramas de información, las cuales protejan la integridad de los archivos con contraseñas, ya que la codificación no basta para proteger sus contenidos.
- ✓ Usuarios y Contraseñas: Se deben implementar controles de seguimiento y cambio de contraseñas, que alerten a los usuarios ante plazos vencidos y contraseñas caducadas.
- ✓ Servicios y Aplicaciones: Se deben deshabilitar todos los servicios innecesarios tanto en dispositivos de red como en los equipos de cómputo, los servicios que no son requeridos no deben ejecutarse, ya que hacen vulnerable al sistema.

En el desarrollo del trabajo se ha podido evidenciar que en Positiva Compañía de Seguros la seguridad en los equipos ha sido aplicada solo a nivel de las configuraciones que viene por defecto. Es muy difícil determinar el nivel de seguridad debido a que las áreas o dependencias tienen su sistema operativo pero solo saben la mitad de sus programas o solo usan las configuraciones por defecto. Por ello es importante, no sólo tener las herramientas de control sino saber para qué? y por qué? utilizarlas.

Según las consideraciones de seguridad que se han implementado en este trabajo y conociendo a cabalidad los requerimientos de Positiva Compañía de Seguros se establece que las soluciones planteadas permiten cumplir con el objetivo de brindar una metodología para garantizar la protección y privacidad de la información ante agentes externos que pretendan acceder a ella de manera fraudulenta.

Finalmente se evidencia con este estudio que cuando el sistema no tiene protección no hay otra salida que proteger su integridad siempre y cuando todos comprendan cual es el nivel de seguridad requerido y cuando todos acuerden que la seguridad es estrictamente necesaria. Puede decirse entonces que Metodologías para realizar hacking ético en bases de datos, juegan un papel muy importante para garantizar la seguridad de la información en las compañías

8. METODOLOGIA DE DIAGNÓSTICO DE SEGURIDAD DE LAS BASES DE DATOS PARA POSITIVA COMPAÑÍA DE SEGUROS S.A

Una vez realizado el análisis de la situación actual de la Casa Matriz de Positiva Compañía de Seguros, se procede a plantear una Metodología para realizar hacking ético en bases de datos, que le permitirá a los encargados de la seguridad informática entorpecer la labor del atacante y minimizar las consecuencias de un inminente incidente de seguridad e incluso evitar que éste se concrete en su totalidad.

Para el logro del objetivo de desarrollar una metodología de diagnóstico de seguridad de las bases de datos para la Casa Matriz de Positiva Compañía de Seguros S.A. en la ciudad de Bogotá se propone realizar un grupo de mecanismos y procedimientos para que sean tenidas en cuenta en sus revisiones de seguridad a partir del principio que la tecnología y las necesidades de la empresa cambian constantemente.

Al momento de establecer los equipos que serán sometidos a las pruebas de vulnerabilidades debe realizarse una lista con los equipos a los cuales se les va a realizar las pruebas, incorporando los que aparecieron después de la última prueba o retirando aquellos que ya no existan, detallando sus especificaciones técnicas.

A continuación se debe seleccionar la herramienta y versión del software a utilizar para hacer estos escaneos, acorde a los equipos candidatos para las pruebas de vulnerabilidades, teniendo en cuenta en su elección que la herramienta sea capaz de detectar lo que podría permitir a un atacante obtener acceso no autorizado, crear una denegación de servicio u obtener información confidencial sobre la red, es decir, que pueda identificar vulnerabilidades entre sistemas operativos, dispositivos de red, aplicaciones Web, bases de datos.

Otro factor a tener en cuenta en esta metodología al realizar el escaneo de la red es que debe garantizarse la revisión de los servicios TCP y UDP de la red, es decir analizar el tráfico para identificar intentos de acceso no autorizado, denegación de servicio u obtener información confidencial sobre la red de un atacante no identificad.

Como resultado del escaneo se obtiene información que comprueba si existen vulnerabilidades; esta información debe agruparse según la gravedad o el tipo; de igual manera la información suministrada debe describir la forma de corregir estas vulnerabilidades, suministrando los enlaces a nuevas versiones de software donde se puedan eliminar las vulnerabilidades detectadas.

Finalmente se procede a elaborar el documento ejecutivo el cual debe contener el proceso de revisión de servicios y privilegios de acceso en los servidores, organizándolos en las diferentes plataformas analizadas; luego se presentan las vulnerabilidades identificadas en las categorías definidas anteriormente discriminadas por cada componente de los sistemas de información. Muy importante es mostrar el detalle de cada una de las acciones de remediación que se debe adelantar por cada componente al interior de la organización.

9. CONCLUSIONES

- El diseño de una Metodología para realizar hacking ético en bases de datos, permite identificar los aspectos relevantes a tener en cuenta a la hora de establecer un modelo de seguridad de la información sólido y sostenible.
- La seguridad informática analiza no solo la función informática, que comprende el análisis de la organización, seguridad, segregación de funciones y gestión de las actividades de proceso de datos, sino también los sistemas informáticos, buscando asegurar la adecuación de los mismos a los fines para los que fueron diseñados..
- Una buena gestión de la seguridad informática se traduce en asegurar a la alta dirección y al resto de las áreas de la empresa que la información que les llega es la necesaria en el momento oportuno.
- Cada vez se hace más importante en las empresas el poder garantizar a sus clientes o usuarios que la información suministrada por ellos este segura. Sea al momento de apertura de servicios o cuentas, o en cualquier proceso que se necesiten datos personales, es necesario que estos no caiga en manos malintencionadas o de terceros trayendo con esto perjuicios tanto a la empresa que la tiene, como al mismo cliente o usuario.
- Con procesos de Ethical Hacking en bases de datos le permite a la Vicepresidencia de TIC de Positiva Compañía de Seguros asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, además de proteger los recursos y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales..

10.RESULTADOS

Los resultados logrados mediante el desarrollo del presente proyecto de grado, obedecen básicamente a la concientización de las directivas y a los administradores de Tecnología acerca de la importancia que tiene el diseño y la implementación de una Metodología para realizar hacking ético en bases de datos a fin de proteger la información.

La ejecución de la presente investigación se dio con el diagnostico en materia de seguridad de la información al interior de Casa Matriz, en dicho diagnostico se evidencio la falta de una estrategia ordenada para garantizar la seguridad de las bases de datos y la aplicación de algunos controles para evitar la ocurrencia de alguna amenaza que pudiera afectar los activos de información.

Con la conformación del equipo de proyecto se establecieron las tareas que se debe realizar al abordar un testeo de seguridad, la manera en la que los resultados de éste deben ser presentados, las normas éticas y legales que deben tenerse en cuenta al momento de concretar el test; además, fue posible, reconocer que muchos de los controles establecidos y en funcionamiento no cumplían con la documentación necesaria, en tanto otros, debían ser reevaluados pues la efectividad de estos, se veía opacada dado que no concernía a su objetivo fundamental, es decir, los controles implantados no eran los apropiados.

Una evidencia de la sensibilización por parte de la Vicepresidencia de TIC, corresponde al envío de alertas de seguridad informática a toda la comunidad de Casa Matriz mediante el correo corporativo.

Las alertas remitidas, conciernen a código malicioso circulando en la red, a través de la siguiente imagen es posible constatar dicha información

Ilustración 21 Acceso a redes inalámbricas

Acceso a Redes Inalámbricas



En días pasados se hizo mención del cambio periódico en las claves de acceso a la red inalámbrica de uso para visitantes y la de uso interno. Apartir del próximo 28 de Enero se realizará este cambio, por lo cual se recomienda a los usuarios tener presente las siguientes recomendaciones y solicitar los permisos requeridos para obtener un acceso autorizado a este recurso, en razón de sus funciones.

Aspectos a tener en cuenta:

• Diferenciación de Usuarios.

Con respecto a la clasificación de usuarios se define:

- **Usuarios Internos**, para aquellos empleados de la Compañía que estando en sus dependencias necesitan acceso a los mismos recursos a los que acceden a través de la red cableada de Positiva Compañía de Seguros S.A, siempre y cuando su uso esté dispuesto con equipos provistos o revisados y aprobados por la Gerencia de Infraestructura de TI.
- **Usuarios de Terceros o Proveedores**, para aquellos que requieran acceso a la Red de acuerdo a su objeto contractual y necesidad del servicio.
- **Usuarios Invitados**, para trabajadores que no pertenecen a Positiva Compañía de Seguros S.A. y a los que se da servicio de conexión a Internet para el acceso a web, a su correo electrónico o a la Intranet y los correspondientes recursos de su empresa.

Restricciones de uso de Redes Inalámbricas:

- La utilización de la red inalámbrica AP-POSITIVA es exclusiva para los denominados USUARIOS INTERNOS, según la definición mencionada anteriormente.
- La red de VISITANTES es exclusiva para USUARIOS TERCEROS Y/O INVITADOS. Su acceso estará supeditado a la autorización formal por parte de un funcionario de la Compañía y será de carácter temporal.
- Los usuarios que no cumplan los requisitos para ser considerados USUARIOS INTERNOS, podrán solicitar acceso a la red inalámbrica de VISITANTES, para lo cual requerirán autorización expresa de su jefe inmediato o supervisor de contrato.

• Forma de solicitudes de acceso y equipos autorizados:

En todo caso, el acceso de uso a la red inalámbrica deberá ser autorizado por Vicepresidentes o Gerentes de área, y para el caso de acceso a la red AP-POSITIVA será exclusiva para equipos portátiles y/o móviles de propiedad de Positiva, y para el caso de terceros que requieran acceso se evaluará en razón al cumplimiento de una línea base de configuración segura, obligatoria y de legalidad de licenciamiento del sistema operativo del equipo, que será revisada por la Gerencia de Infraestructura.

• Cambios en claves de acceso a redes inalámbricas:

Se atiene un cambio periódico de clave de acceso a las redes inalámbricas para invitados de forma mensual y para usuarios internos cada seis meses.

Fuente: El autor

Otro de los resultados relevantes de este ejercicio, se relaciona con el establecimiento de la gestión de vulnerabilidades sobre la infraestructura de servidores y aplicaciones que rodean las bases de datos, permitiendo a la Vicepresidencia de TIC realizar el análisis periódico de Ethical hacking con su respectivo retest sobre los dispositivos que presenten un mayor factor de riesgo según las vulnerabilidades detectadas.

Por otro lado, también se cuenta con el seguimiento a la ejecución de las actividades de remediación definidas, para mitigar las vulnerabilidades detectadas así como la notificación oportuna a los administradores de las plataformas de las vulnerabilidades relevantes identificadas durante la ejecución de los escaneos programados, propuesta en este proyecto.

11.DIVULGACIÓN

Con el fin de socializar el desarrollo y los resultados obtenidos del presente proyecto de grado, se determinó los siguientes medios de divulgación:

- Publicación en el espacio denominado UNIVERSITAS XXI ubicado en la página web de la UNAD, pues allí es posible publicar el contenido del proyecto de grado y sus avances.
- Plegables diseñados de forma sencilla y ágil para facilitar la comprensión del proyecto. El objetivo es llegar a un público puntual para garantizar la socialización del tema tratado en el proyecto de grado.

BIBLIOGRAFÍA

OBS BUSINESS SCHOOL. Etapas del plan de gestión del tiempo en un proyecto. España.: El instituto, 2017.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Código de Práctica para la gestión de la Seguridad de la Información. Requisitos. NTC-ISO-IEC 27002. Bogotá, D.C.: El Instituto, 2013. 37 p

FREELIBROS.ORG Hacking desde cero: Conozca sus vulnerabilidades y proteja su información. Bogotá, D.C.: La Organización, 2017.

CABALLERO, Alonso. Curso Virtual de Hacking Ético. Consultor Hacking Ético Lima Perú: 2016

EL TIEMPO. 10 estafas de moda en las que usted podría caer. (20. Abril, 2015)
[En:http://www.eltiempo.com/politica/justicia/estafas-en-las-que-usted-puede-caer/15593158](http://www.eltiempo.com/politica/justicia/estafas-en-las-que-usted-puede-caer/15593158)

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras. Diario oficial. Bogotá, D.C., 2009. No. 47223. p 1.

DIAZ, Flor Nancy. Principales Estándares para la Seguridad de la Información IT. Investigación. España.: Universidad Pontificia de Salamanca, 2015. 83 p.


OPEN INFORMATION SYSTEM SECURITY GROUP. Metodología de Pruebas de Intrusión ISSAF London.: La Organización 2016

SQLMAP.ORG. Automatic SQL injection and database takeover tool. La comunidad. 2016

IMPERVA. Imperva SecureSphere Web Application Firewall. San Francisco: La empresa 2016

ESET WELIVESECURITY. Auditando con Nmap y sus scripts para escanear vulnerabilidades. Latinoamérica: La Comunidad. 2017

ANEXO A

	FORMATO	
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE	
Código:	Versión: 01	
Fecha de Aprobación:	Página 66 de 70	

1. Información General	
Tipo de documento	Proyecto de Aplicado
Acceso al documento	Universidad Nacional Abierta y a Distancia
Título del documento	Metodología para realizar hacking ético en bases de datos para Positiva Compañía de Seguros S.A en la ciudad de Bogotá
Autor(es)	FLOREZ, Jorge
Director	GONZALEZ, Salomón
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2017. P. 61.
Unidad Patrocinante	Positiva Compañía de Seguros S.A.
Palabras Claves	Sistema de seguridad informática, Hacking ético a bases de datos, escaneo y gestión de vulnerabilidades, pruebas de penetración, Metodología de Análisis de seguridad, ISSAF, ISO/IEC 27001:2013, OWASP

2. Descripción
<p>El proyecto de grado, detalla el diseño de una Metodología para realizar hacking ético en bases de datos para la entidad Positiva Compañía de Seguros S.A.</p> <p>El objetivo es identificar cómo el proyecto proveerá a dicha organización la metodología para realizar diagnósticos a bases de datos mediante técnicas de Ethical hacking que le permitirán garantizar la integridad, disponibilidad y confiabilidad de la información tratada por esta aseguradora; además, pretende evidenciar la medida en que la implementación de esta metodología, le permitirá comprender que el debido respaldo de la información y de los equipos donde se alojan es la mejor alternativa, disminuyendo el impacto reputacional y operacional.</p>

3. Fuentes

OBS BUSINESS SCHOOL. Etapas del plan de gestión del tiempo en un proyecto. España.: El instituto, 2017.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Código de Práctica para la gestión de la Seguridad de la Información. Requisitos. NTC-ISO-IEC 27002. Bogotá, D.C.: El Instituto, 2013. 37 p

FREELIBROS.ORG Hacking desde cero: Conozca sus vulnerabilidades y proteja su información. Bogotá, D.C.: La Organización, 2017.

CABALLERO, Alonso. Curso Virtual de Hacking Ético. Consultor Hacking Ético Lima Perú: 2016

EL TIEMPO. 10 estafas de moda en las que usted podría caer. (20. Abril, 2015)
En:<http://www.eltiempo.com/politica/justicia/estafas-en-las-que-usted-puede-caer/15593158>

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras. Diario oficial. Bogotá, D.C., 2009. No. 47223. p 1.

DIAZ, Flor Nancy. Principales Estándares para la Seguridad de la Información IT. Investigación. España.: Universidad Pontificia de Salamanca, 2015. 83 p.

OPEN INFORMATION SYSTEM SECURITY GROUP. Metodología de Pruebas de Intrusión ISSAF London.: La Organización 2016

SQLMAP.ORG. Automatic SQL injection and database takeover tool. La comunidad. 2016

IMPERVA. Imperva SecureSphere Web Application Firewall. San Francisco: La empresa 2016

ESET WELIVESECURITY. Auditando con Nmap y sus scripts para escanear vulnerabilidades. Latinoamérica: La Comunidad. 2017

4. Contenidos

El Proyecto de Grado consta de:

Objetivo general

Crear una metodología para realizar diagnósticos a bases de datos mediante técnicas de Ethical hacking

Objetivos específicos

Levantar información de metodologías y procedimientos de Ethical hacking para bases de datos

Realizar la experimentación de pruebas de diagnóstico a las bases de datos para identificar y evaluar vulnerabilidades.

Diseñar la metodología de diagnóstico de seguridad de las bases de datos para la Casa Matriz de Positiva Compañía de Seguros S.A. en la ciudad de Bogotá.

- **Marco Referencial**, el cual está constituido por (marco de antecedentes, contextual, teórico, conceptual y legal)
- **Diseño Metodológico**: correspondiente a los pasos a seguir para recopilar información relevante para el desarrollo del proyecto de grado, por ejemplo: línea y tipo de investigación, área de investigación, técnicos y herramientas de recolección de información.
- **Metodología de desarrollo**: Con el fin de desarrollar satisfactoriamente la propuesta se contemplaron cuatro fases vitales las cuales a su vez, permitirán el diseño de una Metodología para realizar hacking ético en bases de datos para Positiva Compañía de Seguros S.A, a saber:

Fase 1: Definición de actividades, contempla recopilación de información, descripción de la red

Fase 2: Establecer los tipos de pruebas que se deben realizar.

Fase 3: Determinar la Metodología de Análisis de Seguridad

Fase 4: Estimación del tipo y cantidad de recursos necesarios para llevar a cabo cada actividad

Cronograma de actividades

Resultados y discusiones: Corresponde al desarrollo del proyecto de grado.

Divulgación: Determinación de medios de divulgación del proyecto de grado.

Conclusiones

Bibliografía e infografía

Anexos

5. Metodología

- La investigación se encuentra enmarcada por los planteamientos de la línea de investigación en Seguridad de la Información, específicamente en el Sistema de Gestión de Seguridad de la Información “SGSI” basado en el estándar ISO/IEC 27001:2013 y de metodologías existentes tales como OWASP e ISSAF que involucra al Oficial de Seguridad y a los administradores de bases de datos de la entidad bajo análisis.
- El tipo de investigación es exploratoria y descriptiva
- Las técnicas e instrumentos de recolección de información definidos corresponden a la observación, entrevista estructurada y encuesta.

La población de esta propuesta implica la Casa Matriz de Positiva ubicada en la ciudad de Bogotá pues es donde se centraliza toda la actividad de administración.

En tanto a la muestra se estima que involucrara cerca de 15 personas, profesionales del área de soluciones e infraestructura que actúan como administradores de los sistemas informáticos (bases de datos, equipos de cómputo, red local) y como Líderes Técnicos de los sistemas de información.

6. Conclusiones

- El diseño de una Metodología para realizar hacking ético en bases de datos, permite identificar los aspectos relevantes a tener en cuenta a la hora de establecer un modelo de seguridad de la información sólido y sostenible.
- La seguridad informática analiza no solo la función informática, que comprende el análisis de la organización, seguridad, segregación de funciones y gestión de las actividades de proceso de datos, sino también los sistemas informáticos, buscando asegurar la adecuación de los mismos a los fines para los que fueron diseñados..
- Una buena gestión de la seguridad informática se traduce en asegurar a la alta dirección y al resto de las áreas de la empresa que la información que les llega es la necesaria en el momento oportuno.
- Cada vez se hace más importante en las empresas el poder garantizar a sus clientes o usuarios que la información suministrada por ellos este segura. Sea al momento de apertura de servicios o cuentas, o en cualquier proceso que se necesiten datos personales, es necesario que estos no caiga en manos malintencionadas o de terceros trayendo con esto perjuicios tanto a la empresa que la tiene, como al mismo cliente o usuario.
- Con procesos de Ethical Hacking en bases de datos le permite a la Vicepresidencia de TIC de Positiva Compañía de Seguros asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, además de proteger

los recursos y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales.

Elaborado por: Florez Rojano Jorge Alonso

Revisado por: González García Salomón

Fecha de elaboración del Resumen: 16 05 2017