ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

FREY MARÍN OCHOA GUEVARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA
2018

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

FREY MARÍN OCHOA GUEVARA

Trabajo de grado presentado como requisito para optar al título de Especialista en Seguridad Informática

Director

Ing. EDGAR ALONSO BOJACA GARAVITO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA
2017

DEDICATORIA

Le doy gracias a Dios primero que todo por darme la vida y ser un profesional idóneo para el bien de la comunidad, a mi madre Belén Guevara, a mi padre Manuel que se encuentra en el cielo, que siempre fueron sus deseos de verme un profesional, a mi esposa Xiomara y a mi familia por darme el apoyo durante el proceso de formación en la Especialización en Seguridad Informática.

CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

El documento de investigación que se desarrolla a continuación corresponde a un estudio basado principalmente en la seguridad de las bases de datos pertenecientes a las organizaciones e instituciones del Estado, en este caso la secretaria de Hacienda Municipal del Municipio de Los Patios. Para la ejecución del estudio se establece una serie de procedimientos a ejecutar, entre ellos esta lo correspondiente al planteamiento del problema, en donde se expone la verdadera situación que se está presentando junto a las posibles consecuencias y así mismo las estrategias y alternativas que se deben implementar frente a ello.

Seguidamente se exponen las correspondientes argumentaciones y razones para el desarrollo de la investigación junto con la parte motiva en aras de cumplir los objetivos específicos que se han establecido. Ahora bien, otra de las acciones importantes y trascendentales consiste en la revisión bibliográfica en donde se obtuvieron diferentes teorías relacionadas con las variables de estudio entre las cuales está el uso de dos metodologías como estrategias de seguridad, la primera de ellas denominada *Pen Test* y la segunda denominada *Ethical Hacking*.

Adicionalmente se plantea la parte metodológica de la investigación, consistiendo en la investigación cuantitativa y la utilización de diferentes instrumentos establecidos como los adecuados para la obtención de información como cumplimiento de las finalidades de investigación estipuladas. Igualmente, en el desarrollo del documento se observan los correspondientes resultados que se han obtenido de las diferentes pruebas, así como la identificación de la falta de seguridad en la información dentro de la institución y así mismo la necesidad de intervenir oportunamente ante ello para ofrecer un sistema seguro en relación a los datos que se manejen y que se caracterizan por ser trascendentales y significativos.

Por último, se establecen las correspondientes referencias bibliográficas que argumentan la información que se ha establecido en la investigación con el ánimo de soportar el aspecto de veracidad y calidad de la información suministrada, finalizando respectivamente con las conclusiones y recomendaciones que se obtuvieron en el desarrollo de la investigación.

1. TÍTULO

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST Y ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS.

2. EL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

A partir de los artículos 285 y 331 de la Constitución Política de 1991 surgen en Colombia las entidades territoriales pertenecientes a la rama ejecutiva del poder público para dar cumplimiento a los fines del Estado, tales como política social, económica y de orden público que de igual manera se encuentran consagrados en el artículo segundo de la Carta Magna.

Las entidades territoriales cuentan con autonomía para la gestión de sus recursos dentro de los límites de la Constitución y la ley, con responsabilidades tan importantes como administrar los recursos y establecer los tributos necesarios para el cumplimiento de sus funciones y participar en las rentas nacionales, basado en la Ley 715 de 2001, donde se establece la distribución de competencias de los servicios de educación, salud y de propósito general entre la Nación y las entidades territoriales[1].

En este sentido, las secretarías de hacienda cumplen un papel importante en el funcionamiento de las entidades territoriales, cuyas dependencias están encargadas de organizar y ejecutar la formulación y seguimiento de las políticas económicas y las relacionadas con la planeación y recaudo fiscal para el funcionamiento sostenible de cualquier municipio.

Este es el caso de la Secretaría de Hacienda del municipio de Los Patios, la cual tiene a su cargo ejecutar la estrategia financiera para el plan de desarrollo económico y social, de acuerdo al marco fiscal de corto y mediano plazo, lo que

[1] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Lección 6 Las Entidades territoriales [en línea]. [Citado 15 de octubre de 2016]. Disponible en Internet en: http://datateca.unad.edu.co/contenidos/109107/Contenido_en_linea/leccin_6_las_entidades_territoriales.html

implica el manejo y procesamiento de datos de alta confidencialidad, tanto para la administración municipal como para los mismos contribuyentes.

Actualmente, la Secretaría de Hacienda está expuesta a amenazas de seguridad de la información, dada la posibilidad de ocurrencia de cualquier evento que pueda causar daño (material o inmaterial) sobre cualquier elemento del sistema. Desde el ámbito externo, esta entidad maneja datos sensibles y de gran interés para la administración municipal y para los diferentes contribuyentes y deudores, por lo que existen amenazas como agresiones técnicas, naturales o humanas. A nivel interno, se han identificado amenazas como la negligencia de los funcionarios que manejan la información y los equipos de cómputo, así como otras condiciones técnicas y fallas en los procesos operativos internos.

La causa de esta problemática se presenta por un lado, por la misma relevancia de la información de los datos sobre recursos económicos, pago de impuestos, cobros y deudas de contribuyentes que pueden llamar la atención de la criminalidad, así como por la falta de recursos tecnológicos, humanos y de infraestructura que no le permiten a esta Entidad Pública, contar con un sistema de seguridad para mejorar la capacidad y las condiciones técnicas que reduzcan la susceptibilidad a las amenazas y la posibilidad para responder o reaccionar a posibles daños.

Dada esta situación y teniendo en cuenta las recomendaciones del Ministerio de las Tecnologías y la Comunicación[2], se requiere trabajar en el fortalecimiento de TIC en la gestión del Estado y la información pública, que permita evaluar, estandarizar y desarrollar la arquitectura de información para contribuir en la seguridad de los datos del municipio y de los diferentes sectores económicos que lo conforman,

[2] COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Fortalecimiento de las TI de la información en la gestión del Estado y la información pública [en línea]. [Citado 15 de octubre de 2016]. Disponible en Internet en: http://www.mintic.gov. co/portal/vive digital/612/w3-propertyvalue-657.html

obteniendo consecuencias significativas en relación a las variables de estudio que se han determinado.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede diagnosticar la seguridad en las Bases de Datos de la Secretaria de Hacienda Municipal de Los Patios, mediante metodologías de Pen Test y Ethical Hacking?

3. JUSTIFICACIÓN

En la actualidad, la seguridad de la información poco a poco, va adquiriendo mayor relevancia en cuanto a la información que tiene cualquier entidad bien sea pública o privada, estando la Secretaría de Hacienda objeto de estudio en el ámbito público, y teniendo entonces la obligación, y por consiguiente la necesidad de guardar la información en total confidencialidad, integridad, disponibilidad y protección. Sobre este asunto, en dicha Secretaría ubicada en el municipio de los Patios, se observa que carece de seguridad informática idónea y adecuada, para evitar que, por factores internos o externos, existan riesgos, fallas, amenazas y daños de información, teniendo como consecuencia pérdidas económicas, administrativas y privadas.

De lo anterior la presente investigación, le permite al organismo cumplir a cabalidad con su misión y visión, al implantar un correcto control y manejo de la información, porque se mejorará en la Secretaría de Hacienda del municipio de los Patios, en un corto y mediano plazo, la seguridad de su sistema de información, garantizando la confidencialidad, integridad, autenticidad y acceso de los datos.

Por otro lado, como la Secretaría de Hacienda es responsable ante la ley de la gestión de los recursos que requiere el municipio, para la ejecución del plan de desarrollo, el proyecto le servirá para minimizar los riesgos en los que está expuesta, principalmente por la criminalidad que se presenta y por la intervención humana, para causar daños a la integridad de la información que viola la ley.

Frente a la gestión integral del riesgo de la Alcaldía Municipal, el proyecto puede ofrecer a la Entidad mecanismos de protección de la información frente a sucesos físicos, tales como eventos naturales ajenos a la intervención humana o técnicos que son causados indirectamente por personas, como la negligencia y todas las

acciones u omisiones que pueden influir en la seguridad del sistema y que no son fácilmente predecibles.

Así mismo, se determina que este espacio es importante para la implementación de estrategias y acciones desde el punto de vista académico en aras de proteger una entidad tan importante que contiene información valiosa, correspondiente a las contribuciones e impuestos que se cancelan.

Por último, la administración municipal podrá cumplir los requerimientos del Ministerio TIC que busca hacer de la administración pública, una gestión eficiente y coordinada mediante las tecnologías de la información, que puedan ofrecer valor agregado al ciudadano y al desarrollo de los diferentes sectores de la economía de Los Patios.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

- Realizar un estudio de seguridad en las Bases de Datos, mediante metodologías de Pen Test y Ethical Hacking en la Secretaria de Hacienda Municipal de Los Patios.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar el estado actual de metodologías de Pen Test y de Ethical Hacking para bases de datos relacionales y no relacionales.

- Determinar las metodologías de Pen Test y de Ethical Hacking a ser utilizadas.

- Planear y realizar el diagnóstico de las bases de datos de la Secretaría de Hacienda Municipal de Los Patios.

- Aplicar las técnicas necesarias con las metodologías Pen Test y Ethical Hacking, para generar un buen desarrollo informático en la Secretaría de Hacienda Municipal de los Patios.

5. ALCANCES Y LIMITACIONES

5.1 ALCANCES

El proyecto parte de la revisión del estado actual de metodologías de Pen Test y de Ethical Hacking para bases de datos relacionales y no relacionales, con la finalidad de seleccionar las metodologías más apropiadas para el desarrollo del proyecto.

Seguidamente, se propone planificar y ejecutar un diagnóstico de las bases de datos de la Secretaria de Hacienda Municipal de Los Patios, que permita presentar finalmente y de forma coherente una propuesta para mejorar la seguridad en las bases de datos que fueron analizadas.

5.2 LIMITACIONES

Se proveen limitaciones técnicas por el mal funcionamiento de algunos equipos de cómputo y redes que se encuentran instalados en la Secretaría de Hacienda de Los Patios.

Existen otras limitaciones por parte de la poca disponibilidad de tiempo del personal que labora en la Alcaldía Municipal, que puede afectar la recolección de información sobre la capacidad y experiencia del recurso humano en la seguridad del sistema de información.

El proyecto debe ser desarrollado en el lapso de tiempo establecido en el cronograma de actividades, lo que limita el detalle del análisis para la realización del diagnóstico del sistema e información.

6. MARCO DE REFERENCIA

6.1 ESTADO DEL ARTE

Para el desarrollo de este proyecto, se tienen en cuenta referentes investigativos que permitan analizar diferentes metodologías y resultados que fueron ejecutados en diferentes ámbitos, como entidades privadas y públicas. La revisión de antecedentes arroja los siguientes resultados:

A nivel internacional:

FERNÁNDEZ, E. Metodología para el diseño de bases de datos seguras. La Mancha: Universidad de Castilla, 2002.

La creciente importancia de la información en la sociedad actual ha llegado a convertirse en el principal activo de las empresas y hace imprescindible su protección. Esta protección abarca una gran cantidad de aspectos, como los siguientes: seguridad física, autenticación, biometría, seguridad en las redes de comunicación, criptografía, seguridad jurídica, etc. Dentro de todos estos aspectos destaca la seguridad de las bases de datos, que es donde residen al fin y al cabo los datos a partir de los cuales las organizaciones obtienen la información y los conocimientos necesarios para su supervivencia[3].

En este referente, se analiza la seguridad en las bases de datos que ha tenido importantes cambios y exigencias debido a los continuos avances tecnológicos, los cada vez más complejos requisitos organizacionales, la difusión de las comunicaciones, el incremento de la vulnerabilidad de los sistemas de información, los cambios legislativos, etc. Este tema aún constituye un problema que es difícil de

[3] FERNÁNDEZ, E. Metodología para el diseño de bases de datos seguras. La Mancha: Universidad de Castilla, 2002.

resolver y requiere de soluciones metodológicas en las que la seguridad sea considerada como un factor importante a lo largo del proceso de diseño de las bases de datos a nivel nacional:

VELASCO, A. El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la Norma ISO 27001.

Se tiene en cuenta este referente porque analiza la existencia y diversas modalidades que incluye el Derecho informático para crear conciencia acerca de la posición que deben tomar los diversos actores económicos en la era de la información para asegurar una adecuada política de seguridad de la información que, ante la falta de una legislación nacional sobre el tema, debe basarse en los estándares internacionales, el derecho comparado y autonomía de la voluntad. La metodología empleada para explicar las diversas áreas de impacto es la seguida por la norma ISO 27001 en el dominio que hace referencia al cumplimiento y que comprende: La protección de datos personales; la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios de comercio electrónico; la propiedad intelectual, y el tratamiento de los incidentes informáticos[4].

A nivel regional:

MOJICA, M. Implementación y administración del sistema de información del Ministerio de Educación Nacional SICIED (sistema interactivo de consulta de infraestructura educativa). Trabajo de Grado. Ingeniero de Sistemas. San José de Cúcuta: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Ingeniería de Sistemas, 2011.

[4] VELASCO, A. El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la Norma ISO 27001 [en línea]. [Citado 18 de octubre de 2016]. Disponible en Internet en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013&lng=en&nrm=iso

Se tiene en cuenta este referente por desarrollarse en el sector público. En este documento, se elaboraron actividades para el mantenimiento de la integridad, la seguridad, la disponibilidad y la confiabilidad de los datos. Así mismo, se instaló el sistema de información Sicied, en los equipos de la Secretaria de Educación de Duitama y Secretaria de Educación de Guainía. Se logró administrar el sistema de forma satisfactoria mediante políticas de seguridad como gestión de autorizaciones, restricciones de integridad como integridad de dominio. Por último, se realizaron jornadas de capacitación para los funcionarios de las secretarias de educación de Duitama y Guainía, con base en el funcionamiento del Sicied[5].

6.2 MARCO TEÓRICO

6.2.1 Amenazas informáticas. Los cambios que ha dado la tecnología en la actualidad son trascendentales, su desarrollo le ha permitido a las entidades públicas y privadas, tener acceso a cualquier información, situación favorable para poder solucionar de forma rápida alguna inquietud que se le presente o sacar provecho de ella, para guardar o compartir información. Es entonces, una herramienta esencial que se usa para lograr los objetivos de negocio o desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy. Porque la seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas[6].

---

[5] MOJICA, M. Implementación y administración del sistema de información del Ministerio de Educación Nacional SICIED (sistema interactivo de consulta de infraestructura educativa). Trabajo de Grado. Ingeniero de Sistemas. San José de Cúcuta: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Ingeniería de Sistemas, 2011.

[6] TARAZONA, C. Amenazas informática s y seguridad de la información. México: Etek Internacional, 2007. p. 138.

Ahora bien, frente a las amenazas informáticas, es evidente que el sistema digital es muy amplio y se ha prestado para que personas marginadas denominadas Hackers tengan fines maliciosos centrados en producir daños para favorecer tan sólo intereses particulares. Sobre este asunto, cabe resaltar que, ante una mejor protección de la situación con conocimientos, herramientas de software y hardware, se puede poseer mayor seguridad y confiabilidad, sin embargo, para ello es pertinente la implementación de sistemas, con estrategias que permitan la reducción de las amenazas, que son preocupantes en una Entidad Pública, pues el compromiso es mayor para evitar que se presenten vulnerabilidades en el sistema.

De lo anterior, conviene señalar que los riesgos de la información se presentan cuando confluyen dos elementos: amenazas y vulnerabilidades, las dos están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Sin embargo, en algunos casos, las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones[7].

Seguidamente, frente a estos dos aspectos mencionados se han suscitado controversias, al indicar que en primer lugar se encuentra la vulnerabilidad para poder recibir amenazas. No obstante, se debe enunciar que las amenazas se pueden generar desde el interior de la organización y es en este aspecto, en donde se debe crear mayor protección para la no obtención de consecuencias perjudiciales.

Asimismo, sobre este tema, se pueden agrupar las amenazas de la información, algunas de estas son[8]: el virus informático o código malicioso, que se genera por programas que contienen malware y se hacen sin el consentimiento expreso del

[7] Ibid., p. 138.
[8] Ibid., p. 138.

autorizado al manejar la plataforma; seguidamente está el uso no autorizado de Sistemas Informáticos, como la misma palabra lo indica se utilizan de forma indebida por personas ajenas a las autorizadas en el programa; también se encuentra el robo de información, que ocurre cuando de forma ilegal cometen el delito al obtener información confidencial que no le pertenece; por otro lado, están los fraudes basados en el uso de computadores, conocido a su vez como fraude cibernético o espionaje, el cual es uno de los más usados por los hackers quienes promueven la piratería informática; seguidamente existe la suplantación de identidad, en ella otra persona se hace pasar por otra, para lograr obtener información o provecho económico; por otro lado está la denegación de servicios, también conocida como DoS, en ella se ataca es al sistema compartido entre varias computadoras, para evitar que continúen extrayendo información no autorizada; otra amenaza, son los ataques de fuerza bruta, en ella intentan reiteradamente recuperar una clave perdida o lo contrario adivinar la clave para acceder fácilmente a la base de datos; así mismo, se encuentra la alteración de la información, en ella personas inescrupulosas, modifican, alteran o eliminan información contenida en los programas; para ultimar, está la divulgación de Información o sabotaje, intervienen personas con malicia, comparten información confidencial y reservada, junto con declaraciones económicas o administrativas; y finalmente se encuentran los desastres naturales, producto de casos fortuitos y de fuerza mayor, los cuales deben ser prevenidos.

Figura 1. Amenazas para la seguridad

Fuente: GUTIERREZ, J y ZUCCARDI, G: Universidad Javeriana.

De lo anterior, en esa breve explicación, la amenaza que se tiene en cuenta según el objeto de estudio, consiste en los actos maliciosos o malintencionados, puesto que la investigación se basa principalmente en establecer estrategias, para estar protegidos, seguros y prevenidos, ante cualquier ataque que se presente.

6.2.2 Seguridad de la información. El panorama de los procesos tecnológicos, en la globalización ha tenido diversos cambios, que surgieron después del pronunciamiento de la OCDE[9] quien desde tiempo atrás, desarrolló por primera vez en 1992 una serie de Directrices para la Seguridad de los Sistemas de Información, las cuales tratan de promover el uso y desarrollo de una cultura de la Seguridad, no sólo en el desarrollo de Sistemas y Redes de comunicación, sino mediante la adopción de "nuevas formas de pensamiento y comportamiento en el uso de la interconexión de esos sistemas". De lo anterior, con la evolución de los sistemas de información y de la forma de hacer negocios o acuerdos, la información se ha

[9] Organización para la Cooperación y el Desarrollo Económico.

convertido en uno de los activos de mayor valor para las personas y especialmente para las organizaciones bien sea públicas o privadas. Teniendo como punto de partida que "los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada vez más dependientes de estos. Sólo un enfoque que tenga en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines, puede proporcionar una seguridad efectiva"[10]. Como lo sostiene el autor Tarazona, se debe plantear lo correspondiente a la seguridad efectiva, con medidas de prevención y teniendo en cuenta una serie de parámetros para reforzar las vulnerabilidades y amenazas.

Así pues, cada día frente a este tema se tiene mayor relevancia, porque suscitan diversas esferas del conocimiento humano, relacionadas bien sea para garantizar la seguridad de la información o para tener el poder social, por medio de procesamientos ilegales de la misma. Es por eso que se considera importante, tener en cuenta las políticas de seguridad que giran en torno a esto, para conocer y tener claridad, de qué está protegido y cuáles serían las herramientas que se requieren para la seguridad, evitando que se presenten ataques cibernéticos, los cuales desvían o alteran la información. La cual, según cifras de Estados Unidos, siguen siendo los virus informáticos la principal fuente de pérdida financiera en las organizaciones, seguidos por los impactos derivados de accesos no autorizados a los sistemas, el robo de información de propiedad industrial, y la pérdida de computadores personales o elementos de computación móvil, son las causas que generan más del 74% del total de las pérdidas financieras[11].

Por otro lado, desde el punto de vista académico también se señala que la información es uno de los aspectos más importantes en las organizaciones puesto que de ahí se guarda la base de datos y demás aspectos relevantes, que deben ser protegidos, detectados y recuperados de la mejor forma posible, para evitar que

[10] TARAZONA. Op. cit., p. 142.
[11] Ibid., p. 140.

concurran como consecuencia incidentes y divulgaciones indebidas en los medios de comunicación, provocando a su vez pérdidas para la entidad, al perder credibilidad, confianza e integridad.

6.2.3 Las metodologías de Pen Test y Ethical Hacking. Ahora bien, con respecto a estas metodologías, son las encargadas de administrar la seguridad informática porque hace que se efectúen y garanticen las políticas de seguridad, disminuyendo entonces los riegos, al contar con las medidas de seguridad y con una base de datos estructurada, según el modelo de datos que representan las relaciones y restricciones existentes entre los objetos, estructurados con independencia, integridad y seguridad. De lo anterior, conviene diferenciar entre Base de Datos y el Sistema General de Bases de Datos (SGBD), la primera, es el almacenamiento donde se guardan los datos y la segunda es lo que manipula la información almacenada mediante procesos de lectura/escritura, al encargarse de modificar los datos y, controlar la integridad y seguridad.

De lo anterior, el *Pen test* conocido también como *penetración testing*, se encarga a su vez de establecer las debilidades, sensibilidades y críticas que tendría la Secretaría de Hacienda del Municipio de los Patios, teniendo como métodos la evaluación de la seguridad del sistema, al manejar los requerimientos propios que evitan la producción de riesgos, como por ejemplo la ubicación y detección de los "hackers", los cuales tienen como objetivo, el control del sistema, para obtener y alterar la información. Consiste entonces "en un modelo que reproduce intentos de acceso de un potencial intruso desde los diferentes puntos de entrada que existan, tanto internos como remotos, a cualquier entorno informático, permitiendo demostrar los riesgos funcionales de las vulnerabilidades detectadas"[12]. Este

[12] MONTERO, H. Técnicas del penetration testing [en línea]. [Citado 18 de octubre de 2016]. Disponible en Internet en: http://www.cybsec.com/upload/VictorMontero-SeminarioTecnicasdelPenetrationTestingArgentina.pdf

modelo es trascendental porque por medio de él, se analizan los ataques que se están presentando a la información de la Entidad e igualmente identifica la vulnerabilidad de la organización, para la creación de acciones que minimicen estas dificultades.

Queda claro entonces, que en la metodología Pen test se tiene en cuenta un ataque basado en fallas y vulnerabilidades conocidas por expertos que no han podido ser resueltas adecuadamente. Estas vulnerabilidades se definen como "debilidades en el diseño de un sistema, en su implementación, operabilidad y gestión que podría ser comprometido, violando su política de seguridad"[13]. Por lo anterior, para unir todas esas falencias se empiezan aplicar las pruebas ejecutando la seguridad en las aplicaciones y teniendo en cuenta los estándares ISO 17799 e ISO 27001 para desarrollar un marco de gestión de la seguridad de la información efectivo, que le permita proteger sus activos de información importantes, minimizando sus riesgos y optimizando las inversiones y esfuerzos necesarios para su protección[14]. Con la norma anunciada no sólo se optimiza la gestión de riesgos con el ambiente de pruebas, sino que a su vez se evalúan los mismos, para evitar los atentados informáticos y la adulteración o pérdida de la información.

Por otro lado, se implementa también la metodología Ethical Hacking (hackeo ético), en ella se evalúan también las vulnerabilidades existentes en el sistema, pero por medio de un test de intrusión, el cual evalúa la seguridad física y lógica de los sistemas de información, así como de las redes de computadoras, bases de datos, aplicaciones web y servidores, etc. Esto se realiza con la finalidad de tener acceso al sistema de información y demostrar que este puede ser vulnerable. Por lo tanto, es de gran utilidad para la Secretaría, porque permite tomar medidas preventivas frente a los posibles ataques que se están presentando o pudieran ocurrir. En este

[13] PÉREZ, M. (2012). Módulo 3: auditorías y seguridad. tema 4: comparativa metodologías auditorías y pentesting. Elche: Campus Virtual, p. 5.
[14] Ibid., p. 143.

sentido, conviene aclarar que el *Ethical Hacking* consiste en “una simulación de posibles escenarios donde se reproducen ataques de manera controlada con actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: Para atrapar a un intruso, primero debes pensar como intruso"[15].

Para ultimar, se reitera que la seguridad informática requiere de diferentes métodos y herramientas para garantizar la protección de la información, a partir de lo cual, los servicios de Pen test y Ethical Hacking permiten hacer diferentes pruebas que incluyen “tácticas de ingeniería social, uso de herramientas de hacking, uso de Metasploit, las cuales explotan vulnerabilidades conocidas” [16] , que al final son recolectadas para atacar con los sistemas operativos, la información expuesta y el manejo de la entidad en la aplicación, logrando la ejecución de la seguridad que evita ser suplantada al tener usuarios de registro y manipulada al poseer nuevas medidas de protección frente a los ataques de fuerza bruta.

6.3 MARCO CONCEPTUAL

- **Amenaza:** Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS)[17].

- **Ataques multi-etapas:** Es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware[18].

---

[15] REYES, A. Ethical Hawking [en línea]. [Citado 18 de octubre de 2016]. Disponible en Internet en: https://www.seguridad.unam.mx/descarga.dsc?arch=2776
[16] Ibid., p. 1.
[17] SYMANTEC. Glosario de Seguridad 101 [en línea]. [Citado 25 de octubre de 2016]. Disponible en Internet en: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad
[18] Ibid., p. 1.

- **Ataques Web:** Es un evento malicioso que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta[19].

- **Autenticidad:** La legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable[20].

- **Confidencialidad:** Datos que solo pueden ser legibles y modificados por personas autorizados, tanto en el acceso a datos almacenados como también durante la transferencia de ellos[21].

- **Disponibilidad:** Acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos[22].

- **Elementos de Información:** También "Activos" o "Recursos" de una institución que requieren protección, para evitar su perdida, modificación o el uso inadecuado de su contenido, para impedir daños para la institución y las personas que salen en la información. Se distingue y divide tres grupos, a) Datos e Información, b) Sistemas e Infraestructura y c) Personal[23].

---

[19] Ibid., p. 1.
[20] RSS ENTRIES. Gestión de Riesgo en la Seguridad Informática 101 [en línea]. [Citado 25 de octubre de 2016]. Disponible en Internet en: https://protejete.wordpress.com/glosario/
[21] Ibid., p. 1.
[22] Ibid., p. 1.
[23] Ibid., p. 1.

- **Gestión de Riesgo:** Método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Está compuesta por cuatro fases: 1) Análisis, 2) Clasificación, 3) Reducción y 4) Control de Riesgo[24].

- **Integridad:** Datos son completos, no-modificados y todos los cambios son reproducibles (se conoce el autor y el momento del cambio) [25].

- **Seguridad Informática:** Procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad[26].

- **Spyware:** Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local[27].

- **Vulnerabilidad:** Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas[28].

---

[24] Ibid. p. 1.
[25] Ibid. p. 1.
[26] Ibid., p. 1.
[27] SYMANTEC. Op. cit., p. 1.
[28] Ibid., p. 1.

6.4 MARCO LEGAL

Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar lo referente a la legalidad del tipo de software instalado en los equipos de cómputo de la empresa.

Ley estatutaria 1266 del 31 de diciembre de 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 del 5 de enero de 2009. Por medio de la cual se modifica el Código Penal, información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 del 30 de julio de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

7. DISEÑO METODOLÓGICO

7.1 TIPO DE INVESTIGACIÓN

Se utilizará un tipo de investigación cuantitativo y descriptivo para recopilar la información requerida para el análisis de la seguridad en las Bases de Datos, mediante metodologías de *Pen Test* y *Ethical Hacking* en la Secretaría de Hacienda Municipal de Los Patios. La investigación descriptiva permite identificar las características del universo de investigación, señala formas de conducta y actitudes del universo investigado[29]. Este tipo de investigación permite identificar, procesar y analizar los datos que se toman por diferentes medios, como la observación directa, la encuesta y las listas de chequeo, que son muy útiles en este tipo de estudios.

7.2 POBLACIÓN Y MUESTRA

7.2.1 Población. La población corresponde a la totalidad de los funcionarios públicos adscritos a la que Secretaría de Hacienda Municipal de Los Patios, Departamento Norte de Santander, para lo cual su función principal es el procesamiento de la información que a diario se ingresa por las diferentes transacciones y operaciones realizadas por la comunidad que lo solicita.

[29] MÉNDEZ, C. Metodología de la investigación para ciencias empresariales. Bogotá: Mc Graw Hill, 2003.

7.2.2 Muestra. La muestra corresponde a los funcionarios que están adscritos a la Secretaría de Hacienda de Los Patios y que tienen información importante para el diagnóstico que se debe aplicar en las bases de datos de esta dependencia.

Por tratarse de un número reducido de personal, se aplicará un muestreo no probabilístico para tomar el 100% de los funcionarios de la Secretaría de Hacienda. También se tomará como muestra la totalidad de los datos contenidos de forma digital en la base de datos

7.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Fuentes primarias. Será la información que el autor del proyecto recopilará directamente en la Secretaría de Hacienda de Los Patios, por medio de instrumentos como la observación directa, la encuesta aplicada a funcionarios y la lista de chequeo sobre las condiciones de la infraestructura física y tecnológica disponible.

Fuentes secundarias. Se tomarán de documentos ya elaborados, como libros sobre gestión de la seguridad informática, bases de datos de la Alcaldía de Los Patios, normatividad y artículos sobre gestión de la información y protección de datos.

7.4 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Fichas técnicas: Se utilizarán para organizar información de diferentes libros, proyectos y artículos sobre el uso e implementación de metodologías de Pen Test y de *Ethical Hacking* para bases de datos relacionales y no relacionales.

Encuesta: Se aplicará una encuesta estructurada con opción de respuesta en selección múltiple para tomar información sobre los conocimientos, experiencia y

habilidades del personal de la Secretaría de Hacienda en el manejo de los datos almacenados en esta dependencia.

Lista de chequeo: Se aplicará una lista de verificación para determinar el estado actual de la infraestructura física y tecnológica con que dispone la dependencia en la actualidad y valorar los posibles riesgos a los que esté expuesta la información.

Observación directa: Se utilizará para recopilar información complementaria para el diagnóstico de las bases de datos de la Secretaria de Hacienda Municipal de Los Patios y sobre la identificación de las metodologías de *Pen Test* y de *Ethical Hacking* más convenientes.

7.5 ANÁLISIS DE INFORMACIÓN

La información será procesada por medios de procesador de texto y hojas de cálculo para facilitar su interpretación. En el caso de las encuestas se utilizarán gráficas de torta y tablas porcentuales para discriminar los resultados. Los resultados de la lista de chequeo se podrán resumir en gráficas de barras para establecer el nivel de cumplimiento de los requisitos técnicos en seguridad de bases de datos.

8. RESULTADOS

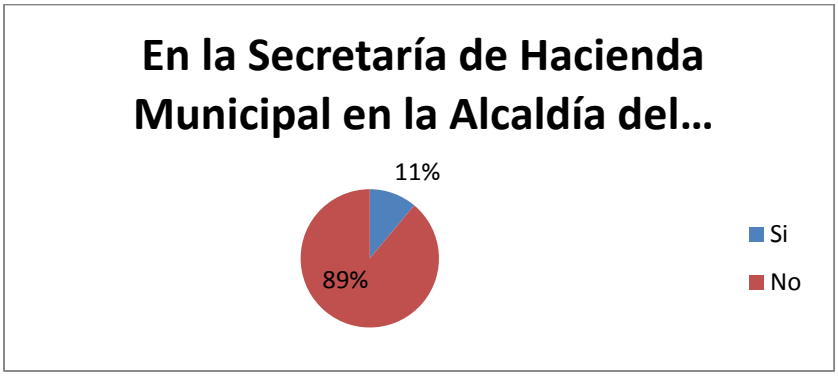
8.1 IDENTIFICACIÓN DEL ESTADO ACTUAL DE METODOLOGÍAS DE PEN TEST Y DE *ETHICAL HACKING* PARA BASES DE DATOS RELACIONALES Y NO RELACIONALES

Para la obtención de los resultados, se aplicó la encuesta como fuente primaria de información, la cual permite a través de cuestionarios resolver las inquietudes que se tienen del objeto de estudio, para de esta forma poder implementar alternativas de solución al mismo.

Para determinar el estado actual de las bases de datos en la Secretaria de Hacienda Municipal, se empleó herramientas de seguridad informática como son los diferentes tipos de software sobre la plataforma LINUX, permitiendo la identificación de vulnerabilidades en los sistemas informáticos implementados para el buen desarrollo de la información en la Institución.

En su desarrollo, se tenía como muestra y población el personal de la Secretaría de Hacienda municipal de los Patios, los cuáles participaron activamente en la respuesta de las preguntas de selección múltiple, relacionadas a los conocimientos, experiencias y habilidades que tienen en la Entidad. De lo anterior, a continuación, se describe con gráficas el porcentaje derivado de cada pregunta, junto con el análisis obtenido de las respuestas:

Gráfica 1. ¿En la Secretaria de Hacienda Municipal y en la Alcaldía de Los Patios, se utiliza la metodología Pen Test y de Ethical Hacking para bases de datos relacionales y no relacionales?



Análisis pregunta 1: Claramente se identifica que en la institución en donde se desarrolla la investigación, no se realiza ningún tipo de metodología.

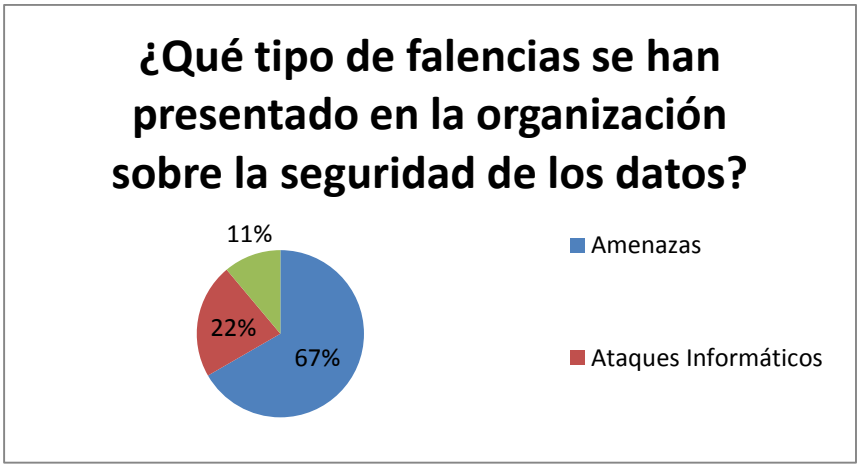
Gráfica 2. ¿Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos?

Análisis pregunta 2: Infortunadamente en la organización, se han presentado obstáculos, situación que genera preocupación conforme a la información que se maneja caracterizada, por ser importante y trascendental.

Gráfica 3. ¿Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos?

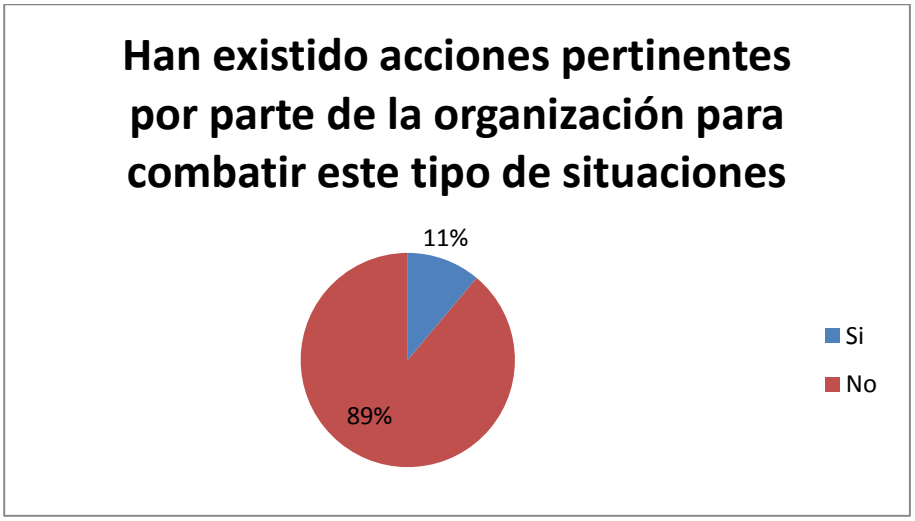
Análisis pregunta 3: Evidentemente se aprecia que en un alto porcentaje se determina la pertinencia y necesidad de implementar metodologías en relación a la protección y seguridad de la base de datos.

Gráfica 4. ¿Qué tipo de falencias se han presentado en la organización sobre la seguridad de los datos?



Análisis pregunta 4: Las opciones que se presentan en la encuesta sobre las falencias presentadas corresponden a las amenazas, ataques informáticos y a la vulneración a los sistemas de información obteniendo como respuesta que el 67% corresponde a las amenazas.

Gráfica 5. ¿Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones?



Análisis pregunta 5: Finalizando el análisis de la encuesta se determina que hasta la fecha no se han presentado acciones y estrategias para disminuir las amenazas que se identifican.

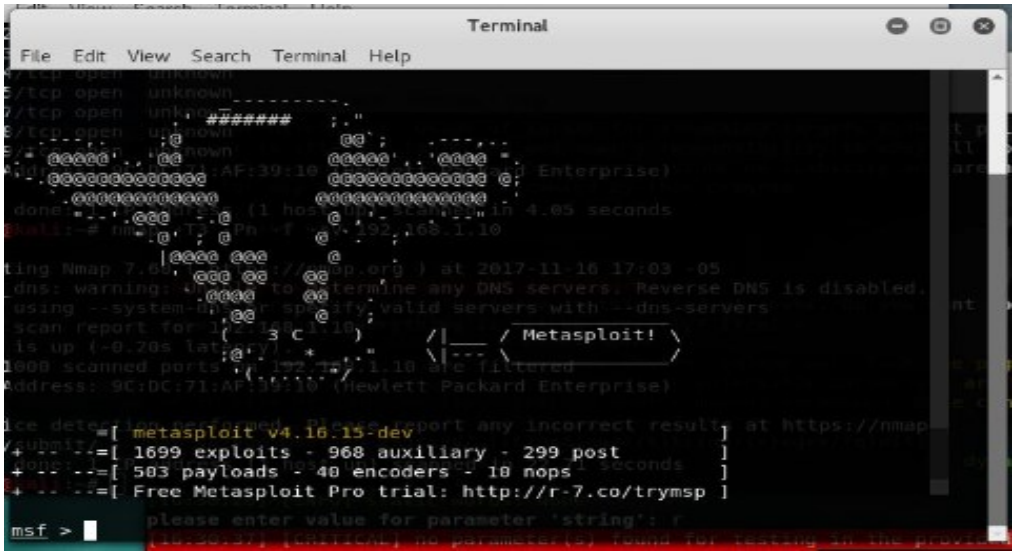
8.2 DETERMINACIÓN DE LAS METODOLOGÍAS DE PEN TEST Y DE ETHICAL HACKING A SER UTILIZADAS

Información Activa: Esta fase se caracteriza por tener un contacto directo con el objetivo permitiendo realizar pruebas en los servidores y simulando el estado en que se encuentra cada elemento informático, basado en las herramientas que caracteriza el sistema operativo utilizado como:

METASPLOIT 2: Es una Maquina diseñada a partir de GNU/LINUX, lo cual cuenta con una gran cantidad de vulnerabilidades y su funcionalidad está enfocada para realizar las pruebas de penetración.

Pruebas de penetración. *Nmap (Network Mapper).30* Es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y la versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes o cortafuegos están en uso, y docenas de otras características. Nmap se ejecuta en la mayoría de los ordenadores y la consola y versiones gráficas están disponibles. Nmap es libre y de código abierto.

Figura 2. Entorno inicio Metasploit



Fuente: Autoria Propia Frey Ochoa

KALI LINUX: Es una distribución de Debían. Para facilitar la auditoria de sistemas de seguridad informática, cuanta con más de trecientas herramientas sofisticadas para la seguridad informática.

Figura 3. Entorno inicio Kali Linux

Fuente: Autoria Propia Frey Ochoa

En esta fase se intenta identificar las máquinas que se encuentran funcionando en este momento en una red, los sistemas operativos con que esté funcionando cada una de estas y versiones que estén utilizando.

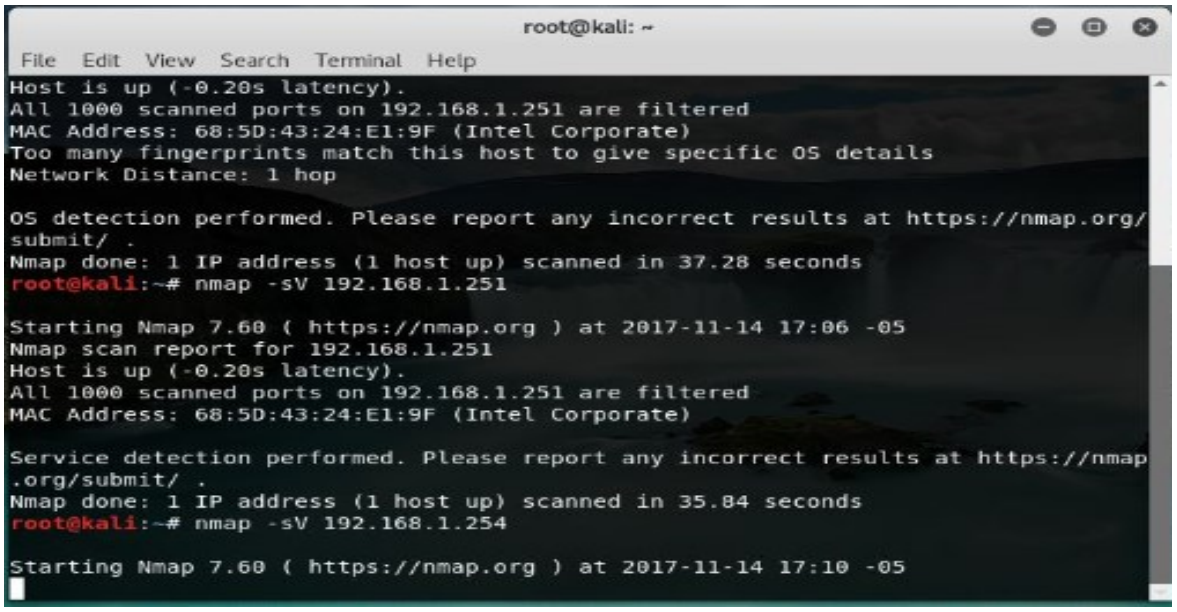
Para este proceso se utiliza el sistema operativo Kali Linux.

Herramientas utilizadas:

1. NMAP

- Nmap –sV (Dirección Ip).

Figura 4. Entorno inicio Nmap con Kali Linux



Fuente: Autoria Propia Frey Ochoa

Con la instrucción sV, se genera un informe más detallado de los puertos que se encuentran activos en la dirección Ip estudiada.

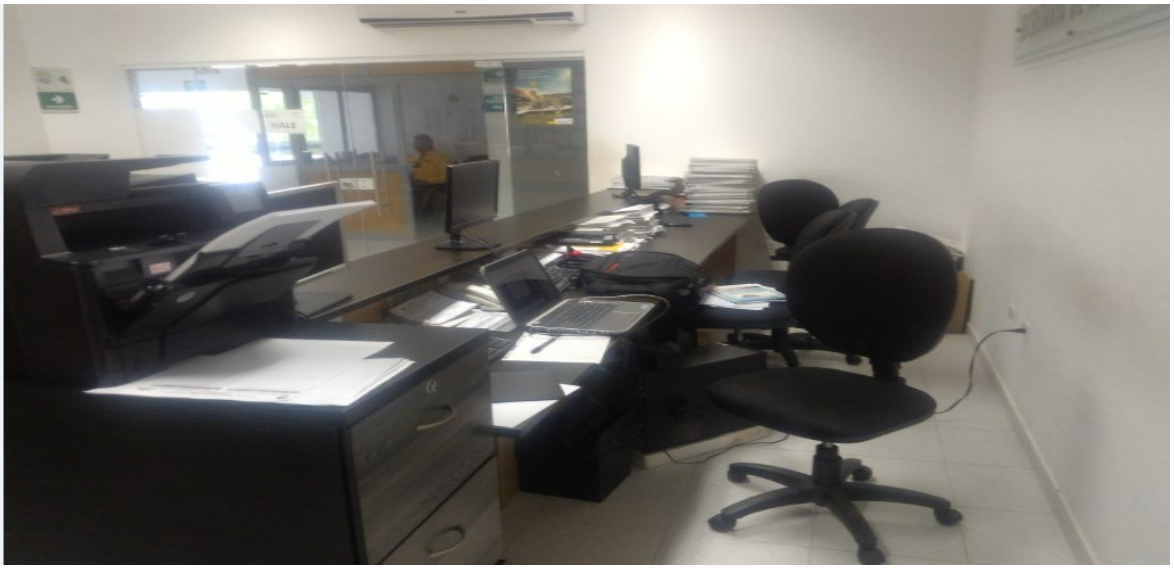
8.3 PLANEACIÓN Y REALIZACIÓN DEL DIAGNÓSTICO DE LAS BASES DE DATOS DE LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Áreas de la Secretaria de Hacienda de la Alcaldía Municipal de Los Patios, donde se realizaron las pruebas de Ethical hacking.

Figura 5. Oficina de atención a usuarios de la Secretaria de Hacienda

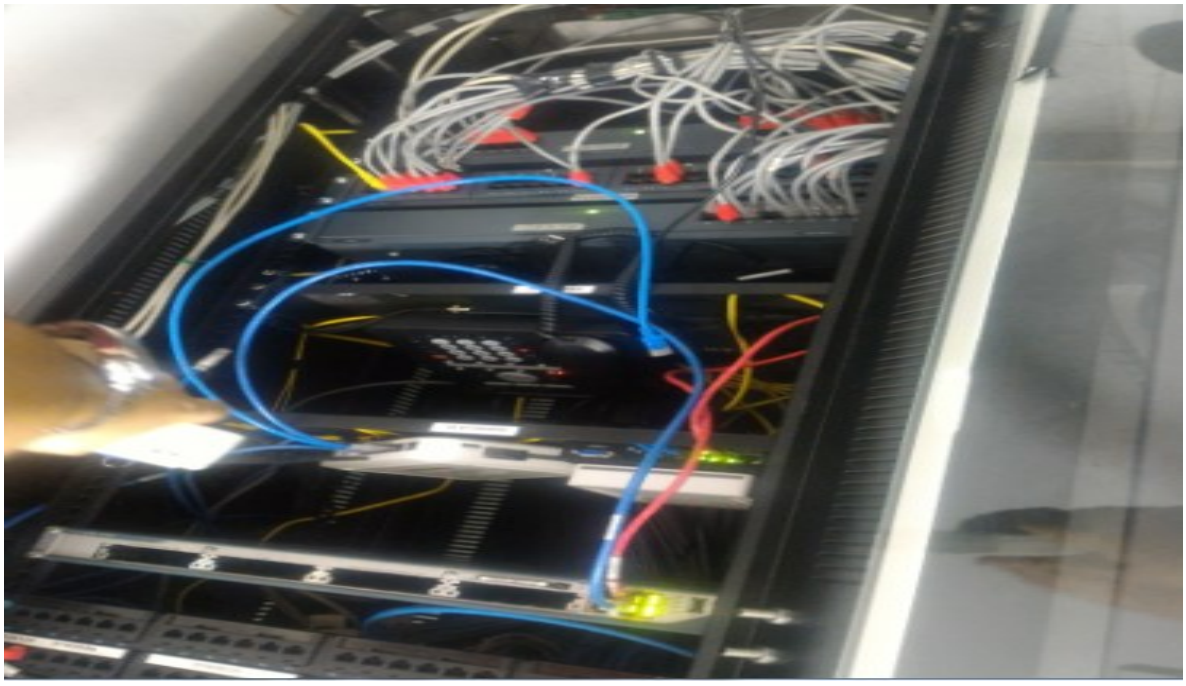
Fuente: Autoria Propia Frey Ochoa

Figura 6. Entorno de Trabajo de los funcionarios de la Secretaria de Hacienda



Fuente: Autoria Propia Frey Ochoa

Figura 7. Rack 1



Fuente: Autoria Propia Frey Ochoa

Como se nuestra en la figura el Rack Número uno, está constituido por:

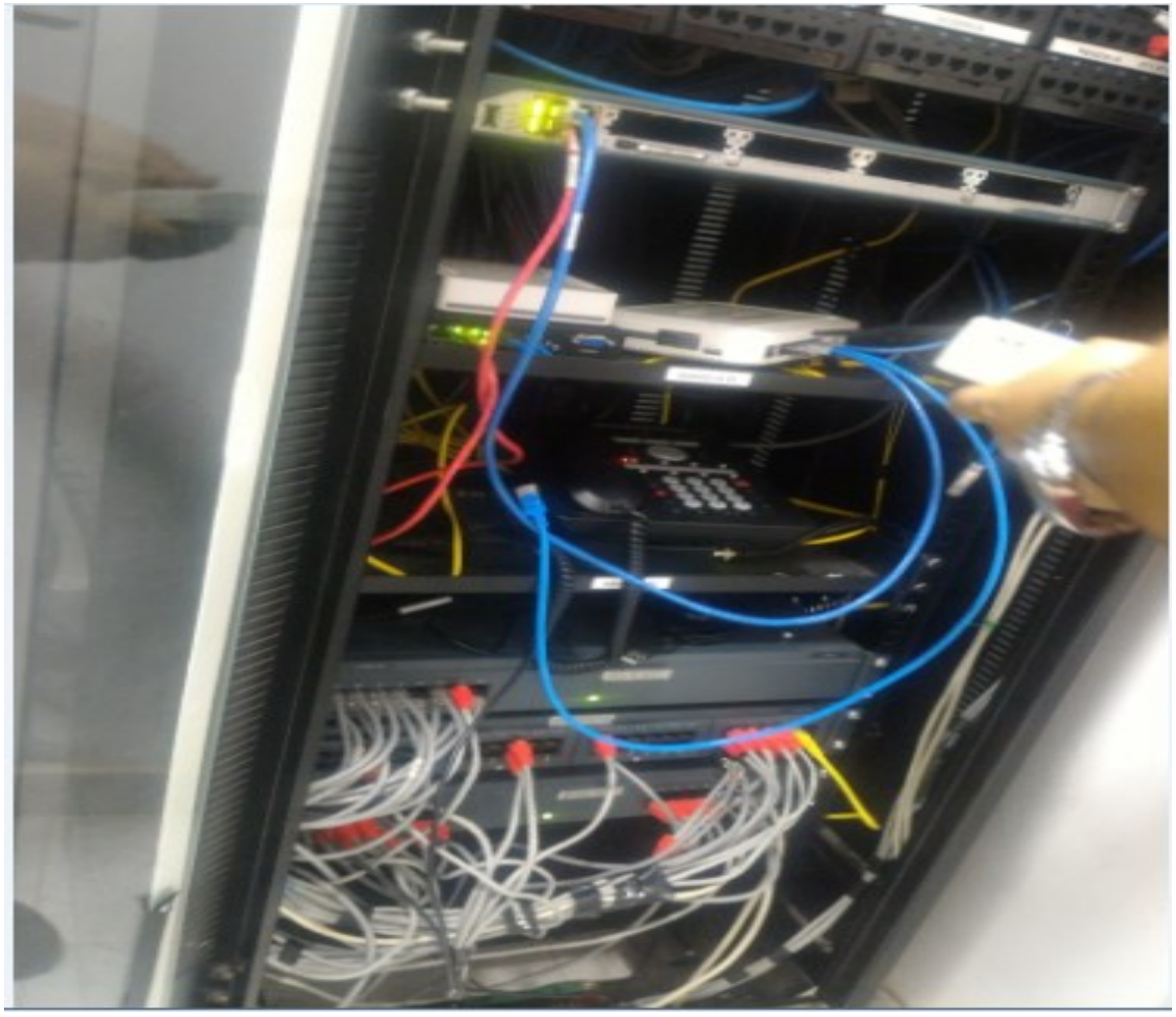
- Tres Switches Marca DLINK.
- Dos Router.
- FIREWALL Marca Sonny Wall Z 205.
- Central Telefónica con proveedor TELECOM.
- Enrutador de Fibra Óptica de 10 megabytes.

Figura 8. Cuarto de Seguridad de Hardware y Servidores

Fuente: Autoria Propia Frey Ochoa

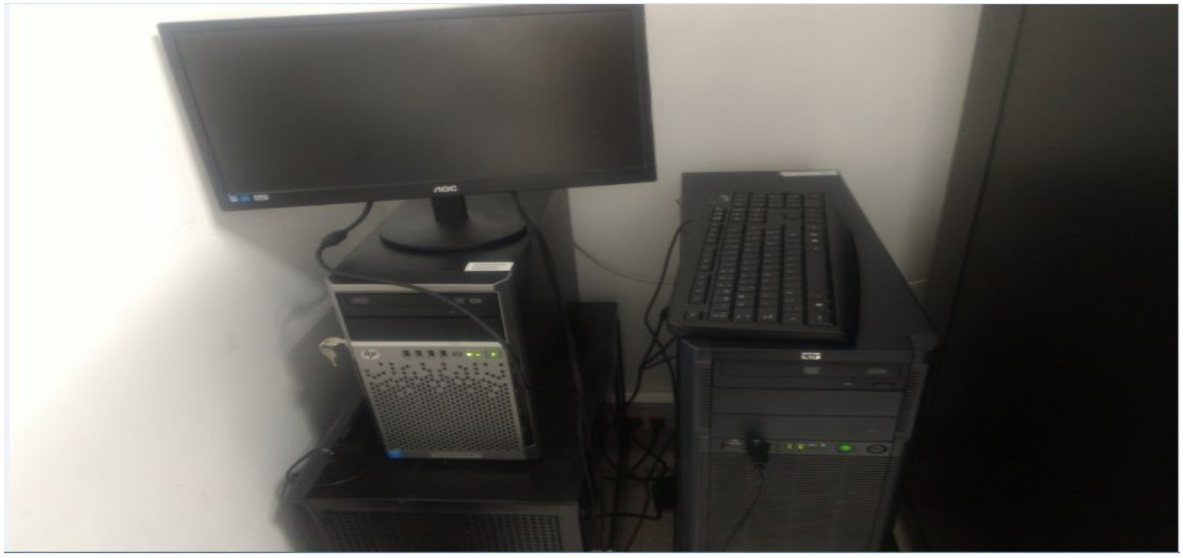
Como se observa en la figura, en la secretaria de hacienda Municipal existe un cuarto donde se encuentra ubicados los servidores y el rack donde están los accesorios necesarios para el funcionamiento del sistema.

Figura 9. Ubicación de los Switches y Reuters



Fuente: Autoria Propia Frey Ochoa

Figura 10. Servidor Marca Hp Modelo Proliant Ml 110



Fuente: Autoria Propia Frey Ochoa

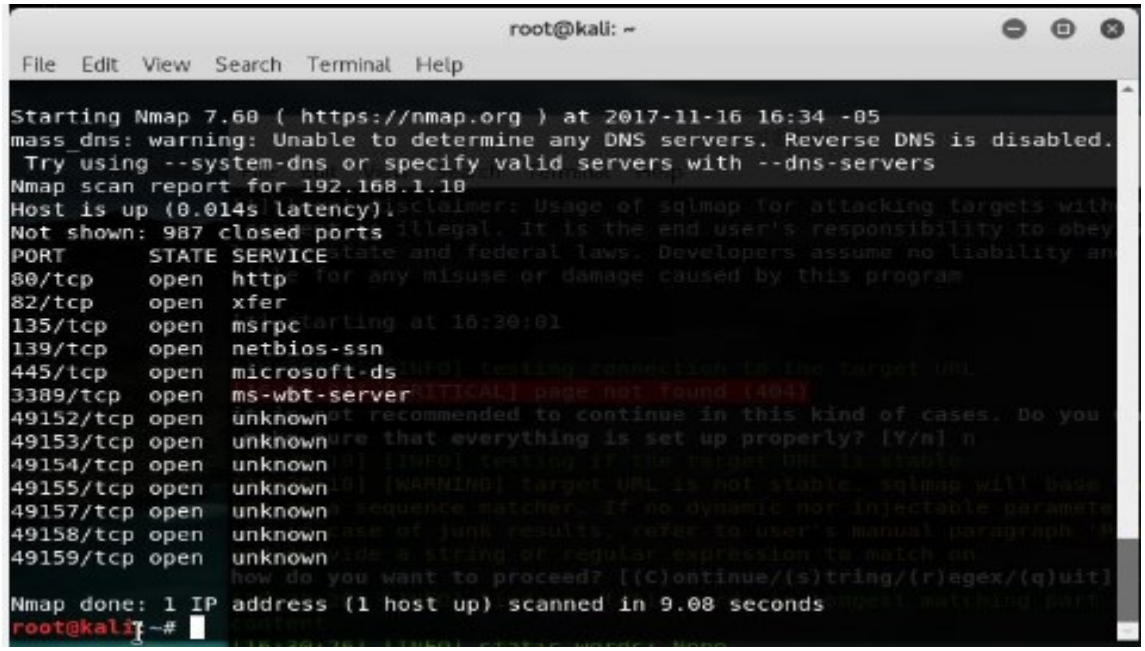
8.4 APLICACIÓN DE LAS TÉCNICAS NECESARIAS PARA LAS METODOLOGÍAS *PEN TEST Y ETHICAL HACKING*, PARA BRINDAR UN BUEN DESARROLLO INFORMÁTICO EN LA SECRETARIA DE HACIENDA MUNICIPAL

Proceso para realizar las pruebas. Una vez realizada la a los funcionarios de la Secretaria de Hacienda del Municipio de Los Patios, se procedió a realizar pruebas de penetración al servidor con la Ip 192.168.1.10, lo cual se encarga de recopilar la información recaudada en Impuestos y Cobro Coactivo, lo cual está programado con un motor de bases Firebird y un lenguaje de programación Delphi

Seguidamente se abre el entorno de la consola de Kali Linux, se procede a configurar la red en el sistema operativo Kali Linux, trabajando con la configuración

en de red en puente y asignando una red estática para luego hacer un ping entre la maquina víctima y la maquina atacante.

Figura 11. Reporte de los puertos encontrados



Fuente: Autoria Propia Frey Ochoa

Como se muestra en la figura Nmap, pemite identificar los puertos, su estado y el servicio que se esta prestando en este servidor:al permite la transferencia de hipertexto entre el servidor web y un navegador.

- El puerto 80 se encuentra activo y trabaja con el servicio http, lo cual al permite la transferencia de hipertexto entre el servidor web y un navegador.

- Se identifica el puerto 135 activo y con el servicio msrpc, que son las herramientas administrativas del DNS.

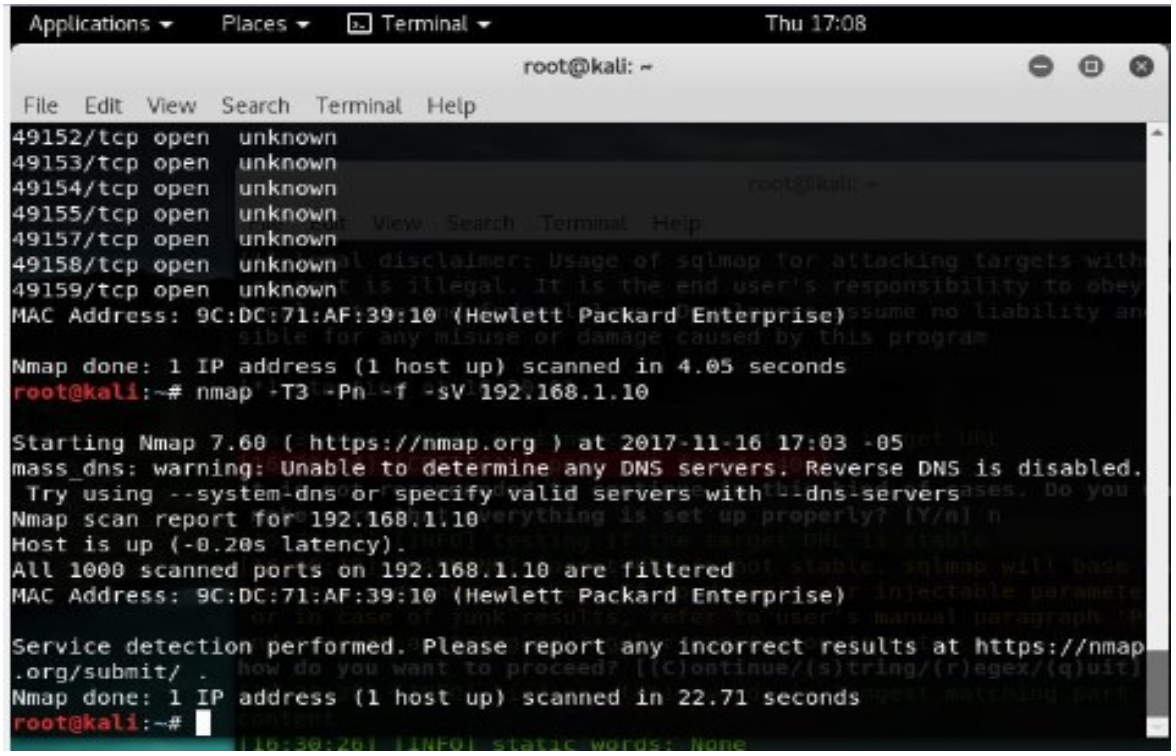
- El puerto 445/tcp, activo lo cual permite compartir registros, archivos dentro del sistema de información.

Los puertos 49152 al 49159 son puertos desconocidos que se encuentran abiertos. Con lo implementado y explorado hasta el momento, se ha analizado que el sistema es vulnerable debido a que el puertos 445 estando activo permite compartir archivos y es muy vulnerable a ataques en el sistema de información de confidencialidad y privacidad para la Administración Municipal.

Figura 12. Inicio del proceso de la explotación de las vulnerabilidades

Fuente: Autoria Propia Frey Ochoa

Figura 13. Instrucciones para mostrar con detalle la búsqueda



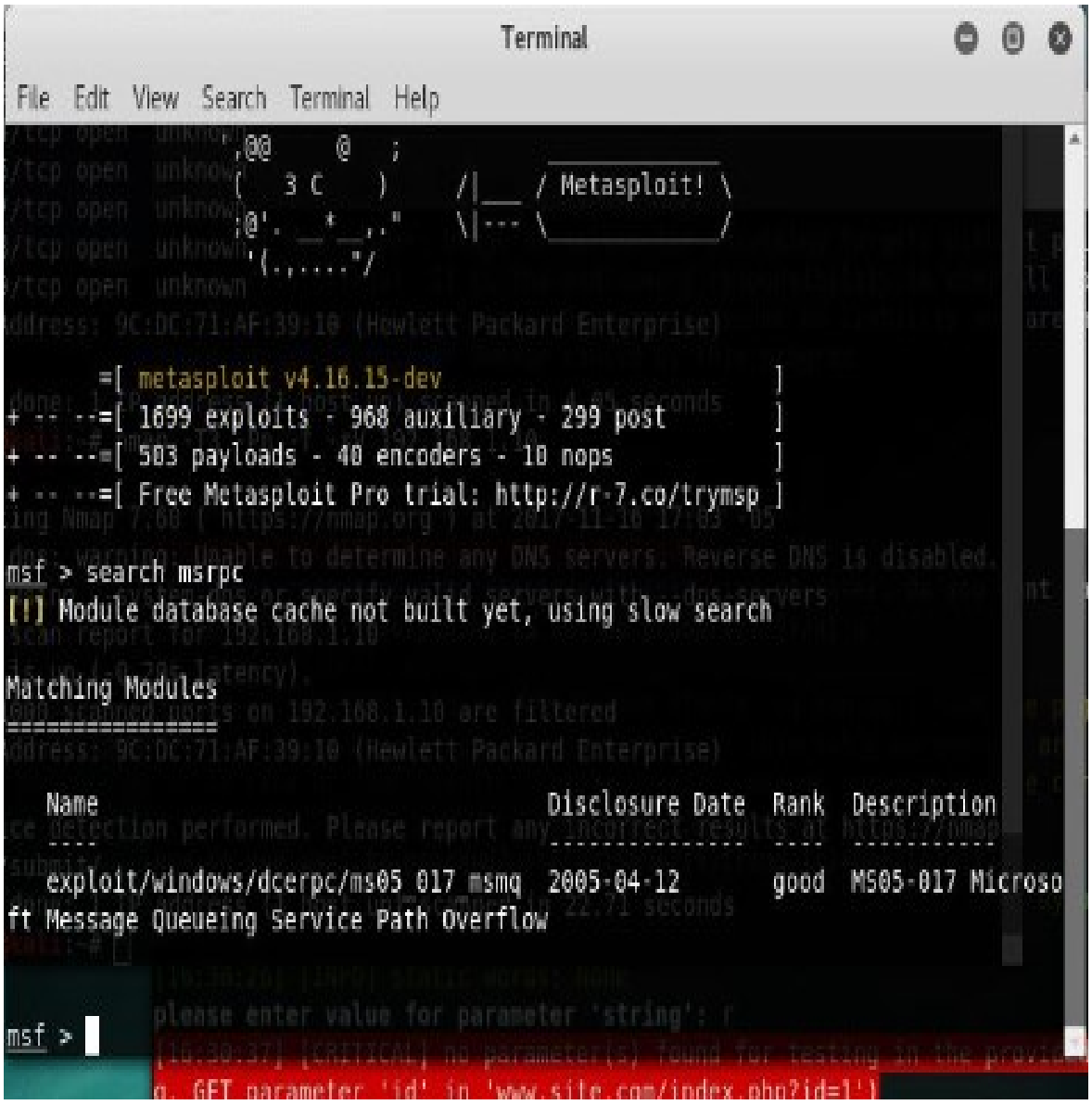
Fuente: Autoria Propia Frey Ochoa

Con la Instrucción –T3 –Pn –f -sV, se realizó un escaneo completo como lo muestra que se detectaron que todos los 1000 puertos de la dirección Ip 192.168.1.10 se filtran .

La dirección Mac: Heuler packer enterprice, los demas resultados no se evidenciaron.

La siguiente fase es hacer un exploit con la herramienta Metasplot de Kali Linux, con esta herramienta permite al auditor encontrar las vulnerabilidades que se presenten en un proceso de información.

Figura 14. Entorno inicial de Metasploit

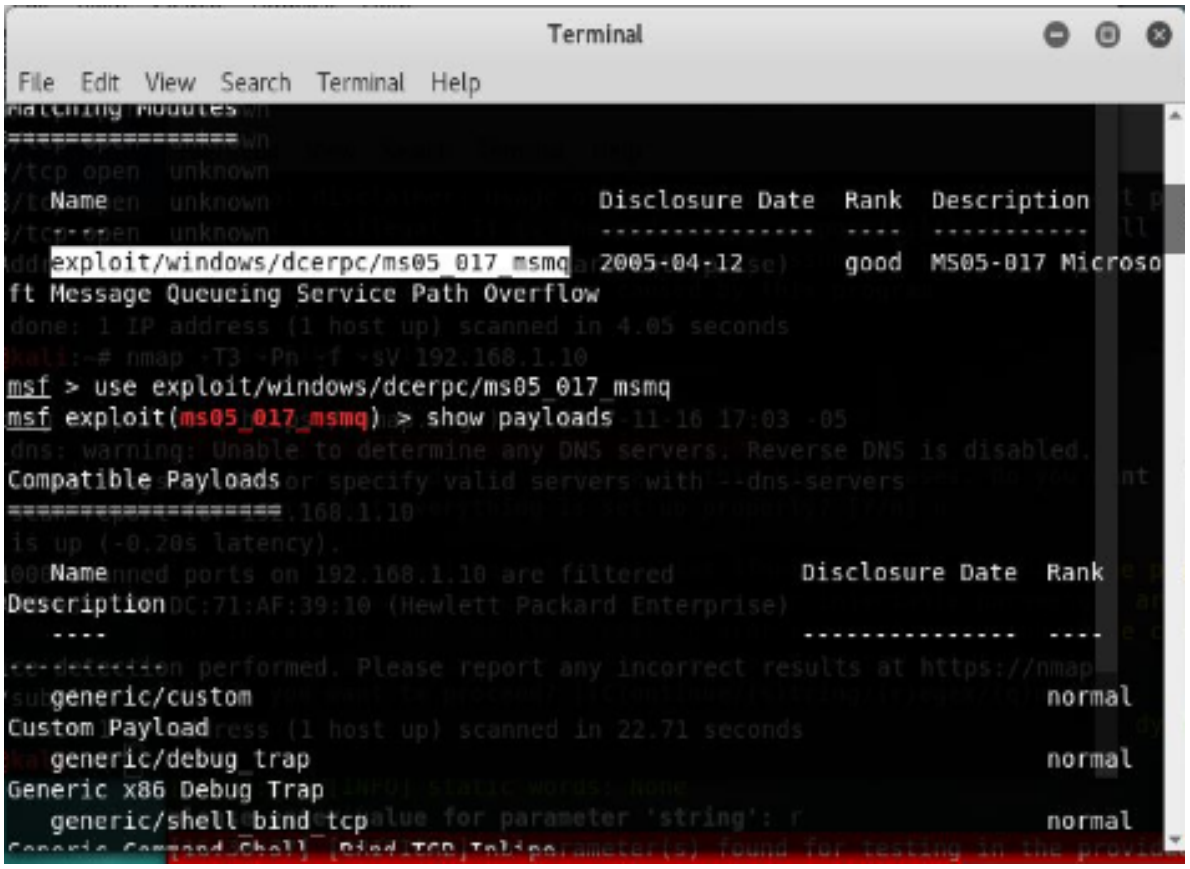


Fuente: Autoria Propia Frey Ochoa

Una vez inicia el sistema de la herramienta Metasploit, donde se muestra una serie de datos donde el auditor considera el exploit a la cual se hara los respectivos

procedimientos de codigo para cumplir con las subrutinas que el programa considere para lograr el objetivo planteado.

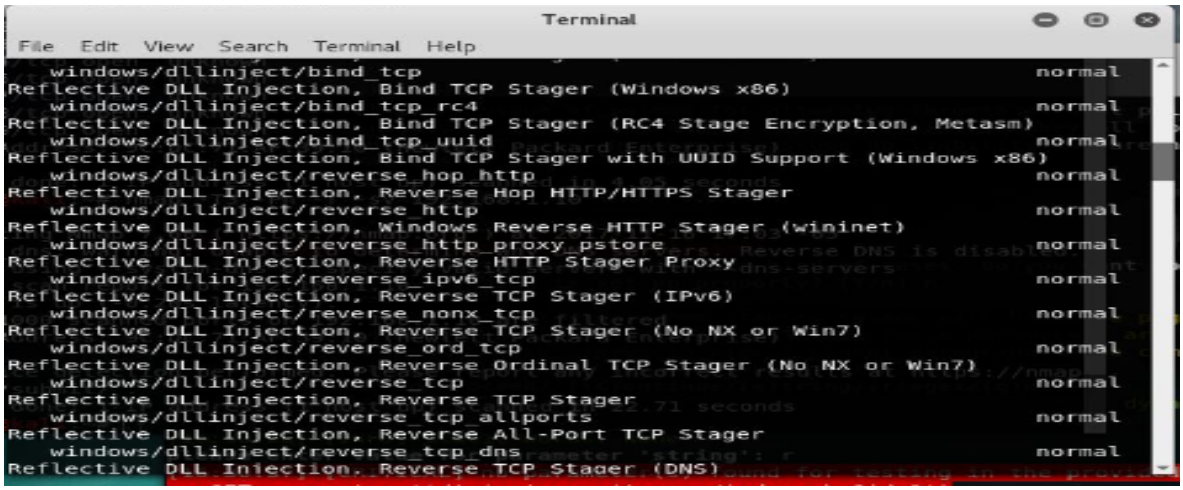
Figura 15. Identificación del exploit a Explorar



Fuente: Autoria Propia Frey Ochoa

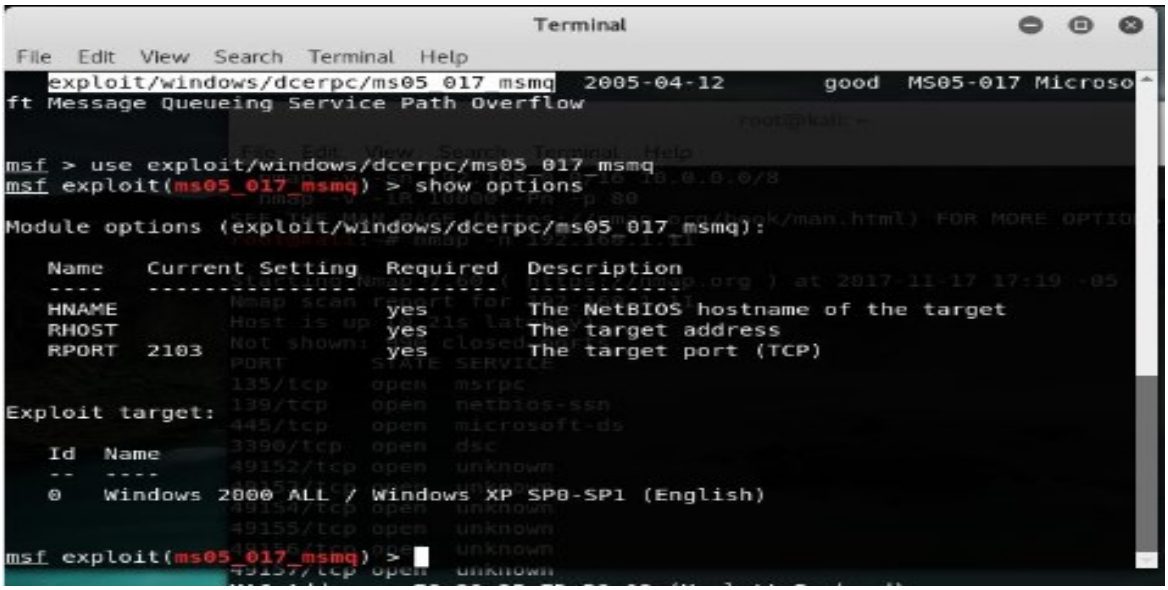
Como se observa en la figura se ha enviado la instrucción para iniciar a explorar las vulnerabilidades use/exploit/Windows/dcerpc/ms05_17 msmq, determinando el exploit en el que se inició la observación por medio del comando Show payload.

Figura 16. Identificación del Exploit



Fuente: Autoria Propia Frey Ochoa

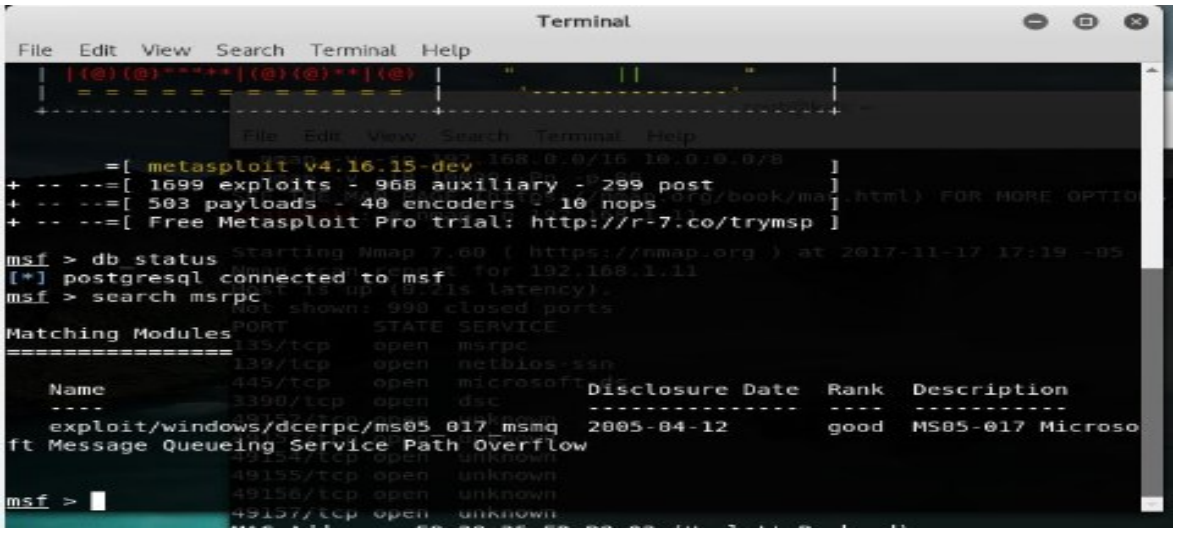
Figura 17. Uso del exploit dcerpc



Fuente: Autoria Propia Frey Ochoa

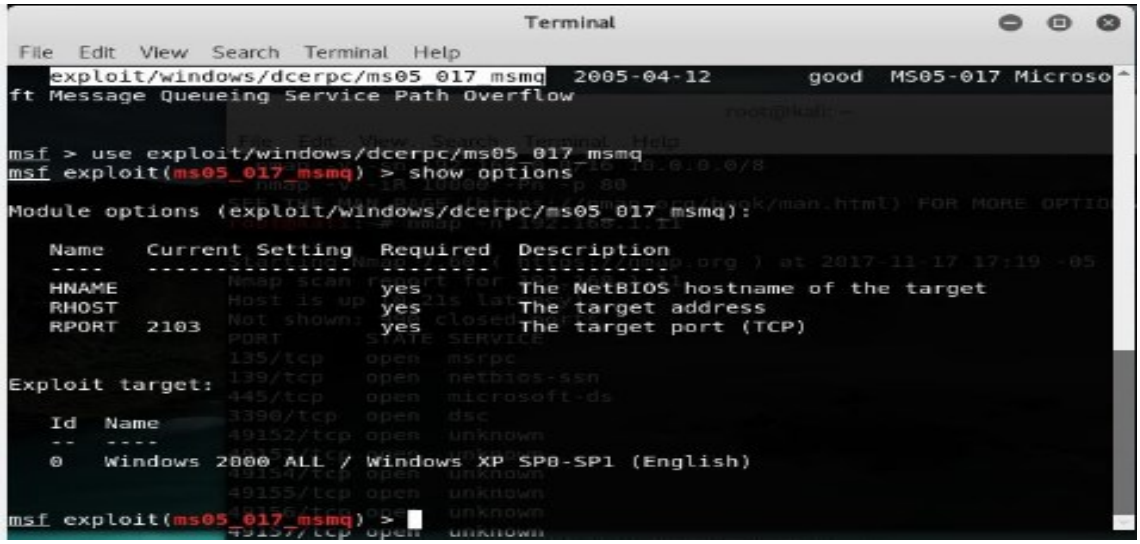
El comando show exploit, permite verificar que parámetros se deben configurar en el exploit, también se observa el funcionamiento del sistema operativo Windows Xp versión Service Pack uno.

Figura 18. Uso del comando db Status, para ingresar al motor de bases de datos postgresql



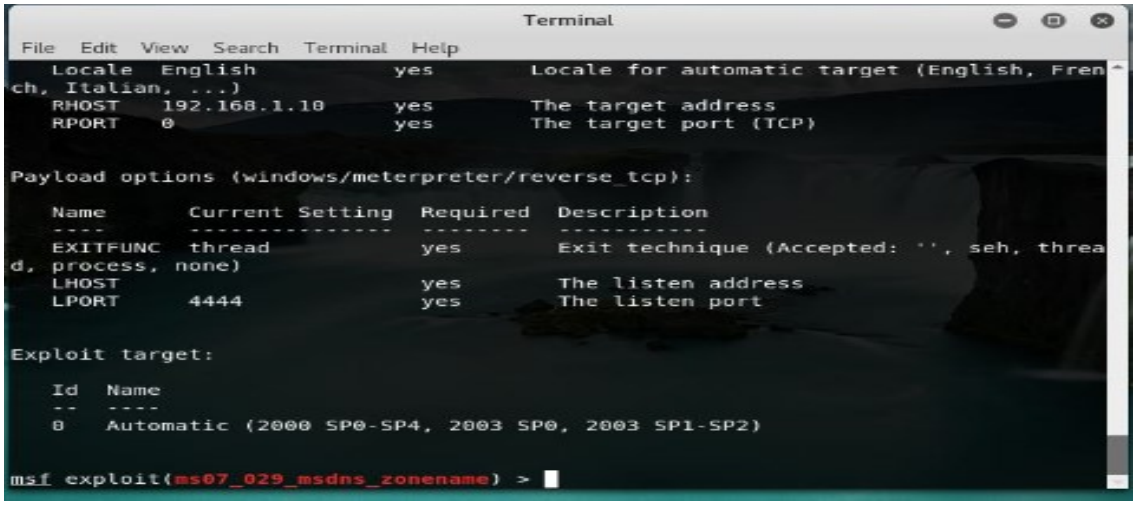
Fuente: Autoria Propia Frey Ochoa

Figura 19. Uso del comando Show Options



Fuente: Autoria Propia Frey Ochoa

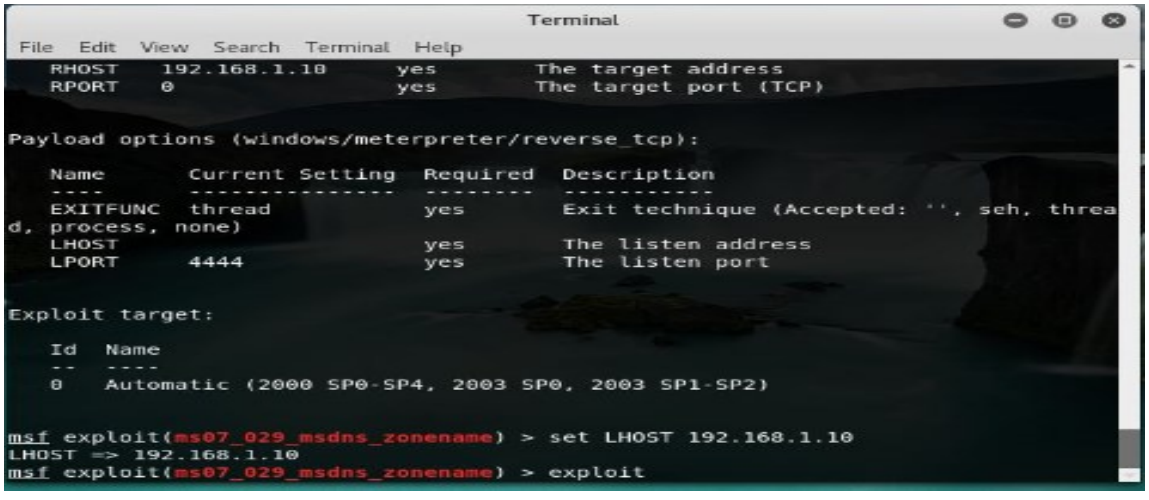
Figura 20. Uso del comando Payload



Fuente: Autoria Propia Frey Ochoa

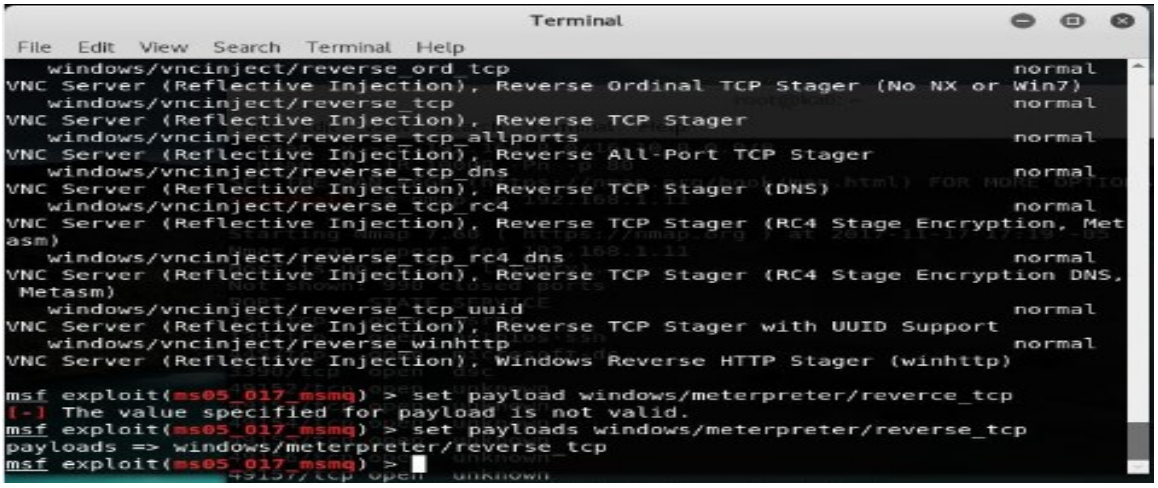
Luego se ejeuta el exploit de metasploit por medio del cual ofrece informción en el puerto 4444 con windows 2000.

Figura 21. Ejecución del Exploit



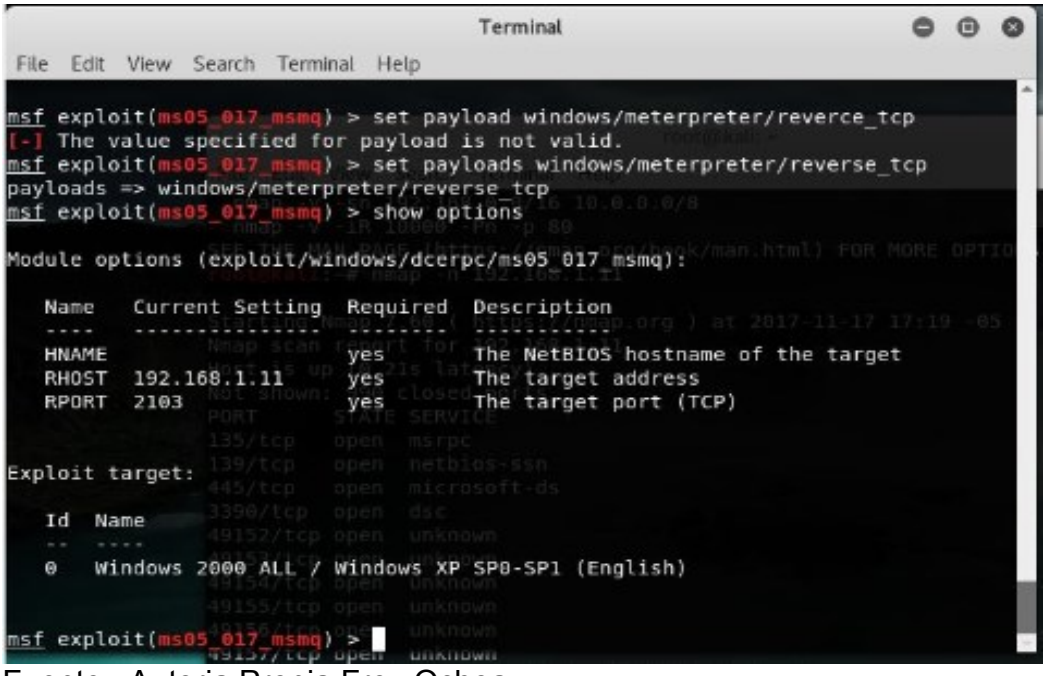
Fuente: Autoria Propia Frey Ochoa

Figura 22. Ejecución del Exploit



Fuente: Autoria Propia Frey Ochoa

Figura 23. Ejecución del Exploit

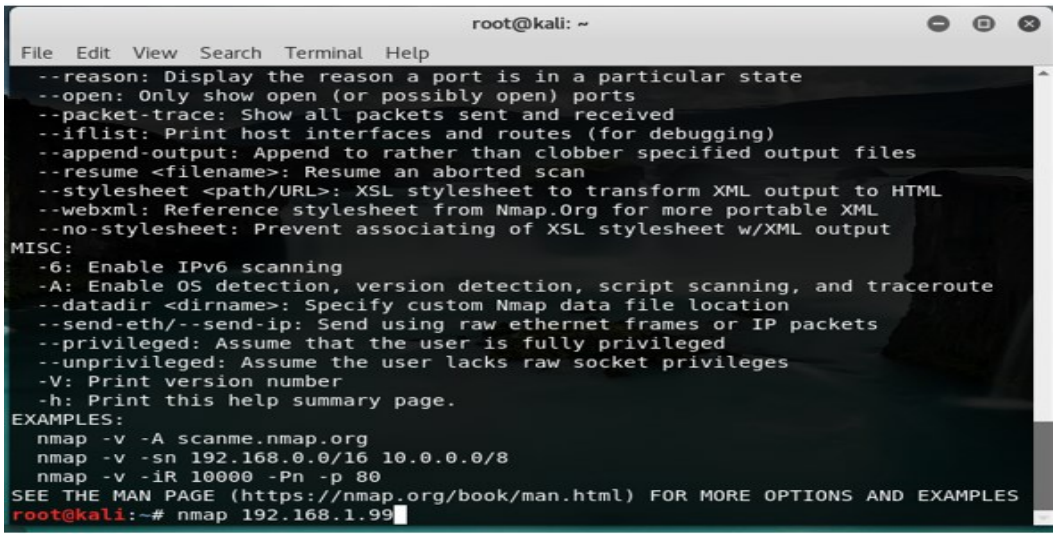


Fuente: Autoria Propia Frey Ochoa

Con la instrucción set payload windows/meterpreter/reverce_tcp, el exploit hace uso del del payload reverse_tcpse, generando una coneion inversa entre el servidor victima identificado con la dirección Ip 192.168.1.11.

Prueba al servidor Web con la IP 192.168.199. Se inicia el proceso con el nmap para proceder a escanear los puertos que se encuentran en el servidor que sera la victima a quien se hara la prueba de posibles vulnerabilidades con las herramientas del sistema opertivo Kali Linux.

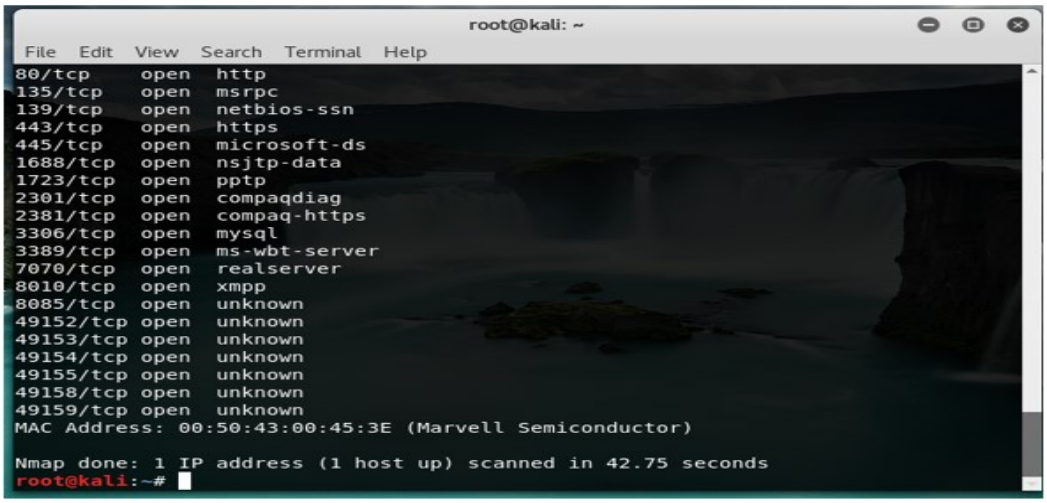
Figura 24. Inicio de Nmap



Fuente: Autoria Propia Frey Ochoa

Una vez se inicia la configuaración de la herramienta con Nmap se procede a ingresar la IP del equipo a quien se la va a ejecutar la prueba de vulnerabilidades con Kali Linux.

Figura 25. Inicio de Nmap



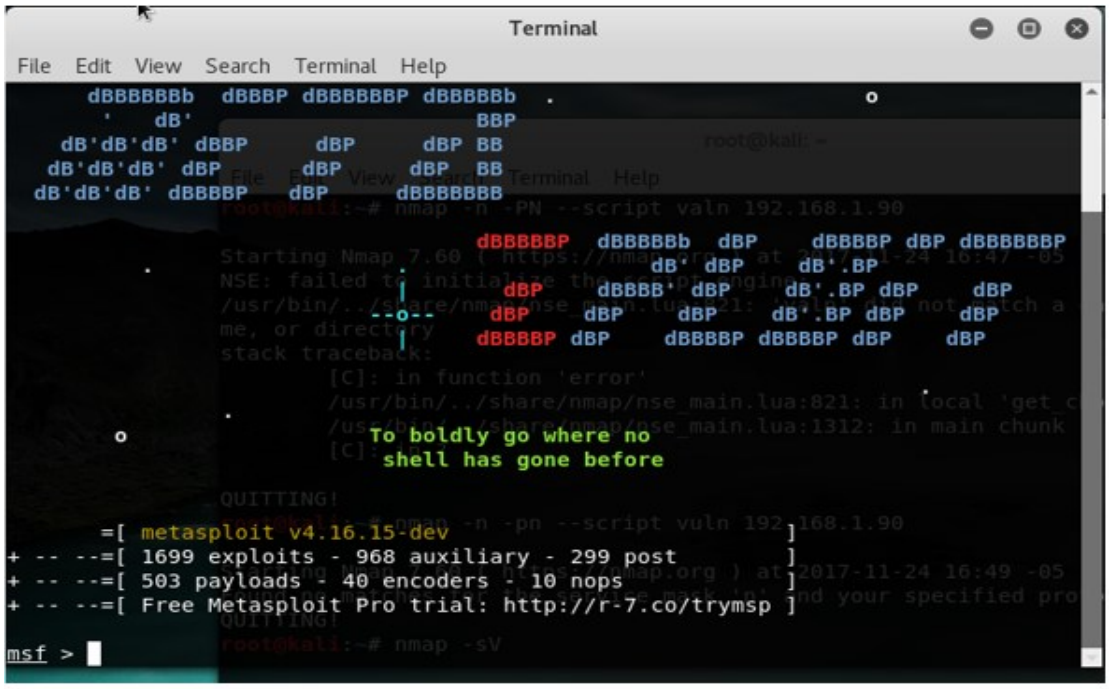
Fuente: Autoria Propia Frey Ochoa

En la figura se identifica el tipo de puerto, su estado y servicio al que se encuentra conectado, se observa que los puertos 80/tcp se encuentra activos, lo cual no e una amenaza para la información, debido a que el servidor esta protegido por un firewall que garantiza que este puerto puede estar activo.

Para el objetivo propuesto se utilizo herramientas de framewoark al servicio de mysql encontrado en el puerto 3306 y qu se encuentra activo, razon por la cual se sigue el proceso atravez de las herramientas de kali linux.

La siguiente fase es abrir el entrono grafico de Kali Linux y selecionar la herramienta de Metasploit para detectar las vulnerabilidades en el sistema.

Figura 26. Inicio de la Herramienta Metasploit de Kali Linux



Fuente: Autoria Propia Frey Ochoa

Una vez situados en el entorno de metasploit se procede a digitar el comando use para especificar el modulo especifico.

Lista de comandos de Metasploit. *help*: Con este comando se puede desplegar la lista de comandos disponibles en la consola de Metasploit, adicionalmente se puede especificar el comando seguido de *-h*, o poner *help* seguido del comando, para obtener información detallada acerca del comando específico

search: seach, se identifican los módulos que contienen dicha característica. Un pequeño truco para comprobar si está actualizado sería buscar una característica reciente para ver si se dispone de ella o no.

info: Muestra detalles del módulo (opciones, objetivos y descripción). Si se está usando ese módulo, basta con poner el comando, de lo contrario se debe especificar la ruta del módulo.

show: Muestra en pantalla las opciones del módulo. Puede ir seguido de actions, advanced, all, auxiliary, en función de las opciones específicas que se pretenden ver.

use: Selecciona el módulo. El comando *back* sirve para quitar la selección.

set: Configurar parámetros de un módulo en concreto. *Unset* sería para borrar la configuración.

setg: Configurar parámetros de los módulos a nivel global, para todos los módulos. *Unsetg* para borrar esta configuración.

connect: Sirve para desarrollar la conexión hacia otras máquinas especificando la ip + el puerto, de esta manera se puede disponer de módulos y configuraciones en otra máquina y acceder desde máquinas remotas. Esta utilidad se vale del famoso *netcat*, así que se dispone de opciones parecidas a las de netcat.

irb: Sirve para ejecutar un intérprete de *Ruby*, de esta forma se puede utilizar script de Ruby sobre msf para automatizar o facilitar el trabajo si se posee manejo en Ruby.

load: Cargar un plugin. *Unload* para la operación inversa.

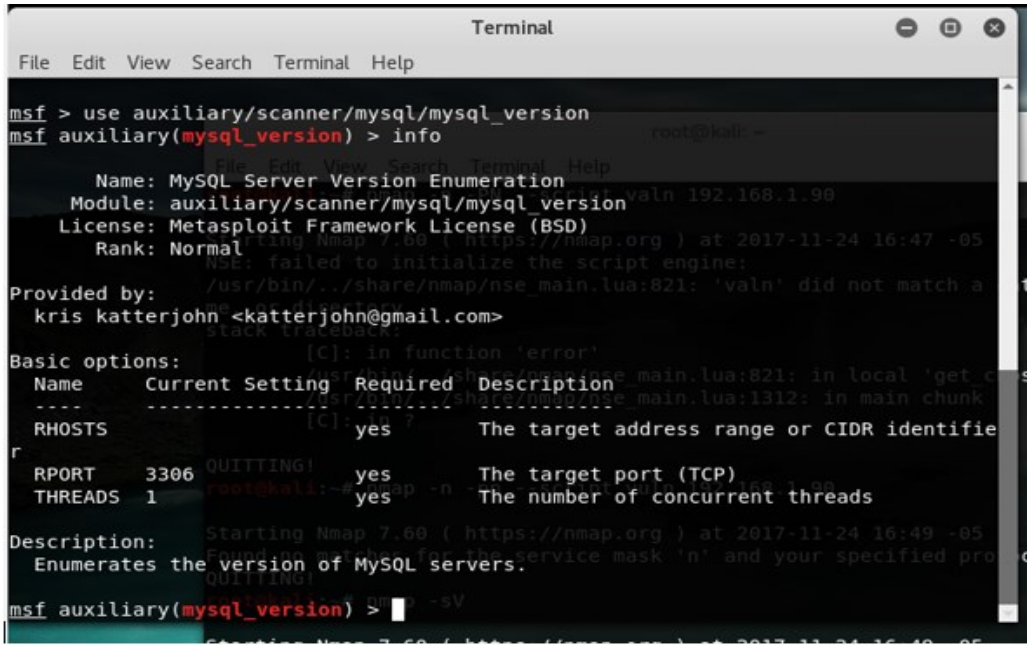
loadpath: Sirve para cargar un directorio independiente, para así tenerlo disponible también desde la consola.

check: Comprobar si es vulnerable o no antes de lanzar el script.

exploit: Lanzar el módulo. Se dispone de las siguientes opciones:

- *j*: Lo lanza en segundo plano (backround).
- *z*: Para que tras una explotación exitosa no se interactúe con la sesión.
- *e*: Se lanza el *payload* con una codificación realizada previamente con un payload.

Figura 27. Inicio de la Herramienta Metasploit de Kali Linux

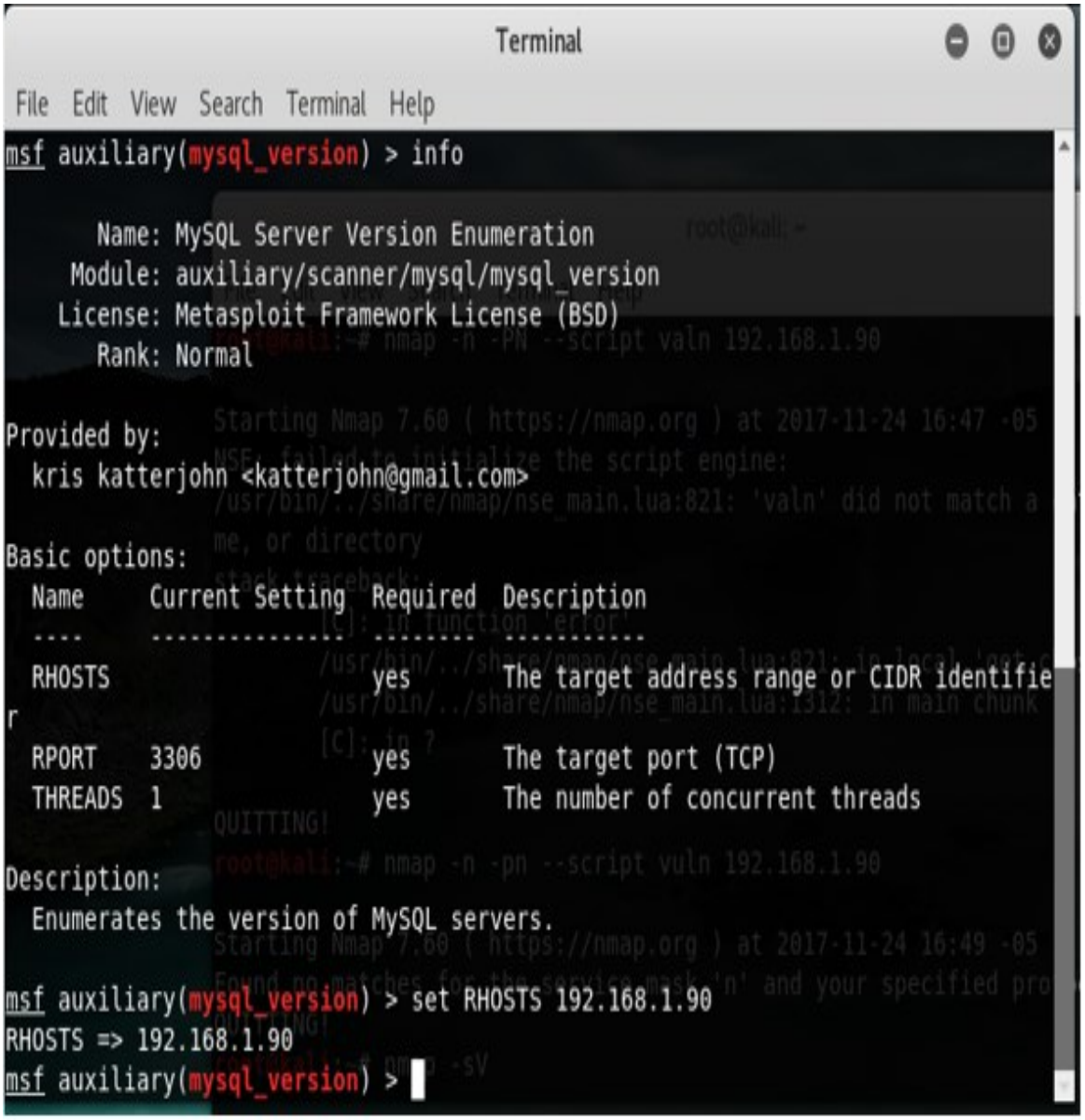


Fuente: Autoria Propia Frey Ochoa

Con el comando auxiliary/scanner/mysql/mysql_version, permite determinar la versión de mysql que se está ejecutando.

El comando info: brinda información esquemática como se muestra en la tabla de la figura, la tarjeta del puerto (tcp) en el puerto de la maquina victima en la configuración actual 3306 necesario.

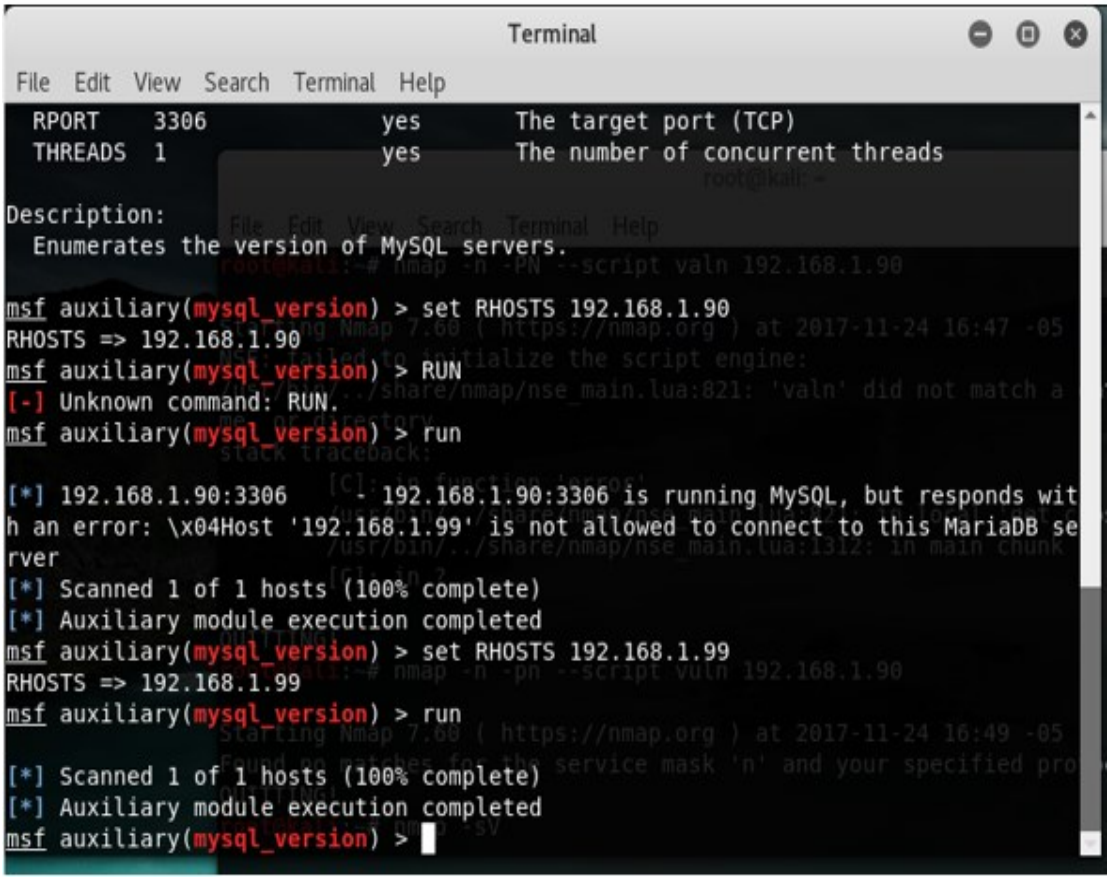
Figura 28. Inicio de la Herramienta Metasploit de Kali Linux



Fuente: Autoria Propia Frey Ochoa

En la siguiente instrucción pide ingresar la Ip de la maquina víctima, en este caso la dirección Ip del Servidor web 192.168.1.90.

Figura 29. Herramienta Metasploit de Kali Linux

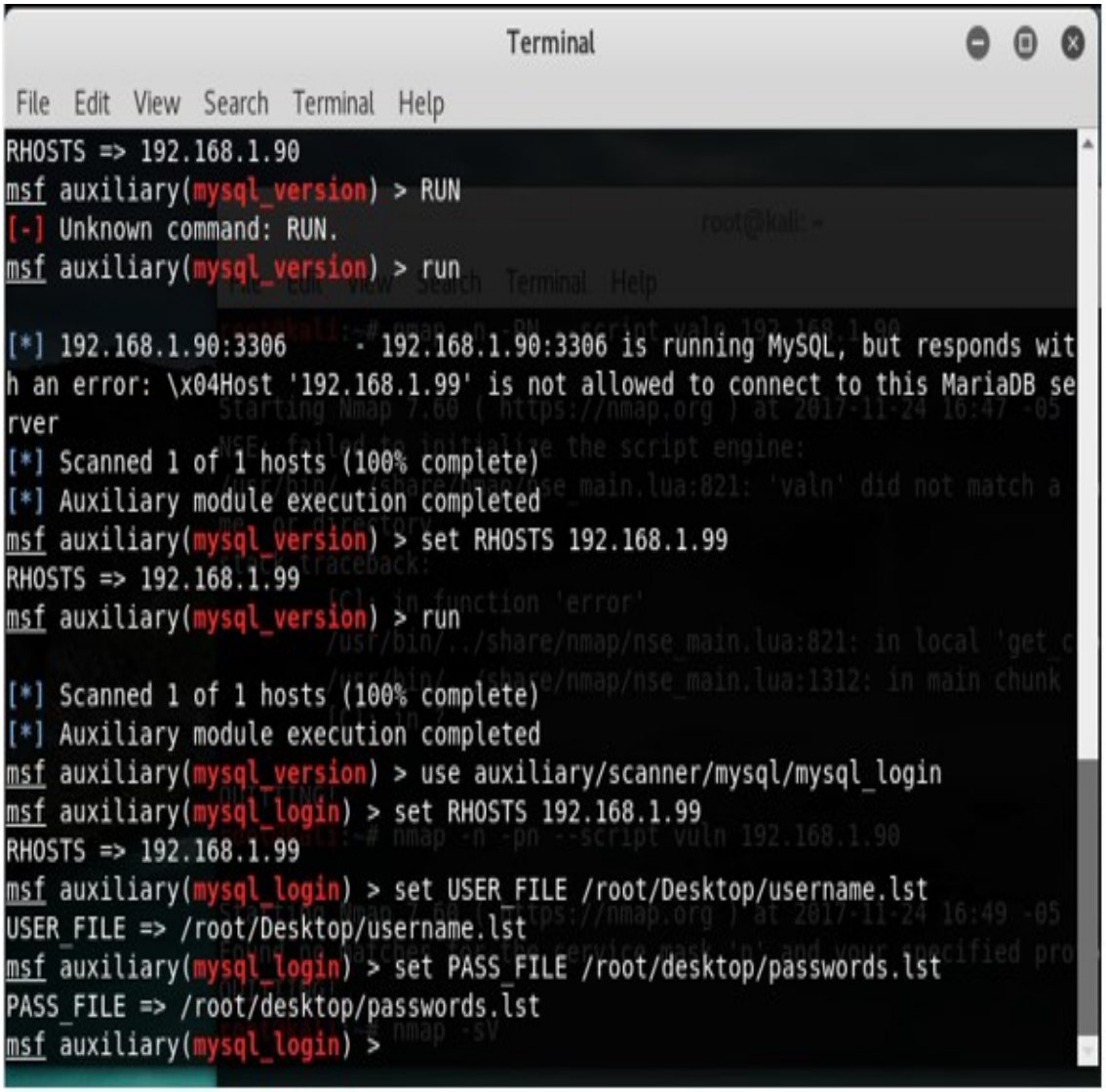


Fuente: Autoria Propia Frey Ochoa

Una vez ingresado el comando set para establecer y mostrar las variables de entorno junto a la Ip de la víctima se ejecuta con el comendo Run.

Como se observa en la dirección Ip 192.168.1.90 no se puede conectar a este servidor con la dirección Ip 192.168.199 que es el servidor web, indica que la ejecución de modulas auxiliares ha sido ejecutada en un 100 por ciento y se ha escaneado uno de un host anfitrión.

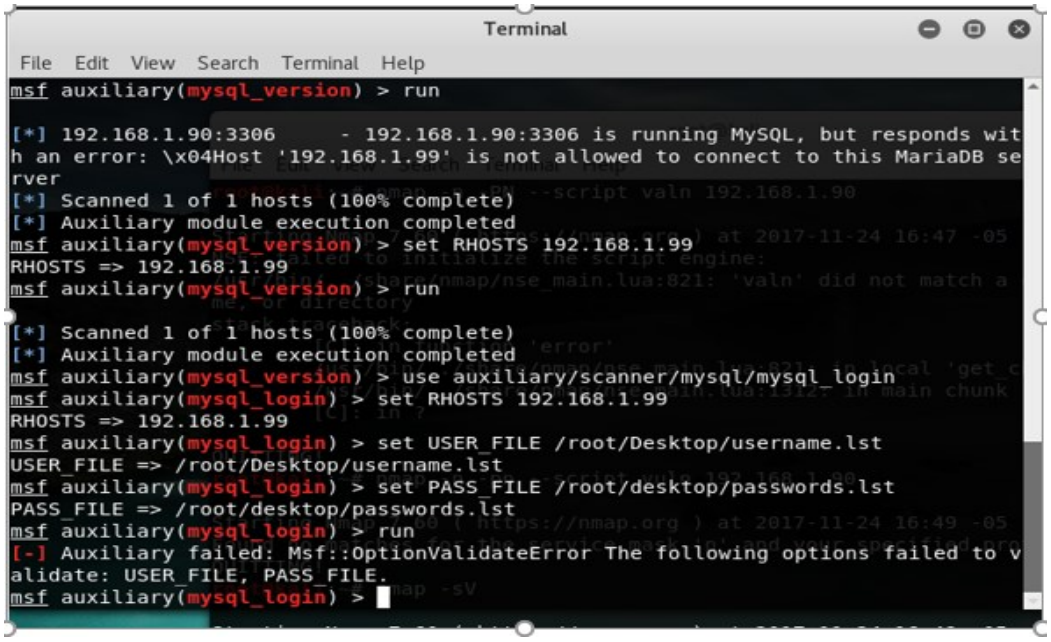
Figura 30. Herramienta Metasploit de Kali Linux



Fuente: Autoria Propia Frey Ochoa

Con el comando use auxiliary/scanner/mysql/mysql_login se indica al Host victima el inicio de sesion, luego se pide que establezca y liste el nombre de usuario, de igual manera se repite el procedimiento para la clave o contraseña de usuario.

Figura 31. Herramienta Metasploit de Kali Linux Solicitud de Contraseña de usuario



Fuente: Autoria Propia Frey Ochoa

8.5 ESULTADOS DEL PROYECTO ESPERADO

Una vez hecho todo el procedimiento se ejecuta la aplicación demuestra que las opciones no pueden validar la información solicitada.

Vulnerabilidades encontradas:

- El puerto 80/tcp se encuentra habilitado, facilita la entrega de información, puede ser vulnerable a ataques de Fuerza bruta, Denegación de Servicio (DoS), puede existir la posibilidad de que se produzca un sniffer.

- El puerto 3389/TCP, existe la posibilidad de obtener una información sobre vulnerabilidades por tener puntos de acceso de fácil ingreso a la información.

- Por el puerto 139/tcp, puede existir la posibilidad de presentarse una denegación de servicio (DoS).

- Las Bases de datos son locales, no existe un motor de bases de datos que suministre y valide la información.

- El Sistema no cuenta con un esquema de seguridad lógica, que mitigue el riesgo de infiltración de usuarios no registrados y autorizados.

- El hardware de los equipos de Cómputo se encuentra en un estado obsoleto de la tecnología actualizada.

- La red interna de la secretaria de Hacienda tiene un sistema de cableado expuesto a cualquier tipo de daño físico.

- El sistema no se encuentra protegido por un por un antivirus propio o pago, solo se activa un antivirus gratuito, lo cual no garantiza la seguridad de la información.

9. CONCLUSIONES

En la secretaria de Hacienda Municipal de Los Patios, existen falencias con la integridad y la confidencialidad de la información que a diario se procesa en eta entidad pública, este es el resultado de las encuestas realizadas a los funcionarios que procesan la información y la almacenan en las bases de datos, es por esto la importancia y la necesidad de haber presentado las metodologías de Pen test y de Ethical hacking en la organización.

Se determinaron metodologías de Pen Test y Ethical Hacking, teniendo en cuenta cada una de las características y funcionalidad de las mismas, además la herramienta inmersa en cada sistema operativo seleccionado para para las pruebas de penetración como lo es Nmap y Kali Linux, que contiene un paquete interno de herramientas muy seguras y robustas para el estudio analizado a las bases de datos en la Secretaria de Hacienda del Municipio de Los Patios.

Se identificaron las bases de datos existentes que se maneja en la secretaria de Hacienda Municipal de Los Patios, encontrando por medio de las pruebas Ethical hacking, el mal estado y funcionamiento en que se encontraban los servidores y el rack; con dicho análisis realizado a los servidores web, se logró identificar cada uno de los puertos por medio de un escaneo con herramientas sofisticadas como las mencionadas en el capítulo anterior para la seguridad Informática.

Para la aplicación y determinación de técnicas necesarias para la implementación de las metodologías Pen Test y Ethical Hacking, se utilizó un laboratorio virtual trabajando con los componentes técnicos en cada una de las herramientas utilizadas para las pruebas de Pen test, encontrando vulnerabilidades existentes en los sistemas de información de la Secretaría de Hacienda Municipal.

10. RECOMENDACIONES

Después del desarrollo de la investigación, se identifica la necesidad de indicar una serie de recomendaciones basadas principalmente los aspectos que se han identificado en el procedimiento que se llevó a cabo, entre ellas están:

- Implementar un plan de contingencia donde se haga con frecuencia el mantenimiento preventivo a los equipos y hardware que comprende el sistema de información en la Secretaria de Hacienda Municipal.

- Realizar periódicamente pruebas de penetración por medio de metodologías Pen Test y Ethical Hacking, para evaluar las vulnerabilidades que se están presentando y, así poder tomar las medidas pertinentes para salvaguardar la información suministrada y guardada en los servidores de la Secretaria de Hacienda Municipal.

- Se recomienda al Administrador del sistema, implementar una máquina virtual que le permita hacer una simulación sobre el estado y funcionamiento del sistema operativo instalado, como están funcionando los puertos de acceso a la información, trabajar con direcciones Ip estáticas y establecer un sistema de control de usuarios al sistema de información, donde se maneje los datos de la información recaudada por cada una de las transacciones y operaciones informáticas dentro de la Secretaria de Hacienda Municipal.

- Establecer un sistema de control de usuarios al sistema de información, donde se maneje los datos de la información recaudada por cada una de las transacciones y operaciones informáticas dentro de la Secretaria de Hacienda Municipal.

- Contratar un proveedor de software que permita implementar una base de datos, donde se refleje la información pública y que permita realizar consultas a cada usuario que lo solicite.

- Implementar un Firewall que permita mitigar los ataques a la información por medio de dispositivos y atreves de la plataforma Web. Así mismo se plantea mejorar el sistema de cableado existente debido a que presentan falencias en las redes instaladas, para garantizar el tráfico de la información.

- Implementar una Base de Datos con un motor de capacidad de almacenamiento y consulta en un tiempo relativamente corto. Igualmente se recomienda hacer un mantenimiento rutinario al software que se encuentra en cada uno de los equipos que están en la red interna.

Por último, se instalar en los equipos de cómputo un antivirus con un proveedor, que garantice la protección de la información que ingresa a través del hardware y software a los servidores de la red.

BIBLIOGRAFÍA

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Fortalecimiento de las TI de la información en la gestión del Estado y la información pública [en línea]. [Citado 15 de octubre de 2016]. Disponible en Internet en: http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-657.html

FERNÁNDEZ, E. Metodología para el diseño de bases de datos seguras. La Mancha: Universidad de Castilla, 2002.

MÉNDEZ, C. Metodología de la investigación para ciencias empresariales. Bogotá: Mc Graw Hill, 2003.

MOJICA, M. Implementación y administración del sistema de información del Ministerio de Educación Nacional SICIED (sistema interactivo de consulta de infraestructura educativa). Trabajo de Grado. Ingeniero de Sistemas. San José de Cúcuta: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Ingeniería de Sistemas, 2011.

MONTERO, H. Técnicas del penetration testing [en línea]. [Citado 18 de octubre de 2016]. Disponible en Internet en: http://www.cybsec.com/upload/VictorMontero-SeminarioTecnicasdelPenetrationTestingArgentina.pdf

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. ISO/IEC 17799:2005. Bogotá: ISO.

PÉREZ, M. (2012). Módulo 3: auditorías y seguridad. tema 4: comparativa metodologías auditorías y pentesting. Elche: Campus Virtual.

REYES, A. Ethical Hawking [en línea]. [Citado 18 de octubre de 2016]. Disponible en Internet en: https://www.seguridad.unam.mx/descarga.dsc?arch=2776

RSS ENTRIES. Gestión de Riesgo en la Seguridad Informática 101 [en línea]. [Citado 25 de octubre de 2016]. Disponible en Internet en: https://protejete.wordpress.com/glosario/

SYMANTEC. Glosario de Seguridad 101 [en línea]. [Citado 25 de octubre de 2016]. Disponible en Internet en: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

TARAZONA, C. Amenazas informática s y seguridad de la información. México: Etek Internacional, 2007.

UNIVERSIDAD DE ALICANTE. (2015). Teoría de base de datos [en línea]. [Citado 18 de octubre de 2016]. Disponible en Internet en: https://si.ua.es/es/documentos/documentacion/office/access/teoria-de-bases-de-datos.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Lección 6 Las Entidades territoriales [en línea]. [Citado 15 de octubre de 2016]. Disponible en Internet en: http://datateca.unad.edu.co/contenidos/109107/Contenido_en_linea/leccin_6_las_entidades_territoriales.html

VELASCO, A. El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la Norma ISO 27001 [en línea]. [Citado 18 de octubre de 2016]. Disponible en Internet en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013&lng=en&nrm=iso

ANEXOS

Anexo A. Lista de chequeo

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

LISTA DE CHEQUEO

No.	Variables	Cumple		Observaciones
		Si	No	
1.	Existe algún sistema de seguridad en la base de datos.		x	
2.	Se implementan metodologías para fortalecer la seguridad de la base de datos.		x	
3	Se realizan diagnósticos constantes sobre la protección hacia la base de datos.		X	
4.	Los funcionarios aplican técnicas metodológicas para el eficiente desarrollo informático		X	
5.	Existen planeaciones periódicas frente a la información de la Secretaria de Hacienda.	X		
6.	Frente a las falencias existentes se ha presentado actuaciones pertinentes.	X		SE SOLICITA AL PROVEEDOR PARA REALIZAR LOS AJUSTES NECESARIOS
7.	Existe un plan de Contingencia para el caso de caída del sistema momentáneo.	X		
8	Existe un Firewall para cada implementación en el sistema		X	SOLO PROTEGE EL WEB-SERVER
9	Se hace capacitaciones periódicas al persona encargado en el área especifica	x		
10	¿Se cuenta con un Inventario de Activos en el centro de cómputo de la Secretaria de Hacienda Municipal?	x		
11	¿Con que frecuencia se revisa el inventario?	x		
12	¿Se lleva una Bitácora de los Equipos?		x	
13	¿Cuenta con servicio de mantenimiento a los Equipos?	X		
14	¿se lleva control de Garantía de los Equipos de Computo	X		
15	¿Se cuenta con un sistema de seguridad para el ingreso al área de informática	x		UNICAMENTE PARA EL ACCESO AL DATA CENTER
16	El motor de Bases de Datos existente esta protocolizado y estandarizado	X		

No.	Variables	Cumple		Observaciones
		Si	No	
17	¿Existe un usuario responsable de los accesos a documentos privados dentro de la secretaria?	X		UNICAMNETE ADMINIDTRADOR DEL SISTEMA
18	¿El personal que manipula la información es especializado en el área de informática?		X	
19	¿Con que frecuencia se hace copias de Seguridad?	X		
20	¿El sistema de tierra garantiza la seguridad de los equipos de cómputo en el área?	X		
21	¿Se han presentado inconsistencias en el manejo de la información?	X		

Anexo B. Encuesta

UNAD Universidad Nacional Abierta y a Distancia

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: Wilson Hernández Blanco

CARGO: Técnico Operativo TI

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ( )

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si ( )

b. No (X)

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si (X)

b. No ( )

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas ( )

b. Ataques informáticos ( )

c. Vulneraciones a los sistemas de información (X)

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ( )

b. No (X)

88'228.647

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: Elizabeth Rojas villa

CARGO: Asesora

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ( )

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si ( )

b. No (X)

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si (X)

b. No ( )

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas (X)

b. Ataques informáticos (X)

c. Vulneraciones a los sistemas de información ( )

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ( )

b. No (X)

Elizabeth Rojas villa

Nov. 17 2014

Universidad Nacional Abierta y a Distancia

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: Luz Carmenza Rodriguez Ch.

CARGO: Profesional Universitario – Contador

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ( )

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si (X)

b. No ( )

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si (X)

b. No ( )

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas (X)

b. Ataques informáticos ( )

c. Vulneraciones a los sistemas de información ( )

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ( )

b. No (X)

Luz Carmenza Rodriguez Ch.
Nov. 17 2014

Universidad Nacional Abierta y a Distancia

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: Martin David Velasco Q

CARGO: Profesional Universitario.

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ( )

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si (X)

b. No ( )

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si (X)

b. No ( )

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas (X)

b. Ataques informáticos ( )

c. Vulneraciones a los sistemas de información ( )

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ( )

b. No (X)

Martin David velasco.

Nov 17 2017

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: INGRID YULIETH PALENCIA VELASCO

CARGO: SECRETARIA

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ( )

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si ( )

b. No (X)

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si ( )

b. No (X)

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas (X)

b. Ataques informáticos ( )

c. Vulneraciones a los sistemas de información ( )

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ( )

b. No (X)

Nov 17/14.

Universidad Nacional Abierta y a Distancia

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: Eustagio pabon Glues.

CARGO: Tesorero.

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ○

b. No ○ No conosco.

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si ⊗

b. No ○

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si ⊗

b. No ○

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas ⊗

b. Ataques informáticos ⊗

c. Vulneraciones a los sistemas de información ○

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ⊗

b. No ○

Nov 17/17

Universidad Nacional Abierta y a Distancia

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: Nubia Esperanza Peña Rangel.

CARGO: Técnico Administrativo

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ◯

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si (X)

b. No ◯

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si (X)

b. No ◯

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas (X)

b. Ataques informáticos ◯

c. Vulneraciones a los sistemas de información ◯

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ◯

b. No (X)

Nov 17 17

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: Dima Carolina Cordoba Colmenares

CARGO: Secretaria

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ( )

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si ( )

b. No (X)

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si ( )

b. No (X)

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas (X)

b. Ataques informáticos ( )

c. Vulneraciones a los sistemas de información ( )

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ( )

b. No (X)

Dima Cordoba.
20.17-17

ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS

Encuesta

ENTIDAD: Secretaria de Hacienda

NOMBRE FUNCIONARIO: William Alfonso Cerena

CARGO: Prof. Universitario

1. En la Secretaria de Hacienda Municipal en la Alcaldía del Municipio de Los Patios se utiliza la metodología Pen Test y Ethical Hacking

a. Si ( )

b. No (X)

2. Se han presentado obstáculos o dificultades en el desarrollo de procedimientos conforme a la seguridad en la base de datos.

a. Si (X)

b. No ( )

3. Desde su punto de vista profesional cree que es pertinente implementar una serie de metodologías adecuadas para la seguridad en la base de datos.

a. Si (X)

b. No ( )

4. ¿Qué tipo de falencias se han presentado en la institución sobre la seguridad de los datos?

a. Amenazas ( )

b. Ataques informáticos (X)

c. Vulneraciones a los sistemas de información ( )

5. Han existido acciones pertinentes por parte de la organización para combatir este tipo de situaciones.

a. Si ( )

b. No (X)

NOV 17/17

RESUMEN ANALITICO ESPECIALIZADO R.A.E

TEMA	Pruebas de Penetración por medio de las metodólogas Pen Test a las Bases de Datos, a la SECRETARIA DE HACIENDA MUNICIPIO DE LOS PATIOS
TÍTULO	**ESTUDIO DE SEGURIDAD EN LAS BASES DE DATOS, MEDIANTE METODOLOGÍAS DE PEN TEST, ETHICAL HACKING EN LA SECRETARIA DE HACIENDA MUNICIPAL DE LOS PATIOS**
AUTORES	FREY MARIN OCHOA GUEVARA
FUENTES BIBLIOGRÁFICAS	-FERNÁNDEZ, E. Metodología para el diseño de bases de datos seguras. La Mancha: Universidad de Castilla, 2002. -MÉNDEZ, C. Metodología de la investigación para ciencias empresariales. Bogotá: Mc Graw Hill, 2003. - ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. ISO/IEC 17799:2005. Bogotá: ISO. -PÉREZ, M. (2012). Módulo 3: auditorías y seguridad. tema 4: comparativa metodologías auditorías y pentesting. Elche: Campus Virtual. - SYMANTEC. Glosario de Seguridad 101 [en línea]. [Citado 25 de octubre de 2016]. Disponible en Internet en: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad TARAZONA, C. Amenazas informática s y seguridad de la información. México: Etek Internacional, 2007.
AÑO	2.018
RESUMEN	El siguiente Trabajo de Tesis hace referencia a el control y seguimiento a las bases de datos implementadas en la Secretaria de Hacienda, Municipio de Los Patios, para lo cual se realizaron pruebas de Ethical Hacking a los servidores que almacenan la información en dicha entidad. Para las pruebas se utilizó varios sistemas operativos con la metodología UNIX bajo LINUX, con software sofisticado como lo es Kali Linux que permite con cada una de las herramientas internas hacer escaneo de puertos, pruebas de penetración y un número significativo de implementaciones logrando los objetivos de evitar

	vulnerabilidades que afecten los diferentes Sistemas Operativos.
PALABRAS CLAVES	Bases de Datos-Ethical Hacking-Linux-Pruebas de Penetración-escaneo- puertos
CONTENIDOS	Rae - Índice general - Índice de tablas y gráficos – Introducción - Justificación - Definición del problema- Objetivos - Marco Teórico – Metodología - Resultados y Discusión - Conclusiones - Recomendaciones – Referencias
DESCRIPCION DEL PROBLEMA	la Secretaría de Hacienda del municipio de Los Patios, la cual tiene a su cargo ejecutar la estrategia financiera para el plan de desarrollo económico y social, de acuerdo al marco fiscal de corto y mediano plazo, la Secretaría de Hacienda está expuesta a amenazas de seguridad de la información, dada la posibilidad de ocurrencia de cualquier evento que pueda causar daño (material o inmaterial) sobre cualquier elemento del sistema. Desde el ámbito externo, esta entidad maneja datos sensibles y de gran interés para la administración municipal y para los diferentes contribuyentes y deudores, por lo que existen amenazas como agresiones técnicas, naturales o humanas. A nivel interno, se han identificado amenazas como la negligencia de los funcionarios que manejan la información y los equipos de cómputo, así como otras condiciones técnicas y fallas en los procesos operativos internos.
OBJETIVOS	OBJETIVO GENERAL: Realizar un estudio de seguridad en las Bases de Datos, mediante metodologías de Pen Test y Ethical Hacking en la Secretaria de Hacienda Municipal de Los Patios OBJETIVOS ESPECIFICOS: • Identificar el estado actual de metodologías de Pen Test y de Ethical Hacking para bases de datos relacionales y no relacionales. • Determinar las metodologías de Pen Test y de Ethical Hacking a ser utilizadas.

	• Planear y realizar el diagnóstico de las bases de datos de la Secretaría de Hacienda Municipal de Los Patios. • Aplicar las técnicas necesarias con las metodologías Pen Test y Ethical Hacking, para generar un buen desarrollo informático en la Secretaría de Hacienda Municipal de los Patios.
METODOLOGÍA	Se utilizará un tipo de investigación cuantitativo y descriptivo para recopilar la información requerida para el análisis de la seguridad en las Bases de Datos, mediante metodologías de Pen Test y Ethical Hacking en la Secretaría de Hacienda Municipal de Los Patios. La investigación descriptiva permite identificar las características del universo de investigación. Este tipo de investigación permite identificar, procesar y analizar los datos que se toman por diferentes medios, como la observación directa, la encuesta y las listas de chequeo, que son muy útiles en este tipo de estudios.
PRINCIPALES REFERENTES TEÓRICOS	Amenazas Informáticas, Seguridad de la Información, metodologías de Pent Test y Ethical Hacking.
PRINCIPALES REFERENTES CONCEPTUALES	Amenaza, Ataque Multi etapas, Confidencialidad, Disponibilidad y elementos de Información.
RESULTADOS	- Para la obtención de los resultados, se aplicó la encuesta como fuente primaria de información, la cual permite a través de cuestionarios resolver las inquietudes que se tienen del objeto de estudio. - Para determinar el estado actual de las bases de datos en la Secretaria de Hacienda Municipal, se empleó herramientas de seguridad informática como KALI LINUX. - En su desarrollo, se tenía como muestra y población el personal de la Secretaría de Hacienda municipal de los Patios, los cuáles participaron activamente en la contestación

	de las preguntas de selección múltiple, relacionadas a los conocimientos, experiencias y habilidades que tienen en la Entidad. De lo anterior, a continuación, se describe con gráficas el porcentaje derivado de cada pregunta.
CONCLUSIONES	1- Al resolver las encuestas con la tabulación y análisis de cada pregunta que los funcionarios de la Secretaría de Hacienda del municipio de los Patios resolvieron, arrojando como resultados inconvenientes en cuanto a la seguridad de la información y teniendo un 67% de falencias frente al tema de estudio. Demostrando la importancia y la necesidad de haber presentado las metodologías de Pen test y de Ethical hacking en la organización, pues hasta la fecha no se había desarrollado un estudio similar. 2- Con las pruebas Ethical hacking en cada área de la secretaría, teniendo como muestra fotografías que permitieron vislumbrar el mal estado en que se encontraban los servidores y el rack; con dicho análisis realizado a los servidores web, se logró identificar cada uno de los puertos por medio de un escaneo con herramientas sofisticadas para la seguridad Informática.