UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SISTEMAS

TÍTULO DEL TRABAJO

INCIDENCIA DE HACKING ÉTICO EN EL SERVIDOR DE BASE DE DATOS DE CATASTRO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAN MIGUEL, AÑO 2019

AUTORA:

JESSICA ESTEFANÍA LEMA TENELEMA

GUARANDA, AGOSTO DEL 2019

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS,
GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SISTEMAS

TEMA:

INCIDENCIA DE HACKING ÉTICO EN EL SERVIDOR DE BASE DE DATOS DE CATASTRO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAN MIGUEL, AÑO 2019.

PROYECTO DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARA OPTAR EL TÍTULO DE INGENIERA EN SISTEMAS COMPUTACIONALES.

AUTOR:
JESSICA ESTEFANÍA LEMA TENELEMA

DIRECTOR:
ING. RODRIGO DEL POZO

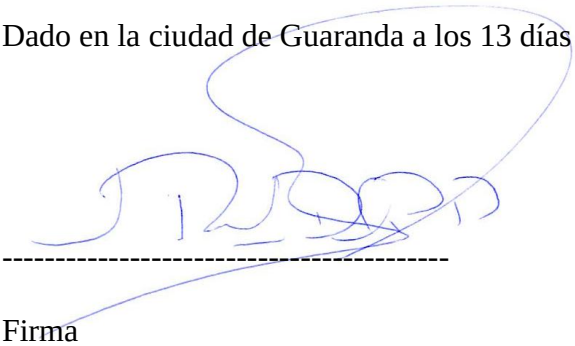
PARES ACADEMICOS:
ING. DARWIN CARRIÓN
LIC. EDGAR RIVADENEIRA

GUARANDA, AGOSTO DEL 2019

ACEPTACIÓN DEL DIRECTOR

Por la presente dejo constancia que he leído la propuesta del trabajo de titulación, presentado, por la señorita **LEMA TENENLEMA JESSICA ESTEFANÍA cuyo** tema es **INCIDENCIA DE HACKING ÉTICO EN EL SERVIDOR DE BASE DE DATOS DE CATASTRO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAN MIGUEL, AÑO 2019.**y en tal virtud acepto asesorar a la estudiante en calidad de Director durante la etapa de proyecto de investigación e informe final, hasta su presentación y evaluación.

Dado en la ciudad de Guaranda a los 13 días del mes de marzo del 2019



Firma
Ing. Rodrigo Humberto del Pozo Durango
C.C.: 0200856557

ÍNDICE GENERAL

PORTADA ..... **II**

ACEPTACIÓN DEL DIRECTOR ..... **III**

ÍNDICE GENERAL ..... **IV**

ÍNDICE DE ILUSTRACIONES ..... **VII**

ÍNDICE DE TABLAS ..... **VIII**

ÍNDICE DE ANEXOS ..... **IX**

DATOS INFORMATIVOS **1**

RESUMEN **2**

SUMMARY **3**

CAPITULO I

ANTECEDENTE O ESTADO DEL ARTE **5**

ANTECEDENTES DEL PROBLEMA **6**

DESCRIPCION DEL PROBLEMA **7**

FORMULACION DEL PROBLEMA **7**

PREGUNTAS DIRECTRICES **7**

OBJETIVOS **10**

OBJETIVO GENERAL 10

OBJETIVOS ESPECÍFICOS 10

CAPITULO II

MARCO GEO REFERENCIAL **12**

MARCO CONCEPTUAL **13**

MARCO TEÓRICO **14**

HACKING 14

ÉTICO 14

HACKING ÉTICO 14

OBJETIVOS DEL HACKING ÉTICO 14

Tipos de Hacking Ético *15*
Fases para detectar vulnerabilidades *15*
Vulnerabilidad Informática *17*
Tipos de vulnerabilidades *17*
¿CÓMO EXPLOTAN ESTAS VULNERABILIDADES? 20
KALI LINUX 20
Ventajas *20*
¿Qué tiene Kali? *21*
NESSUS 21
METASPLOIT 22
FORMAS DE ATACAR A SERVIDORES 24
FUERZA BRUTA 25
CROSS SITE SCRIPTING 26
CAPITULO III
METODOLOGIA 28
METODOS DE INVESTIGACION 28
MÉTODO CUALITATIVO 28
MÉTODO CUANTITATIVO 28
TIPOS DE INVESTIGACION 28
PARA REALIZAR EL PROYECTO UTILIZARE LOS SIGUIENTES MÉTODOS. 28
MÉTODO DESCRIPTIVO 28
MÉTODO BIBLIOGRÁFICO 28
MÉTODO DE INVESTIGACIÓN DE CAMPO. 29
TECNICAS E INSTRUMENTOS PARA LA OBTENCIÓN DE DATOS 29
ENTREVISTA 29
OBSERVACIÓN DIRECTA 29
POBLACIÓN 29
MUESTRA 29
CAPITULO IV
MARCO ADMINISTRATIVO 31
RECURSOS Y FINANCIAMIENTO 32

MONTO 32

BIBLIOGRAFÍA..... 33

ANEXOS

ÍNDICE DE ILUSTRACIONES

Ilustración 1:Mapa geo referencial del GAD San Miguel 12

ÍNDICE DE TABLAS

Tabla 1: Cronograma De Actividades.....31

Tabla 2: Presupuesto del Proyecto.....32

ÍNDICE DE ANEXOS

ANEXO 1: FORMATO DE ENTREVISTA.....37

ANEXO 2: FORMATO DE TÉCNICA DE OBSERVACIÓN 39

DATOS INFORMATIVOS

Modalidad: Presencial

Autora: Jessica Estefanía Lema Tenelema

Carrera: Sistemas

Área técnica de la carrera: Ciencia

Sector: Público

Línea de investigación: Proyecto de investigación

Periodo: 2018-2019

Fecha de Presentación: Agosto del 2019

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SISTEMAS

TÍTULO DEL TRABAJO DE TITULACIÓN

Incidencia de hacking ético en el servidor de base de datos de catastro del Gobierno Autónomo Descentralizado del Cantón San Miguel, Año 2019

Autora: Jessica Estefanía Lema Tenelema

Director: Ing. Rodrigo del Pozo

RESUMEN

El presente proyecto de investigación comprende la elaboración de un proceso para hackear el servidor de la base de datos de catastro del Gobierno Autónomo Descentralizado Municipal San Miguel de Bolívar, año 2019.

A través del estudio de distintos instrumentos, se optara por el software que mejor se acople, en base a investigación se elegirá el sistema que mejor se adapte a las necesidades presentes para realizar hacking ético en el servidor de la base de datos de catastro.

Esto permitirá detectar vulnerabilidades informáticas que estén presentes en este servidor.

Mediante diferentes métodos, los mismos que se aplicarán al servidor de base de datos de catastro, se obtendrá información que permitirá conocer el nivel de seguridad con el que cuenta el servidor en la actualidad.

Con la investigación que se realice se demostrará la importancia de evaluar el nivel de seguridad informática con el que cuenta un servidor, para evitar que intrusos ingresen a los sistemas que se encuentren alojados en este y roben, destruyan o alteren información para su beneficio.

Palabras claves: hacking ético, servidor, base de datos, catastro, vulnerabilidades, seguridad informática.

STATE UNIVERSITY OF BOLIVAR

FACULTY OF ADMINISTRATIVE SCIENCES BUSINESS AND COMPUTER MANAGEMENT

CARRERA DE SISTEMAS

TITLE OF THE DEGREE WORK

Incidence of ethical hacking in the cadastre database server of the Decentralized Autonomous Government of San Miguel Canton, Year 2019

Author: Jessica Estefanía Lema Tenelema

Director: Ing. Rodrigo del Pozo

SUMMARY

This research project includes the development of a process to hack the server of the cadastre database of the San Miguel de Bolívar Autonomous Decentralized Municipal Government, 2019.

Through the study of different instruments, we will opt for the software that best fits, based on research the system that best suits the present needs will be chosen to perform ethical hacking in the database server of the cadastre.

This will allow detecting computer vulnerabilities that are present in this server.

By means of different methods, the same ones that will be applied to the cadastral database server, information will be obtained that will allow to know the level of security with which the server counts at present.

With the research that is carried out, it will be demonstrated the importance of evaluating the level of computer security that a server has, to prevent intruders from entering the systems that are housed in it and stealing, destroying or altering information for their benefit.

Keywords: ethical hacking, server, database, cadastre, vulnerabilities, computer security.

CAPÍTULO I

ANTECEDENTE O ESTADO DEL ARTE

Para poder plantear el estado del arte se ha investigado la ejecución de procesos para llevar a cabo hacking ético en otras instituciones a nivel nacional e internacional, en los repositorios de libre acceso, se ha conseguido lo siguiente:

En la investigación de la Maestría en Ingeniería de Sistemas de Información de la Escuela de Posgrado, Facultad Regional de Buenos Aires. Universidad Tecnológica Nacional de Argentina, previo a la obtención del título (Giannone, 2016) con el Tema: "Método de Inclusión de Hacking Ético en el Proceso de Testing de Software" menciona que debido al crecimiento exponencial de Internet y a que las organizaciones poseen cada vez más información, se hace imprescindible bloquear y eliminar todas las intrusiones posibles. Gracias al hacking ético es posible detectar y corregir algunas de las vulnerabilidades antes que el sistema salga a la luz. Con el fin de mejorar este proceso se intentan incluir estas técnicas y métodos en el proceso tradicional de testing de software dentro de las organizaciones. El software inseguro está debilitando las finanzas, salud, defensa, energía, y otras infraestructuras críticas.

En la investigación de la Universidad Abierta de Cataluña de Barcelona, España la con el Título: "Hacking Ético y Seguridad en Red" menciona que el profesional del hacker ético tienen que poseer un conjunto de herramientas de seguridad que cada una cumplan su propia función, para buscar soluciones de manera ética.

En el proyecto de investigación de la Universidad Técnica de Ambato, previo a la obtención del Título de Ingeniero en Sistemas Computacionales e Informáticos (Rojas Buenaño, 2018) con el tema "Hacking Ético Para Analizar y Evaluar la Seguridad Informática en la Infraestructura de la Empresa Plasticaucho Industrial S.A." nos indica que el impulso tecnológico que ha tenido el mundo se ha visto frustrado por hechos lamentables efectuados

por ciberdelincuentes. El 2017 fue un año marcado por ataques de tipo ransomware que infectaron un sin número de ordenadores cifrando la información de usuarios comunes pasando por departamentos de gobierno, hospitales, y llegando a empresas multinacionales que se vieron obligados a parar sus operaciones para detener la propagación del malware en sus infraestructuras. Es por ello que a nivel de infraestructura tecnológica un factor decisivo a la hora de sufrir un ataque informático implica una adecuada gestión de configuración en los servicios implementados y una correcta administración y despliegue de actualizaciones en sistemas operativos y aplicaciones. Si un atacante logra penetrar la seguridad perimetral y obtener acceso a la red interna puede aprovechar deficientes configuraciones en los servicios internos y buscar vulnerabilidades que no han sido parchadas, esto conllevaría a que en algunos casos comprometa toda la infraestructura tecnológica.

ANTECEDENTES DEL PROBLEMA

Desde que la tecnología se a vuelta un requisito indispensable para la sociedad, muchos viven de esta, pero no todos lo hacen respetando los principios de ética y moral, existen personas que se denominan hacker, ciberdelincuentes, paladines, que se dedican únicamente a hurgar todo tipo de sistemas, a través de instrumentos informáticos que ellos mismo desarrollan o los adquieren con la finalidad de evadir la seguridad de los sistemas con los que cuentan las empresas públicas y privadas y robar, modificar, destruir y así sacar un beneficio propio.

El GAD del Cantón San Miguel de Bolívar posee múltiples equipos informáticos, entre los cuales se encuentra un servidor que aloja la base de datos de catastro, posee aplicaciones informáticas que prestan los servicios y que almacenan información relevante en la entidad, las mismas pueden estar expuestas a varias amenazas internas y/o externas, atacantes que pueden alterar o manipular los datos de manera malintencionada poniendo el riesgo la integridad de la institución.

DESCRIPCION DEL PROBLEMA

Desde que la tecnología se a vuelta un requisito indispensable para los seres humanos, muchos viven de esta, pero no todos lo hacen respetando los principios de ética y moral.

Hay personas que se denominan hacker, ciberdelincuentes, intrusos informáticos, que se dedican únicamente a hurgan todo tipo de sistemas informáticos, a través de instrumentos informáticos que son ellos mismo desarrollan o los adquieren con la finalidad de hacer penetraciones a sistemas de empresas tanto públicas como privada y así sacar alguna ventaja de esto.

Robar, modificar, destruir son algunos verbos que describen las actividades que estos ciberdelincuentes realizan cuando lograr entrarse a un sistema objetivo.

El GAD del Cantón San Miguel de Bolívar posee múltiples equipos informáticos, entre los cuales se encuentra un servidor que aloja la base de datos de catastro, el cual va a ser escaneado con la finalidad de encontrar vulnerabilidades informáticas.

Las aplicaciones informáticas que prestan los servicios y que almacenan información relevante en el GAD, pueden estar a varias amenazas internas y/o externas, atacantes que pueden alterar o manipular los datos de manera malintencionada poniendo el riesgo la integridad del gobierno autónomo descentralizado del Cantón San Miguel de Bolívar.

FORMULACION DEL PROBLEMA

¿Cómo de hacking ético en el servidor de base de datos de catastro del Gobierno Autónomo Descentralizado del Cantón San Miguel, evitara que intrusos informáticos tomen el control del servidor, y alteren modifique o eliminen los datos que están alojados en este?.

PREGUNTAS DIRECTRICES

- ¿Cómo fundamentar teóricamente el hacking ético del Gobierno Autónomo Descentralizado De San Miguel?

- ¿De qué levantar la información y estructura del sistema informático de catastros?
- ¿Por qué analizar el estado actual de seguridad informática de Catastros en la institución?
- ¿Cómo detectar las vulnerabilidades del servidor de la base de datos de catastro?
- ¿Cuándo explotar la vulnerabilidad encontrada e intentar tomar acceso al servidor?

JUSTIFICACIÓN

Con el pasar de tiempo se ha visto la necesidad de implementar sistemas de seguridad más robustos y con ellos de llevar a cabo técnicas de intrusiones que estén controladas, lo cual se simula a un ataque real.

Es por ello que se da paso al presente proyecto, el cual pretende a través de investigación, ver el estado de seguridad con el que cuenta el servidor que aloja la base de datos de catastro.

El proyecto se presenta en base a la necesidad esencial que tiene el GAD San Miguel de implementar sistemas de seguridad más robustos para detectar dónde está el peligro o la vulnerabilidad de los sistemas y programas informáticos institucionales.

Es **necesario** efectuar el presente proyecto de investigación debido a que en el Gobierno Autónomo Descentralizado San Miguel, tiene la necesidad de ejecutar hacking ético en el servidor de base de datos de catastro para que ayude a evaluar la seguridad informática e identificar vulnerabilidades presentes en este con el fin de tomar las medidas adecuada antes de que suceda un incidente.

Es importante realizar hacking ético ya que **permitirá** combatir a los piratas informáticos con malas intenciones y así proteger todos los sistemas informáticos que se encuentran instalados en el servidor utilizado para realizar la investigación.

El proyecto es **pertinente** tomando en cuenta que no se ha realizado ningún trabajo similar en el servidor puesto a prueba y al realizarlo servirá como aporte para fortalecer la seguridad de los sistemas informáticos.

Este proyecto de investigación es **factible** ya que se cuenta con el apoyo y predisposición del Gobierno Autónomo Descentralizado San Miguel y por ende poder aprovechar esta información para la prevención y protección de datos.

OBJETIVOS

Objetivo General

- ✓ Identificar las vulnerabilidades presentes en el servidor de base de datos de catastro de la municipalidad del Cantón San Miguel a través de hacking ético.

Objetivos Específicos

- ➢ Fundamentar teóricamente el hacking ético del Gobierno Autónomo Descentralizado de San Miguel para garantizar las seguridad de la información y esta confiable y oportuna
- ➢ Levantar la información y estructura del sistema informático de catastros.
- ➢ Analizar el estado actual de seguridad informática de Catastros en la institución.
- ➢ Detectar la vulnerabilidades del servidor de la base de datos de catastro
- ➢ Explotar la vulnerabilidad encontrada e intentar tomar acceso al servidor.

CAPÍTULO II

MARCO GEO REFERENCIAL

El presente trabajo de Investigación se lo realizara en el Gobierno Autónomo Descentralizado Municipal San Miguel.

País: Ecuador

Provincia: Bolívar

Cantón: San Miguel

Lugar de Investigación: Gobierno Autónomo Descentralizado de San Miguel.

Latitud: -1.70816

Longitud: -79.04155

Fuente de datos: GoogleMaps, Gobierno Autónomo Descentralizado de San Miguel, Bolívar, Ecuador.

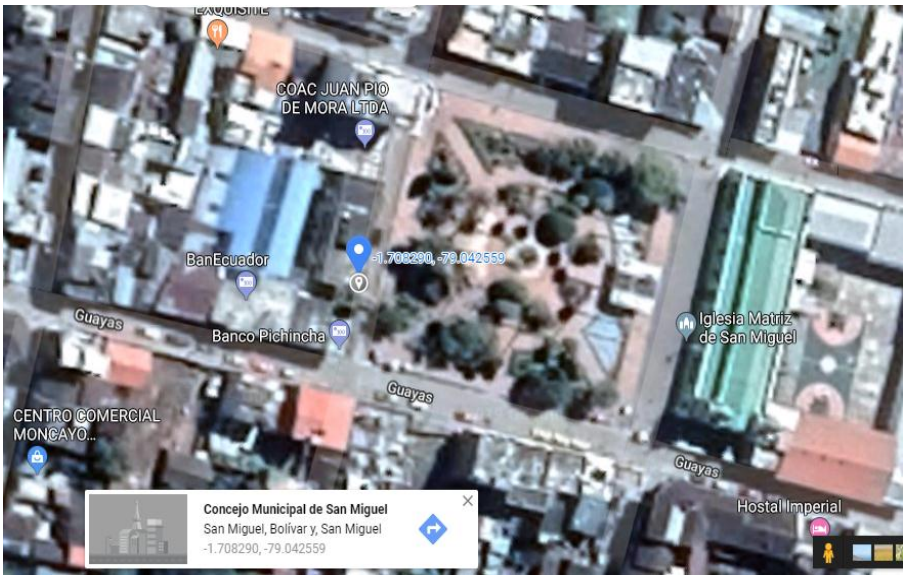


Ilustración 1:Mapa geo referencial del GAD San Miguel

Fuente: https://www.google.com/maps/@-1.708263,-79.0427293,144m/data=!3m1!1e3

MARCO CONCEPTUAL

Hacking: según (Écija, 2017) afirma que "es el conjunto de técnicas a través de las cuales se accede a un sistema informático vulnerando las medidas de seguridad establecidas originariamente."

Ético: según (MX E. , 2016) menciona que **"**marca las pautas o principios del obrar humano."

Seguridad informática: (Equipo de Expertos, 2018) indica que es "el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente."

Vulnerabilidad: según (INCIBE, 2017) **"**es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible".

Servidor: según (Medrano, 2016) afirma que. "es uno de los factores clave de la transformación digital que progresivamente se va dando en las empresas."

Catastro: según (Flores, 2014) afirma que. **"**Es el registro administrativo dependiente del Estado en el que se describen los bienes inmuebles rústicos, urbanos y de características especiales."

Base De Datos: según (Capacho Portilla & Nieto Bernal, 2017, pág. 18) "el término base de datos se define como una colección de datos, que contiene información relevante para una empresa".

MARCO TEÓRICO

Hacking

(Avast, 2018) indica que“el hacking informático recurre a la manipulación de la conducta normal de un equipo y de los sistemas que tiene conectados. Esto se hace generalmente mediante scripts o programas que manipulan los datos que pasan a través de una conexión de red con el fin de acceder a la información del sistema. Las técnicas de hacking incluyen el uso de virus, gusanos, troyanos, ransomware, secuestros del navegador, rootkits y ataques de denegación de servicio.”

Ético

Según (Tori, 2008, pág. 13) dice que “para emular la metodología de ataque de un intruso informático y no ser lo, tiene que haber ética de por medio, más allá de todas las condiciones, términos y activos que haya alrededor del caso”.

Hacking Ético

Según (Abraham, 2019) “es la utilización de los conocimientos de seguridad en informática para realizar pruebas en sistemas, redes o dispositivos electrónicos, buscando vulnerabilidades que explotar, medidas sin poner en riesgo el sistema”.

Objetivos del Hacking Ético

Evaluar la seguridad informática.

Identificar vulnerabilidades en sistemas, redes o infraestructuras de sistemas” (Ortega, 2019).

Tipos de Hacking Ético

Debido a la forma de ejecución se puede clasificar al hacking ético en tres tipos:

- Hacking de caja negra (black-box hacking)
- Hacking de caja gris (gray-box hacking)
- Hacking de caja blanca (white-box hacking)

Hacking de caja negra: el chequeo es llevado a cabo desde la parte inicial sin tener información como si fuera un intruso cualesquiera y por ello conlleva más tiempo. (Tori, 2008)

Hacking de caja gris: en este tipo de hacking se cuenta con la información del objetivo que son proporcionados por la entidad. (Tori, 2008)

.

Hacking caja blanca: Como menciona el autor (Carrecedo, 2010) "Se dispone de toda la información de la organización. Análisis en profundidad de vulnerabilidades (scripts).Informe detallado de vulnerabilidades y recomendaciones.".

Fases para detectar vulnerabilidades

Según el autor (wordpress, 2017) Usualmente se siguen las siguientes fases:

Fase 1: Reconocimiento

(wordpress, 2017) Esta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo.

Fase 2: Escaneo

(wordpress, 2017) En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

Fase 3: Obtener acceso

(wordpress, 2017) En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración.

Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

Fase 4: Mantener el acceso

(wordpress, 2017) Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Fase 5: Borrar huellas

(wordpress, 2017) Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

Vulnerabilidad Informática

(Peralta, 2014) El termino vulnerabilidad informática hace énfasis a las debilidades que se encuentran en los sistemas informáticos, ya que a través de esta debilidad un atacante cualquiera puede destruir, robar, y cometer fraudes con los datos que allí se encuentran alojados.

Hay distintos tipos de vulnerabilidades que se pueden encontrar en una aplicación.

Tipos de vulnerabilidades

Según (Días, 2014) nos menciona que existen distintos tipos de vulnerabilidades informáticas se clasifican en:

Vulnerabilidad de desbordamiento de buffer (Buffer Overflow)

Se trata de un tipo de ataque muy común entre los hackers donde se puede causar un problema muy serio en los sistemas. Existen inúmeros tipos de ataques de desbordamiento pero el más común es el de la pila. Este ataque consiste cuando un determinado programa por fallo en su implementación no es capaz de controlar la cantidad de datos que están en el buffer, haciendo que por final ultrapase la capacidad del buffer. Debido a ese fallo los datos son movidos a otro lado sobrescribiendo o modificándolos, con eso se puede conseguir tener un control del propio sistema. Ese tipo de ataque se hace muy común porque la mayoría de

los sistemas están desarrollado en C, porque en su diseño el lenguaje ha priorizado espacio y performance sobre seguridad. Según los expertos en seguridad informática ese tipo de ataque será durante muchos años uno de los más importantes.

Inyección de código

Se trata de una vulnerabilidad que está basada en la existencia de parámetros de una determinada aplicación que no son validados de manera correcta. Entonces el atacante aprovecha para lanzar algunos valores de parámetros dinámicos que irán a enlazar con la base de datos de la aplicación. Se trata como entrar con algunos valores que no son validados previamente por los desarrolladores pero que podrá modificar el comportamiento de la aplicación, como por ejemplo hasta devolver una password o bien validar un usuario.

Ataque al usuario

Se trata del tipo de ataque más utilizado y donde se puede conseguir más informaciones como las cookies de los usuarios. También se puede utilizar el ataque por vía del correo electrónico, donde se envía un correo con un link incrustado que tiene un script. La idea es hacer que a través de este link pueda motivar al usuario a ejecutarlo y poner en machar algún comando malicioso. Para complementar el ataque del usuario, se habla de la publicación en sitio Web vulnerables que consiste en la incluir algún dato en libro de visita, foros, blogs o cualquier sitio Web, donde permite al usuario introducir sus datos sin ser validados por el servidor, con esto se permite robar alguna información del propio usuario.

Ataque a la aplicación

Consiste en introducir en alguna aplicación Web vulnerable algún código malicioso, normalmente las aplicaciones Web están protegidas pero siempre es posible hacer el ataque

mediante algún tag que no está previsto. Los tags son etiquetas internas que se ponen en los códigos.

Cracker

Se trata de la técnica donde los hackers consisten en sacar los códigos de registro de un determinado programa y con eso poder validar la aplicación para su uso. La función principal del proceso es poder instalar una aplicación que está protegida mediante su registro. Para realizar esta técnica se requiere mucho conocimiento de programación a bajo nivel, porque en la mayoría de los casos se tiene que desensamblar algún ejecutable.

Ingeniería Social

Consiste en una manera que tienen los hackers en engañar a los usuarios haciéndose pasar por otras personas o entidades. Existen inúmeros tipos de ingeniería social, una de las más conocidas es la técnica del Phising. Con esa técnica se puede conseguir credenciales de algún usuario, como contraseña, información de la tarjeta de crédito o hasta informaciones bancarias. El nombre se origina de la palabra pescar (fishing) en inglés. Esta técnica consiste en suplantar la identidad con fines maliciosos.

Race condition

Ocurre cuando varios procesos intentan acceder al mismo tiempo en un determinado recurso compartido.

Redes Wi-Fi

Según estudios realizados cerca de 20% de las redes Wi-Fi son fácilmente atacables, el principal motivo es porque todavía utilizan un mecanismo de autentificación y de encriptación obsoleto (WEP) y también por desconocimiento de los usuarios.

¿Cómo explotan estas vulnerabilidades?

(Rubio, 2011) Cuando una vulnerabilidad es descubierta, puede pasar que el descubrimiento lo realice un cracker, y cree una aplicación que lo explote. Las aplicaciones que sirven para explotar vulnerabilidades tienen el nombre de exploit (aunque también se puede escribir como xploit o sploit). Cuando está recién hecho, se dice que estos exploits son de 0day (día cero), y por tanto, hay muchos sistemas en producción sensibles de su acción.

No obstante, los exploits también son buenas herramientas de seguridad, porque ayudan a comprobar si un sistema es fiable o no. Por lo que también existen muchas base de datos de exploits en Internet. La más conocida es la que usa el programa metasploit.

Kali Linux

Según (MLX, 2018) menciona que Kali es una disribucion de Linux basada en Debian. Su objetivo es simple; incluya tantas herramientas de penetración y auditoría de seguridad como sea posible en un paquete conveniente. Kali entrega también muchas de las mejores herramientas de código abierto para realizar pruebas de seguridad que se recopilan y están listas para usar.

Ventajas

Según (Ciberaula, 2016) da a conocer las siguientes ventajas:

1. Linux es muy robusto, estable y rápido: Ideal para servidores y aplicaciones distribuidas. A esto se añade que puede funcionar en máquinas humildes: Linux puede correr servicios en un x86 a 200 MHz con calidad

2. Linux es libre: Esto implica no sólo la gratuidad del software, sino también que Linux es modificable y que Linux tiene una gran cantidad de aplicaciones libres en Internet.

Todo ello arropado por la inmensa documentación de Linux que puede encontrarse en la Red

3. Linux ya no está restringido a personas con grandes conocimientos de informática: Los desarrolladores de Linux han hecho un gran esfuerzo por dotar al sistema de asistentes de configuración y ayuda, además de un sistema gráfico muy potente. Distribuciones Linux como Red Hat/Fedora tienen aplicaciones de configuración similares a las de Windows.

¿Qué tiene Kali?

1. Kali tiene herramientas de seguridad
2. Tiene herramientas clásicas de recopilación de información como NMap y Wireshark.
3. Kali también tiene herramientas basadas en WiFi como Aircrack-ng, Kismet y Pixie. Para atacar contraseñas, hay herramientas como Hydra, Crunch, Hashcat y John the Ripper.
4. Luego hay suites más completas de herramientas, incluidas Metasploit y Burp Suite.
5. Eso es solo un pequeño porcentaje de las herramientas de seguridad disponibles por defecto con Kali. Pasaría mucho tiempo para revisarlos a todos, pero se puede ver claramente que muchas de las herramientas más populares están representadas.

Nessus

(Advisors, 2018) Menciona que es el estándar mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red. Nessus se ha utilizado por más de 1 millón los usuarios en todo

el mundo, por lo que es el líder mundial de evaluación de la vulnerabilidad, configuración de seguridad y cumplimiento de las normas de seguridad.

¿Por qué escoger Nessus Escáner de Vulnerabilidad?

- **Referente Mundial:** Con la mayor base instalada y mejor experiencia en la industria, Nessus ofrece a los clientes la capacidad de identificar sus mayores amenazas y responder rápidamente.

- **Detallado:** Paneles de mando detallados para ayudar a los clientes a fortalecer las redes contra las amenazas cibernéticas

- **Rentable:** Nessus reduce el tiempo y costo de seguridad en el escanning y asegura los cumplimientos de seguridad

- **Cumplimiento para PCI:** Puede utilizar productos de Nessus para realizar exploraciones de la red interna.

Metasploit

(ElTecnólogoEM, 2019) Dice que. **Metasploit Framework** es uno de los marcos de pruebas de penetración más utilizados por las corporaciones a las agencias de aplicación de la ley. Metasploit se compone de más de 1500 módulos que ofrecen funcionalidades que cubren cada fase de una prueba de penetración, lo que hace que la vida de un penetest sea comparativamente más sencilla.

Esto es un marco de código abierto. También ofrece un enfoque extenso en el desarrollo de nuevos exploits y en la automatización de varias tareas que reducen toneladas de esfuerzos manuales y ahorran una gran cantidad de tiempo.

¿Para qué sirve Metasploit Framework?

Con Metasploit Framework puedes hacer lo siguiente:

- **Interacciones previas al compromiso:** este paso define todas las actividades previas al compromiso y las definiciones de alcance, básicamente todo lo que necesita discutir con el cliente antes de que comience la prueba.

- **Recopilación de inteligencia:** esta fase se trata de recopilar información sobre el objetivo sometido a prueba, al conectarse al objetivo directa o pasivamente, sin conectarse al objetivo en absoluto.

- **Modelado de amenazas:** esta fase consiste en hacer coincidir la información descubierta con los activos para encontrar las áreas con el nivel de amenaza más alto.

- **Análisis de vulnerabilidad:** Esto implica encontrar e identificar vulnerabilidades conocidas y desconocidas y validarlas.

- **Explotación:** esta fase funciona aprovechando las vulnerabilidades descubiertas en la fase anterior. Esto normalmente significa que se esta tratando de obtener acceso al objetivo.

- **Después de la explotación:** las tareas reales que se deben realizar en el objetivo, que implican descargar un archivo, apagar un sistema, crear una nueva cuenta de usuario en el destino, etc., son parte de esta fase. Esta fase describe lo que necesita hacer después de la explotación.

- **Informes:** esta fase incluye resumir los resultados de la prueba en un archivo y las posibles sugerencias y recomendaciones para corregir las debilidades actuales en el objetivo.

Formas de Atacar a Servidores

(HDCO, 2016) Hay distintas maneras de atacar a servidores, entre las cuales:

Ataque por Injection

Los ataques de inyección, más específicamente sqli (Structured Query Language Injection) es una técnica para modificar una cadena de consulta de base de datos mediante la inyección de código en la consulta. El SQLI explota una posible vulnerabilidad donde las consultas se pueden ejecutar con los datos validados.

SQLI siguen siendo una de las técnicas de sitios web más usadas y se pueden utilizar para obtener acceso a las tablas de bases de datos, incluyendo información del usuario y la contraseña. Este tipo de ataques son particularmente comunes en los sitios de empresas y de comercio electrónico donde los hackers esperan grandes bases de datos para luego extraer la información sensible. Los ataques también se encuentran entre los ataques más fáciles de ejecutar, que no requiere más que un solo PC y una pequeña cantidad de conocimientos de base de datos.

DDoS

La Denegación de Servicio (DoS) o Denegación de Servicio Distribuida (DDoS) son las formas más comunes para congelar el funcionamiento de un sitio web. Estos son los intentos de inundar un sitio con solicitudes externas, por lo que ese sitio no podría estar disponible para los usuarios reales. Los ataques de denegación de servicio por lo general se dirigen a puertos específicos, rangos de IP o redes completas, pero se pueden dirigir a cualquier dispositivo o servicio conectado.

Los ataques de denegación de servicio funcionan cuando una computadora con una conexión a Internet intenta inundar un servidor con paquetes. DDoS, por otro lado son cuando muchos dispositivos, a menudo ampliamente distribuidos, en un intento de botnet para inundar el objetivo con cientos, a menudo miles de peticiones.

Los ataques DDoS vienen en 3 variedades principales:

1. Los ataques de volumen, donde el ataque intenta desbordar el ancho de banda en un sitio específico.

2. Los ataques de protocolo, donde los paquetes intentan consumir servicios o recursos de la red.

3. Ataques a aplicaciones, donde las peticiones se hacen con la intención de "explotar" el servidor web, mediante la capa de aplicación.

Fuerza Bruta

Estos son básicamente intenta "romper" todas las combinaciones posibles de nombre de usuario + contraseña en una página web. Los ataques de fuerza bruta buscan contraseñas débiles para ser descifradas y tener acceso de forma fácil. Los atacantes cuentan con buen tiempo, así que el truco es hacer que tus contraseñas sean lo bastante seguras y así el atacante se cansaría antes de descifrar tu contraseña. Mientras que las computadoras se vuelven más y más poderosa la necesidad de contraseñas más fuertes se vuelve cada vez más importante. El caso más reciente de esta vulnerabilidad, se ha visto en cuanto a la vulneración de cuentas de algunos famosos alojadas en iCloud.

Cross Site Scripting

Los atacantes utilizan Cross-site Scripting (XSS) para inyectar scripts maliciosos en lo que serían sitios web inofensivos. Debido a que estos scripts parecen provenir de sitios web de confianza, el navegador de los usuarios finales casi siempre ejecuta la secuencia de comandos, la concesión de los piratas informáticos el acceso a la información contenida en las cookies o tokens de sesión utilizados con ese sitio. El XSS generalmente se utiliza para obtener acceso de un usuario de la cuenta.

Malware

(Ramiro, 2018) Malware es una forma corta de software malicioso. El malware incluye virus informáticos, gusanos, caballos de Troya, spyware, adware deshonesto, software delictivo, la mayoría de los rootkits y otro software malicioso y no deseado.

CAPITULO III

METODOLOGIA

Para el desarrollo del presente proyecto de investigación se utilizaran diferentes métodos, instrumentos y técnicas de investigación, que me permita la recolección y análisis de información para de esa manera dar solución al problema planteado.

METODOS DE INVESTIGACION

Método Cualitativo

Permitirá analizar el nivel de seguridad actual del servidor, de las funciones que está desempeñando el sistema de catastro en el GAD San Miguel de Bolívar.

Método Cuantitativo

A través de este método se recolectará, analizará y comprobará las variables y la hipótesis establecida en la investigación, mediante el uso de datos estadísticos para establecer la exactitud de los procesos.

TIPOS DE INVESTIGACION

Para realizar el proyecto utilizare los siguientes métodos.

Método Descriptivo.

Esta investigación me permitirá conocer actualmente cual es el nivel de seguridad con el que cuenta el servidor que aloja la base de datos de catastro a través de una descripción de características del área de interés a investigar.

Método Bibliográfico

Se utilizara el método bibliográfico con el propósito de conocer y analizar los fundamentos teóricos más relevantes y todos los recursos disponibles para realizar el presente trabajo de investigación mediante la utilización de libros, artículos, trabajos de grado, internet, etc.

Método de Investigación de Campo.

Se utilizará al momento de realizar la encuesta con la finalidad de determinar la aceptación del trabajo en el GAD San Miguel y así obtener información para la puesta en marcha del proyecto.

TECNICAS E INSTRUMENTOS PARA LA OBTENCIÓN DE DATOS

Las técnicas que se van a utilizar para la recolección de información son: entrevista y observación directa, estas van a ser empleadas en el momento necesario, para de esta manera proseguir con la investigación y obtener información que nos ayudara a la elaboración del proyecto.

Entrevista

Me permitirá obtener información mediante el dialogo en un encuentro formal con el Jefe y Administrador de Sistemas Informáticos, y así conseguir información útil para el desarrollo del proyecto de investigación.

Observación directa

Se observará las funciones que se está realizando en el servidor y el nivel de seguridad con el que cuenta y procederé a ejecutar una simulación en un ambiente controlado y bajo supervisión del Administrador de la Unidad de Sistemas Informáticos.

POBLACIÓN

Según (Rojas, 2010) menciona que. “Es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado”

Para la presente investigación se tomó como población a la totalidad del personal que labora en la Unidad de Sistemas Informáticas del Gobierno Autónomo Descentralizado San Miguel.

MUESTRA

Como la población en estudio es pequeña se toma en su totalidad.

MARCO ADMINISTRATIVO

Tabla 1: Cronograma De Actividades

N°	ACTIVIDADES	MESES/SEMANAS																											
		Noviembre				Diciembre				Enero				Febrero				Marzo				Abril				Mayo			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	Selección de la modalidad de titulación.																												
2	Presentación de documentos para la denuncia del tema.																												
3	Presentación de la denuncia del tema.																												
4	Aprobación del tema.																												
5	Desarrollo del proyecto.																												
6	Recolección de información y datos.																												
7	Presentación del avance del proyecto.																												
8	Entrega de proyecto e informe de investigación.																												
9	Entrega de ejemplares-																												
10	Defensa del proyecto de investigación.																												

RECURSOS Y FINANCIAMIENTO

Talento humano

Autora:

Jessica Estefanía Lema Tenelema

Tutor:

Ing. Rodrigo del Pozo

Materiales:

Equipo de computación

Internet

Suministro de oficina (flash memory, hojas, cuadernos)

INGRESOS	**MONTO**
Aporte de autora Estefanía Lema	950.00
INGRESOS TOTALES	**950.00**
EGRESOS	**MONTO**
Computadora personal	500,00
Internet	100.00
Copias Escaneo	20.00
Suministro De Oficina	20.00
Impresiones	90.00
Movilización	60,00
Anillados y Empastados	40.00
Imprevistos	70.00
Alimentación	50.00
TOTAL	**950.00**

Tabla 2: Presupuesto del Proyecto
Elaborado por: Estefanía Lema

BIBLIOGRAFÍA

Codigo Organico Integral Penal. (2017). ECUADOR.

Advisors. (2018). Obtenido de https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

GALILEO Ingeniería y Servicios S.A. (2018). Obtenido de http://www.galileoiys.es/portfolio-item/gestion-catastral/

Abraham. (julio de 2019). *enter.co*. Obtenido de https://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

Ariosa, D. (2013). *ecured.cu*. Obtenido de https://www.ecured.cu/Seguridad_en_los_servidores

Avast. (2018). *Avast*. Obtenido de https://www.avast.com/es-es/c-hacher

Capacho Portilla, J. &., & Nieto Bernal, W. (2017). *Diseño de Base de Datos.* Colombia: Universidad de Norte.

Ciberaula. (15 de Marzo de 2016). Obtenido de http://linux.ciberaula.com/articulo/ventajas_inconvenientes_linux

Días, C. (2014). *Hacking ético y seguridad en Red.*

Días, C. (2014). *Hacking Ético y Seguridad en Red.* Barcelona, España: Universidad Abierta de Cataluña.

Écija, A. (18 de Marzo de 2017). *ciberderecho*. Recuperado el 22 de Mayo de 2019, de http://www.ciberderecho.com/que-es-el-hacking/

ElTecnólogoEM. (12 de 2019). *Eliezer Molina EL TECNÓLOGO.* Obtenido de https://eliezermolina.net/que-es-y-para-que-sirve-metasploit-framework/

Equipo de Expertos. (2018). *www.universidadviu.com*. Obtenido de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Expertos, E. d. (s.f.). *www.universidadviu.com*. Obtenido de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Flores, M. (17 de Marzo de 2014). *inmogesco.com*. Obtenido de

https://inmogesco.com/blog/terminos-inmobiliarios-catastro/

Galileo. (2018). *www.galileoiys.es.* Obtenido de http://www.galileoiys.es/portfolio-item/gestion-catastral/

Giannone, A. (2016). *Método de Inclusión de Hacking Ético en el Proceso de Testing de Software.* Buenos Aires, Argentina: Revista Latinoamerica de Ingeniería de Software.

HDCO. (2016). *HostDime.* Obtenido de http://blog.hostdime.com.co/tipos-de-ataques-mas-comunes-a-sitios-web-y-servidores/

Huilca Chicaiza., G. N. (2012). *HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLOS.* Ambato: Universidad Técnica de Ambato.

Ibáñez, L. H. (2014). *Bases de Datos.* Madrid, España: RA - MA.

INCIBE. (13 de 20 de 2017). *www.incibe.es*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Medrano, E. L. (16 de Septiembre de 2016). *iinfortelecom.es/blog*. Obtenido de https://infortelecom.es/blog/que-es-un-servidor-y-para-que-sirve/

MLX. (08 de 02 de 2018). *Más Linux.* Obtenido de https://maslinux.es/que-es-kali-gnu-linux/

MX, E. (06 de Enero de 2016). *definicion.mx*. Obtenido de https://definicion.mx/etica/

Nicolas, G. (12 de Julio de 2016). *www.ecured.cu*. Obtenido de https://www.ecured.cu/Servidor_Bases_de_Datos

P, H. (21 de oviembre de 2014). Obtenido de https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/

Peralta, H. (21 de noviembre de 2014). Obtenido de https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/

Ramiro, R. (2018). *CIBERSEGURIDAD*. Obtenido de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-

prevenirlos/?fbclid=IwAR3W8Z_NPEdSZbSUisdrhSak88uk3YAzR6lfHD2c4XvfBg937CMhWX01CGc

Reyes, F., Gonzáles, A., Miranda, D., & Crecente, R. (2009). *Sistema de Información Catastral adaptado a la realidad del gobierno local en Ecuador.* Loja.

Rojas Buenaño, A. I. (2018). *HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.* Ambato: Universidad Técnica de Ambato.

Rubio, M. (25 de 05 de 2011). *ALTENWALD.* Obtenido de https://altenwald.org/2011/05/25/vulnerabilidades-y-exploits/

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

Usuario, S. (01 de 12 de 2015). *GPB Turístico.* Obtenido de http://www.bolivar.gob.ec/gpbTuristico/index.php/es/layout/servicios/113-san-miguel/298-san-miguel

wordpress. (2017). *wordpress.com*. Obtenido de https://hilfrank.wordpress.com/fases-de-un-ataque-informatico/

ANEXOS

ANEXO 1: FORMATO DE ENTREVISTA

UNIVERSIDAD ESTATAL DE BOLÍVAR
FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA
ESCUELA DE SISTEMAS
UNIDAD DE TITULACIÓN

ENTREVISTA

Objetivo: Identificar las vulnerabilidades presentes en el servidor de base de datos de catastro de la municipalidad del Cantón San Miguel.

Entrevistador:……**Fecha:**……

Entrevistado:……**Lugar de la entrevista**:…….....

1. ¿Se ha realizado alguna prueba para detectar vulnerabilidades en el servidor de BD de catastro?

_____

_____

2. ¿Los dispositivos y periféricos son exclusivamente utilizados para el servidor de BD de catastro?

_____

_____

3. ¿El GAD cuenta con alguna herramienta de software para detectar vulnerabilidades el servidor de BD de catastro?

_____

_____

4. ¿Se permite el acceso al departamento de equipos informáticos a todo el personal?

_____

_____

5. ¿El personal tiene acceso a los puertos de comunicación el servidor de BD de catastro?

_____

_____

6. ¿Las contraseñas que utilizan en el servidor de BD de catastro, tienden a cambiarse con frecuencia?

_____

_____

ANEXO 2: FORMATO DE TÉCNICA DE OBSERVACIÓN

Proyecto:	Incidencia de Hacking Ético en el Servidor de Base de Datos de Catastro del Gobierno Autónomo Descentralizado del Cantón San Miguel, Año 2019.	**Observador:**		
Lugar:				
Objetivo de la observación:				
ACTIVIDADES		**SI**	**NO**	**DE VEZ EN CUANDO**
Los dispositivos y periféricos son exclusivamente utilizados para este servidor				
Se permite el acceso a este servidor a todo el personal				
Tiene herramientas para detectar intrusiones				
Las contraseñas que utiliza en este servidor, tiende a cambiar con frecuencia				
Los puertos del servidor de catastros están disponibles para todo el personal				