UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS GETIÓN EMPRESARIAL E INFORMATICA

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

ESCUELA DE SISTEMAS

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

INFORME FINAL DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARA OPTAR EL TÍTULO DE INGENIERA EN SISTEMAS COMPUTACIONALES

AUTORA:

JESSICA ESTEFANÍA LEMA TENELEMA

DIRECTOR:

ING. RODRIGO DEL POZO

PARES ACADEMICOS:

ING. DARWIN CARRIÓN LIC. EDGAR RIVADENEIRA

GUARANDA, AGOSTO DEL 2019

DERECHOS DE AUTOR

Yo Jessica Estefanía Lema Tenelema en calidad de autor del trabajo de investigación "**INCIDENCIA DE HACKING ÉTICO EN EL SERVIDOR DE BASE DE DATOS DE CATASTRO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAN MIGUEL, AÑO 2019**", autorizo a la Universidad Estatal de Bolívar hacer uso a todo los contenidos que pertenecen o parte de los contiene esta obra, con fines estrictamente académicos o de investigación.

Los derechos que como autora me corresponden, con excepción de la presente autorización, seguirán vigentes a mi favor, de conformidad con lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento.

Asimismo, autorizo a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de investigación en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Jessica Estefanía Lema Tenelema

C.I: 020241963-6

20190201002P01314 DECLARACION JURAMENTADA
OTORGA: JESSICA ESTEFANIA LEMA TENELEMA
CUANTIA: INDETERMINADA
DI 2 COPIAS

En la ciudad de Guaranda, provincia Bolívar, República del Ecuador, hoy día martes diecisiete de septiembre de dos mil diecinueve, ante mí DOCTOR HERNÁN RAMIRO CRIOLLO ARCOS, NOTARIO SEGUNDO DE ESTE CANTÓN, comparece la señorita Jessica Estefanía Lema Tenelema, por sus propios derechos. La compareciente es de nacionalidad ecuatoriana, mayor de edad, de estado civil soltera, domiciliada en San Pablo de Atenas, cantón San Miguel, provincia Bolívar, y de transito por este lugar, con celular número: cero nueve siete nueve seis dos cinco dos siete cinco, correo electrónico: estefanilema@gmail.com; a quien de conocerla doy fe en virtud de haberme exhibido su cédula de ciudadanía en base a la que procedo a obtener su certificado electrónico de datos de identidad ciudadana, del Registro Civil, mismo que agrego a esta escritura como documentos habilitantes; bien instruida por mí el Notario en el objeto y resultados de esta escritura de Declaración Juramentada que a celebrarla proceden, libre y voluntariamente.- En efecto juramentado que fue en legal forma previa las advertencias de la gravedad del juramento, de las penas de perjurio y de la obligación que tienen de decir la verdad con claridad y exactitud, declaran lo siguiente: "Que previo a la obtención del Título de Ingeniera en Sistemas Computacionales de la Facultad de Ciencias Administrativas Gestión Empresarial e Informática, otorgado por la Universidad Estatal de Bolívar, manifestó que el criterio e ideas emitidas en el presente Proyecto de Investigación:**"INCIDENCIA DE HACKING ÉTICO EN EL SERVIDOR DE BASE DE DATOS DE CATASTRO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN SAN MIGUEL, AÑO 2019"**, es de mi exclusiva responsabilidad en calidad de autora, es todo cuanto tengo que decir en honor a la verdad". Hasta aquí la declaración juramentada que junto con los documentos anexos y habilitantes que se incorpora queda elevada a escritura pública con todo el valor legal, y que a los compareciente aceptan en todas y cada una de sus partes, para la celebración de la presente escritura se observaron los preceptos y requisitos previstos en la Ley Notarial; y, leída que le fue a la compareciente por mí el Notario, se ratifica y firma conmigo en unidad de acto quedando incorporada en el Protocolo de esta Notaría, de todo cuanto DOY FE.

Srta. Jessica Estefanía Lema Tenelema
C. C. 0202419636

DR. HERNÁN RAMIRO CRIOLLO ARCOS
NOTARIO SEGUNDO DE CANTÓN GUARANDA

Se otorgó ante mi y en fe de ello confiero ésta Primera **copia certificada, firmada y sellada en** 3+5.
Guaranda, 17 **de** Septiembre **del 20**19.

Dr. Hernán Criollo Arcos
NOTARIO SEGUNDO DEL CANTÓN GUARANDA

REPÚBLICA DEL ECUADOR
Dirección General de Registro Civil, Identificación y Cedulación

Dirección General de Registro Civil, Identificación y Cedulación

CERTIFICADO DIGITAL DE DATOS DE IDENTIDAD

Número único de identificación: 0202419636

Nombres del ciudadano: LEMA TENELEMA JESSICA ESTEFANIA

Condición del cedulado: CIUDADANO

Lugar de nacimiento: ECUADOR/BOLIVAR/SAN MIGUEL/SAN PABLO DE ATENAS

Fecha de nacimiento: 22 DE MARZO DE 1995

Nacionalidad: ECUATORIANA

Sexo: MUJER

Instrucción: SUPERIOR

Profesión: ESTUDIANTE

Estado Civil: SOLTERO

Cónyuge: No Registra

Fecha de Matrimonio: No Registra

Nombres del padre: LEMA PUCHA JOSE ANGEL

Nacionalidad: ECUATORIANA

Nombres de la madre: TENELEMA ANGELA

Nacionalidad: ECUATORIANA

Fecha de expedición: 10 DE OCTUBRE DE 2017

Condición de donante: SI DONANTE

Información certificada a la fecha: 17 DE SEPTIEMBRE DE 2019
Emisor: HERNAN RAMIRO CRIOLLO ARCOS - BOLIVAR-GUARANDA-NT 2 - BOLIVAR - GUARANDA

N° de certificado: 197-261-12643

197-261-12643

Lcdo. Vicente Taiano G.
Director General del Registro Civil, Identificación y Cedulación
Documento firmado electrónicamente

La institución o persona ante quien se presente este certificado deberá validarlo en:**https://virtual.registrocivil.gob.ec**, conforme a la LOGIDAC Art. 4, numeral 1 y a la LCE.
Vigencia del documento 1 validación o 1 mes desde el día de su emisión. En caso de presentar inconvenientes con este documento escriba a **enlinea@registrocivil.gob.ec**

REPÚBLICA DEL ECUADOR
DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN

CÉDULA DE CIUDADANÍA
Nº 020241963-6

APELLIDOS Y NOMBRES
LEMA TENELEMA
JESSICA ESTEFANIA

LUGAR DE NACIMIENTO
BOLIVAR
SAN MIGUEL
SAN PABLO DE ATENAS

FECHA DE NACIMIENTO 1995-03-22
NACIONALIDAD ECUATORIANA
SEXO MUJER
ESTADO CIVIL SOLTERO

INSTRUCCIÓN SUPERIOR
PROFESIÓN / OCUPACIÓN ESTUDIANTE
V4133V4222

APELLIDOS Y NOMBRES DEL PADRE
LEMA PUCHA JOSE ANGEL

APELLIDOS Y NOMBRES DE LA MADRE
TENELEMA ANGELA

LUGAR Y FECHA DE EXPEDICIÓN
GUARANDA
2017-10-10

FECHA DE EXPIRACIÓN
2027-10-10

CERTIFICADO DE VOTACIÓN
24 - MARZO - 2019
CNE

0004 F
JUNTA No

0004 - 070
CERTIFICADO No

0202419636
CÉDULA No

LEMA TENELEMA JESSICA ESTEFANIA
APELLIDOS Y NOMBRES

PROVINCIA: BOLIVAR

CANTÓN: SAN MIGUEL

CIRCUNSCRIPCIÓN:

PARROQUIA: SAN PABLO DE ATENAS

ZONA: 1

Factura: 001-002-000018926

20190201002P01314

NOTARIO(A) HERNAN RAMIRO CRIOLLO ARCOS

NOTARÍA SEGUNDA DEL CANTON GUARANDA

EXTRACTO

Escritura Nº:	20190201002P01314

ACTO O CONTRATO:	
DECLARACIÓN JURAMENTADA PERSONA NATURAL	
FECHA DE OTORGAMIENTO:	17 DE SEPTIEMBRE DEL 2019, (10:03)

OTORGANTES

OTORGADO POR

Persona	Nombres/Razón social	Tipo interviniente	Documento de identidad	No. Identificación	Nacionalidad	Calidad	Persona que le representa
Natural	LEMA TENELEMA JESSICA ESTEFANIA	POR SUS PROPIOS DERECHOS	CÉDULA	0202419636	ECUATORIANA	COMPARECIENTE	

A FAVOR DE

Persona	Nombres/Razón social	Tipo interviniente	Documento de identidad	No. Identificación	Nacionalidad	Calidad	Persona que representa

UBICACIÓN

Provincia	Cantón	Parroquia
BOLÍVAR	GUARANDA	ANGEL POLIVIO CHAVEZ

DESCRIPCIÓN DOCUMENTO:	
OBJETO/OBSERVACIONES:	
CUANTÍA DEL ACTO O CONTRATO:	INDETERMINADA

NOTARIO(A) HERNAN RAMIRO CRIOLLO ARCOS

NOTARÍA SEGUNDA DEL CANTÓN GUARANDA

APROBACIÓN DEL TUTOR DEL TRABAJO DE TITULACIÓN

Yo, RODRIGO HUMBERTO DEL POZO DURANGO en calidad de director del proyecto 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"** presentado por la señorita JESSICA ESTEFANÍA LEMA TENELEMA, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas Gestión Empresarial e Informática, de la Universidad Estatal de Bolívar, considero que la misma reúne los requisitos y méritos necesarios en el campo metodológico y en el campo epistemológico, para ser sometida a la evaluación por parte del jurado examinador que se designe, por lo que lo APRUEBO, a fin de que el trabajo investigado sea habilitado para continuar con el proceso de titulación determinado por la Universidad Estatal de Bolívar.

En la ciudad de Guaranda a los 5 días del mes de agosto del año 2019.

Ing. Rodrigo Del Pozo
DIRECTOR DEL PROYECTO

APROBACIÓN DEL PAR ACADEMICO N°1 DEL TRABAJO DE TITULACIÓN

Yo, DARWIN PAUL CARRIÓN BUENAÑO en calidad de par académico del proyecto 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"** presentado por la señorita JESSICA ESTEFANÍA LEMA TENELEMA, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas Gestión Empresarial e Informática, de la Universidad Estatal de Bolívar, considero que la misma reúne los requisitos y méritos necesarios en el campo metodológico y en el campo epistemológico, para ser sometida a la evaluación por parte del jurado examinador que se designe, por lo que lo APRUEBO, a fin de que el trabajo investigado sea habilitado para continuar con el proceso de titulación determinado por la Universidad Estatal de Bolívar.

En la ciudad de Guaranda a los 5 días del mes de agosto del año 2019.

Ing. Darwin Carrión
PAR ACADÉMICO

APROBACIÓN DEL PAR ACADEMICO N°2 DEL TRABAJO DE TITULACIÓN

Yo, EDGAR PATRICIO RIVADENEIRA RAMOS en calidad de par académico del proyecto 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"** presentado por la señorita JESSICA ESTEFANÍA LEMA TENELEMA, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas Gestión Empresarial e Informática, de la Universidad Estatal de Bolívar, considero que la misma reúne los requisitos y méritos necesarios en el campo metodológico y en el campo epistemológico, para ser sometida a la evaluación por parte del jurado examinador que se designe, por lo que lo APRUEBO, a fin de que el trabajo investigado sea habilitado para continuar con el proceso de titulación determinado por la Universidad Estatal de Bolívar.

En la ciudad de Guaranda a los 5 días del mes de agosto del año 2019.

Lic. Edgar Rivadeneira
PAR ACADÉMICO

DEDICATORIA

Este presente proyecto se lo dedico a Dios quien me dio fuerzas pasa seguir adelante y no rendirme en las dificultades y llegar hasta este momento tan importante de mi formación profesional.

A mi familia principalmente a mis padres quienes me guiaron por el buen camino, ellos son mi mayor inspiración, con su apoyo constante su dedicación y esfuerzo hicieron lo posible para que yo alcanzara el éxito de este objetivo.

A mi hijo quien es mi mayor motivación el cual me impulso día a día para llegar a culminar esta etapa en mi vida.

A mis maestros, quienes con su nobleza y entusiasmo depositaron sus conocimientos y experiencia en mí, para guiarme y poder llegar hasta este momento.

Estefanía Lema

RECONOCIMIENTO

Principalmente agradezco a la Universidad Estatal de Bolívar, por haberme permitido ser parte de ella y abrirme sus puertas e impartir conocimientos a través de los diferentes docentes quienes me tutelaron durante todo el tiempo de estudio.

A mi Director Ing. Rodrigo del Pozo, a mis pares académicos Ing. Darwin Carrión y Lic. Edgar Rivadeneira quienes me asesoraron, orientaron y colaboraron durante todo el proceso que ha llevado la realización de este proyecto.

Al Gobierno Autónomo Descentralizado San Miguel de Bolívar por concederé la autorización para la realización del presente proyecto a través de los diferentes miembros de la institución y de manera especial al Abg. Stalin Carrasco alcalde del cantón quien me colaboro y apoyo con todo cuanto fue necesario.

Estefanía Lema

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

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

Guaranda, julio de 2019

RESUMEN

El presente proyecto de investigación comprende la elaboración de un proceso para identificar cual es el estado de seguridad informática con el que cuenta el servidor de base de datos de catastro del Gobierno Autónomo Descentralizado San Miguel. Para lo cual se realizó una entrevista al jefe de la unidad de sistemas, y se obtuvo información relevante de nuestro host objetivo, además a través de la observación directa se determinó posibles vulnerabilidades a las que está expuesto actualmente este servidor. En base a investigaciones realizadas se optó por el sistema operativo Kali Linux ya que este cuenta con múltiples herramientas pentest para la ejecución de hacking ético. Luego del estudio de distintos instrumentos pentest, se utilizó Nmap para el escaneo de los puertos, también con Nessus se realizó un escaneo avanzado y se encontró vulnerabilidades presentes en este, se eligió el framework Metasploit para la ejecución del ataque, en un ambiente controlado. Este proceso permitió detectar vulnerabilidades informáticas, además se pudo conocer el estado crítico de seguridad con el que cuenta el servidor en la actualidad. Con la investigación que se realizó se demuestra la importancia de llevar a cabo procesos para evaluar el nivel de seguridad informática con el que cuenta un servidor, determinando cuales son las posibles vulnerabilidades, para ello tomar medidas correctivas y preventivas 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, pentest, 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

Guaranda, July 2019

SUMMARY

This research project includes the development of a process to identify what is the state of computer security that has the database server cadastre of the San Miguel Decentralized Autonomous Government. For which an interview was made to the head of the systems unit, and relevant information was obtained from our target host, and through direct observation, possible vulnerabilities were determined to which this server is currently exposed. Based on research carried out, the Kali Linux operating system was chosen as it has multiple pentest tools for executing ethical hacking. After the study of different pentest instruments, Nmap was used to scan the ports, Nessus also performed an advanced scan and found vulnerabilities in it, the Metasploit framework was chosen to execute the attack, in a controlled environment. This process allowed us to detect computer vulnerabilities, as well as to know the critical security status that the server currently has. The research carried out demonstrates the importance of carrying out processes to evaluate the level of computer security that a server has, determining what the possible vulnerabilities are, in order to take corrective and preventive measures to prevent intruders from entering the systems that are housed in it and steal, destroy or alter information for your benefit.

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

CAPITULO I

INTRODUCCIÓN

En el departamento de la unidad de sistemas del Gobierno Autónomo Descentralizado San Miguel a través de la ejecución del proceso de hacking ético se ha determinado que el servidor de base de datos de catastro presenta varias vulnerabilidades, convirtiéndose esto una amenaza ya que la información alojada en este servidor puede ser alterada y ocasionar conflictos

En el capítulo I se detalla el contenido y estudio de la investigación: está compuesto por los antecedentes o estados del arte, formulación, preguntas directrices, objetivos generales y específicos y justificación del proyecto de investigación.

En el capítulo II está compuesto por la revisión de los temas relacionados a la investigación como el hacking ético, sus ventajas, tipos, modalidades de ejecución, vulnerabilidades informáticas, fases , servidor, base de datos, sistemas catastrales, Kali Linux, Metasploit, Nmap y otros temas importantes para el desarrollo de la investigación.

El capítulo III se explica la metodología de la investigación en el cual incluye los métodos y técnicas de investigación, técnicas de recolección de datos y respectivos análisis e interpretación de resultados.

Continuando en el capítulo IV tenemos la discusión, resultados, conclusión y recomendaciones de la investigación.

En el capítulo V concluimos con el desarrollo de la propuesta, su justificación, sus objetivos tanto general como específico y la aplicación de las fases para la detección de vulnerabilidades.

La elaboración y ejecución de esta investigación ha sido de gran importancia para identificar el grado de vulnerabilidad con el que cuenta el servidor de base de datos de catastro y con ello brindar posibles soluciones para ayudar a que el jefe de la unidad de sistemas tome medidas correctivas y salvaguardar la información que aloja este servidor.

ANTECEDENTES 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 de su 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. A medida que la infraestructura digital se hace cada vez más compleja e interconectada, la dificultad de lograr la seguridad en aplicaciones aumenta exponencialmente.

En la investigación de la Universidad Abierta de Cataluña de Barcelona, España (Días, Hacking Ético y Seguridad en Red, 2014) con el Título: "Hacking Ético y Seguridad en Red" menciona que ha visto que en la área de seguridad hay por un lado aquella persona que se preocupa en investigar los fallos de seguridad y al mismo tiempo buscar soluciones para esta misma, y por otro lado existe otra persona que se dedica a buscar estos mismos fallos pero luego de hacer uso de este mismo conocimiento para

solucionarlo, se dedica a violar la integridad de la información, robar contraseñas, infiltrar en sistemas etc. La primera persona se la hacker ético y la segunda hacker no ético. El profesional de hacker ético tiene que conocer un conjunto de herramientas de seguridad y cada una tiene su función propia. Algunas son utilizadas para hacer auditorías de seguridad donde se puede realizar una búsqueda automática de los fallos en la red o sistemas. También existen las que se puede utilizar para realizar pruebas de penetración. Para realizar un estudio se ha utilizado dos herramientas que son Nessus y Metasploit. Se ha podido comprobar la potencia de estas dos herramientas y la gran utilidad que tienen.

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." 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.

En el proyecto de investigación de la Universidad Técnica de Ambato previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos (Huilca Chicaiza., 2012) con el tema "Hacking Ético para Detectar Vulnerabilidades en los Servicios de la Intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos". Concluye que la información representa un papel muy importante dentro de las instituciones pues es la parte más primordial y día a día se encuentra expuesta a sufrir modificaciones y en muchos casos a ser robada en su totalidad, es por esto importante asegurar la información.

DESCRIPCION DEL PROBLEMA

Desde que la tecnología se ha vuelto una necesidad 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.

FORMULACIÓN DEL PROBLEMA

¿Cómo la aplicación de los resultados de un proceso del 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 levantar la información relevante del servidor de base de datos de catastro?
- ¿Por qué analizar el estado actual de seguridad informática del servidor de base de datos de catastro 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?

OBJETIVOS

Objetivo General

Identificar el estado de seguridad del servidor de base de datos de catastro del Gobierno Autónomo Descentralizado San Miguel a través de hacking ético.

Objetivos Específicos

- Levantar la información relevante del servidor de base de datos de catastro.
- Analizar el estado actual de seguridad informática del servidor de base de datos de catastro en la institución.
- Detectar las vulnerabilidades del servidor de base de datos de catastro.
- 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 de investigación, el cual pretende 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 evaluar la seguridad informática e identificar vulnerabilidades presentes, 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 la autorización y la predisposición del Gobierno Autónomo Descentralizado San Miguel y por ende poder aprovechar esta información para la prevención y protección de datos.

CAPITULO 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 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."

Hacker: (G A. , 2016) nos dice que es la "persona con talento, conocimiento, inteligencia e ingenuidad, relacionada con operaciones de computadoras, redes, seguridad, etc."

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

Hacking Ético: (G A. , 2016) habla que "consiste en romper la seguridad de una organización de forma sistemática y organizada con previa autorización escrita por dicha organización."

Seguridad informática: (Equipo de Expertos, 2018) indican 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."

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".

Servidor de base de datos: indica (InformaticaModerna, 2019) que es un "ordenador especialmente diseñado con arquitectura de alto rendimiento, en el cual se instala un robusto sistema operativo de servidor y un software que gestiona sistemáticamente grandes cantidades de datos pertenecientes a un mismo contexto".

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."

Sistema Catastral: (GALILEO Ingeniería y Servicios S.A, 2018). Habla que "el sistema de Gestión Catastral está enfocado a la explotación, gestión y actualización de datos catastrales (alfanumérica y cartográfica). Provee un servicio de información y asistencia a los ciudadanos en materia catastral, además permite al Municipio ejercer las funciones catastrales derivadas del convenio de colaboración con el organismo competente, la Dirección General del Catastro".

MARCO TEÓRICO

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, con el fin de reportarlas para tomar medidas sin poner en riesgo el sistema”.

Por lo tanto el hacking ético es una prueba de instrucción que combina pruebas técnicas y herramientas utilizados para una detección integral de vulnerabilidades de los sistemas informáticos.

Objetivos del Hacking Ético

- Evaluar la preparación de la institución para resistir y/o detectar un ataque dirigido, sea éste externo o interno y fortalecer la seguridad de los Sistemas de Información.
- Acceder a los ordenadores de la organización, con permisos de sus propietarios.
- Detectar debilidades y vulnerabilidades de la infraestructura de las tecnologías de información de las organizaciones, y elaborar informes.
- Proporcionar mayor protección y fiabilidad a los sistemas de información de las empresas.

Ventajas

- Conocer las vulnerabilidades de los diferentes sistemas informáticos para sugerir tomar los correctivos necesarios a tiempo, antes de ser víctimas de un ataque.

- Protección de la inversión, ahorro de costos y tiempo al prevenir pérdidas de información, en lugar de los costos asociados cuando se responde a un evento de forma reactiva.
- Mantenimiento de la imagen corporativa y de la confianza de los contribuyentes, contrario a lo que ocurriría cuando un incidente comprometa la seguridad.

Tipos de Hacking

Según (Capa8, 2015) indica que dependiendo de dónde se ejecuten las pruebas de intrusión el hacking ético puede ser interno o externo.

Hacking Ético Externo: Este tipo de hacking se realiza desde Internet sobre la infraestructura de red pública del cliente; es decir sobre aquellos equipos de la organización que están expuestos a Internet porque brindan un servicio público. Ejemplo de equipos públicos: Enrutador, Firewall, Servidor Web, Servidor de Correo, Servidor de nombres (DNS) etc.

Hacking Ético Interno: Como su nombre sugiere este tipo de hacking se ejecuta en la red interna del cliente, desde el punto de vista de un empleado de la empereza, un consultor o un asociado de negocios que tiene acceso a la red corporativa.

En este tipo de pruebas de intrusión se suele encontrar más huecos de seguridad que en su contra-parte externa debido a que muchos administradores de sistemas se preocupan por proteger el perímetro de su red y subestiman el atacante interno. Esto es un error puesto que estudios demuestran que la mayoría de ataques exitosos provienen del interior de la empresa. Un ejemplo, en una encuesta sobre seguridad informática realizada a un grupo de empresarios en el Reino Unido, cuando se les pregunto quiénes eran los atacantes, se obtuvieron estas cifras: Externo 25% Interno 75%.

Modalidades de Hacking

(Capa8, 2015) Dependiendo de la modalidad que el cliente provea al consultor, el servicio de hacking ético se puede ejecutar en una de las 3 modalidades:

- Caja Negra
- Caja Gris
- Caja Blanca

La modalidad escogida afectara el costo y la duración de las pruebas de intrusión, puesto que a menor información recibida mayor será el tiempo invertido en investigar por parte del auditor.

Hacking de caja negra: Esta modalidad se aplica a pruebas de intrusión externas, se llama de este modo, por que el cliente solamente le proporciona el nombre de la empresa a auditar al consultor, por lo que este obra a ciegas, la infraestructura de la organización es una caja negra para él.

Si bien este tipo de auditorías se considera más realista dado que usualmente un agresor externo que elige una víctima X no tiene más información al inicio que el nombre de la organización a atacar, también es cierto que requiere una mayor inversión de tiempo y por ende el costo incluido es superior también. adicionalmente se debe notar que el Hacker ético a diferencia del Cracker no cuenta con todo el tiempo del mundo para efectuar las pruebas de intrusión, por lo que la fase preliminar de indagación no puede extenderse más allá de lo que en términos prácticos sea posible para el cliente en razón de costo, tiempo, beneficio.

Por lo tanto se dice que este tipo de hacking se efectúa usualmente sobre la red perimetral o pública del cliente, con absoluto desconocimiento de la infraestructura informática del

cliente, es decir que no proporcionan ninguna información sobre sus sistemas informáticos. El objetivo es emular un ataque externo, realizado por un pirata informático que no tiene relación con la empresa cliente.

Hacking de caja gris: Suele utilizarse como sinónimo para referirse a las pruebas de intrusión internas, pero algunos auditores les llaman también así a una prueba externa a la cual el cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como las direcciones IP y el tipo, función del equipo (Router, Firewall, Server, etc.).

Cuando el termino se aplica a pruebas internas se denomina así porque el consultor recibe por parte del cliente los accesos solamente que tendría un empleado de la empresa, es decir, un punto de red para la estación de auditoria y datos de configuración local (IP, Mascara de subred, Gateway y DNS); pero no le revela información adicional como por ejemplo: usuario, clave para ingresar al dominio, la existencia de subredes anexas, etc.

Por lo tanto el hacking de caja gris es aquel que se efectúa sobre la red privada del cliente, pero sin que se brinde mayor información sobre la misma; emulando un ataque perpetrado por un usuario interno no-autorizado, ya sea un empleado de la empresa o un asesor externo que tiene acceso físico a la red de la organización.

Hacking de caja blanca: Algunas veces denominado hacking transparente. Esta modalidad se aplica a pruebas de intrusión solamente y se llama de esta forma por que la empresa cliente le da al auditor información completa de las redes y los sistemas a auditar.

Es decir, que además de asignarle un punto de red e información de configuración para la estación de auditoria, como en el hacking de caja gris el consultor recibe información extensa como diagramas de red, listado detallado de equipos a auditar incluyendo nombres, tipos, plataformas, servicios principales, direcciones IP, información sobre subredes remotas, etc., debido a que el consultor evita investigar toda esta información por sí mismo, este tipo de hacking suele tomar menos tiempo para ejecutarse y por ende reduce costos también.

Entonces esta clase de hacking también se efectúa sobre la red privada del cliente, pero en esta ocasión se debe proporcionar un punto de red con direccionamiento IP válido y un listado de las direcciones IP de los equipos a analizar. La idea es simular un ataque perpetrado por un usuario interno autorizado.

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 (Huilca Chicaiza., 2012) hay múltiples vulnerabilidades informáticas y según sus características se clasifican en un determinado tipo u otro. Las vulnerabilidades más conocidas:

Vulnerabilidad de desbordamiento de buffer (Buffer Overflow)

Existen varios 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 último pase 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.

Inyección de código

Se trata de una vulnerabilidad que está basada en la existencia de parámetros de determinadas aplicaciones 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 u**suario**

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 marcha algún comando malicioso. Para complementar el ataque del usuario, se habla de la publicación en sitios web vulnerables que consiste en incluir algún dato en el 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.

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.

Ingeniería Social

Consiste en una manera que tienen los hackers en engañar a los usuarios haciéndose pasar por otras personas o entidades.

Redes Wi-Fi

Estos ataques se dan porque todavía se utiliza 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 estos 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.

Fases para detectar vulnerabilidades

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

Fase 1: Reconocimiento

Esta etapa involucra la obtención de información con respecto a una potencial víctima que en este caso es el servidor de base de datos de catastro.

Fase 2: Escaneo

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el servidor de base de datos de catastro como direcciones IP, nombres de host, datos de autenticación, entre otros.

Fase 3: Obtener acceso

En esta instancia comienza a materializarse el ataque al servidor de base de datos de catastro a través de la explotación de las vulnerabilidades y defectos que se encontraron durante las fases de reconocimiento y escaneo.

Fase 4: Mantener el acceso

Una vez que se ha conseguido acceder al sistema, se buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet.

Fase 5: Borrar huellas

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 jefe de la unidad de sistemas.

Formas de Atacar a Servidores

(HDCO, 2016) Indica que 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.

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.

Es cuando un intruso bloquea la transmisión de la información para que el receptor no la reciba por lo tanto afecta al principio de disponibilidad de la información.

Fuerza Bruta

Estos son básicamente intenta “romper” todas las combinaciones posibles de nombre de usuario y contraseña. Los ataques de fuerza bruta buscan contraseñas débiles para ser descifradas y tener acceso de forma fácil.

Malware

Según (Ramiro, 2018)es una forma corta de software malicioso. El malware no es lo mismo que el software defectuoso, es decir, el software que tiene un propósito legítimo pero contiene errores dañinos. 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.

Kali Linux

Según (MLX, 2018) menciona que “Kali incluye herramientas de penetración y auditoría de seguridad como sea posible en un paquete conveniente.”

En el presente proyecto se utiliza este sistema operativo ya que este tiene muchas herramientas de código abierto para realizar pruebas de seguridad que se recopilan y están listas para usar.

Ventajas

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

1. Linux es muy robusto, estable y rápido.

2. Linux es libre.

3. Linux ya no está restringido a personas con grandes conocimientos de informática.

Kali dispone de:

1. Kali tiene herramientas de seguridad
2. Tiene herramientas clásicas de recopilación de información como Nmap y Wireshark.
3. 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.

Por lo tanto Kali Linux tiene herramientas y aplicaciones relacionadas con la seguridad informática de las cuales se hace uso, destacando algunas tan conocidas como nmap, que a través de esta escanearemos los puertos del servidor de base de datos de catastro.

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 escaneo y asegura los cumplimientos de seguridad

En este proyecto se utiliza Nessus porque a través de este se identifica las debilidades y errores de configuración del servidor de base de datos de catastro, que pueden ser usados por los ataques. A través de este se reduce el tiempo de respuesta y costo de la aplicación del escaneo.

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. 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 pentest sea comparativamente más sencilla".

Se utiliza en el proyecto ya que este es 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.

Con Metasploit Framework se puede hacer:

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

- **Análisis de vulnerabilidad:** Implica encontrar e identificar vulnerabilidades conocidas y desconocidas presentes en el servidor de base de datos de catastro y validarlas.

- **Explotación:** Esta fase funciona aprovechando las vulnerabilidades descubiertas en la fase anterior. Esto normalmente significa que se está tratando de obtener acceso al servidor de base de datos de catastro.

MARCO LEGAL

Código Orgánico Integral Penal (COIP)

Capítulo Segundo

Delitos Contra Los Derechos De Libertad

Sección Sexta

Según el (Código Orgánico Integral Penal, 2017) los delitos contra el derecho a la intimidad personal y familiar son:

Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Sección Novena

Según (Código Orgánico Integral Penal, 2017) los delitos contra el derecho a la propiedad son:

Art. 186.- Estafa.- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.
4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.

La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.

La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos privados públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años.

La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días.

Nota: Inciso cuarto reformado por artículo 2 de Ley No. 0, publicada en Registro Oficial Suplemento 598 de 30 de Septiembre del 2015.

Art. 187.- Abuso de confianza.- La persona que disponga, para sí o una tercera, de dinero, bienes o activos patrimoniales entregados con la condición de restituirlos o usarlos de un modo determinado, será sancionada con pena privativa de libertad de uno a tres años.

La misma pena se impone a la persona que, abusando de la firma de otra, en documento en blanco, extienda con ella algún documento en perjuicio de la firmante o de una tercera.

Art. 188.- Aprovechamiento ilícito de servicios públicos.- La persona que altere los sistemas de control o aparatos contadores para aprovecharse de los servicios públicos de energía eléctrica, agua, derivados de hidrocarburos, gas natural, gas licuado de petróleo o de telecomunicaciones, en beneficio propio o de terceros, o efectúen conexiones directas, destruyan, perforen o manipulen las instalaciones de transporte, comunicación o acceso a los mencionados servicios, será sancionada con pena privativa de libertad de seis meses a dos años.

La pena máxima prevista se impondrá a la o al servidor público que permita o facilite la comisión de la infracción u omita efectuar la denuncia de la comisión de la infracción.

La persona que ofrezca, preste o comercialice servicios públicos de luz eléctrica, telecomunicaciones o agua potable sin estar legalmente facultada, mediante concesión, autorización, licencia, permiso, convenios, registros o cualquier otra forma de contratación administrativa, será sancionada con pena privativa de libertad de uno a tres años.

Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptados, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Capítulo Tercero

Delitos Contra Los Derechos Del Buen Vivir

Sección Tercera

Indica el (Código Orgánico Integral Penal, 2017) que los delitos contra la seguridad de los activos de los sistemas de información y comunicación son:

Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Art. 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Art. 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema

informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

CAPÍTULO III

METODOLOGÍA

En el presente proyecto de investigación se utilizaron métodos, técnicas e instrumentos que se detallan a continuación:

Método Cualitativo

Se desarrollado bajo un enfoque cualitativo porque el problema requiere investigación interna, pues es muy importante lo que se logró detectar con la aplicación del hacking ético para detectar vulnerabilidades en el servidor de base de datos de catastro del Gobierno Autónomo Descentralizado San Miguel.

Tipos de Investigación

Entre los tipos de investigación utilizados para el desarrollo de este proyecto están:

Método descriptivo: El cual permitió conocer el nivel de seguridad con el que cuenta el servidor de base de datos de catastro a través de una descripción de características del área a investigar.

Método bibliográfico: Se consideró esta modalidad ya que se utilizó libros, artículos, trabajos de grado, páginas de internet, etc. los cuales ayudaron a conocer y analizar los fundamentos teóricos más relevantes y todos los recursos disponibles para realizar el presente proyecto de investigación.

Método de campo: Se utilizó este tipo de investigación puesto que el estudio del problema se lo realizo en lugar donde se están generando los hechos; de esta manera podemos conocer problemas que se producen en el Gobierno Autónomo Descentralizado San Miguel al no llevar a cabo procesos controlados de hacking ético para evaluar el estado de seguridad con el que cuenta el servidor.

Técnicas o instrumentos para la investigación

Los instrumentos que se utilizaron para el desarrollo de esta investigación fueron:

La observación: Se observó las funciones que se realiza el servidor de base de datos de catastro y el nivel de seguridad con el que cuenta, se ejecutó una simulación de ataque en un ambiente controlado y bajo supervisión del jefe de la unidad de sistemas.

Se pudo observar que los dispositivos y periféricos no se utilizan exclusivamente en el servidor de base de datos de catastro, estos son utilizados para diferentes servidores.

El acceso a este servidor es restringido para personas externas, pero puede acceder el personal de la institución.

Se evidencio que la unidad de sistemas no cuenta con un IDS (Sistema de Detección de Intrusiones). (Ver Anexo E)

La entrevista: Permitió recopilar información necesaria sobre el servidor de base de datos de catastro.

Una vez realizada la entrevista al jefe del unidad de sistemas del Gobierno Autónomo Descentralizado San Miguel, se determinó que al pasar del tiempo no se ha llevado a cabo ningún proceso para el determinar el nivel de seguridad en el servidor de base de datos de catastro, se denota que no todos los dispositivos de entrada y salida de datos son utilizados estrictamente en este, también mencionó que este servidor no cuenta con una herramienta de software que le ayude a determinar posibles fallos o intentos de intrusiones, por estas razones es que se lleva a cabo esta investigación dentro de la institución, para que pueda adelantarse a los posibles y futuros ataques solucionando las vulnerabilidades y mejorando los procesos internos de seguridad.

Una vez analizada la entrevista se llegó a la conclusión que es necesario poner en marcha el proceso de hacking ético al servidor de base de datos de catastro; con la finalidad de que ayude a detectar las vulnerabilidades de este, se cuenta con la predisposición del alcalde y la colaboración del jefe del unidad de sistemas, para obtener información detallada, sistematizada e integral. (Ver Anexo F)

Población y muestra

Población: Para la presente investigación se tomó como población al jefe de la unidad de sistemas del Gobierno Autónomo Descentralizado San Miguel.

Muestra: El objeto de estudio es pequeño y se toma su totalidad.

Análisis de Riesgos

Si se considera que la información que se maneja en el servidor de base de datos de catastro es de gran valor para el Gobierno Autónomo Descentralizado San Miguel se debe empezar a pensar en poner en práctica un Plan Director de Seguridad.

Fase 1. Definición del alcance

El primer paso que se siguió fue definir el alcance de este análisis de riesgo. El alcance de esta investigación es el servidor de base de datos de catastro que está en custodia de la unidad de sistemas, del Gobierno Autónomo Descentralizado del Cantón San Miguel, Provincia Bolívar, Ecuador.

La unidad de sistemas es la encargada de la administración de los equipos y sistemas informáticos, dar soporte técnico a los equipos y sistemas que brindan servicios a la institución. Para cumplir con sus objetivos, la unidad cuenta con un departamento sistemas informáticos.

Fase 2. Identificación de activo

Una vez definido el alcance se procedió a identificar los activos. Entre los activos de información, según la clasificación de la ISO 17799:2005, se encuentran:

- Activos físicos (computadoras, servidores, medios magnéticos, enrutadores, entre otros)

Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
Servidor de base de datos de catastro	Servidor con Sistema Operativo Microsoft 2003 Server	Unidad de Sistemas	Servidor (físico)	Departamento de sistemas	Si

Tabla 1: Identificación de activo

Fase 3. Identificación de vulnerabilidades y amenazas

(Guanoluisa & Maldonado, 2015) Nos dicen que "una vulnerabilidad o fallo de seguridad, es todo aquello que hace que nuestros sistemas de información funcionen de forma diferente para lo que estaban pensados, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible".

La seguridad de servidores es tan importante como la seguridad de la red debido a que los servidores usualmente contienen una gran cantidad de información vital de la organización.

Si un servidor está comprometido, todos sus contenidos pueden estar disponibles para que un pirata los manipule o robe a su gusto. En la siguiente tabla se detallan algunos de los problemas más importantes.

Vulnerabilidades	Amenazas
Servicios inutilizados y puertos abiertos	**Servicios no deseados, tales como telnet, dhcp, o dns, se ejecuten en un servidor o estación de trabajo sin que el administrador se entere, lo cual en consecuencia puede causar tráfico indeseado al servidor, o más aún, un camino de entrada potencial para los piratas.**
Servicios sin sus parches	Los desarrolladores y administradores de sistemas a menudo encuentran fallas en las aplicaciones de servidores y publican la información de la falla en sitios de internet que se dedican al seguimiento de errores y seguridad. Aun cuando estos mecanismos constituyen una forma efectiva de alertar a la comunidad sobre vulnerabilidades de seguridad, depende de los administradores de sistemas el aplicar los parches de sistemas a tiempo. Esto es particularmente cierto puesto que los crackers tienen acceso a las mismas fuentes e intentarán utilizar esta información para violar sistemas que no hayan sido emparchados.
Administración desatendida	Una de las amenazas más grandes a la seguridad de los servidores son los administradores distraídos que olvidan remendar sus sistemas. Algunos administradores fallan al momento de poner parches en sus servidores y estaciones de trabajo, mientras que otros fallan en leer los mensajes del registro de eventos del kernel del sistema o tráfico de

	la red. Otro error común es dejar las contraseñas o llaves a servicios sin modificar. Si un administrador de bases de datos no cambia las contraseñas, hasta un cracker sin mucha experiencia puede utilizar una contraseña conocida por todo el mundo para ganar acceso con privilegios administrativos.
Servicios intrínsecamente inseguros	Una categoría de servicios de red inseguros son aquellos que requieren nombres y contraseñas de usuario sin encriptar para la autenticación. Telnet y FTP son dos de estos servicios. Un software de husmeo de paquetes que esté monitoreando el tráfico entre un usuario remoto y tal servicio, puede fácilmente robarse los nombres de usuario y contraseña. Tales servicios pueden también ser presa fácil de lo que en términos de seguridad se conoce como un ataque de hombre en el medio. Un hacker que gana acceso a una base de datos puede tener acceso a todas las cuentas de usuarios en la red, incluyendo la cuenta del administrador.

Tabla 2: Identificación de vulnerabilidades y amenazas

Fase 4. Estimación del riesgo

La estimación del riesgo según (Guanoluisa & Maldonado, 2015) es la "Actividad para asignar valores a la posibilidad y las consecuencias de un riesgo"

Valoración de Impacto

Para valorar el impacto se establece 1 para el valor mínimo, 2 para el valor medio y 3 para el valor alto.

Servidor de Base de Datos de Catastro					
Vulnerabilidad	**Fuente de Amenaza**	**Confiabilidad**	**Integridad**	**Disponibilidad**	**Impacto**
Servicios inutilizados y puertos abiertos	Hacker	3	3	3	**3**
Servicios sin sus parches	Hacker	2	1	2	**2**
Administración desatendida	Hacker	3	3	2	**3**
Servicios intrínsecamente inseguros	Hacker	1	3	1	**2**

Tabla 3: Valoración del impacto

El promedio de valoraciones entre los criterios de confidencialidad, integridad y disponibilidad en cuanto a los servicios inutilizados y puertos abiertos es de 3, en los servicios sin sus parches es de 1,67 lo que en números enteros es 2, en administración desatendida es de 2,67 lo que en números enteros es 3, en servicios intrínsecamente inseguros es de 1,67 lo que en números enteros es 2 de impacto en el activo Servidor de Base de Datos de Catastro frente a la amenaza que un hacker llegase a cumplir sus objetivos.

Valoración de Incidentes

Para valorar los incidentes se establece 1 para el valor poco probable, 2 para el valor medianamente probable, 3 para el valor probable y 4 para el valor muy probable.

Servidor de Base de Datos de Catastro			
Tipo de Amenaza	**Vulnerabilidad**	**Fuente de Amenaza**	**Probabilidad**
Tráfico indeseado al servidor	**Servicios inutilizados y puertos abiertos**	**Hacker**	**4**
Información de fallos en sitios de internet dedicados al seguimiento de errores y seguridad.	Servicios sin sus parches	Hacker	**2**
Administradores distraídos	Administración desatendida	Hacker	**3**
Servicios de red que soliciten nombres y contraseñas de usuario sin encriptar para la autenticación.	Servicios intrínsecamente inseguros	Hacker	**3**

Tabla 4: Valoración de incidentes

La probabilidad de ocurrencia de la amenaza "Tráfico indeseado al servidor" es alta por lo que su valoración es 3, la probabilidad de ocurrencia de la amenaza "Información de fallos en sitios de internet dedicados al seguimiento de errores y seguridad" es media por lo que su valoración es 2, la probabilidad de ocurrencia de la amenaza "Administradores distraídos" es alta por lo que su valoración es 3, la probabilidad de ocurrencia de la amenaza "Servicios de red que soliciten nombres y contraseñas de usuario sin encriptar para la autenticación" es media por lo que su valoración es 2.

Fase 5. Evaluación del riesgo

Esta fase se dedica a la evaluación del riesgo, para lo cual se identificó el activo, así como también sus respectivas vulnerabilidades y el impacto que provoca si la amenaza ocurre.

Aquí se muestra los resultados obtenidos de la evaluación del riesgo al activo “Servidor Microsoft 2003 Server”.

El producto entre la probabilidad de ocurrencia de una amenaza y el impacto que esta pudiese ocasionar da como resultado el nivel de riesgo de cada activo, en donde 1-2 se considera bajo, 3-4 se considera moderado, 5-8 se considera alto, de 9-12 se considera crítico.

Servidor de Base de Datos de Catastro									
Tipo de Amenaza	**Vulnerabilidad**	**Fuente de Amenaza**	**Confiabilidad**	**Integridad**	**Disponibilidad**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**	**Riesgo**
Tráfico indeseado al servidor	Servicios inutilizados y puertos abiertos	Hacker	3	3	3	3	4	12	Critico
Información de fallos en sitios webs de seguimiento de errores y seguridad.	Servicios sin sus parches	Hacker	2	1	2	2	2	4	Moderado
Administradores distraídos	Administración desatendida	Hacker	3	3	2	3	3	9	Alto
Servicios de red que soliciten nombres y contraseñas de usuario sin encriptar para la autenticación.	Servicios intrínsecamente inseguros	Hacker	1	3	1	2	3	6	Alto

Tabla 5: Nivel de riesgo

Plan de Contingencia

El plan de contingencia es importante para salvaguardar la integridad de la información que posee el servidor de base de datos de catastro del Gobierno Autónomo Descentralizado San Miguel, en este caso, ante un ciberataque que compromete el sistema catastral y pueden existir filtrados de archivos o documentos confidenciales.

Este plan establece las directrices a seguir ante un ciberataque. Este procedimiento guía al personal de seguridades de la institución a identificar, mitigar y restablecer los sistemas informáticos ante intrusiones ilegales, caída de servicios, o fallos en la infraestructura tecnológica. Así mismo, los identifica como los únicos autorizados para realizar declaraciones sobre los incidentes ocurridos, sus causas y soluciones temporales y a largo plazo

Ahora definimos las acciones a tomar para recuperarnos de la ocurrencia de un desastre. Este Plan de Recuperación contiene 3 etapas:

1. Prevención

Actualmente, resulta imposible crear un entorno informático inaccesible a delincuentes informáticos aunque si se puede constituir un entorno preventivo que dificulte el acceso a los hackers, incorporando medidas preventivas:

a. Medidas preventivas organizativas

- Desarrollar dentro de la organización buenas prácticas para la gestión de la fuga de información.
- Definir una política de seguridad y procedimientos para los ciclos de vida de los datos.

- Establecer un sistema de clasificación de la información.
- Definir roles y niveles de acceso a la información.
- Protección del papel. Desarrollo de políticas para la destrucción del papel, conservación de documentación, políticas de escritorio limpio.
- Control de los dispositivos extraíbles (pendrives, discos externos, cd, etc.)
- Desarrollo de planes de formación en materia de ciberseguridad y seguridad de la información, buenas prácticas de los sistemas informáticos etc.

b. Medidas preventivas legales:

- Solicitud de aceptación de la política de seguridad por parte de los empleados.
- Cláusulas contractuales con empleados en relación a la custodia, conservación y utilización de la información.
- Cláusulas contractuales con terceros en materia de confidencialidad.
- El establecimiento de una política de uso de medios tecnológicos, que determine el alcance del uso de los dispositivos y medios puestos a disposición del jefe de la unidad de sistemas por parte del Gobierno Autónomo Descentralizado San Miguel y las facultades del alcalde en relación con el control de la actividad de los empleados, así como las consecuencias derivadas del incumplimiento de la misma.

2. Detección

El momento en el que se detecta un incidente de fuga de información es un momento crítico en la entidad. Una buena gestión de la fase de detección del ataque informático puede suponer una reducción significativa del impacto del ataque.

Esta fase es muy importante, ya que muchas veces se tiene conocimiento de la irrupción una vez la información sustraída se revela al público o a la red, o el ciberdelincuente se pone en contacto el miembro correspondiente del Gobierno Autónomo Descentralizado San Miguel, para revenderles la información, extorsionarles o amenazarles.

Las principales medidas en esta fase de detección son técnicas, pues resulta imprescindible contar con una continua monitorización de los sistemas que permita detectar cualquier entrada sospechosa. Sin embargo también podemos encontrar medidas legales y organizativas:

a. Medias de detección organizativas:

Diseñar un protocolo interno de gestión del incidente en el que se identifique un gabinete de crisis u órgano decisorio de las medidas a adoptar. Esta unidad debe estar compuesto por personas con capacidad de decisión, que puedan decidir, gestionar y coordinar la situación con calma, evitando consecuencias adicionales negativas.

b. Medidas de detección legales:

Se deberán registrar las incidencias o brechas de seguridad en el Documento de Seguridad que la empresa u organización debe desarrollar y mantener actualizado, de tal forma que quede constancia de tipo de incidencia, el momento en que se ha producido o detectado, la persona que realiza la notificación, la persona o personas a quien se realiza la notificación, los efectos que se derivan de la incidencia, las medidas correctoras que se han aplicado de acuerdo al Código Orgánico Integral Penal (COIP).

Además, si la empresa realizase un tratamiento de datos de nivel medio o nivel alto, se deberán registrar, además de los extremos ya mencionados, los procedimientos de recuperación realizados, la persona o personas que realizó el proceso de recuperación, los datos que han sido restaurados.

3. Recuperación

Una vez que se detecta una entrada ilegal en los sistemas informáticos del despacho es necesario llevar a cabo un plan organizado de recuperación, cuyo objetivo no es otro que recuperar el servicio y dejarlo tal y como estaba antes del incidente. Para ello se deben implantar medidas técnicas de recuperación de la información: backups de los sistemas, copias de seguridad etc.

Entre las medidas organizativas que se pueden desarrollar para la recuperación se encuentra la elaboración de planes de continuidad del negocio que contemplen situaciones excepcionales que puedan producirse por ataques informáticos y que abarquen situaciones tanto de robo de información, como de bloqueo del sistema e incluso de borrado de datos. Además, se recomienda realizar un informe por un perito externo de cara a la presentación de una denuncia ante las autoridades, que permita recoger todas las pruebas que faciliten una posterior investigación.

Otras Medidas

Por último debemos atender a otras medidas accesorias que se pueden implementar dentro de nuestro despacho de abogados y que van a contribuir a crear un entorno de seguridad y concienciación en materia de prevención, detección, recuperación y respuesta ante ataques informáticos como:

- Atender a las buenas prácticas de la ISO 27001 en materia de seguridad de la información.
- Apoyarse en terceros expertos independientes que puedan ayudar tanto en el desarrollo de todo el proceso, desde el desarrollo de políticas internas, como en la custodia de información a la hora de actuar ante alguno de los incidentes expuestos.

CAPITULO VI

DISCUSIÓN

Para el desarrollo del presente proyecto de investigación se realizó el estudio de diversos conceptos, teorías de autores como Tori, Díaz, Huilca entre otros, los cuales fueron una ayuda fundamental en la investigación con respecto al hacking ético para poder determinar las vulnerabilidades existentes en el servidor de base de datos de catastro que es el objeto de estudio.

En el Gobierno Autónomo Descentralizado San Miguel se llevó a cabo el proceso de hacking ético para determinar el nivel de seguridad del servidor de base de datos de catastro a través de la ejecución del escaneo de puertos y servicios, ya que en este nunca antes se lo ha realizado, lo que lo ha tenido expuesto a amenazas.

El hacking ético le permitirá encontrar, conocer y solventar las vulnerabilidades que piratas informáticos maliciosos puedan utilizar para acceder a la base de datos del servidor de base de datos de catastro y perjudicar a la entidad.

RESULTADOS

Con el conocimiento que se obtuvo a través del levantamiento de la información se logró ejecutar favorablemente las fases del hacking ético en el servidor de catastro del Gobierno Autónomo Descentralizado San Miguel y con ello se tomó medidas correctivas.

Al finalizar este trabajo, permitió conocer las vulnerabilidades a los que está expuesto el servidor de base de datos de catastro que como resultado permite visualizar el 10% vulnerabilidades críticas, 10% medias y datos de información.

Luego de detectar las vulnerabilidades a nivel de puertos y servicios con los que cuentan el servidor de base de datos de catastro se ejecutó la explotación de estas falencias de manera inmediata, en un ambiente controlado bajo la supervisión del jefe inmediato de la unidad de sistemas.

CONCLUSIÓN

- La unidad de sistemas del Gobierno Autónomo Descentralizado San Miguel no cuenta con un IDS (Sistema de Detección de Intrusiones) para detectar posibles intrusiones al servidor de base de datos de catastro de acuerdo a la entrevista realizada al jefe de la unidad.
- El servidor de base de datos de catastro de la unidad de sistemas no es totalmente seguro por lo que está poniendo en riesgo la seguridad de la información alojada en el mismo.
- El servidor de base de datos de catastro de la institución está inmerso a amenazas y esto conlleva un riesgo para la entidad.
- El ataque que se realizó al servidor de base de datos de catastro fue exitoso por lo que se puso en riesgo la seguridad de la información pudiendo haber sido alterada, modificada o en el peor de los casos pudo ser borrada en su totalidad.

RECOMENDACIONES

- Debido a la inexistencia de un IDS en la unidad de sistemas para que detecte intrusiones en el servidor de base de datos de catastro, se recomienda implementar uno de estos.
- Por la inseguridad que posee el servidor de base de datos de catastro es necesario aumentar seguridad en este para asegurar la información.
- Se debe considerar la importancia y sensibilidad de la información y servicios que presta el servidor de base de datos de catastro por lo que es necesario establecer políticas de seguridad dentro de la unidad de sistemas.
- Se recomienda poner en práctica el proceso de Hacking ético para detectar vulnerabilidades en los servidores del Gobierno Autónomo Descentralizado San Miguel, porque con la detección de las mismas a tiempo se reportaran las fallas de seguridad alertando al jefe de la unidad de sistemas y se podrá brindar posibles soluciones para que este inmediatamente arregle los problemas encontrados y así evitar un posible robo o alteración de la información.

CAPÍTULO V

PROPUESTA DE SOLUCIÓN DEL PROBLEMA

Tema

Hacking Ético en el Servidor de Base de Datos de Catastro del Gobierno Autónomo Descentralizado del Cantón San Miguel

Justificación

Es primordial la ejecución del presente proyecto ya que la detección de vulnerabilidades en el servidor de base de datos de catastro de la unidad de sistemas de Gobierno Autónomo San Miguel ayudará a determinar a qué ataques está expuesto este.

La aplicación del proceso de hacking ético permitirá detectar a tiempo fallas de seguridad en el servidor de base de datos de catastro, siendo de ayuda y alerta para el jefe de la unidad de sistemas antes que se lleve a cabo un ataque.

El proyecto es necesario ya que el servidor con sus respectivos servicios tienen que estar bien configurados con todas las medidas de seguridad, para que su información siempre se encuentre disponible, sea integra y confiable.

La investigación ejecutada es importante porque a través de ella se brindará posibles soluciones con la finalidad de proteger la información que se encuentra alojada en el servidor de base de datos de catastro.

Objetivos

Objetivo General

Identificar las vulnerabilidades en el servidor de base de datos de catastro del Gobierno Autónomo Descentralizado San Miguel a través de hacking ético.

Objetivos Específicos

- Seleccionar las herramientas necesarias para la ejecución de hacking ético.
- Realizar pruebas de penetración en el servidor de base de datos de catastro.
- Presentar las vulnerabilidades encontradas y el grado de incidencia en la inseguridad en el servidor de catastro de la unidad de sistemas del gobierno autónomo descentralizado san miguel.

Análisis de Factibilidad

Según el tipo de propuesta se debe tener en cuenta ciertos aspectos de viabilidad:

Política: El Gobierno Autónomo Descentralizado San Miguel tiene como política asegurar la información por lo cual es viable usar el hacking ético para detectar vulnerabilidades.

Socio Cultural: Si hay un buen manejo de la información se minimizarán las vulnerabilidades y se ayudará a tratar la información de los ciudadanos en forma ética y confidencial.

Tecnológica: El uso de hacking ético mejorara las condiciones de seguridad del servidor de base de datos de catastro del Gobierno Autónomo Descentralizado San Miguel.

Ambiental: En la realización del presente proyecto no se afectará al medio ambiente.

Económico-financiera: El proyecto en el ámbito económico es factible de realizarlo ya que todas las herramientas de software que se utilizaran son libres por lo cual no se pagaran los costos de licencia.

Legal: El proyecto de investigación es viable porque está cumpliendo todas las leyes normas y metodologías de hacking ético.

Análisis de las vulnerabilidades a través del hacking ético

El Gobierno Autónomo Descentralizado San Miguel somete su servidor de base de datos de catastro a la evaluación mediante una prueba de intrusión bajo las siguientes consideraciones:

- Dotación del nombre de la red Wi-Fi y su respectiva contraseña.
- No indisponer los recursos de red o información durante el proceso de la prueba.
- No modificar o eliminar archivos o directorios.
- No cambiar la configuración en ninguno de los equipos.
- Mantenerse ajeno a los empleados y clientes.
- Sobretodo mantener una estricta confidencialidad de la información que se administre en la Intranet, sin embargo se autoriza para los fines de esta investigación técnica mostrar el proceso y los resultados de la detección de vulnerabilidades.

Par empezar con la ejecución del proceso de hacking ético se conecta a la red Wi-Fi, y esta asigna la dirección IP 192.168.10.105

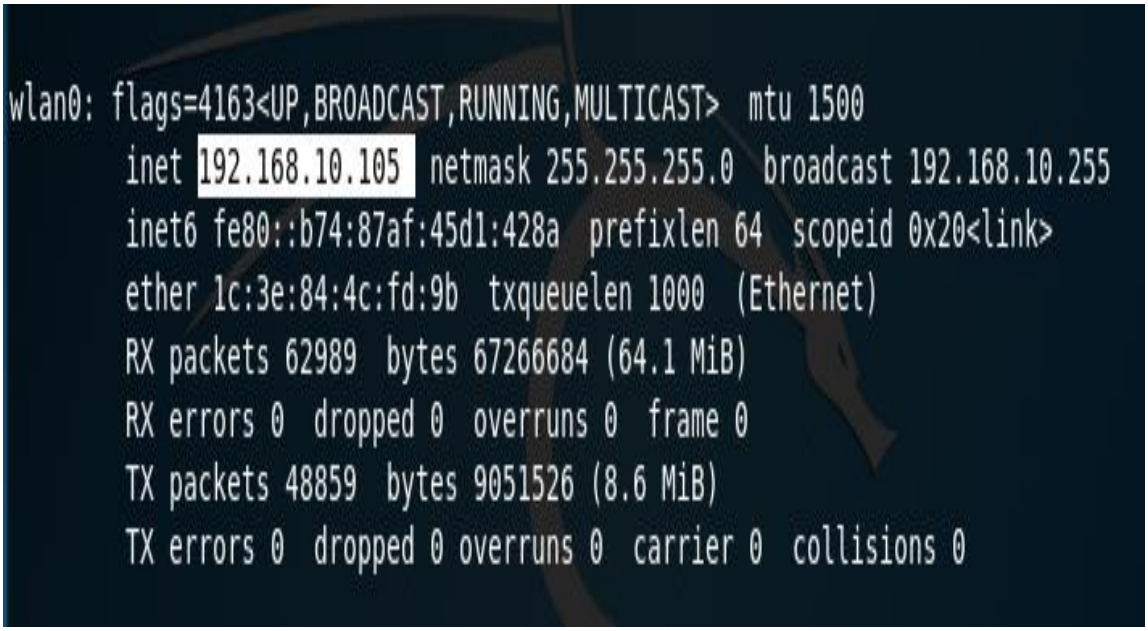


Ilustración 2: Dirección IP del atacante

El proceso de búsqueda de vulnerabilidades se realizó a través de las fases del hacking ético.

Fase 1: Reconocimiento

Para proceder a la realización del hacking ético en la institución se procedió al reconocimiento de la situación actual en el ámbito de seguridad informática en el servidor de base de datos de catastro.

Objetivo

- Encontrar las direcciones IP del servidor de catastro dentro de la unidad.
- Utilizar el comando ping para probar la conectividad con el servidor de base de datos.

Ejecución de la herramienta Nmap

A través de la ejecución de la herramienta Nmap con del comando nmap –sP 192.168.101.1-255 se logró determinar cuáles son los host activos en esta intranet, de esta forma se encuentra el host objetivo.

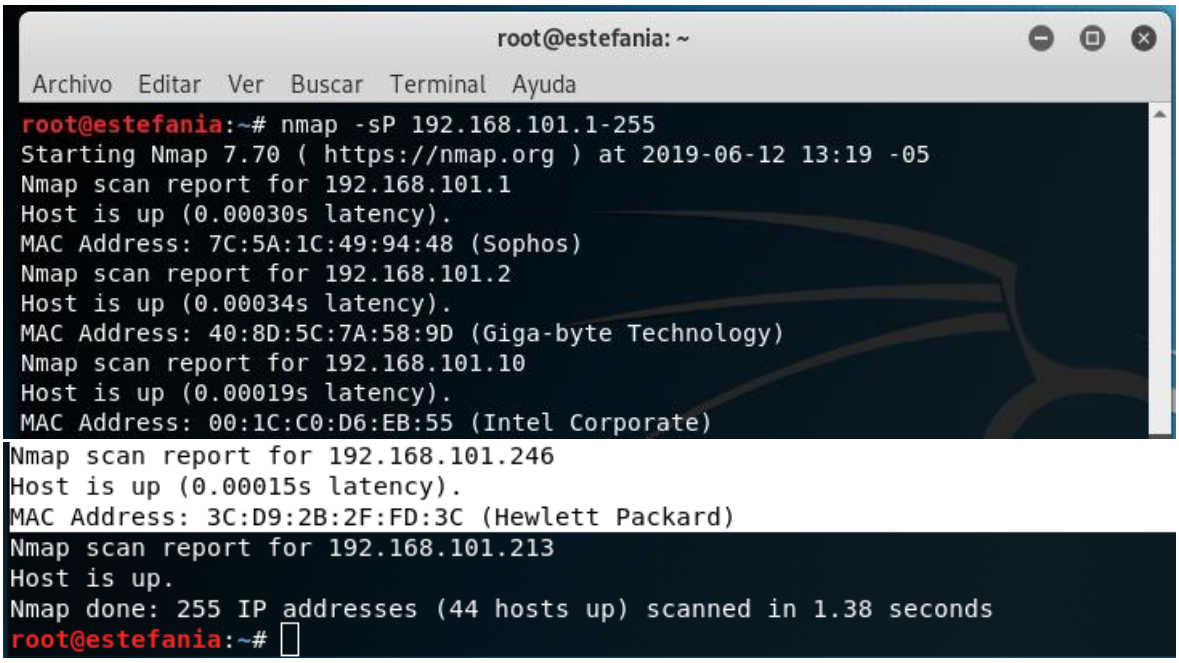


Ilustración 3: Ejecución de la herramienta Nmap

Ejecución del comando ping al host objetivo

Se realizó un ping al servidor de base de datos de catastro con IP número 192.168.101.246 para probar que la conectividad, esta salida indica el tiempo de respuesta de conexión.

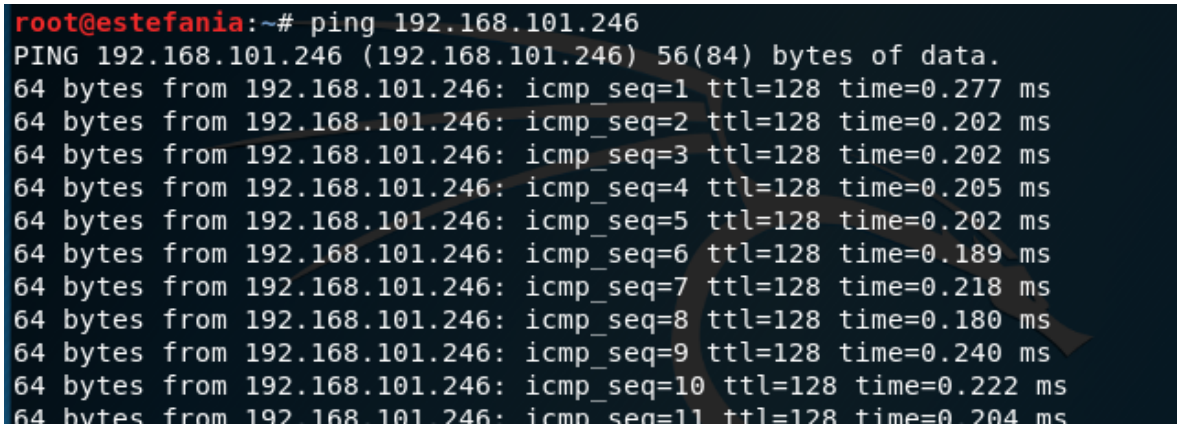


Ilustración 4: Ejecución del comando ping al host objetivo

Resultados

- Host activos en red encontrados con éxito.
- Prueba de conectividad exitosa entre la máquina del atacante y el servidor de base de datos de catastro.

Fase 2: Escaneo

La fase de escaneo es el siguiente paso que se debe llevar a cabo después de conocer el host objetivo, tomando en cuenta que el escaneo es la denominación de las características de una red o sistemas remotos para identificar los servicios que ofrece, las versiones con las que cuenta, SO, entre otros, se procede al escaneo de red en forma activa para lo cual se empleó herramientas Nmap y Nessus.

Objetivo

- Realizar escaneo de puertos para detectar puertos abiertos en el servidor de base de datos de catastro

- Ejecutar escaneo de puertos para determinar cuáles son los servicios que corriendo en el servidor de base de datos de catastro.
- Efectuar escaneo de vulnerabilidades para determinar el grado de vulnerabilidad del servidor de base de datos de catastro.

Escaneo de los puertos del servidor de base de datos de catastro

El escaneo de los puertos se lo realizó con una herramienta nmap, se procede a verificar el estado de los puertos con sus respectivos servicios en los servidores de mayor importancia para detectar posibles vulnerabilidades según la información recabada anteriormente.

Ilustración 5: Escaneo de los puertos del servidor de catastro

Se selecciona Nmap, indica todos los posibles comandos que se pueden utilizar con esta herramienta.

```
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Ilustración 4: Comandos de Nmap

Con el comando nmap –sV –O 192.168.101.246 se trata de buscar los puertos abiertos para determinar cuáles son los servicios y las versiones que están ejecutando, y que Sistema Operativo está instalado.

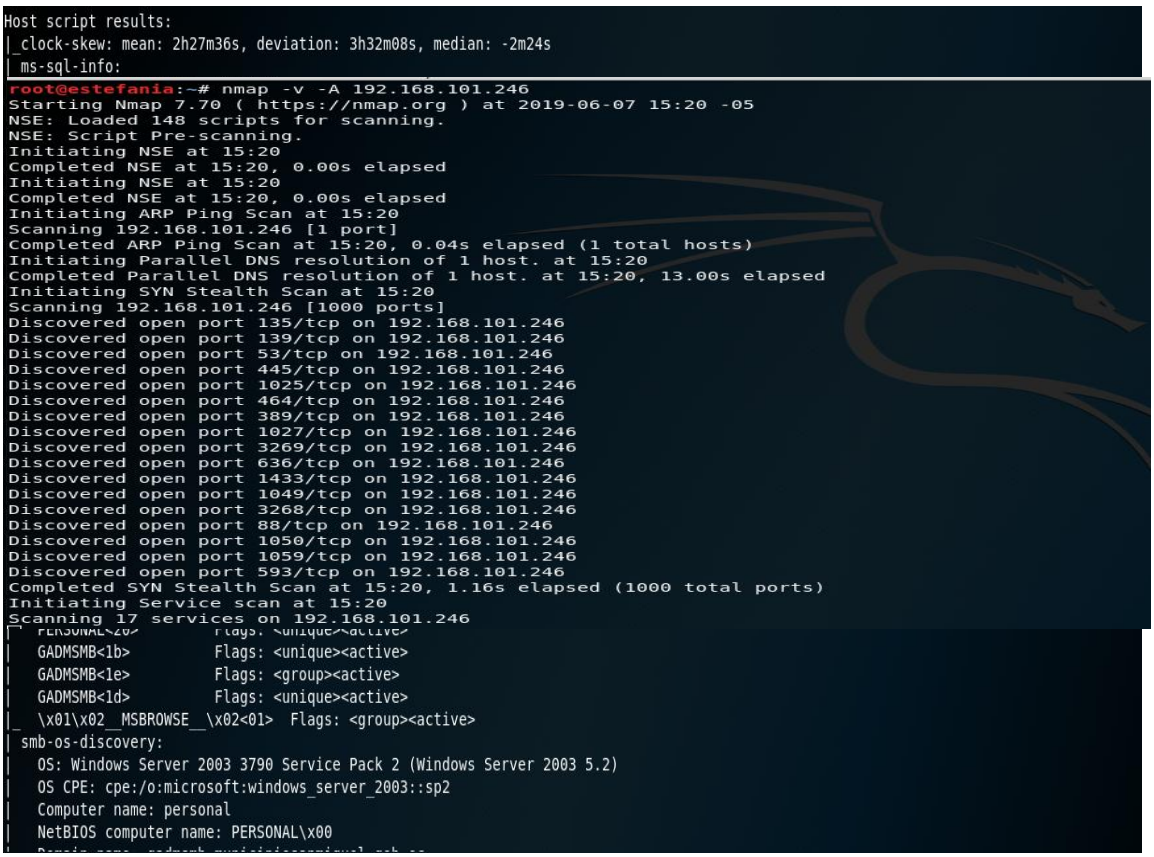
```
root@estefania:~# nmap -sV -O 192.168.101.246
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-07 15:15 -05
Nmap scan report for 192.168.101.246
Host is up (0.00017s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-06-07 20:13:00Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1025/tcp open  msrpc        Microsoft Windows RPC
1027/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
1049/tcp open  msrpc        Microsoft Windows RPC
1050/tcp open  msrpc        Microsoft Windows RPC
1059/tcp open  msrpc        Microsoft Windows RPC
1433/tcp open  ms-sql-s     Microsoft SQL Server 2000 8.00.2039; SP4
3268/tcp open  ldap
3269/tcp open  tcpwrapped
MAC Address: 3C:D9:2B:2F:FD:3C (Hewlett Packard)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 154.45 seconds
root@estefania:~#
```

Ilustración 6 : Puertos abiertos

Con nmap –v –A 192.168.101.246 muestra más información en detalle durante la exploración, junto con el sistema operativo, las versiones de servicio, y la salida de traceroute.

De la ejecución de los comandos de nmap se encuentran 17 puertos abiertos, los servicios que



se están ejecutando y la versión de estos.

Ilustración 7: Información en detalle del servidor

En base a la ejecución del comando anteriormente expuesto se determina que el servidor de base de datos de catastro tiene SO Windows XP 2003 SP2.

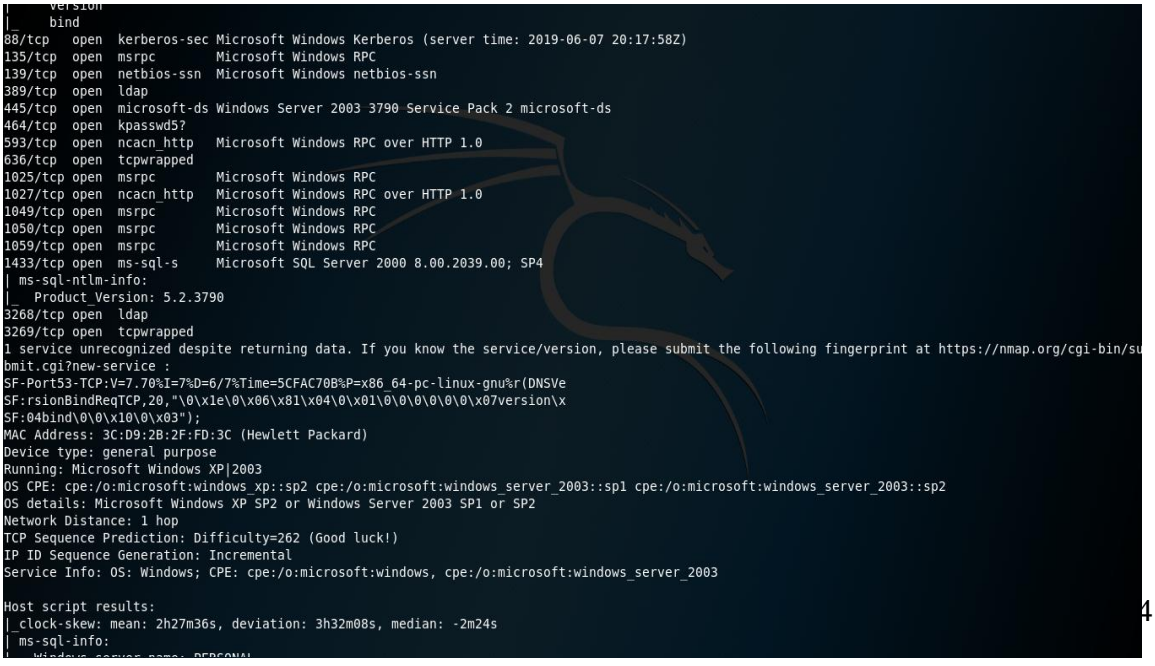


Ilustración 8: Identificación de SO Windows XP 2003 SP2

Se encuentra el nombre del dominio del Gobierno Autónomo Descentralizado San Miguel

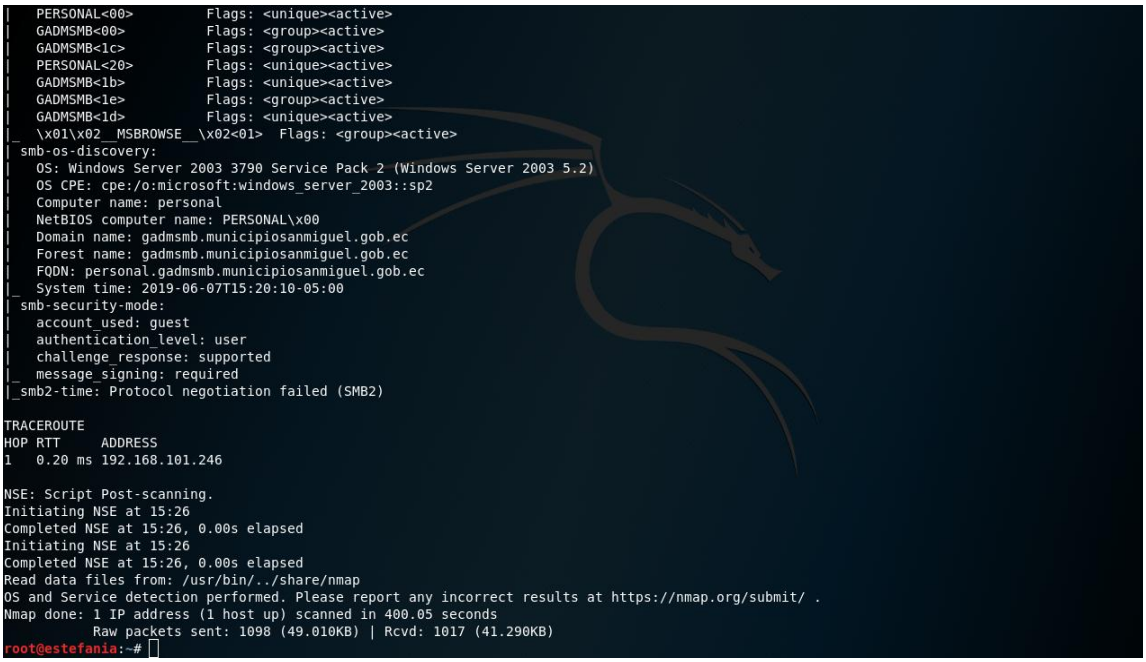


Ilustración 9: Nombre del dominio del GAD San Miguel

Escaneo de vulnerabilidades

Inicio de Nessus

Par empezar a utilizar Nessus, lo primero que se debe hacer es inicializar el servicio**.**

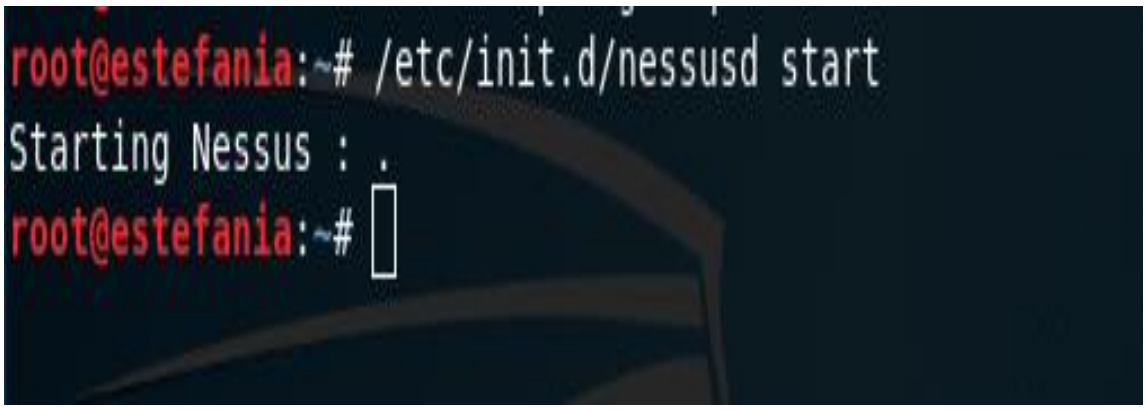


Ilustración 10: Inicializar el servicio de Nessus

Ingresar el usuario y la contraseña para ingresar al servicio de Nessus, luego clic en “Sign In”

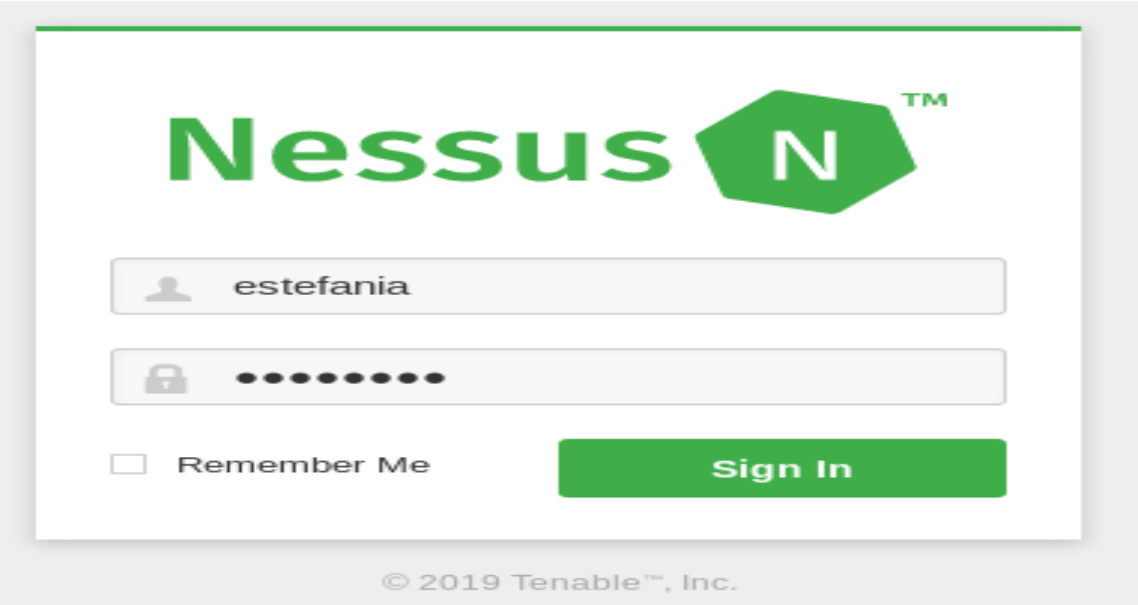


Ilustración 11: Inicio de sección Nessus

Una vez dentro de la herramienta Nessus proceder para realizar un nuevo escaneo se da clic en “New Scan”

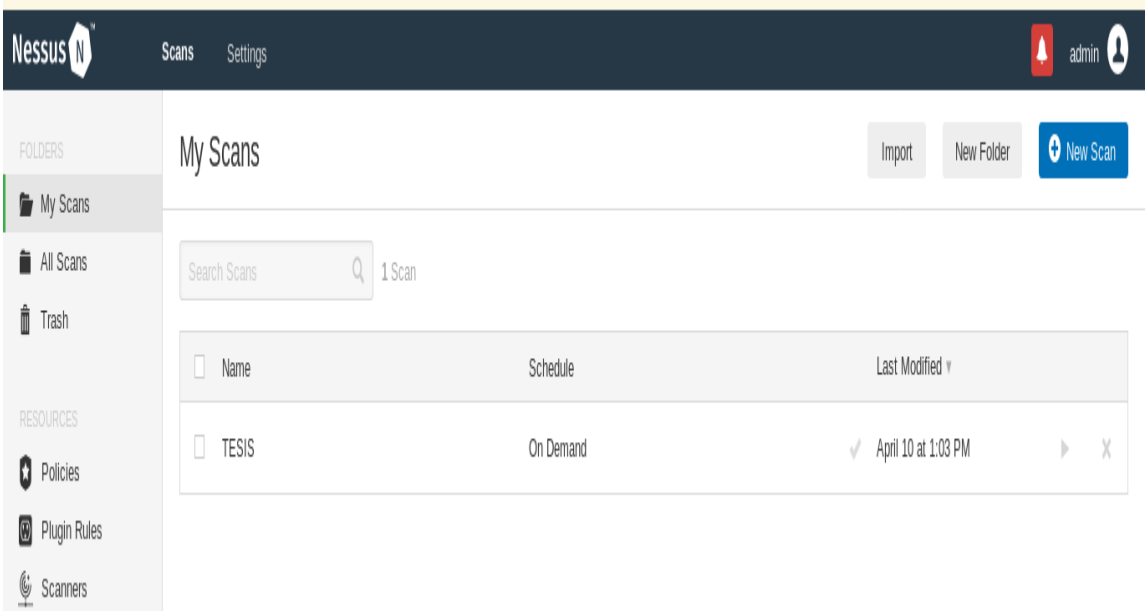


Ilustración 12: Página nuevo escaneo en Nessus

Seguidamente muestra todos los tipos de escaneos con los que cuenta Nessus, se escoge el módulo de Escaneo Avanzado “Advanced Scan”.

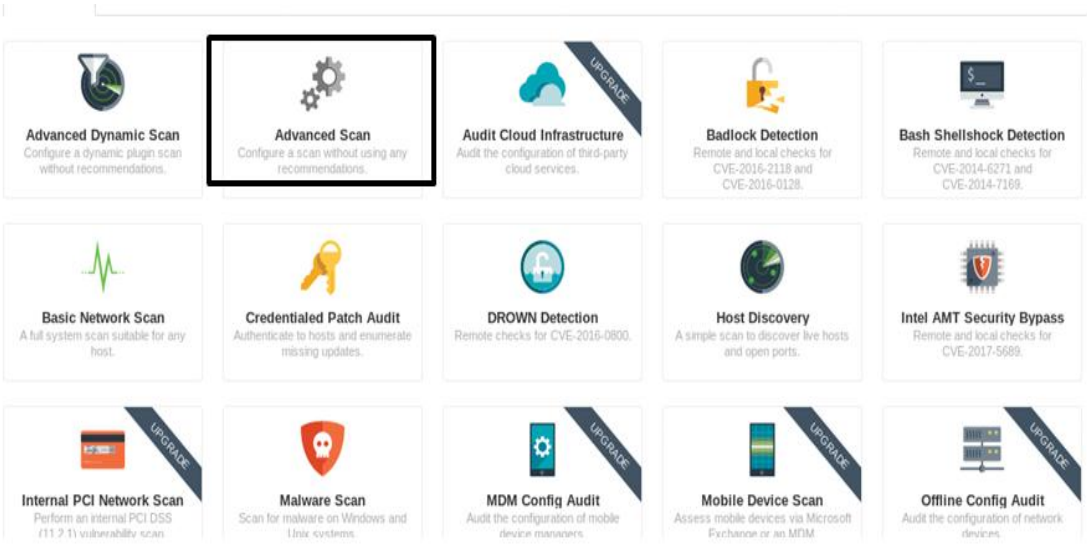


Ilustración 13: Módulos de Escaneo en Nessus

Se procede a crear una actividad de escaneo de vulnerabilidades, se abre una ventana con tres viñetas, la primera es la de ajustes en la cual se llena los campos de: nombre, descripción, carpeta de destino, la dirección IP objetivo, si se desea hay la opción de subir una carpeta de direcciones IP objetivo.

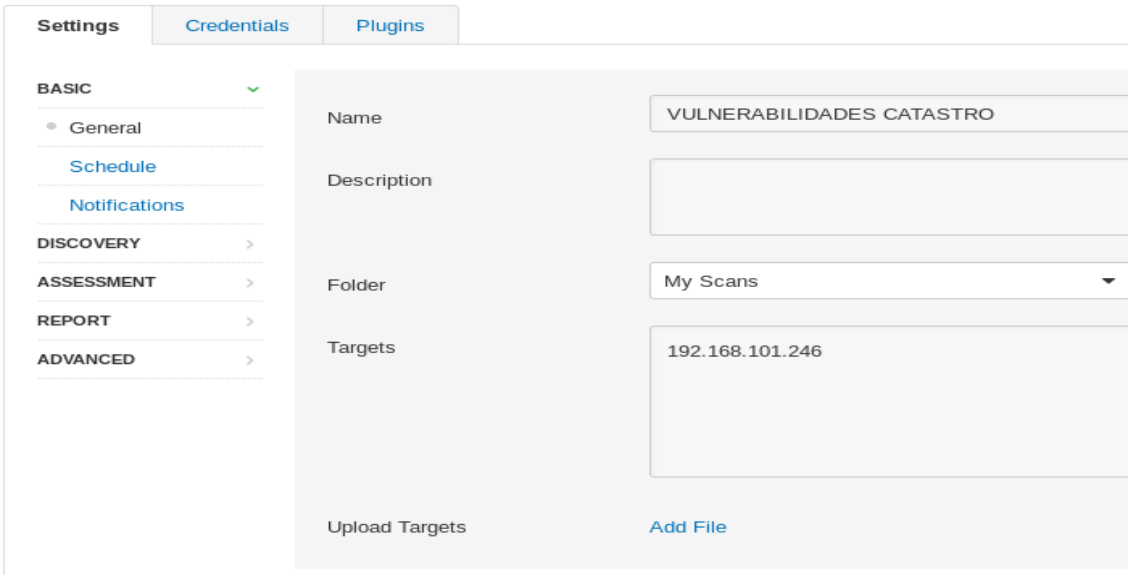


Ilustración 14: Ventana para crear nueva actividad de escaneo de vulnerabilidades

En la viñeta corresponde a las credenciales, en este caso se escoge la opción Host.

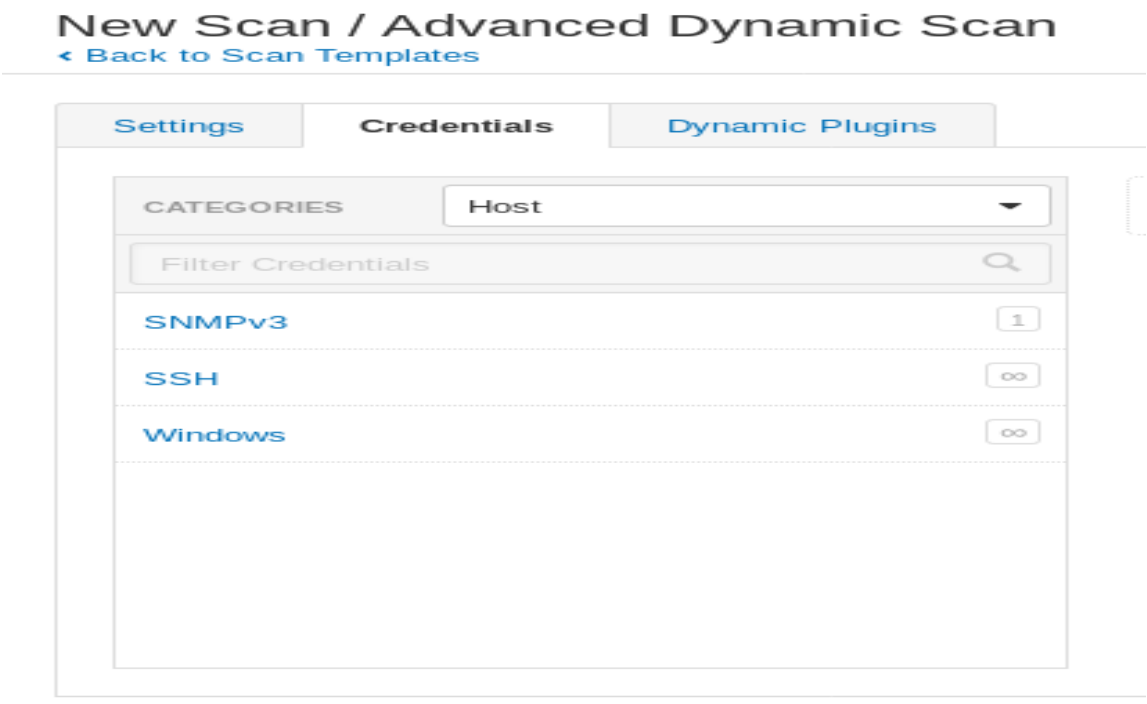


Ilustración 15: Ventana de credenciales

La siguiente ventana corresponde a los plugins dinámicos en caso de necesitarlos. Finalmente se da clic en Guardar “Save”.

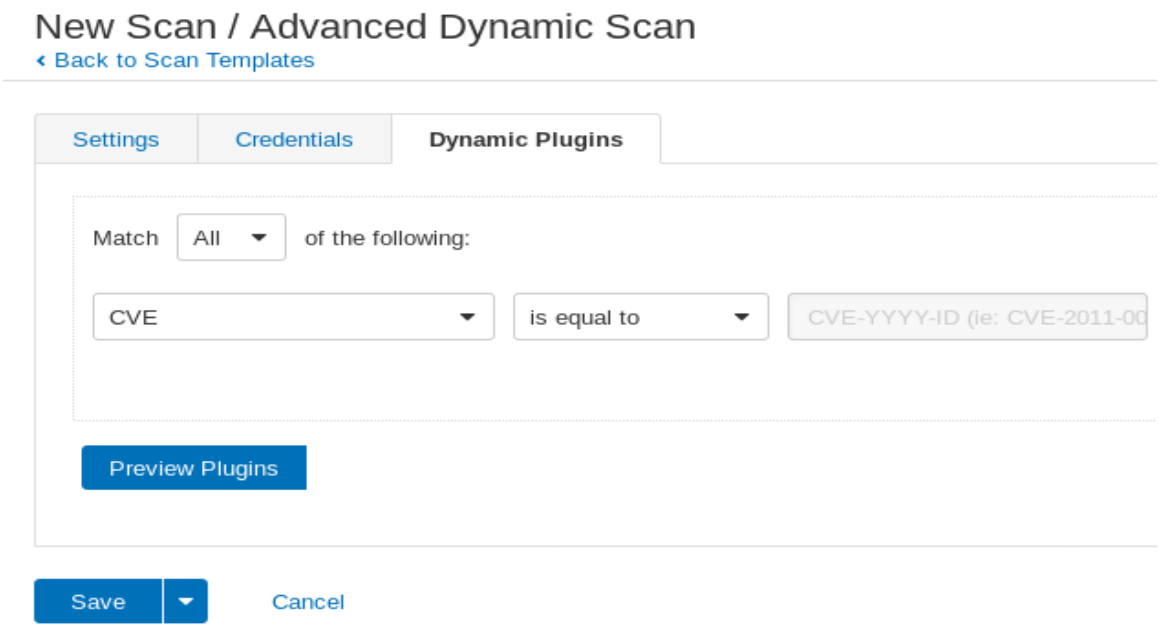


Ilustración 16: Plugins dinámicos

En la opción My Scans que corresponde al historial de los escaneos se puede observar el scans que se está realizando.

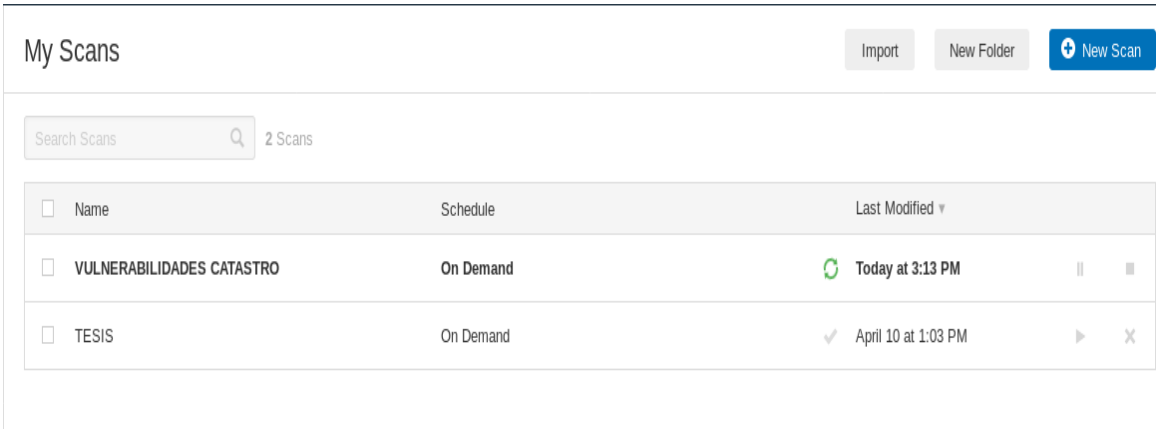
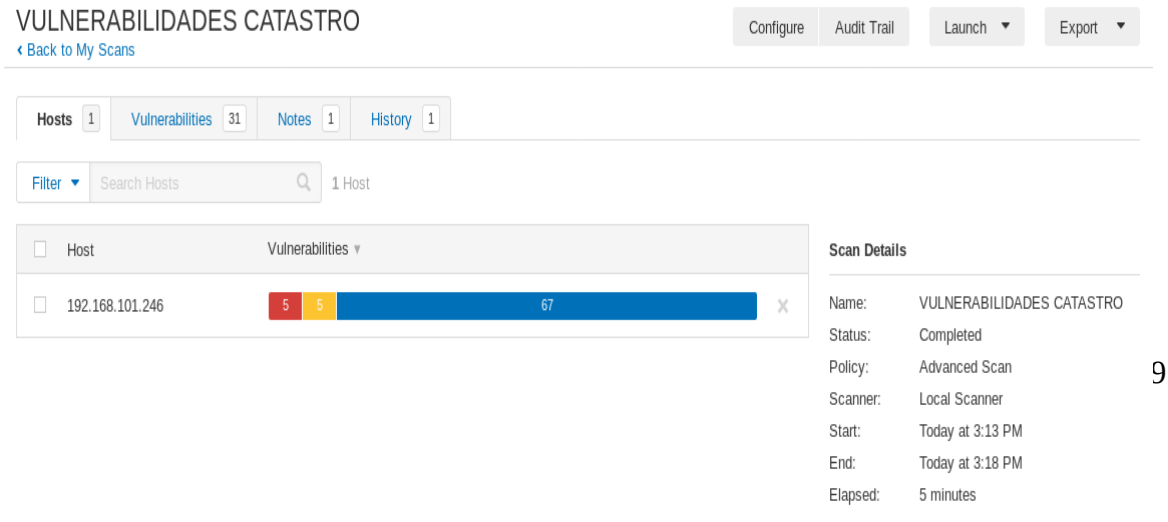


Ilustración 17: Historial de los escaneos

Luego de haber esperado a que se concluya el análisis seguidamente proporciona todas las



vulnerabilidades existentes en la base de datos del servidor de catastró indicando el grado de severidad de las mismas también se ha encontrado que este servidor posee un 20% de vulnerabilidades el 10% es de vulnerabilidad critica, un 10% de vulnerabilidad media e información.

Ilustración 18: Resultados del escaneo

Pastel que determina el grado de vulnerabilidad que tiene el servidor de base de datos

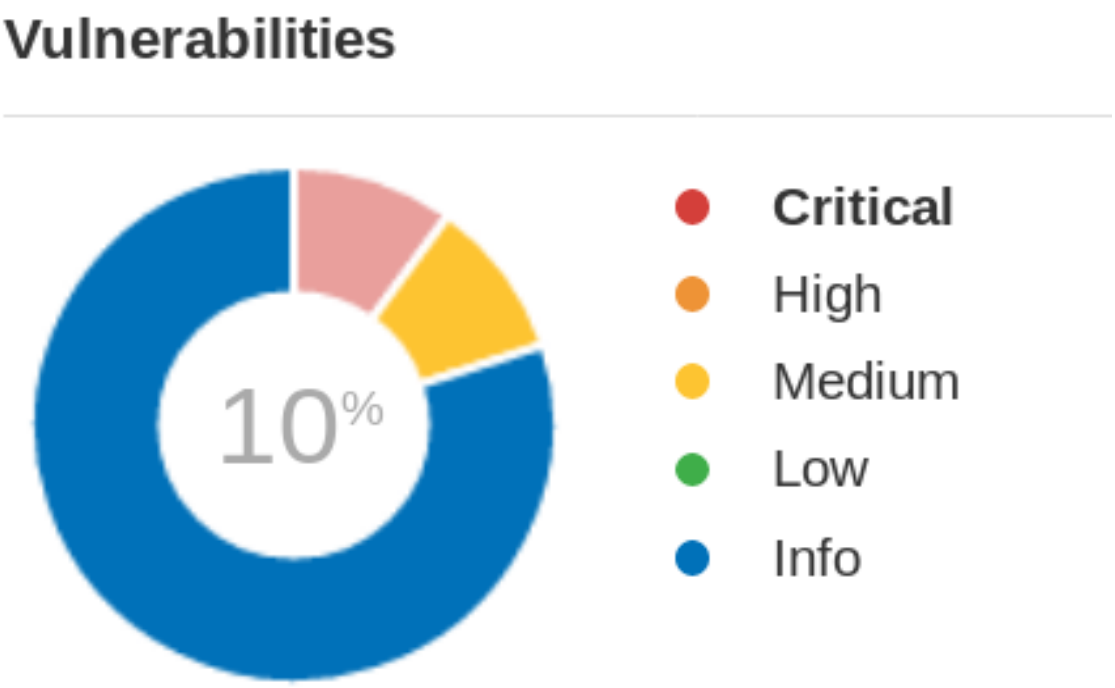


Ilustración 19: Grado de vulnerabilidad en el servidor de base de datos

Resultados

- Se encuntra informacion de puertos abiertos, de SO, servicios que se estan ejecutando, Service Pack que esta instalada.

Direccion IP	Sistema Operativo	Puertos abiertos	Servicio	Version
192.168.101.246	Windows XP SP2	53/tcp	domain	Sistema de nombre de dominio
		88/tcp	Kerbero-sec	Microsoft Windows Kerberos
		135/tcp	msrcp	Microsoft Windows RPC
		139/tcp	netbios-ssn	Microsoft Windows netbios-ssn
		389/tcp	ldap	
		445/tcp	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
		464/tcp	kpasswds	
		593/tcp	ncacn_http	Microsoft Windows RCP over HTTP 1.0
		636/tcp	tcpwrapped	
		1025/tcp	msrpc	Microsoft Windows RPC
		1027/tcp	ncacn_http	Microsoft Windows RPC over GTTP 1.0
		1049/tcp	msrpc	Microsoft Windows RPC
		1050/tcp	msrpc	Microsoft Windows RPC

		1059/tcp	msrpc	Microsoft Windows RPC
		1433/tcp	ms-sql-s	Microsoft SQL Server 200 8.00.2039; SP4
		3268	ldap	
		3269	tcpwrapped	

Tabla 6: Puertos y servicios que se han encontrado abiertos durante la etapa del escaneo

- Se encuentran 5 vulnerabilidades criticas y 5 vulnerabilidades medianas al momento de escanear el servidor de base de datos de catstro con la herramienta Nessus. Vulnerabilidades que pueden estar expuestas a taques reales.

192.168.101.246

5	0	5	0	39
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 49

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	84729	Microsoft Windows Server 2003 Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	56210	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials
MEDIUM	5.0	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	56211	SMB Use Host SID to Enumerate Local Users Without Credentials

Ilustración 20: Listado de vulnerabilidades

Fase 3: Obtención de Acceso

Una vez que ha realizado el escaneo de los puertos, identificación de puertos abiertos y el escaneo de vulnerabilidades se procede a explotar las vulnerabilidades y tratar de ganar acceso desautorizado a los recursos informáticos vulnerables.

Objetivos

- Atacar al servicio de Microsoft Windows SMB utilizando Metasploit para tratar de abrir sesión en el servidor de base de datos, ya que como se pudo averiguar en fases anteriores, el servidor posee un sistema operativo Windows XP 2003 server, por lo tanto es viable realizar este tipo de ataque.
- Atacar a msrpc utilizando el mismo Framework Metasploit ya que en su base de datos este dispone de una variedad de exploit para este servicio.

Ataque al servicio de Microsoft Windows SMB

Este ataque se lo aplico al puerto 445 correspondiente al servicio de Microsoft Windows SMB, para esto se empleó el framework metasploit que se instaló en Kali Linux, el cual es una herramienta GNU escrita en Perl y con utilización de diversos lenguajes de programación como C, Pyton, ASM, etc. Metasploit se ejecuta bajo una consola CYGWIN y trabaja con una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades, se indica que sistema atacar, tipo de ataque a utilizar e información necesaria para atacar al host.

Para ejecutarlo en modo consola, se inicia el servicio de postgresql y luego escribir msfconsole.

Ilustración 21: Ataque al servicio de Microsoft Windows SMB

Consecutivamente muestra la pantalla de Metasploit

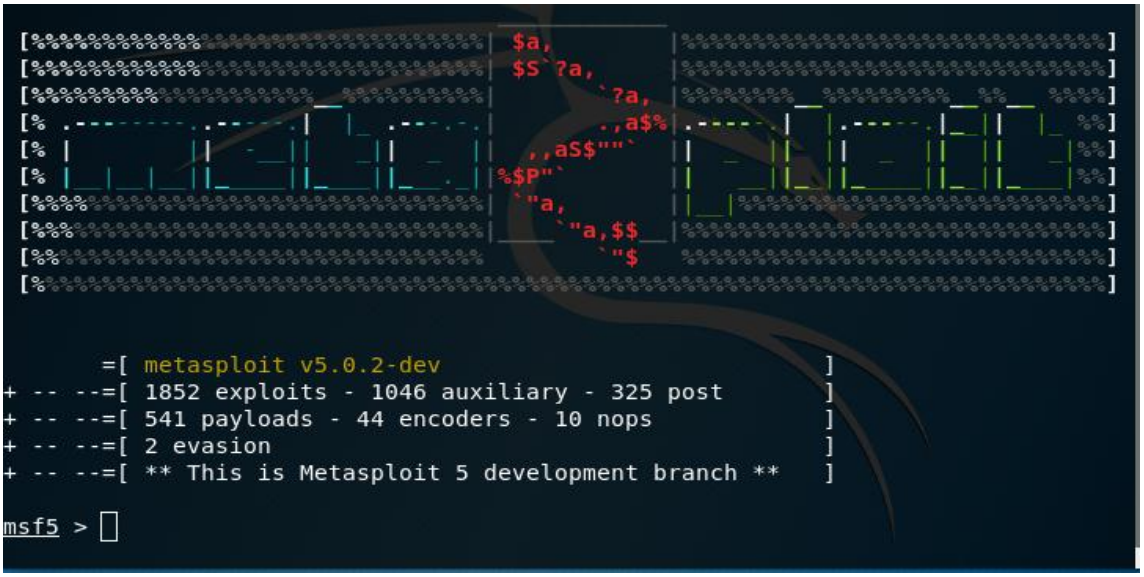


Ilustración 22: Pantalla de metasploit

Ya dentro de la consola de metasploit se escribe el comando show exploits el mismo que genera una gran lista de exploits disponibles, de los cuales se selecciona alguno y dependiendo del sistema a atacar en este caso se escoge el exploit ms08_067_netapi ya que este es el más estable actualmente, se intenta provocar un buffer overflow en el sistema y conseguir inyectar código malicioso a través de un payload.

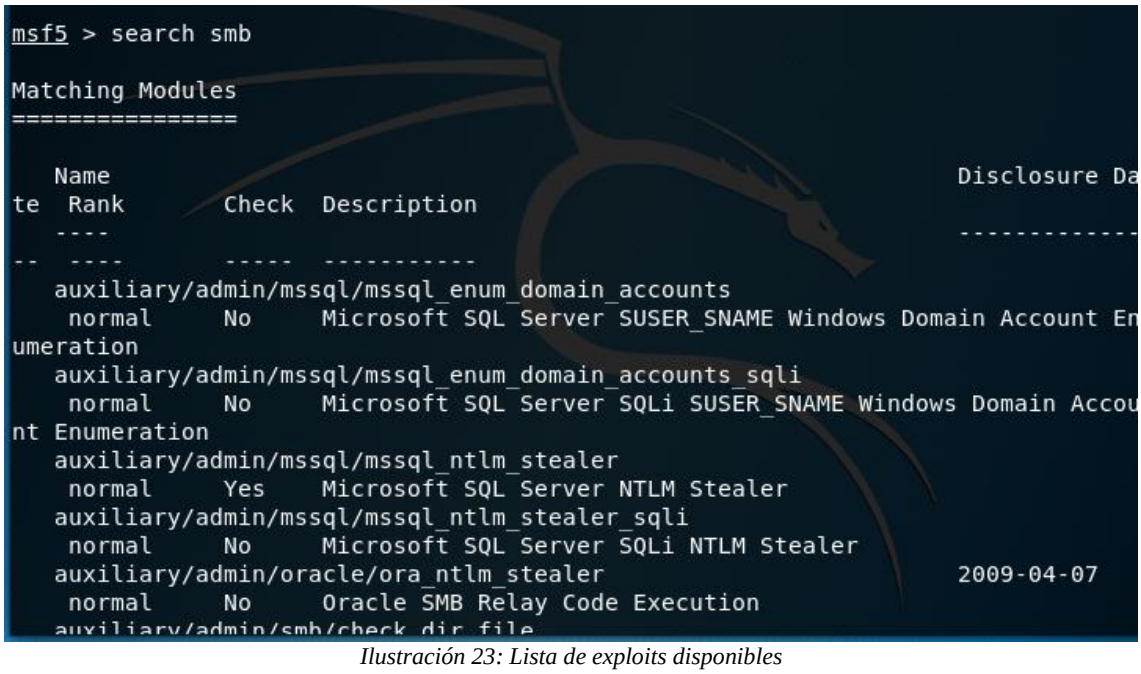


Ilustración 23: Lista de exploits disponibles

En la lista que se despliega de los exploits, se encuentra el exploit ms08_067_netapi

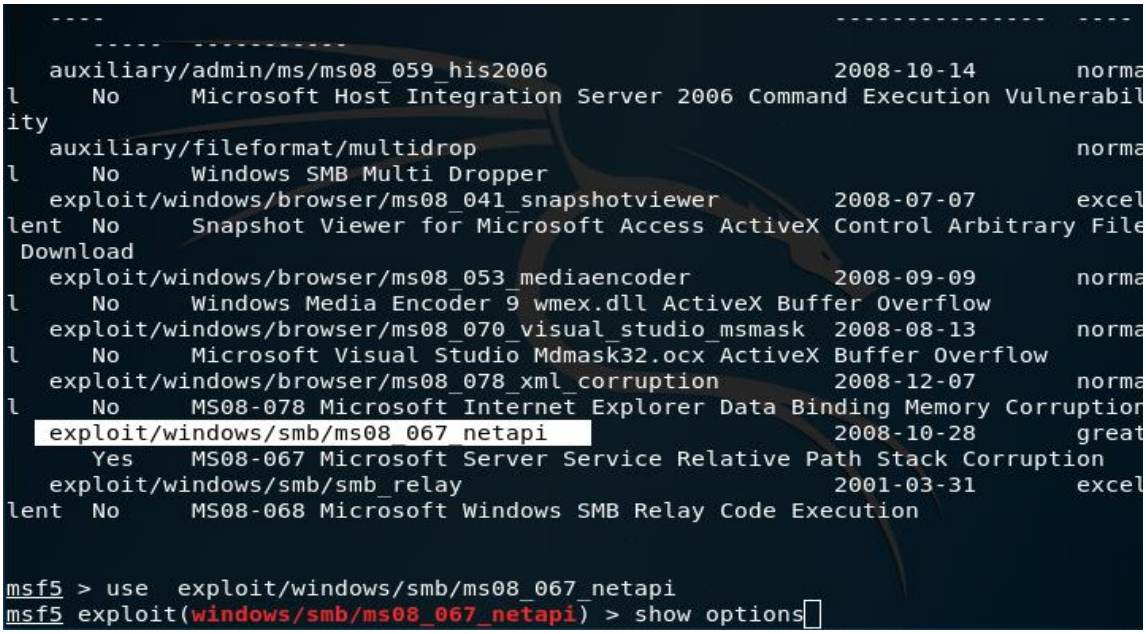


Ilustración 24: Selección de exploit ms08_067_netapi

Una vez encontrado exploit, se ingresa mediante la línea use exploit/windows/ms08_067_netapi.

Ilustración 25: Utilización del exploit escogido

Se ingresa los datos requeridos, en este caso RHOST, LHOST y RPORT

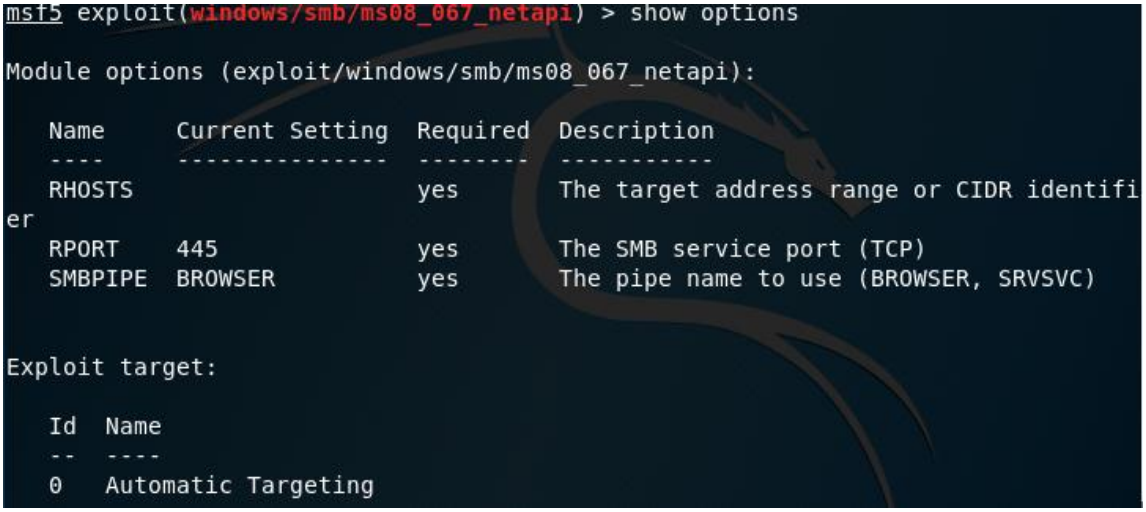


Ilustración 26: Ingreso de RHOST, LHOST y RPORT

Para asignar los datos requeridos en el procedimiento anterior, se escribe la línea set RHOST IP de la maquina víctima y set RHOST IP de la máquina del atacante, en este caso RPORT está asignado 445 y es el puerto a atacar.

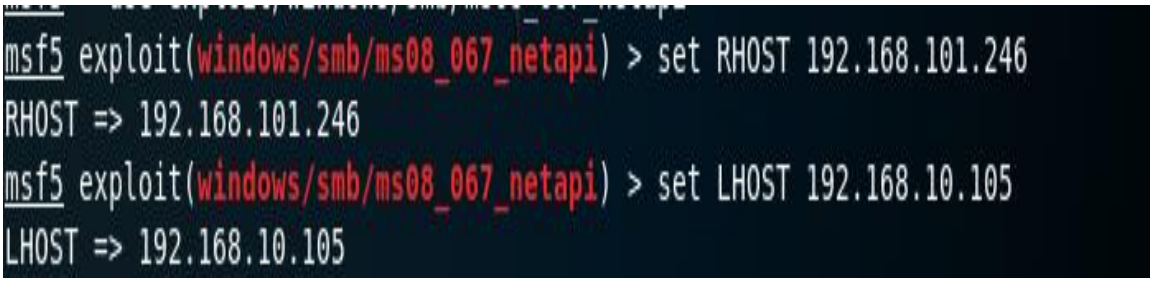


Ilustración 27: Ingreso de RHOST Y LHOST

Luego de esta configuración seleccionar payload Windows/meterpreter/bind_tcp para tratar de establecer una conexión remota.

Ilustración 28: Selección de payload Windows/meterpreter/bind_tcp

Nuevamente escribir show options para verificar que las configuraciones se hayan grabado con éxito.

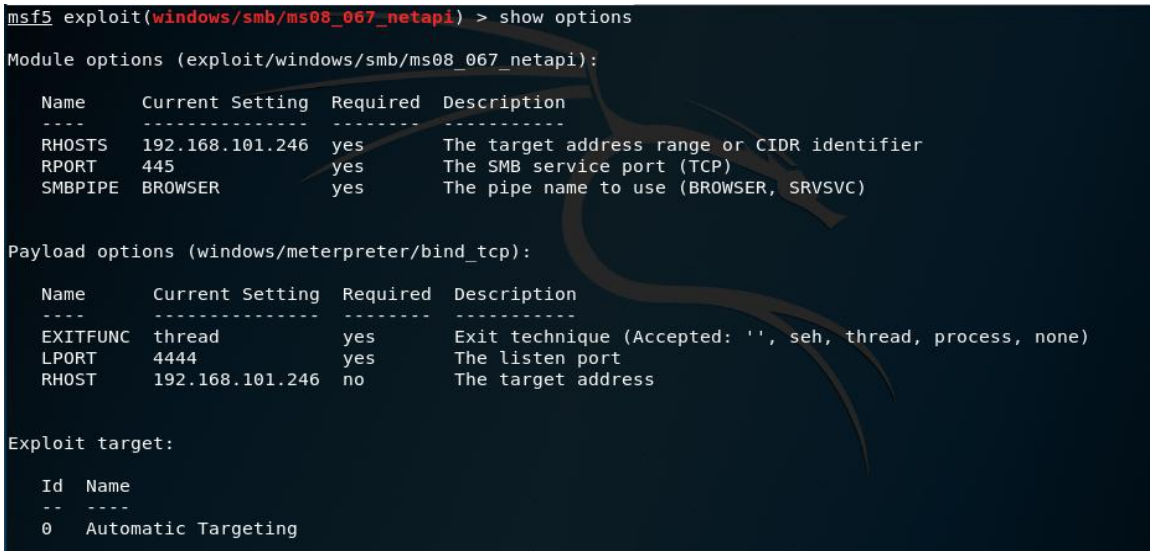


Ilustración 29: Configuraciones guardadas con éxito

Seguidamente se procede a ejecutar el exploit.

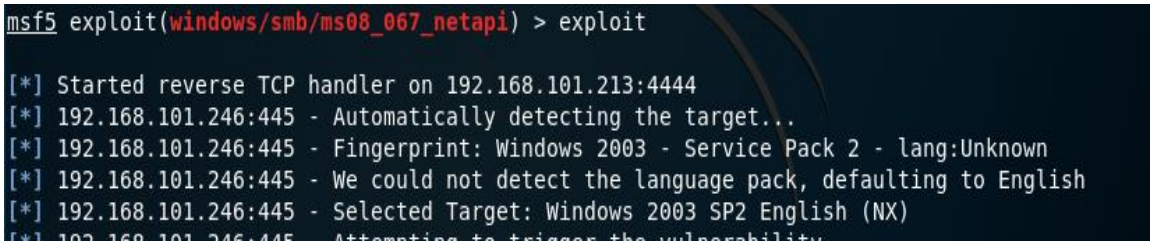


Ilustración 30: Ejecución del exploit

Si los resultados que se obtienen son favorables ya se tendrá acceso al host específico, usualmente cuando el puerto 445 está abierto se puerto realizar este tipo de ataque.

Ataque al servicio de Microsoft Windows RPC

Este ataque se lo aplico al puerto 135 correspondiente al servicio de Microsoft Windows RPC, para ello igual que en el apartado anterior se empleó el framework metasploit que se instaló en Kali Linux.

Para ejecutarlo en modo consola, se tiene como primero paso iniciar el servicio de postgresql y luego escribir msfconsole.

Ilustración 31: Iniciar Metasploit

Ya ejecutado el paso anterior, se procede a ingresar search ms03_026_dcom para buscar un exploit acorde al servicio que se desea explotar.

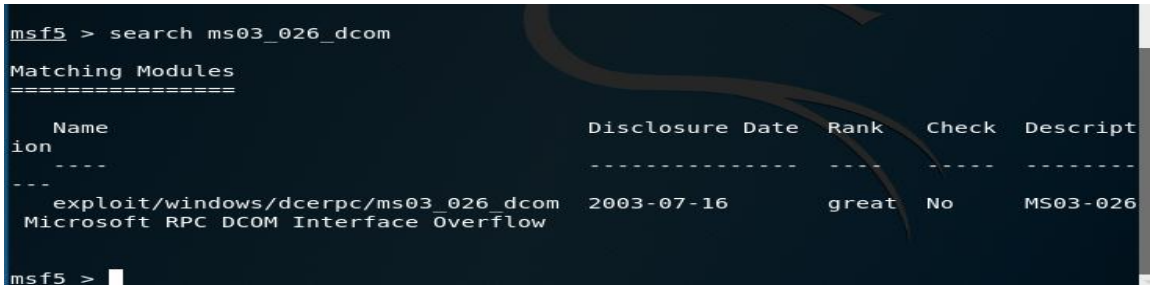


Ilustración 32: Búsqueda del exploit

Ya encontrado el exploit seguida de la palabra use se ingresa la dirección completa del exploit a utilizar: use exploit/windows/dcerpc/ms03_026_dcom

Ilustración 33: Utilización del exploit ms03_026_dcom

Con show options se verifica las configuraciones requeridas en este exploit.

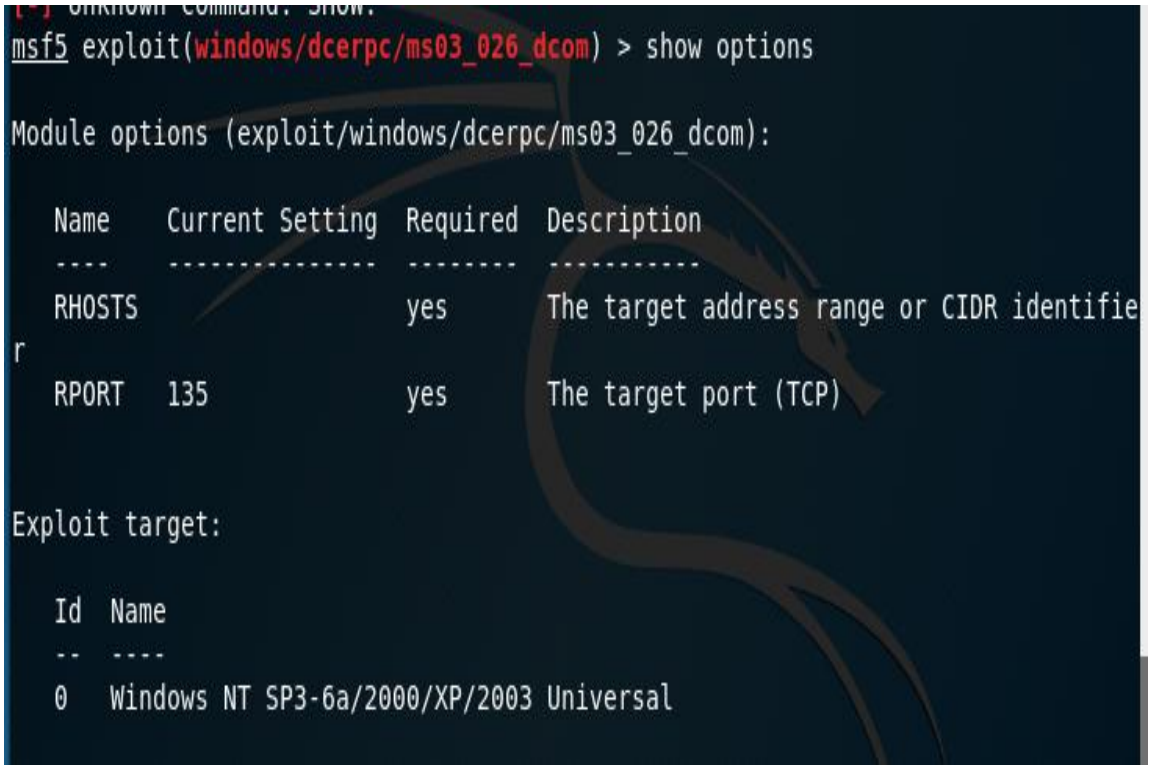


Ilustración 34: Verificación de las configuraciones del exploit

Se necesita configurar RHOST y RPORT

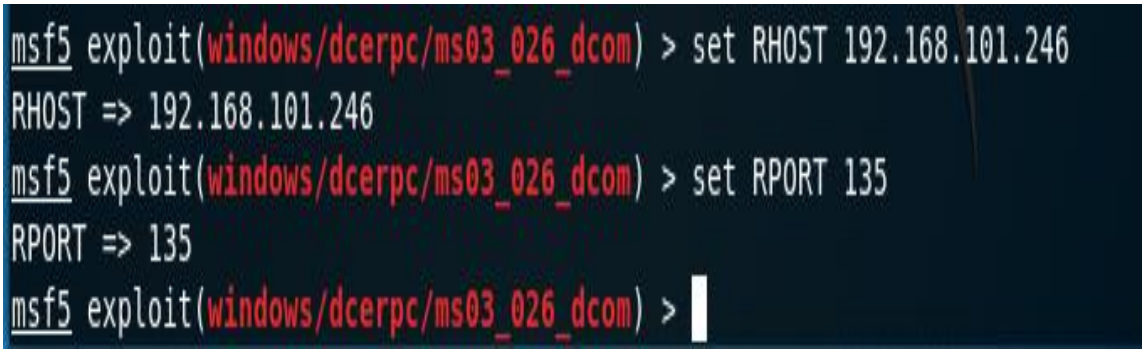


Ilustración 35: Configuración de RHOST y RPORT

Luego de haber ingresado las respectivas configuraciones, se digita show options para verificar se hayan grabado los cambios.

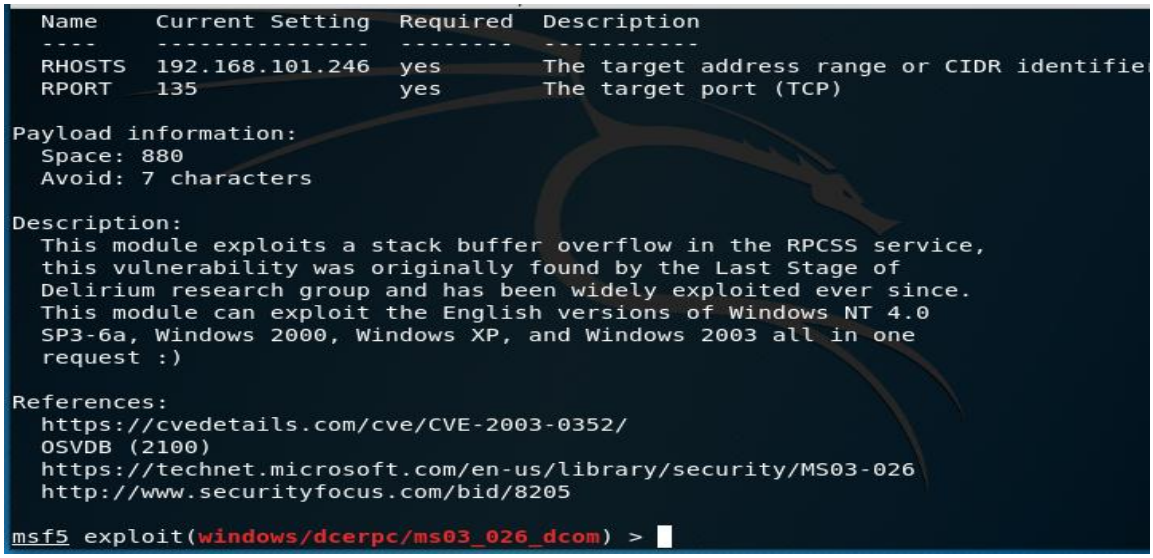


Ilustración 36: Verificación de cambios realizados

Ya con las con las configuraciones necesarias se procede a explotarlo con el comando exploit.

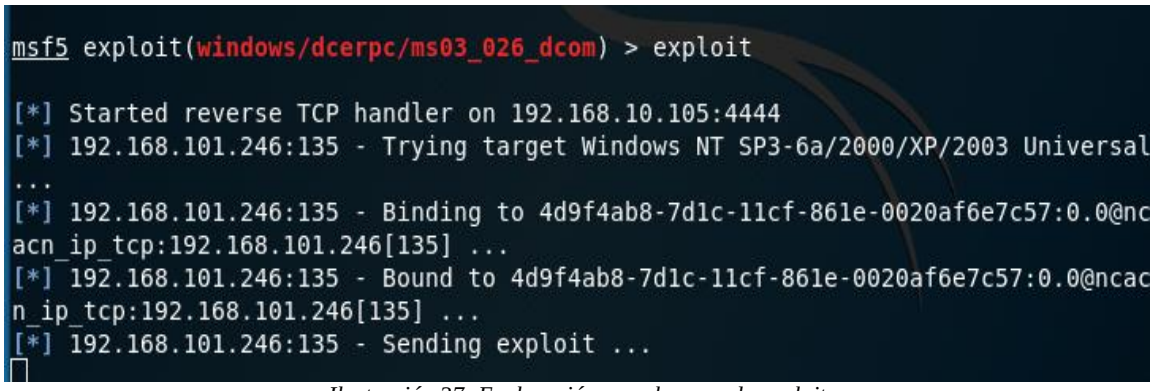


Ilustración 37: Exploración con el comando exploit

Resultados

- Luego de haber detectado las vulnerabilidades, se ha procedido a explotarlas con resultados favorables, y se han tomado medidas correctivas para las mismas.

Fase 4: Mantener Acceso

En la actual ejecución de hacking ético no es necesaria mantener el acceso, puesto que todas las pruebas, accesos y ataques, fueron realizados con la finalidad de contribuir a la seguridad del servidor de base de datos de catastro en un ambiente controlado, bajo la autorización y supervisión del jefe inmediato de la unidad de sistemas del Gobierno Autónomo Descentralizado San Miguel.

Fase 5: Cubrir Huellas

Es preciso indicar que en la ejecución de hacking ético no es necesaria la realización de la fase de borrador de huellas, puesto que todas las pruebas, accesos y ataques, fueron realizados en un ambiente controlado, bajo la autorización y supervisión del jefe inmediato de la unidad de sistemas del Gobierno Autónomo Descentralizado San Miguel.

Conclusiones Y Recomendaciones

Conclusiones

Mediante la aplicación del hacking ético se pudo determinar las siguientes vulnerabilidades críticas:

- A través del escaneo de puertos se ha determinado que el servidor de base de datos de catastros se ha descubierto servicios pirateables que están expuesto a posibles ataques.
- MS08-067: Servicio de Microsoft Windows Server Crafted Solicitud de RPC que maneja la ejecución remota de código (958644) (ECLIPSEDWING) (verificación sin credenciales): El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código en el servicio 'Servidor' debido al manejo inadecuado de las solicitudes RPC. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud RPC especialmente diseñada, para ejecutar código arbitrario con privilegios de "Sistema".
- MS09-001: Ejecución remota de código de vulnerabilidades de Microsoft Windows SMB (958687) (verificación sin credenciales): El host remoto se ve afectado por una vulnerabilidad de corrupción de memoria en SMB que puede permitir que un atacante ejecute código arbitrario o realice una denegación de servicio contra el host remoto.
- MS17-010: Actualización de seguridad para el servidor de Microsoft Windows SMB (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (comprobación sin credenciales): El host remoto de Windows está afectado por las siguientes vulnerabilidades:
    1. Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo incorrecto de ciertas

solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario.

2. Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo incorrecto de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)

- Sistema operativo Windows no compatible (remoto): A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no se admite. Como resultado, es probable que contenga vulnerabilidades de seguridad.
- Sistema operativo Windows no compatible (remoto): A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no se admite. Como resultado, es probable que contenga vulnerabilidades de seguridad.
- El problema se solucionara una vez que se tome la decisión política de implementar lo que esta propuesta recomienda para el Gobierno Autónomo Descentralizado San Miguel.

Recomendaciones

- Se recomienda editar el /etc/inetd.conf y comentar cualquier servicio innecesario.
- Emplear encapsuladores TCP cuando corresponda.
- Instalar software antivirus.
- Ejecutar escaneos regulares programados del antivirus.
- Aplicar filtrados de enrutador.
- Microsoft ha lanzado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.
- Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha lanzado parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8. Para los sistemas operativos de Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios interrumpan el uso de SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 se puede desactivar siguiendo las instrucciones del proveedor que se proporcionan en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API de NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.
- Actualizar a un paquete de servicio o sistema operativo compatible.
- Se debe realizar cambios de contraseñas constantemente para tener mayo seguridad y evitar amenazas.

BIBLIOGRAFÍA

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/

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

Capa8. (01 de 09 de 2015). *Capa 8.* Obtenido de http://capaocho8.com/conoces-los-tipos-de-hacking/

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

Codigo Orgánico Integral Penal. (2017). Ecuador.

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/

Flores, M. (17 de Marzo de 2014). *inmogesco.com*. Obtenido de https://inmogesco.com/blog/terminos-inmobiliarios-catastro/

G, A. (29 de 11 de 2016). *Mundo Datos.* Obtenido de https://mundodatos.tech.blog/2016/11/29/hacking-etico-que-es-que-objetivos-persigue/

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.

Guanoluisa, J., & Maldonado, I. (2015). *ANÁLISIS DE RIESGOS Y DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONSEJO NACIONAL DE IGUALDAD DE DISCAPACIDADES "CONADIS".* Quito.

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.

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

InformaticaModerna. (2019). *Informatica Moderna.* Obtenido de http://www.informaticamoderna.com/ServerDB.htm

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/

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

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.

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

ANEXOS

Anexo A: Manual De Instalacion de Kali Linux

Para proceder a la instalación del sistema operativo una vez descargado de la página oficial https://www.kali.org/, se ejecuta el instalador y muestra la pantalla de inicio de instalación del sistema operativo.

Ilustración 38: Pantalla de inicio de instalación

Seguidamente se despliega una página en la cual se debe ir siguiendo los pasos que requiere para la instalación primeramente indica que seleccione la ubicación.

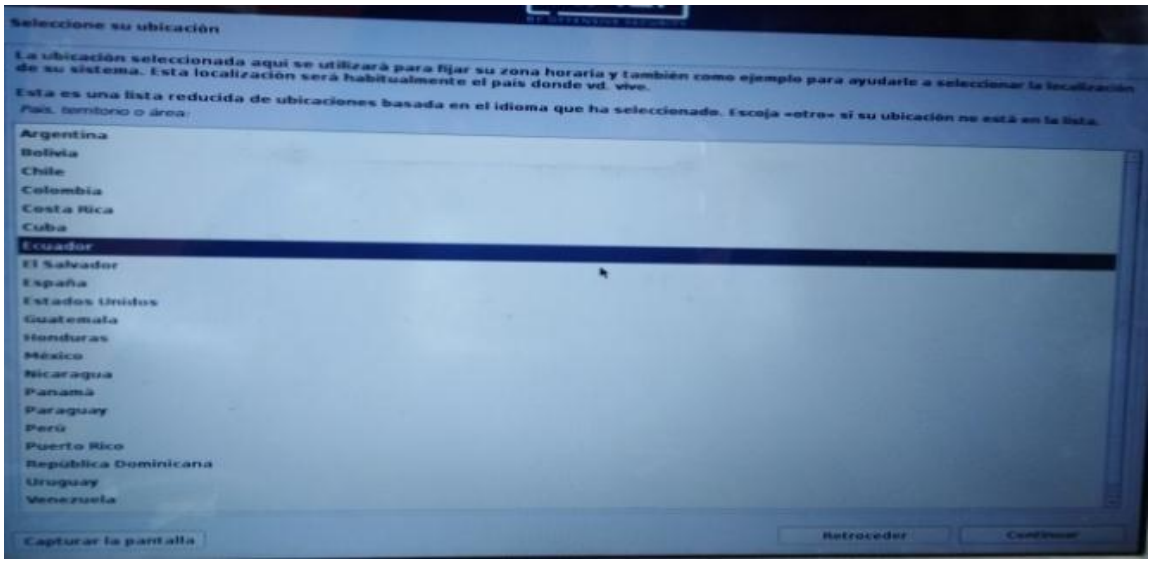


Ilustración 39: Selección de la Ubicación

A continuación se elige la configuración del teclado.

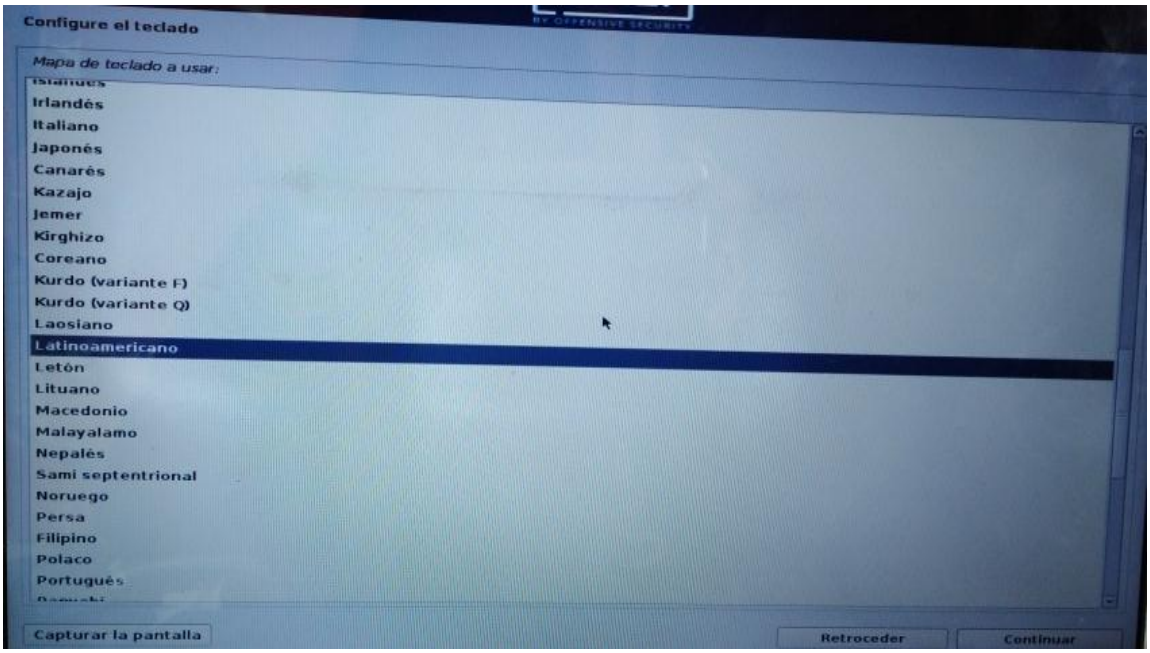


Ilustración 40: Configuración del teclado

Al continuar el proceso de instalación se van instalando los componentes necesarios para el funcionamiento de Kali Linux

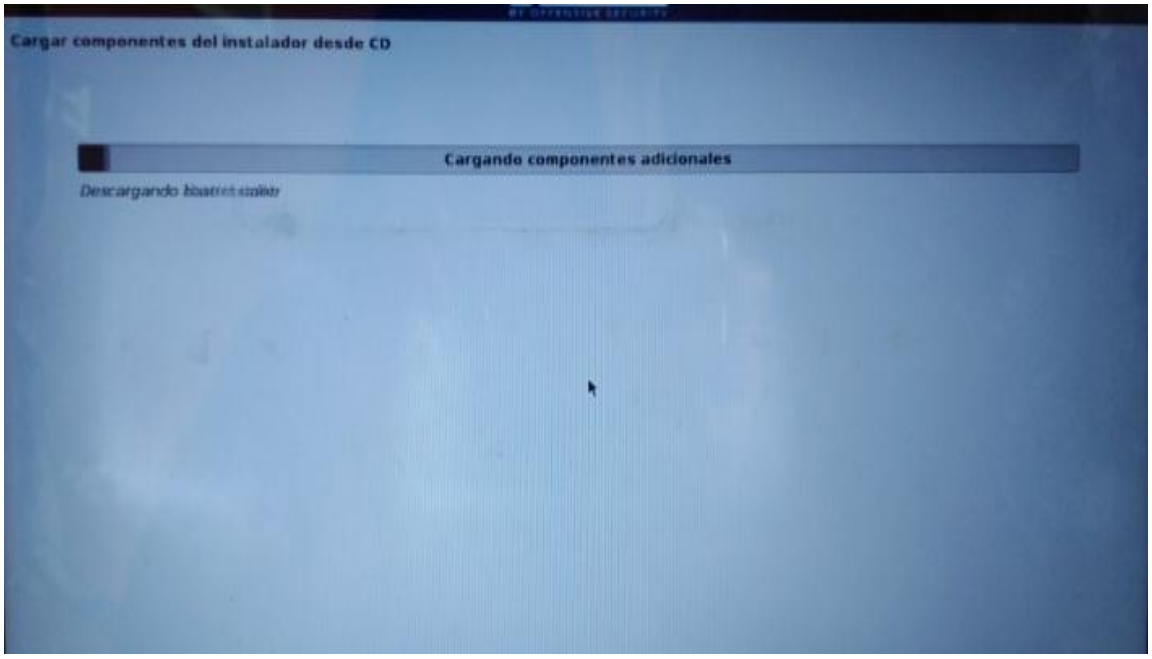


Ilustración 41: Instalación de componentes requeridos

Seguidamente obtendrá la pantalla para ingresar el nombre de la red.

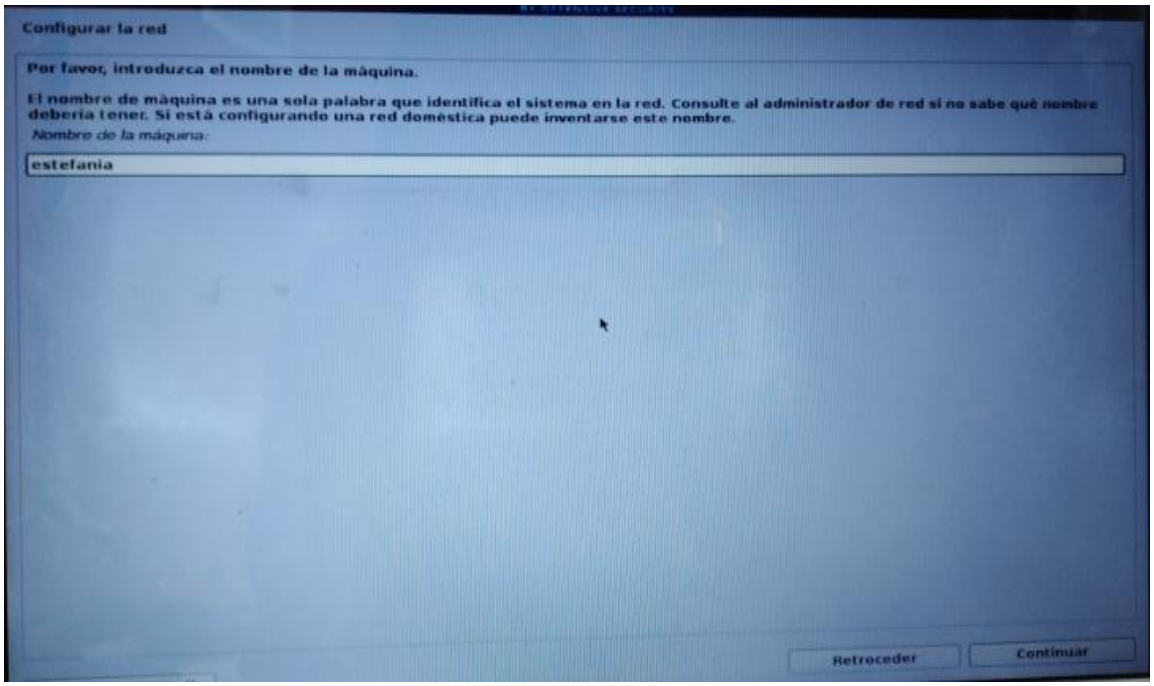


Ilustración 42: Configuración de red.

El siguiente paso indica seleccionar o configurar el reloj.

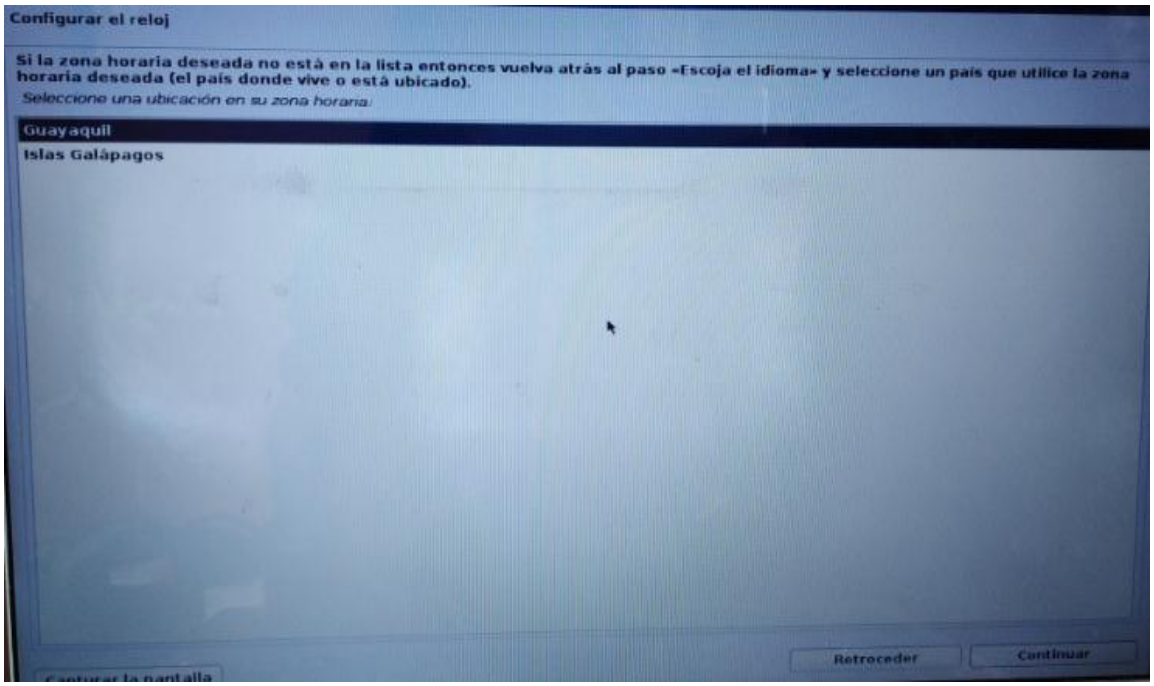


Ilustración 43: Configuración de reloj

Se selecciona la partición de los discos en la que indica distintos esquemas en este caso se procede a escoger la manual.

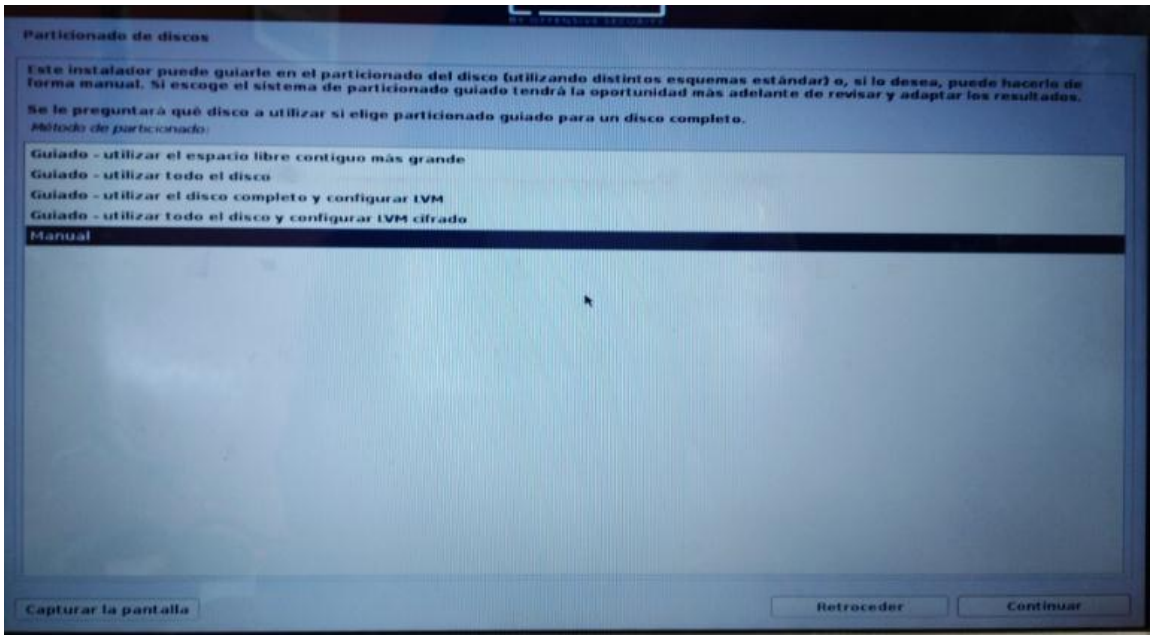


Ilustración 44: Partición de discos

En la siguiente ventana muestra un resumen de partición y puntos de montaje que tiene el sistema, en este caso se escoge la opción de espacio libre.

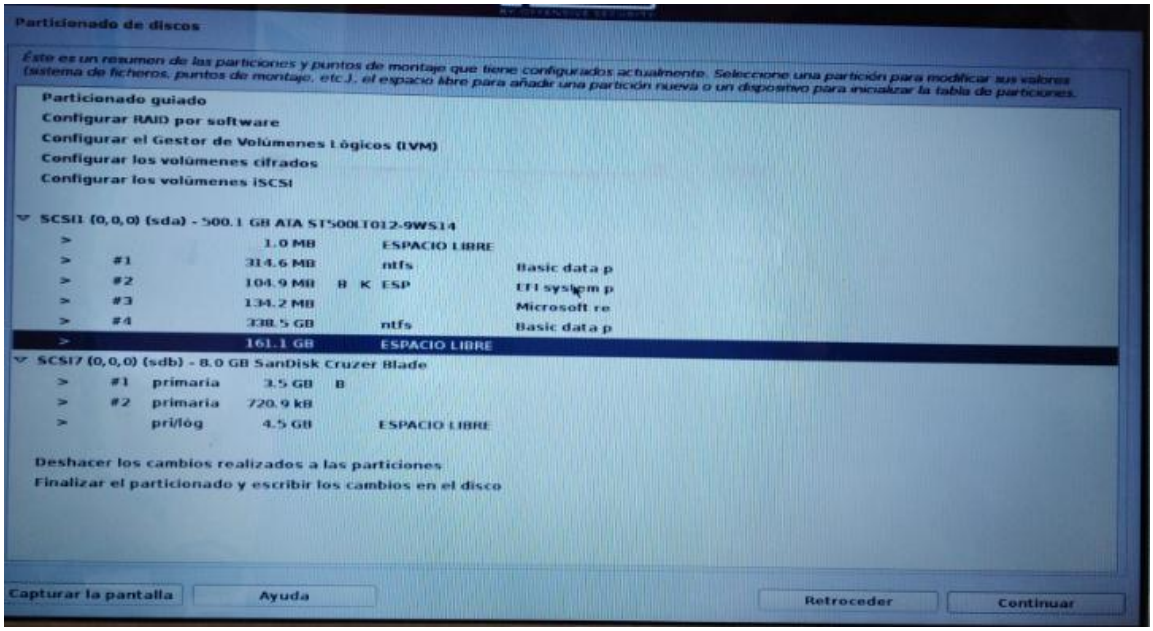


Ilustración 45: Elección de la partición

Guardar cambios de partición en el disco

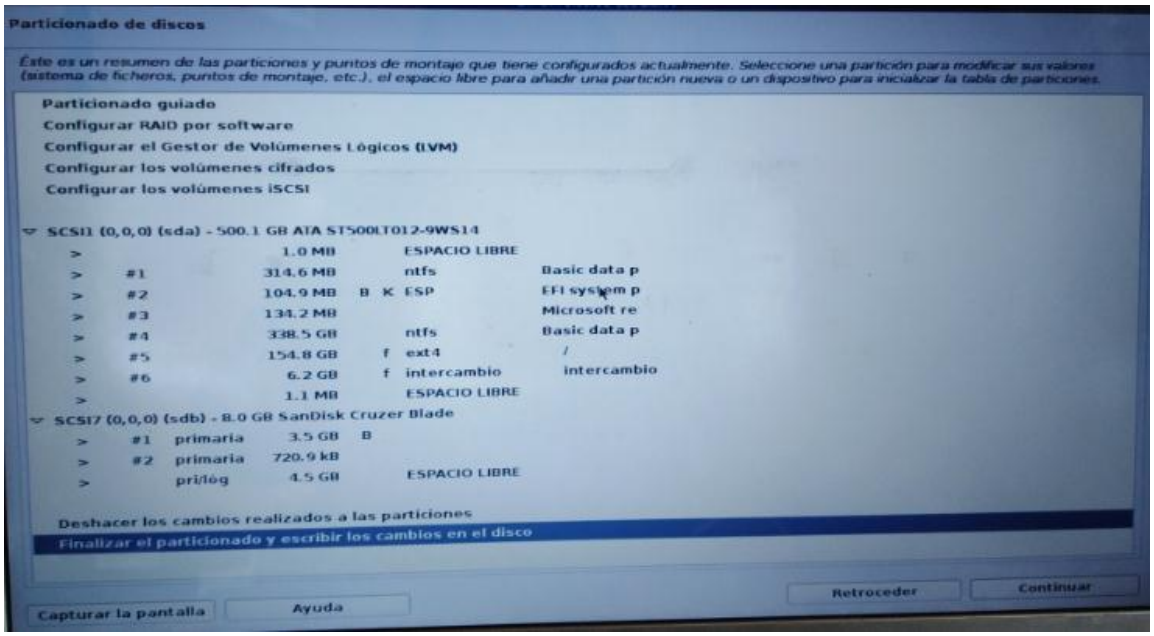


Ilustración 46: Guardar partición creada

Para concluir con la partición del disco se genera una pantalla en la que se indica si se está de acuerdo o no con los cambios que se realizó anteriormente, se escoge la opción sí.

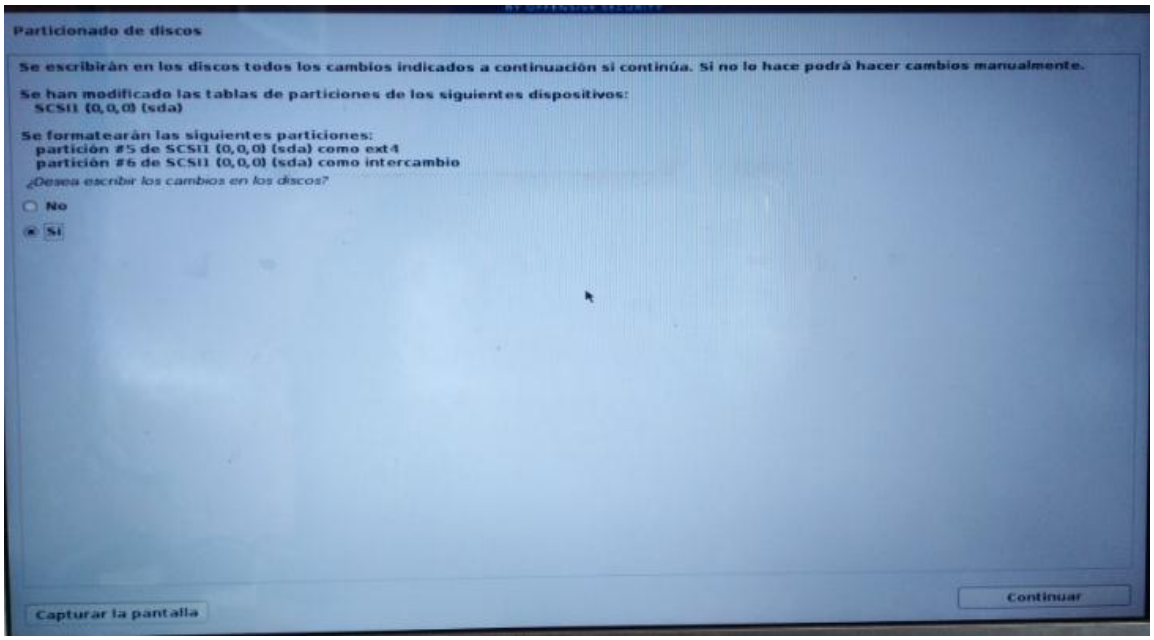


Ilustración 47: Grabar partición en el disco

Se espera que concluya el proceso de instalación.

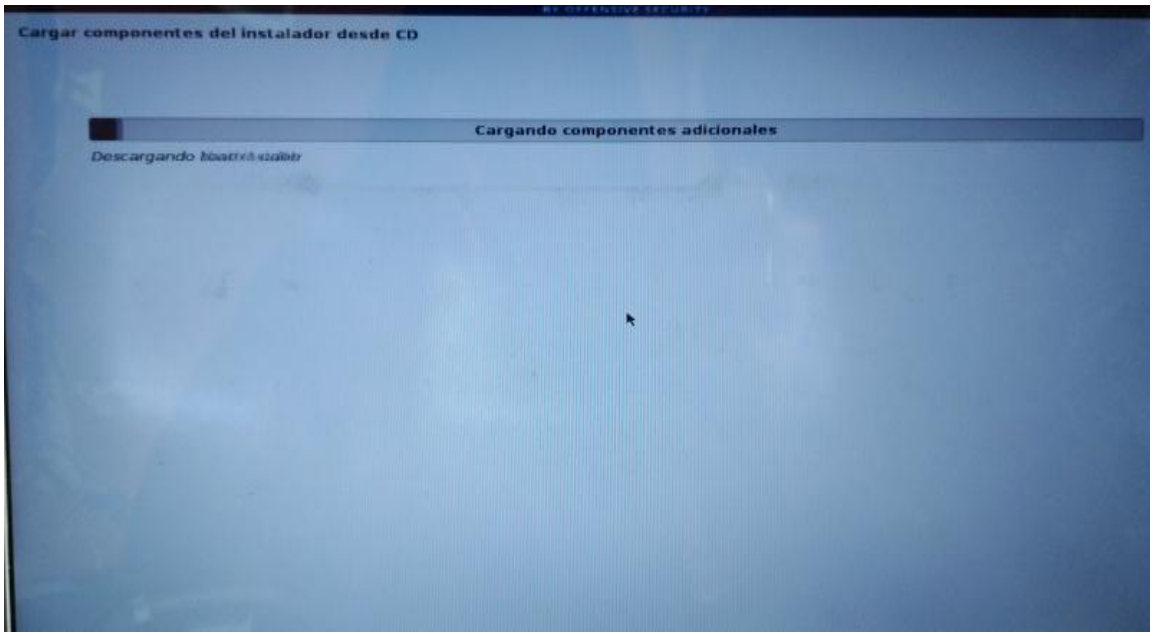


Ilustración 48: Conclusión proceso de instalación

Continuando con la instalación aparece una ventana en la cual pregunta si desea utilizar una réplica en red si está o no de acuerdo con la configuración de paquetes, seleccione la opción NO.

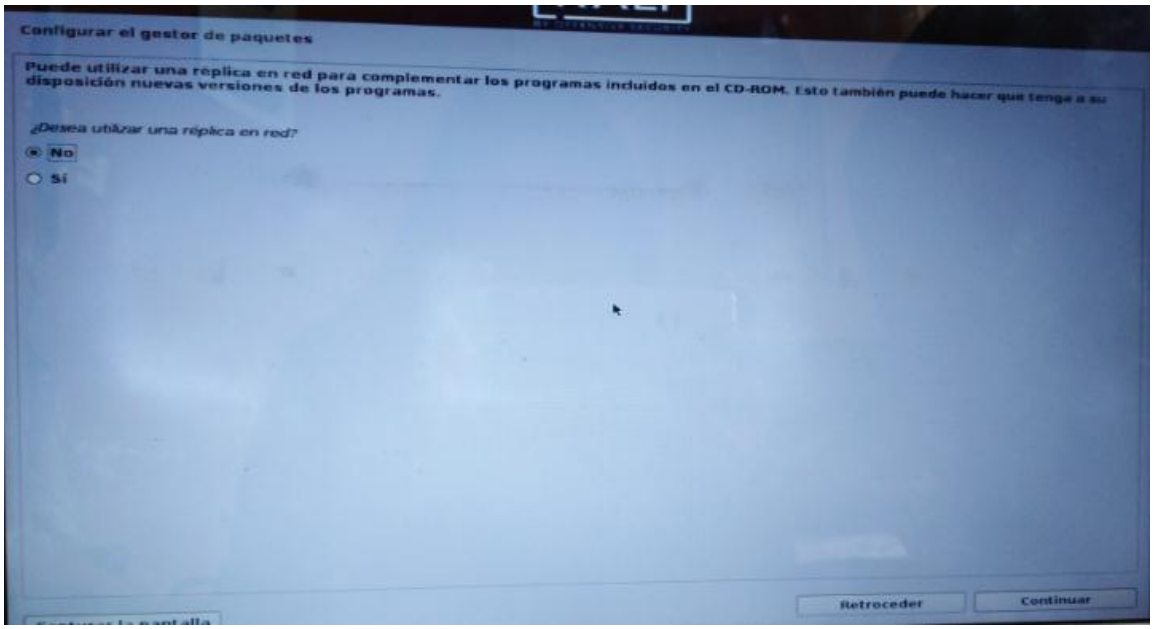


Ilustración 49: Réplica en red

Se procede a instalar el cargador de arranque GRUB en el disco duro.

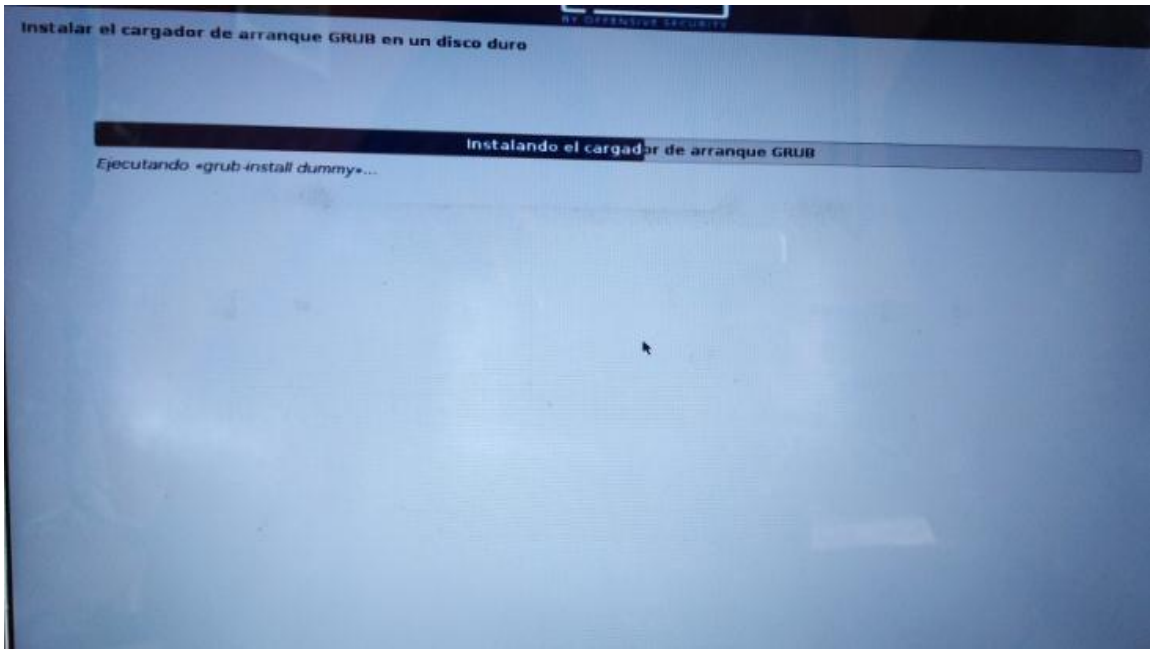


Ilustración 50: Cargador de arranque GRUB

Al culminar muestra una página que indica que el sistema se ha instalación.

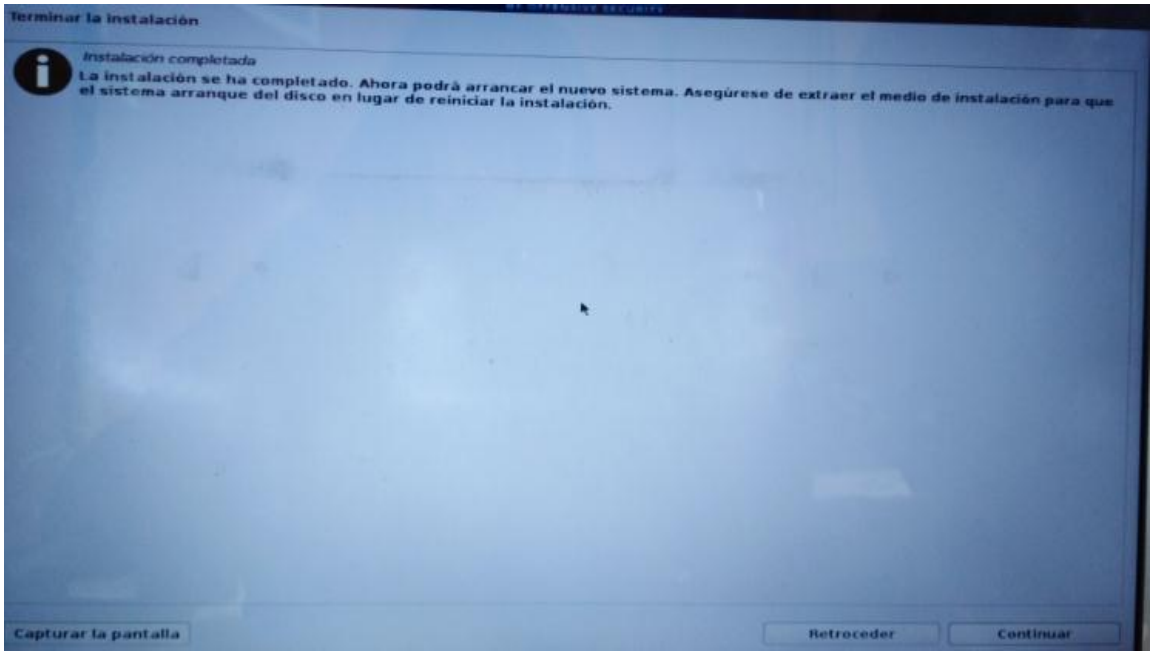


Ilustración 51: Sistema se ha instalación

Ya finalizada la instalación del sistema operativo, está listo para utilizarlo.

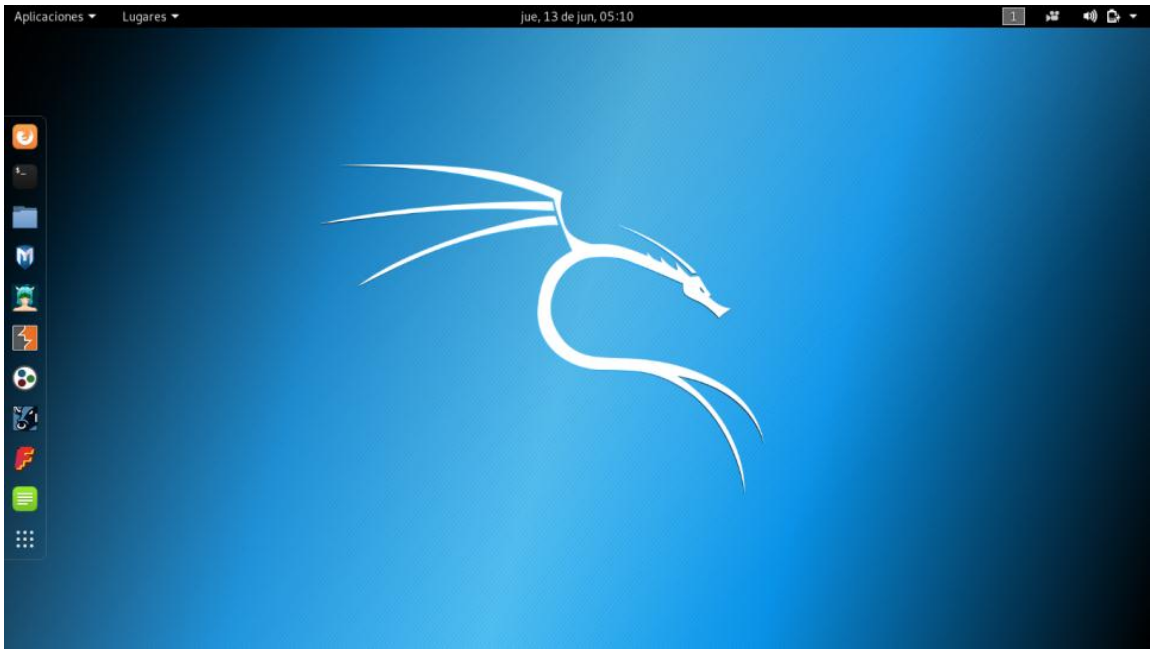


Ilustración 52: Pantalla de Kali Linux

Anexo B: Instalación de Nessus

Para proceder a la instalación del NESSUS se ingresa a la página oficial https://www.tenable.com/downloads/nessus y se descargar el paquete de instalación.

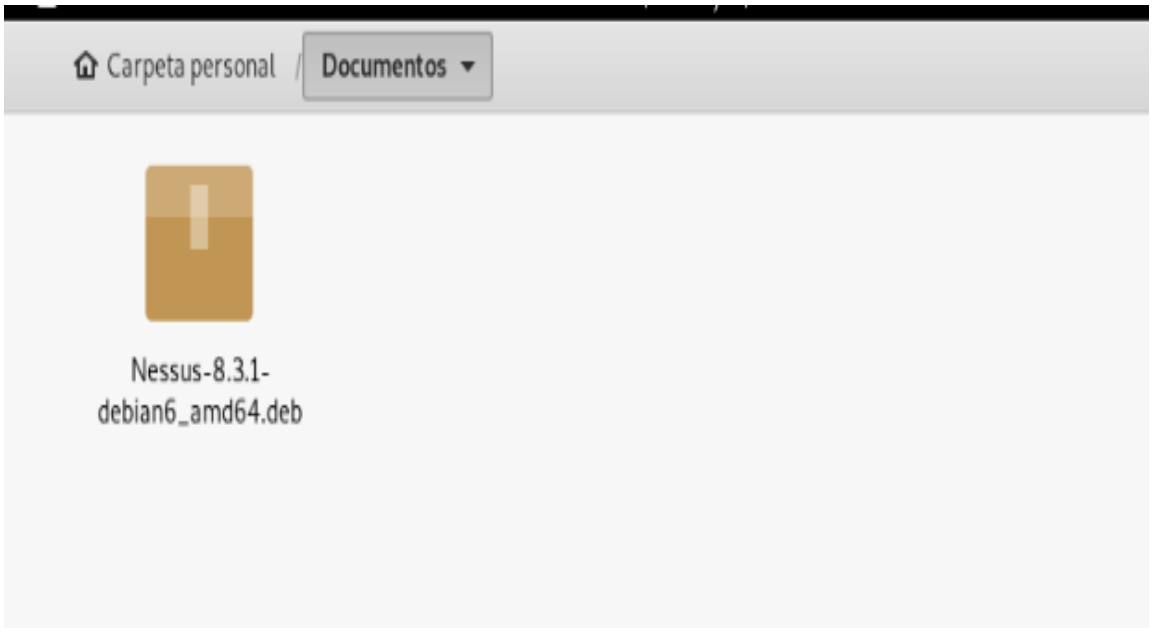


Ilustración 53: Descarga del paquete de instalación

A través de la termina se bebe direccionarse a la carpeta donde se encuentra el paquete y se lo ejecuta. Luego de la ejecución se inicializa el servicio.

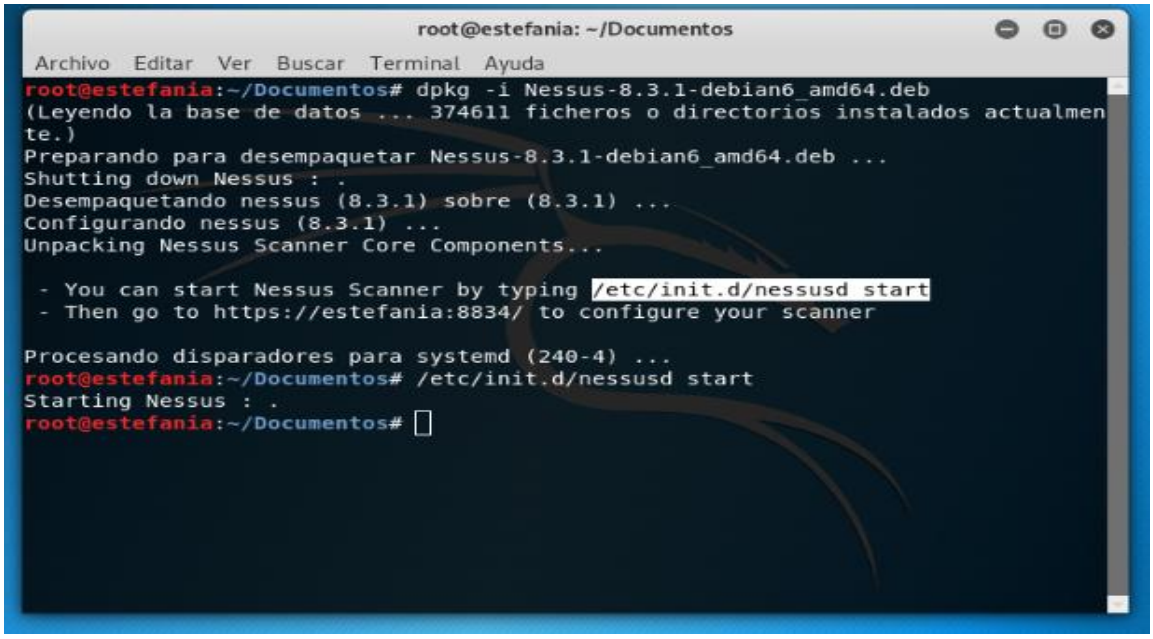


Ilustración 54: Inicialización del servicio

Luego de inicializado el servidor se ingresa al navegador web Iceweasel para continuar con la instalación y configuración de Nessus. Al ingresar a la URL https://estefania:8834 se presenta el mensaje sobre la confiabilidad de la conexión.

Se da clic en Go Back para continuar con la instalación.

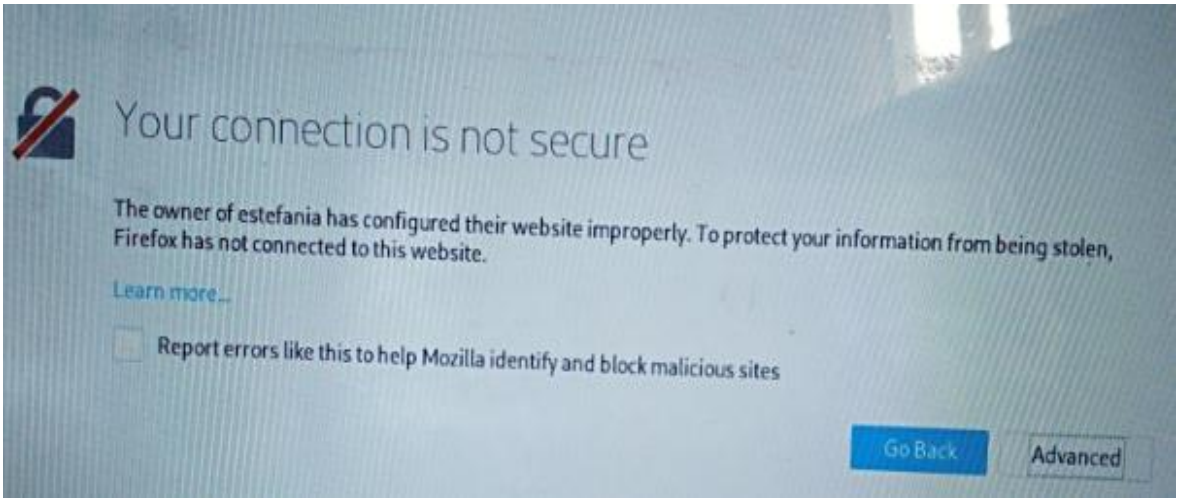


Ilustración 55: Ingresar a la URL https://estefania:8834

Se selecciona Add Exception, para añadir excepciones a la dirección.

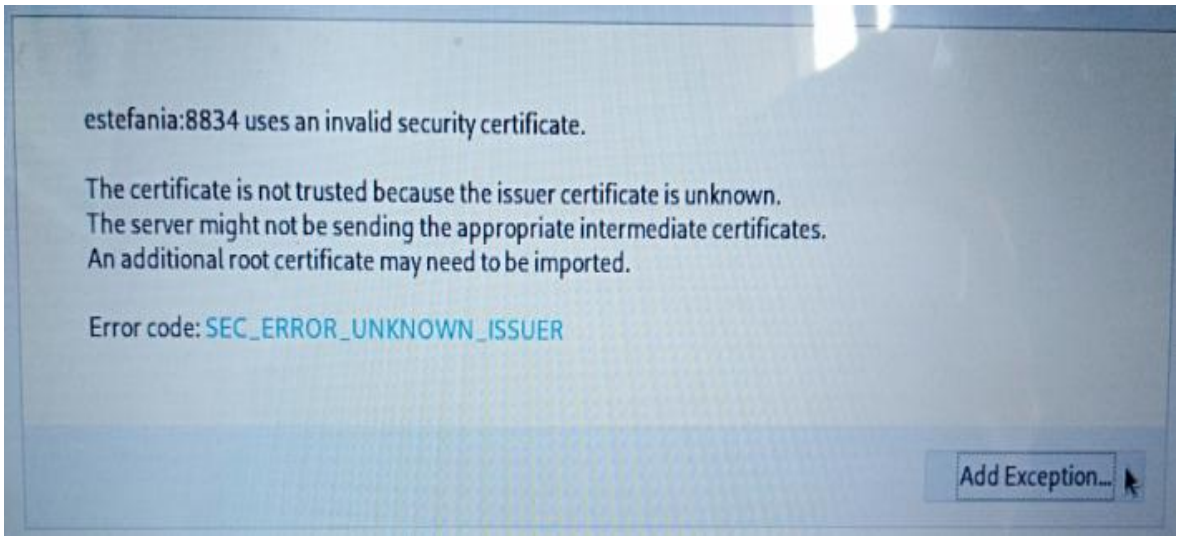


Ilustración 56: Añadir excepciones a la dirección

Siguientemente genera una ventana para ingresar las credenciales, completado los datos se da clic en Continue para continuar la instalación.

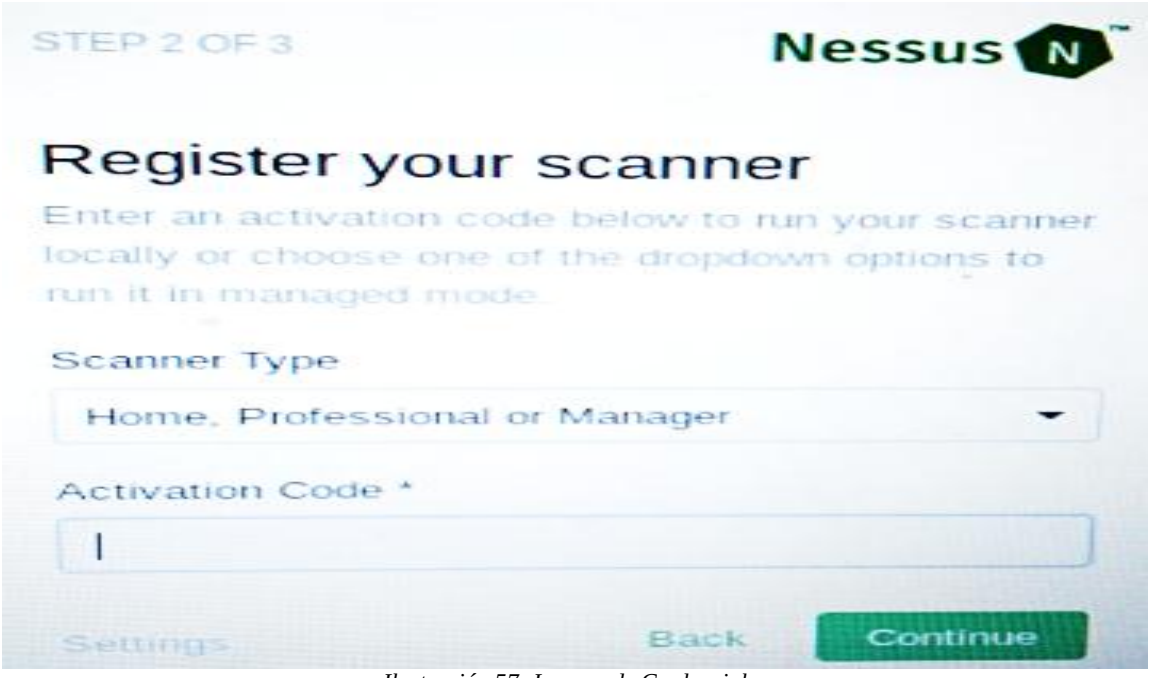


Ilustración 57: Ingreso de Credenciales

Se inicia la instalación de Nessus.

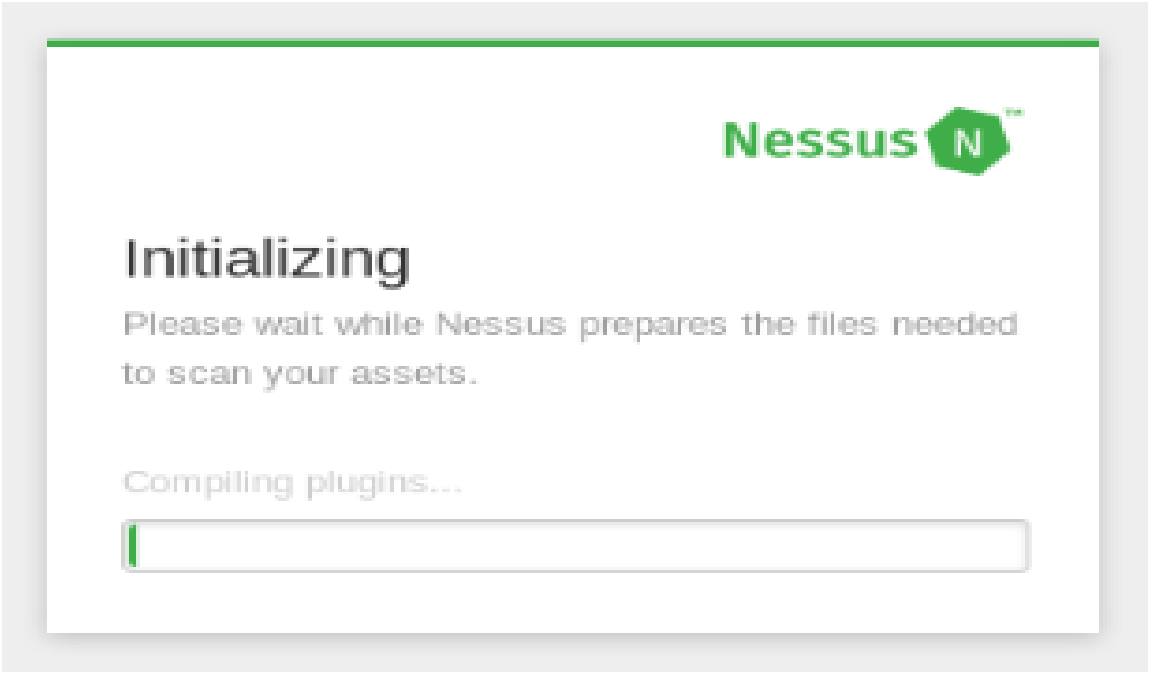


Ilustración 58: Inicio de la instalación

Al concluir con la instalación se crea una ventana para crear usuario en Nessus.

Ilustración 59: Ingreso a Nessus

Anexo C: Instalación de Nmap

Para la instalación del nmap se debe abrir la terminal de Kali Linux y tipiar la línea de código apt-get install nmap.

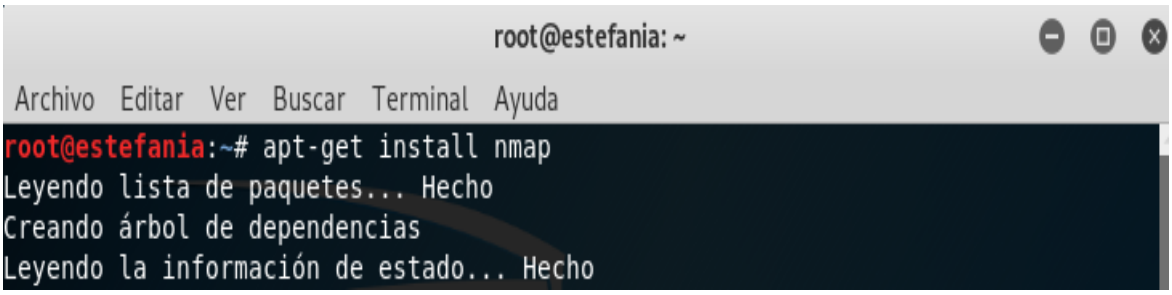


Ilustración 60: Instalación del nmap

Anexo D: Instalación del Framework Metasploit

Para instala Metasploit se debe iniciar el servicio de postgresql y se verifica que el estado se encuentre activo.

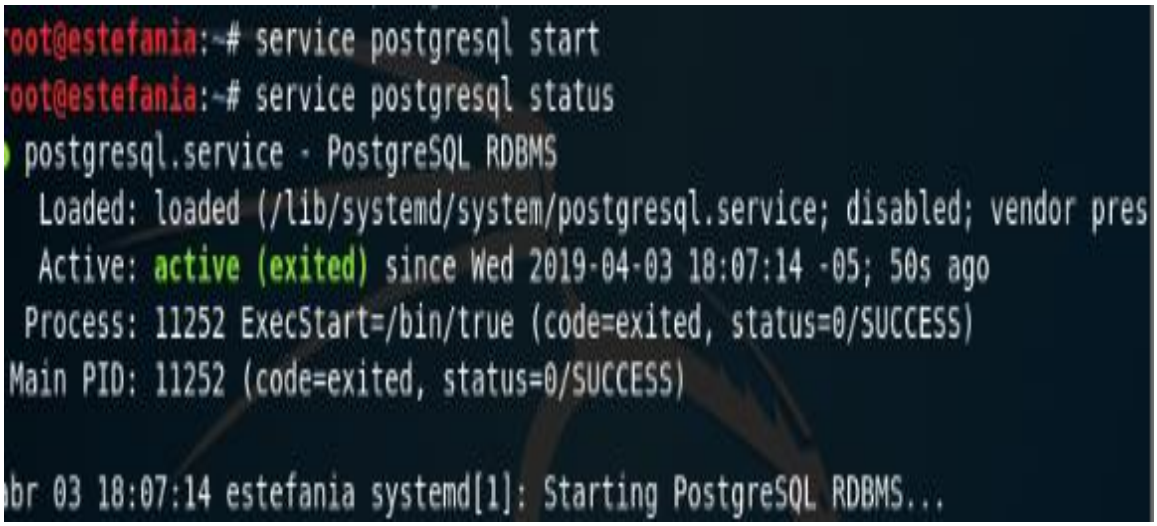


Ilustración 61: Inicio del servicio de postgresql

Se debe iniciar el servicio de Metasploit y con msfconsole se empieza a correr el programa.

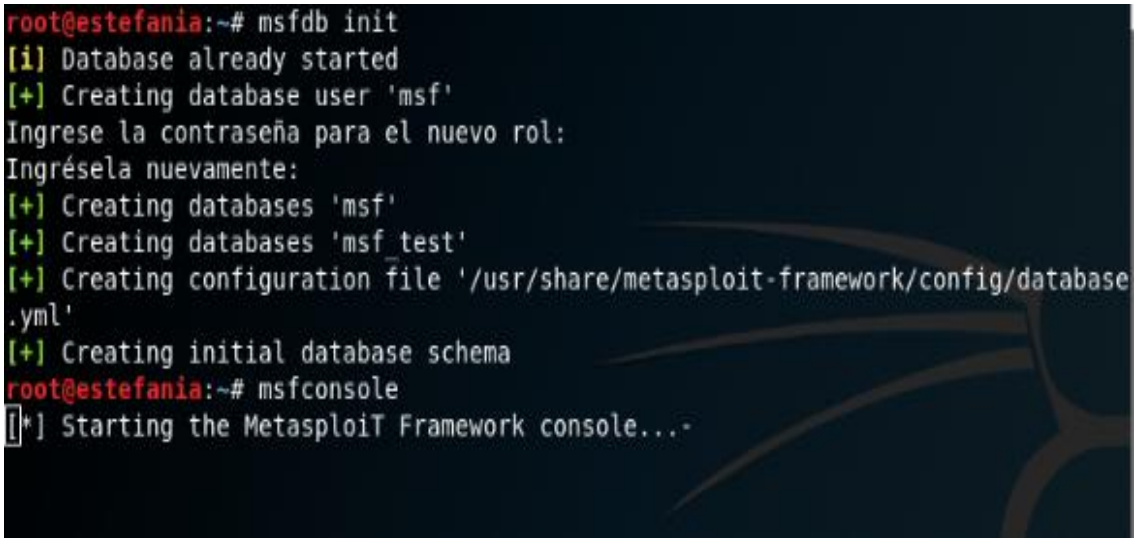


Ilustración 62: Inicio del servicio de Metasploit

Ya terminado el proceso muestra la pantalla de Metasploit y la versión instalada.

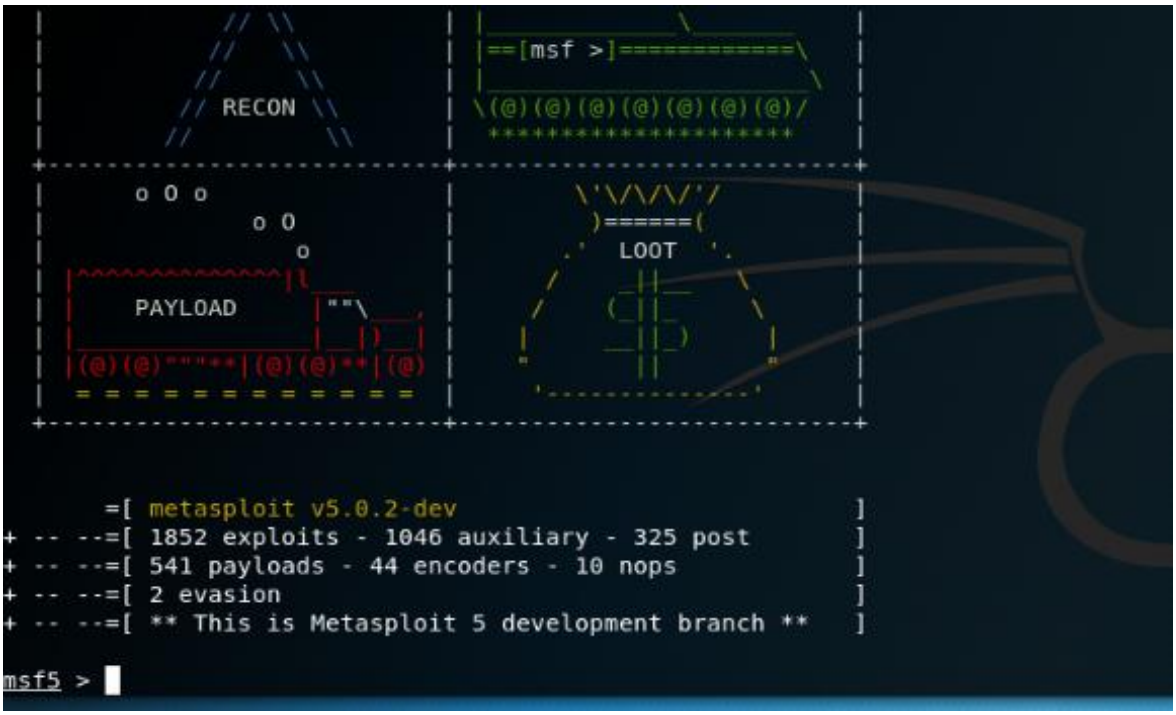


Ilustración 63: versión de Metasploit instalada

Anexo E: Ficha 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:** Estefanía Lema
Lugar:	Gobierno Autónomo Descentralizado del Cantón San Miguel	
Objetivo de la observación:	Identificar las vulnerabilidades presentes en el servidor de base de datos de catastro de la municipalidad del Cantón San Miguel.	

ACTIVIDADES	**SI**	**NO**	**DE VEZ EN CUANDO**
Los dispositivos y periféricos son exclusivamente utilizados para este servidor		X	
Se permite el acceso a este servidor a todo el personal		X	
Tiene herramientas para detectar intrusiones		X	
Las contraseñas que utiliza en este servidor, tiende a cambiar con frecuencia			X
Los puertos del servidor de catastros están disponibles para todo el personal	X		

Fuente: Análisis De Observación Del Gobierno Autónomo Descentralizado San Miguel

Anexo F: Entrevista al Jefe Inmediato de la Unidad de Sistemas

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: Estefanía Lema **Fecha:** 25/02/2019

Entrevistado: Ing. Marcelo Núñez **Lugar de la entrevista:** GAD SAN MIGUEL

1. **¿Se ha realizado alguna prueba para detectar vulnerabilidades en el servidor de BD de catastro?**
   No se ha realizado ninguna prueba para detectar vulnerabilidades en este servidor en ninguna ocasiones.
2. **¿Los dispositivos y periféricos son exclusivamente utilizados para el servidor de BD de catastro?**
   No, ciertos equipos y periféricos se utilizan en otros equipos informáticos de acuerdo a la necesidad que se presente.
3. **¿El GAD cuenta con alguna herramienta de software para detectar vulnerabilidades el servidor de BD de catastro?**
   No cuenta con ninguna herramienta software instalada en el servidor de BD de catastro.
4. **¿Se permite el acceso al departamento de equipos informáticos a todo el personal?**
   Si se permite el acceso al personal, pero no tienen permiso para manipular el servidor de BD de catastro.
5. **¿El personal tiene acceso a los puertos de comunicación el servidor de BD de catastro?**
   Si, las unidades de Administración, Avaluos, Catastro, Planificación, Rentas y usuarios en general tienen permisos restringidos.
6. **¿Las contraseñas que utilizan en el servidor de BD de catastro, tienden a cambiarse con frecuencia?**
   Esto se hace de vez en cuando.

Gobierno Autónomo Descentralizado Municipal San Miguel de Bolívar TECNOLOGÍA Y SISTEMAS

Anexo G: Solicitud de autorización

San Miguel, 31 de Mayo de 2019

Dr. Stalin Carrasco

ALCALDE DEL CANTÓN SAN MIGUEL DE BOLÍVAR

De mi consideración,

Yo, **JESSICA ESTEFANÍA LEMA TENELEMA**, con C.I. 0**202419636**, estudiante de la Universidad Estatal de Bolívar, Escuela de Sistemas me dirijo a usted, con la finalidad de solicitar la autorización para realizar mi **Proyecto de Titulación** en el **Gobierno Autónomo Descentralizado del Cantón San Miguel**, ya que este es un requisito indispensable para culminar mis estudios de tercer nivel y obtener mi título de Ingeniera en Sistemas computacionales.

De ante mano agradezco la atención prestada a esta solicitud, deseándole éxitos en todas las funciones que usted desempeña.

Atentamente.

JESSICA ESTEFANÍA LEMA TENELEMA

0202419636

SOLICITANTE

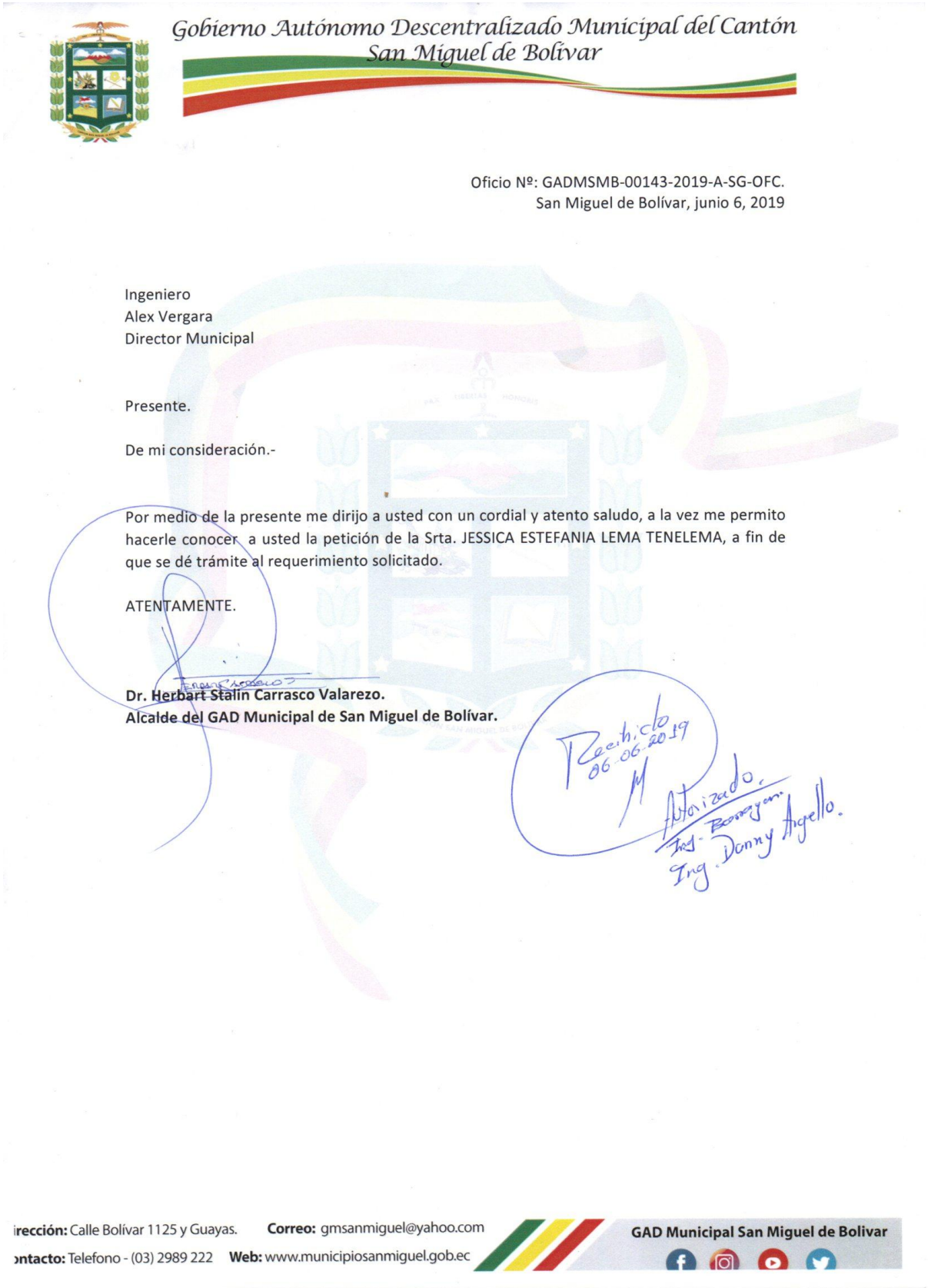
Gobierno Autónomo Descentralizado Municipal SAN MIGUEL de Bolívar PROSECRETARIA

FECHA 31-05-2019 HORA 10:30

ENTREGUE Jessica Lema RECIBIO

0979625273

Anexo H: Aprobación para realizar el proyecto



Gobierno Autónomo Descentralizado Municipal del Cantón
San Miguel de Bolívar

Oficio Nº: GADMSMB-00143-2019-A-SG-OFC.
San Miguel de Bolívar, junio 6, 2019

Ingeniero
Alex Vergara
Director Municipal

Presente.

De mi consideración.-

Por medio de la presente me dirijo a usted con un cordial y atento saludo, a la vez me permito hacerle conocer a usted la petición de la Srta. JESSICA ESTEFANIA LEMA TENELEMA, a fin de que se dé trámite al requerimiento solicitado.

ATENTAMENTE.

Dr. Herbart Stalin Carrasco Valarezo.
Alcalde del GAD Municipal de San Miguel de Bolívar.

Recibido
06.06.2019

Autorizado.
Ing. Donny Angello.

Anexo I: Unidad de Sistemas

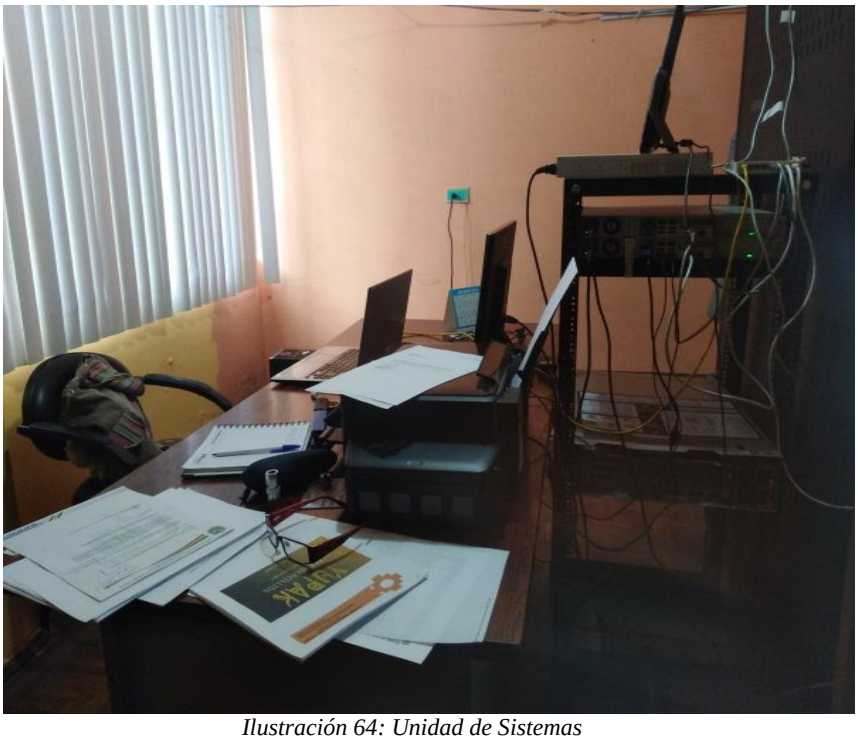


Ilustración 64: Unidad de Sistemas

Ilustración 65: Jefe de la Unidad de Sistemas

Anexo J: Certificado del Urkund