PRUEBAS DE PENETRACIÓN EN LAS REDES DE DATOS EN CUALQUIER ENTIDAD PÚBLICA O PRIVADA

AUTOR:

JUAN SEBASTIÁN FERRE BUSTOS

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGICAS E INGENIERIA
ESPECIALIZACION SEGURIDAD INFORMATICA
BOGOTA
2020

PRUEBAS DE PENETRACIÓN EN LAS REDES DE DATOS EN CUALQUIER ENTIDAD PÚBLICA O PRIVADA

AUTOR:

JUAN SEBASTIÁN FERRE BUSTOS

PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR DE PROYECTO
INGENIERO EDGAR MAURICIO LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGICAS E INGENIERIA
ESPECIALIZACION SEGURIDAD INFORMATICA
BOGOTA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá 5 octubre 2020

DEDICATORIA.

Dedico este trabajo de grado a Dios y mi familia porque me brindaron la oportunidad de realizar este estudio. Le doy gracias a Dios por ser mi compañía y mi guía a lo largo de este tiempo donde adquirí nuevos conocimientos, y por regalarme el tiempo y el don del aprendizaje, para absorber la información que me brindo la universidad.

Doy gracias a mi madre Gladys Bustos Ariza por regalarme su apoyo para realizar la especialización, por los valores ético que me han enseñado, y por haberme regalado los medios para tener una formación educativa.

A mi hermano mayor Camilo Andrés Ferrer por su apoyo y por ser parte fundamental de mi vida ya que con sus consejos y su ejemplo como persona y como profesional me han guiado en mi vida personal y profesional.

AGRADECIMIENTO.

Agradezco a Dios por regalarme la oportunidad de realizar mis estudios en la universidad nacional abierta y a distancia, y regalarme la sabiduría el esfuerzo para ayudarme con el tiempo para culminar.

Agradezco a mi madre por enseñarme a esforzarme por mis sueños, por inculcarme valores que me ayudan a compórtame en sociedad, y todo el esfuerzo que realizo para sacarme adelante. Mi Hermano Mayor por darme el apoyo para realizar la especialización y los consejos que me brindo para realizar este trabajo de grado.

Doy gracias a mi director de trabajo de grado Ingeniero Edgar Mauricio López por sus consejos y accesorias para realizar esta monografía y por su tiempo dedicado que siempre estuvo con la mayor disposición para orientar el trabajo de grado.

GLOSARIO

Pentest: “se le llama regularmente a una serie de prácticas que se realizan para determinar la seguridad de redes de datos.[1]

Hacker: Personas que tienen grandes conocimientos de herramientas de software y conocimiento en redes de datos con lenguajes de desarrollo de software.[2]

Hacker de sombrero blanco: este término son profesionales con un gran nivel de conocimiento en aéreas de la tecnología. Se encargan de auditar las vulnerabilidades de los sistemas de la información. y no realizan ataques para dañar la infraestructura tecnología

Hacker de sombrero negro: es aquel que realiza ataques para encontrar fallas de seguridad, debilidades y vulnerabilidades para sacar provecho con el fin de de obtener beneficios propios o para comunidades

Sistema de información: es un grupo de elementos los cuales procesan la información y la publican en el momento que es solicitada

Kali: es un software de open Source, el cual tiene como fin proveer entrenamiento en seguridad informática Y pruebas de penetración

Nmap: Esta herramienta es un software de código libre, que se utiliza para realizar escaneo de puertos, servicios y descubrir servidores en una red informática.

---

[1]GUILLÉN José Introducción al pentesting [En línea] tesis de grado Universidad de Barcelona_2017_Disponible_en_http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

[2] CORNEJO GLORIA. investigación sobre el hacker y sus posibles comienzos en la Comunidad estudiantil. Tesis de grado. Unipiloto Bogotá 2015. Disponible en http://polux.unipiloto.edu.co:8080/00002887.pdf

Resumen

La ingeniería es una ciencia aplicada la cual utiliza diferentes metodologías. Se basan en estudios para mejorar procesos como son los que tiene que ver con la seguridad de la información. Este trabajo de grado se realiza para obtener una guía metodológica donde se realizan pruebas de penetración en las redes de datos.

En la actualidad el nivel de seguridad de los sistemas informáticos empresariales es un tema de gran importancia pero que por falta de recursos o falta de conocimiento se resta importancia. Algunas empresas no están preparadas ni cuentan con el personal calificado en seguridad informática ya que no se tiene la información necesaria o no se tiene la solvencia economía para contratar una auditoría donde se muestre las fallas de las redes de datos gracias a la tecnología ha permitido el desarrollo de las pruebas de penetración, el objetivos es la identificación de vulnerabilidades mediante el uso de técnicas y herramientas, que permiten prevenir de los posibles ataques informáticos.

Los resultados que se espera cuando se termine esta monografía es tener conocimientos condensados en este informe que puedan servir como pautas para la solución de problemas de seguridad informática en las entidades públicas o privadas

Se pretende tener una metodología para la cual las empresas se puedan apoyar, será encaminada en la eficiencia. Para tener pautas, que será un procedimiento para tener una idea, en el desarrollo en las actividades cotidianas para implementar pruebas de pentesting.

ABSTRACT

Engineering is a science that uses different methodologies to apply control analyzes. Using tools which are based on studies to improve processes such as those related to information security. This degree work is carried out to obtain a methodology to carry out penetration tests in data networks.

Entities face the problem that they do not have the knowledge or qualified personnel to solve security problems, as they do not have the necessary information or they do not have the financial solvency to contract an audit that shows security flaws. Of the information that is available, it is for this reason that it is important to carry out this monograph which will allow people with basic knowledge of systems to evaluate the data network that they have.

The expected results when this monograph is finished is to have condensed knowledge in this report that can serve as guidelines for solving computer security problems in public or private entities.

It is intended to have a methodology for which companies can support, it will be aimed at efficiency. To have guidelines, which will be a procedure to have an idea that can be applied in the development of the activities of an entity.

Contenido

LISTA DE FIGURAS

INTRODUCCIÓN

Las vulnerabilidades en los activos informáticos, permiten a una persona mal intencionada poder entrar a manipular las redes de datos dándoles la oportunidad de manipular la integridad de los datos. Las vulnerabilidades son debilidades que pone en riesgo la seguridad de la información, Las vulnerabilidades se pueden combatir con actualizaciones en los sistemas operativos o con cambios del hardware. Las diferentes vulnerabilidades que se pueden encontrar se publican antes de que existan una solución.

Las principales vulnerabilidades son aprovechadas por programas conocidos como códigos maliciosos, estos permiten aprovecharse de alguna debilidad que se estén ejecutando en una computadora. Estas vulnerabilidades se corrigen cuando se actualiza los sistemas operativos.

Existen personas con el suficiente conocimiento y experiencia para realizar pruebas de penetración a las redes de datos ellos son nombrados los Ethical Hackers. Este nombre se utiliza para diferenciar a profesionales que usan su conocimiento para el aseguramiento de la información usando ataques a las redes de datos, con conocimiento de los dueños de las redes, aplicando métodos que pueden utilizar personas inescrupulosas, los Ethical Hackers buscan vulnerabilidades que pueden ser utilizadas para realizar daños.

El origen para la realización de este trabajo de grado se debe a las dificultades que se presentan en las empresas al no contar con un documento guía que les permita evaluar su red de datos, el objetivo general de este trabajo de grado se basa en esta dificultad, Se ha desarrollado y diseñado una metodología para tal actividad.

1. DEFINICION DEL PROBLEMA

Cuando una empresa sufre ataques a su información se ve afectada la operatividad y credibilidad de esta, existe mucha información dispersa o diferentes metodologías que ayudan a evaluar una red de datos, es por eso que este documento toma importancia como una base o guía para iniciar en las pruebas de pentesting ya que sirve Como base o fundamento para la elaboración de una metodología independientemente de la empresa.

Hugo Scolinkcreó autor del libro “que es la seguridad informática” el cual, sirve como una guía para ayudar a comprender lo fundamental que es la seguridad informática en este mundo, que es dependiente de la informática. Es por eso que se desea desarrollar este trabajo de grado el cual también servirá para saber que se necesita a la hora de encontrar vulnerabilidades en las redes de datos.

Planteamiento del problema

Actualmente las empresas se ven atacadas constantemente en su red de datos, existen diferentes maneras de atacar una red de datos, para detectar los puntos críticos que tienen, se deben realizar estudios, dado esto las empresas tienen un problema, el cual es saber ¿Qué tan vulnerables son las redes de datos ante posibles ataques de personas altamente cualificadas en cibera taques?

Las empresas ya sean públicas o privada desean tener una metodología para proteger su información, sin tener que gastar tanto tiempo y dinero en la búsqueda de soluciones ya que los expertos en seguridad cobran por su conocimiento y existen pequeñas empresas que no tienen el recurso económico para acceder a ellos.

Formulación del problema.

¿Como realizar una metodología para diagnosticar una red de datos?

2. JUSTIFICACION

Se considera importante la elaboración de esta monografía de grado ya que actualmente la información es fundamental en una empresa, Si la información que maneja la empresa es afectada esto se puede ver reflejado en pérdidas para esta, es por esto que se considera fundamental este trabajo de grado.

Hoy en día las entidades han clasificado a sus redes de datos como un activo importante, porque estás permiten la interconexión de dispositivos de almacenamiento y pueden correr riesgos de poder ser vulnerados si no se tiene los parámetros de seguridad aceptables, Pueden tener posibles ataques sobre las vulnerabilidades y fallos de seguridad que estás tengan afectando los servicios e información que se transporta por estas, que personas mal intencionadas quieran realizar para dañar o modificar información fundamental para las entidades

Actualmente los ataques que sufren los sistemas informáticos, siempre son una amenaza a las redes datos, corporativa, es por esto que se plantea un procedimiento mediante el cual los encargados de administrar las redes de datos puedan tener una metodología para realizar pruebas de seguridad informática

Esta metodología debe estar basada en la práctica y la facilidad para que el administrador de la red, pueda implementar un análisis sin tener un amplio conocimiento sobre ataques informáticos, con este trabajo de grado se desarrolla una práctica para el análisis de las debilidades de la red de datos en cuestión seguridad informática y con base a esto tener las políticas de seguridad informática adecuadas.

3. OBJETIVOS

3.1. General

- Documentar una Metodología para encontrar fallas y vulnerabilidades sobre los sistemas informáticos de una red corporativa.

3.2. Específicos.

- Determinar las metodologías más comunes para encontrar vulnerabilidades en las redes de datos.

- Identificar herramientas tecnológicas para detectar fallas en las redes de datos.

- Estudiar las certificaciones de calidad para detectar fallas en las redes de datos.

- Determinar la información que se tiene que obtener para realizar un análisis de la Seguridad informática en una entidad

4. MARCO REFERENCIA

4.1. Marco teórico

A lo largo de la historia los avances tecnológicos han permitido el nacimiento de nuevas maneras de cometer delitos, como lo son los informáticos, los cuales utilizan como medio el internet y sus componentes de propagación, cuyo objetivo son las redes de datos de las organizaciones.

La monografía está basada en la documentación y creación de una metodología el cual tiene un procedimiento para determinar que se necesita para realizar pruebas de penetración sobre redes de datos, con el objetivo de minimizar los riesgos que se puedan encontrar, en una red de datos, dado que actualmente algunas entidades no tienen dentro de su estructura la prioridad de tener procedimiento para la realización de pruebas de penetración a sus redes de datos.

La metodología planteada en este documento será desarrollada no solo para documentar un procedimiento sino también para minimizar los riesgos que se presentan y concientizar a las entidades de la importancia de tener pruebas de pentesting a partir de los riesgos que se presentan.

Para la realización de la metodología que se desea plantear, para desarrollar pruebas de pentesting se debe conocer información en diferentes aspectos tales como lo son:

4.1.1. Caja Negra. En este caso, el equipo de profesionales sólo recibe el nombre de la institución, por lo que se trabaja con la información que se puede recolectar a través de medios públicos. Este tipo de pruebas simula el ataque de un cracker, por lo que permite medir el alcance e impacto que tendría un evento real.[3]

3 CAISA Jimena. Implementación de Pruebas Caja Negra y Caja Blanca. Tesis de grado._Latacunga_Ecuador_Unidad_académica_de_ciencias_de_la_ingeniería_y _Aplicadas_2010.Disponible_http://repositorio.utc.edu.ec/bitstream/27000/1166/1/ T-UTC-0823.pdf

4.1.2. Caja Blanca. Esto se desarrolla cuando se trabaja directamente sobre los activos a analizar y reduciendo el tiempo de las fases previas a la identificación y explotación de las vulnerabilidades.

4.1.3. Caja Gris. Es una agrupación de los tipos que se menciono anteriormente, en dónde se tiene información, pero no toda al equipo de consultores, tal como: segmentos de red, direcciones IP de servidores pertenecientes a la infraestructura de TI.

4.1.4. Red de datos. esta constituidos por la agrupación de dispositivos los cuales conforman una infraestructura cuyo diseño ayuda a él envió de información mediante la transmisión de archivos. Las diferentes redes han sido implementadas para suplir unos objetivos, con una infraestructura o arquitectura específica el cual mejora el intercambio de los contenidos. Pueden clasificarse de distintas maneras de acuerdo a la arquitectura física, el tamaño y la distancia de cobertura.[4]

4.1.5. Pentesting. El objetivo principal de las pruebas de penetración llamadas también pentest es una actividad que simula ataques pero que cuentan con el debido permiso de una empresa para identificar las vulnerabilidades y fortalezas que cuenta la empresa en su infraestructura tecnológica. Gracias a estas pruebas se puede hallar las vulnerabilidades con las que pueden estar expuestas las empresas. Esto ayuda a implementar un plan que brinda las correcciones en las redes de datos

4.1.6. Hacker. La palabra hacker fue nombrada por primera vez en 1960 en la academia de Massachusetts y está relacionada con el ruido que desprendían los dispositivos telefónicos en cuando se golpeaban para que sirvieran, pero en este contexto hace referencia a un profesional con conocimientos en informática para poder modificar o intervenir sistemas de información.

4.1.7. Vulnerabilidad, Riesgo y Amenaza Cuando se presentan vulnerabilidades en las redes de datos esto trae problemas. Dado que están expuestas a diferentes ataques informáticos por hackers maliciosos que ingresan a los sistemas de almacenamiento de datos[5]

---

4 FERRER Juan. Diseño de la distribución y cobertura de la red LAN. Tesis de grado. Armenia- Colombia. Universidad del Quindio.2015 Disponible en https://drive.google.com/file/d/1aONqwARiwOUghQ7kie3DhpIU96GUXPpz/view?usp=sharing

- **Una amenaza** es una situación que se presenta en un momento y afecta los diferentes activos informáticos, estas amenazas puede ser realizadas por diferentes personas externas o internas.

- **El riesgo.** va de la mano a las dificultades que se presentan por amenazas que pueden afectar el comportamiento natural del negocio si no se cuentan con las medidas necesarias.

- **Las vulnerabilidades.** la probabilidad de que se utilice una amenaza, son de diferentes circunstancias esto genera, un impacto y afectaciones susceptibles para los activos de la información

4.2. Marco conceptual

Se requiere estudiar para una mejor comprensión para el desarrollo de esta metodología algunos conceptos para tener una excelente administración de la información, tener las bases como las normas que se encuentran preestablecida las cuales permitirán que las personas o entidades sin mucho conocimiento puedan comprender que se necesita para tener asegurada la información.

Para el desarrollo de la metodología se debe poseer varios conceptos claros, tales como son:

4.1.1. Seguridad Informática. El concepto de seguridad informática tiene como objetivo en resguardar los activos del sistema de información de una entidad y que el ingreso a los datos que están almacenados solo pueda ser manipulada por las personas que estén habilitadas para tal fin.[6]

La seguridad informática, su trabajo es encargarse de las buenas

[5] CASTRO Duvan.riesgos, amenazas y vulnerabilidades de los sistemas de Información_Tesis_de_grado_Bogotá_D.C._universidad_católicadecolombia. 2013._Disponible. http://bdigital.unal.edu.co/view/types/thesis.html

[6] ALVARES Luis. Seguridad Informática auditoria de sistemas. Tesis de grado. México_D.C._Universidad_Iberoamericana._2005.Disponible. https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0000162027.

prácticas, cuyo objetivo es establecer las buenas condiciones de seguridad para la manipulación de datos en un sistema informático. Hoy en día se establece que la base de seguridad de la infamación está basada 3 pilares los cuales son:

- Confidencialidad
- Integridad
- Disponibilidad

4.1.2. Las amenazas. Las amenazas que se presentan en el diferente sistema informático se pueden originar por un hacker que entra en el sistema por medio de software que permite, al atacante tener control de la máquina víctima, robando así los datos o manipulándolos, a continuación, algunas amenazas conocidas:

- **Puertas traseras***:* Son componentes de código de un software que se encuentran ubicados sin realizar ninguna función, los cuales se implementan dando la instrucción causando dificultades en los sistemas informáticos.

- **Virus***:* es una línea seguidas de código software que ingresan en un archivo que se ejecuta llamado huésped de manera que cuando el archivo se inicia el virus también, infectando a otros programas. Y d

- **Como proteger nuestro sistema**. Para proteger los Sistema informático se debe realizar un detallado estudio de las diferentes vulnerabilidades, las diferentes pérdidas de información que se pueden encontrar.[7]

Con base a este análisis se debe diseñar políticas de seguridad que tengan como prioridad definir criterios de responsabilidades y normas a seguir para evitar tales vulnerabilidades o disminuir sus consecuencias en caso de que se presenten, a esto se le llama metodología de seguridad, son la herramienta que garantizan la integridad de los sistemas que resguardan información. Las metodologías de protección de la información se pueden clasificar en activas y pasivas

[7] BUSTAMANTE Ruben.Seguridad en Redes. Tesis de grado. Estado de Hidalgo._Universidad_Autónoma_del_estado_de_Hidalgo.2014_Disponible_https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Se guridad%20en%20redes.pdf

- **Activas***:* protegen los diferentes sistemas informáticos de daños, gracias al uso de contraseñas para el ingreso a sistemas y aplicaciones, encriptación de los diferentes archivos que se transfieren en las comunicaciones,
- **Pasiva:** disminuye los impactos y los diferentes efectos que causan los inconvenientes que puedan presentarse en el hardware

4.1.3. Redes de datos. están interconectadas por host los cuales transmiten información, Esta interconexión es a través de un enlace físico Algunos profesionales creen que una red de datos es la unión de tres o más Host conectadas. Para Transmitir la información las redes de datos se dividen según su extensión geográfica las cuales son[8]

- Área de red local (LAN)
- Área de red metropolitana (MAN)
- Área de red amplia (WAN)

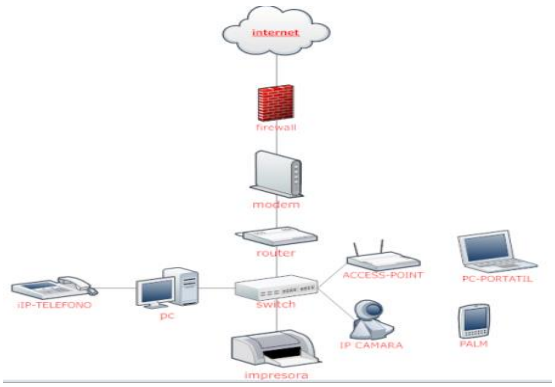
Entre los equipos que se interconecta en una red de computadores, se tienen los siguientes:

- ***Router.*** Dispositivo que se utiliza para comunicar redes de datos se maneja en la capa tres del modelo OSI
- ***Switch.*** Es un componente informático que permite la interconexión de redes de datos .El objetivo principal es interconectar dos o más elementos de red,
- ***Modem.*** Un modem es un dispositivo que permite convertir las señales digitales en señale inalámbricas

Servidor. Es un dispositivo que permite compartir un recurso para realizar algunas tareas requeridas por los usuarios.

8FERRER Juan. Diseño de la distribución y cobertura de la red LAN. Tesis de grado. Armenia- Colombia. Universidad del Quindio.2015 Disponible en https://drive.google.com/file/d/1aONqwARiwOUghQ7kie3DhpIU96GUXPpz/view?usp=sharing

Figura Esquema de una red LAN



Fuente: Propia del autor

:

4.3. ANTECEDENTES.

En el área de la seguridad informática se han venido desarrollando en los últimos años diferentes tipos de aplicaciones e investigaciones con el fin de reducir los riesgos a los que se enfrentan las empresas y dar soporte a las operaciones del negocio. A continuación, se describen algunos de los avances que han logrado en Colombia en diferentes entidades y/o universidades.

En la Universidad Nacional Mayor de San Marcos, facultad de Ciencias Matemáticas, en el 2003, se desarrolló el proyecto. Plan de seguridad informática para una entidad financiera. El cual consiste en definir un plan de seguridad para una entidad financiera, empieza por definir la estructura organizacional (roles y funciones), después pasa a definir las políticas, para finalmente concluir con un plan de implementación o adecuación a las políticas anteriormente definidas. [10]

En la Universidad Nacional Abierta y a distancia, escuela de ciencias básicas e ingeniería, Especialización en seguridad informática, en el 2017 se desarrolló el proyecto diseño de un sistema de gestión de la seguridad de la información (sgsi) en el área tecnológica de la comisión nacional del servicio civil - cnsc basado en la norma iso27000 e iso27001 el objetivo fue. Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27000 e 27001 para mejorar la seguridad de las tecnologías de información y las comunicaciones (TI's)

---

9 AGUIRRE Juan, diseño del sistema de gestión. Tesis de grado. Pereira Colombia.Universidad_Tecnología_de_Pereira_2013_Disponible_http://scienti.colciencias.gov.co:8081/cvlac/visualizador_/generarCurriculoCv.do?cod_rh=0000715638

En la Universidad Nacional Abierta y a distancia, escuela de ciencias básicas e ingeniería, Especialización en seguridad informática, en el año 2014 se desarrolló el proyecto propuesta de procedimiento para la ejecución de pentest dentro del esquema de pruebas de las fábricas de[12] software para aplicaciones web su objetivo principal fue Proponer un procedimiento para la ejecución de pentest dentro del esquema de pruebas de las fábricas de software.

4.4. MARCO METODOLÓGICO

En el área de la seguridad informática existen metodologías o estándares los cuales ayudan o permiten la actividad ordenada y con estándares de calidad ya que son planteadas por expertos en el área de procesos de una manera ordenada, algunas de estas metodologías conocidas por los profesionales de seguridad informática son:

4.4.1. OSSTMM. La guía metodológica de Abierta de Testeo de Seguridad u Open Source Security Testing Metodología Fue inventada por la entidad de la Seguridad y Metodologías Abiertas ISECOM y a finales del año 2000 fue publicada, esta metodología marco las bases ya que no se tenía un estándar que reuniera los temas y actividades que se tienen que tener como fundamento por un profesional en seguridad informática.[13]

10 CÓRDOVA Rodríguez, plan de seguridad informática para una entidad financiera. Tesis_de_grado._Lima.Disponible_Universidad_Nacional_Mayor_de_San_Marcos2003.Disponible._http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/Cordova_RN/T_completo.pdf en la Comisión Nacional del Servicio Civil (CNSC).

11 CAMARGO Juan. Diseño de un sistema de gestión. Tesis de grado. Bogotá D.c Universidad_nacional_abierta_y_a_distancia_2017_Diposnible_https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11992/1/75104100.pdf

12 PÁEZ Miguel. Procedimiento para la ejecución de pentest. Tesis de grado. Bogotá D.C_Universidad_nacional_abierta_y_a_distancia_2014_Disponible_https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstr eam/10596/23458/1/nfpinzonb.pdf

La metodología OSSTMM permite establecer herramientas que se pueden aplicar en cada parte de la elaboración de actividades propuestas, Como se pudo detallar esta metodología se basa en un modelo de análisis que permite evaluar las vulnerabilidades de forma detallada, amplia y de manera ordenada, que se basa en una documentación que agrupa los resultados y las recomendaciones de la seguridad informática. Con esta metodología se pretende que las entidades tengan las medidas para tomar las decisiones con respecto a la seguridad de la información

4.4.2. OWASP. Es una organización que detalla las diferentes prácticas y los tipos de conceptos que están relacionados con las etapas que se tiene que realizar para Recopilar el Top 10 de las vulnerabilidades en los sitios web que, expertos en sus diferentes aéreas, de la seguridad evalúan[14]

4.4.3. ISSAF. Es una metodología muy conocida para el testeo de portales web, La metodología tiene de 2 fases, en la primera se realizan los siguientes temas:[15]

- Fundamentos del Pentesting
- Comprensión de las herramientas de testeo.

En la segundad fase, se estructuran todas las técnicas que se necesitan para testear el desarrollo de software

4.5. MARCO LEGAL

Todos los individuos que interactúan con la información tienen que cumplir los reglamentos que se encuentran vigentes, dado que el desconocimiento de estas no es justificación para ser exonerado de cumplir los reglamentos.

El desarrollo de la seguridad informática es una serie de procesos en donde se evalúan y determinan los riesgos, los cuales se apoyan en leyes y normas que integran las necesidades de las entidades, Cuando se desea desarrollar una metodología que involucre la manipulación de la información para las entidades ya sea pública o privada se tiene que basar en las normas, estándares que se aplican en función de las actividades.

4.5.1. Regulación a nivel internacional. A continuación se da una breve descripción sobre ISO/IEC 27000, estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La reglamentación ISO 27000 está basado en las mejores prácticas para desarrollar recomendaciones en seguridad de la información, para gestionar todo lo relacionado a los sistemas que se basan en la Gestión de la seguridad de la información. Estos documentos se encuentran así:

- **ISO/IEC 27000**: muestra la descripción general y la información que se necesita para ser utilizada en toda la serie 27000.
- **ISO/IEC 27001**.: Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Esta norma internacional retiene los requerimientos para el desarrollo de un SGSI, esta norma la certifica por las organizaciones externas a la organización. En sus Anexo A, cita una lista de los objetivos de control y controles que desarrolla

4.5.2. Regulación a nivel nacional: A continuación, se describen algunos reglamentos vigentes a nivel nacional que influyen directa o indirectamente en la seguridad informática de las empresas en Colombia

- La **Ley 1581 de 2012** prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Esta prohibición NO REGIRÁ cuando se trate de: Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia

- **Ley 527 de 18 de agosto de 1999,** sobre Mensajes de Datos, Comercio electrónico y Firma Digital: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Firma digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje

13 ZULUAGA Allen.Haking Ético basado en la metodología OSSTMM.Tesis de grado. Armenia_Universidad_nacional_abierta_y_a_distancia_2017.Disponible_https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/23458/1/nfpinzonb.pdf

14 BRIONES Gerson auditoria de seguridad del servidor web de la empresa publynext s.a. utilizando mecanismos basados en owasp Tesis grado. Guayaquil. Universidad de guayaquil 2018 Disponible http://repositorio.ug.edu.ec/handle/redug/26837

15 DÍAZ Eny. Análisis de metodologías para pruebas de penetración Mediante Ethical hacking. Tesis de grado. Tesis de grado. Yopal. Universidad nacional abierta y a distancia 2018.Disponible_https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/27647/1/erdiazb.pdf

permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos.

- **Ley 1273 de 5 de enero de 2009 La ley 1273** del 5 de enero de 2009, fue creada para sancionar todos aquellos delitos que van en contra del buen uso de la información y aquellos que irrumpen con la propiedad privada, la idea de esta ley fue proteger a todas aquellas personas que cuentan con algún tipo de información financiera y personal. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

4.6. MARCO HISTÓRICO.

Desde hace algunos años la seguridad informática, va de la mano de las redes privadas de la empresa. Se tiene que Implementar controles seguros en los activos informáticos para evitar que personas ajenas tenga acceso a la información. Las pruebas de penetración (o “pen Testing”) son una activada para atacar y poner a prueba un sistema de informático para encontrar vulnerabilidades que un atacante podría encontrar. El objetivo primordial de las pruebas de penetración es determinar las vulnerabilidades de seguridad. También se usan para probar el cumplimiento de los sistemas de seguridad de una organización para saber si cumple con políticas de calidad para el manejo de la información.

A inicios de 1960 el incremento de los sistemas informáticos dados por la creciente popularidad de la comunicación telefónica trajo nuevas dificultades de seguridad, como ejemplo en 1965 diferentes expertos en seguridad informática realizaron una conferencia basada en seguridad de sistemas, en 1967 el ingeniero Willis ware utilizo por primera vez la palabra penetración para ilustrar un ataque contra las redes de datos. Se planteo como amanzana a las redes de datos por el ejército de estados unidos a finales de 19677, el departamento de defensa contrato a Willis ware para crear una entidad que estudiara la seguridad en las redes de datos, el estudio arrojo que la amenaza más tangible es por medio de las computadoras.

5. METODOLÓGIA

Esta monografía está encaminada a documentar una metodología para realizar, pruebas de pentesting relacionadas a las redes de datos, este documento tiene como base encontrar los mecanismos que se necesitan para garantizar la seguridad de la información, protegiendo la red de datos ante posibles vulnerabilidades que se encuentren.

5.1. **M**etodologías para realizar pentesting

Mediante el desarrollo e investigación de esta monografía se realizó un análisis comparativo de las metodologías para implementar pruebas de penetración, se contemplan las metodologías nombradas en el marco teórico.

Las metodologías elegidas permiten analizar las vulnerabilidades que se encuentran en las redes de datos, con pruebas controladas en las redes de datos para comprobar la seguridad de una red. Se establece un listado de las metodologías más comunes.

En el momento de elegir una metodología depende del ámbito y los objetivos planteados. Cada una de estas ayudas en diferentes ámbitos que son idóneos en determinados casos, Es importante decir que no se tiene una metodología mejor o peor que otra, sirven de guías que ayudan en diferentes puntos de un objetivo para la evaluación de seguridad Informática.

Se expone las cualidades y propiedades más relevantes de cada una de ellas, que sirven como fundamento para el planteamiento y hallazgo de una nueva metodología. Una cualidad fundamental de estas metodologías es la licencia con el que se han desarrollado, el cual permiten su implementación de manera libre.

Las metodologías que se estudian son las del marco metodológico la cuales son:

- OSSTMM
- ISSAF
- OWASP

Los criterios más significativos de cada una de las metodologías son los siguientes:

- **Alcance**: fija las pruebas a realizar. Esto depende de tipo de entidad profesionales y áreas donde se desarrollen.

- **Minuciosidad:** se tiene en cuenta la exactitud que logra cada una de las metodologías. El nivel de minuciosidad, que emplea cada una de las metodologías en la implementación de las diferentes pruebas, de intrusión.

- **Fases.** Las diferentes etapas que brindan los métodos a la hora de implementar el proyecto. Esta etapa es fundamental en el desarrollo de los objetivos del trabajo, dado que esto ayuda en la elaboración del diseño de la metodología, tomando las mejores experiencias que ellas exponen.

- **Ventajas.** Cada una de ellas brinda una serie de atributos que es fundamental describir. Esto ayuda a obtener una visión general de lo que brinda cada una, favoreciendo para la adquisición de las mejores actividades en el desarrollo de la nueva metodología.

- **Limitaciones**, no existe una metodología superior o inferior que otra. se señalan las ventajas de cada metodología y se expone sus restricciones.

4.1.1. OSSTMM: esta metodología es un estándar de referencia en el ámbito de testeo de seguridad. Dicha metodología es un estándar internacional que brinda al profesional una ayuda para el testeo de seguridad en cualquier ámbito ya sea desde, el exterior o interior.

Para realizar pruebas de seguridad exhaustivas. Permite que se realicen mediciones precisas de los niveles de seguridad en los niveles operacionales. Está constituida para ser coherente, como proyecto de código abierto brinda la posibilidad de que se le aporten ideas para implementar pruebas de seguridad más precisas y también da la posibilidad que sea de libre difusión de información.[16]

- **Alcance**: Está enfocada hacia cualquier tipo de entidad, independientemente del tipo de organización, volumen o, tecnología La metodología agrupa a cualquier ambiente donde se necesiten aspectos de seguridad informática.
- **Meticulosidad**. La metodología es muy minuciosa dado que su implementación tiene como objetivo encontrar las fallas de los sistemas de seguridad informática. que no representan por sí solos una amenaza, pero en grupo pueden ser fallos de seguridad de consideración.

- **Fases.** Esta segmentada en cuatro fases. Las cuales aportan diferentes etapas del desarrollo de seguridad informática, Las cuales son:

  - Fase de preparación.
  - Fase de interacción.
  - Fase de investigación.
  - Fase de intervención.

A continuación, se detallan las cuatro fases:

- ✓ **Fase de preparación.** Es donde se inicia la auditoria, para esto es fundamental entender los requerimientos, el alcance y las limitaciones de estos.

- ✓ **Fase de interacción** Esta fase es fundamental ya que es el corazón del pentesting, por lo que es fundamental conocer el alcance de los objetivos planteados.

- ✓ **Fase de investigación.** Esta etapa desarrolla las pruebas de pentesting, abarca gran parte de la metodología dado que manipula la información.

- ✓ **Fase de intervención.** Esta etapa la fase final del test de seguridad, afirmando que las pruebas no afecten a la información encontrada aquí no puede ser divulgada hasta que las otras fases se terminen.

- **Ventajas** Las ventajas resumidas de esta metodología son:

  - Es una metodología que brinda la posibilidad de escalabilidad, dado que maneja una metodología revisable. abierta, y pública.

  - Es una metodología competente dado que su implementación de test de intrusión se puede desarrollar sin importar la dimensión de la organización,

  - La metodología muestra las tareas a realizar desde una perspectiva de alto nivel, pero de forma independiente a la tecnología utilizadas

- **Limitaciones** Los siguientes son las restricciones que se pueden evidenciar de la metodología:

- La metodología no aconseja herramientas, es necesario que el encargado de realizar las pruebas de pentesting trabaje con las herramientas con las que tenga la experiencia

- Se fundamenta mucho en la inventiva y experiencia del profesional, dado esto no es fácil la implementación de esta metodología para novatos.

4.1.2. OWASP: Su enfoque es más para pruebas de penetración de caja negra. Es una entidad sin ánimo de lucro a nivel global con el objetivo de ayudar a mejorar la seguridad del software, su objetivo principal es que las organizaciones tengan importancia de la seguridad del software, la metodología brinda herramientas de software que se basan en los conocimientos sobre las aplicaciones, cuentan con un Top 10 mundial sobre los ataques informáticos más conocidos durante un año especifico. es un proyecto fundado en el 2001 el cual fue creado por la fundación OWASP, lucha contra el software inseguro

- **Alcance.** La metodología trabaja en el ambiente de aplicaciones Web de las entidades, mediante pruebas de intrusión centradas en la fase de vida de la implementación del desarrollo de software en las etapas de producción y pruebas para obtener código de programación confiables y seguro,

- **Meticulosidad** El planteamiento de la metodología es minucioso en el entorno de las actividades de pentesting de portales Web, en todos los estudios necesarios para el testeo de diversas aplicaciones

- **Fases** OWASP, detalla cómo Desarrollar la verificación de cada una de las vulnerabilidades. La metodología está distribuida en tres pilares los cuales son el modo pasivo, modo activo y el desarrollo de un informe final.

- **Modo pasivo**: implementa las pruebas que determinan encontrar un entendimiento de la lógica del sistema y señalar cuales son los puntos de acceso a la misma.

- **Modo activo**: Esta fase es la más trascendental y minuciosa dado que interactúa con las aplicaciones Web. Está segmentada en 9 clases. Las cuales son:

  - ✓ **Recopilación de la información** obtiene la mayor cantidad de información que pueda ser posible de la aplicación que es motivo de estudio Existen varias maneras, como el uso de herramientas de escaneo público, envío de peticiones HTTP.

  - ✓ **Pruebas de Autenticación** es el medio donde se verifica la originalidad del emisor para tal fin se utiliza cuentas de usuario predeterminadas, saltarse sistemas de autenticación, fuerza bruta, es fundamental la comprensión de cómo funcionan procesos de autenticación para realizar las pruebas nombradas anteriormente.

  - ✓ **Pruebas de gestión de sesiones:** gran parte de entornos web tienen rutinas para el manejo de sesiones, en común es fundamental la emisión de algún control de rutina para autenticación de testigo.

  - ✓ **Pruebas de Autorización** hace alusión a las concesiones que se debe tener para tener permiso de acceso a los diferentes recursos con que se cuentan, solo a los usuarios que tengan permisos a ellos

    - ✓ **Pruebas de denegación de servicio**:

    denegación de servicios anulan diferentes recursos del sistema que es atacado y inhabilita el acceso a los usuarios que tiene permiso acceder a ellos.

    ✓ **Redacción de informes**: Cuando se termina la fase donde se realizan las pruebas pasivas y activas es fundamental la entrega de un informe. El informe, se tiene que evidenciar los riesgos más relevantes debe ser orientado al personal técnico y a la alta gerencia.

- **Ventajas**

  - Está orientado a la realización de ejemplos con herramientas que son claras con un buen fundamento que facilita demasiado la utilización en las áreas de aplicaciones web, los cuales permiten la orientación al momento de realizar la tarea de pentesting

  - comprende perfectamente las amenazas más usuales en los entornos Web, un ejemplo claro es que referencia Clara es el l TOP-TEN de las amenazas de las aplicaciones web

- **Limitaciones**

  - La implementación de las pruebas se basa únicamente en los portales Web, de forma que debe agregar por parte de otra metodología para abarcar lo relacionado a las redes de datos y de los sistemas que sostienes los Portales Web.

16. JENIFFER Rizzo propuesta de un modelo estándar de seguridad aplicando Métodos de Testing & Ethical hacking [en línea] tesis de grado pontificia universidad católica del ecuador .2013 disponible http://repositorio.puce.edu.ec/bitstream/handle/22000/11352/tesis-puce-%20rizzo%20raza%20jeniffer.pdf?sequence=1&isallowed=y

4.1.3. **ISSAF** metodología que está estructurada para ayudar a detallar el análisis de seguridad en diferentes dominios que son específicos de las actividades de seguridad informática. Su principal objetivo es brindar procedimientos que permite la autenticación de los sistemas de información que están en un entorno real. La metodología está desarrollada por la OISSG. La cual permite clasificar toda la información de las evaluaciones de seguridad en diversos dominios utilizando diferentes criterios de pruebas.

Esta metodología se encuentra principalmente enfocada en cubrir los procesos de seguridad y la evaluación de estos para así obtener un panorama completo de las vulnerabilidades existentes. Permite el desarrollo de matriz de riesgo para verificar la efectividad en la implementación de controles

- **Alcance** cubre el análisis de la seguridad en diferentes aspectos de cualquier entidad independiente del tamaño de su red de datos.

- **Meticulosidad**. Esta metodología esta detallada demasiado, dado que los aspectos de evaluación reúnen diversos dominios, que van desde los muy generales hasta muy específicos.

- **fases**

  - Fase I: Planificación
  - Fase II: Evaluación
  - Fase III: Presentación de informes

Fase I: Planificación Se delimitan de los objetivos, y responsabilidades, para crear un documento legal donde se aclare y especifique los plazos, alcance, enfoque y límites.

Fase II: Evaluación. Esta fase es donde se implementa los test de intrusión. Se realiza mediante enfoques que están encaminado a las diferentes capas del sistema, para obtener acceso a niveles a los cuales no se tiene permiso por los administradores del sistema Esta fase está dividida en 9 pasos.

- ✓ Recolección de información
- ✓ Sondeo de la red

- ✓ Identificación de vulnerabilidades
- ✓ Intrusión
- ✓ Ganar acceso y escalonado de privilegios
- ✓ Enumeración extra o adicional
- ✓ Comprometer usuarios y sitios remotos
- ✓ Mantenimiento del acceso
- ✓ Cubrir las huellas

FASE III: Informe En la última fase de la metodología está conformada por el desarrollo de dos informes los cuales son:

- ✓ • Informe oral, solo si se consigue encontrar una vulnerabilidad critica. Esta deber ser Expuesta de inmediato para que la entidad tenga conocimiento de ella.

- ✓ • Un informe final que es presentado por escrito, cuando las pruebas que fueron definidas en el alcance fueron terminadas, donde se muestran los resultados que se encuentran y las conclusiones con las recomendaciones para futuras mejoras.

- **Ventajas** La metodología aporta las siguientes ventajas:

➢ El planteamiento que expone parte de cero, mostrando diferentes compendios de conocimientos brinda la libertad y neutralidad de la información actual en el mercado.

➢ Muy utilizada ya que tienen, pasos muy explicados y que son lineales en la fase de evaluación. Lo cual brinda la facilidad de implementarlos. Es una metodología muy detallada lo cual ayuda a profesionales que no tienen tanta experiencia-

.

- **Limitaciones**

.

➢ La metodología brinda herramientas específicas de la evaluación. Esto hace que dependa de las herramientas y de tecnología existente en el mercado

➢ la metodología está en continua actualización de sus herramientas tecnológicas pero la metodología no se ha modernizado desde el año 2006, lo que puede dar puntos de vista obsoletos de la metodología

Las metodologías para encontrar vulnerabilidades en las redes de datos, tienen similitud en algunas fases o pasos, las diferencias entre unas y otras se establecen en las formas de intervención, los criterios y requerimientos, teniendo en cuenta los conceptos que cada una ofrece, a continuación, se realiza una comparación de las 3 metodología que se exponen en el marco metodológico. Ver tabla 1.

ASPECTOS	ISSAF	OSSTMM	OWASP
Permite realizar pruebas y análisis de seguridad	Si	Si	Si
Establece requisitos previos para la evaluación	Si	No	Si
La metodología define un proceso detallado para la realización de pruebas	Si	Si	Si
Define áreas de alcance	Si	No	Si
Contiene plantillas para realizar las pruebas	Si	Si	Si
Detalla técnicas para cada prueba	Si	No	Si
Contiene ejemplos de pruebas y resultados	Si	No	Si
Recomienda herramientas para cada prueba	Si	No	Si
Presenta procesos de análisis y evaluación de riesgos	Si	Si	Si
Define dimensiones de seguridad a evaluar	No	Si	Si
Establece valores o niveles de evaluación de riesgos	Si	Si	Si
Enumera y clasifica las vulnerabilidades encontradas	Si	No	Si
Realiza estimación de impacto	Si	Si	Si
Genera reportes e informes	Si	No	Si

Tabla 1 Metodologías
Fuente. Propia del Autor

Las metodologías planteadas en la tabla 1. Para el desarrollo de pruebas de pentesting cubren lo relacionado a la realización de un test de intrusión (pentesting) desde las etapas iníciales, hasta la recolección de la información y etapas de modelado. Para poder tener una mejor visión de la entidad que será estudia. Mediante la investigación de vulnerabilidades, explotación e informe, la habilidad técnica del personal que realice las pruebas de intrusión es fundamental conjuntamente con el compromiso que se adquiere con la entidad y por último se plantea un informe donde se agrupa el proceso desarrollado.

5.2. Metodología para encontrar fallas y vulnerabilidades

Después de haber analizados las diferentes metodologías, se desea diseñar una metodología, que sea útil y de fácil entendimiento, Que este orientada a los profesionales que no tienen mucha experiencia a la hora de implementar pruebas de pentesting, con lo cual se aporta un punto de vista resumido y practico.

En esta etapa se evidencia las cualidades que se desea obtener en el planteamiento de la metodología, estructurándola de la misma forma que las metodologías OSSTMM, ISAFF y OWASP y con esto poder tener una visión que sirva de modelo de comparación.

5.2.1. Alcance: se desea cubrir con la metodología que abarque los entornos de cualquier entidad desarrollado en los ambientes tecnológicos a los sistemas informáticos, infraestructura de redes inalámbricas como cableadas, ambientes de entorno web y bases de datos

5.2.2. Meticulosidad. con el desarrollo de la metodología a estudiar brindara una visión muy general de las pruebas de pentesting.

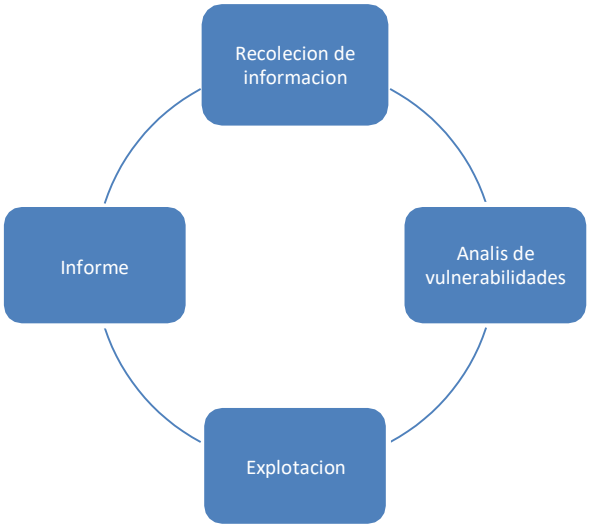
5.2.3. Fases Se expone de manera genérica las fases de intrusión que se implementan en las pruebas de pentesting, se tiene como referencia las fases de las metodologías que fueron estudiadas

Este proyecto según el objetivo principal planteado está orientado a diseñar una propuesta metodológica que permita realizar pruebas de pentesting en entidades ya sea pública o privada.

Se adopta alguna característica como base de la metodología OSSTMM. Para el presente trabajo de acuerdo a sus características a fines, para el desarrollo de los objetivos planteados, como lo son,

una documentación que agrupa los resultados y una serie de pasos que sirven de guía. Como proyecto de código abierto brinda la posibilidad de que se le aporten ideas para implementar pruebas de seguridad más precisas y también da la posibilidad que sea de libre difusión de información En la figura 1. Se planteas los pasos que se eligieron para el desarrollo de la metodología.

Figura 2 Metodología planteada



Fuente: Autor del Documento

5.2.3.1. **Recolección de información.** La realización de esta fase tiene como objetivo agrupar la mayor cantidad de información que sea posible de los sistemas donde realizaran las pruebas de penetración, esta fase es primordial para el desarrollo con éxito de las siguientes fases, dado que un estudio profundo del entorno, brinda la posibilidad de un mejor conocimiento y valoración de la situación actual. Con la recolección de la información, diferentes ataques se efectúan en las empresas. Este proceso radica en acumular información, el atacante usa diferentes métodos para tal fin como son recolectar direcciones IP, nombres de dominio, sistemas operativos etc.

la fase de recopilación de la información se divide en 2 etapas, el primero destinado a encontrar la información pública del objetivo que se desea auditar a esto se le conoce como (footprinting) y la segunda parte es recolectar información muy concreta de los elementos que constituyen la red a esto se le llama (fingerprinting)

(Footprinting): Con la ayuda del Internet se puede obtener información pública sobre el objetivo que se desea estudiar. Para esto se implementan técnicas que están basadas DNS, whois etc., las cuales ayudan a encontrar bases de datos que son públicas y con esto conseguir datos de dominios o direcciones Ip, para la implementación de esta de la fase se implementan algunas técnicas como lo son:

- Técnicas avanzadas en buscadores (Google, Bing),

- Paginas especializadas (www.kartoo.org, www.goolag.org, www.netcraft.com) donde se encuentra la información servidores DNS y dominios encontrada en los buscadores.

- Software para encontrar los metadatos de los archivos de los sitios Web, FTP, etc. Existen herramientas de automatización para estas tareas como (Anubis o foca)

(Fingerprinting) se desea encontrar que sistemas están operativos, mediante el escaneo de puertos para detectar que sistema que versiones cuenta, se puede con esto determinar qué servicios son ejecutados. Las herramientas con las que se logra la detección y captura de información pueden ser (nmap, netcat, hping, traceroute).

mediante el envío de paquetes ICMP método se puede encontrar si el host está activo, . también se hace uso de herramientas que escanean puertos que se implementan para la detección de puertos de un sistema y con esto encontrar los servicios que están conectados. Con esto se puede encontrar si un puerto está abierto o cerrado.

5.2.3.2. **Análisis de vulnerabilidades.** El estudio de vulnerabilidades es el paso siguiente. Cuando se ha recopilado la información que es posible, se implementa técnicas diferentes en función de encontrar los objetivos de las pruebas de pentesting. Utilizando software analizador que estén actualizados, se puede realizar el escaneo para encontrar diferentes vulnerabilidades, las cuales se pueden clasificar de acuerdo a parámetros que han desarrollado estándares internacionales, rangos de criticidad tales como alta, media y bajas

Se enumera las vulnerabilidades que son conocidas, implementando herramientas que son automáticos, las cuales permiten identificar las vulnerabilidades que presentan las redes de datos, los elementos de detección de vulnerabilidades pueden ser (OpenVas, Nessus. Saint, GFI Languard, Saint, WatchFire, hackvertor, Nikto, WFuzz), Dichos software tienen que verificar la información que tiene los diferentes protocolos que están en la estructura del modelo OSI,

las posibles vulnerabilidades a partir de la información que estas recopilan, tal actividad tiene como meta la identificación de vulnerabilidades como pueden ser.

- Incorrecto rendimiento en el uso de las políticas de seguridad.
- Listas de control de acceso, mal configurados
- contraseñas, perfiles débiles o por defecto.
- Configuraciones por defecto y errores de configuración
- Falta actualizaciones de seguridad e instalación de parches

Las herramientas detectan vulnerabilidades que son conocidas, que son publicadas en base de datos públicas con anterioridad. Es fundamental entender el funcionamiento del escáner de vulnerabilidades.

con el inventario de la información recopilada mediante herramientas de escaneo, se debe enumerar las vulnerabilidades para planificar correctamente la manera en que pueden ser explotadas. Logrando una correlación entre las vulnerabilidades encontradas y la etapa de comprobación de vulnerabilidades en la fase de explotación.

La información que se puede recopilar en esta fase es encontrar las vulnerabilidades de lo siguiente:

- accesos de modo remoto.
- elementos de la red de comunicaciones cableada (switcher, router) e inalámbrica (PA WiFi).
- estaciones de trabajo y servidores.
- en sistemas de gestión de bases de datos.
- aplicaciones de ámbito local o ámbito Web, ya sea en Intranet o en Internet (Web, correo, telnet, ftp, SSH, https, etc.).

5.2.3.3. Explotación de vulnerabilidades.

La explotación que se ejecutan en las vulnerabilidades, está dado por las herramientas que se presentan y tiene que ver mucho de los procedimientos a la hora de efectuar las explotaciones, dado eso las vulnerabilidades que se hallan documentadas en la página de exploit – db.com, se podrá detallar los script, o la manera de realizar explotaciones.

Es importante mencionar, si no se encuentra reportado en las bases de datos de la herramienta exploit, no es criterio que determine que el riesgo es bajo frente a reporte realizado por el escáner de vulnerabilidades. Es importante que el administrador tenga encuentra la criticidad para ejecutar las modificaciones o actualizaciones correspondiente.

De manera general esta fase se trata de explotar la vulnerabilidad que se encuentran, logrando la intrusión en los sistemas donde se encuentran las vulnerabilidades, cuando se logra la consolidación se debe tener la evidencia de que existe la vulnerabilidad para mejorar los privilegios y realizar los correctivos necesarios. se muestra en el impacto que puede generar cada uno de los ataques que son simulados para obtener una visión de un ataque en un entorno real por parte de personas inescrupulosas. Se debe tomar medidas de prevención para evitar las instrucciones a los sistemas y dispositos de red para tener confidencialidad de la información sensible y proteger la integridad de los sistemas auditados

El desarrollo de las explotaciones de vulnerabilidades, se implementan diferentes técnicas. Las técnicas son implementadas de manera habitual por los atacantes que son reales para lograr el acceso a sistemas. Para las vulnerabilidades se pueden utilizar exploit, el cual utiliza su código de comando el cual permite causar un comportamiento el cual no es deseado. Otras técnicas que se pueden utilizar son

- Secuestro de sesiones.
- Explotación con inyección de secuencias de datos sobre entradas que no están correctamente validadas, tales como SQL Inyection,
- Explotación de vulnerabilidades clásicas en sitios Web, Cross-Site Scripting, HTTP Response Splitting, Cross-Site Request Forgery, etc
- Ataques de fuerza bruta o de diccionario sobre los servicios
- Explotación de los mecanismos de cifrado de la red Wi-Fi y posterior captura del tráfico de los sistemas de usuario conectados a la red.
- Desbordamientos de buffer, desbordamiento de memoria dinámica,

Format String.

- Ataques de fuerza bruta o de diccionario sobre los servicios y los mecanismos de autenticación para acceder a sistemas objetivos.

Para borrar las huellas del acceso para no ser detectado del ataque por parte de los administradores se debe eliminar los logs o cualquier evidencia que pueda exponer la intrusión, esto se puede hacer mediante el uso de rootkit o diferentes herramientas las cuales permiten borrar el contenido de las evidencias de las acciones realizadas

5.2.3.4. **Informe.** Las pruebas que se implemente, se tiene que archivar y documentar, esto es importante para tener un lineamiento y establecer un documento el cual contiene la información de lo implementado en las pruebas realizadas Este informe tiene que ser establecido previamente por la entidad o el encargado de la seguridad informática,

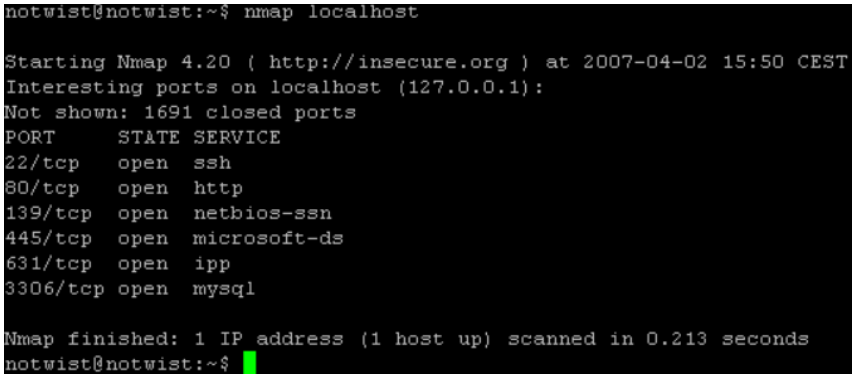
NOTA esta etapa no será desarrollada en la metodología y su manipulación es de tipo puramente informativo.

5.3. HERRAMIENTAS TECNOLÓGICAS.

Con la ayuda de herramientas tecnológicas se ha podido transformar la manera en que trabajamos en las áreas de la informatica, lo síguete son algunas herramientas que se usas para realizar actividades de pentesting

- **Nmap**: Se usa para escanear en red. Puede encontrar dispositivos finales de redes conectadas, sus puertos abiertos, ejecutar servicios y puede construir un mapa de red. También se pueden encontrar versiones de sistemas operativos, servicios y demonios en ejecución. Esta información se puede usar en combinación con vulnerabilidades bien conocidas que se encuentran en bases de datos de acceso público.

Figura 3 Terminal de Nmap



Fuente: Propia del autor

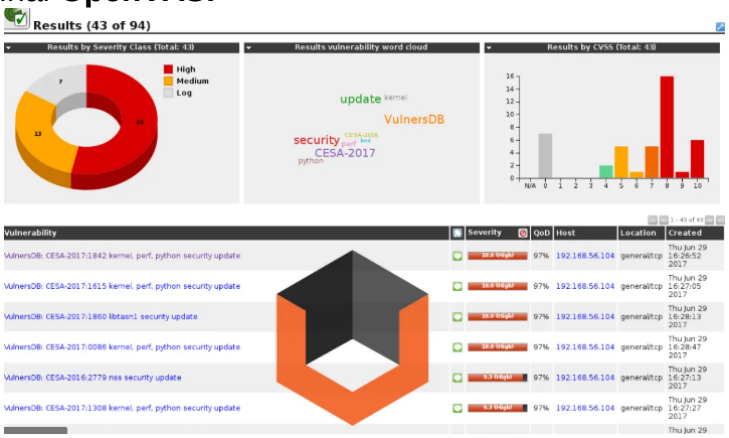
- **Metasploit Framework**: Es un proyecto de código abierto que proporciona la infraestructura, el contenido y las herramientas para realizar pruebas de penetración y una amplia auditoría de seguridad. Consta de múltiples componentes que trabajan en conjunto para proporcionarle una herramienta completa de prueba de penetración.

Figura 4 Terminal **Metasploit**

Fuente Propia del autor

- **OpenVAS:** Es un marco que contiene varios servicios y herramientas forjadas de Nessus, funciona en Linux y Microsoft Windows. Utiliza varios escáneres para descubrir vulnerabilidades en servidores desde una máquina cliente.

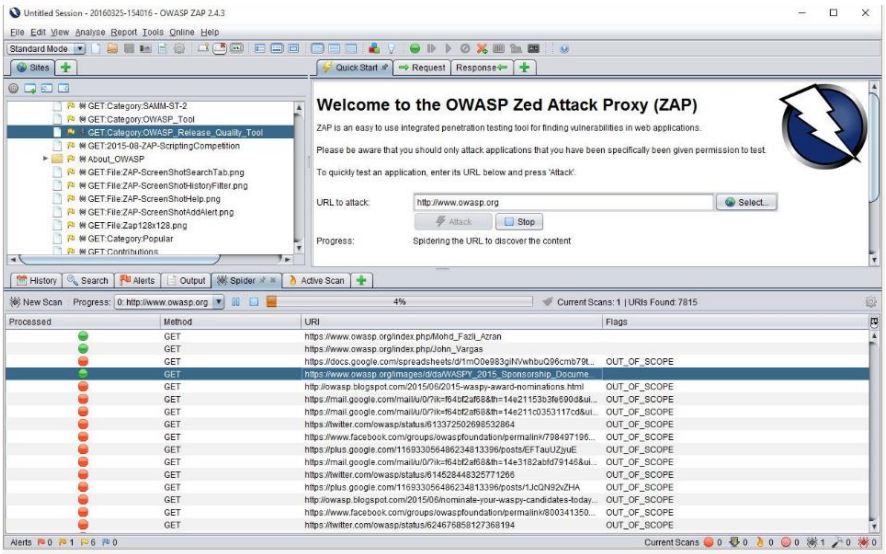
Figura 5 Terminal **OpenVAS:**



Fuente: Terminal de Openvas

- **Owasp Zap:** Es una herramienta gratuita de análisis dinámico de vulnerabilidades. Forma parte del grupo de proyectos de la fundación OWASP y es ampliamente utilizado alrededor del mundo. Ofrece gran cantidad de documentación y soporte además permite realizar distintos tipos de análisis y ataques, permitiendo configurar perfiles específicos para ajustarlos a las características de las aplicaciones.

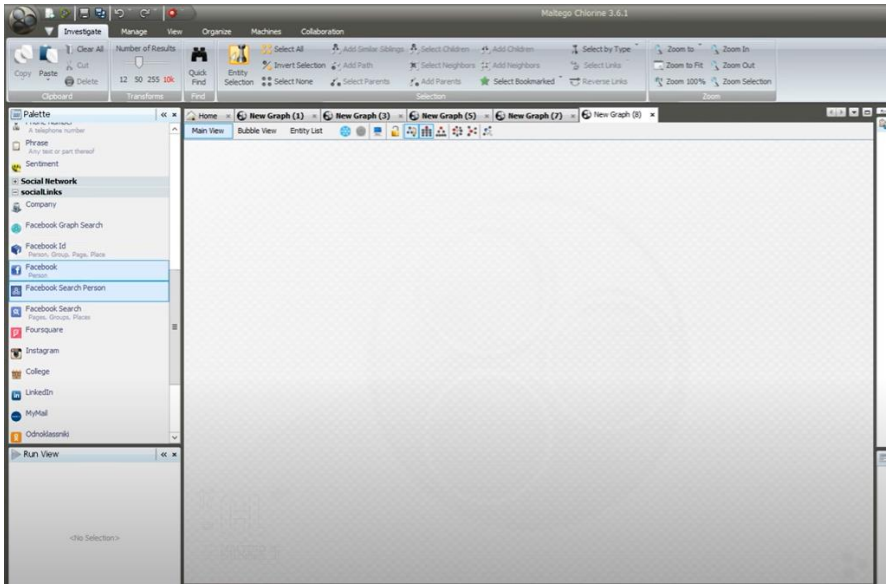
Figura 6 Terminal Owasp Zap



Fuente: Terminal Owasp Zap

- **Maltego**: Es una herramienta de tipo OSINT (inteligencia de fuente abierta), que representa un grupo de herramientas que utilizan fuentes de información disponibles públicamente. La herramienta usa listas de índices y bases de datos para buscar información relevante.

Figura 7 Terminal Maltego



Fuente: Terminal de Maltego

5.4. CERTIFICACIONES EN LAS REDES DE DATOS

para prevenir ataques de ciberseguridad es fundamental prevenir los ingresos no autorizados a las instalaciones donde se almacena o manipula la información, entre otras medidas, se debe tener una red de datos que tenga las normas y estándares internacionales de dispositivos de control donde se encuentre la red de datos dato. Se puede presentar las amenazas internas por parte de personal no autorizado también se debe proteger el cableado y los equipos que provoquen un ataque de la disponibilidad del servicio. La importancia del buen funcionamiento en una red de datos es fundamental para la administración de la información en las entidades, dado esto la infraestructura tecnológica es la responsable de la operatividad de los sistemas corporativos, es fundamental que se contemple, que la infraestructura este certificada por sus respectivas normas o regulaciones.

El resguardo de la infraestructura de las redes de datos se puede realizar mediante estándares, protocolos y leyes que ayudan a certificarla. Las cuales son implementadas para mitigar los posibles riesgos a la información almacenada en la infraestructura de datos.

La seguridad de la información abarca bases de datos, software, hardware, archivos y todo lo que una organización valore y sea un riesgo si está al alcance de otras personas, este tipo de información son conocidos como información confidencial y privilegiada.

Los requisitos de seguridad en los ambientes de redes de datos deben de implementar los diseños de las certificaciones de calidad, los cuales deben de ser considerados a la hora ponerlos en funcionamiento siguiendo lo establecidos para una óptima operación. Las entidades pueden tener amezas de la información ya sea de forma externa o interna de tal manera que si no se sigue los lineamientos adecuados se puede tener las siguientes vulnerabilidades.

- Integridad de los datos
- Suplantación o Robo de identidad
- Acceso o Borrado de información no autorizado
- Acceso a la Red no autoriza

Con esto se considera el importante desempeño que están jugando las redes de datos actualmente, por lo que se debe realizar constantes estudios en este campo con el fin de prevenir o corregir los problemas que cada vez son más frecuentes; ya que el diseño de una red de datos es uno de los factores más importantes a la hora de implementarlos en la infraestructura de las redes de telecomunicaciones.

Teniendo en cuenta la importancia que la red de datos cumpla con los estándares y normas para el buen funcionamiento de los elementos se debe realizar una inspección bajo los siguientes estándares de calidad.

5.4.1. Organismos:

- **ANSI:** American National Standards Institute. Organización Privada sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización voluntaria del sector privado de los Estados Unidos.

- **EIA:** Electronics Industry Association. Fundada en 1924. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los

componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.

- **TIA**: Telecomunicaciones Industria Association. Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.

- **ISO:** International Standards Organization. Organización no gubernamental creada en 1947 a nivel Mundial, de cuerpos de normas nacionales, con más de 140 países.

- **IEEE**: Instituto de Ingenieros Eléctricos y de Electrónica. Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet,802.5 Token Ring, ATM y las normas de Gigabit Ethernet.

5.4.2. Estándares:

- **ANSI/TIA/EIA-568**: Cableado de Telecomunicaciones en Edificios Comerciales, esta norma y sus recientes actualizaciones definen los requerimientos de un sistema de cableado estructurado, independiente de las aplicaciones y de los proveedores.

- **ANSI/TIA/EIA-569: Cuartos** de Telecomunicaciones en Edificios Comerciales. Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales.

- **ANSI/TIA/EIA-607**: Sistemas de tierra y aterramientos para los sistemas de telecomunicaciones en edificios comerciales.

- **ANSI/TIA/EIA-606-A:** Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales

- **ANSI/TIA/EIA-607**: Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales

- **ANSI/TIA/EIA-758:** Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

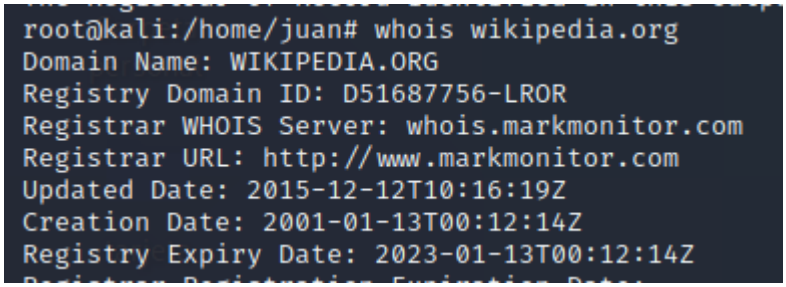
5.5. IMPLEMENTACION HERRAMIENTAS TECNOLOGICAS.

Se realiza un ejemplo práctico de las herramientas tecnológicas enfocadas escenario de la metodología planteada

5.5.1. Recolección de Información. Esta fase toma tiempo. ya que se agrupa la información que es posible adquirir, que más adelante será implementada a lo largo de las otras fases. La información que se desea obtener son direcciones IP, topologías de red, información de empleados etc., se tiene que decir que la información que se desea obtener depende de los objetivos que se han trazado. Implementando herramientas tecnológicas se puede obtener información como se muestra a continuación:

Whois: intenta agrupar la mayor cantidad de información posible acera de un objetivo, la forma correcta de implementar la herramienta es utilizando la terminal de Kali Linux, la información que se obtiene, se puede ver cuando fue creado el dominio, cuando es su fecha de expiración, quien es el operador del dominio, como ejemplo se usa la URL de Wikipedia.org. ver figura 8.

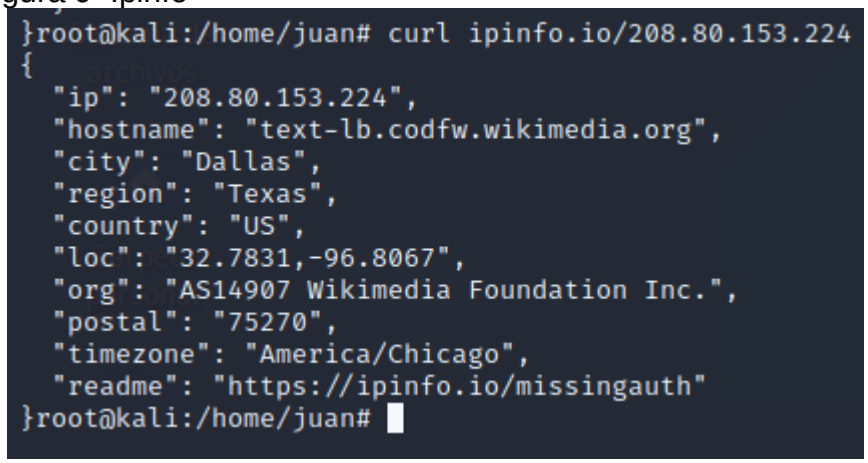
Figura 8. **Test Whois**



Fuente. Propia del autor

Ipinfo: permite obtener información mediante consola con la ayuda del comando curl ipinfo.io el cual arroja información de la localización con coordenadas geográficas. ver figura 9.

Figura 9 Ipinfo



Fuente. Propia del autor

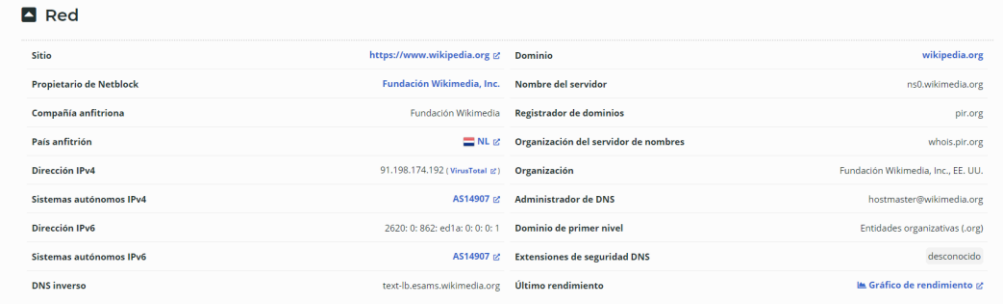
Netcraft. Es una herramienta pública que permite analizar rápidamente servidores y subdominios para identificar qué versiones de sistemas están utilizando y así identificar vulnerabilidades. ver figura 10.

La información que nos arroja, el título de la página, fecha de la primera vista, lenguaje en que está escrito y una descripción de la página, también muestra descripción de red de la página. Ver figura 10 y 11.

Figura 10 Descripción Netcraft

Fuente. Propia del autor

Figura 11. Descripción de red



Fuente. Propia del autor

Tracert: El comando Tracert, ayuda determinar los diferentes saltos que necesita para llegar a el objetivo final, con esto se puede determinar si atraviesa por un firewall, para esto existen herramientas en Windows que permiten detallar todos los saltos, antes de llegar al objetivo. Ver figura 12.

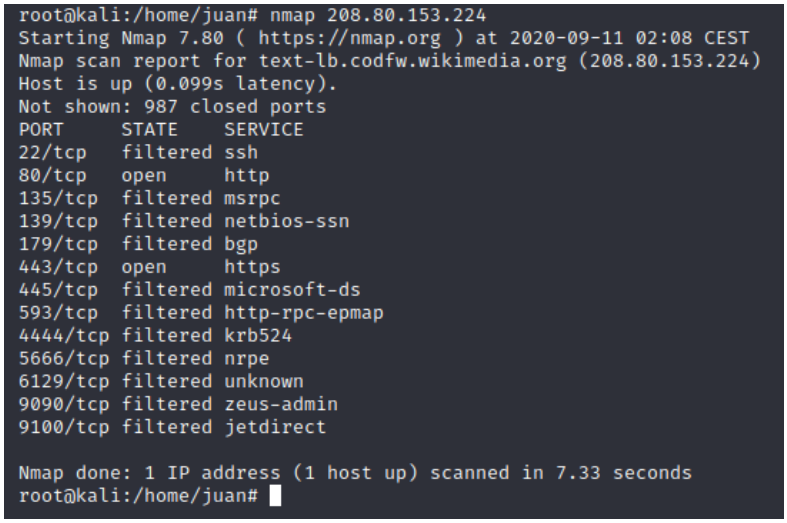
Figura 12. Comando Tracert

Fuente. Propia del autor.

5.5.2. Análisis de vulnerabilidad Teniendo la información obtenida con anterioridad se busca vulnerabilidades. Se realiza escaneo de los diferentes puertos.

Lo cual permite encontrar vulnerabilidades que sirven como parámetros de ataque. Se desarrolla el escaneo de los puertos con Nmap, el cual permite detallar los puertos que están asociado por el servidor, para este fin se implementa una prueba en la página de www.wikipedia.org en el cual pose algunos puertos abiertos. Ver figura 13.

Figura 13. NMAP



Fuente. Propia del autor

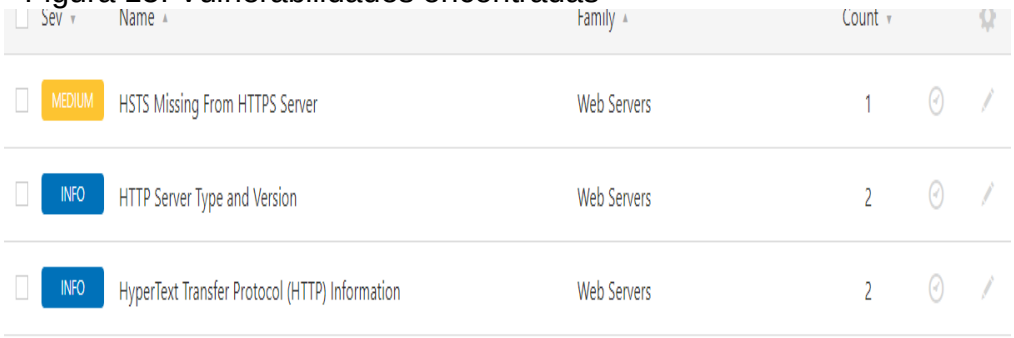
Nessus Utilizando analizadores de vulnerabilidad, los cuales están actualizados, se escanea algún tipo de vulnerabilidad en ip 208.80.153.224 el cual corresponde a el dominio Wikipedia.org de la en la figura 9 se evidencias las vulnerabilidades encontradas.

Figura 14. Escaneo de vulnerabilidades.

Fuente. Propia del autor

La Figura 15 evidencia las vulnerabilidades más critica que reporta Nessus.

Figura 15. Vulnerabilidades encontradas



Fuente. Propia del autor

Se detalla en la figura 16, el escaneo de vulnerabilidades, permite encontrar fallos en servicios y sistemas operativos, como se puede ver en el puerto 443, logrando de esta forma enfocar un ataque a esta vulnerabilidad.

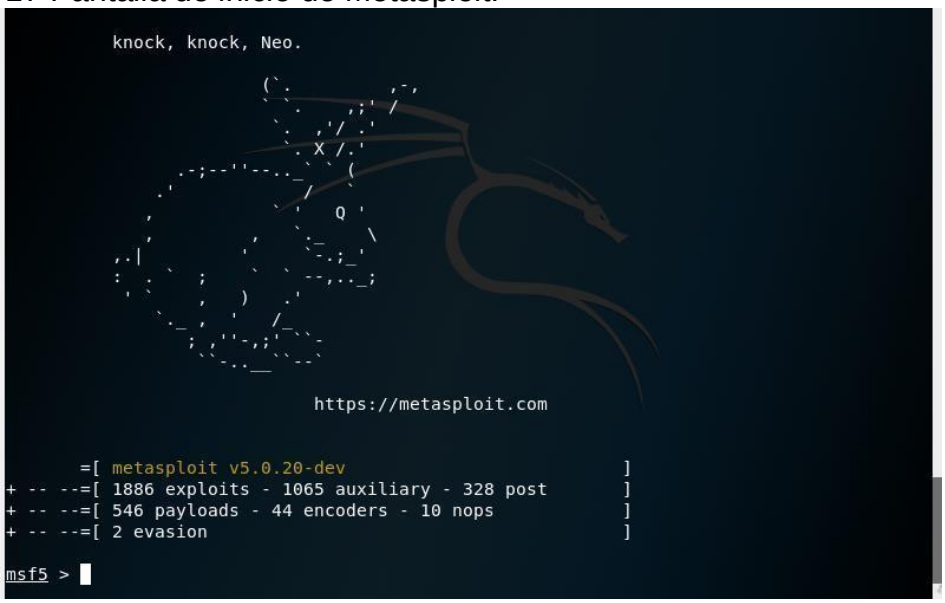
Figura 16 Fallos en servicios

Fuente: Propia del autor

5.5.3. Explotación de Vulnerabilidades. Cuando se encuentra los servicios y sus respectivas vulnerabilidades, lo siguiente es encontrar la explotación de la vulnerabilidad. Con esto se debe probar si dicha vulnerabilidad se puede realizar algún ataque significativo que presente una amenaza., se puede comprobar si funciona el ataque hacia la entidad. O la amenaza encontrada no representa un riesgo para la entidad.

Para tal objetivo Metasploit se utiliza como herramienta para implementar pruebas. Nessus tiene una información de vulnerabilidades, Metasploit tiene información de exploits que se pueden implementar y aprovechar. Con esto se puede detectar si se encuentra una vulnerabilidad en un host remoto, implementando un exploit que se ejecuta en la consola de comandos de kali Linux, digitando "**msfconsole**" el cual puede abrir la consola de Metasploit. Ver imagen 17.

Figura 17 Pantalla de inicio de Metasploit.



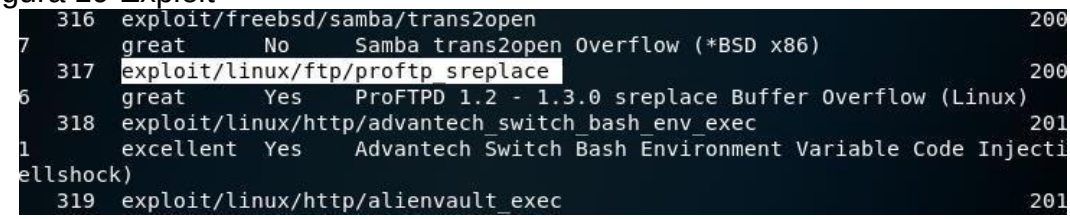
Fuente: Propia del autor

Implementado el comando "**search**" para encontrar una posible vulnerabilidad en el servicio Https que está en el puerto 443 como se pudo ver con análisis de vulnerabilidades con Nessus., el cual arroja diferentes Exploit que están disponibles. Ver figura 18 y 19

Figura 18 Comando Search

Fuente: Propia del autor

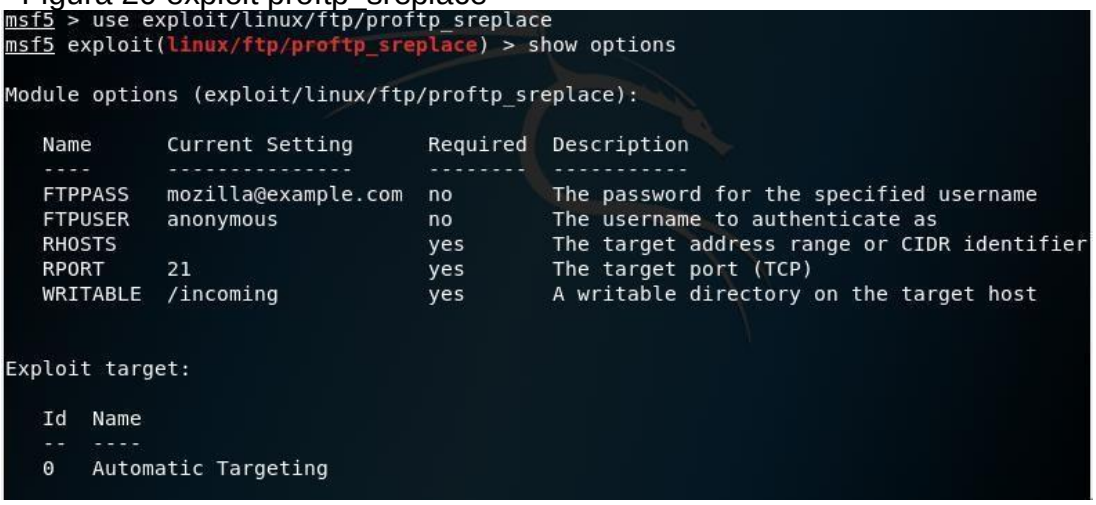
Figura 19 Exploit



Fuente: Fuente: Propia del autor

Con el comando "**use**" se implementa uno de los exploit el cual es el **proftp_sreplace.** Se puede detallar las opciones de configuración con el comando **show options,** donde arroja el comando **Rhost** se utiliza en la ip a la cual se quiere acceder en este caso **la IP** 208.80.153.224 la cual corresponde a la URL www.unad.edu.co. Ver figura 20.

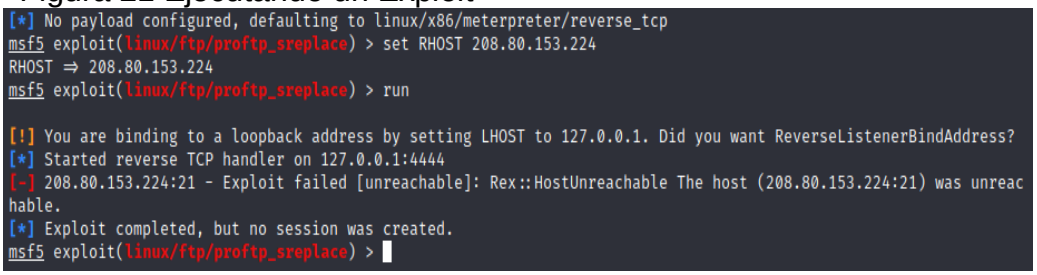
Figura 20 exploit proftp_sreplace



Fuente: Propia del autor

No necesariamente se tiene que acceder como se ve en la figura 21

Figura 21 Ejecutando un Exploit



Fuente: Imagen tomada de la terminal del sistema operativo Kali

5.5.4. Informe. En esta etapa se compone de la operación de las pruebas implementadas y del resultado que se tiene. Se implementa la documentación con base a los detalles que se lograron en las pruebas, este informe será el que obtenga el cliente el cual sirve como parámetros para tomar decisiones pertinentes

En los informes que se generan se basan en poder evidenciar la información que se recolecta durante el proceso de pentesting tal como lo recomienda la entidad de offensive-security desarrolladores de Kali Linux.

NOTA: no se tiene un alcance de informe debido a que solo se presenta una metodología para realizar pruebas de pentesting y no se presenta informes a ninguna entidad.

5.5.5. Desarrollo metodológico en Red datos.

Dado los lineamientos de la metodología de pentesting es fundamental realizar una prueba de la misma. Para validar su efectividad, esto se puede desarrollar mediante un prototipo con una escenario virtual o real que este orientado en las pruebas de pentesting. El trabajo no tiene como objetivo la construcción de un prototipo, esto puede ser para trabajos futuros de la implementación de la metodología, dado esto se especifica los elemento o requisitos mínimos que se tiene que tener a nivel de tecnología y arquitectura para el diseño del prototipo.

Con la ayuda del prototipo brindará los requisitos mínimos a nivel de tecnología actuales, esto permitirá la implementación del test de pentesting sobre las fases de la metodología planteada en un ambiente controlado de una red de datos. Los ámbitos a cubrir son los siguientes:

- Infraestructura de red
  - Entornos de red cableados: Router, Switcher
  - Elementos de seguridad: Firewall
  - Accesos remotos: VPN
  - Entornos inalámbricos: WIFI
  - Sistemas operativos.
  - Servicios de públicos de correo electrónico, FTP, HTTP, DNS.
  - Aplicaciones locales y servicios de Intranet

Simular la red de datos puede variar según la tecnología, Estos elementos se deben configurar de la forma más segura posible como lo es en un entorno real. Se diseña 4 zonas para el prototipo las cuales son: las conexiones a internet, zona de servidores, zona de DMZ y zona LAN con acceso a wifi. Los sistemas operativos se deben simular entornos de producción que sean reales con servicios o aplicaciones más implementadas, con una configuración que sea segura para que sea un entorno real,La escogencia de las unidades para la elaboración del prototipo será para un futuro desarrollo del diseño del trabajo actual

6. RESULTADOS Y DISCUSIÓN

La metodológica planteada está dividida en 4 etapas, cabe recalcar que

los procedimientos en cada etapa pueden variar dependiendo de lo que cada entidad necesite, esta puede ser usada por cualquier profesional en red de datos, se debe implementar actividades de escaneo, instrucciones, para lograr evaluar la seguridad de una red de datos y con esto determinar el funcionamiento correcto de las políticas de seguridad informática

Se puede detallar que es posible encontrar elementos fundamentales de información desde las etapas iníciales. Es fundamental tener en cuenta que, dentro del análisis, todas las redes de datos no son iguales y no se comportan de igual manera, dicho esto las metodologías varían los resultados, según lo que se desee y los escenarios que se estudien, pero como base se tiene las 4 etapas de la metodología planteada la cual sirve como un plan para la ejecución de pruebas de pentesting.

6.1. **ANÁLISIS DE RECOLECCIÓN DE INFORMACIÓN**.

Con la recolección de la información se logra un objetivo de la metodología planteada, dado que es la primera meta al realizar los diferentes tipos de pruebas que se basan en esta fase, con esto se puede establecer objetivos de ataques para determinar las etapas posteriores de la metodología, las herramientas tecnológicas que se implementan como whois, ayudan a realizar el respectivo reconocimiento de información. De igual forma las herramientas que permitieron el reconocimiento de búsqueda pasiva con aplicaciones de internet capaz de determinar información relevante

En la actualidad se encuentran diferentes ataques informáticos el cual pueden realizar debido a el desconocimiento de las personas que laboran en las empresas, como puede ser ataques de ingeniería social, donde el atacante suplanta identidades con información recolectada de internet.

6.2. ANÁLISIS DE VULNERABILIDADES.

Los ataques informáticos son una amenaza constante debido a que los delincuentes informáticos realizan fraudes, dado esto los administradores tienen que estar atentos a los reportes y todo el bug que se encuentran, para estar un paso delante del delincuente por tal motivo es que los analizadores de vulnerabilidades son fundamentales en las redes de datos.

Dado las vulnerabilidades que descubren o reportan a diario, es fundamental que se ejecuten actividades con frecuencia de escaneo de las redes para estudiar los dispositivos con los que se cuentan, para posteriormente realizar explotaciones y poder determinar cómo mitigarlas

6.3. **ANÁLISIS SOBRE EXPLOTACIÓN DE VULNERABILIDADES**.

La explotación que se ejecutan en las vulnerabilidades, está dada por las herramientas que se presentan y tiene que ver mucho de los procedimientos a la hora de efectuar las explotaciones, dado eso las vulnerabilidades que se hallan documentadas en la página de exploit – db.com, se podrá detallar los scripts, o la manera de realizar explotaciones.

Es importante mencionar que, si no se encuentra reportado en las bases de datos de la herramienta exploit, no es criterio que determine que el riesgo es bajo frente a reporte realizado por el escáner de vulnerabilidades. Es importante que el administrador tenga encuentra la criticidad para ejecutar las modificaciones o actualizaciones correspondiente

7. CONCLUSIONES

Gracias a el incremento de las redes de datos, se pretenden cada día buscar la manera de estar más protegidos, pero también los hackers maliciosos están actualizando sus métodos para encontrar las vulnerabilidades o debilidades.

Es necesario saber los conceptos técnicos, estándares y normas, que ayudan a aclarar las ideas de lo que se necesita para el correcto funcionamiento de una red de datos, estos permiten tener un criterio para que las redes datos cumpla con estándares de calidad.

La recopilación de la información permite brindar una mayor perspectiva de cómo se encuentra la red de datos y cuáles son sus principales carencias, este análisis constituye el punto de partida para proponer el posterior desarrollo de la metodología planteada.

Se debe analizar la situación actual de la red de datos de cualquier entidad para permitir brindar una mayor perspectiva de cómo se encuentra y cuáles son sus principales carencias, falencias y necesidades, así mismo permite contar con un documento actualizado, donde se caracterice su infraestructura, este análisis constituye el punto de partida para proponer el posterior método de protección.

Se determino la información puntual para el completo monitoreo de la red de datos para la realización de pruebas de pentesting para encontrar las vulnerabilidades. Las cuales ayudan a brindar más información a los empleados encargados de la seguridad, el funcionamiento de este servicio puede brindar soporte, en el momento en el que se presente algún acontecimiento, con el cual se podrá evidenciar y usar como prueba para alguna eventualidad del orden informático

Se resalta la importancia de tener profesionales actualizados, basada en las normas y estándares, lo cual pueda aportar a una certificación de la misma a futuro, aportando a su escalabilidad, garantizando su buen funcionamiento y rendimiento en las redes de datos corporativas.

Se permite con la realización de este trabajo, tener pautas para la elaboración de pruebas de pentesting de las redes de datos, permitiendo alcanzar competencias de consideración que más tarde podrán ser de beneficio cuando se requiera actualizar o/y plantear una red de datos

La realización de esta monografía permite tener pautas para la elaboración de pruebas de pentesting, permitiendo alcanzar competencias de consideración que más tarde podrán ser de beneficio para continuar en el estudio de este campo, en el cual pueda servir de soporte al momento que se requiera actualizar.

Es necesario saber los, estándares y normas, que ayudan a aclarar las ideas de lo que se necesita para el correcto diseño de una red de datos, los cuales se describen en la monografía, estos permiten tener un criterio para que las redes datos cumpla con estándares de calidad.

De acuerdo a los avances tecnológicos, se debe tener una actualización de los diferentes estándares y normas, ya que constantemente están sometidos a variaciones, evitando así tener estándares o normas descontinuados, sobre todo si se desea tener una red de datos certificada.

Contar con este documento ayuda a las entidades a tener medidas de seguridad por lo cual este estudio será de gran ayuda para minimizar los impactos generados por los códigos maliciosos o malware.

La metodología está diseñada para que cualquier administrador o dueño de una empresa, esté en la capacidad de poder saber que necesita para realizar pruebas de seguridad informática.

Se concluyó que los softwares que se utilizan en las pruebas de penetración en las redes de datos son de suma importancia, sin embargo, dichas herramientas de seguridad deben estar acompañada de excelentes conocimientos en los ambientes productivos, refiriéndonos no solo al software sino al hardware y configuración de la red como tal dentro de las empresas o donde se vayan a realizar las pruebas de penetración.

Mediante el análisis de metodologías de seguridad informática y la óptima utilización de técnicas de intrusión es posible diseñar una propuesta metodológica que ayude a ejecutar de forma satisfactoria procedimientos de prueba de Intrusión, en el cual se pudo agregar tecnologías de software de código abierto.

8. RECOMENDACIONES.

A la hora de implementar cualquier actividad se debe agrupar en actas el estado actual de la red de datos, esto para luego de desarrollar la metodología planteada se tenga una evidencia para hacer mediciones y detallar los cambios, esto permite que se tenga una práctica de mejoras continua.

Siempre las vulnerabilidades se continuarán presentando, por tal motivo es fundamental que los equipos este en constante actualización de sus sistemas para la identificación de nuevas vulnerabilidades con el objetivo de encontrar e implementar soluciones que sea necesarias

Se ha desarrollado una guía metodológica para las entidades que detalla los pasos para realizar pruebas de pentesting. Gracias a esto se debe brindar la lectura de esta monografía al grupo encargado de la seguridad de la información, de tal forma que se pueda encontrar estrategias para poner en marcha para la disminución de posibles vulnerabilidades que tenga la red de datos

Las posibles vulnerabilidades que se puedan encontrar en seguridad son bastantes complejas e identificarlas, para tal motivo el enfoque que es más eficiente para esto es asignar a profesionales expertos con excelentes herramientas para determinar esta tares, se aconseja que se tenga énfasis en que el personal que se encargue de las actividades relacionadas a la seguridad de la información este en contante capacitación en diferentes herramientas para encontrar vulnerabilidades

Es fundamental que en el momento del desarrollo de la metodología que se apropie todas las áreas de las organizaciones estén comprometidas y, guiadas por la alta gerencia, para estar enfocadas en la disminución de vulnerabilidades de penetración y proteger la red de datos contra posibles ataques.

9. REFERENCIAS

ALFONSO E. OTEO. Tipos de Ataques Informáticos.{en línea } {2014} Disponible en http://www.coreoneit.com/tipos-de-ataques-informaticos/

Ardita, J. C. Security_System.obtenido {en línea } {2014} D i s p o n i b l e http://www.cybsec.com

Arieta Gutiérrez Javier.” Medidas para aumentar la seguridad informática_en_el_centro_de_trabajo”_tomado de_{en línea } {2019} Disponible https://www.slideshare.net/mariorafaelquirozmartinez/medidas-para-aumentar-la- seguridad-informatica-en-su-centro-de-trabajo

Baloch, R. .Ethical hacking and penetration testing guide. Boca Raton: CRC Press. .{en línea } {2014} Disponible http://www.coreoneit.com/tipos-de-ataques-informaticos/

Borghello, C Seguridad de la Información. Obtenido de. .{en línea } {13 de Julio de 2014} Disponible.http://www.seguinfo.com.ar/proteccion/vulnerar.htm

BROAD, James y BINDER, Andrew. Hacking with kali, Practical Penetration Teniques. {en línea} {2017} Disponible http://www Waltham, Syngress, 2014, 223p.

BECHIMOL, Daniel. Hacking desde cero. Buenos Aires, Fox Andina, {en línea} {2018} Disponible http://www.seguinfo.com.ar/ataques/ataques.htm

CARRASCO, F vulnerabilidades de Seguridad. Obtenido de: CIO América Latina: {en línea}{2011}Disponible http://www.cioal.com/2011/06/30/90-de- las empresas- han-sido-victimas-de-vulnerabilidades-de-seguridad/

CRIATIAN BORGHELLO. Amenazas Lógicas – Tipos de ataques. Obtenido de:_{en_línea}{2011}Disponible_http://www.segu_info.com.ar/ataques/ataques.htm

CodigoVerde. Prueba de Penetración (Pentest). Obtenido de {en line }{2020}_Disoponible_http://codigoverde.com/consultoriaespecializada/

prueba-de- penetración-pentest/

David A. Franco, Jorge L Perea y Plinio Puello “Metodología para La Detección de Vulnerabilidades en Redes de Datos” {en linea }{2020}_Disponible https://scielo.conicyt.cl/pdf/infotec/v23n3/art14.pdf

DAVID FRANCO, JORGE L. PEREA & LUIS C. TOVAR. (2013). Herramientas_para_la_Detección_de_Vulnerabilidades_tomado_de: {en line }{2020}_Disponible_http://www.scielo.cl/scielo.php?pid=S071807642013000500003&script=sci_arttext

DAZA TRIANA, S. M., & GIRALDO MURILLO, M. A. Aplicación de un sistema de gestión de vulnerabilidades para la infraestructura {en linea {2020}_Disponible_http://repository.ean.edu.co/bitstream/10882/2590/1/DazaSan dra2012.

FRANCO, D. A., PEREA, J.L., & TOVAR, L. C. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. {en line{2020}_Disponible_de:http://www.scielo.cl/scielo.php?pid=S0718076420130005000 03&script=sci_arttext

FERNANDO CATORIRA (2012). Penetración Test, ¿En qué consiste?_ {en line {2020}_Disponible_:_http://www.welivesecurity.com/laes/2012/07/24/ppenetración-test-en- que consiste/

GONZALES, J. C. Vulnerabilidades de seguridad en las empresas Obtenido_de:_{enlinea}_{2020}_Disponible_http://eprints.uanl.mx/3567/1/VULNERABILIDADES_DE_SEGURIDAD_E N_LAS_EMPRESAS.pdf

HERRERA STEFANI D. Vulnerabilidad de los Sistemas Informáticos._Obtenido_de_{enlinea}_{2020}_Disponible_http://vulnerabilidadtisg.blogspot.com/

HOWARD, J. D. Analysis of security on the Internet 1989-1995. _{enlinea}_{2020}_Disponible, de http://www.cert.org

Huerta, A. V. Seguridad en Unix y Redes. Obtenido de: _{en línea}_{2020}_Disponible http://www.kriptopolis.com

MAURO MAULINI, Desarrollo y Seguridad de Aplicaciones web y Móviles_{enlínea}_{2020}_Disponible:http://tecnologiasweb.blogspot.com/2010/12/que-es-pen-testherramientas- de-pen.html

MIFSUD, E. MONOGRÁFICO: Introducción a la seguridad informática - Vulnerabilidades de un sistema informática. {en línea}_{2020}_Disponible de_http://recursostic.educacion.es/observatorio/web/es/component/content/art icle/1040introduc cion-a-la-seguridad-informatica?start=3

MYERSON, J. Servicios en la nube: mitigar riesgos, mantener la {en línea}_{2020}_Disponible_http://www.ibm.com/developerworks/ssa/cloud/library/clcloudservicerisks/

ROMERO, A. (Aspectos Básicos de la Seguridad en Aplicaciones Web.{en_línea}_{2020}_Disponible:http://www.seguridad.unam.mx/documento/?id=17

SEGURIDAD INFORMÁTICA. Seguridad Informatica (Ethical Hacksing, Pen-test,_Anti-Script_Kiddies)..{en_línea}_{2020}_Disponible http://antisecsecurity.blogspot.mx/2014/04/webpwn3r-webapps-security- scanner.html

SEGURIDAD INFORMÁTICA. Vulnerabilidades de un sistema Informático.Tomado_de_{en_línea}_{2020}_Disponible:http://descargas.pntic.mec.es/mentor/visitas/demo_SeguridadInformatica/ud1_introduccin_a_la_seguridad_informtica.html

SERRANO, M. Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala. tomado de Universidad Javeriana{en_línea}_{2020}_Disponible_http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

Toni Puig. Gestión de Riesgos de los Sistemas de Información. tomado{en_línea}_{2020}_Disponible:http://www.mailxmail.com/curso-gestion- riesgos- sistemas información/identificacion-vulnerabilidades-impactos

ANEXOS.

Documento RAE:

Fecha de Realización:	16/05/2020
Programa:	Especialización seguridad informática
Línea de Investigación:	Monografía
Título:	Pruebas de penetración en las redes de datos en cualquier entidad pública o privada
Autor(es):	Ferrer Bustos Juan Sebastián Ferrer
Palabras Claves:	Pentest, Hacker, Sistema de información, Metodología, Amenaza.
Descripción:	Trabajo de grado para optar al título de especialista en seguridad informática, que consta del desarrollo de una Monografía para el estudio de una metodología para la realización de pruebas de pentesting en cualquier entidad. Se describe la metodología que se desarrolla basada en la documentación, para realizar pruebas de pentesting. Los resultados que se encuentran con la terminación de la monografía es tener conocimientos condensados que sirvan como pautas para la solución de problemas de seguridad informática en las entidades públicas o privadas.

Fuentes bibliográficas destacadas:

David A. Franco, Jorge L Perea y Plinio Puello (2011) “Metodología para La Detección de Vulnerabilidades en Redes de Datos” Obtenido de: https://scielo.conicyt.cl/pdf/infotec/v23n3/art14.pdf

ALFONSO E. OTEO (2014). Tipos de Ataques Informáticos. Obtenido de: http://www.coreoneit.com/tipos-de-ataques-informaticos/

CARRASCO, F (2011) vulnerabilidades de Seguridad. Obtenido de: CIO América Latina: http://www.cioal.com/2011/06/30/90-de- las empresas-han-sido-victimas-de-vulnerabilidades-de-seguridad/

CRIATIAN BORGHELLO (2009). Amenazas Lógicas – Tipos de ataques.

<table>
<tr><td colspan="2">Obtenido de: http://www.segu-info.com.ar/ataques/ataques.htm

DAZA TRIANA, S. M., & GIRALDO MURILLO, M. A. (2012) Aplicación de un sistema de gestión de vulnerabilidades para la infraestructura Obtenido.de:http://repository.ean.edu.co/bitstream/10882/2590/1/DazaSandra2012.

FRANCO, D. A., PEREA, J.L., & TOVAR, L. C. (2013) Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios._Obtenido_de:http://www.scielo.cl/scielo.php?pid=S071807642013000500003&script=sci_arttext</td></tr>
<tr><td>Contenido del documento:</td><td>INTRODUCCIÓNError! Bookmark not defined.
1. DEFINICION DEL PROBLEMA
2. JUSTIFICACION
3. OBJETIVOS
4. MARCO REFERENCIA
4.1. MARCO TEÓRICO
4.2. MARCO CONCEPTUAL
4.3. ANTECEDENTES.
4.4. MARCO METODOLÓGICO
4.5. MARCO LEGAL
4.6. MARCO HISTÓRICO.
5. METODOLÓGIA
6. RESULTADOS Y DISCUSIÓN
7. CONCLUSIONES
8. RECOMENDACIONES.
9. REFERENCIAS</td></tr>
<tr><td>Conceptos adquiridos :</td><td>La realización de esta monografía permite tener pautas para la elaboración de pruebas de pentesting ,permitiendo alcanzar competencias de consideración que más tarde podrán ser de beneficio para continuar en el estudio de este campo, en el cual pueda servir de soporte al momento que se requiera actualizar.</td></tr>
</table>

	Es necesario saber los, estándares y normas, que ayudan a aclarar las ideas de lo que se necesita para el correcto diseño de una red de datos, los cuales se describen en la monografía, estos permiten tener un criterio para que las redes datos cumpla con estándares de calidad.
Conclusiones:	Mediante el análisis de metodologías de seguridad informática y la óptima utilización de técnicas de intrusión es posible diseñar una propuesta metodológica que ayude a ejecutar de forma satisfactoria procedimientos de prueba de Intrusión, en el cual se pudo agregar tecnologías de software de código abierto. Contar con este documento ayuda a las entidades a tener medidas de seguridad por lo cual este estudio será de gran ayuda para minimizar los impactos generados por los códigos maliciosos o malware. La recopilación de la información permite brindar una mayor perspectiva de cómo se encuentra la red de datos y cuáles son sus principales carencias, este análisis constituye el punto de partida para proponer el posterior desarrollo de la metodología planteada. Se resalta la importancia de tener profesionales actualizados, basada en las normas y estándares, lo cual pueda aportar a una certificación de la misma a futuro, aportando a su escalabilidad, garantizando su buen funcionamiento y rendimiento en las redes de datos corporativas.