METODOLOGIA PARA HACKING ETICO EN BASES DE DATOS

JUAN CARLOS MONROY SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

METODOLOGIA PARA HACKING ETICO EN BASES DE DATOS

JUAN CARLOS MONROY SALAZAR

Monografía presentada como requisito para optar
al título de Especialización en Seguridad Informática

Director Proyecto
ING. YENNY STELLA NÚÑEZ ALVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, D.C. 04/05/2020

DEDICATORIA

Este trabajo lo dedico en primer lugar al señor todopoderoso quién es el que me da la vida, los recursos, la sabiduría y la fuerzas para seguir adelante, a mi esposa, a mis hijos por su paciencia y a todos aquellos que me apoyaron para lograr el cumplimiento de este objetivo.

AGRADECIMIENTOS

Este trabajo cuenta con el apoyo de muchas personas y a las que agradezco de todo corazón entre quienes se encuentran el Ingeniero Edilberto Bermúdez Penagos, la Ingeniera Yenny Stella Núñez que me guio como directora del proyecto y quién con su paciencia en este proceso se pudo llevar a feliz término esta investigación, a todos aquellos tutores con los que pude contar durante esta especialización y que aportaron su granito con sus conocimientos. Muchas Gracias.

CONTENIDO

Pág.

INTRODUCCIÓN 16

1. JUSTIFICACIÓN 17

2. OBJETIVOS 18

2.1 OBJETIVO GENERAL 18

2.2 OBJETIVOS ESPECÍFICOS 18

3. PLANTEAMIENTO DEL PROBLEMA 19

3.1 DEFINICIÓN DEL PROBLEMA 19

3.2 FORMULACIÓN DEL PROBLEMA 20

3.3 ALCANCE DE PROYECTO 20

4. MARCO REFERENCIAL 21

4.1 MARCO TEORICO 21

4.1.1 Bases de datos. 21

4.1.2 Tipos de bases de datos. 21

4.1.2.1 Bases de datos relacionales. 23

4.1.2.2 Bases de datos no relacionales. 24

4.1.2.3 Bases de datos orientadas a objetos. 25

4.1.2.4 Bases de datos objeto-relación. 26

4.1.2.5 Bases de datos híbridas.....26
4.1.3 Estado actual de las bases de datos. 27
4.2 MARCO CONCEPTUAL 27
4.2.1 ¿Qué es hacking?.....27
4.2.2 ¿Qué es seguridad informática?.....28
4.2.3 ¿Qué es un sistema gestor de base de datos (SGBD)? 28
4.2.4 ¿Qué es un Administrador de bases de datos?.....28
4.3 MARCO LEGAL 29
4.4 MARCO TECNOLÓGICO 30
4.4.1 Herramientas de análisis.....30
4.4.1.1 Nessus. 30
4.4.1.2 Metasploit.....31
4.4.1.3 Sqlmap. 31
4.4.1.4 Dbpwaudit. 31
4.4.1.5 Database browser. 32
4.4.1.6 THC-orakel cracker. 32
4.4.1.7 Oracle auditing tools. 33
4.4.1.8 Nikto. 33
4.4.2 Tipos de hackers y su forma de operar. 34
4.4.2.1 Los Black Hat. 34
4.4.2.2 Los White Hat. 34
4.4.2.3 Los Greyhat Hackers. 35

4.4.2.4 Los Crackers. 35

4.4.2.5 Los Lamer. 35

4.4.2.6 Blue Hat. 36

4.4.2.7 Hacktivistas. 36

4.4.2.8 Los Script-kiddies. 36

5. VULNERABILIDADES COMUNES EN UNA BASE DE DATOS 37

5.1 NOMBRE DE USUARIO/PASSWORD DÉBIL 37

5.2 PREFERENCIAS DE PRIVILEGIOS DE USUARIOS POR PRIVILEGIOS DE GRUPO 38

5.3 ABUSOS DE PRIVILEGIOS 38

5.4 ATAQUES DE INYECCIÓN SQL 39

5.4.1 Parametrizar las consultas *SQL* 41

5.4.2 No mostrar al usuario la información de error generada por la base de datos. 41

5.4.3 Rechazar las peticiones con caracteres sospechosos. 42

5.4.4 Convertir siempre el valor a su tipo correspondiente. 42

5.5 AUDITORIA DÉBIL 42

5.6 DENEGACIÓN DE SERVICIO 44

5.6.1 Prevención de ataques denegación de servicio. 45

5.6.1.1 Monitoreo y conocimiento de la plataforma. 45

5.6.1.2 Correcto diseño de la plataforma y planificación de procedimientos. 45

5.6.1.3 Realización de auditorías y corrección de vulnerabilidades. 46

5.7 EXPLOTACIÓN A BASES DE DATOS MAL CONFIGURADAS 46

5.8 VULNERABILIDADES DE PROTOCOLO DE COMUNICACIÓN 47

6 Fases del hacking ético 48

6.1 RECONOCIMIENTO.....48

6.2 ESCANEO 49

6.3 OBTENER ACCESO 51

6.4 ESCRIBIR INFORME 52

6.5 PRESENTACIÓN INFORME 52

7. METODOLOGÍAS DE HACKING ETICO.....53

7.1 OSSTMM (OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL) 53

7.1.1 Ámbitos y alcance de OSSTMM. 54

7.1.2 Minuciosidad de OSSTMM. 55

7.1.3 Usabilidad de OSSTMM.....55

7.1.4 Métricas de OSSTMM.....55

7.1.5 Ventajas de OSSTMM. 55

7.1.6 Limitaciones de OSSTMM. 56

7.2 ISSAF (INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK 56

7.2.1 Ámbito y alcance de ISSAF. 58

7.2.2 Meticulosidad de ISSAF.....59

7.2.3 Usabilidad de ISSAF.....59

7.2.4 Métricas de ISSAF. 59

7.2.5 Ventajas de ISSAF. 59

7.2.6 Limitaciones de ISSAF. 60

7.3 ANÁLISIS DE LAS METODOLOGÍAS DE HACKING ÉTICO 60

8. CONCLUSIONES 61

9. RECOMENDACIONES 62

BIBLIOGRAFÍA 63

LISTA DE TABLAS

Pág.

Cuadro 1. Caracteres especiales SQL.....42

Cuadro 2. Mecanismos de Hacking 51

LISTA DE FIGURAS

Pág.

Figura 1. Bases de datos dinámica.....22
Figura 2. Bases de datos estáticas.....23
Figura 3. Modelo base de datos relacional 24
Figura 4. Bases no relacionales.....25
Figura 5. Editor de tablas universal.....32
Figura 6. Opciones disponibles de nikto 34
Figura 7. Comprobador de contraseñas 37
Figura 8. Esquema inyección SQL.....40
Figura 9. Ocultando errores de *SQL* 41
Figura 10. Fases de un hacking.....48
Figura 11. Escaneo con herramienta de ping 50
Figura 12. Escaneo de puertos.....50
Figura 13. Logo OSSTMM 3 54
Figura 14. Fases evaluación ISSAF.....58

GLOSARIO

AUTENTICACIÓN: tratamiento por el cual se da autorización a alguien para dar acceso a un sistema o cualquier recurso a través de una contraseña u otros dispositivos ya sean electrónicos (tarjetas inteligentes, token) o biométricos.

BASES DE DATOS: sistema de información organizada en un sistema de forma tal que cuando sea necesario un dato el ordenador es capaz de seleccionarlo rápidamente.

CRACKER: persona que modifica las restricciones de un sistema o programa de manera indebida, para beneficio propio con fines lucrativos.

DATO: es un valor que representa la información que recibe el computador, que pueden ser números, letras o símbolos.

HACKER: persona apasionada por la programación que busca las técnicas de mejora en la seguridad de los sistemas.

HACKING: actividad de intrusión que realiza un hacker.

INFORMÁTICA: es aquello relacionado con la computación donde se utilizan técnicas y procesos para almacenar, procesar y transmitir información.

SEGURIDAD: es el conjunto de sistemas, medios humanos u organizativos con acciones que eliminan o reducen riesgos y amenazas que llegan a afectar una persona, una entidad, información y objetos.

VULNERABILIDAD: es una debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o sus datos y aplicaciones.

RESUMEN

El proyecto tiene como finalidad profundizar sobre las metodologías utilizadas en la realización de pruebas de intrusión controladas sobre sistemas informáticos como hacking ético en bases de datos, estableciendo cómo se pueden encontrar las vulnerabilidades, riesgos potenciales e identificación de debilidades a través del uso de distintos tipos de herramientas de análisis como mecanismo para poder prevenir ataques externos y gestionar mejor los riesgos a los que se ven expuestas las organizaciones.

De igual manera se describe las diferentes fases desarrolladas por un hacking ético donde se aplica un reconocimiento pasivo y activo de la información o BD objetivo, un escaneo utilizando herramientas de exploración para perpetrar ataques para lograr obtener y mantener el acceso a las BD, llegando finalmente a la explotación del sistema, sin olvidar cubrir el rastro, esto en el sentido de evitar la detección del personal de seguridad. Todo esto en búsqueda de generar políticas y mecanismos de defensa oportunos y que salvaguarden la integridad de las bases de datos de la organización.

Asimismo, este proyecto expone algunas de las metodologías y herramientas disponibles, que pueden ser utilizadas de una forma profesional por los hackers, para encontrar vulnerabilidades que pueden ser detectadas o expuestas en los equipos donde se encuentran las bases de datos, haciendo que el personal encargado de la seguridad y gestión de riesgos tome los correctivos necesarios fortaleciendo la seguridad en sus bases de datos e infraestructura.

PALABRAS CLAVE: vulnerabilidades, riesgos, hacking ético, seguridad, bases de datos.

ABSTRACT

The project aims to delve into the methodologies used in conducting controlled intrusion tests on computer systems such as ethical hacking in databases, establishing how vulnerabilities, potential risks and identification of weaknesses can be found through the use of different types of analysis tools as a mechanism to prevent external attacks and better manage the risks to which organizations are exposed.

In the same way, the different phases developed by ethical hacking are described, where a passive and active recognition of the information or objective DB is applied, a scan using exploration tools to perpetrate attacks to obtain and maintain access to the DBs, finally arriving to the exploitation of the system, without forgetting to cover the trail this in the sense of avoiding the detection of security personnel. All this in search of generating timely policies and defense mechanisms that safeguard the integrity of the organization's databases.

Likewise, this project exposes some of the available methodologies and tools, which can be used in a professional way by hackers, to find vulnerabilities that can be detected or exposed on the computers where the databases are located, making the personnel in charge of security and risk management take the necessary corrections, strengthening security in your databases and infrastructure.

KEY WORDS: vulnerabilities, risks, ethical hacking, security, databases.

INTRODUCCIÓN

Debido al auge y crecimiento constante en el que se encuentran las tecnologías y todo lo relacionado con las telecomunicaciones, hoy en día se tiene la posibilidad de acceder a información desde la red e internet sin necesidad de estar en los lugares donde reside o se encuentra dicha información, por este motivo es necesario que la seguridad en las empresas sea algo primordial para el resguardo y protección de las bases de datos donde se encuentran los datos o activos más valiosos de cualquier organización.

El hacking ético es el encargado de exponer las vulnerabilidades de un sistema informático en ambientes controlados permitiendo que esta práctica sea la base para tomar medidas que se pueden aplicar para reducir riesgos. Precisamente realizan ataques desde el punto de vista ético buscando fallos de protección en las compañías y en la actualidad, estos hackers están conviniendo con las compañías ser sus consultores de seguridad porque ellos lo que hacen es colocarse en el lugar del ciber-criminal para así adelantarse a sus acciones.

Las pruebas de penetración que realiza el hacker ético son complejas y por consiguiente deben ser realizadas de forma profesional donde hay un complemento de técnicas en el que multiplican los intentos de acceso desde diferentes puntos de entrada en un entorno informático, para así identificar aquellas vulnerabilidades que pueden ser explotadas. Un problema de seguridad que se encuentra en muchos sistemas de cómputo y bases de datos es el de prevenir que personas inescrupulosas accedan a los sistemas, ya sea para sacar información o efectuar cambios en las bases de datos, dejándolas en algunas ocasiones inservibles e irrecuperables.

1. JUSTIFICACIÓN

Toda información que es guardada en una base de datos dentro de una organización es muy importante y por lo tanto, se debe tener mucho cuidado en su protección y seguridad frente a los ataques externos o internos que se puedan presentar. En este sentido, se busca profundizar en aquellas metodologías que ayudan a mitigar y a centrar esfuerzos para mejorar la seguridad ante un ciberataque en las bases de datos, el poder gestionar las vulnerabilidades que se puedan presentar sobre los equipos en los que se encuentran dichas bases de datos y así poder tomar las medidas preventivas y correctivas llegado el caso.

Se contextualizará y documentará sobre hacking ético y en las distintas herramientas que se pueden utilizar para realizar intrusiones en las bases de datos sin afectar la integridad de las mismas, solo con el objetivo de investigar, conocer, detectar o recrear cómo actuaría un cracker en una situación de ciberataque o exposición del sistema de información de una organización. El hecho no es solo generar políticas de seguridad, lo importante es que se debe analizar qué mecanismos de defensa se pueden implementar basados en acciones reales que faciliten estar un paso adelante de los ciber-delincuentes que pueden estar a la espera de una puerta trasera o la mínima omisión de configuración de seguridad. Todo esto contribuye a darle mayor importancia a la seguridad de la información dentro las empresas y a que se invierta más en estrategias que gestionen y minimicen el número de riesgos y vulnerabilidades a los que se exponen los activos de información almacenados en las bases de datos.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Profundizar en las metodologías para realizar diagnósticos a bases de datos mediante técnicas de *Ethical hacking*

2.2 OBJETIVOS ESPECÍFICOS

Recolectar información de metodologías y procedimientos de *hacking* ético para bases de datos

Identificar las fases para *hacking* ético

Analizar las fases a realizar para *hacking* ético a bases de datos

Identificar y analizar las vulnerabilidades en las bases de datos.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

En la actualidad, una gran parte de las organizaciones manejan información importante que es almacenada en bases de datos, las cuales muchas veces evidencian problemas de seguridad que propician un escenario adecuado para que los ciber-atacantes exploten fallas y vulnerabilidades como; usuarios o contraseña en blanco o débil, asignación inadecuada de privilegios, características de bases de datos innecesariamente habilitadas, desbordamiento de búfer, bases de datos sin actualizar, datos sensibles sin cifrar, entre otros, que hacen más fácil la intrusión comprometiendo claramente a este tipo de sistemas.

Se han visto ataques presentados por hackers en muchas áreas no solo a nivel de comunicaciones, sino también se han visto ataques a centrales eléctricas como la sucedida en Ucrania, donde toda la ciudad quedó sin energía de un momento a otro y donde se pensó que había sido por alguna saturación en la central o algún error humano, pero no fue así, sino que alguien inescrupuloso decidió afectar a una población de cerca de 230.000 habitantes con tan solo dar un clic. Este ciberataque fue conocido como *Black Energy*, ataque muy sonado por afectar un servicio indispensable. Después, este mismo país fue blanco de otro ataque que fue llamado *industroyer*.

“En Colombia se presentó un ataque a la registraduría por un hacker conocido como “Oroboruo”, un paisa que atacó días antes de las votaciones del plebiscito a esta entidad. A sus 27 años, “Oroboruo” previo a las votaciones del plebiscito, vulneró en 3.196 oportunidades a 1.374 dominios, muchos de ellos del gobierno, a los que les inyectaba código malicioso y los desconfiguraba”[1]. Lo que hace concluir que los ciber-delincuentes están a la vanguardia de la tecnología y cada vez son más expertos en la realización de ciberataques que conllevan a robo, destrucción o alteración de la información como los datos personales, bancarios, financieros, localizaciones y demás que se encuentren en una base de datos.

Lo más aconsejable para evitar este tipo de ataques es el uso de estrategias de seguridad informática y entre ellas se encuentra el *Ethical Hacking* que es una metodología que permite evaluar la seguridad desde una óptica del cracker, pero en un ambiente controlado, explotando todas las vulnerabilidades de la infraestructura tecnológica, identificando aquellas debilidades presentes en el sistema de información y comunicación, ya sea por tener una mala configuración en

[1] AVILA JIMENEZ, Cristian. La historia detrás de cinco ‘hackers’ colombianos y sus delitos. [Online]. Colombia: eltiempo.com, [citada: 6 octubre 2016]. https://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

equipos y aplicaciones o para establecer acciones proactivas para mitigar, minimizar o prevenir al máximo la posibilidad de un ciberataque en la organización.

3.2 FORMULACIÓN DEL PROBLEMA

¿Cómo las metodologías para hacking ético ayudan a tener una visión más amplia en cuanto a la seguridad y protección en las bases de datos?

3.3 ALCANCE DE PROYECTO

El proyecto se limita a la investigación y documentación de información sobre las metodologías y procedimientos de hacking ético para bases de datos, construyendo un documento de consulta académica sobre el tema.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

4.1.1 Bases de datos. “Son un conjunto de datos que se encuentran relacionados entre sí y que busca satisfacer una necesidad recopilando y organizando la información que dentro de una empresa son datos valiosos como la información de personas, de productos, pedidos u otras cosas, es decir, de una manera simple, es un contenedor que permite almacenar la información de forma ordenada con diferentes propósitos y usos.”[2]. Esta organización de la información se da de tal manera que las bases de datos en todo momento están disponibles y por medio de un programa en el computador logran seleccionar aquellas fracciones de datos que necesiten, cuando lo necesiten.

Las bases de datos tradicionales se organizan por campos, registros y archivos. Un campo es una pieza única de información; un registro es un sistema completo de campos; y un archivo es una colección de registros. Cada base de datos se compone de una o más tablas que guarda un conjunto de datos. Cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro [3]

4.1.2 Tipos de bases de datos. Hay diferentes tipos de bases de datos, entre las más comunes que se encuentran están las OLTP y OLAP.

“Las bases OLTP (*On Line Transaction Processing*) o dinámicas son bases en las cuales la información se modifica en tiempo real, es decir, que durante la operación del sistema se puede insertar, eliminar, modificar y consultar datos en línea”[4]. Estas bases de datos son expuestas a ser modificadas con frecuencia. En la Figura 1 se puede observar un ejemplo de base dinámica.

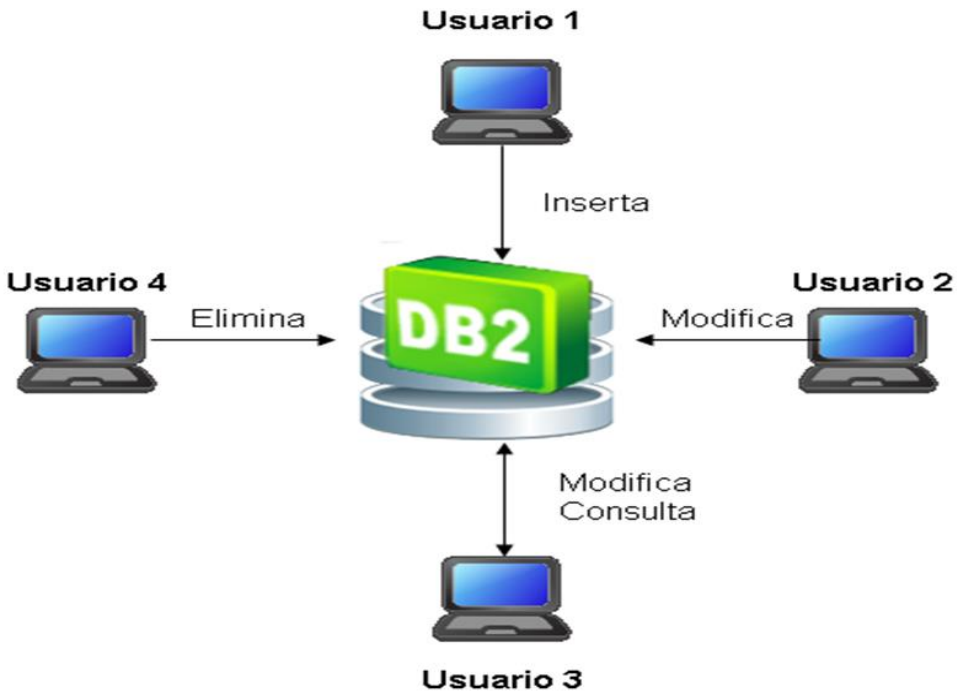
---

[2] Conceptos básicos sobre bases de datos. [Online]. Colombia: Microsoft, [citada: 19 septiembre 2018]. https://support.office.com/es-es/article/conceptos-b%C3%A1sicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204

[3] CALAMEO. Bases de datos. [Online]. [Citada: 19 septiembre 2018] https://es.calameo.com/books/004304179b1c20a4b3659

[4] ANGUIANO MORALES, Jorge Daniel. Características y tipos de bases de datos [Online]. IBM Developers, [Citada: 30 junio 2014] https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/index.html

Figura 1. Bases de datos dinámica

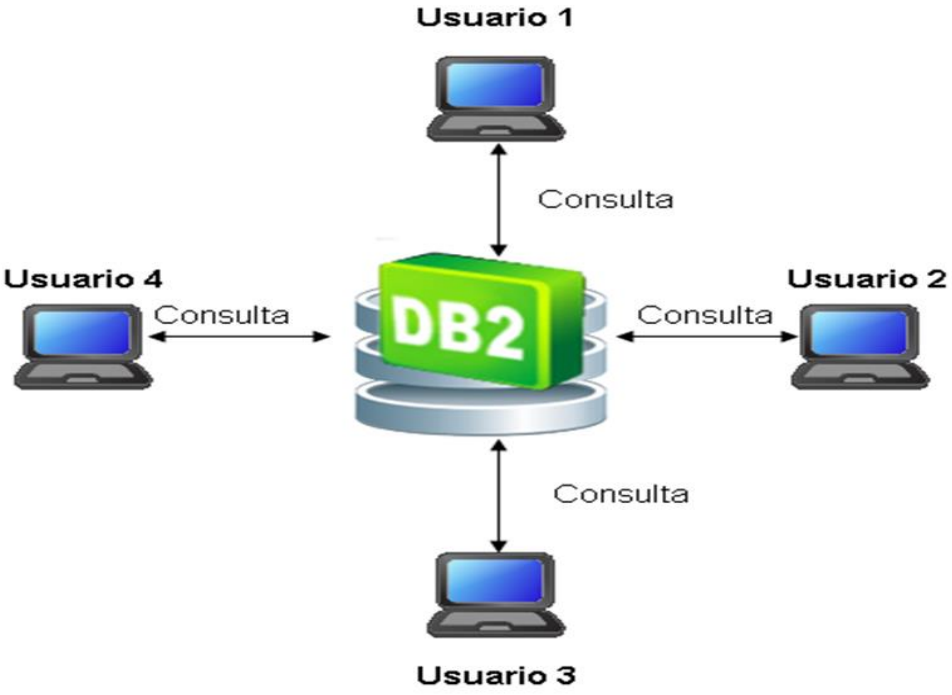


Fuente: ANGUIANO MORALES, Jorge Daniel. Características y tipos de bases de datos [Online]. IBM Developers, [Citada: 30 junio 2014] https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/index.html

"Las bases de datos OLAP (*On Line Analytical Processing*) o estáticas, son aquellas en donde la información manejada en tiempo real no es afectada, es decir, sobre los datos solo se consulta más no se inserta, no se elimina y tampoco se modifican datos. Este tipo de bases de datos son implementadas en *Business Intellingence* para mejorar el desempeño de las consultas con volúmenes grandes de información"[5]. Estas bases son de "solo lectura", pero que guardan un histórico simplemente para utilizarlas como un control durante un tiempo. En la Figura 2 se puede ver un ejemplo de bases de datos estáticas.

[5] ANGUIANO. Op. cit. Disponible en internet: https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/index.html

Figura 2. Bases de datos estáticas



Fuente: ANGUIANO MORALES, Jorge Daniel. Características y tipos de bases de datos [Online]. IBM Developers, [Citada: 30 junio 2014] https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/index.html

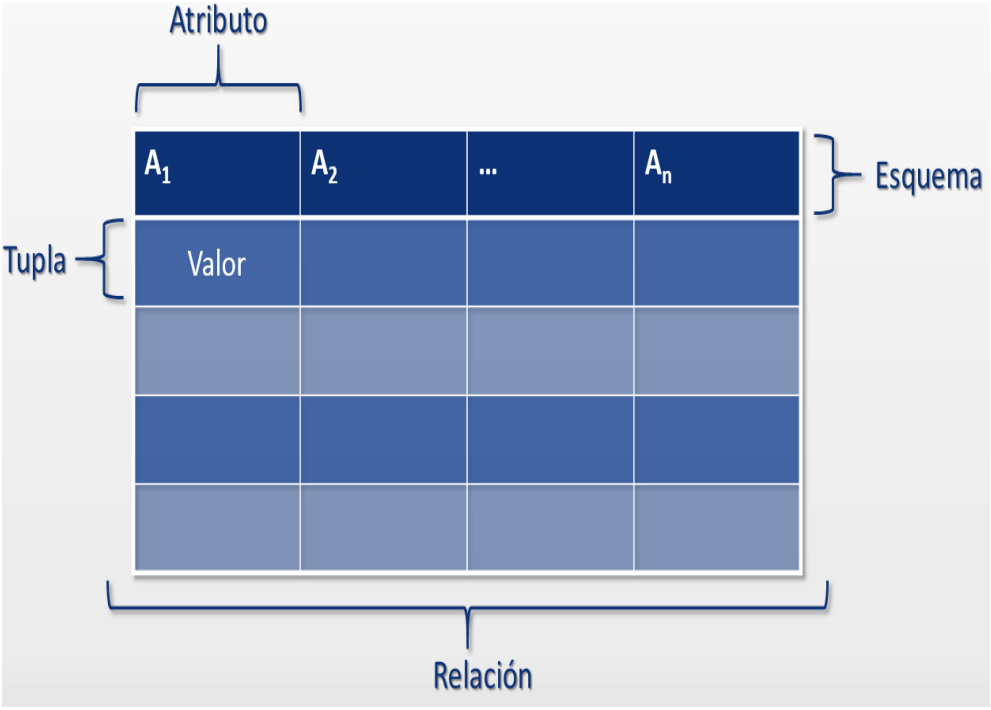
4.1.2.1 Bases de datos relacionales. Es el modelo más utilizado en la actualidad y estas bases esencialmente son un compuesto de tablas constituidas por filas (registros) y columnas (campos). Los registros son los objetos descritos en la tabla y los campos son los atributos. El modelo relacional según el matemático y teórico de bases de datos Edgar F. Coddes: es "una relación representa un conjunto de entidades con las mismas propiedades. Cada relación se compone de una serie de filas o registros (las llamadas tuplas), cuyos valores dependen de ciertos atributos (columnas)"[6].

Estas bases de datos de forma intuitiva y directa son tratadas como un conjunto de tablas que contienen un conjunto de objetos utilizados para almacenar y gestionar los datos. Las tablas son formatos utilizados por este modelo relacional y que se constituyen por filas horizontales y columnas verticales para que los datos a

[6] Digital Guide IONOS. Bases de datos relacionales: el modelo de datos en detalle. [Online]. [Citada: 9 mayo 2019]. https://www.ionos.mx/digitalguide/hosting/cuestiones-tecnicas/bases-de-datos-relacionales/

presentar estén agrupados y de forma ordenada. En la Figura 3 se muestra un ejemplo de modelo relacional con una tabla.

Figura 3. Modelo base de datos relacional



Fuente: Digital Guide IONOS. Bases de datos relacionales: el modelo de datos en detalle. [Online]. [Citada: 9 mayo 2019]. https://www.ionos.mx/digitalguide/hosting/cuestiones-tecnicas/bases-de-datos-relacionales/

4.1.2.2 Bases de datos no relacionales. Estas bases de datos no manejan el esquema de tabular filas y columnas, sino que trabajan con un modelo de almacenamiento optimizado. La expresión *NoSQL* hace énfasis a las reservas de datos que no manejan consultas con datos SQL, sino que emplean otros lenguajes de programación para consultar datos. Dentro de las opciones de *NoSQL* disponibles en la actualidad se encuentran: *Cassandra*, *MongoDB*, *Jackrabbit*, *CouchDB*, *BigTable* y Dinamo. En la Figura 4 se pueden observar algunos logos de bases *NoSQL*.

Figura 4. Bases no relacionales

Fuente: https://image.slidesharecdn.com/1bigdatayredessociales-141113170438-conversion-gate01/95/1-big-data-y-redes-sociales-22-638.jpg?cb=1423001155

Documento es el nombre que se le da al almacenamiento de datos como un conjunto de cadenas con nombre y valores generalmente en codificación JSON. Este almacén de documento no requiere que tenga la misma estructura por lo que lo hace flexible y de forma libre.

Este tipo de bases de datos admite actualizaciones en campos específicos y no en todo el documento. Dentro de este tipo de bases de datos se pueden tener soluciones como:

- “Almacenes de clave/valor
- Almacenes de familia de columnas
- Almacenes de documentos
- Almacenes de grafos”[7]

Con este modelo de bases de datos no relacionales es que hoy en día se conciben las redes sociales por el manejo tan grande de datos que se generan por los millones de usuarios.

4.1.2.3 Bases de datos orientadas a objetos. Son bases de datos que se encuentran formadas por objetos de distintos tipos y con unas operaciones definidas. “Estas bases de datos pueden manejar información binaria (como objetos multimedia) de

[7] LÓPEZ DE IPIÑA, Diego. Bases de datos no relacionales [online]. Madrid: Fundación Universidad Rey Juan Carlos. [citado: 4 julio 2012]. https://es.slideshare.net/dipina/nosql-cassandra-couchdb-mongodb-y-neo4j

forma eficiente. El límite de estas bases de datos está en su especialización ya que pueden estar diseñadas para un tipo de objetos en particular "[8].

Cuando se hace referencia a un objeto, es porque existe una agrupación de datos que establecen el punto de acceso a estos datos. Un objeto determina a una entidad que contiene (atributos, conexiones o relaciones y funciones o métodos para acceder a los datos almacenados).

4.1.2.4 Bases de datos objeto-relación. Estas bases de datos son sistemas mixtos donde el modelo relacional se amplía a tipos indeterminados de datos como objetos, y se hace necesaria esta ampliación para poder gestionarlos con:

- Tipos de datos complejos y personalizables: mientras que las bases de datos relacionales solo pueden procesar datos alfanuméricos, con los tipos de datos personalizables también se pueden gestionar archivos multimedia estructurados de forma compleja.
- Constructores de tipos: permiten derivar tipos nuevos de los tipos básicos ya existentes.
- Funciones y métodos: como SQL no permite crear funciones, los sistemas objeto-relacionales han de proveer extensiones con las cuales puedan definirse funciones de acceso y edición de tipos de datos complejos[9]

El rendimiento de estas bases de datos se ve expuesto debido a que tienen que realizar lectura, búsqueda y carga de objetos, por este motivo la velocidad se degrada fundamentalmente.

4.1.2.5 Bases de datos híbridas. Son bases de datos que manejan tanto características de las bases de datos relacionales como características de la orientada a objetos utilizando y soportando tanto el disco como la memoria de almacenamiento de datos. Por ser una tecnología reciente aún existen pocas en el mercado

"Esta base de datos es utilizada cuando se necesita un alto rendimiento por parte del sistema con respecto al pequeño tamaño que los sistemas de las bases proporcionan solo en memoria. Este sistema ofrece durabilidad y bajo costo, es decir, costos-beneficios en cuanto a bases sustentados en discos. Para aumentar

[8] ECHEVERRY, Juan. PULGARÍN, Luis. Arquitectura híbrida. [Online]. Universidad de Santa Rosa Cabal. 2015. [citado: 23 octubre 2018] http://arquitecturashibridas.blogspot.com/2015/02/que-es-una-base-de-datos-hibridos-una.html

[9] Digital Guide IONOS. Op. cit Disponible en internet: https://www.ionos.mx/digitalguide/hosting/cuestiones-tecnicas/bases-de-datos-relacionales/

su productividad el sistema guarda y conserva los datos usando los discos y la memoria para los datos que están en uso dinámico"[10].

4.1.3 Estado actual de las bases de datos. En la actualidad, las bases de datos siguen siendo imprescindibles para toda organización. Las bases de datos como todo software ha tenido sus mejoras y evoluciones, las primeras fueron las bases de datos relacionales, luego siguieron las bases de datos no relacionales y las últimas que aparecieron fueron las bases de datos híbridas. Las bases de datos que siguen dominando el mercado son: DB2, SQL *Server*, *Oracle* e IBM.

Oracle: Base de datos desarrollada con compatibilidad en casi todos los sistemas operativos, predomina la cantidad de perfiles con destrezas en esta tecnología y el gran número de mecanismos que posee para su administración y monitoreo

DB2 de IBM: Base de datos que se utiliza en sistemas Unix/Linux, es la segunda después de *Oracle* y en Mainframe es un incuestionable ganador.

SQL SERVER: Base de datos únicamente compatible con sistemas operativos Windows. Cuentan con una alta disponibilidad ya que ofrece más tiempo y conmutación rápida, esto sin arriesgar la memoria del sistema. Afortunadamente en los motores de base de datos y análisis de *SQL Server* vienen directamente añadidas las funciones de memoria lo que mejoran la flexibilidad y facilitan el uso.

4.2 MARCO CONCEPTUAL

4.2.1 ¿Qué es hacking? Es aquella actividad que realiza una persona valiéndose de varias técnicas y métodos para ingresar a otros sistemas informáticos, generalmente con scripts o programas que evitan las medidas de seguridad para lograr acceder a un sistema. Estas técnicas básicamente incluyen el uso de virus, gusanos, troyanos, *ransomware*, *rootkits* entre otros que tienen la capacidad de "leer" la forma como están construidas o configuradas las aplicaciones encontrando riesgos y fallos por donde se puede acceder sin autorización a un sistema.

La persona que realiza este tipo de ataques es llamada *hacker*, pero a ellos se les ve de forma negativa, por la labor que han venido realizando, siendo una equivocación ya que en la actualidad se cuenta con algunos *hackers* que son éticos y hay empresas que los contratan para que ayuden a mejorar la seguridad de la infraestructura tecnológica

[10] ECHEVERRY. Op. Cit. Disponible en internet: http://arquitecturashibridas.blogspot.com/2015/02/que-es-una-base-de-datos-hibridos-una.html

4.2.2 ¿Qué es seguridad informática? Es la labor que se realiza a través de herramientas, procedimientos y estrategias para garantizar que la información de una entidad está protegida asegurando su integridad, disponibilidad y confidencialidad.

“La seguridad informática es la disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta.”[11].

Dentro de la seguridad informática también se debe tener presente lo que respecta al software y el hardware y por eso existe la seguridad online, seguridad en software y seguridad en hardware.

4.2.3 ¿Qué es un sistema gestor de base de datos (SGBD)? Es un complejo agrupamiento de programas diseñado para permitir el uso de una base de datos, conocidos como software de base. “Normalmente, los gestores de bases de datos incluyen programas que organizan y cargan los datos del usuario en discos u otros soportes de almacenamiento de acceso directo, al mismo tiempo que establecen y mantienen varios índices de los datos almacenados”[12].

Este sistema ayuda en el procedimiento de definición, construcción y manipulación de BD para distintas aplicaciones.

- En la definición de una BD se establecen los tipos, estructuras y restricciones de los datos.
- En cuanto a la construcción de una BD es la técnica de guardar los datos en un espacio de aprovisionamiento dominado por el SGBD, después de especificada la BD.
- En la manipulación de una BD, se consulta información, se actualiza (modifica, introduce o elimina bases de datos) y se genera informes a partir de la información guardada.

4.2.4 ¿Qué es un Administrador de bases de datos? Es el DBA (*Data Base Administrator*), que son aquellas personas delegadas de controlar los sistemas de BD, que entre sus ocupaciones están;

- Definir y modificar el esquema de la BD y las restricciones de los datos.

[11] BACA URBINA, Gabriel. Introducción a la seguridad informática. México: Patria, 2016. p.12.
[12] SAFFADY, William. Informática documental para bibliotecas. Madrid: Díaz de santos, 1987. 123p. ISBN: 84-86251-47-8.

- Crear y modificar las estructuras de almacenamiento físicas y los métodos de acceso.
- Autorizar el acceso a la BD de los usuarios.
- Garantizar el funcionamiento correcto del sistema y prestar soporte técnico: se ocupa de los problemas de violación de la seguridad del sistema de BD, o de respuesta lenta del sistema.
- Realizar copias de seguridad (*backups*) del contenido de la BD, etc.[13]

4.3 MARCO LEGAL

Debido a la constante evolución de la tecnología, las personas en la actualidad manejan y guardan información en medios electrónicos y bases de datos, lo que ha producido que se den los delitos informáticos con fines maliciosos, lucrativos o para la alteración de dicha información. Por esto se desarrollan normativas gubernamentales que ayudan a tratar estos delitos.

Para muchas organizaciones el término de delito informático ha causado controversia ya que cada uno emite su propio concepto desde su punto de vista. Para poder tener claridad se tomará como referencia de un concepto universal que es “el Convenio de Ciberdelincuencia del Consejo de Europa, donde se definen los delitos informáticos como: los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”[14].

En Colombia se cuenta con una normativa que trata con rigor lo concerniente al tema de la seguridad de la información y es la ley 1273 de 2009, donde según el juez segundo de control de garantías Alexander Díaz quién también es el autor de esta ley indicó en una entrevista dada al diario el espectador, que el país tiene la mejor normatividad del continente; tan es así que “fue considerada por el Congreso de la Fiadi (Federación Iberoamericana de Asociaciones de Derecho e Informática) en Santa Cruz de la Sierra, por todos los informáticos de América asociados a este organismo como la mejor ley de delitos informáticos del continente”[15]

Por medio de la ley 1273 de 2009 se perfecciona el código penal creando un nuevo bien jurídico amparado por el significado “de la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las

[13] COBO YERA, Ángel. Diseño y programación de bases de datos. Madrid: Visión libros. 116p. ISBN: 978-84-9821-459-8.
[14] División ComputerForensic. Definición de Delito Informático. [Online]. [Citado: 14 abril 2020] http://delitosinformaticos.info/delitos_informaticos/definicion.html
[15] EL ESPECTADOR. En busca de cura para los delitos informáticos. [Online], 13 mayo 2014 [citado: 14 abril de 2020]. http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170

tecnologías de la información y las comunicaciones"[16]. Esta ley se divide en dos capítulos en los que se trata de la integridad, confidencialidad, disponibilidad, atentados e infracciones de aquellos datos en los sistemas informáticos.

Los delitos informáticos en Colombia a partir de la Ley 1273 de 2009, se tipificaron así: "acceso abusivo a un sistema informático, obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos"[17].

Lo anterior es un gran progreso de avance en armas jurídicas contra los ciber-delincuentes, ya que la norma es lo bastante clara, abarcando con todo lo relacionado acerca de la protección de la información, tanto para las empresas como para personas naturales. Con la ley 1273 las empresas se pueden ver protegidas para que en el momento que lo necesiten realicen las denuncias respectivas a violaciones de cláusulas internas relacionadas con la confidencialidad, manejo inadecuado o sin autorización de información delicada para la organización.

4.4 MARCO TECNOLÓGICO

4.4.1 Herramientas de análisis. Si se sabe que las vulnerabilidades existen, también se pueden encontrar herramientas que ayuden a facilitar el análisis y hallazgo de esas vulnerabilidades que afectan un recurso. "Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal configurado permite que un agente externo, acceda sin permisos apropiados al recurso o información"[18]. Dentro de las herramientas de análisis que se pueden encontrar están:

4.4.1.1 Nessus. Herramienta tipo escáner que detecta fallos de seguridad, es creada por la empresa Tenable quienes dentro de sus soluciones, cuentan con una aplicación más completa que es la *nessus tenable*.io que es gestionado en la nube y "proporciona los datos procesables y precisos que necesita para identificar, investigar y priorizar la reparación de vulnerabilidades y las configuraciones

[16] OJEDA PEREZ, Jorge Eliecer. RINCON RODRIGUEZ, Fernando. ARIAS FLOREZ, Miguel Eugenio. DAZA MARTINEZ, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia [Online]. Bogotá. [Citada: 1 febrero 2010] http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

[17] Ibid.,

[18] ROMERO CASTRO, Martha Irene. et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. Área de innovación y desarrollo, S.L. 2018. 121p.

incorrectas en su entorno moderno de TI"[19]. Cuenta con la capacidad para evaluar una empresa u organización, llegando a categorizar los riesgos suministrando estadísticas y reportes constantes.

Esta herramienta escanea bases de datos, diferentes sistemas operativos tanto físicos como virtuales y gran cantidad de infraestructuras. Está diseñado de forma profesional hacia la seguridad, donde cada gestión de vulnerabilidades es sencilla, fácil e intuitiva.

4.4.1.2 Metasploit. Herramienta que lanza ataques con comandos cortos, ayudando con la evaluación de vulnerabilidades de seguridad. Creado por HD. *Moorer* en el 2003, tiene muchos *exploits* con conocidas vulnerabilidades que tienen módulos conocidos como *payloads*, que son códigos que explotan esas vulnerabilidades. De esta herramienta se puede conseguir tanto la versión gratuita como la de pago y al ser flexible permite varias configuraciones. Es muy eficaz por lo que se hace necesario tener soluciones anti pirateo para repeler y solucionar ataques. Es un proyecto de código abierto que fue desarrollado en primera instancia en lenguaje Perl, pero en la actualidad se encuentra en lenguaje Ruby.

4.4.1.3 Sqlmap. Es aquella herramienta de código abierto que funciona para hacer testeo en cualquier base de datos, permite automatizar los procesos logrando descubrir y examinar fallos de inyección *SQL*. Esta desarrollada en *Phyton* y como características esta herramienta brinda soporte en:

- "Conexiones directas a las bases de datos sin pasar por una inyección SQL, proporcionando credenciales DBMS, dirección IP, puerto y nombre de la base de datos.
- Enumerar usuarios, *hash* de contraseñas, privilegios, roles, BD, tablas y columnas.
- buscar nombres de bases de datos específicos, tablas específicas en todas las bases de datos, o columnas específicas en todas las tablas de bases de datos"[20] .

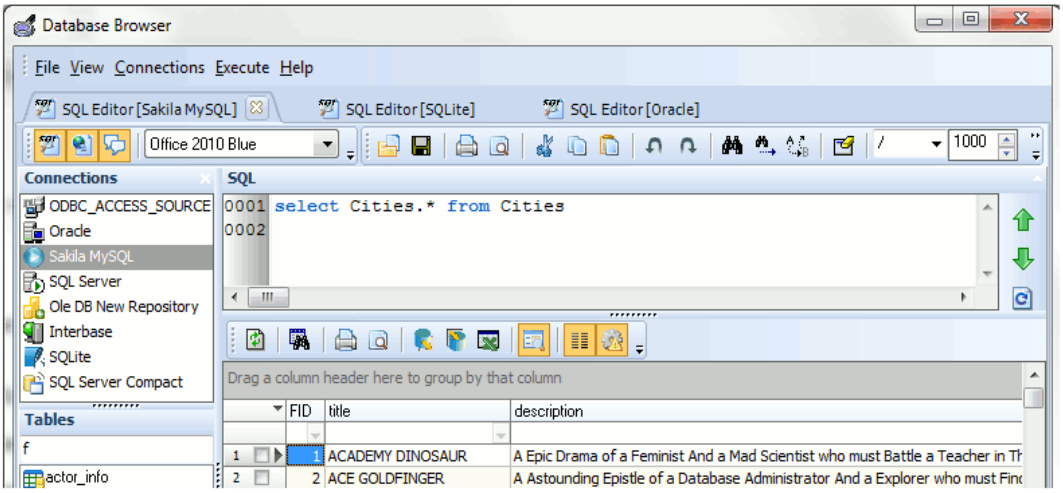
4.4.1.4 Dbpwaudit. Es una herramienta desarrollada en Java que admite ejecutar auditorias en línea para calidad de contraseña en varios motores de bases de datos. Esta aplicación por su diseño permite que sean agregados fácilmente los controladores adicionales en las bases de datos. La estructura se encuentra en dos archivos, uno es el aliases.conf usado para designar controladores a los alias y el otro es el rules.conf que indica a la aplicación como manipular los anuncios de error del análisis.

[19] TENABLE. Tenable.io. [Online]. [2020]. https://es-la.tenable.com/products/tenable-io
[20] ASSUMPCAO G, Bernardo. STAMPAR, Miroslav. Sqlmap Automatic SQL injection and database takeover tool. [Online]. http://sqlmap.org/

El desarrollador de *DBPwAudit* fue Patrick Karlsson quién además fundo cqure.net para ayudar a los profesionales de la seguridad, todas las herramientas que son publicadas en el sitio son desarrolladas y actualizadas por él.

4.4.1.5 Database browser. El navegador de bases de datos funciona de forma universal para edición de tablas y es gratuito. “Esta herramienta fácil de usar permite al usuario conectarse a cualquier base de datos y explotar o modificar datos, ejecutar *scripts SQL*, exportar, importar e imprimir datos”[21]. En la Figura 5 se puede observar un pantallazo de la apariencia del editor de tablas universal.

Figura 5. Editor de tablas universal



Fuente: ETL-TOOLS.COM. Database Browser. [Online]. [Citado: 22 abril 2020] https://www.etl-tools.com/database-browser/overview.html

Dentro de los beneficios con los que se puede contar en la herramienta están: el número de conexiones no es limitado, funciona con muchas bases de datos, exporta datos a diferentes formatos, soporta cadenas de conexión ODBC, navega entre tablas con un solo clic, filtra y agrupa datos de ejecución de registros.

4.4.1.6 THC-orakel cracker. THC es una herramienta práctica que descifra y rompe las contraseñas de una base de datos *Oracle* en segundos. Su trabajo es analizar los mecanismos de autenticación en las BD de *Oracle*, ya que uno de los modos de autenticación de red en *Oracle* es el intercambio de claves débil, mecanismos que

[21] ETL-TOOLS.COM. Database Browser. [Online]. [Citado: 22 abril 2020] https://www.etl-tools.com/database-browser/overview.html

en la actualidad se utilizan en los controladores *JAVA* de *Oracle*. En los controladores originales de *Oracle*, es bien sabido que un ataque atenúa la forma de autenticarse a la versión vulnerable.

4.4.1.7 Oracle auditing tools. Es aquel grupo de herramientas que están basadas en *Java* y pueden usarse para auditar la seguridad dentro de los servidores de bases de datos de *Oracle*. El OAT utiliza librerías creadas que acceden a la función WinExec en el kernell32.dll en Windows o en el sistema *unix* es llamada libc. Estas funciones propician que cualquier acción en el servidor pueda apropiarse en el mismo contexto de la seguridad con el usuario que inicio el servicio de *Oracle*.

El OAT internamente posee un servidor TFTP que simplifica los intercambios de archivos y dicho servidor se apoya en el servidor www.gordian.com. Como explotación de vulnerabilidades incluye pruebas de contraseña (común/diccionario), admite conexión de códigos de *shell* con formato incorrecto, con paquetes de TCP que bloquean el servidor remoto para así obtener privilegios de DBA en ellos.

4.4.1.8 Nikto. Herramienta muy utilizada para diferentes funciones, entre las que se encuentran escaneo de vulnerabilidades y auditoria de servidores ente otros. Nikto está programada en lenguaje *perl*, permitiendo análisis de los servidores precisando información de la seguridad y las vulnerabilidades por desactualización que puedan presentar los mismos.

Nikto verifica la estructura del servidor como diversos archivos de índice, que respaldan lo que se guarda en el servidor y otras cosas. El creador de esta herramienta es David Lodge, quién también se encarga de su mantenimiento. Según los investigadores especializados del instituto Internacional de Seguridad Cibernética, Nikto tiene la capacidad para comprobar servidores web/url y es posible aprovecharlos en funciones de *hacking*. En la Figura 6 se ven las diferentes opciones que tiene disponibles nikto.

Figura 6. Opciones disponibles de nikto

Fuente: CATOIRA, Fernando. Auditando un servidor web con nikto, argentina, 2012. https://www.welivesecurity.com/la-es/2012/06/05/auditando-servidor-web-nikto/

4.4.2 Tipos de hackers y su forma de operar. En el mundo de la informática existen personas que les gusta hacer cosas inusuales y prohibidas a quienes por su forma de operar se les denomina *hackers* o ciber-delincuentes, entre estos tipos de *hackers* se encuentran:

4.4.2.1 Los Black Hat. Significa (sombrero negro) o ciber-delincuentes que se dedican a las actividades ilícitas donde vulneran sistemas y extraen información importante y confidencial, estos hackers son personas que intentan ingresar a un sistema o red sin alguna autorización todo con fines maléficos para robar contraseñas, información financiera y datos personales para así poder obtener beneficios monetarios o en otras ocasiones solo destruirla.

4.4.2.2 Los White Hat. Significa (sombrero blanco) o *hackers* éticos que son aquellos que se dedican a estudiar, trabajar e investigar para encontrar vulnerabilidades en los sistemas y después corregir aquellas fallas encontradas que ayuden a mejorar la seguridad en los sistemas. “Son altruistas, ya que su motivación es la de buscar, localizar y arreglar los posibles fallos de seguridad en el código. Suele decirse que los *hackers* de sombrero blanco se conforman con el

agradecimiento de la empresa cuyo software parchean y que en casos excepcionales aceptan una camiseta o un bolígrafo de la marca"[22].

4.4.2.3 Los Greyhat Hackers. Son aquellos denominados de (sombrero gris) y que se encuentran en un punto medio entre el bien y el mal del mundo *hacking*, buscan traspasar la seguridad en empresas o encontrar agujeros de seguridad para después ofrecer sus servicios o sacar beneficio vendiendo su descubrimiento, son profesionales que les gusta negociar con el gobierno al encontrar errores de seguridad. No son *hackers* dañinos como para robar cuentas y desocuparlas.

Dentro de los hackers de sombrero gris se encuentran los "italianos *Hacking Team* que venden sus herramientas de espionaje a regímenes represivos como Azerbaiyán, Kazajistán, Uzbekistán, o Arabia Saudí"[23].

4.4.2.4 Los Crackers. Cuentan con un gran conocimiento en seguridad informática, su finalidad es la de dañar o destruir los sistemas y los computadores, colapsan servidores, infectan redes, incrustan virus, modifican software y entran a sistemas con restricciones robando contraseñas. Dominan a la perfección el entorno en el que se mueven, es decir, sobresalen sobre la seguridad de un programa alterando su funcionalidad. Dentro de este universo se encuentran distintas clases de crackers como son:

- Los *crackers* de sistemas: que son aquellos que alteran un software para dejarlo como si fuera original.

- *Crackers* de criptografía: los que se dedican a romper todo lo que tiene que ver con criptografía.

- *Cyberpunk*: se especializan en dañar páginas web o sistemas informatizados.

- Los *Phreakers*: son ciber-delincuentes que se dedican a irrumpir y afectar el área de las telecomunicaciones, todo lo vinculado con centrales de teléfono, grabadas de llamadas y llamadas gratuitas.

4.4.2.5 Los Lamer. Son personas que les falta aquellas habilidades técnicas y que no son competentes para la materia, es decir, quieren obtener beneficios del *hacking* sin tener conocimientos del tema, podrían llamarse *hackers amateurs*.

[22] ELDIARIO.ES. Los hackers llevan sombrero blanco, gris y negro. [Online]. España, 2016. [Citada: 22 abril 2020] https://www.eldiario.es/tecnologia/hackers-llevan-sombrero-blanco-negro_0_505349668.html
[23] Ibid.,

Estos *hackers* hacen ciber-vandalismo e infectan con software malicioso sin preocuparse por el funcionamiento interno de los sistemas.

4.4.2.6 Blue Hat. Llamados *hackers* de sombrero azul y son aquellos encargados de probar y buscar fallas en software antes de que sean lanzados al mercado. Generalmente son principiantes sin ganas de prepararse ya que pueden usar técnica simple de ataque inundando la IP con paquetes y así dar un ataque *DoS*.

4.4.2.7 Hacktivistas. Son aquellos *hackers* que realizan infiltraciones a los sistemas seguros con fines políticos. Son ciberactivistas y se consideran defensores de la libertad y de la información, pero sus acciones son ilegales para conseguirlo. Este tipo de *hackers* revelan los movimientos ilegales que los gobiernos encubren a los ciudadanos. “En 2013, Edward Snowden puso al descubierto como la Agencia de Seguridad Nacional había estado espiando a los ciudadanos estadounidenses (y de otros países) sin pedir permiso, vulnerando sus derechos. Desde el 2013 Snowden vive en un lugar desconocido y sin poder regresar a su casa”[24].

4.4.2.8 Los Script-kiddies. Son aquellos sujetos que aplican programas o script de otros *hackers* para así descifrar los fallos en sistemas, redes y sitios web. No son capaces de crear programas o *exploits* complejos, ya que el único objetivo que tienen es el de deslumbrar a los amigos u obtener renombre en los grupos fanáticos de las computadoras.

[24] La vanguardia. Hacktivistas: en el límite del bien. [Online]. [Citado: 23 mayo 2017]. En la vanguardia. [Actualizado: 27 septiembre 2018] https://www.lavanguardia.com/vida/junior-report/20170519/422741815247/hacktivistas-limite-bien.html

5. VULNERABILIDADES COMUNES EN UNA BASE DE DATOS

Estando en un mundo donde la informática va en crecimiento y donde todo lo que se crea es para hacer la vida más fácil al usuario, es precisamente en este punto donde las bases de datos que guardan esa información pueden ser vulnerables y sufrir algún tipo de ataque por otras personas. A continuación, se dará a conocer algunas de esas vulnerabilidades que se pueden encontrar en una base de datos.

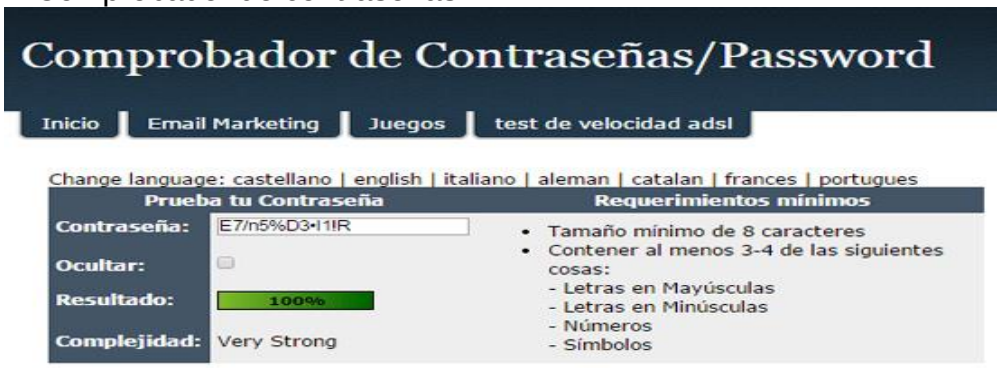
5.1 NOMBRE DE USUARIO/PASSWORD DÉBIL

En la actualidad la autenticación que se basa en contraseñas es quizás una de las más importantes que se usan a diario. Cuando los esquemas de autenticación son débiles esto permite que los atacantes asuman la identidad de los usuarios legítimos en las bases de datos y allí es donde los *hackers* aprovechan ingresando para borrar, robar y manipular información. Se debe optar por que esas contraseñas sean más complejas y difíciles de conseguir por parte de un atacante.

Dentro de las políticas es recomendable que su longitud sea de mínimo 8 caracteres, que además tenga caracteres especiales, números, mayúsculas, minúsculas para que sea precisamente fuerte, entre más caracteres se usen mayor será su complejidad, trate de que la clave no este asociada con nada significativo y que no tenga ningún sentido, sino solo para aquel que la creo. Esto hará que sea más difícil su descifrado, a través de un ataque con diccionarios, por fuerza bruta o con alguna técnica automatizada.

Al crear una contraseña se puede validar que tan segura y fuerte es con los comprobadores de contraseñas. En la Figura 7 se puede observar cómo crear una clave con buen nivel de complejidad.

Figura 7. Comprobador de contraseñas



Fuente: Consejos para crear una contraseña perfecta y memorable. 2015. https://blog.acens.com/general/contrasena-perfecta-memorable/

5.2 PREFERENCIAS DE PRIVILEGIOS DE USUARIOS POR PRIVILEGIOS DE GRUPO

En las organizaciones puede darse el fenómeno que dentro de las bases de datos les asignen privilegios muy elevados a usuarios que no los necesitan y esto llega a ser un verdadero problema. Por esto es aconsejable revisar aquellos privilegios concedidos a los usuarios que tendrán contacto con la información para que no realicen cambios más allá de los autorizados, es decir, se tiene que aplicar el control de acceso a nivel de consulta para que se restrinjan los privilegios y solo se utilicen los mínimos requeridos. Si un usuario solo necesita consultar en la base de datos, no se le deben asignar privilegios para que modifique la información ya que esto es una puerta que se puede dejar abierta para que un *hacker* realice un ataque.

Esta vulnerabilidad tiene su origen desde el momento que son creados los usuarios por parte del administrador de la base de datos o el DBA "*Data Base Administrator*" que no tiene una política de control de accesos o es poco adecuada a la empresa. Como ejemplo en una base de datos *SQL Server* 2012 se debe tener en cuenta lo siguiente:

- Clasificar los objetos de la base de datos, tablas, procedimientos almacenados, funciones y vistas haciendo uso de esquemas ("*schemas*"), por ejemplo: contabilidad, gerencia, recursos humanos; esto de acuerdo a la política interna definida para control de acceso.
- Hacer uso del manejo de la asignación de permisos mediante roles, en vez de asignarlos directamente al usuario.
- Emplear el "principio del privilegios mínimo" en la asignación de permisos.
- Es muy recomendable desactivar la cuenta invitado. Solamente necesita acceso a la base de datos MSDB.
- Hacer uso de las herramientas de auditoría de MS *SQL Server*.
- Monitorizar aquellos usuarios con permisos DBO, son los usuarios con permisos de administración en la base de datos[25].

5.3 ABUSOS DE PRIVILEGIOS

Este tipo de vulnerabilidad puede llegar a materializarse porque aquellos usuarios internos con privilegios, accesos legítimos y permisos definidos que pueden llegar a excederse con dichos permisos para fines que no están autorizados, como el del

[25] GARCIA CARVAJAL, Miguel José. Database Main Threats Analisys Using MS SQL Server. [Online]. 2013.[Citada: 18 mayo 2020] https://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo9_paper_10.pdf

beneficio personal, o lucro a terceros ajenos a la organización. La solución "está relacionada con la política de control de acceso que se aplican no sólo a lo que los datos son accesibles, pero ¿cómo se accede a los datos? Al hacer cumplir las políticas de seguridad web, sobre cosas como la ubicación, el tiempo, el cliente de aplicación y el volumen de los datos recuperados, es posible identificar a los usuarios que están abusando de los privilegios de acceso"[26].

Al interior de las bases de datos se puede realizar la detección de estos abusos de privilegios, estableciéndoles controles como son:

- Elaborar rastreo a las consultas ejecutadas, mediante el establecimiento de registros en una tabla de auditoria.
- Explorar los planes de auditoria estructurados en la base de datos, donde se descubran muestras de conexión anormales, como por ejemplo consultas en horarios no laborales y eliminación o actualización de registros.
- Apuntar las intenciones de conexión realizadas, aplicando herramientas distintas a las diseñadas para interactuar con la base de datos, por ejemplo *SQLCMD* o MS Excel que permiten conectarse y consultar datos de MS *SQL Server*

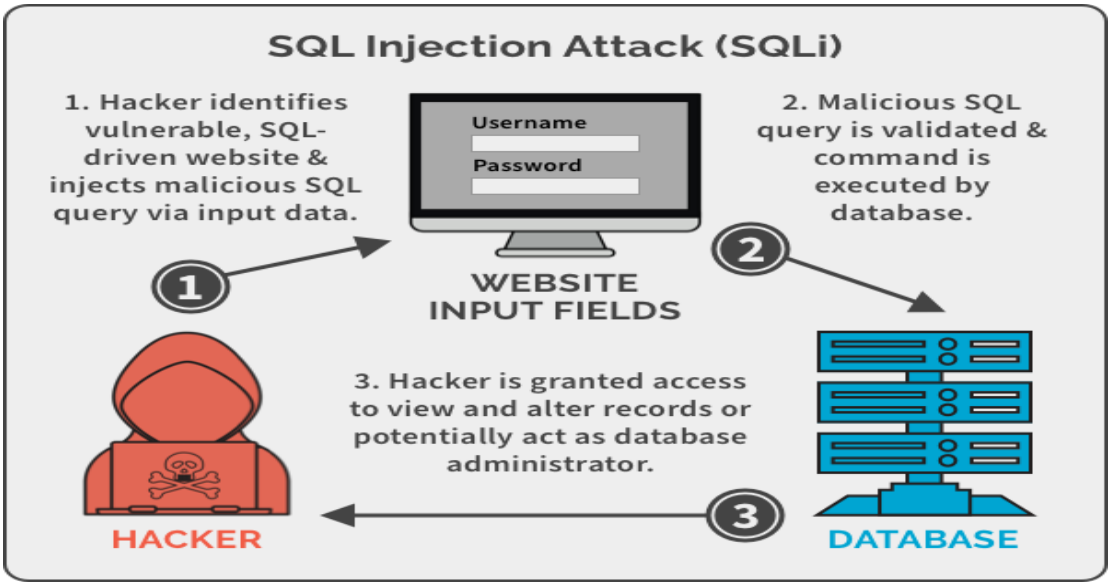
5.4 ATAQUES DE INYECCIÓN SQL

Es aquel ataque en el que se inserta un código *SQL* en los datos de entrada desde el cliente para así llegar a la aplicación, es decir, el atacante al insertar el código tiene la autonomía de modificar las consultas originales que realiza la aplicación, para de esta forma ejecutar otras diferentes con la intención de acceder a las bases de datos y así aprovechar la información que se encuentra en alguna de las tablas o borrar los datos almacenados, entre otras muchas cosas.

Dentro de los efectos de dichos ataques están que se puede acceder no sólo a las tablas que tengan relación con la aplicación, sino también, a otras tablas que tienen referencia a otras bases de datos que se encuentren en el mismo servidor. En la Figura 8 se muestra un esquema de un ataque de inyección *SQL*.

[26] Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas. [Online]. OnaSystem. [Citada: 2018]. https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/

Figura 8. Esquema inyección SQL



Fuente: https://estradawebgroup.com/ImagesUpload/SQL-injection-attack-example.png

Entre los problemas que se pueden presentar por los ataques de inyección *SQL* están:

- Confidencialidad. La información almacenada en las bases de datos es sensible, por esta razón la pérdida de confiabilidad se vuelve un contratiempo constante en los sitios donde hay vulnerabilidades a este tipo de ataques.
- Autenticación. Cuando el sistema para loqueo que se maneja para el acceso a una zona limitada de una web es débil, por medio de este patrón de ataques es posible que se acceda sin tener el conocimiento del usuario ni la contraseña.
- Integridad. Ya que este tipo de ataques por inyección SQL aprueba leer información destacada que esta almacenada en las bases de datos, es posible producir cambios o hasta borrar la información con este tipo de vulnerabilidad.

La inyección de código a las bases de datos *NoSQL* son más graves que en bases de datos *SQL* ya que este tipo de bases de datos utiliza en ocasiones lenguajes imperativos, es decir, de una orden o imposición en vez de ser declarativos, tienen menos restricciones en relaciones y chequeos de consistencia y esa inyección se ejecuta en la capa de aplicación o en la base de datos según el sistema (allí es donde se analiza y evalúa la cadena). Estas bases de datos *NoSQL* tienen deficiencias en seguridad.

Algunas de las medidas que se pueden tomar para evitar ataques de este tipo son:

5.4.1 Parametrizar las consultas *SQL*. Un error común que se comete es que el uso de valores llega sin detallar el tipo para el mismo. Como ejemplo seria así:

"*var id = Request.QueryString["id"];*
*var query = "SELECT * FROM HOUSES WHERE ID=" + id;*"[27]

Para evitar esto, lo que se debe hacer es parametrizar las sentencias *SQL*, de tal forma que se especifique el tipo que se espera en cada parámetro.

"*var objConnection = new OleDbConnection(strDbConnectionString);*
objConnection.Open();
*const string query = "SELECT * FROM HOUSES WHERE ID=?";*
var objCommand = new OleDbCommand(query, objConnection);
var id = new OleDbParameter("@idParam", OleDbType.Integer) { Value = id};
objCommand.Parameters.Add(id);
var objReader = objCommand.ExecuteReader();;"[28]

5.4.2 No mostrar al usuario la información de error generada por la base de datos. Casi siempre en los mensajes de error se da mucha información, que describe al usuario como es la estructura de la base de datos y por eso es mejor no mostrar dicha descripción, ya que un atacante puede aprovechar dicha vulnerabilidad. Para esto por ejemplo con *CSharp* tiene una instrucción que es "*try catch*" la cual evita mostrar el error en la aplicación al usuario final, así como se ve en la Figura 9.

Figura 9. Ocultando errores de *SQL*

```
try{
    /* ..... */
} catch(SqlException e)
{
    /* ..... */
}
```

Fuente: TOVAR VALENCIA, Orlando. Inyección de sql, tipos de ataques y prevención en asp.net – c#. [Online]. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2948/Trabajo%20de%20grado.pdf?sequence=1

[27] TORRES, Gisela. Tips para evitar SQL Injection. [Online]. 2010. [Citada: 21 mayo 2020]. https://www.returngis.net/2010/10/tips-para-evitar-sql-injection/
[28] Ibid.,

5.4.3 Rechazar las peticiones con caracteres sospechosos. Para generar consultas en las bases de datos se utilizan muchos caracteres que en el lenguaje *SQL*, algunos de ellos pueden ser filtrados para así prevenir un ataque de inyección. En el cuadro 1. Se encuentran los caracteres especiales.

Cuadro 1. Caracteres especiales SQL.

CARÁCTER ESPECIAL	SIGNIFICADO SQL
;	Delimitador de consultas.
,	Carácter delimitador de cadena de datos.
–	Comentario.
/* */	Delimitadores de comentario. El texto entre /* y */ no es evaluado.
xp_	Se utiliza en el inicio del nombre de procedimientos almacenados extendidos de catálogo, como xp_cmdshell.

Fuente: TORRES, Gisela. Tips para evitar SQL Injection. [Online]. 2010. [Citada: 21 mayo 2020]. https://www.returngis.net/2010/10/tips-para-evitar-sql-injection/

5.4.4 Convertir siempre el valor a su tipo correspondiente. En un ejemplo, es de si se está esperando un valor de tipo numérico, se debe asegurar ese valor convirtiéndolo a dicho tipo para que no incluya texto malintencionado o adicional. La instrucción puede ser así:

"*var id = Request.QueryString["id"];*
int result;
if (Int32.TryParse(id, out result))
//Do things"[29]

5.5 AUDITORIA DÉBIL

Este tipo de ataques se da cuando las políticas de auditoria en las bases de datos no son lo suficientemente fuertes, generando así riesgos de detección, recuperación, análisis forense y cumplimiento. Los sistemas de gestión de bases de datos nativa (DBMS) auditan el rendimiento inaceptable, pero son vulnerables a los ataques en privilegios ya que muchos administradores de bases (DBA) y desarrolladores desactivan las auditorias de bases de datos.

[29] TORRES, Op, cit. Disponible en internet: https://www.returngis.net/2010/10/tips-para-evitar-sql-injection/

Estas auditorías permiten a los administradores de las BD conocer las consultas que se ejecutan en el motor de base de datos y las actividades que realizan los usuarios teniendo así modo de generar algunos controles para la seguridad con eficacia y confiabilidad. Una solución es tener auditorias de bases de datos establecidas en red y dicha auditoria no debe tener impactos negativos en el rendimiento de las bases de datos ya que se ejecutan independientemente y recopilan datos al detalle.

En las bases de datos se pueden llevar a cabo auditorias de actividades y de transacciones, así:

- Auditoria de actividades: es la que controla todo lo que el usuario realiza en los objetos (tablas, vistas, restricciones) de las bases de datos. El registro de esta auditoria (RA) debe tener una adecuada administración por su crecimiento continuo y alto, que puede exceder el tamaño de la BD.
Para habilitar o deshabilitar la auditoria, el usuario primero debe tener privilegios de AUDIT SYSTEM, segundo ejecutar los comandos SQL, que en el caso de Oracle son:

- Habilitar: CATAUDIT.SQL
- Deshabilitar: CATNOAUDIT.SQL

En la base de datos es posible auditar en tres niveles que son; los estatutos SQL, los objetos y los privilegios. En los estatutos hace referencia a todas las reglas de tipo SQL que se puedan ejecutar, las más usuales son aquellas reglas que el servidor recibe de la base de datos para autorizar una conexión (inicio de sesión) o una desconexión.

El manejo referente a los objetos tiene que ver con las creaciones, las modificaciones y los borrados de objetos de sistema o de usuario. Lo que respecta a los privilegios, son los permisos otorgados a los usuarios que consultan información o efectúan transacciones. Por ejemplo “existen más de 80 privilegios diferentes en el servidor de la base de datos Oracle”[30].

- Auditoria de transacciones: es aquella auditoria donde se implementan unos controles en serie, que admiten utilizar una bitácora de todas las transacciones realizadas por los usuarios. Esta auditoria tendrá un registro como el de actividades pero que se llama registro de auditoria de transacciones (RAT), siendo este registro superior al RA (registro de actividades), porque va a tener mucha más información, ya que se rastrea cada movimiento que el usuario realiza con cada conexión que ejecuta.

[30] VILLALOBOS MURILLO, Johnny. Auditando en las bases de datos. [Online]. Costa Rica, 2008. [Citada: 19 mayo 2020]. https://dialnet.unirioja.es/descarga/articulo/5381374.pdf

Hay unos objetos especiales en los sistemas gestores de bases de datos relacionales llamados *Trigger* (desencadenador), que son una agrupación de sentencias *SQL* asociadas a una tabla, con el fin de que al recibir la tabla una transacción, el *Trigger* entra a verificar, validar y aplicar las sentencias almacenadas. “La idea de implementar el *Trigger* como auditoría de transacciones es excelente, siempre y cuando se tome en cuenta que él interfiere en el rendimiento de la transacción, aun así, si es necesario implementarlo tenga presente hacerlo en forma adecuada y moderada”[31].

Un ejemplo de código para crear un *Trigger* que reaccione cuando se haga una actualización, un borrado o una inserción es el siguiente:

“*Create trigger* auditor
after update on cuentas
for each row
begin
insert into RAT
values (user, date, :new.cliente, :old.saldo, :new.saldo) end

De esta forma se almacena en el registro de auditoría los valores de usuario (user), fecha (date), cliente (:new.cliente), saldo anterior (:old.saldo), saldo actual (:new.saldo). Las variables de saldo anterior y nuevo saldo corresponden a Oracle”[32].

Para que no se vea afectado el rendimiento de las transacciones, se debe considerar; utilizar *trigger* en tablas críticas, información que no sea necesaria eliminar, no tener un solo registro de auditoria, solo auditar transacciones relevantes, que los registros de auditoria no estén en el mismo disco de los sistemas y hacer *backup* periódicamente.

5.6 DENEGACIÓN DE SERVICIO

Este ataque llamado *DoS* (*Denial of Service*), de lo que trata es de bloquear o dejar inoperativo cualquier tipo de servicio y la orientación del ataque es el consumo de recursos ya sea de hardware, software o de ambos. “Si ampliamos el concepto de *DoS*, cuando se realiza una acción de este tipo lanzada desde numerosos equipos, se está en presencia de un ataque de Denegación de servicio distribuida o *DDoS* (*Distributed Denial of Service*). Normalmente utiliza una estructura por capas, donde el atacante se conecta a servidores maestros, que son otros sistemas previamente

[31] VILLALOBOS MURILLO. Op. cit. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/5381374.pdf
[32] Ibid.,

comprometidos por él”[33]. Como técnicas a utilizar para este ataque pueden estar el desbordamiento de búfer, inundación de la red, corrupción de datos, sobrecarga de la memoria y la CPU, provocando así la caída del servidor.

5.6.1 Prevención de ataques denegación de servicio. Los ataques por denegación de servicio como cualquier otro ataque son difíciles de contener, pero se hace necesario realizar prevenciones que ayuden a minimizar los riesgos, entre los que se encuentran:

5.6.1.1 Monitoreo y conocimiento de la plataforma. El conocimiento de la información acerca del servicio que se presta, debe tenerse de forma integral y no por segmentos, ya que es parte esencial para acercarse a las labores de prevención de los ataques sacando la mejor ventaja. Cuando el monitoreo se hace de forma correcta, hay que tener en cuenta los procedimientos que son frecuentes en el servicio a resguardar, revisar los valores máximos que los dispositivos involucrados (BD, *Firewalls*, servidores, *routers*, etc.) pueden soportar y tener una visión del crecimiento que se espera en los servicios, que impacten en los datos. El monitoreo debe involucrar también el tráfico encriptado, ya que los ataques *DoS* están empleando protocolos SSL para pasar inadvertidos, precisamente porque este tipo de tráfico no se monitorea, por el hecho de que hay que des-encriptar y esto trae dificultades tanto de rendimiento, como legales que se asocian al exponer los datos transportados en el SSL.

5.6.1.2 Correcto diseño de la plataforma y planificación de procedimientos. Un buen diseño de infraestructura del servicio se da por los datos recopilados en el monitoreo y conocimiento de la plataforma. En parte cuando se tiene la magnitud de los equipos; es posible proporcionar para que el nivel de carga sea mayor y que soporte niveles superiores de lo normal, haciéndoles menos vulnerables a los ataques. El sobredimensionamiento es una medida que tiene costos altos y esto es de tener en cuenta.

A la hora de prevenir ataques *DoS*, se hace posible que se deshabiliten funcionalidades que no son usadas y que pueden ser manejadas como línea de ataque. Un ejemplo seria la desactivación del comando *monlist* en los servidores NTP o los de recursividad en los servidores DNS. Cuando los elementos del servicio lo admiten, es bueno limitar el número de conexiones y de nuevas conexiones por segundo, tanto para el total como para usuarios exclusivos.
Como otra medida aplicable para minimizar los efectos del ataque *DoS*, es la de aplicar las configuraciones en las políticas de calidad de servicio (*QoS*) a los flujos del tráfico.

[33] BENCHIMOL, Daniel. Hacking desde cero conozca sus vulnerabilidades y proteja su información. Buenos Aires: fox andina, 2011. 192p

“La planificación de las acciones tomadas en caso de contingencia es un punto importante que podría tomarse como parte de la prevención, así como el estudio de la automatización de tareas en el caso de detección de ataque y puesta en marcha de contramedidas, de manera que se detecte y detenga el ataque antes de que este provoque daños al servicio”[34].

5.6.1.3 Realización de auditorías y corrección de vulnerabilidades. En este punto, como ultima prevención, deben efectuarse auditorías constantes para descubrir y reparar aquellas vulnerabilidades encontradas en los servicios. En dichas auditorías es necesario revisar configuraciones, pruebas de carga, actualizaciones de parches, sistemas y aplicaciones según sea indispensable.

5.7 EXPLOTACIÓN A BASES DE DATOS MAL CONFIGURADAS

En toda organización se hace necesario que existan bases de datos para guardar información esencial como por ejemplo la nómina, los sistemas de información, las finanzas, etc. y es frecuente hallar en las BD las cuentas y parámetros que traen su configuración predeterminada. Sumado a esto se da que falte algún parche de actualización, lo que deja vulnerable las BD. Un hacker buscara estos puntos inseguros en las bases de datos como primera medida, verificando como comprometer la seguridad, por eso en las bases se hace obligatorio que las compañías estén muy pendientes de los parches no aplicados y de las vulnerabilidades detectadas.

> Las evaluaciones de configuración deben proporcionar una imagen clara del estado actual de la configuración de los sistemas de datos. Estas evaluaciones también deben identificar las bases de datos que no cumplan con las políticas de configuración definidas. Cualquier parche de seguridad no aplicado debe instalarse lo antes posible. Si se descubre una vulnerabilidad y el parche aún no está disponible, ya sea porque el proveedor no lo ha proporcionado o porque todavía no se ha instalado, se debe implementar una solución de parche virtual. Este tipo de solución bloquea cualquier intento de explotar estas vulnerabilidades. Por lo tanto, al minimizar el plazo de exposición con parches virtuales se protege a la base de datos contra los intentos de explotación de sus vulnerabilidades hasta que se instala un parche[35].

---

[34] ARIZMENDI ALONSO, Luis Javier. Ataques DoS y DDoS, prevención, detección y mitigación. [Online]. 2014.[Citada: 21 mayo 2020]. http://luisarizmendi.blogspot.com/2014/03/ataques-dos-y-ddos-prevencion-deteccion.html

[35] IMPERVA. Las diez principales amenazas para las bases de datos. [Online]. [Citada: 15 marzo 2012]. https://es.slideshare.net/Imperva/las-diez-principales-amenazas-para-las

5.8 VULNERABILIDADES DE PROTOCOLO DE COMUNICACIÓN

En las bases de datos se ha visto un ascendente crecimiento de fallas relacionados con el protocolo de comunicaciones. La solución a este problema es de competencia de los proveedores de bases de datos. IBM y Oracle han desarrollado parches que tienen que ver con este protocolo dando buenos resultados a sus bases de datos.

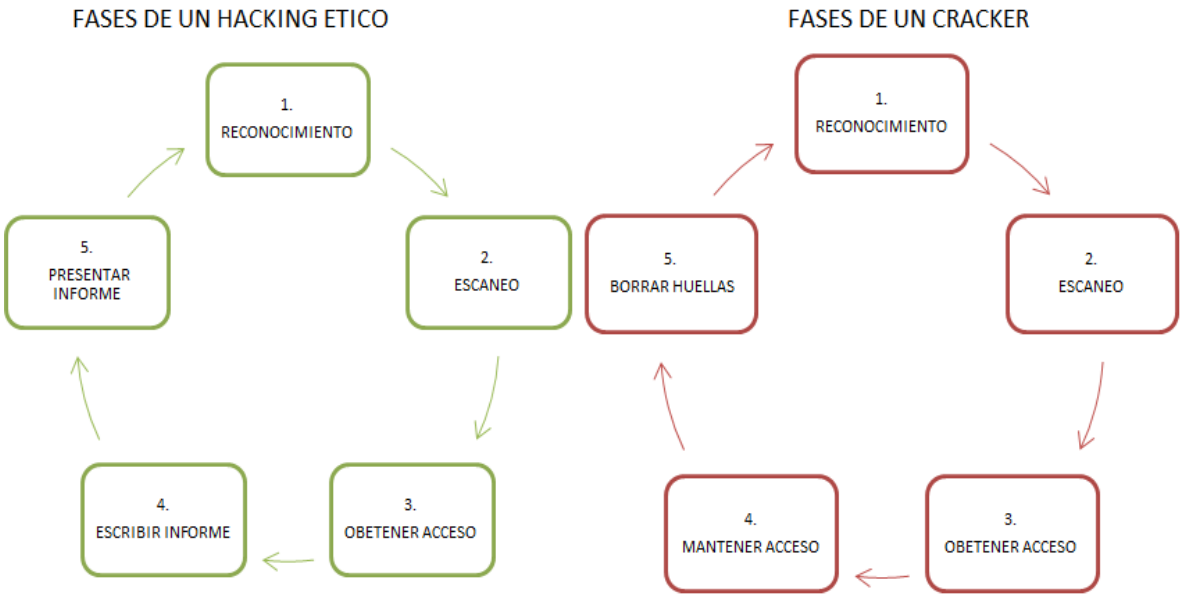
“Los ataques de protocolo de comunicación de base de datos se pueden combatir con tecnología denominada validación de protocolo. La tecnología de validación de protocolo esencialmente examina (desarma) el tráfico de la base de datos y lo compara con los valores esperados. En caso de que el tráfico activo no cumpla las expectativas, se pueden tomar medidas de alerta o bloqueo”[36].

[36] Ibid.,

6 FASES DEL HACKING ÉTICO

Tanto el Hacker ético como el cracker, deben ejecutar unas fases o seguir un orden en el momento de realizar un hacking o una intrusión a un sistema. En la Figura 10 se puede ver las fases de cada uno de los *hackers* representados en un ciclo que se denomina círculo del *hacking*.

Figura 10. Fases de un hacking



Fuente: Autor.

Como se logra observar el *hacker* ético sigue el proceso de las fases del cracker, pero solo llegando hasta la fase 3, a continuación se describen las fases así:

6.1 RECONOCIMIENTO

En esta fase se encuentra lo concerniente a la preparación y captura de información, a través de la investigación y levantamiento de información del objetivo. Es aquí donde se debe colocar el mejor esfuerzo para que todo lo indagado sobre el cliente o la victima sean de la mejor calidad para la auditoria. En el reconocimiento se pueden dar 2 técnicas, que son: el reconocimiento activo y el reconocimiento pasivo.

Reconocimiento pasivo: es donde no se tiene ningún tipo de contacto con el objetivo, es decir se buscan otras estrategias para obtener la información. Por

ejemplo se puede obtener información a través de los buscadores de internet como Google que es la más utilizada, rápida y asertiva. Otras opciones pueden ser la de analizar (redes, protocolos o paquetes) a través del *sniffing* de red, buscando en la basura, búsqueda en bases de datos de internet como *Who-Is*.

Reconocimiento activo: en el que se da una adquisición e intercomunicación directa con el cliente para obtener la información, que puede ser a través de la ingeniería social, escaneo de puertos, barridos de ping y mapeo de la red para identificar equipos de comunicaciones que pueden encontrarse. Lo importante en esta fase es analizar bien la información que fue recolectada para así poder diseñar un buen planteamiento para realizar el ataque con exactitud.

6.2 ESCANEO

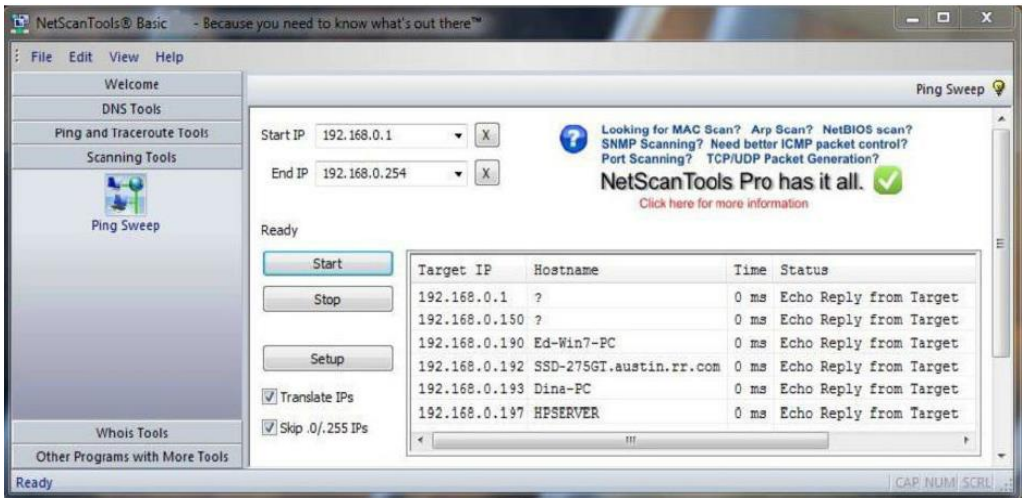
Fase en la que el hacker toma la información que fue recolectada de la fase anterior e identifica las vulnerabilidades, para antes de enviar el ataque. En este punto ya por lo menos se debe saber el rango de direcciones IP, si es *hacking* externo, si es *hacking* interno se debe haber detectado hasta las IP de las subredes de la organización que se va a auditar.

El siguiente paso será validar que equipos se encuentran activos, puertos abiertos, nombres de los equipos, sistemas operativos que manejan, software, cuentas de usuario, etc. Entre los recursos que el auditor puede utilizar se encuentran los *ping-sweepers* para barrido de *ping* o el *TCP-ping* que además ayuda a evaluar qué equipo está activo, NMAP para escaneo de puertos donde se conocerá el estado del puerto:

- Abierto. Puerto disponible que escucha conexiones hacia algún servicio.
- Cerrado. Puerto no disponible, aunque sea accesible la aplicación no responde a peticiones de conexión.
- Filtrado. Aquel puerto al que no es posible alcanzar ya que existe un aparato en medio que filtra paquetes como puede ser el *router* o *firewall*.

En la Figura 11 se visualiza un escaneo a través de una herramienta de *ping* para detectar equipos a través de IP.

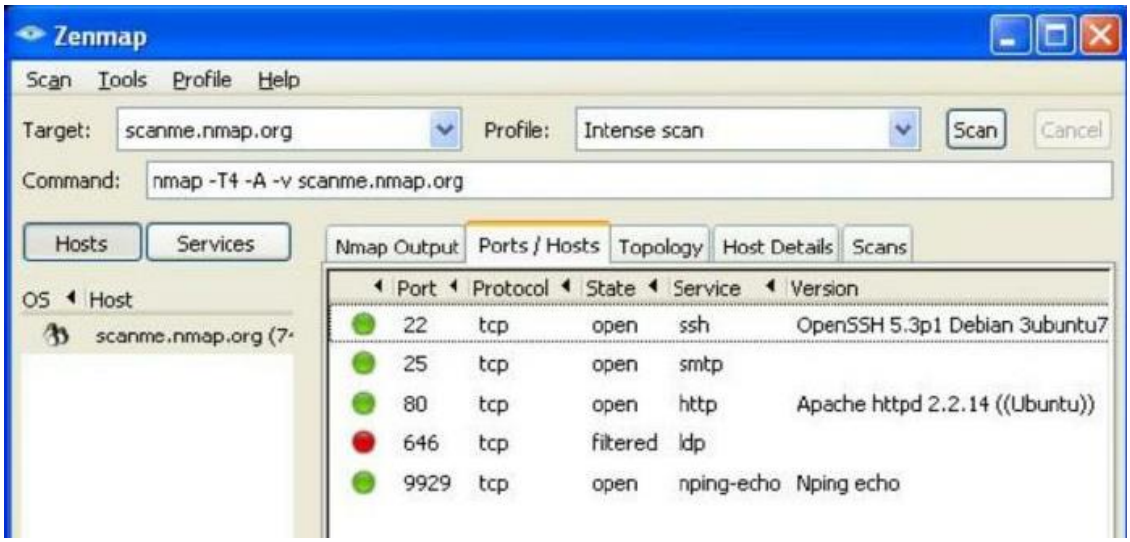
Figura 11. Escaneo con herramienta de ping



Fuente: ASTUDILLO, Karina B. Hacking ético 101, cómo hackear profesionalmente en 21 días o menos! 2013. Registro IEPI, certificado No. GYE-004179

Llegado el caso que no sea posible la detección de equipos por medio del *ping* se puede utilizar un escaneo de puertos y en la Figura 12 se puede observar cómo sería una detección de puertos y el estado de los mismos.

Figura 12. Escaneo de puertos



Fuente: ASTUDILLO, Karina B. Hacking ético 101, cómo hackear profesionalmente en 21 días o menos! 2013. Registro IEPI, certificado No. GYE-004179.

6.3 OBTENER ACCESO

Es donde se lleva a cabo la explotación o el *hacking* como tal. Se efectúa la incursión al sistema rompiendo esas vulnerabilidades encontradas en la fase de escaneo. La explotación puede hacerse por medio de la red LAN, inalámbrica o sin conexión. Las técnicas que se pueden aplicar en esta fase son:

• *Exploits*: se puede dar de dos formas, manual o automática. En el cuadro 2 se muestran estos mecanismos de explotación.

Cuadro 2. Mecanismos de Hacking

Exploración manual	Exploración automática
El *hacker* puede utilizar un método de explotación revelado y difundido por un tercero o usar un *exploit* desarrollado por él mismo.	El *hacker* está limitado usualmente a utilizar solamente los *exploits* incluidos con la herramienta de explotación utilizada.
El *hacker* tiene mayor control sobre lo que desea explotar y cómo ejecutar el *exploit*	La forma de ejecución del *exploit* depende de la implementación realizada por el desarrollador.
Se requiere conocimiento sobre protocolos TCP/IP; manejo de comandos y entender el manejo interno de la seguridad de los S.O como *Windows*, *Unix*, *Mac* Os, entre otros; saber programar en diferentes lenguajes como C, *Assembler*, *Java*, etc; y entender el funcionamiento del software que se pretende explotar.	El *hacker* solo necesita conocer cómo usar la herramienta de explotación. Sin embargo, si se trata de un *hacking* ético profesional, el consultor debería tener además sólidas bases de *networking*, sistemas operativos y seguridad informática.
Con este mecanismo el hacking se ejecuta usando comandos, conexiones a puertos, enviando paquetes de datos personalizados y/o programando código de bajo nivel o scripts.	El hacker usa un software de explotación, generalmente desarrollado por un tercero que puede o no estar parametrizado y básicamente elige uno o varios tipos de exploits, escoge el objetivo y los ejecuta sin mayor intervención.

Fuente: Autor

• Ataques *man in the middle*. Ataque hombre en el medio donde se puede capturar tráfico sensible.

• Secuestro de sesión.
• Romper o adivinar claves utilizando diccionarios a través de, *Dictionary Attack* o *Brute Force Attack*.

6.4 ESCRIBIR INFORME

Esta fase es donde se prepara el escrito, tomándose el tiempo para recopilar todo lo investigado en las anteriores fases, como hallazgos e identificación de riesgos de todos los equipos analizados. Para llegar a obtener un buen informe se pueden seguir unos pasos como pueden ser el de tener, una bitácora, imágenes, llevar registro de todo lo hallado, ayudándose siempre con aplicaciones de documentación ya sean del computador o del celular.

6.5 PRESENTACIÓN INFORME

Para concluir en esta última fase el objetivo es mostrar los resultados del proceso de ejecución de las pruebas llevadas a cabo en todas las fases. Lo más aconsejable es trabajar con formatos que ahorren tiempo en el instante de construir el informe final, esto ayudara a tener una mejor concentración en lo realmente importante, que es transmitir detallada y comprensiblemente lo que fue descubierto, sus resultados y sugerencias.

Se debe tomar en cuenta que el informe va a ser leído no solo por personal con conocimientos técnicos sino por directivos de alto nivel, por lo que hay que considerar que el documento cuente con un resumen ejecutivo, que este ubicado en los primeros apartes del informe. Desde luego lo esencial de este resumen ejecutivo es que tenga un lenguaje entendible, claro sin utilizar redacción técnica. Este resumen debe proporcionar un contexto amplio de lo encontrado en la auditoria, pero sin entrar en particularidades. Todo puede llevar inclusión de imágenes según lo considere el auditor.

7. METODOLOGÍAS DE HACKING ETICO

Para las personas que estudian sobre la seguridad informática es interesante aprender acerca del *Hacking* ético. Debido a las situaciones de ataques en la actualidad una empresa tiene la necesidad de contar con especialistas en seguridad y explorar las vulnerabilidades que se puedan presentar para realizar controles que mejoren la seguridad de los sistemas. A continuación, se plantean las metodologías que se pueden abordar para seguridad en bases de datos.

7.1 OSSTMM (OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL)

En su traducción al español conocida como el manual de la metodología abierta de testeo de seguridad, tiene una alta calidad y un buen orden en sus contenidos. Posee la facultad de manejar secciones con una serie de módulos particulares para integrar tareas en revisión de puntos de seguridad de la información, de los procesos, de las comunicaciones, física, inalámbrica y tecnologías de internet.

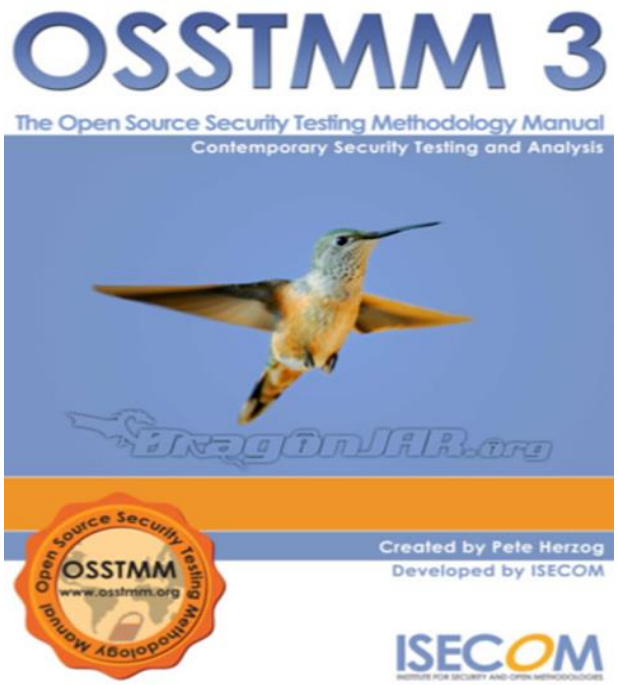
Un aspecto considerable es que esta metodología llega no solo a lo técnico y de procedimiento de seguridad, sino que se encarga de normativas como las acreditaciones de los profesionales encargados del testeo, formatos de conclusiones, normas y tiempos a tener en cuenta en cada tarea. Cuenta con la incorporación de un concepto como el de valores de evaluación de riesgo que admite discriminar y separar las diferentes problemáticas.

La metodología OSSTMM se apoya en 7 fases que se encuentran alineadas con lo que fue explicado en el capítulo de las fases del *hacking* ético y que son:

- Descubrimiento: Obtención y análisis de la documentación del sistema existente.
- Verificación de enumeración: Pruebas del sistema operativo, la configuración y los servicios en comparación con la documentación del sistema.
- Investigación y verificación de vulnerabilidades: Investigación y análisis de vulnerabilidades mediante pruebas de penetración.
- Prueba de integridad: prueba de integridad de todos los resultados.
- Mapeo de seguridad: mapeo de la seguridad medida. Mapeo de los resultados en sistemas y servicios.
- Valor de evaluación de riesgos: cálculo del RAV y clasificación de riesgos de las debilidades encontradas.
- Informes: mapeo de los resultados y entrega de recomendaciones

ISECOM (*Institute for Security an Open Methodologies*) creo OSSTMM, en la actualidad se encuentran en la versión 3, siendo re-escrita totalmente, el mapa de seguridad re-ordenado, con nuevos conceptos de *dashboard* y más relevancia y destacada descripción en los RAVs o Valores de Evaluación de Riesgo. En la Figura 13 se observa el logo de la última versión de la metodología OSSTMM.

Figura 13. Logo OSSTMM 3



Fuente: Dragonjar. OSSTMM (Open Source Security Testing Methodology Manual) 3.0. [Online]. https://www.dragonjar.org/osstmm-open-source-security-testing-methodology-manual-3-0.xhtml

7.1.1 Ámbitos y alcance de OSSTMM. Esta metodología está encaminada a cualquier tipo de organización, sin importar su tamaño, su seguridad y tecnología. El propósito de OSSTMM es el de establecerse como guía de desarrollo de una auditoria para seguridad operacional (OPSEC), aplicando en cualquier ambiente que soliciten seguridad. OSSTMM relaciona aspectos como:

- “Estandarización a nivel de acreditación, presentando cinco certificaciones.
- Comercialización de los servicios ejecutados por los profesionales.
- Formalización de los resultados según las normas éticas y legales a cumplir.

- Planificación mostrando la trazabilidad y tiempos requeridos en cada una de las fases"[37].

7.1.2 Minuciosidad de OSSTMM. En la ejecución del test de intrusión, esta metodología es muy integra y cuidadosa, ya que para revelar fallos de seguridad basa su búsqueda de manera minuciosa en los distintos sistemas, evitando falsos positivos. En muchas ocasiones hay elementos insignificantes, que por sí solos no son un peligro, pero que al acumularse pueden implicar sentencias graves de seguridad.

7.1.3 Usabilidad de OSSTMM. Se puede valorar esta metodología en un nivel medio/alto de usabilidad, ya que se requiere de una buena preparación y conocimiento que en realidad cubre esta metodología con las certificaciones que recomienda. OSSTMM en la práctica es uno de los modelos más empleados por los profesionales que se ocupan de la seguridad de los sistemas, suministrando una reseña esencial en el sector. La licencia de esta metodología es OML (*Open Methodology License*), es decir, se admite su libre uso, el disfrute de mecanismos de código abierto y exploración pública.

7.1.4 Métricas de OSSTMM. Las medidas de esta metodología en la práctica son objetivas e indispensables para evaluar el riesgo. Son medidas técnicas, demostrables e incuestionables, que muestran el siguiente factor de riesgo del sistema. Este método cuenta con el RAV (*Risk Assesment Values*) que son los valores de evaluación del riesgo y que se puntualizan en cada módulo, teniendo como principal finalidad la de calcular la degeneración de la seguridad con relación al eje de tiempo. RAV emplea componentes de adaptación como son, seguridad operacional, limitaciones y comprobación de pérdidas para la explotación de resultados finales de manera porcentual.

7.1.5 Ventajas de OSSTMM. Dentro de las ventajas que se pueden destacar en la metodología, se encuentran:

- Tiene habilidad de adaptación y reacción, por ser una metodología abierta, revisable y pública. Es el método más actualizado de los aquí estudiados.
- Sus estándares internacionales se suplementan y cumplen con la ISO 27001 de seguridad de la información y las guías de mejores prácticas ITIL.

[37] FUERTES MAESTRO, Antonio. Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad. Madrid, 2014, 85p. Trabajo Fin de Máster (Máster en seguridad informática). Universidad Internacional de la Rioja.

- Admite evaluar el progreso de la seguridad, alcanzando unas medidas de los productos de las pruebas, basado en lo realizado y lo obtenido y no en un análisis teórico del riesgo.
- A nivel mundial es una metodología de referencia aceptada para ejecutar pruebas de intrusión.
- Su estudio está relacionado al crecimiento estructurado y ordenado, con condición profesional facultado para la automatización de tareas.
- Es una metodología de alto nivel, que sin importar la tecnología muestra las tareas a llevar a cabo. Esto contribuye dándole mayor supervivencia y flexibilidad.
- Con la metodología OSSTMM, se tiene la ventaja que al manejarla se alcanza un profundo entendimiento de la interconexión de los procesos, las personas, el software y los sistemas.
- Es una metodología que no solo hace énfasis a los medios técnicos en al área de la seguridad, sino que a su vez evalúa las competencias de los encargados de las pruebas de testeo.

7.1.6 Limitaciones de OSSTMM. Como limitantes en la metodología se pueden resumir estos puntos:

- La versión 3 de OSSTMM y la versión 2 no son compatibles.
- Al no recomendar herramientas, el auditor debe completar su trabajo con aquellas que tenga experiencia.
- No es una metodología sencilla para novatos, ya que el auditor debe apoyarse en su destreza y creatividad.
- Dado que la metodología OSSTMM no admite una división entre la recopilación de datos activos y la comprobación del producto alterado; así como no diferencia entre verificaciones activas y pasivas; el complementarse con otros métodos de intrusión sería complejo porque el proceso de enlazar ciertas partes sería lento.

7.2 ISSAF (INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK

Esta metodología de testeo que al traducirlo al español sería Marco de Evaluación de Seguridad de Sistemas de Información, es uno de los *frameworks* más atrayentes que ejecuta un minucioso análisis por completo de aquellos aspectos que pueden perjudicar el testeo de seguridad. Fue creada por la OISSG (*Open Information System Security Group*). ISSAF tiene la información organizada alrededor de unas pautas llamadas “criterios de evaluación” donde cada área de aplicación fue escrita y revisada por expertos. Estos criterios son:

- “Una descripción del criterio de evaluación

- Puntos y Objetivos a cubrir
- Los pre-requisitos para conducir la evaluación
- El proceso mismo de evaluación
- El informe de los resultados esperados
- Las contramedidas y recomendaciones
- Referencias y Documentación Externa"[38]

Para estructurar de forma ordenada los trabajos de testeo, estos criterios de evaluación, se catalogan desde lo más general, como son los criterios esenciales de la Administración de Proyectos de Testeo de Seguridad, hasta métodos tan precisos como la realización de pruebas de Inyección de Código *SQL* o como las tácticas del *Cracking* de contraseñas.

ISSAF dentro de los procesos con TI de alto nivel está como los preferidos por los departamentos de TI en el mundo, en cuanto a evaluación de la seguridad y la OISSG quiere posicionarlo como esa base de prestigio a los sistemas de seguridad de la información de una organización, con todas las especificaciones acreditadas por profesionales de la seguridad en todo el mundo.

La metodología ISSAF está proyectada a evaluar los sistemas, la red de trabajo e inspección de aplicaciones, se enfoca sobre 3 fases y 9 pasos para la evaluación como se puede ver en la figura 14, que las fases son:

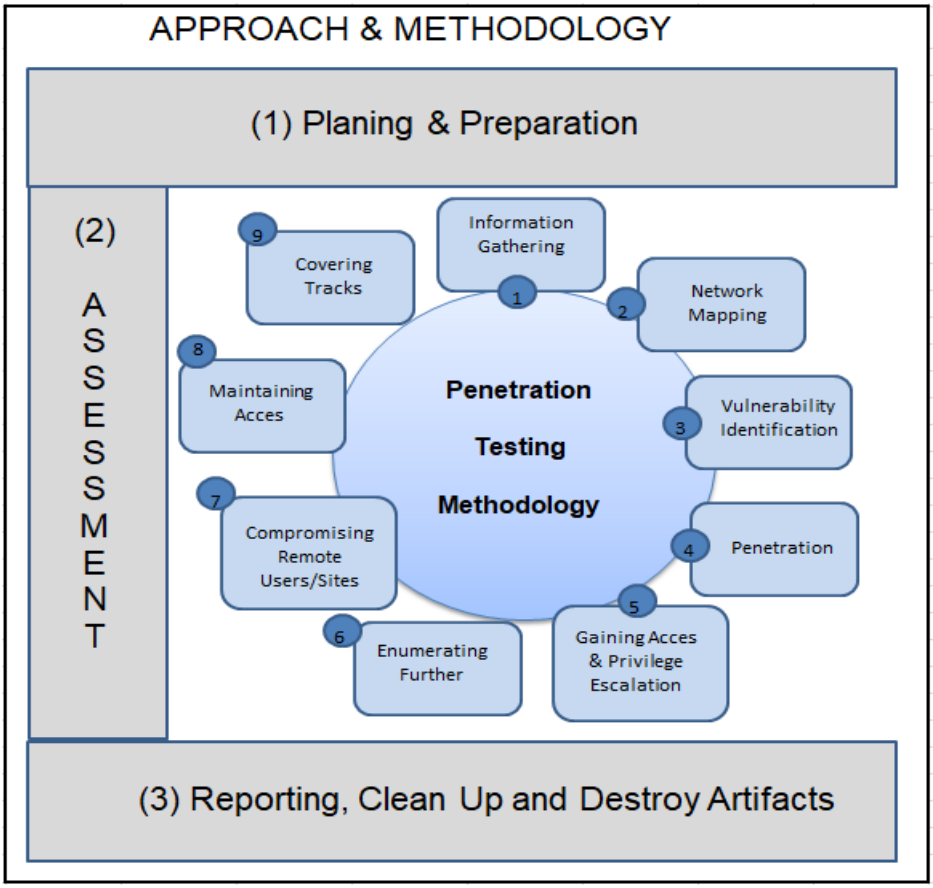
- Planificación y preparación:
- Evaluación
- Reportes, Limpieza y Destrucción de objetos

Y en los 9 pasos están:

- Recolección de información
- Mapeo de la red de trabajo
- Identificación de vulnerabilidades
- Penetración
- Obtener acceso y escalada de privilegios
- Enumeración adicional
- Comprometer usuarios remotos y sitios
- Mantener el acceso
- Cubrir rastros

[38] DIAZ BARRERA, Enny Rocio. Análisis de metodologías para pruebas de penetración mediante ethical hacking. Yopal, 2018, 97p. Trabajo de grado (Especialista en Seguridad Informática). Universidad – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Figura 14. Fases evaluación ISSAF



Fuente: Autor

En esta metodología hay un punto importante a tener en cuenta y es el de no dejar que el *framework* se des-actualice, porque muchas de las herramientas que se manipulan pueden quedar obsoletas, sobre todo en las técnicas de testeo directas destinadas a determinados productos o tecnologías. No es que esto sea una desventaja sino que el auditor debe tenerlo en cuenta en el momento de usar la metodología.

7.2.1 Ámbito y alcance de ISSAF. La metodología ISSAF es amplia, abarcando un análisis de seguridad en casi todos los entornos de cualquier entidad, sin importar su dimensión. Esta aplicación admite análisis de sistemas en equipamientos de red, sistemas de gestión de bases de datos, sistemas operativos y aplicaciones.
Otro componente significativo de ISSAF es la ejecución de requerimientos normativos y buenas prácticas. Es una metodología que se dedica al test de intrusión, en una de las cinco certificaciones que presenta.

7.2.2 Meticulosidad de ISSAF. Esta metodología explica al detalle cada procedimiento, partiendo de lo general a lo más detallado, vinculando cada tarea aún de las aplicaciones de código abierto, es por esto que ha de suponerse que el *framework* tiene que estar actualizado, para que los productos no queden inservibles.

7.2.3 Usabilidad de ISSAF. Es altamente usada, y requiere de un estudio medio de la misma para su ejecución. El ciclo de intrusión envuelve todos los periodos necesarios, aportando gran nivel de detalle, lo que la hace fácil de manejar y provechoso para los auditores novatos. ISSAF está bajo una licencia de código abierto, lo que la faculta para su uso libre.

7.2.4 Métricas de ISSAF. Las mediciones de riesgo en esta metodología se encuentran más en el sentido teórico que práctico. Por eso es posible basarse en la siguiente formula:

Riesgo = Valor activo*Amenaza*Vulnerabilidad

Donde el valor activo (es cualitativo y cuantitativo), la amenaza o amenazas que pueden acarrear daños (efecto cualitativo de probabilidad) y la vulnerabilidad que es el fallo en un sistema en el cual una amenaza puede explotarla y da un (efecto cualitativo) llegando a dañar el activo analizado.

7.2.5 Ventajas de ISSAF. Dentro de las virtudes de la metodología se pueden resumir en:

- ISSAF ha sido desarrollado desde cero, lo que la hace tener un esquema de ideas independiente y neutro de aquellos productos actuales del mercado. Por ser un mecanismo abierto, las personas de seguridad informática pueden acceder a un certificado por parte de la corporación que la creó.
- Su uso es alto, por realizar una minuciosa explicación de los pasos a seguir en las pruebas, los informes y los resultados finales. Como es un método lineal, se facilita el manejo para los auditores novatos.
- “Aporta mucha información y soporte acerca de cómo implementar estándares y buenas prácticas del sector TI tales como IEC/ISO 27001:2005(BS7799), Sarbanes *Oxley* SOX404, *CoBIT*, SAS70 y COSO”[39]

[39] FUERTES MAESTRO, Antonio. Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad. Madrid, 2014, 85p. Trabajo Fin de Máster (Máster en seguridad informática). Universidad Internacional de la Rioja.

7.2.6 Limitaciones de ISSAF. Se pueden encontrar las siguientes restricciones:

- No hay una delimitación de la magnitud del test de intrusión y esto puede llevar a un desorden en las restricciones para la ejecución del test.
- En el momento de la valoración, según la indicación del manual técnico, ISSAF precisa de herramientas puntuales, que obligan a que la metodología dependa de tecnologías existentes y de otras aplicaciones.
- Desde el año 2006 ISSAF no ha vuelto a realizar actualizaciones, por lo que puede dar una sensación de que ya es obsoleta en la parte de test de intrusión, no siendo el caso de la parte de valoración genérica.
- En cuanto a la seguridad en sus aspectos profundos no cubre asuntos de *cloud computing* y protección de datos.

7.3 ANÁLISIS DE LAS METODOLOGÍAS DE HACKING ÉTICO

Una vez estudiadas las metodologías de hacking para bases de datos, se puede encontrar unos criterios que ayudan a realizar la escogencia de una metodología. Entre dichos criterios que se pueden tener en cuenta están:

- Que sea comprensible y lógica.
- Que sea estándar en sus métricas y que permita hacer los análisis de manera repetitiva siguiendo los mismos procesos, tratando de que se aplique lo menos posible el criterio personal del evaluador.
- Que posea niveles de riesgo que cuantifiquen el resultado.
- Que sea implacable y evite los falsos positivos, ya que esto produciría una incorrecta percepción de seguridad.
- Que proporcione estándares internacionales.
- Que tenga actualizaciones recientes y tenga vigencia en la actualidad.
- Que trabaje en diferentes tecnologías y ambientes, ya que hay algunas por ejemplo que están desarrollados y orientados a la red o a aplicaciones web.
- Y por último que sea *ethical.*

8. CONCLUSIONES

• A través de este trabajo se logró investigar y analizar la información concerniente a las metodologías que existen en cuanto al *hacking* ético en BD, entendiendo que cada vez los ataques cibernéticos se incrementan y son más sofisticados, concluyendo con esto que las organizaciones deben evolucionar en sus tecnologías y en la seguridad tanto de sus redes como en sus bases de datos para que sean menos propensas a ser vulnerables.

• Dentro de las metodologías estudiadas según el análisis lo que ayuda a que las bases de datos tengan menos vulnerabilidades y una mayor seguridad es siempre ir más adelante y esto se puede dar cuando una organización contrata un *hacker* para que realice de forma profesional un *hacking* descubriendo anticipadamente los errores que pueden tener los sistemas o la infraestructura tecnológica. Además ayuda a estar preparado ante una eventualidad de ataque, porque al realizar pruebas de intrusión la empresa estará más a la vanguardia y actualizada en las formas de ataques existentes y fallas que la misma empresa pueda tener.

• Se investigan y analizan sobre aquellas vulnerabilidades más comunes en una base de datos y por las cuales se pueden presentar riesgos con la seguridad, llegando a entender que medidas son las que se deben tomar al respecto.

• Se analizaron los tipos de hackers y herramientas que existen para poder llevar a cabo un *hacking* ético, en realidad es bueno poder contar con un *hacker* profesional dentro de una organización, para que colabore con la seguridad interna, monitoreando aquellas fallas que se puedan presentar en los sistemas, incluyendo configuraciones en BD, presentando informes regularmente de los resultados para tomar los correctivos necesarios.

9. RECOMENDACIONES

- Se deben realizar auditorías de seguridad en las compañías con periodicidad adecuada recordando que la seguridad debe ser gestionada.

- Es bueno en las empresas realizar o tener en cuenta no solo el método de seguridad en la parte externa o perímetro de la red sino también tener seguridad en la parte interna de la organización y sobre todo en los equipos donde se encuentren las BD ya que allí en muchas oportunidades no se toma las medidas respectivas del caso.

- Los equipos de comunicaciones que se encuentran dentro de la seguridad de las organizaciones deben contar con las últimas actualizaciones o parches y las configuraciones deben ser las mejores en cuanto a detección de vulnerabilidades.

- Se hace necesario que el DBA continuamente tenga las BD actualizadas en parches, verificar que la configuración de seguridad siempre sea la correcta y que si tiene errores se corrijan de inmediato o lo más pronto posible dado el caso.

BIBLIOGRAFÍA

ALONSO. Bases de datos relacionales [Online]. 2006 [Citada: 13 octubre 2018]. https://www.um.es/geograf/sigmur/temariohtml/node63_mn.html

ANGUIANO MORALES, Jorge. Características y tipos de bases de datos. [Online]. IBM Developers, 2014 [Citada: 30 junio 2018]. https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/index.html

ARIZMENDI ALONSO, Luis Javier. Ataques DoS y DDoS, prevención, detección y mitigación. [Online]. 2014.[Citada: 21 mayo 2020]. http://luisarizmendi.blogspot.com/2014/03/ataques-dos-y-ddos-prevencion-deteccion.html

ASTUDILLO, Karina B. Hacking ético 101, cómo hackear profesionalmente en 21 días o menos! 2013. Registro IEPI, certificado No. GYE-004179

ASSUMPCAO G, Bernardo. STAMPAR, Miroslav. Sqlmap Automatic SQL injection and database takeover tool. [Online]. http://sqlmap.org/

AVILA JIMENEZ, Cristian. La historia detrás de cinco 'hackers' colombianos y sus delitos. [Online]. Colombia: eltiempo.com, 2016 [citada: 6 octubre 2019]. https://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

BACA URBINA, Gabriel. Introducción a la seguridad informática. México: Patria, 2016. p.12.

Bases de datos y sus vulnerabilidades más comunes. [Online]. Telefónica Company. 2015 [Citada: 6 junio 2019]. https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

BARRERA, Arturo. 6 principales tipos de hackers y sus perfiles [Online]. Next U. [Citada: 18 febrero 2020] https://www.nextu.com/blog/tipos-de-hackers/

BENCHIMOL, Daniel. Hacking desde cero conozca sus vulnerabilidades y proteja su información. Buenos Aires: fox andina, 2011. 192p.

CABALLERO QUEZADA, Alonso Eduardo. Introducción a OSSTMM (Open Source Security Testing Methodology Manual). [Online]. 2015. [Citada: 25 abril 2020] http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual

CALAMEO. Bases de datos. [Online]. [Citada: 19 septiembre 2018] https://es.calameo.com/books/004304179b1c20a4b3659

CATOIRA, Fernando, Vulnerabilidades, estadísticas e impacto. [Online], instituto nacional de tecnologías de la comunicación, [Citada: 31 julio 2012]. https://www.welivesecurity.com/la-es/2012/07/31/vulnerabilidades-estadisticas-e-impacto/

CATOIRA, Fernando. Auditando un servidor web con nikto, argentina, 2012. https://www.welivesecurity.com/la-es/2012/06/05/auditando-servidor-web-nikto/

COBO YERA, Ángel. Diseño y programación de bases de datos. Madrid: Visión libros. 116p. ISBN: 978-84-9821-459-8.

Conceptos básicos para entender Internet: El Hacking. [Online] http://blogs.enfemenino.com/ciberderecho/2016/01/11/conceptos-basicos-internet-hacking/

Conceptos básicos sobre bases de datos. [Online]. Colombia: Microsoft, [citada: 19 septiembre 2018]. https://support.office.com/es-es/article/conceptos-b%C3%A1sicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204
Consejos para crear una contraseña perfecta y memorable. 2015. https://blog.acens.com/general/contrasena-perfecta-memorable/

Conoce los tipos de hacker y su forma de operar. En: 24 Horas, Bogotá. 2017 [Citado: 14 julio 2018] https://www.24horas.cl/tendencias/ciencia-tecnologia/conoce-los-tipos-de-hackers-y-su-forma-de-operar--2299770

Consejos para crear una contraseña perfecta y memorable. 2015. https://blog.acens.com/general/contrasena-perfecta-memorable/

DACCACH T. José C. Ley de delitos informáticos en Colombia. [Online], En: Delta asesores. [Citado: 20 mayo 2019] https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Datos no relacionales y NoSQL. [Online]. En: Microsoft Azure. [Citado: 12 febrero 2018] https://docs.microsoft.com/es-es/azure/architecture/data-guide/big-data/non-relational-data

Definición de Base de datos. [Online], 2009 [Citada: 29 agosto 2018]. https://sistemas.com/base-de-datos.php

DELGADO, Esmeralda. Introducción al desarrollo de la base de datos [online]. http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro14/11_caractersticas_de_la_base_de_datos.html

DIAZ BARRERA, Enny Rocio. Análisis de metodologías para pruebas de penetración mediante ethical hacking. Yopal, 2018, 97p. Trabajo de grado (Especialista en Seguridad Informática). Universidad – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Digital Guide IONOS. Bases de datos relacionales: el modelo de datos en detalle. [Online]. [Citada: 9 mayo 2019]. https://www.ionos.mx/digitalguide/hosting/cuestiones-tecnicas/bases-de-datos-relacionales/

División ComputerForensic. Definición de Delito Informático. [Online]. [Citado: 14 abril 2020] http://delitosinformaticos.info/delitos_informaticos/definicion.html

Dragonjar. OSSTMM (Open Source Security Testing Methodology Manual) 3.0. [Online]. https://www.dragonjar.org/osstmm-open-source-security-testing-methodology-manual-3-0.xhtml

ECHEVERRY, Juan. PULGARÍN, Luis. Arquitectura híbrida. [Online]. Universidad de Santa Rosa Cabal. 2015 [Citado: 23 febrero 2019]

http://arquitecturashibridas.blogspot.com/2015/02/que-es-una-base-de-datos-hibridos-una.html

ELDIARIO.ES. Los hackers llevan sombrero blanco, gris y negro. [Online]. España, 2016. [Citada: 22 abril 2020] https://www.eldiario.es/tecnologia/hackers-llevan-sombrero-blanco-negro_0_505349668.html

EL ESPECTADOR. En busca de cura para los delitos informáticos. [Online], 13 mayo 2014 [citado: 14 abril de 2020]. http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170

El Hacking Ético y su importancia para las empresas. [Online]. En: Enter, Bogotá, 2014 [Citado: 28 febrero 2019] https://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

El secuestro de información desangra a las empresas del país. [Online], En: EL portafolio, Colombia. [Citado: 29 Enero 2019] https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

ETL-TOOLS.COM. Database Browser. [Online]. [Citado: 22 abril 2020] https://www.etl-tools.com/database-browser/overview.html

FLOREZ R, Jorge A. Metodología para realizar hacking ético en bases de datos para positiva compañía de seguros S.A. en la ciudad de Bogotá, Universidad Nacional Abierta y a Distancia (UNAD) [online]. Bogotá, 2017 [citada: 20 noviembre 2018] https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17375/1/19418118.pdf

FUERTES MAESTRO, Antonio. Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad. Madrid, 2014, 85p. Trabajo Fin de Máster (Máster en seguridad informática). Universidad Internacional de la Rioja.

GARCIA CARVAJAL, Miguel José. Database Main Threats Analisys Using MS SQL Server. [Online]. 2013.[Citada: 18 mayo 2020] https://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo9_paper_10.pdf

GARCÍA MARTÍN, David. Inyección SQL [Online], En: redeszone, Colombia, 2010 [Citada: 06 octubre 2018]. https://www.redeszone.net/seguridad-informatica/inyeccion-sql-manual-basico/

GARCIA M.J., Database Main Threats Analisys Using MS SQL Server. Bucaramanga: Universidad Cooperativa de Colombia, [Online], https://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo9_paper_10.pdf

GARCIA SANCHEZ, María. Bases de Datos. [Online] http://cursos.aiu.edu/base%20de%20datos%20SOG/Sesi%C3%B3n%201.pdf

GÓMEZ I, Camilo. Diseño de metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL [Online], (Universidad Militar Nueva Granada). [Citada: noviembre 2011] https://repository.unimilitar.edu.co/bitstream/handle/10654/7212/GomezGonzalezIvanCamilo2012.pdf;jsessionid=63C67DB043F7ED4DC6FCE9A571299F94?sequence=2

Hacking ético: mitos y realidades. [Online], En: revista seguridad unam mex, México: universidad nacional autónoma de México. [Citado: 2018] https://revista.seguridad.unam.mx/numero-12/hacking-%c3%a9tico-mitos-y-realidades

Historia Nessus. Nessus. [Online]. [Citada: 17 marzo 2020]. https://es.wikipedia.org/wiki/Nessus

IBM Knowledge Center. Bases de datos relacionales. [Online]. 2009 [Citada: 30 Abril 2019] https://www.ibm.com/support/knowledgecenter/es/SSEPGG_8.2.0/com.ibm.db2.udb.doc/admin/c0004099.htm

IMF, Business School. Cuáles son las herramientas más usadas por los hackers. [Online] [Citado: 16 septiembre 2019]. https://blogs.imf-formacion.com/blog/tecnologia/cuales-son-las-herramientas-mas-usadas-por-los-hackers-201808/

IMPERVA. Las 10 amenazas principales de las bases de datos. [Online]. 2013 [Citado: 25 octubre 2018] http://www.redseguridad.com/actualidad/info-tic/imperva-identifica-las-10-amenazas-principales-de-las-bases-de-datos

Inyección SQL. [Online]. [2015]. https://www.avast.com/es-es/c-sql-injection

JUNTA DE ANDALUCIA. Metodología y Frameworks de testeo de la seguridad de las aplicaciones. [Online]. España; 2011. [Citado: 27 abril 2020] http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html

Las 10 grandes amenazas de seguridad en las bases de datos. [Online], En: TICbeat. 2013 [Citado: 17 abril 2018]. https://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/

La historia detrás de cinco 'hackers' colombianos y sus delitos. [Online], En: El tiempo, Bogotá, 2016 [Citada: 6 octubre 2019] https://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

La vanguardia. Hacktivistas: en el límite del bien. [Online]. [Citado: 23 mayo 2017]. En la vanguardia. [Actualizado: 27 septiembre 2018] https://www.lavanguardia.com/vida/junior-report/20170519/422741815247/hacktivistas-limite-bien.html

Ley 1273 de 2009. [Online] https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Ley 1273 de 2009. [Online] http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

LÓPEZ DE IPIÑA, Diego. Bases de datos no relacionales [online]. Madrid: Fundación Universidad Rey Juan Carlos. 2012 [citado: 4 julio 2018]. https://es.slideshare.net/dipina/nosql-cassandra-couchdb-mongodb-y-neo4j

Los 10 Principales Riesgos de Seguridad para las aplicaciones WEB según OWASP. [Online], [Citada: 1 abril 2019]. https://www.omatech.com/blog/2019/04/01/riesgos-de-seguridad-owasp/

MAULINI, Mauro. Desarrollo y Seguridad de Aplicaciones Web y Móviles. [Online]. 2012 [Citada: 13 junio 2018] http://tecnologiasweb.blogspot.com/2010/12/que-es-una-inyeccion-ldap.html

MENENDEZ, Maikel. BOLUFE, Mallelin. Ethical hacking: Test de intrusion. Principales metodologías. [Online], Ciudad de la Habana, 2009 [Citada: 13 mayo 2019]. https://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias2.shtml

Metodologías y herramientas de Ethical Hacking. [Online] 2013. [Citada: 15 febrero 2020] https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

MIERES, Jorge. Introducción al hacking ético, ética y legalidad. [Online]. 2013 [Citada: 19 de febrero 2019]. http://www.it-docs.net/ddata/863.pdf

MUÑOZ, Ana. ¿Qué es un hacker y que tipos de hacker existen? [Online]. En: Computerhoy, 2015 [Citada: 31 octubre 2019]. https://computerhoy.com/noticias/software/que-es-hacker-que-tipos-hacker-existen-36027

NEVADO C, María V. Introducción a la base de datos relacional. Pg. (22). [Online]. España: Madrid. 2014 [citada: 1 marzo 2019] https://books.google.com.co/books?id=0lUpB1lNUdIC&printsec=frontcover&dq=%22bases+de+datos+relacionales%22&hl=es&sa=X&ved=0ahUKEwj93Z2EsZbfAhWSuVkKHTvRDVUQ6AEIKDAA#v=onepage&q=%22bases%20de%20datos%20relacionales%22&f=false

OJEDA, Diego. Ataques a infraestructuras críticas. En: El Espectador, Bogotá. [Citada: 2 noviembre 2018] https://www.elespectador.com/tecnologia/puede-un-hacker-dejar-sin-luz-colombia-articulo-821696

OJEDA PEREZ, Jorge Eliecer. RINCON RODRIGUEZ, Fernando. ARIAS FLOREZ, Miguel Eugenio. DAZA MARTINEZ, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia [Online]. Bogotá. [Citada: 1 febrero 2010] http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Oracle. ¿Qué es una base de datos relacional? [Online]. [2019] https://www.oracle.com/co/database/what-is-a-relational-database/

OWASP, Inyección de código. [Online] https://www.owasp.org/index.php/Inyecci%C3%B3n_de_C%C3%B3digo

Qué es el hacking. [Online]. [2015]. https://www.avast.com/es-es/c-hacker

ROMERO CASTRO, Martha Irene. et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. Área de innovación y desarrollo, S.L. 2018. 121p.

SAFFADY, William. Informática documental para bibliotecas. Madrid: Díaz de santos, 1987. 123p. ISBN 84-86251-47-8.

SARMIENTO, William. RODRÍGUEZ, Elkin. Proyecto Trabajo de grado. Definición de una Metodología Personalizada de Hacking Ético, Pg. 27-30. [Online], [Citada: 15 junio 2019]. https://repository.ucatolica.edu.co/bitstream/10983/23377/1/Trabajo%20de%20Grado%20Seg.%20de%20la%20Informacion%20Final.pdf

Seguridad informática. [Online]. [Citado: 24 abril 2019] https://www.significados.com/seguridad-informatica/

SQLMAP. Automatic SQL injection and database takeover tool. [Online]. http://sqlmap.org/

Tecnologías información. Bases de Datos: Tipos, Usos y Beneficios. [Online] https://www.tecnologias-informacion.com/basesdedatos.html

TENABLE. Tenable.io. [Online]. [2020]. https://es-la.tenable.com/products/tenable-io

Tipos de Hackers. [Online] [2017]. https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers

Tipos de seguridad informática más importantes a conocer y tener en cuenta. [Online]. En: OBS Business school, España: Universidad de Barcelona. https://obsbusiness.school/int/blog-investigacion/sistemas/tipos-de-seguridad-informatica-mas-importantes-conocer-y-tener-en-cuenta

TORRES, Gisela. Tips para evitar SQL Injection. [Online]. 2010. [Citada: 21 mayo 2020]. https://www.returngis.net/2010/10/tips-para-evitar-sql-injection

Trabajo de grado (Especialista en Seguridad Informática). Universidad – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería

VILLALOBOS MURILLO, Johnny. Auditando en las bases de datos. [Online]. Costa Rica, 2008. [Citada: 19 mayo 2020]. https://dialnet.unirioja.es/descarga/articulo/5381374.pdf

Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas. [Online] [2018]. https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/

ZULUAGA MATEUS, Allen David. Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Armenia, 2017, 141p. Trabajo de grado (Especialista en Seguridad Informática). Universidad – UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería.