

Universidad Luterana Salvadoreña

Facultad de Ciencias del Hombre y la Naturaleza

Licenciatura en Ciencias de la Computación



Seminario de Especialización: Seguridad Informática con Énfasis en Hacking Ético

Docente: **Msc. José Roberto Rivas**
Ing. Marvin Guillén
Ing. Cristian Pleitéz

Ciclo: 01 – 2020

Documento Final – Proyecto de Seminario de Especialización

“HARDENING DE BASES DE DATOS”

“Hardening aplicado a Base de Datos SQL Server 2019, Oracle 11g
Release2 y MySQL 9.0.19”

Carnet	Apellidos	Nombres	Participación
AB01132926	Ayala Bardales	Reina Beatriz	100%
DP02110390	Díaz Palacios	Rafael Antonio	100%
RP01132524	Ramírez Pérez	José Balmore	100%
RS01134313	Rivera Sánchez	Carlos Efraín Antonio	100%

San Salvador, 16 de mayo de 2020



Hardening de bases de datos SQL Server 2019, Oracle 11g Release 2, MySQL 9.0.19, por Reina Beatriz Ayala Bardales, Rafael Antonio Díaz Palacios, José Balmore Ramírez Pérez, Carlos Efraín Antonio Rivera Sánchez, se distribuye bajo una [Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional](https://creativecommons.org/licenses/by-nc-nd/4.0/).

INDICE

INTRODUCCIÓN	4
MARCO REFERENCIAL.....	5
OBJETIVOS	5
OBJETIVO GENERAL	5
OBJETIVOS ESPECÍFICOS.....	5
METODOLOGÍA DE LA INVESTIGACIÓN.....	5
Modalidad de la investigación.....	6
Tipo de investigación	6
MARCO TEÓRICO	6
ÁREA DE INVESTIGACIÓN	6
SITUACIÓN ACTUAL.....	6
Lista de vulnerabilidades y ataques a bases de datos que se han realizado en los últimos años	7
PROBLEMÁTICA A SOLVENTAR.....	14
APORTES O MEJORAS DEL PROCESO DE HARDENING DE BASES DE DATOS.....	14
¿Qué es Hardening de Bases de Datos?	15
ESTRATEGIAS DE HARDENING	16
BASE DE DATOS	21
Importancia de una base de datos.....	21
Ventajas de una base de datos.....	22
Principales Benchmarks que existen	24
¿Qué son los CIS Benchmarks?.....	24
¿Qué son los DISA STIG?	25
Benchmark de Fabricantes de Productos.....	27
Mejores Prácticas de Seguridad en Torno a la Implementación de Sistemas Gestores de Bases de Datos	27
Comparación de Herramientas Automatizadas para aplicar Hardening a Base de Datos.....	28
CONCLUSIONES	41
RECOMENDACIONES	42
LICENCIAMIENTO	43
FUENTES DE INFORMACIÓN	43

INTRODUCCIÓN

Desde el inicio de la era digital o de la computación, una de las razones fundamentales ha sido la seguridad de la información; el surgimiento de ataques virales, robo de información, o daño a equipos computacionales, afectan hoy en día a las empresas en torno a sus activos informáticos y de paso limitan las operaciones administrativas de las mismas.

En la actualidad el uso de las redes informáticas ha facilitado el incremento del flujo de información, permitiendo así que cualquier usuario esté siempre comunicado, que tenga acceso a cualquier tipo de información e interactuar con otros usuarios, tan solo con usar un dispositivo que le permita tener una conexión a Internet.

La información que manejan las entidades educativas, gubernamentales, bancos, comercios, entre otros, está almacenada en una Base de Datos, por lo cual toda entidad debe proporcionar un esquema de seguridad a su información, debido a que este es el activo más importante que tiene cada compañía.

Así pues, el hardening se presenta como una de las medidas más importantes de seguridad a implementar en toda organización, ya que permite establecer distintas barreras u obstáculos de protección, para hacer frente a los posibles atacantes, ya sean tanto a nivel externo (amenazas desde las redes e internet), así como atacantes internos, (personas que hacen uso del sistema internamente), cabe aclarar que muchos de ellos pueden ser simplemente personas que ocasionan daños sin intención o por indebida manipulación de los equipos informáticos. Por lo cual en este proyecto realizaremos un proceso de aplicación de hardening para tres bases de datos diferentes, las cuales son: SQL Server 2019, Oracle 11g Release 2, y MySQL 9.0.19, estableciendo las herramientas utilizadas y los mecanismos empleados para dicho proceso, así mismo, damos a conocer información de los diversos ataques a bases de datos que se han dado en la actualidad.

MARCO REFERENCIAL

OBJETIVOS

OBJETIVO GENERAL

- Establecer un esquema de seguridad con la implementación de Hardening para fortalecer la seguridad y disminuir el riesgo de futuros ataques a la Base de Datos.

OBJETIVOS ESPECÍFICOS

- Identificar riesgos, vulnerabilidades o fallas de seguridad en las bases de datos SQL Server 2019, Oracle 11g Release 2 y MySQL 9.0.19.
- Definir diferentes roles de usuarios de Base de Datos para incrementar el nivel de seguridad de esta.
- Implementar un esquema de seguridad de Hardening a las Bases de Datos para endurecer la seguridad.
- Generar recomendaciones para mitigar los fallos o vulnerabilidades encontradas sobre las bases de datos.
- Hacer análisis de vulnerabilidades a la Base de Datos mediante diferentes herramientas como los CIS Benchmarks o herramientas automatizadas para así reducir los riesgos de amenazas de robo o alteración de información.

METODOLOGÍA DE LA INVESTIGACIÓN

En todo proyecto se debe establecer de forma clara los pasos a seguir para alcanzar los objetivos propuestos, por lo tanto, es de vital importancia especificar una metodología que defina de modo sistemático, como se realizará y administrará dicho proyecto, esto ayudará a alcanzar los objetivos planteados.

Modalidad de la investigación

La modalidad de la investigación que utilizamos es la Investigación Aplicada, que también se le puede conocer como práctica o empírica, este tipo de investigación busca el empleo de los conocimientos adquiridos. Por lo antes expresado la investigación aplicada se enfoca a la resolución de problemas habituales o concretos de la sociedad usando los conocimientos adquiridos en una forma inmediata (Tamayo, 2004)

Tipo de investigación

El proceso de investigación es primordial para conocer a profundidad la problemática por la cual se necesita del sistema, realizar un buen análisis y determinar los requerimientos del sistema.

El tipo de Investigación que contempla este proyecto es la Investigación aplicada, ya que su principal objetivo, se basa en resolver un problema práctico de gestión de vulnerabilidades, con un alcance determinado y limitado. De este modo se generan pocos aportes al conocimiento científico desde un punto de vista teórico, pero se logran poner en práctica los conocimientos adquiridos en el desarrollo de cada una de estas etapas.

MARCO TEÓRICO

ÁREA DE INVESTIGACIÓN

El área Tecnológica es en la cual está basada nuestra investigación, específicamente en el área de las Bases de Datos, que es en la cual aplicaremos el Hardening.

SITUACIÓN ACTUAL

En Latinoamérica, tres de cada cinco empresas sufren por lo menos un incidente de seguridad en la red y una de cada cinco, es víctima de 'secuestro' de información. Así lo reveló el estudio (ESET Security Report, 2018), que se realizó con 4.500 ejecutivos, técnicos y gerentes de 2.500 empresas de 15 países de la región.

El análisis detalló que los países más afectados son Perú con el 25 por ciento, México con el 20 por ciento, seguido de Argentina con el 15 por ciento, Brasil con el 14 por ciento y Colombia con el 10 por ciento.

La amplia variedad de amenazas informáticas, pueden emplearse para robar información valiosa de las compañías, desde ataques externos hasta fraudes financieros, que incluye alteración de datos y el pago de sobornos al cibercrimen.

En la era digital, la información es un factor muy importante para las compañías, por ello, deben hacer un análisis de riesgo de la seguridad informática para determinar el nivel y el impacto, conocer las debilidades y fortalezas de la compañía, tener más control, hacer monitoreo y establecer estrategias para protegerse de los ciberataques y que no puedan ser vulneradas sus bases de datos, ya que estas son uno de los activos más importantes de las compañías.

Lista de vulnerabilidades y ataques a bases de datos que se han realizado en los últimos años

En los últimos años, los ataques informáticos han crecido como espuma, debido a la globalización digital a la que todas las empresas, negocios, comercios, instituciones educativas y la sociedad en general se han integrado.

El uso de las TIC's, se ha vuelto una necesidad, más que un lujo, ya que casi todas las empresas desde las micro hasta las grandes han optado por el uso de estas, ya que los procesos que llevan a cabo se han facilitado en comparación a la forma tradicional en la cual las desarrollaban.

Por la misma razón hay personas que se dedican al robo de información a través de las redes informáticas para cometer fraudes, o cualquier tipo de ilícitos.

Las empresas en la actualidad recurren al uso de herramientas tecnológicas para guardar su preciado activo, el cual es toda la información de clientes, proveedores, activos, etc. Utilizando las bases de datos, ya sea en discos duros o en la nube. Por dicha razón los ataques informáticos en los últimos años han crecido; en esta investigación daremos a conocer los tipos de amenazas

existentes y los ataques que se han suscitado específicamente a las bases de datos para el robo, alteración o modificación de la información.

Según la investigación de Alex Rothacker, gerente AppSec's Team, Security Heuristics of Application Testing Technology for Enterprise Research, (Sharpmind Software, s/f), su equipo ha encontrado 10 tipos comunes de vulnerabilidades en las bases de datos por las que las organizaciones padecen ataques una y otra vez.

Alrededor de la mitad de las vulnerabilidades nombradas por Rothacker y su equipo están directa o indirectamente relacionadas con las prácticas flojas de gestión de parches en el entorno de base de datos. Ese es un pensamiento aterrador considerando sólo el 38% de los administradores aplican los ajustes de seguridad en sus bases de datos Oracle, en el ciclo de revisión inicial de tres meses. Y casi un tercio de ellos toman un año o más para aplicar el primer parche.

A continuación, mostramos la lista que según Rothacker, son las vulnerabilidades más comunes que existen en la actualidad.

1.- Nombre de usuario/password en blanco, por defecto o débil.

No es nada raro conseguir en el día a día pares de usuario/password como sa/1234, esta es la primera línea de defensa y un punto fundamental de la armadura de nuestras bases de datos. Es importante hacer revisiones periódicas de credenciales.

2.- Inyecciones SQL.

Cuando la plataforma de base de datos falla para desinfectar las entradas, los atacantes son capaces de ejecutar las inyecciones SQL de forma similar a como lo hacen en los ataques basados en Web, lo que les permite elevar sus privilegios y obtener acceso a una amplia gama de funcionalidades. Muchos de los proveedores han dado a conocer soluciones para evitar estos problemas, pero no servirá de mucho si los parches no se aplican o no se toman los correctivos correspondientes.

3.- Preferencia de privilegios de usuario por privilegios de grupo.

Las organizaciones necesitan garantizar que los privilegios no se les den a los usuarios por asignación directa, quienes finalmente los recogerán como los conserjes recogen las llaves en sus llaveros. En cambio, Rothacker recomienda que los usuarios sólo reciban privilegios por parte de grupos o funciones y que los privilegios sean manejados colectivamente. De esta forma será más fácil eliminar derechos a un usuario con simplemente eliminarlo del grupo, sin que queden derechos ocultos u olvidados asignados a dicho usuario.

4.- Características y funciones de base de datos innecesariamente habilitadas.

Cada instalación de base de datos viene con paquetes adicionales de todas las formas y tamaños que en su mayoría rara vez son utilizados por una sola organización. Dado que el nombre del juego en materia de seguridad de base de datos es el de reducir las superficies de ataque, las empresas necesitan buscar los paquetes que no utilizan y desactivarlos. Esto no sólo reduce los riesgos de ataques (0) day a través de estos vectores, sino que también simplifica la gestión de parches.

5.- Configuración de seguridad ineficiente.

Del mismo modo, las bases de datos tienen una gran cantidad de opciones de configuración y consideraciones diferentes a disposición de los administradores para ajustar el rendimiento y funcionalidades mejoradas. Las organizaciones necesitan conseguir y desactivar aquellas configuraciones inseguras que podrían estar activadas por defecto para mayor comodidad de los DBA o desarrolladores de aplicaciones. Las configuraciones de bases de datos en producción y desarrollo deben ser radicalmente diferentes.

6.- Desbordamientos del búfer.

Otro favorito de los piratas cibernéticos, las vulnerabilidades de desbordamiento de búfer son explotadas por las inundaciones de las fuentes de entrada con valores diferentes o muy

superiores a los que la aplicación espera - por ejemplo, mediante la adición de 100 caracteres en un cuadro de entrada pidiendo un número de Seguro Social -. Los proveedores de bases de datos han trabajado duro para solucionar los problemas técnicos que permiten estos ataques se produzcan. Esta es otra razón por la cual los parches son tan importantes.

7.- Escalada de privilegios.

Del mismo modo, las bases de datos con frecuencia exponen vulnerabilidades comunes que permiten a un atacante escalar privilegios en una cuenta con privilegios bajos hasta tener acceso a los derechos de un administrador. A medida que estas vulnerabilidades son descubiertas, los proveedores las corrigen y los administradores deben mantener las actualizaciones y parches actualizados.

8.- Ataque de denegación de servicio.

El caso del SQL Slammer es siempre un ejemplo muy esclarecedor de cómo los atacantes pueden utilizar las vulnerabilidades de los DBMS para derribar los servidores de base de datos a través de un alto flujo de tráfico. Aún más ilustrativo es el hecho de que cuando el Slammer atacó en 2003, un parche ya estaba por ahí que se dirigió a corregir la vulnerabilidad por la que se generó su ataque. Hoy en día siete años más tarde, SQL Slammer todavía está dando dolores de cabeza en los servidores no actualizados.

9.- Bases de datos sin actualizar.

Esto podría sonar repetitivo, pero vale la pena repetirlo. Los administradores de base de datos a veces no aplican un parche en el momento oportuno porque tienen miedo de este dañe sus bases de datos. Pero el riesgo de ser hackeado hoy es mucho más alto que el riesgo de aplicar un parche que descomponga la base de datos. Además, existen ante esos temores los backups y las réplicas. Quizás este punto pudo haber sido válido un par de años atrás, pero los proveedores ahora tienen mucho más cuidado con sus arreglos.

10.- Datos sensibles sin cifrar, tanto en reposo como en movimiento.

Tal vez sea obvio, pero las organizaciones no deben almacenar los datos sensibles en texto plano en una tabla. Y todas las conexiones a la base de datos siempre que manejen datos sensibles deben utilizar el cifrado.

Ataques de Inyección SQL

Explorando internet podemos ver que los ataques de inyección SQL, son de los ataques más comunes que se perpetran a las grandes empresas, estos se dan porque existen vulnerabilidades del Lenguaje de Consulta Estructurado (SQL) en donde los atacantes las utilizan para penetrar o inhabilitar las bases de datos. El objetivo de estos ataques es atacar directamente una aplicación o reenviar lógica a una base de datos en donde se puede poner en peligro todos los datos almacenados.

Según la Escuela de Organización Industrial (EOI, 2016) *Las inyecciones SQL son actualmente el segundo tipo de amenaza de más importante (27 %) y atacan a los sitios web mediante la introducción de afirmaciones SQL en un formulario web para saturar la base de datos asociada.*

ATAQUE A SONY PICTURES MEDIANTE INYECCIÓN SQL

En junio de 2012, la gran empresa cinematográfica Sony Pictures Entertainment fue objetivo de los ciberdelincuentes. El grupo de hackers conocido como LulzSec se atribuye el robo de datos personales de un millón de usuarios de Sony Pictures Entertainment, la división de cine de Sony.

La técnica empleada para perpetrar el ataque es la conocida como SQL injection, mediante la cual lograron los datos de más de 1.000.000 de usuarios, incluyendo contraseñas, direcciones de correo electrónico, direcciones postales y fechas de nacimiento. También han podido acceder

a detalles de la administración de Sony Pictures, incluidas las contraseñas, además de 75.000 “códigos de la música” y 3,5 millones de “cupones de la música”.

Los autores de la acción critican la seguridad de Sony, ya que han podido acceder a sus bases de datos mediante una inyección simple de código SQL.

Además, se da la característica que Sony tenía almacenado más de 1.000.000 de contraseñas en texto plano, sin cifrar, con lo que el acceso a esta información se facilitó enormemente. LulzSec se jacta también de haber atacado con éxito las bases de datos de Sony BMG de Bélgica y Holanda.

EL CASO DE MARRIOT

Según BBC News (2018) Los datos de 500 millones de clientes del grupo de hoteles Marriott International fueron víctimas de un ataque de un hacker el viernes 30 de noviembre, al parecer mediante inyección SQL.

La compañía dijo que la base de datos de reservas de huéspedes de su división Starwood fue violada por un individuo no autorizado.

Según una investigación interna, un atacante pudo acceder a esta red desde el año 2014.

Marriott International compró Starwood en 2016, creando así la cadena de hoteles más grande del mundo con más de 5.800 propiedades.

Marriott comunicó que fue alertado por una herramienta de seguridad interna de que alguien estaba intentando acceder a la base de datos de Starwood.

Después de investigar, descubrió que una "parte no autorizada había copiado y cifrado la información".

Los registros contienen información de hasta 500 millones de clientes, estimó la empresa.

En los perfiles de unos 327 millones de ellos había información "combinada" entre datos como nombre, dirección, teléfono, dirección de e-mail, número de pasaporte, información de la cuenta o sobre la llegada y salida al hotel del cliente.

Pero Marriott también confirmó que algunos registros incluían información cifrada de la tarjeta de crédito utilizada para el pago, si bien no podía descartar la posibilidad de que las claves de cifrado también hubieran sido robadas.

Otros ataques a bases de datos por inyección SQL nos los presenta Moes (s/f) fundador de SoftwareLab, el cual con su investigación nos explica que, durante las últimas dos décadas, un gran número de ataques de inyección SQL han sido dirigidos hacia grandes páginas web, empresas y plataformas de redes sociales. Algunos de estos ataques han resultado en grandes filtraciones de datos. Algunos de los ejemplos más notorios incluyen los siguientes:

- En 2008, dos hackers nacidos en Rusia usaron técnicas de inyección SQL para atacar Heartland Payment Systems, un proveedor entonces exitoso de soluciones de tramitación de pagos. Clasificada como la filtración de datos de tarjetas de crédito más grande hasta el momento, el ataque dio a los hackers acceso a la información de más de 150 millones de tarjetas de crédito y costó a la empresa afectada más de 300 millones de dólares. En 2018, los hackers fueron condenados a una sentencia conjunta de más de 16 años.
- En 2016, un grupo de hackers explotó las vulnerabilidades de vBulletin, un popular software de tablón de mensajería online, para atacar a 11 tableros de mensajes dedicados a los juegos, la mayoría de ellos en ruso. Durante el ataque, los hackers consiguieron robar datos de registro de más de 27 millones de cuentas.
- También en 2016, los hackers usaron métodos de inyección SQL para lanzar un ciber ataque contra el banco nacional de Qatar. Los hackers consiguieron robar más de 1.4 GB

de datos, que fueron publicados poco después. Estos datos implicaban la información de cuentas de miles de clientes, incluidos los miembros de la familia real del país, oficiales de la inteligencia, polémicos líderes religiosos, así como varios ciudadanos británicos, franceses y estadounidenses que estaban indicados como espías en la base de datos del banco.

PROBLEMÁTICA A SOLVENTAR

Crear un nivel de seguridad eficiente tiene como propósito la implementación de Hardening a la Base de Datos en este proyecto y así poder garantizar la integridad y confidencialidad de la información que esta almacenada en la misma. En la actualidad para poder protegerse de los ataques informáticos, existe un sin número de herramientas, tales como dispositivos, aplicaciones o programas estos pueden detectar cualquier tipo de amenazas de riesgos que el sistema este expuesto tales como: accesos no autorizados a un computador o a una red informática. Estos accesos no autorizados pueden ser escaneo de puertos, ataques de hackers, crackers, inyecciones SQL

La finalidad o la problemática que pretendemos solventar al implementar el proceso de Hardening en las tres diferentes Bases de Datos, es robustecer o endurecer la seguridad de ellas, detectar la mayor cantidad de vulnerabilidades y disminuir los riesgos de sufrir cualquier tipo de ataque que pueda modificar, alterar, borrar o robar su preciado activo como lo es la información almacenada en las mismas.

APORTES O MEJORAS DEL PROCESO DE HARDENING DE BASES DE DATOS

La búsqueda de nuevas políticas y tecnologías y sobre todo lo propenso o vulnerables que puede estar una empresa al sufrir un ataque cibernético, los lleva a recurrir a realizar el aseguramiento de sus datos o información, implementando el proceso de Hardening; el diseño de un esquema de seguridad bajo las normas internacionales de buenas prácticas de seguridad y herramientas como los CIS Benchmarks y Benchmarks de fabricantes (que son los que utilizamos), garantizará

la factibilidad operacional de la Base de Datos, además puede servir como apoyo para la creación de un manual de políticas de seguridad, para que los administradores y usuarios tengan un manejo sencillo y seguro de la misma.

¿Qué es Hardening de Bases de Datos?

Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc., innecesarios en el sistema, así como cerrando puertos que tampoco estén en uso además de muchos otros métodos y técnicas.

Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad. Una de las primeras cosas que hay que dejar en claro del Hardening es que no necesariamente logrará forjar equipos “invulnerables”. Es importante recordar que, según el modelo de defensa en profundidad, se conseguirá una red más segura o no.

Antes de profundizar en el concepto de hardening vale aclarar que las palabras hardening y bastionamiento son sinónimos en el tema de seguridad informática ya que ambas significan el aseguramiento de un sistema informático.

La empresa Tarlogic (2016), define el Hardening como “la protección de un sistema o conjunto de sistemas informáticos mediante la aplicación de configuraciones de seguridad específicas para prevenir ataques informáticos, contener la elevación de privilegios, mitigar el robo de información, y obtener la trazabilidad necesaria para analizar un ataque en el caso de que haya sucedido”.

Como es de aclarar, el bastionamiento puede abarcar desde medidas en software dependiendo del sistema operativo que manejen las estaciones de trabajo (entre ellas destacarían antivirus, políticas de grupo, permisos de cuentas, etc.) así como también medidas en hardware que ayudan a proteger la periferia del sistema y su red en términos físicos (como ejemplo se tendrían

firewalls, implementación de DMZ, IDS, honeynets, routers, UPS, entre otros). Otra palabra muy utilizada y que tampoco aparece en la RAE, pero que es de uso extendido para hardening es "securizar", incluso alguna veces se usa la palabra "hardenizar" que deriva claramente del inglés" (Martínez, 2009).

La empresa Grammatech (2016) señala respecto del hardening en software que este "se realiza a través de tres técnicas básicas: análisis de la vulnerabilidades, parches y monitoreo de software".

Hardening es un concepto utilizado dentro del ámbito de la seguridad informática, en la actualidad se aplica dentro de aplicaciones web, servidores, Base de Datos, entre otros.

El hardening en sí, se entiende como un proceso para asegurar o endurecer un sistema informático mediante capas u obstáculos, que servirán para ralentizar el sistema y así poder dificultar la actividad del atacante que utiliza las vulnerabilidades con la finalidad de llevar a cabo el robo, alteración o modificación de la información. Este concepto se aplica para el aseguramiento de sistemas que tengan una combinación entre hardware y software; en el caso de esta investigación, el hardening aplica para la protección de las Bases de Datos.

ESTRATEGIAS DE HARDENING

La mayoría de las estrategias se enfocan en el aseguramiento o endurecimiento de un sistema en específico, pudiendo ser un sistema operativo (software) o un equipo (hardware), lo más común que se hace es la instalación de un antivirus, parcheo o actualizaciones constantes, también el manejo de contraseñas seguras o usar correctamente el internet y los dispositivos removibles. Además, si lo que se quiere es descubrir vulnerabilidades, se puede usar pentesting con el fin encontrarlas y luego corregirlas.

Para este caso, como el hardening lo estamos aplicando a Bases de Datos, utilizamos una de las herramientas internacionales más importantes como los CIS Benchmarks, los Benchmark de fabricantes (que son los que utilizamos), y también DISA STIG, que es la agencia de apoyo de

combate del DoD (Departamento de Defensa) de EEUU, garantizará la factibilidad operacional de la Base de Datos, además puede servir como apoyo para la creación de un manual de políticas de seguridad, para que los administradores y usuarios tengan un manejo sencillo y seguro de la misma. Así mismo se busca información relacionada a dos herramientas automatizadas para el escaneo de vulnerabilidades y aplicación de hardening, se hace una comparación de su funcionamiento, y se da la recomendación de cuál puede ser más útil; dichas herramientas son NESSUS y NEXPOSE.

CIBERSEGURIDAD

Los términos "ciberseguridad" y "seguridad de la información" se suelen usar indistintamente, pero en realidad la ciberseguridad es una parte de la seguridad de la información. Concretamente, la ciberseguridad se puede definir como la protección de los activos de información, abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados.

Generalmente, la ciberseguridad hace referencia a las amenazas que afectan a una entidad debido a la existencia de un ciberespacio global. A diferencia de la seguridad de la información, la ciberseguridad no incluye los peligros naturales, los errores personales o la seguridad física. Para decirlo de una manera más simple, si eliminamos las amenazas derivadas de un comportamiento humano ofensivo y adverso que vienen a través de sistemas interconectados, la ciberseguridad no sería un problema, y la seguridad de la información por sí sola sería suficiente.

En la era digital se habla de Ciberseguridad, que se asocia a las ciberamenazas, al cibercrimen, pero también a las buenas prácticas para proteger la información y prevenir o detectar los ataques cibernéticos.

Las amenazas de la seguridad informática llegan a través de programas dañinos o maliciosos que se instalan en un dispositivo o se penetran por medio de la nube.

Information Systems Audit and Control Association (ISACA), un referente en la materia define la ciberseguridad como "una capa de protección para los archivos de información. A partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo" (ISACA, 2018 citado por Riesgos Cero 2019).

LA PROTECCIÓN DE ACTIVOS DIGITALES

En el núcleo de su marco de seguridad cibernética, el Instituto Nacional de Normas y Tecnología (NIST, 2014) identifica cinco funciones clave necesarias para la protección de los activos digitales. Estas funciones coinciden con metodologías de gestión de incidentes e incluyen las siguientes actividades:

- Identificar—Usar el entendimiento de la organización para minimizar el riesgo de los sistemas, activos, datos y capacidades.
- Proteger—Diseñar salvaguardas para limitar el impacto de los eventos potenciales en servicios e infraestructuras críticos.
- Detectar—Implementar actividades para identificar la ocurrencia de un evento de ciberseguridad.
- Responder—Tomar las medidas adecuadas tras conocerse un evento de seguridad.
- Recuperar—Planificar para tener resiliencia y recuperar de forma oportuna los servicios y capacidades comprometidos.

La ciberseguridad tiene como propósito cumplir ciertos objetivos en la protección de los activos digitales. Estos incluyen la confidencialidad, integridad y disponibilidad de los activos entre otros aspectos. Estas estrategias se analizarán más adelante de una forma más detallada.

CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Para entender mejor la ciberseguridad y la protección de activos digitales, es útil tener en cuenta tres conceptos clave que se utilizan para guiar las políticas de seguridad de la información, (ISACA, 2017) como se muestra en la siguiente imagen. Los conceptos son:

- Confidencialidad
- Integridad
- Disponibilidad



La confidencialidad es la protección de la información contra el acceso no autorizado o la divulgación. Diferentes tipos de información requieren diferentes niveles de confidencialidad, y la necesidad de confidencialidad puede cambiar a lo largo del tiempo. La información personal, financiera y médica requiere un mayor grado de confidencialidad que, por ejemplo, las actas de una reunión del personal.

La integridad es la protección de la información contra la modificación no autorizada. Por ejemplo, si un banco transfiere \$10.000 a otra institución financiera, es importante que la cantidad no cambie a \$100.000 durante dicho intercambio. El concepto de integridad también se aplica a mensajería electrónica, archivos, software y configuraciones.

Cualquier violación de la integridad es importante, ya que puede ser el primer paso de un ataque exitoso contra la disponibilidad o confidencialidad del sistema. Los sistemas contaminados y los datos corruptos deben ser tratados de inmediato con el objetivo de evaluar el nivel potencial de violación o daños. **DISPONIBILIDAD.** Esto se refiere que los usuarios autorizados puedan recuperar la información en todo momento que la necesiten.

La disponibilidad garantiza el acceso oportuno y confiable al uso de la información y los sistemas. Esto incluye salvaguardas para asegurar que los datos no se eliminan de forma accidental o malintencionada. Esto es particularmente importante en un sistema de misión crítica, ya que cualquier interrupción en su disponibilidad puede resultar en una pérdida de productividad e ingresos. Del mismo modo, la pérdida de datos puede afectar la capacidad de la dirección para tomar decisiones y respuestas efectivas. La disponibilidad puede protegerse mediante el uso de redundancia, copias de seguridad y la implementación de la gestión y planificación de la continuidad del negocio.

No repudio El no repudio es una consideración importante en la ciberseguridad. Se refiere al concepto de garantizar que un mensaje u otra información es genuina. Cuando se envía información, es importante verificar que proviene de la fuente de la que se dice que proviene. El no repudio provee un medio para que la persona que envía o recibe información no pueda negar que envió o recibió dicha información. Se implementa a través de firmas digitales y registros de transacciones.

VULNERABILIDAD, AMENAZAS, RIESGOS Y CONTROL DE LA SEGURIDAD INFORMÁTICA.

Creemos conveniente dar a conocer los siguientes conceptos, los cuales, muchas veces no se conocen o son mal utilizados, estos son definidos por ISACA (2017) de la siguiente manera:

VULNERABILIDAD. Debilidad en el diseño, implementación, operación o el control interno de un proceso que podría exponer el sistema a amenazas adversas provenientes de eventos de amenaza. Aunque gran parte de la ciberseguridad se centra en el diseño, implementación y gestión de controles para mitigar el riesgo, es fundamental para los profesionales de la seguridad entender que el riesgo nunca puede ser eliminado.

AMENAZA. Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que sea capaz de actuar contra un activo de una manera que pueda dañarlo. ISO / IEC 13335 define una amenaza en términos generales como una posible causa de un incidente no deseado.

Algunas organizaciones hacen una distinción entre una fuente de amenaza y un evento de amenaza, clasificando una fuente de amenaza como el proceso real o el agente que intenta causar daño, y un evento de amenaza como el resultado de la actividad maliciosa de un agente de amenaza.

RIESGO. El deber principal de la ciberseguridad es identificar, mitigar y gestionar el Ciberriesgo a los activos digitales de una organización. Ciberriesgo es aquella parte de la gestión global del riesgo que se centra exclusivamente en el riesgo que se manifiesta en el dominio ciber (Entornos de información interconectados). Aunque la mayoría de la gente tiene una comprensión inherente de la palabra riesgo en su vida diaria, es importante comprender el riesgo en el contexto de la ciberseguridad, lo cual significa saber cómo determinar, medir y reducir el riesgo de manera efectiva.

CONTROL. Se dice que es una serie de procedimientos empleados con la finalidad de reducir o eliminar las vulnerabilidades de un sistema informático, estas medidas o controles pueden ser dispositivos o aplicaciones.

BASE DE DATOS

Una Base de Dato es un conjunto, colección o depósito de datos almacenados en un soporte informático de acceso directo. Los datos deben estar relacionados y estructurados de acuerdo con un modelo capaz de recoger el contenido semántico de los datos almacenados. (LLanos Ferraris, 2010)

Importancia de una base de datos

En las organizaciones y empresas las bases de datos son la parte principal para las grandes organizaciones de hoy en día, ya que establecen un activo fijo muy importante para la toma de decisiones administrativas, agrupar y almacenar todos los datos de la empresa en un único lugar, evitar la redundancia y mejorar la organización de la agenda, realizar una interlocución adecuada con los clientes.

Si una Base de Datos se gestiona adecuadamente, la organización obtendrá diferentes ventajas. Aumentará su eficacia, habrá trabajos que se realicen con mayor rapidez y agilidad debido a la simplificación de los mismos, podremos mejorar la seguridad de los datos que almacenamos, y con todos estos factores, maximizaremos los tiempos y por tanto, se producirá una mejora en la productividad.

Ventajas de una base de datos

Las ventajas que podemos tener de las bases de datos son numerosas a continuación se hablará de las más importantes.

Independencia de los datos a los programas y aplicaciones.

La inserción, borrado o actualizaciones de la informaciones y datos no implica a alterar las aplicaciones que maneja la Base de Datos puesto que la información que está guardada en estructuras independientes en donde no están las aplicaciones.

➤ Redundancia.

La información que estar almacenada en la base de datos no se duplicará por lo tanto la redundancia de datos se reducirá al mínimo la duplicidad de la información incluso pueden ser perjudiciales.

➤ Integridad de la información.

La integridad de la información en la Base de Datos se refiere a la corrección y exactitud de la información en la misma.

➤ Mayor seguridad en los datos.

La asignación de privilegios de roles de usuarios que interrelacionan con la Base de Datos dará una mayor seguridad a la información.

➤ Coherencia de los resultados.

La información que se almacena en la base de datos siempre se la hará una sola vez, por lo tanto, cuándo se utilicen los datos en algún procedimiento los resultados de los mismo siempre serán coherentes.

➤ **Datos más documentados.**

La estructuración de los datos que nos ofrece la Base de Datos esto se refiere a datos sobre datos.

➤ **Acceso simultáneo a los datos.**

Se permite el acceso simultáneo de usuario a la información de la Base de Datos

Balance de Requerimientos Conflictivos.

La asignación de un Administrador de la Base de Datos dará un manejo apropiado sobre de la estructura, diseño y de información almacenada en la Base de Datos, la asignación de un DBA será beneficioso para los requerimientos de una organización.

➤ **Reducción del espacio de almacenamiento.**

La optimización de almacenamiento nos permite utilizar menos espacio en los discos.

➤ **Acceso a los datos más eficiente.**

La estructura de la Base de Datos y el almacenamiento de la información en ella permiten a los usuarios de esta, un óptimo acceso a dicha información también permite el acceso simultáneo de usuarios al mismo tiempo.

➤ **Estandarización.**

Esto se debe a que es más fácil estandarizar procesos, nombres de datos, formas, etc.

➤ **Flexibilidad y rapidez al obtener datos.**

La información de la Base de Datos puede ser accedida más fácil con solo escribir oraciones.

Esto evita el antiguo proceso de llenar una petición al Centro de Cómputos para poder obtener un informe.

➤ **Eficiencia de los programadores.**

Los programadores de la organización o entidades no deben preocuparse por la organización o manejo de la información de la Base de Datos, es por eso que tienen mayor tiempo para concentrar en resolver otros problemas inmediatos, mejorando de ese modo su productividad.

Principales Benchmarks que existen

El Center of Internet Security CIS (Centro de Seguridad de Internet) es el principal estándar de la industria reconocido para la guía de configuración segura, que desarrolla listas de verificación exhaustivas derivadas del consenso para ayudar a identificar y mitigar vulnerabilidades de seguridad conocidas en una amplia gama de plataformas.

Cada punto de referencia CIS o Benchmark proporciona una guía prescriptiva para establecer una postura de configuración segura para su infraestructura de TI, incluida una descripción detallada y una justificación de las vulnerabilidades potenciales junto con pasos claros de auditoría y remediación. Como tal, los puntos de referencia CIS son la opción abrumadora de elección para los auditores de todo el mundo al asesorar a las organizaciones sobre la adopción de un estándar de construcción seguro para cualquier iniciativa de gobierno y seguridad.

¿Qué son los CIS Benchmarks?

Los puntos de referencia CIS son las mejores prácticas para la configuración segura de un sistema. Estos están disponibles para más de 140 tecnologías; los puntos de referencia CIS se desarrollan a través de un proceso único, basado en el consenso compuesto por profesionales de ciberseguridad y expertos en la materia en todo el mundo. Los puntos de referencia de CIS son las únicas guías de configuración de seguridad basadas en el consenso y las mejores

prácticas desarrolladas y aceptadas por el gobierno, las empresas, la industria y el mundo académico.

¿Cuáles son los perfiles de nivel 1 y nivel 2 dentro de un punto de referencia CIS?

La mayoría de los puntos de referencia CIS utilizan muchos perfiles de configuración. Un perfil no es más que un conjunto de configuraciones asignadas a las recomendaciones o lineamientos del control de aseguramiento.

El perfil de Nivel 1 consiste en las recomendaciones básica que se pueden implementar con bastante rapidez y está diseñado para no tener un impacto extenso en el rendimiento. La intención del punto de referencia o benchmark de perfil Nivel 1, es reducir de modo superficial un ataque mientras los equipos (hardware) se mantienen utilizables, es decir, no se obstaculiza la funcionalidad de la empresa. Este puede ser utilizado cuando la empresa no tiene muchos activos o información que sea de gran importancia.

El perfil de Nivel 2 se considera "defensa en profundidad" y está destinado a entornos donde la seguridad de la empresa es primordial ya que sus activos o información es bastante importante y/o delicada, la cual debe tener el mayor aseguramiento para no ser robada. Si las configuraciones del perfil Nivel 2, no se utilizan adecuadamente o con supervisión pueden tener un efecto adverso, es decir, la información puede ser comprometida y ser un blanco fácil para un atacante.

Cada recomendación dentro de cada CIS Benchmark está asociado con un perfil. Independientemente del perfil que planea implementar, le recomendamos aplicarlo primero en un entorno de prueba, para aprender a usarlo y determinar el impacto que este tendrá.

¿Qué son los DISA STIG?

DISA es la agencia de apoyo de combate del DoD (Departamento de Defensa) de EE. UU., responsable de mantener la posición de seguridad de la red de información del DoD (DoD Information Network, DODIN). Una de las formas en que DISA lleva a cabo esta tarea es desarrollando, difundiendo y exigiendo la implementación de STIG.

Como parte del Departamento de Defensa, la Agencia de Sistemas de Información de Defensa (DISA) es una agencia de apoyo de combate que brinda soporte de TI y comunicación a todos los institutos e individuos que trabajan para el DoD. DISA supervisa los aspectos tecnológicos y de TI de la organización, entrega y gestión de información relacionada con la defensa.

Las pautas que DISA proporciona a las organizaciones se denominan Guías de implementación técnica de seguridad (STIG). Estas guías describen cómo una organización debe manejar y administrar el software y los sistemas de seguridad.

En síntesis, las STIG son guías portátiles basadas en estándares que permiten consolidar sistemas para reducir amenazas y mitigar el impacto como parte de una estrategia exhaustiva de defensa mayor. Las STIG son obligatorias para los sistemas de TI del DoD de EE. UU. y, por lo tanto, proporcionan una línea base segura y examinada que permite medirlas con otras entidades ajenas al DoD.

Lista completa de DISA STIG

La Guía de implementación técnica de seguridad (STIG) son los estándares para los dispositivos / sistemas DoD. Cada STIG proporciona orientación técnica para asegurar sistemas / software de información que de otro modo podrían ser vulnerables.

El DoD actualiza regularmente los STIG para garantizar que los desarrolladores puedan configurar adecuadamente el hardware y el software, implementar protocolos de seguridad y organizar procesos de capacitación.

Puede usar un STIG para identificar posibles debilidades en su código. El uso de un analizador estático, como Klocwork (herramienta de análisis de código estático, analiza el código fuente en tiempo real, simplifica las revisiones de código y extiende la vida útil del software complejo), Nessus, etc. Esto con la finalidad de identificar las debilidades o vulnerabilidades de seguridad de DISA STIG más rápido.

Benchmark de Fabricantes de Productos.

Existen los benchmark que proporcionan los fabricantes de cada producto, ya que ellos están en la obligación de publicar sus controles de seguridad o buenas prácticas en torno al uso de cada uno de sus productos. Por ejemplo, en el caso de nuestro proyecto, utilizamos la base de datos MySQL 9.0.19, del cual ni CIS ni DISA STIG han brindado un benchmark, por lo cual tuvimos que recorrer a la página del fabricante para poder descargar el benchmark sugerido para esa versión.

Mejores Prácticas de Seguridad en Torno a la Implementación de Sistemas Gestores de Bases de Datos.

Los problemas de configuración o configuraciones por defecto pueden comprometer un sistema completo. Es importante configurar de forma personalizada los componentes que se utilizan y evitar usar configuraciones genéricas.

Según PowerData (2017) Cuando hablamos de integridad en base de datos nos estamos refiriendo a la completitud, la exactitud y la coherencia del conjunto de datos de una base de datos. Podemos tener una percepción de esta integridad en base de datos cuando vemos que entre dos instancias o entre dos actualizaciones de un registro de datos, no hay ninguna alteración, lo que significa que los datos están intactos y sin cambios.

Una de las formas más efectivas de garantizar la integridad en base de datos es implementando algunas de las mejores prácticas de seguridad, existen muchas, pero a continuación mencionamos las que PowerData (2017) considera las más importantes:

- **Recurrir al enmascaramiento de datos** o permitir a los usuarios acceder a cierta información sin poder verla ayuda a mantener la confidencialidad incluso en entornos de pruebas.
- **Minimizar los extras y limitarse a los servicios, aplicaciones y funcionalidades que realmente son necesarios** para asegurar el normal funcionamiento de las operaciones del negocio, de esta forma se reduce el riesgo.

- **Asegurarse de que los administradores de la base de datos entiendan la importancia de garantizar su protección.**
- **Mantener actualizadas las bases de datos** y eliminar los componentes desconocidos.
- **Recurrir a herramientas como el análisis de código estático**, que ayudan a reducir los problemas de inyección de SQL, desbordamiento de búfer y problemas de configuración.
- **Hacer copias de seguridad frecuentes** y emplear una fuente de alimentación ininterrumpida, (SAI o UPS) que garantice que un corte de energía no causa la pérdida de datos.
- **Audita.** Una vez que hayamos creado una configuración que creamos que puede ser totalmente segura, realicemos actividades de auditoría para asegurarnos que no te desvías de tu objetivo. Por ejemplo, se podría poner algún tipo de alarma para que nos avisara de cualquier cambio que se pudiera dar en dicha configuración.
- **Monitoriza toda acción relacionada con la base de datos.** Monitorizar la actividad que se lleva a cabo en nuestra base de datos nos puede dar algún tipo de pista en caso de estar siendo utilizada de forma indebida o para la detección de intrusos.
- **Control de acceso y gestión de derechos.** No todos los datos son igual de importantes y no todos los usuarios son creados igual. Es necesario establecer una jerarquía y garantizar que cada tipo de usuario sólo pueda realizar las acciones que se le permiten en la base de datos, para garantizar de esa forma la integridad de la información. En el caso de los datos confidenciales, como pueden ser todo tipo de contraseñas, es recomendable utilizar algún tipo de cifrado de datos para que la información no sea legible a simple vista.

Comparación de Herramientas Automatizadas para aplicar Hardening a Base de Datos.

En la actualidad hay muchas herramientas para el escaneo de sistemas informáticos de cualquier

tipo, para detectar vulnerabilidades y poder solventarlas.

A continuación, presentamos la comparación entre dos de las más usadas: Nexpose de Rapid7 versus Open VAS versus Nessus Professional de Tenable. (Tenable, 2020)

			
— EVALUACIÓN DE VULNERABILIDADES			
Cobertura de CVE	Más de 50 000 CVE: la mayor cantidad en la industria Lea este informe de investigación para obtener más información.	< 26 000 CVE	< 42 000 CVE
Precisión de escaneo	El índice de falsos positivos más bajo de la industria, mejor que la precisión de seis sigma ¹	No publicado	No publicado; los clientes informan muchos falsos positivos
Velocidad del lanzamiento de verificaciones de vulnerabilidades	Lanzamiento de nuevas verificaciones de vulnerabilidades (plugins) dentro de un promedio de 24 horas posteriores a la revelación de la vulnerabilidad	No publicado	No publicado

Plantillas de escaneo prediseñadas	Plantillas para vulnerabilidades importantes (WannaCry, Spectre y Meltdown, etc.), auditorías SCAP y OVAL, y más [haga clic para ver la captura de pantalla]	Sin plantillas prediseñadas para WannaCry, Spectre y Meltdown, etc.	Sin plantillas prediseñadas para WannaCry, Spectre y Meltdown, etc.
Live Results	Live Results identifica las vulnerabilidades utilizando los datos de escaneo existentes con nuevas actualizaciones de plugins para proporcionar visibilidad en tiempo real [haga clic para ver la captura de pantalla]	No disponible	No disponible
Agrupamiento de vulnerabilidades	Grouped View presenta vulnerabilidades similares en un solo hilo para facilitar la gestión [haga clic para ver la captura de pantalla]	No disponible	No disponible
— EVALUACIÓN/AUDITORÍA DE CONFIGURACIÓN DE SEGURIDAD (SCA)			
Plantillas prediseñadas de cumplimiento y de evaluación de configuración	Más de 700 plantillas de cumplimiento y de configuración (CIS, DISA STIG, HIPAA, PCI DSS, USGCB, FDCC, y más), sin ningún costo adicional Lea este informe de investigación para obtener más información.	Se incluye un conjunto muy limitado de plantillas de configuración. No es compatible con las auditorías CIS, DISA STIG, USGCB o FDCC.	Se incluye un conjunto limitado de plantillas de configuración. CIS, USGCB, FDCC y políticas personalizadas disponibles por un costo adicional (licencia de Policy Manager).
— INFORMES E INTERFAZ DEL USUARIO			
Creación flexible de informes	Las plantillas de informes prediseñadas simplifican la creación de informes. Los informes pueden adaptarse con base en las vistas personalizadas por equipo o cliente. [haga clic para ver la captura de pantalla]	Plantillas de informes y capacidades de filtrado limitadas	Plantillas de informes prediseñadas. Los informes pueden crearse y adaptarse con base en las vistas personalizadas.
Formatos de exportación de informes	HTML, CSV, PDF, .Nessus XML y Nessus DB	HTML, PDF, XML y texto	HTML, CSV, PDF, XML y RTF/texto
Informes con marca	Opción de añadir una marca personal (nombre/logotipo)	No disponible	No disponible
Distribución automática por correo electrónico de los informes una vez finalizados los escaneos	Incluida	No disponible	No disponible
Calidad de la interfaz del usuario	Interfaz del usuario moderna [haga clic para ver la captura de pantalla]	Interfaz del usuario obsoleta	Interfaz del usuario moderna

- INVESTIGACIÓN DE SEGURIDAD			
Investigación de seguridad de expertos	Tenable Research proporciona inteligencia esencial de amenazas y vulnerabilidades, y ha descubierto cientos de nuevas vulnerabilidades	Ninguna	Rapid7 cuenta con un respetado equipo de investigación de seguridad

- COMPATIBILIDAD CON PLATAFORMAS			
Sistemas operativos compatibles	Debian/Kali Linux (varias versiones), Red Hat EL (varias versiones), CentOS (varias versiones), Oracle Linux (varias versiones), FreeBSD (varias versiones), Fedora (varias versiones), SUSE Linux Enterprise (varias versiones), Ubuntu (varias versiones), Windows Server (2008, 2008 R2, 2012, 2012 R2, 2016), Windows (7, 8, 10)	Los usuarios deben crear sus propios binarios OpenVAS a partir del código fuente o utilizar paquetes de la comunidad no compatibles. No funciona en Windows.	Red Hat EL (varias versiones), CentOS (solo v7), Oracle Linux (solo v7), Ubuntu (varias versiones), Windows Server (2008 R2, 2012 R2, 2016), Windows (7, 8.1, 10)
Opciones de implementación	Unidad USB en vivo, instalación en la nube o tradicional	Instalación tradicional	Instalación tradicional o en la nube

- COSTO TOTAL DE PROPIEDAD (TCO)			
Costo de adquisición, operación y soporte del producto	Suscripción a Nessus Professional: <USD 3000/año para IP ilimitadas. Las amplias capacidades prediseñadas, la automatización y el soporte de los proveedores minimizan el esfuerzo manual.	Descarga gratuita. ² Se requiere un trabajo manual significativo para la implementación, la operación y el autosuporte.	Suscripción a Nexpose: La licencia de 500 IP comienza en >USD 10 000/año y aumenta significativamente con las IP. Costo adicional para Policy Manager. Capacidades prediseñadas, automatización y soporte de los proveedores limitados.

- VIABILIDAD DEL PRODUCTO			
Inversión en productos	Tenable está realizando una gran inversión en Nessus. Solo en 2018, se hicieron un lanzamiento importante, dos lanzamientos menores y 9 lanzamientos de actualizaciones menores de la versión	OpenVAS ha lanzado solo dos versiones en los últimos cuatro años	Rapid7 parece estar eliminando gradualmente a Nexpose

ADOPCIÓN EN LA INDUSTRIA			
Clientes de pago	Más de 30,000 ³	N/C	<7100 ⁴
Descargas acumuladas	Casi dos millones	No publicado	No publicado
N.º 1 en participación en el mercado para la VA de aplicaciones ⁵	Sí [haga clic para ver el gráfico]	No	No

Adjuntamos también otra comparación realizada por el especialista en seguridad Daniel González, desde el sitio gbadvisors donde incluye las herramientas Tenable.io, Qualysguard y Rapid7 (Guedez. 2017).



INSTALACIÓN

<i>Premisas / Indicadores</i>	<i>Qualysguard</i>	<i>Puntaje</i>	<i>Rapid7</i>	<i>Puntaje</i>	<i>Tenable</i>	<i>Puntaje</i>
Virtualización en la Nube	Parcialmente Cloud	+ 2	No opera en la Nube	- 1	Parcialmente Cloud	+ 2
Servicio local para virtualización	Cuenta con Servicio de Virtualización	+ 2	No aplica	- 1	Cuenta con Agentes de Virtualización	+ 3
Consumo de recursos	Instala escaner local en red	+ 2	Consume mucho ancho de banda, tarda mucho en iniciar	- 2	Se instala fácilmente en SO Windows, Linux y Mac Os	+ 3
Aspectos particulares	Instalación mediante máquina virtual; y/o aplicativo en red	+ 1	Solicita datos irrelevantes para la instalación	- 1	Agentes trabajan con dispositivos móviles	+ 4
Total: + 7			Total: - 5			Total: + 12

INTERFAZ GRÁFICA Y ESCANER DE VULNERABILIDADES

<i>Premisas / Indicadores</i>	<i>Qualysguard</i>	<i>Puntaje</i>	<i>Rapid7</i>	<i>Puntaje</i>	<i>Tenable</i>	<i>Puntaje</i>
Tipo de interfaz	Interfaz obsoleta basada en ventanas emergentes que entorpece la configuración	- 4	Diseño de tableros poco intuitivos que se cargan en la Nube	- 4	Simple, concreta y orientada al uso con plantillas pre-definidas basadas en SCADA	+ 3
Configuración	Admite únicamente direcciones IP	- 2	Requiere creación previa de políticas y credenciales por separado	- 4	Viene con políticas pre-cargadas que luego pueden redefinirse	+ 3
Despliegue de escaneo	Demanda configuración previa de políticas de funcionamiento	- 4	Necesita configuración previa para ejecutar escaneo	- 2	Pluggins pre-cargados para realizar escaneos	+ 3
Tiempo para finalizar escaneo	No se tienen datos	0	Dos horas	- 4	No se tienen datos	0
Total: - 10			Total: - 14			Total: + 9

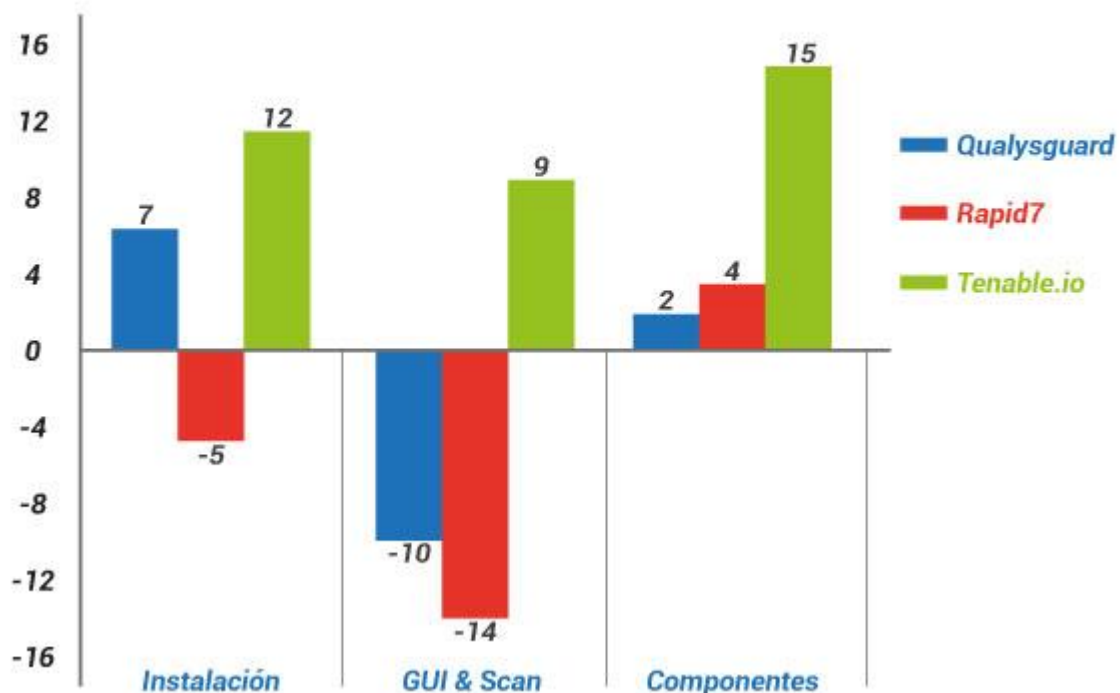
CARACTERÍSTICAS GENERALES

Premisas / Indicadores		Qualysguard	Ptos.	Rapid7	Ptos.	Tenable	Ptos.
Instalación	Virtualización en la Nube	Parcialmente Cloud	+ 2	No opera en la Nube	- 1	Parcialmente Cloud	+ 2
	Servicio local para virtualización	Cuenta con Servicio de Virtualización	+ 2	No aplica	- 1	Cuenta con Agentes de Virtualización	+ 3
	Consumo de recursos	Instala escaner local en red	+ 2	Consume mucho ancho de banda, tarda mucho en iniciar	- 2	Se instala fácilmente en SO Windows, Linux y Mac Os	+ 3
	Aspectos particulares	Instalación mediante máquina virtual; y/o aplicativo en red	+ 1	Solicita datos irrelevantes para la instalación	- 1	Agentes trabajan con dispositivos móviles	+ 4
		Total: + 7		Total: - 5		Total: + 12	
Uso de la Interfaz Gráfica y Escaneos de Vulnerabilidad	Tipo de interfaz	Interfaz obsoleta basada en ventanas emergentes que entorpece la configuración	- 4	Diseño de tableros poco intuitivos que se cargan en la Nube	- 4	Simple, concreta y orientada al uso con plantillas pre-definidas basadas en SCADA	+ 3
	Despliegue de escaneo	Admite únicamente direcciones IP	- 2	Requiere creación previa de políticas y credenciales por separado	- 4	Viene con políticas pre-cargadas que luego pueden redefinirse	+ 3
	Configuración	Demanda configuración previa de políticas de funcionamiento	- 4	Necesita configuración previa para ejecutar escaneo	- 2	Plugins pre-cargados para realizar escaneos	+ 3
	Tiempo para finalizar escaneo	No se tienen datos	0	Dos horas	- 4	No se tienen datos	+ 0
		Total: - 10		Total: - 14		Total: + 9	
Componentes del Servicio	Modelo de escaneo	Cuenta con Agente configurado totalmente desde la Nube, lo cual consume bastante ancho de banda	+ 1	Integra Agente para monitoreo	+ 3	Cuenta con Agentes para dispositivos móviles	+ 3
	Tipo de servicio	Solución SaaS que deja por fuera servicios bajo modelo On-Premise	+ 1	Escáner activo	+ 2	Escaneo activo que se integra con servicio de escaneo pasivo (PVS)	+ 4
	Políticas	Necesitan ser configuradas antes del inicio del servicio, lo que entorpece el resultado	+ 1	Configuración limitada para la creación de políticas de auditoría	+ 1	Cuenta con políticas para análisis de malware que opera en conjunto con antivirus	+ 4
	Aspectos adicionales	Carece de opción para escaneo de vulnerabilidades a través de MDM	- 1	No ofrece soporte o documentación para detección malware	- 2	Ejecuta análisis de vulnerabilidades a través de MDM	+ 4
		Total: + 2		Total: + 4		Total: + 15	

COMPONENTES DEL SERVICIO

Premisas / Indicadores	Qualysguard	Puntaje	Rapid7	Puntaje	Tenable	Puntaje
Modelo de escaneo	Cuenta con Agente configurado totalmente desde la Nube, lo cual consume bastante ancho de banda	+ 1	Integra Agente para monitoreo	+ 3	Cuenta con Agentes para dispositivos móviles	+ 3
Tipo de servicio	Solución SaaS que deja por fuera servicios bajo modelo On-Premise	+ 1	Escáner activo	+ 2	Escaneo activo que se integra con servicio de escaneo pasivo (PVS)	+ 4
Políticas	Necesitan ser configuradas antes del inicio del servicio, lo que entorpece el resultado	+ 1	Configuración limitada para la creación de políticas de auditoría	+ 1	Cuenta con políticas para análisis de malware que opera en conjunto con antivirus	+ 4
Aspectos adicionales	Carece de opción para escaneo de vulnerabilidades a través de MDM	- 1	No ofrece soporte o documentación para detección malware	- 2	Ejecuta análisis de vulnerabilidades a través de MDM	+ 4
Total: + 2			Total: + 4			Total: + 15

COMPARATIVA GENERAL





Basados en las investigaciones realizadas en la web, como grupo hemos elaborado la siguiente tabla donde hacemos una comparación entre Nessus y Nexpose.

Comparación de Herramientas Automatizadas Nessus vs Rapid7			
		Nessus de Tenable Network Security	NeXpose Rapid7
1	Características principales	Nessus de Tenable Network Security. Más que un simple escáner, es una plataforma integrada que te ofrece con la misma licencia la más extensa cobertura para la Gestión de Vulnerabilidades y verificación de configuraciones, plugins y actualizaciones de CVE, SCADA checks con las variaciones de UNIX y Linux, y Regulaciones de Cumplimiento	Rapid7 te brinda la posibilidad de clasificar las amenazas según su nivel de riesgo, además cuenta con diferentes paneles de fácil uso, que te ayudarán a entender y sacar máximo problema de la herramienta de forma rápida y simple. Con Rapid7 podrás automatizar la gestión de vulnerabilidades y riesgos de seguridad, además podrás obtener reportes en tiempo real, lo que le permitirá a tu equipo estar un paso adelante de las amenazas.
2	Version de Sistema.	NESSUS Network Security maneja tres versiones distintas, Nessus Professional, Nessus Manager y Nessus Cloud. Con la versión más básica, Nessus Profesional.	RAPID7 maneja 4 versiones, una gratuita llamada "Community Edition", que puedes utilizar por siete días para escanear un número máximo de IPs. Le siguen las versiones "Express", "Express Pro" y "Enterprise4".

3	Modelo de Escaneo	Nessus de Tenable Network Security puede detectar en sólo un día lo que otras soluciones para la Gestión de Vulnerabilidades pueden tomarle meses, incluso con el respaldo y la verificación por demás innecesaria de herramientas complementarias, con el índice de falsos positivos más bajo de la industria.	NeXpose Rapid7 No publicado
4	Interfaz gráfica.	Nessus de Tenable Network Security, tiene una interfaz fácil de usar, completamente funcional y personalizable, con un diseño intuitivo que ejecuta sin problemas ni complicaciones lo que el usuario realmente necesita.	NeXpose Rapid7 La interfaz gráfica Además de ser poco atractiva y amigable, no puede ser personalizada y presenta una falla importante respecto a los filtros que, bajo ciertas condiciones, sencillamente no funcionan.
5	Recursos	Nessus de Tenable Network Security no interfiere con los recursos de la máquina y, para evitar hacerla colapsar, incorpora Agentes alojados en el servidor que hacen menos pesada la acción del escáner, lo cual favorece la realización en paralelo de varios escaneos sin quitarle recursos al dispositivo y aprovechando al máximo sus características particulares.	NeXpose de Rapid7, si bien ya viene preconfigurada con una cantidad de políticas para iniciar el escaneo, también presenta complicaciones al momento de manejar excepciones, y estas no escalan bien. Así, puede gastarse tiempo preciosísimo en configurar políticas antes de dar y establecer la combinación ideal de permisos y restricciones con usuarios múltiples. Y esto se repite al momento de dar accesos y controlar a múltiples usuarios, lo cual debe hacerse individualmente antes de poder hacer cualquier cosa con la herramienta.
6	Sistemas operativos soportados	Soportado en sistemas: Debian/Kali Linux (varias versiones), Red Hat EL (varias versiones), CentOS (varias versiones), Oracle Linux (varias versiones), FreeBSD (varias versiones), Fedora (varias versiones), SUSE Linux Enterprise (varias versiones), Ubuntu (varias versiones), Windows Server (2008, 2008 R2, 2012, 2012 R2, 2016), Windows (7, 8, 10)	Soportado en sistemas: Red Hat EL (varias versiones), CentOS (solo v7), Oracle Linux (solo v7), Ubuntu (varias versiones), Windows Server (2008 R2, 2012 R2, 2016), Windows (7, 8.1, 10)

7	Costo de adquisición, operación y soporte del producto	Suscripción a Nessus Professional: <USD 3000/año para IP ilimitadas. Las amplias capacidades prediseñadas, la automatización y el soporte de los proveedores minimizan el esfuerzo manual.	Suscripción a Nexpose: La licencia de 500 IP comienza en >USD 10 000/año y aumenta significativamente con las IP. Costo adicional para Policy Manager. Capacidades prediseñadas, automatización y soporte de los proveedores limitados.
8	Informes con marca	Opción de añadir una marca personal (nombre/logotipo).	No disponible
9	Distribución automática por correo electrónico de los informes.	Incluida	No disponible
10	Cobertura de evaluaciones y vulnerabilidades	Más de 50 000 Cobertura de evaluación y vulnerabilidades	Menos de 42 000 Coberturas de evaluación y vulnerabilidades
11	Plantillas de escaneo	Plantillas para vulnerabilidades importantes (WannaCry, Spectre y Meltdown, etc.), auditorías SCAP y OVAL, y más.	Sin plantillas prediseñadas para WannaCry, Spectre y Meltdown, etc.
12	Resultados en tiempo real	Live Results identifica las vulnerabilidades utilizando los datos de escaneo existentes con nuevas actualizaciones de plugins para proporcionar visibilidad en tiempo real.	No disponible
13	Agrupaciones de pruebas	Grouped View presenta vulnerabilidades similares en un solo hilo para facilitar la gestión.	No disponible
14	Plantillas de cumplimiento	Más de 700 plantillas de cumplimiento y de configuración (CIS, DISA STIG, HIPAA, PCI DSS, USGCB, FDCC, y más), sin ningún costo adicional.	Se incluye un conjunto limitado de plantillas de configuración. CIS, USGCB, FDCC y políticas personalizadas disponibles por un costo adicional (licencia de Policy Manager).

15	Creación de informes personalizados	Plantillas de informes prediseñadas. Los informes pueden crearse y adaptarse con base en las vistas personalizadas.	Plantillas de informes prediseñadas. Los informes pueden crearse y adaptarse con base en las vistas personalizadas.
16	Formatos de exportación de informes	HTML, CSV, PDF, Nessus XML y Nessus DB	HTML, CSV, PDF, XML y RTF/texto
17	Informes con imagen corporativa	Opción de añadir una imagen corporativa en los reportes	Parcialmente parametrizables, no permite quitar completamente la marca del producto.
18	Investigación de seguridad de expertos	Tenable Research proporciona inteligencia esencial de amenazas y vulnerabilidades, y ha descubierto cientos de nuevas vulnerabilidades.	Rapid7 cuenta con un respetado equipo de investigación de seguridad
19	Opciones de instalación	Instalación en unidad USB en vivo, instalación en la nube o tradicional.	Instalación tradicional o en la nube
20	Cobertura de evaluaciones y vulnerabilidades	Más de 50 000 Cobertura de evaluación y vulnerabilidades	Menos de 42 000 Coberturas de evaluación y vulnerabilidades

Análisis sobre las Herramientas Automatizadas.

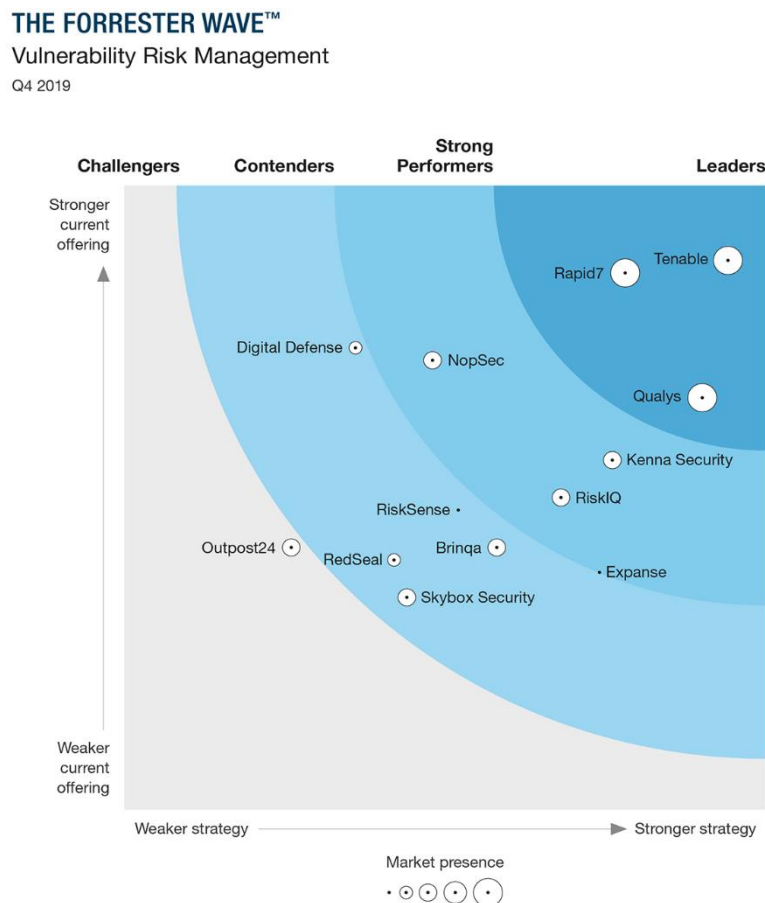
Mantener controladas las vulnerabilidades es de suma importancia para garantizar la operatividad de una organización. La responsabilidad de conocer las herramientas de seguridad informática que han surgido recae en los administradores de las bases de datos. Dos de las más populares son Nessus y Nexpose, de las cuales se ha realizado la comparación.

¿Cuál es mejor?, ¿Cuál debería usar?

Para responder a estas preguntas es importante tener claras algunas funcionalidades importantes que este tipo de herramientas debe tener:

- El software debe ayudarte a realizar un escaneo completo y continuo de las plataformas es decir debe ser multiplataforma.
- El software debe facilitar las integraciones con tecnologías como la Inteligencia Artificial para detectar contenido malicioso y mantener al mínimo los falsos positivos.
- El software debe ser automático, fácil de implementar y cumplir con las exigencias ante las amenazas en continua evolución.
- Por último, El software debe contar con su propio sistema de reportes para monitorear toda la actividad en tiempo real y poder realizar y presentar informes de la auditoria y conocer en detalle los puntos vulnerables; así como supervisar las actividades en la red corporativa de todo el personal.

Ahora tanto Tenable como Rapid7 se encuentran posicionados como las mejores herramientas de Gestión del Riesgo de Vulnerabilidades en el cuarto trimestre de 2019 según el informe de la firma consultora Forrester Wave, una de las empresas de investigación y asesoramiento más influyentes del mundo y que en esta ocasión Tenable (2019) la comparte.



Basándonos en la investigación realizada en la web sobre las herramientas automatizadas, Nessus de la empresa Tenable y Nexpose de la empresa Rapid7, podemos apreciar que las dos tienen potenciales muy similares, y al final cada empresa que necesite una herramienta de estas, deberá elegirla en base a sus necesidades y sobre todo a los equipos que posea.

Ambas herramientas nos pueden ayudar con el propósito de realizar un *pen test* de nuestras aplicaciones, una más rápidas que otra, una con reportes más parametrizables que otra, pero finalmente y lo más importante es contar con una herramienta y dominarla a la perfección pues sin ese conocimiento se vuelve indiferente las bondades de una frente a la otra.

Pero generalizando, como grupo podemos elegir y recomendar a Nessus ya que muestra una ventaja sobre Nexpose que a las empresas y administradores de las bases de datos les puede convenir y facilitar el trabajo, por ejemplo: la interfaz gráfica, la rapidez de sus análisis, la infraestructura en la nube y el monitoreo en tiempo real, y una cosa importante es su precio, Nessus es más económico que Rapid7.

CONCLUSIONES

Con el presente proyecto de investigación llegamos a las siguientes conclusiones:

- Al no realizar una gestión adecuada de vulnerabilidades, y sobre todo una corrección de estas, se pueden materializar las amenazas altas y críticas a las que se está expuesto, a tal punto de llevar a la pérdida de confidencialidad, integridad o disponibilidad de la información de la organización, afiliados y clientes.
- Así mismo concluimos que debemos implementar las buenas prácticas para el aseguramiento de nuestras bases de datos, utilizando las herramientas internacionales como los CIS Benchmarks, DISA STIGS, normas ISO y NIST.

- El uso de herramientas automatizadas es de mucha ayuda y abonan para ampliar el aseguramiento de nuestras bases de datos, ya que con ellas se pueden realizar escaneos más rápidos de las vulnerabilidades y así poder corregirlas.
- La gran mayoría de vulnerabilidades internas se encuentran asociadas a la actualización de aplicaciones, parches de seguridad y configuraciones básicas mal aplicadas o que no han sido aplicadas, por lo que son un riesgo latente para la organización.
- Una organización está protegida frente a ataques básicos externos con acceso solamente a través de internet; sin embargo, un atacante con el tiempo suficiente para realizar la exploración y explotación de vulnerabilidades, por ejemplo, diccionario de datos o inyecciones SQL, le permitirían comprometer la seguridad de la organización.
- Para finalizar, se sabe que no hay sistemas cien por ciento seguros, todos presentan vulnerabilidades, y al aplicar el proceso de Hardening o endurecimiento de forma correcta y supervisada, es una ayuda indispensable para ahorrar bastantes dolores de cabeza a los administradores de bases de datos, ya que se pretende hacerle difícil la vida al atacante, ganar tiempo para solventar vulnerabilidades a tal grado que en ocasiones se puede evitar un ataque, así mismo se evita que usuarios sin ninguna mala intención, que no tengan mucha experiencia en el uso de gestores de bases de datos, puedan poner en riesgo la información de esta.


RECOMENDACIONES

- En la actualidad no hay sistema informático cien por ciento seguro, con el avance tecnológico que se vive, han surgido nuevas herramientas de hacking y así mismo los ataques a los sistemas informáticos han ido al alza, por lo que se recomienda que el administrador de la base de datos mantenga una política de actualizaciones diarias sobre parches de seguridad y escaneo de vulnerabilidades.
- También se recomienda crear un plan de contingencia en donde se documenten todos

los procedimientos que se han implementado para la seguridad de la Base de Datos con la finalidad de que, si se hace efectiva una amenaza, se logre en corto tiempo eliminar esa amenaza y restablecer la funcionalidad eficiente de la Base de Datos.

- Se sugiere llevar un control diario de políticas de contraseñas sobre los usuarios que interactúa con la Base de Datos para así lograr una mayor seguridad de la información.
- Se recomienda auditar todos los procesos como inicios de sesión, cambios de contraseñas y otros procesos críticos en las bases de datos y generar un informe diario, en caso de que se materialice un ataque, este pueda ser de mucha ayuda para esclarecer el incidente, poder recuperar la información en un dado caso se perdiera y restablecer la funcionalidad de esta.

LICENCIAMIENTO

Con lo estudiado en el seminario de especialización de Seguridad Informática con énfasis en Hacking Ético y las enseñanzas a lo largo de toda la carrera en la Universidad Luterana Salvadoreña podemos darnos cuenta de la importancia del licenciamiento de los proyectos, por lo que adquirimos una licencia Creative Commons  [Atribución-NoComercial-SinDerivadas 4.0 Internacional](https://creativecommons.org/licenses/by-nc-nd/4.0/) la cual está plasmada al reverso de la portada de este documento.

FUENTES DE INFORMACIÓN

- BBC NEWS (2018). “Cuáles fueron los peores hackeos informáticos de la historia y porqué el que sufrió Marriot es uno de los más graves”. Recuperado de <https://www.bbc.com/mundo/noticias-46426990>
- CASAS ANGUITA, J., REPULLO LABRADOR, J., & DONADO CAMPOS, J. (2003, mayo). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos. Atención Primaria, 31(8). Recuperado de

<http://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion--13047738>

- Chávez, J. D. (2015, 07 12). Universidad Politécnica Territorial del estado Aragua. Retrieved from Principios Básicos de Seguridad en Bases de Datos, Recuperado de https://www.researchgate.net/publication/279983428_Principios_Basicos_de_Seguridad_en_Bases_de_Datos
- CIS Benchmarks. <https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/>
- Cybersecurity Insiders (2018). Recuperado de <https://www.tenable.com/whitepapers/cybersecurity-insiders-2018-application-security-report>
- DISA STIG. <https://www.stigviewer.com/stigs>
- Grammatech. (2016). Software Hardening. 2016, de grammatech.com. Recuperado de <https://www.grammatech.com/software-hardening>
- Guedez, Alexander. (2017). “Comparativa de Seguridad Digital: Tenable.io vs Qualysguard vs Rapid7”. Recuperado de <https://www.gb-advisors.com/es/comparativa-tenable-io-vs-qualysguard-vs-rapid7/>
- Instituto Nacional de Normas y Tecnología (NIST), Framework for Improving Critical Infrastructure Cybersecurity, EE.UU., 2014, <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- ISACA, (2017). Fundamentos de Ciberseguridad. Guía de estudio, 2ª Edición, USA.

- ISACA (2018). Citado por Riesgo Cero, (2019). Recuperado de <https://www.riesgoscero.com/academia/especiales/todo-lo-que-debe-saber-sobre-ciberseguridad>
- Llanos Ferraris, Diego R. (2010). "Fundamentos de Informática y Programación en C". España
- Martínez, Lorenzo. (2009). ¿Nos expresamos correctamente? 2020, de securitybydefault.com Recuperado de <http://www.securitybydefault.com/2009/11/nos-expresamos-correctamente.html>
- McAfee. (2012). McAfee. Seguridad de bases de datos de McAfee, Recuperado de <http://www.mcafee.com/es/resources/solution-briefs/sb-database-security.pdf>
- Moes, Tibor (s/f). "¿Qué es inyección SQL? Los 5 ejemplos reales de ataques. SoftwareLab Blog". Recuperado de <https://softwarelab.org/es/que-es-inyeccion-sql/>
- Montenegro Mena, L. (2012). Proceso de Hardening. Recuperado de <https://seguinfo.wordpress.com/2012/04/03/proceso-de-hardening/MySQL>
- OACENA (2016). "Ataques de SQL Injection a Sony". Recuperado de <https://www.eoi.es/blogs/ciberseguridad/2016/04/18/597/>
- PEREZ SANDOVAL, J. (2011). Universidad Carlos III de Madrid. Departamento de Informática. LAS BASES DE DATOS, SU SEGURIDAD Y AUDITORIA EL CASO MYSQL, Recuperado de <http://e-archivo.uc3m.es/handle/10016/12011>
- PowerData (2017). "La importancia de la seguridad e integridad en las bases de datos". Recuperado de <https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/la-importancia-de-la-seguridad-e-integridad-en-base-de-datos>

- Rapid7 (2019). No todos los clientes de Rapid7 utilizan Nexpose.
<https://www.rapid7.com/about/customers>
- Rothacker, Alex (s/f). “Los 10 tipos de vulnerabilidades de bases de datos más comunes”. Citado por Sharpmind Software. Recuperado de:
<http://sharpmindsoftware.com/los-diez-10-tipos-de-vulnerabilidades-de-bases-de-datos-mas-comunes.b.aspx>
- Segu-Info. (s.f.). Políticas de Seguridad de la Información. Recuperado de
<http://www.segu-info.com.ar/politicas/polseginf.htm>
- Tamayo y Tamayo, Mario (2004). El proceso de la Investigación Científica. México: Noriega Editores.
- TARLOGIC. (2016). Bastionado de sistemas (hardening). 2016, de Tarlogic. Recuperado de <https://www.tarlogic.com/servicios-ciberseguridad/bastionado-de-sistemas-hardening/>
- Tenable. (2019). Prácticamente todos los clientes de Tenable utilizan Nessus o un producto basado en la tecnología de Nessus. <https://www.tenable.com/about-tenable/about-us>.
- Tenable. (2019). Informe de Forrester Wave sobre empresas líderes en manejo del riesgo de vulnerabilidades. Recuperado de https://es-la.tenable.com/analyst-research/forrester-wave-2019?utm_source=homepage&utm_medium=tenable-website&utm_campaign=00018454&utm_content=forrester-wave#wave-form
- Villamar, E., & Gomez, J. (s.f.). VIRTUALIZACION DE SERVIDORES DE TELEFONIA IP EN GNU/LINUX. Recuperado de http://www.adminso.es/images/6/6d/Eugenio_cap1.pdf
- <https://www.digitalocean.com/community/tutorials/como-instalar-y-proteger-phpmyadmin-en-ubuntu-18-04-es>

- <https://codigofacilito.com/articulos/asignar-permisos-mysql>
- <https://dev.mysql.com/doc/refman/5.7/en/mysql-secure-installation.html>
- <https://es-la.tenable.com/products/nessus/nessus-professional>
- <https://www.rapid7.com/products/nexpose/features/>
- <https://www.rapid7.com/info/gartner-2020-magic-quadrant-siem/>