INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES

Martha Irene Romero Castro
Grace Liliana Figueroa Moràn
Denisse Soraya Vera Navarrete
José Efraín Álava Cruzatty
Galo Roberto Parrales Anzúles
Christian José Álava Mero
Ángel Leonardo Murillo Quimiz
Miriam Adriana Castillo Merino

Ingeniería y Tecnología

3ciencias

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES

Martha Irene Romero Castro
Grace Liliana Figueroa Moràn
Denisse Soraya Vera Navarrete
José Efraín Álava Cruzatty
Galo Roberto Parrales Anzúles
Christian José Álava Mero
Ángel Leonardo Murillo Quimiz
Miriam Adriana Castillo Merino

Editorial Área de Innovación y Desarrollo,S.L.

ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

C/ Els Alzamora, 17 - 03802 - ALCOY (ALICANTE) info@3ciencias.com

Primera edición: **octubre 2018**

ISBN: **978-84-949306-1-4**

DOI: http://dx.doi.org/10.17993/IngyTec.2018.46

AUTORES

Martha Irene Romero Castro, Magister en Informática Empresarial, Magister en Docencia Universitaria e Investigación Educativa, Especialista en Redes de Comunicación de Datos, Ingeniera en Sistemas, Coordinadora de la Carrera de Ingeniería en Computación y Redes, Docente Titular Principal de la Universidad Estatal del Sur de Manabí.

Grace Liliana Figueroa Moran, Magister en Informática Empresarial, Magister en Docencia Universitaria e Investigación Educativa, Licenciada en Ciencias de la Educación mención Administración Educativa, Especialista en Redes de Comunicación de Datos, Miembro de la Comisión Académica de la Carrera de Ingeniería en Computación y Redes de la Facultad de Ciencias Técnicas, Docente Titular Principal de la Universidad Estatal del Sur de Manabí.

Denisse Soraya Vera Navarrete, Ingeniero en Sistemas Informáticos por la Universidad Tecnológica Israel. Magister en Seguridad Informática aplicada por la Escuela Superior Politécnica del Litoral, Ecuador. Ex directora de Tecnología del Centro Zonal ECU911 Portoviejo, Actualmente, profesor a tiempo completo de la Universidad Laica Eloy Alfaro de Manabí (ULEAM) en la Facultad de Ciencias Informáticas (FACCI). Líder del Proyecto de Investigación "Sistema de Gestión de la Seguridad de la Información" en la FACCI-ULEAM.

José Efraín Álava Cruzatty, Ingeniero en Telecomunicaciones y Magister en Telecomunicaciones por la Universidad Católica Santiago de Guayaquil. Desde el 2008 ocupó puestos como el del INGENIERO JUNIOR en la empresa SURATEL S.A.; ANALISTA DE OPERACIÓN & MANTENIMIENTO PROVINCIAL en la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES; ANALISTA TÉCNICO en el VICEMINISTERIO DE ACUACULTURA Y PESCA; y desde el 2015 a la actualidad se desempeña como Docente en la Universidad Estatal del Sur de Manabí.

Galo Roberto Parrales Anzúles, Licenciado en Análisis de Sistemas por la Universidad Laica Eloy Alfaro de Manabí, Diploma Superior en Educación Universitaria por Competencias por la Universidad del Azuay, Magister en Educación Informática por la Universidad de Guayaquil. Investiga temas relacionados con Redes y Telecomunicaciones, Plataformas Educativas E – Learning, Plataformas de Comercio Electrónico y Marketing Digital. Actualmente Docente de la Universidad Estatal del Sur de Manabí. Ecuador.

Cristhian José Álava Mero, Ingeniero en Sistemas Informáticos, Universidad Técnica de Manabí, Master en Informática Empresarial, Universidad Autónoma de los Andes, Actualmente Docente de la Facultad de Ciencias Técnicas de la Universidad Estatal del Sur de Manabí.

Leonardo Raúl Murillo Quimiz, Ingeniero en Computación y Redes por la Universidad Estatal del Sur de Manabí, Magister en Educación Informática por la Universidad de Guayaquil. Investiga temas relacionados con redes y telecomunicaciones. Actualmente profesor y coordinador del área de seguimiento a graduados de la Universidad Estatal del Sur de Manabí. Ecuador.

Miariam Adriana Castillo Merino, Magister en Gerencia Educativa, Ingeniera en Computación y Redes, Docente contratado Carrera Ingeniería Forestal, Tecnología de la Información, Unidad de Nivelación y Admisión, Universidad Estatal del Sur de Manabí, Ecuador.

PRÓLOGO

Actualmente la informática y en especial la información es uno de los activos principales de las organizaciones y empresas, existen diferentes tipos de amenazas que atentan contra el buen funcionamiento de estos entes, como los virus, los malware, cibercriminales, spyware y un sinnúmero de amenazas existentes, diariamente se utilizan diferentes equipos en especial móviles que están conectados a internet, la mayor fuente de amenazas para la seguridad.

Este libro tiene como objetivo principal conocer los diversos conceptos de la seguridad informática, se estudiarán los mecanismos de prevención tanto preventivos, correctivos y detectivos de las amenazas que se puedan suscitar. Este trabajo de investigación está dirigido a estudiantes de informática, profesionales de la seguridad y docentes que incursionan en el mundo de la seguridad informática, ya que las herramientas descritas son usadas en varias áreas del conocimiento de la seguridad. El contenido de la obra en sus diferentes capítulos aporta conocimientos sobre los fundamentos de la ciberseguridad, conceptos sobre riesgos, amenazas y las diferentes vulnerabilidades que se pueden encontrar en la infraestructura de una organización y las posibles soluciones para mitigar estas amenazas.

También en este trabajo se analiza las diferentes metodologías para el análisis de las vulnerabilidades, la detección, los diferentes tipos de escaneos y sobre todo la remediación de las vulnerabilidades, también se hace énfasis en las diferentes herramientas para el análisis de vulnerabilidades tanto propietarias como libres y por último el capítulo final detalla un ejemplo de una auditoria de seguridad para detectar las diferentes vulnerabilidades existentes en una red de datos y por último el capítulo final trata sobre métodos de defensa en profundidad en los sistemas y la concienciación de los usuarios hacia los problemas que representan el no seguir las políticas de seguridad de la empresa.

Los autores

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

En este capítulo se analizará los conceptos relacionados a la seguridad informática, las bases principales, sus componentes, términos usados, definiciones sobre virus, criptografía y los diferentes mecanismos de prevención, corrección en seguridad informática, también se abordará temas relacionados a los diferentes mecanismos de autenticación de usuarios.

1.1. La seguridad en términos generales

Al hablar de términos de seguridad informática se debe entender a las bases que conforman los cimientos de esta ciencia, para las partes más complejas de esta disciplina, una de estas bases es el concepto de seguridad, la cual consiste en un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo, si la seguridad se aborda desde el tema disciplinario el concepto se puede definir como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, un animal, el ambiente o un bien. Existen países en donde la seguridad es un tema nacional, aunque depende del tipo de seguridad, existen muchos tipos de ésta, por ejemplo, la seguridad ambiental, la seguridad económica, la seguridad sanitaria y en casi la mayoría de los países cuando se hace un análisis de la palabra seguridad, se hace referencia a la seguridad de las personas, por ejemplo, evitar el estado de riesgo de un robo, de un daño físico o de un bien material.

La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma. Se definió que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

Así que, cuando se está buscando hacer algo más seguro, estas acciones son algo que se debe de considerar sin importar el área, se aplica a cualquier intento de tener mejor o mayor seguridad en cualquier tema que se requiera.

1.2. Concepto de seguridad informática

Lo primero que se debe mencionar es que en muchos casos se suelen confundir dos conceptos la **seguridad informática** y **la seguridad de la información**, aunque suenen muy parecidos tienen puntos clave que hacen una diferencia.

La **seguridad informática** se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y

métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.

Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

Actualmente la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y en muchos casos más compleja de manejar, ya que los procesos en muchos casos no son tan visibles para los involucrados.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes como son los siguientes:

- Los usuarios
- La información, y
- La infraestructura

Los **usuarios** son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información deben de protegerse del mismo usuario.

La **información** se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo.

Por último, está la **infraestructura** esté puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización.

Aguirre (2006), también afirma que la seguridad informática puede definirse como el conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la **información o los sistemas** ante una eventual amenaza que se pueda suscitar.

1.3. Los virus informáticos

Unos de los primeros conceptos cuando se habla de seguridad informática, es el de virus informático. Las computadoras solo entienden código binario como ceros y unos, en el mundo de las computadoras y de la informática existen muchos conceptos como el de programas, videojuegos, sistemas operativos y cualquier clase de software.

El software es uno de los conceptos más abstractos, se lo define como todo lo intangible de la computadora, son instrucciones que el ordenador espera que se realicen, las cuales pueden ser instrucciones complejas o instrucciones sencillas.

Según Beynon-Davies (2015), el término software o programa es utilizado para describir una secuencia de varias instrucciones que es leído por un computador, los cuales son escritos en un determinado lenguaje de programación que pueden ser clasificados de la siguiente manera:

- Lenguaje de máquina
- Lenguaje ensamblador
- Lenguajes de alto nivel

Analizado el tema clave sobre el software, un virus informático es un programa que tiene como objetivo dañar o cambiar el funcionamiento de la computadora. Esta es una definición bastante clara, pero el virus informático no siempre tiene que ser un programa completo, puede ser hasta cierto punto fragmentos de un programa.

Según Vieites (2013), se define al virus informático, como un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o autoreplicación, el cual trata de reproducirse de forma acelerada para extender su alcance.

Un virus informático puede hacer muchas cosas, por ejemplo, eliminar archivos, evitar accesos a las computadoras, robo de información, bloqueo de funciones de un sistema operativo o de programas dentro de una computadora. También Vieites (2013), indica que existen varios tipos de virus que se los puede definir de la siguiente manera:

- Virus de sector de arranque (BOOT)
- Virus de archivos ejecutables
- Virus de macros
- Virus de lenguajes de Script
- Malware

- Gusanos
- Troyanos
- Spyware
- Keyloggers
- Adwares
- Dialers
- Backdoors
- Otros
- Rootkits
- Bacterias
- Bombas de tiempo

Se mencionó algunos, ya que la lista es bastante grande pero la mayoría son programados para causar daños relacionados con la red y tener la capacidad de autopropagación, esto quiere decir que se multiplica el mismo muchas veces y se posiciona en partes automatizadas del sistema operativo infectado.

Las bombas de tiempo, son virus que se activan al pasar un determinado tiempo o al producir un evento, el que puede ser, por ejemplo, abrir el navegador, pero los eventos suelen ir relacionados con ciertos cálculos matemáticos y registros de memoria, aunque también existen los que se activan con tareas sencillas, estos son solamente algunos de los tipos que se podrían mencionar.

También existe el denominado software malicioso que no es considerado como virus como tal, pero que también genera daños a la computadora, algo muy importante que se debe tener claro es que, el software malicioso debe de tener ciertas características para ser considerados como virus informático, una de las características elementales es que debe de poder reproducirse y generar copias, ya que es la forma en la que se propagan teniendo un comportamiento biológico similar al de los virus que se pueden encontrar en la naturaleza y atacan a los animales y personas.

1.4. Concepto de autenticación

La autentificación se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto, no se debe cometer el error en pensar que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo o una persona.

La autenticación es bastante usada en el mundo de la computación, sólo que actualmente la contraseña del correo o de una red social ha hecho olvidar que este método de validación era ya muy común, por ejemplo, todas las credenciales que expiden para realizar una votación en determinado país es un método de autenticación, otro ejemplo es cuando se ingresa a un país y solicitan un documento

como la visa o pasaporte, también es un método de autenticación, otro caso es cuando se asigna un número de cuenta o ID de identificación en el trabajo para acceder a ciertas áreas o también para llevar un registro de los movimientos y en caso de ser necesario poder validar esos movimientos. La Figura 1 muestra un ejemplo de autentificación de usuarios.

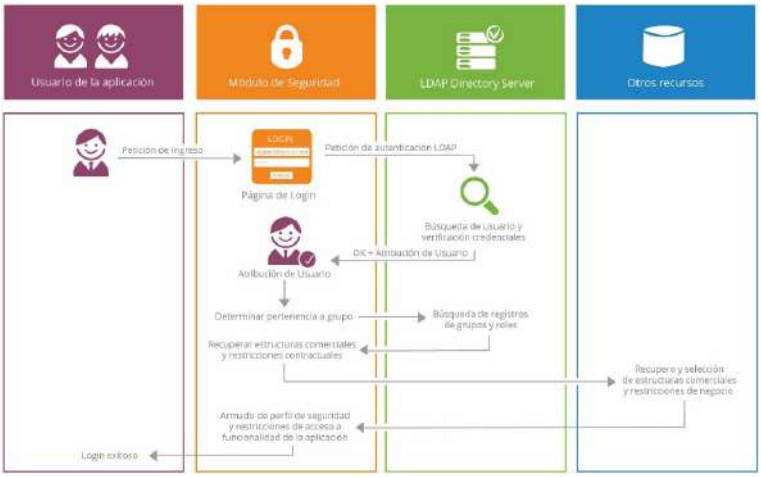

Figura 1. Autenticación de usuarios**.**

Fuente: https://sysone.gitbooks.io/isb/content/security/intro.html

Existen diversos tipos de autenticación, se va a conocer algunos de ellos los más implementados ya que todos los días se trabaja en encontrar más y mejores métodos.

Se tiene los tipos de autenticación en los que se tiene algo conocido, en teoría únicamente por el usuario, por ejemplo, una contraseña, eso es lo más común, pero en teoría, ya que, si se proporciona el usuario y la contraseña del correo electrónico, también puede entrar otro usuario y no significa que sea la persona dueña de la cuenta.

Otro tipo de autenticación es la que se basa en algo de propiedad del usuario, por ejemplo, la tarjeta de crédito, pasaportes o también son los Tokens que generan números aleatorios o palabras claves. También existen las tarjetas conocidas como inteligentes o que contienen cierta información, se pueden parecer a una tarjeta de crédito, pero el comportamiento o información puede variar.

Se tiene también los tipos de autenticación basados en una característica física, este tipo en comparación con lo que ya se mencionó se puede decir que son los más nuevos. Cuando se habla de características físicas se puede mencionar a:

- La voz
- Las huellas dactilares
- El ojo
- La escritura

La autenticación se puede considerar como parte de un método de control de acceso, la mayoría de las ocasiones esto se complementa con otras partes de un sistema, ya que hoy en día debido al manejo de la información y la personalización de los gadgets que se tiene disponibles, se vuelve una labor compleja la de tener control y manejo dentro del sistema.

Los tipos de autenticación no son excluyentes, así que, si se usa un método, no es una barrera para usar otro, de hecho, en sistemas complejos el usuario se puede encontrar con sistemas que utilizan tres tipos de autenticación, obviamente se tiene que pensar en el usuario, a veces es muy molesto siempre y cuando analizando el costo vs el beneficio.

1.5. Mecanismos preventivos en seguridad informática

Los mecanismos preventivos en la seguridad informática son los más olvidados, los cuales son vistos como una pérdida de tiempo, la parte administrativa en la mayoría de los casos lo ve como un costo extra, es algo parecido como por ejemplo, con los seguros médicos o seguros de vehículos, se puede pagar 10 años el seguro de un carro y nunca tener un accidente, en primera instancia se podrá analizar que es algo muy bueno, pero después en algún momento se podrá pensar que es un desperdicio haber pagado una cantidad 10 años y sin usarla.

La definición de los mecanismos preventivos, consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos. Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero.

La mayoría de los ataques informáticos se pueden evitar o por lo menos disminuir el impacto, si se hiciera utilizando mecanismos preventivos, deficiencia de sistemas y otros problemas podrían encontrarse, evitarse y resolverse gracias a un buen trabajo durante esta etapa. La Barrera más fuerte a la que se enfrenta una empresa al querer aplicar los mecanismos preventivos, es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización.

Entre los elementos que se pueden aplicar en los mecanismos preventivos se puede mencionar a:

- El respaldo de información: Es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general, las empresas entienden que los problemas con información son muy costosos, parece muy fácil pero seleccionar los mecanismos de respaldo no es tan sencillo como se analizar, se tiene que considerar los siguientes factores: Qué formatos de archivo se tienen, por ejemplo, MP3, archivos de texto, bases de

datos y otros, las imágenes y vídeos por ejemplo, son archivos que normalmente necesitan atención especial.

- Horario de respaldo: Otro reto es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.
- Control de los medios: El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.
- La comprensión de la información: No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas.

Estos son sólo algunos de los puntos que se deben considerar, solamente para el mantenimiento y respaldo de la información. Otros ejemplos de proceso que se tienen en el mecanismo preventivo son:

- Actualización de sistemas
- Antivirus
- Firewall
- Navegación por internet
- Contraseñas
- Accesos remotos.

Estos son sólo algunos de los procesos, pero la organización puede personalizar lo que quiere considerar en los mecanismos preventivos.

1.6. Mecanismos correctivos en seguridad informática

Los mecanismos correctivos tienen una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo, así que, contratar expertos para resolver el problema o el tiempo que le dedicara a el equipo de trabajo siempre va a costar mucho, en un porcentaje muy alto se acaban pagando servicios de solución a otras empresas, adquiriendo soluciones o comprando software y parches de actualización que logran resolver el problema.

Otra característica de los mecanismos correctivos es que el tiempo es limitado, así que el tiempo se vuelve algo muy apreciado en estos casos, pero también es muy escaso. Probablemente la empresa o la persona puede poder obtener dinero, pero tiempo es casi imposible.

Dentro de los mecanismos de corrección se tienen diferentes pasos de ejecución para enfrentar este problema serio en los que se puede mencionar:

- Catalogación y asignación de problemas: En este paso se hace un catálogo de los problemas a los que se pueden enfrentar, detectar y clasificar es algo muy recurrente en todo lo relacionado con la seguridad informática, ya que es una forma para poder saber cómo abordar las situaciones y buscar alguna respuesta o solución a lo que se presenta.
- Análisis del problema: En este paso es muy evidente que la actividad que se hace es analizar el problema que se ha presentado, en muchos casos esta parte se realiza por los expertos, ya no, por las personas involucradas en el problema.
- Análisis de la solución: Antes de intentar solucionar el problema se debe de analizar la propuesta de la solución, se ha cometido un error, puede ser que no de forma directa, pero es un error, el impacto no va a ser más o menos, si es culpa del usuario o de un tercero, así que la solución tiene que estar bien planteada y ejecutada. Antes de empezar a realizar los cambios, actualizaciones y movimientos se debe tratar de analizar y de predecir qué es lo que va a suceder.
- La documentación: Este componente es vital, ya que los cambios que se hacen probablemente son algo que se hizo con un tiempo limitado, rápido y que involucraron muchos recursos, así que la documentación es muy importante, ya que puede ser que por las velocidades no se recuerden todos los pasos y cambios que se han realizado. En caso de encontrar algún problema se puede consultar la documentación para detectar si la solución era correcta.

1.7. Mecanismos detectivos en seguridad informática

Los mecanismos de detección son los más complejos y son en los que se necesita tener alto grado de conocimientos técnicos dependiendo de la materia que se aborde, por ejemplo, seguridad de plataformas en línea, en específico de un tipo de bases de datos o tecnología como Wordpress, esto depende del sistema, aplicación o el ecosistema que tenga funcionando.

Los mecanismos de detección parten de que se tiene la idea de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial a un determinado recurso. Siempre que se trabaja en los mecanismos de detección se tiene la premisa en mente, se debe de trabajar como si lo que se fuera a encontrar es lo peor y se debe estar preparados para la peor de las situaciones posibles.

Estos mecanismos de detección tienen dos objetivos:

- Poder detectar el punto exacto del ataque para poder llegar a una solución y recuperarse del mismo, pero no siempre es posible esto, depende de los problemas que se afrontan.
- Detectar la actividad que se considera sospechosa y conocer lo sucedido, ya que si no se encuentra donde fue el ataque, lo mínimo que se necesita es saber qué fue lo que sucedió y partir de esa parte.

Lo que es ideal es que se cumpla el objetivo primero, pero no siempre sucede lo ideal, así que se tiene que adaptar al problema, a la situación y todo lo que va saliendo en cada uno de los casos.

Uno de los conceptos que están inmersos en este tipo de mecanismos es la **intrusión**, la cual se la define como una secuencia de acciones realizadas de forma deshonesta, en donde la mayoría de las ocasiones se quiere lograr acceso no autorizado. Dentro de los mecanismos de detección el término más famoso de seguridad informática es el de detección de intrusiones, la cual se define como el proceso de identificación y respuesta ante las actividades ilícitas observadas contra algunos recursos de la red, sistema, plataforma o empresa.

Los mecanismos de detección de intrusión tienen unos pasos que se ejecutan como manera básica de detección que se menciona a continuación:

Revisión de patrones de acceso: En este caso lo que se hace es ver los patrones de acceso, esto quiere decir que se va a analizar los accesos y tratar de encontrar si se está manejando un patrón, por ejemplo, acceso a determinadas horas o el mismo usuario haciendo accesos a la misma sección o módulo. Los patrones siempre van a indicar algo, pueden ser muchos o Las mayorías falsas alarmas, pero es seguro, que si se hizo un ataque se puede encontrar patrones que llamen la atención para después encontrar el problema.

Revisión de transacción: En la mayoría de los casos se obtienen ciertos archivos o se intenta descargar o subir algo de información, así que la transacción es un método muy rápido para lograr esto, la mayoría de los intentos van a ir acompañados de al menos una transacción, esto no es una garantía, pero es algo muy probable, siempre durante la detección si se logra encontrar una transacción es como encontrar el objetivo del atacante lo cual es muy valioso.

Bloqueo automático: Algunas aplicaciones no tienen un sistema de bloqueo, así que, aunque en algunos casos se encuentre el problema y ya se tenga las razones, Si no se cuenta con un mecanismo de bloqueo de emergencia, el atacante podrá seguir haciendo lo que quería. Algunos de los mecanismos de bloqueo comunes son los de paro absoluto, es decir el bloqueo del sistema completo, es algo un poco drástico, pero en muchas ocasiones no se quiere otro riesgo y se considera la mejor opción a la mano.

1.8. El concepto de encriptación en seguridad informática

La encriptación o también conocido como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea la autorizada, aunque el mensaje sea interceptado, como en muchos casos la información simplemente no significa nada para el interceptor, ya que no cuenta con los elementos involucrados en la encriptación, así que la información simplemente no sirve, la Figura 2 muestra un ejemplo de encriptación.

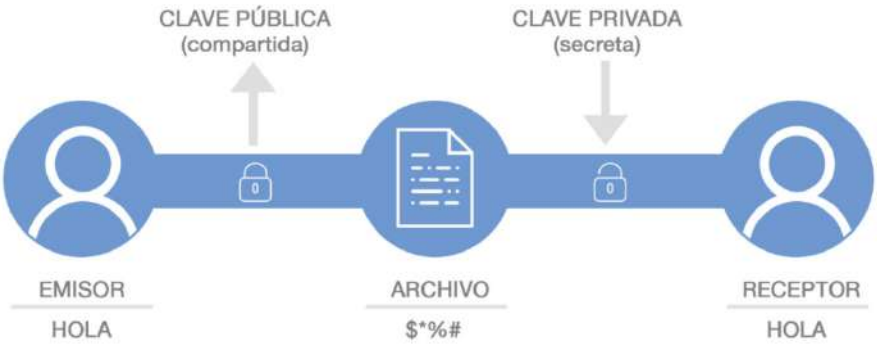

Figura 2. Ejemplo de encriptación.
Fuente: https://www.nextvision.com/2017/08/24/todo-sobre-encriptacion-de-datos-para-empresas/

Se puede decir también, que la encriptación busca la seguridad y la persistencia de los datos mediante un proceso en el cual se involucran algunas partes claves dependiendo del método, por ejemplo, en algunos métodos se utilizan contraseñas o llaves para autentificar la encriptación y la desencriptaciòn de la información, siempre se debe de recordar los objetivos principales de la encriptación y cifrado de datos que se nombran a continuación:

- Confidencialidad
- Autenticación
- Integridad de los datos

La confidencialidad consiste en que la información sólo puede ser accedida por su legítimo dueño o destinatario, la autentificación quiere decir que el emisor y el receptor son los que pueden confirmar la identidad, finalmente la integridad de la información significa que no debe ser posible que sea alterada en caso de que sea interceptada la información.

Según Marrero Travieso (2003), existen muchas amenazas de varias fuentes principalmente de internet que pueden ser:

- Correos electrónicos infectados por virus
- Firewalls mal Configurados
- Suplantación de contraseñas
- Contraseñas débiles
- Robo y destrucción de información, etc.

1.8.1. Métodos de encriptación

Algunos de los métodos de encriptación disponibles actualmente y que son bastantes conocidos se puede mencionar a:

- Encriptación simétrica
- Encriptación asimétrica de clave pública y privada

- Encriptación WPA
- Encriptación WEP
- Firma digital

Estos métodos mencionados anteriormente son la mayoría que se va a encontrar en el mundo de la seguridad informática. Estos métodos de encriptación son bastantes buenos para almacenar y transferir la información.

Encriptación simétrica

Según (Santos, 2014) este tipo de criptografía está basado en métodos criptográficos que usan una misma clave para cifrar y descifrar el mensaje, estos extremos cuando establecen la comunicación deben establecer un acuerdo sobre la clave que tienen que usar, para posteriormente los dos tener acceso a la misma clave, en donde el remitente cifra el contenido de la misma y el destinatario la descifra con el mismo mecanismo. Se puede indicar varios ejemplos de cifrado simétrico.

- Algoritmo de cifrado DES, usa claves basados en 56 bits
- Algoritmos de cifrado 3DES, Blowfish, e IDEA, usan claves de 128 bits
- Algoritmos de cifrado RC5 y AES

Encriptación asimétrica

También (Santos, 2014) indica que este tipo de encriptación se basa en que si el emisor cifra la información el receptor lo puede descifrar o viceversa, en este caso cada usuario del sistema debe poseer una pareja de claves y se tiene dos tipos.

- Clave privada: Custodiada por el propietario, por lo tanto, solo él tiene acceso a ella sin darla a conocer a nadie.
- Clave pública: conocida por uno o todos los usuarios

Como ejemplo de este tipo de algoritmos usados por este tipo de cifrado se tiene a **MD5** y **SHA**.

Firma digital

La Firma digital, es algo habitual en el uso de documentos oficiales, es decir documentos que involucran a una institución gubernamental. El objetivo de la firma es autentificar la identidad de quién envía el mensaje y quién firma el documento, las firmas digitales acostumbran manejar diferentes datos, además de información que se envía, por ejemplo, la hora y la fecha en que se hizo.

La firma digital es una forma matemática de adjuntar la identidad de una persona a un mensaje, está basada en la criptografía de clave pública, esto quiere decir que estos sistemas están utilizando dos claves, la primera sería la clave pública que es la que se conoce y la otra clave sería una clave privada qué es la que solamente el emisor del mensaje conoce.

Encriptación WEP y WPA

La encriptación WEP y WPA tienen algo en común, las dos son aplicadas a las señales inalámbricas y están basados en protocolos de conexión Wifi la primera y la segunda se basa en servidores de autentificación.

En el caso de WEP se tiene tres opciones, de 64 bits, de 128 bits y 256 bits, en donde la más utilizada es la de 128 bits ya que ofrece un buen nivel de seguridad sin tener que ser tan grande y sin aumentar lo complicado del tema. Actualmente la encriptación de 256 bits aún no es soportada por todos los dispositivos.

Existen siempre diferentes opiniones de cómo es que se puede considerar a un método de cifrado, como un buen método de cifrado o un método confiable, pero se puede llegar a una conclusión, un sistema de cifrado se puede considerar como bueno cuando la seguridad de cifrado consiste en la clave y no en el algoritmo.

Aunque se conozca el algoritmo, no se puede llegar a un descifrado de la información gracias a la clave. La mayoría de las aplicaciones que se dan a la encriptación hoy en día son:

- Mensajes de autenticidad
- Facturas electrónicas
- Banca electrónica
- Votos electrónicos
- Notificaciones
- Mensajería instantánea
- Correos electrónicos
- Almacenamiento de información

CAPÍTULO II: FUNDAMENTOS DE LA CIBERSEGURIDAD

En este capítulo se analizará los conceptos relacionados a la ciberseguridad, sobre las amenazas, riesgos y vulnerabilidades que hay en una organización, se tratará también sobre las diferentes superficies de ataques que pueden existir para que un cibercriminal pueda lanzar su ataque, se analizará en que consiste la ingeniería social y la ley de mínimos privilegios.

2.1. Los tres pilares de la seguridad

Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores y clientes de la empresa, la base de datos de facturación son datos estructurados de tal forma que se convierten en información, que aportan valor como compañía.

Los pilares de la seguridad de la información se fundamentan en esa necesidad que todos tienen de obtener la información, de su importancia, integridad y disponibilidad de la información para sacarle el máximo rendimiento con el mínimo riesgo. La Figura 3 muestra los principales pilares de la seguridad de la información.

Figura 3. Pilares de la seguridad**.**
Fuente: Elaboración propia.

Según la Figura 3, la seguridad está fundamentada por 3 pilares, pero puede haber más que puedan fundamentar a la seguridad, en este caso, si alguno de los lados es débil se perderá seguridad o usabilidad, si falta alguno de los lados la organización queda expuesta a ataques, para esto se debe conocer en detalle cuál es la función de cada lado en el gráfico.

Ahora que se compre la importancia de la información se puede deducir que si aquella, que es vital para la organización cayera en manos inapropiadas puede perder su valor, se perderá intimidad o capacidad de maniobra y además la reputación puede verse dañada sin contar con que la información puede ser accedida por cibercriminales y cualquier otra potencial fuente de riesgos para un determinado proyecto.

Confidencialidad: La confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas, para garantizar la confidencialidad se recurre principalmente a tres recursos:

- Autenticación de usuarios: Sirve para identificar qué quién accede a la información es quien dice ser.
- Gestión de privilegios: Para los usuarios que acceden a un sistema puedan operar sólo con la información para la que se les ha autorizada y sólo en la forma que se les autorice, por ejemplo, gestionando permisos de lectura o escritura en función del usuario.
- Cifrado de información: Según Costas Santos (2011), el cifrado también denominado encriptación, evita que ésta sea accesible a quién no está autorizado, para ello se transforma la información de forma inteligible a una no legible y es aplicable tanto a la información que esté autorizado para ello como para la que no lo está, sólo mediante un sistema de contraseñas puede extraerse la información de forma inteligible y es aplicable tanto a la información que está siendo transmitida como a la almacenada.

Los principios de confidencialidad no solo deben aplicarse para proteger la información sino todos aquellos datos e información de los que sea responsables. La información puede tener carácter confidencial no solo por ser de alto valor para la organización, sino por ejemplo porque puede estar amparada por legislación de protección de datos de carácter personal, un ejemplo de violación de la confidencialidad son las filtraciones sufridas por entidades bancarias, grandes empresas y gobiernos para exponer públicamente algunas de sus actividades.

La integridad: Es el segundo pilar de la seguridad, consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas. Para garantizar la integridad de la información se debe considerar lo siguiente:

1. Monitorear el tráfico de red para descubrir posibles intrusiones.
2. Auditar los sistemas para implementar políticas de auditorías que registre quien hace que, cuando y con qué información.

3. Implementar sistemas de control de cambios, algo tan sencillo como por ejemplo comprobar los resúmenes de los archivos de información almacenados en sistema para comprobar si cambian o no.
4. Como otro recurso se tiene las copias de seguridad, que en caso de no conseguir impedir que se manipule o pierda la información permitan recuperarla en su estado anterior.

Disponibilidad: Para poder considerar que se dispone de una seguridad mínima en lo que a la información respecta, se tiene a la disponibilidad, de nada sirve que solo el usuario acceda a la información y que sea incorruptible, si el acceso a la misma es tedioso o imposible, la información para resultar útil y valiosa debe estar disponible para quien la necesita, se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles, por ejemplo un ataque distribuido de denegación de servicio o DDoS puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar. Ogro ejemplo de perdida de disponibilidad sería que la dirección de correo electrónico sea utilizada para lanzar campañas de spam y en consecuencia añadida a listas negras, impidiendo que ninguno de los destinarios de los emails legítimos los reciba. Para este propósito se implementan políticas de control como:

- El acuerdo de nivel de servicio o (SLA).
- Balanceadores de carga de tráfico para minimizar el impacto de DDoS.
- Copias de seguridad para restauración de información perdida.
- Disponer de recursos alternativos a los primarios.

La información y sistemas son seguros si sólo accede a la información y recursos quién debe, sí se puede detectar y recuperar de manipulaciones voluntarias o accidentales de la información y si se puede garantizar un nivel de servicio y acceso a la información aceptable según las necesidades.

Carpentier (2016), indica que el uso de sistemas de información implica establecer normas y procedimientos aplicados al uso y sistemas de información ante posibles amenazas como:

- Elaborar varias normas y procedimientos.
- Definición de acciones que deben emprender las personas.
- Definición del perímetro que se va a afectar.

2.2. Evaluación de riesgos, amenazas y vulnerabilidades

Cuando se plantea mejorar la seguridad de una empresa se debe tener en cuenta varios factores que se muestra a continuación:

- Recursos
- Amenazas

- Vulnerabilidades
- Riesgos

Se entiende a los recursos como los bienes tangibles e intangibles con los que se cuenta para realizar las tareas, la información de que se dispone es un bien intangible, ya sean las bases de datos de clientes, proveedores, los manuales de producción, las investigaciones y las patentes. Por otro lado, se tiene a los bienes tangibles, qué son los recursos físicos de que se dispone en la empresa, servidores, equipos de red, computadoras, teléfonos inteligentes, vehículos, bienes inmuebles, etc., la Figura 4 muestra un ejemplo de bienes tangibles e intangibles.

Figura 4. Ejemplo de bienes tangibles e intangibles**.**
Fuente: https://ciberconta.unizar.es/ifinanzas/10-intangibles.htm

El **riesgo** es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional.

Las **amenazas** son esos sucesos que pueden dañar los procedimientos o recursos, mientras que las **vulnerabilidades** son los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirían que una amenaza tuviese éxito a la hora de generar un problema. El principal trabajo de un responsable de la seguridad es la evaluación de los riesgos identificando las vulnerabilidades, amenazas y en base a esta información evaluar los riesgos a los que están sujetos las actividades y recursos. Se debe considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad se puede aplicar la representación clásica que indica lo siguiente, mostrado en la Figura 5.

Figura 5. Fórmula para medir el riesgo**.**
Fuente: elaboración propia.

La Figura anterior indica que el riesgo es igual al resultado de sumar el impacto producido por la amenaza por la probabilidad de que una vulnerabilidad permita que dicha amenaza tenga éxito.

En un sistema de evaluación de riesgo sencillo se podría asignar un valor numérico a la importancia de una vulnerabilidad y otro valor a la importancia de una amenaza, la tabla 1 muestra un ejemplo de evaluación de riesgos.

Tabla 1. Comparativa de evaluación de riesgos.

Amenaza	Impacto	Probabilidad	Riesgo
Robo de credenciales en un sistema de control biométrico	3	0	0
Infección por Spyware	3	2	6
Pérdida de suministro eléctrico	1	1	1

Fuente: elaboración propia.

En la tabla anterior las amenazas que no causan daño tendrían un impacto 0, mientras que las que causan un gran daño tendrían un valor de impacto igual a 3, del mismo modo la probabilidad puede ser nula, baja, media o alta, con lo que se podría dar valores de probabilidad de 0 a 3, multiplicando ambos valores se obtendría el valor de riesgo, de esta forma se podría clasificar los distintos riesgos a los que se está expuesto y actuar en consecuencia, empezando por los de mayor gravedad, por ejemplo, si existe una amenaza de ataques mediante robo de credenciales para acceder a un recurso cifrado, el impacto de perder dicha información seria alta, pero ya que se tiene un sistema de autenticación biométrico, las probabilidades de que exista una probabilidad aprovechable son prácticamente nulas, por lo tanto el riesgo es cero para esa amenaza.

Tipos de amenazas

Existen amenazas difícilmente controlables como las naturales como los desastres o errores humanos, pero que deben ser tenidas en cuenta a la hora de calcular riesgos, una persona podría borrar accidentalmente información de un servidor o podría enviar un correo electrónico con información confidencial a un destinatario erróneo, del mismo modo el Hardware de los recursos informáticos de la empresa puede verse dañado por el uso, por inundaciones, fallas eléctricas, etc.

En cambio, las amenazas voluntarias son aquellas de derivan de ataques deliberados ya sean de agentes internos o externos de una organización, los agentes internos pueden ser por ejemplo empleados descontentos o ex empleados cuyas credenciales

de acceso no han sido revocadas. Mientras que los agentes externos pueden ser competencia desleal, activistas, terroristas, cibercriminales, etc.

Vulnerabilidades.

Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a 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 que permite que un agente externo, acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta.

Por ejemplo si se usa el gestor de contenidos Wordpress para desarrollar una página web, se puede buscar vulnerabilidades del CMS, de algunas de sus plantillas o de los plugins que se utilizarán para dar funcionalidad a la página web en https://wpvulndb.com/, la Figura 6 muestra la página principal de este sitio de búsqueda de vulnerabilidades.

Figura 6. Sitio web de vulnerabilidades de sistemas**.**

Fuente: https://wpvulndb.com/

Si se busca base de datos más amplia o relativas a más sistemas se puede acudir a las bases de CVE o Common Vulnerabilities and Exposures, por ejemplo, se puede recurrir al boletín de vulnerabilidades del Centro Criptológico Nacional de España o CCN-CERT, la Figura 7 muestra la página principal de este buscador de vulnerabilidades.

Figura 7. Base de datos de vulnerabilidades de España**.**
Fuente: https://www.ccn-cert.cni.es/

En este tipo de buscadores se puede filtrar la información de vulnerabilidades expuesta por fabricantes, versiones, recursos, etc., y pueden estar gestionados por equipos de respuestas a incidentes informáticos por sus siglas en inglés CERT, pertenecientes a instituciones tanto públicas como privadas que comparten y difunden esta información, ya que la mejora global de la seguridad incrementa la seguridad individual y fuerza a desarrolladores y fabricantes a eliminar vulnerabilidades de sus sistemas. Por ejemplo, la tabla 2 analiza un caso práctico de evaluación de riesgos.

Tabla 2. Evaluación de riesgos en una empresa.

Amenaza	Impacto	Probabilidad	Riesgo
Robo de credenciales en sistema de identificación biométrico	3	0	0
Infección por Spyware	3	2	6
Pérdida de suministro eléctrico	1	1	1
Ataque por ransomware	2	2	4

Fuente: elaboración propia.

En este caso si se dispone de un servidor de almacenamiento de ficheros y se consideran las distintas amenazas que pueden afectarle, se tendría por ejemplo el acceso no autorizado, la infección por spyware, la pérdida de suministro eléctrico o la infección por ransomware, el impacto de cada caso sería alto para el acceso no autorizado, porque sería imparable, alto para el spyware porque podría filtrar información de forma oculta sin acceso físico, bajo para la pérdida de suministro eléctrico ya que sería fácil de solucionar y medio para el ransomware, ya que sólo se necesitaría restaurar copias de seguridad.

Respecto a la probabilidad dado que se obtiene control de acceso biométrico, la posibilidad de robo de credenciales es nula, la probabilidad de infección por malware es media, suponiendo que no se tenga las medidas, idóneas la misma probabilidad se aplicaría a el ransomware, la pérdida de suministro eléctrico sería de baja probabilidad. Por tanto, los riesgos de mayor a menor importancia quedarían de la siguiente manera:

1. Infección por spyware
2. El ransomware
3. La pérdida de suministro eléctrico
4. Robo de credenciales

2.3. Ley de mínimos privilegios

Al implementar cualquier sistema organizativo, de reparto de tareas y responsabilidades se debe tener claro que no todo el mundo tiene porque acceder a todos los recursos de la organización, ni tiene que hacerlo de forma permanente. Cada individuo y cada herramienta debe acceder solo a aquello imprescindible para el desempeño de sus funciones, sabiendo a lo que se puede acceder y a lo que no, hay que decidir qué se puede hacer con la información o recursos a los que se tiene acceso, a esto se le denomina **privilegios y permisos.**

Los **privilegios** son permisos de actuación que un usuario, sea una persona o un sistema tiene para actuar sobre otros recursos, la Figura 8 muestra un ejemplo de privilegios asignados a un usuario.

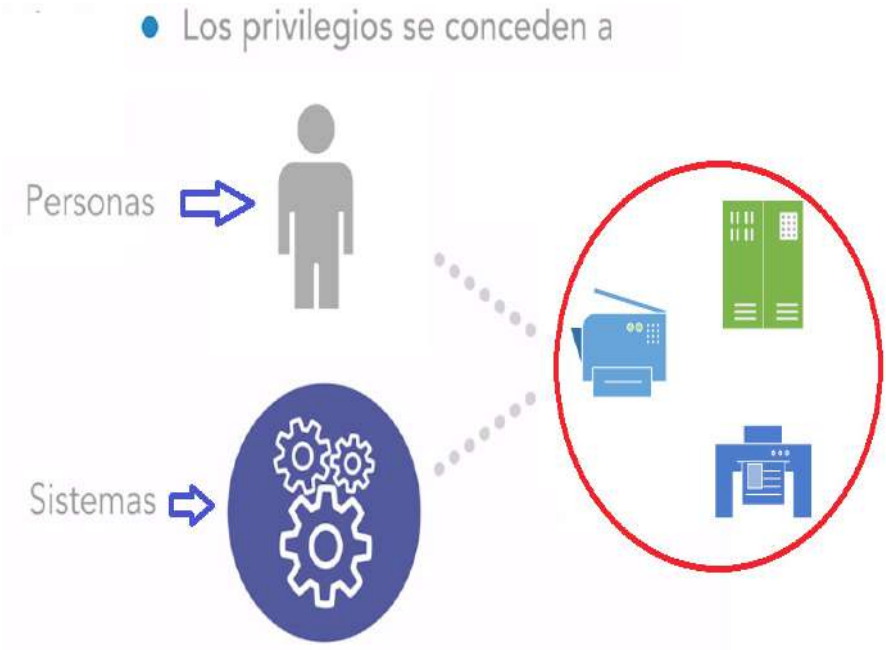

Figura 8. Concesión de privilegios**.**
Fuente: elaboración propia.

Uno de los sistemas más conocidos de privilegios, es el de los tipos de cuentas de usuario de un sistema operativo, tanto en Windows, Mac o Linux las cuentas de usuarios se dividen básicamente en usuarios normales y administradores, aunque se pueden crear más grupos con características específicas.

Los usuarios normales solo pueden hacer uso de las herramientas que hay instaladas en la computadora y acceder a la información de su directorio de usuario, los administradores tienen privilegios para acceder a otras estructuras de archivos que no sean las propias de su usuario, pueden instalar o eliminar software del sistema y pueden cambiar parámetros de configuración del sistema operativo como por ejemplo la configuración de red.

La ley de mínimos privilegios establece que para la realización de una tarea, un usuario debe disponer de los privilegios mínimos necesarios durante el tiempo imprescindible y con el alcance limitado a lo que exija la tarea, por ejemplo si se trabaja con una computadora se debería tener un usuario normal y otro con privilegios de administrador, de este modo solo se usaría el usuario administrador cuando se tuviese que hacer cambios de configuración, instalar o desinstalar software, aplicar actualizaciones parches de seguridad o gestionar las copias o respaldos, el resto del tiempo para operar con el contenido habitual, para navegar por internet, gestionar el correo electrónico, etc., se operaría con un usuario sin privilegios especiales lo que minimiza el riesgo de infección por malware, espionaje, filtración de datos, corrupción de archivos del sistema y demás, la Figura 9 muestra los privilegios mínimos necesarios de un usuario.

Figura 9. Mínimos privilegios necesarios de un usuario**.**
Fuente: elaboración propia.

Se puede ver el usuario con el que se está operando en Windows a través del comando "**whoami**" en la línea de comando, lo cual indica el nombre de la computadora y el nombre de usuario, si se añade unos complementos al comando sé informará a que grupo pertenece y de los privilegios asignados como se muestre en la Figura 10.

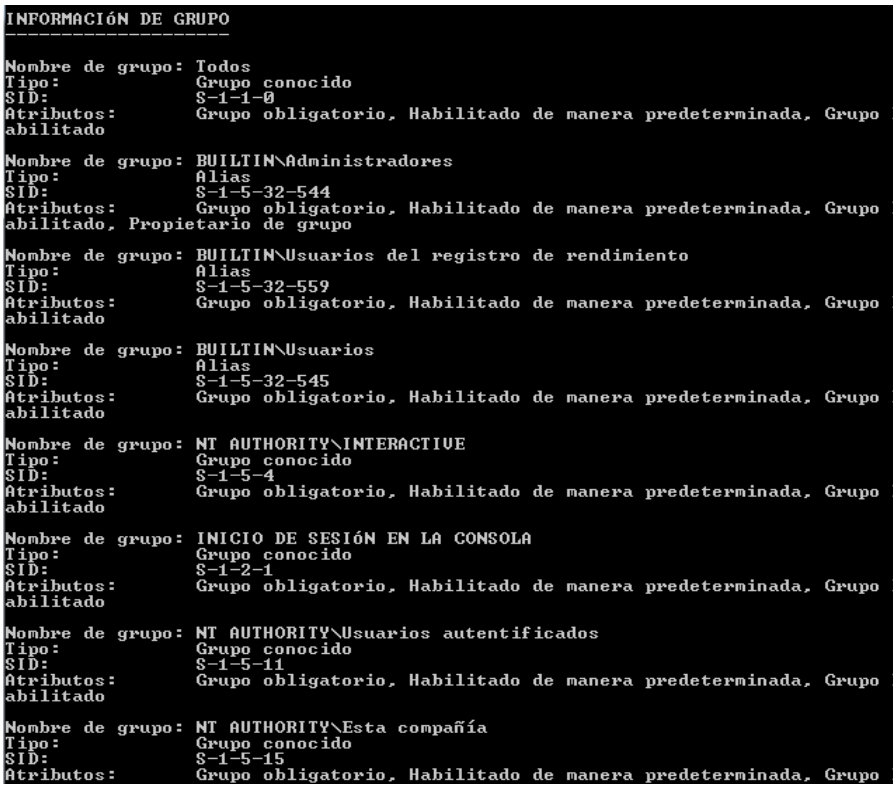

Figura 10. Comando para verificar permisos y roles de usuario en Windows**.**

Fuente: elaboración propia.

Si se ejecuta el mismo comando como administrador se muestra una lista de privilegios más larga. Conceder los permisos adecuados a cada usuario de un sistema, es tan importante para la disponibilidad, como lo es para la confidencialidad y la integridad revocar ese permiso cuando ya no sea necesario, por esto que las políticas de privilegios no solo deben ocuparse de la asignación, también de la revocación de los mismos, por ejemplo, cuando un empleado cambia de departamento, abandona la empresa o está de vacaciones.

2.4. Ingeniería social

Según Hadnagy (2011), La ingeniería social es cualquier acto que induce a una persona a realizar una acción que puede, o no, ser en su mejor interés.

Los fundamentos de la ingeniería social se basan en la forma de aplicar determinados conocimientos psicológicos y sociológicos fundamentales, es decir no se trata de conocimientos excesivamente complejos porque el atacante normalmente no dispone de muchos detalles de su víctima y tiene que basarse en generalidades, estadísticamente válidas para obtener en la misma proporción resultados estadísticamente positivos. La ingeniería social se nutre inicialmente de una serie de conceptos básicos y estadísticamente ciertos de la psicología del individuo, entre estos conceptos destacan 4 que hacen a la persona más vulnerables a este tipo de acciones como son:

- No decir "NO"
- Exceso de confianza
- El exceso de halagos hacia la persona
- Empatía

A la persona le cuesta decir "**NO**", es fácil escuchar a alguien solo con un sí a una petición, pero cuando se trata de decir no, casi nunca nos escuchamos tal cual, sonaría grosero, ese no casi siempre va acompañado de una excusa, porque a las personas les gusta ayudar a los demás, los hace sentir bien y cuando quieren decir no se necesita razonarlo y excusarlo tanto a la persona a la que se lo dicen cómo a la persona misma, por eso sí el ingeniero social es capaz de neutralizar el uso de excusas, estará cerrándole las puertas al objetivo que se encontrará en la encrucijada entre decir simplemente no o ceder a la petición sea total o parcialmente.

La **confianza**, las personas son confiadas por naturaleza, si algo es permisible la mayor parte de la gente lo dará por válido, se tiende a creer en las cosas sí parecen reales lo sean o no, el más claro ejemplo está en la gran cantidad de noticias falsas y cadenas que se distribuyen en las redes sociales como Facebook o WhatsApp.

La **adulación**, a las personas les encanta que los adulen, todos buscan reconocimiento en la vida profesional, particular o sentimental, se quiere ser reconocido en la empresa, en la familia o en el deporte que se practica, cuando se alimenta el EGO la sensación de superioridad hace sentir segura al individuo y en consecuencia se baja el nivel de atención a otros detalles.

La **empatía**, un buen ingeniero social aprovecha esta vulnerabilidad para que la persona se preocupe por sus simulados problemas de forma que ayudarle, haga sentir mejor al individuo que atender a sus propias preocupaciones.

La **tribu o los clanes**, desde el punto de vista más sociológico la principal barrera o vulnerabilidad según se mide para un ingeniero social, es la tribalizaciòn, los clanes, todos somos vulnerables en cuanto a que por defecto confiamos, esta confianza es más fuerte si cabe con la gente del círculo cercano, la familia, los amigos, compañeros de trabajo. La persona es más receptiva a todo aquello que les cuenta gente del clan o tribu, es más fácil creer en algo que diga la madre o el hijo, que lo que le cuente cualquier extraño y por difícil que resulte de creer, el asunto del que le hablen carece totalmente de importancia.

El **contexto**, al hablar de tribu o clan no solamente se habla de la gente que se conoce directamente, también se habla de los contextos, ya que el elemento de una tribu a la que se pertenece, sólo tendrá sentido en dicho contexto.

Una de las formas más habituales de uso de la ingeniería social para atacar infraestructuras informáticas es la obtención de información personal de la plantilla de una organización, consciente que dicha información permita descubrir contraseñas y acceso a recursos restringidos. También se usa la ingeniería social para generar campañas genéricas de email fraudulentos conocidas como **Phishing**, destinadas a distribuir por ejemplo malware.

Actualmente la ingeniería social es el principal método de distribución de ransomware, un malware que cifra los archivos y pide un rescate económico. El Phishing funciona porque el email parece auténtico, suplanta la identidad corporativa de una empresa reconocible, es muy común suplantar a compañías eléctricas, proveedores de servicios telefónicos, el caso del espía Phishing es una variación del Phishing que, en lugar de distribuirse masivamente, emplea email redactados y diseñados para engañar específicamente a una persona. Es común suplantar a un miembro de la compañía de posición jerárquica, a un proveedor o aun cliente, así consiguen crear una historia consistente capaz de engañar a la víctima específica mediante la ingeniería social.

Para defenderse de los ataques de ingeniería social se debe ser siempre meticuloso a la hora de identificar la identidad e quien nos escribe o visita alguna oficina y la titularidad de las páginas web que se visita, de este modo será más difícil caer en los engaños de lo que aparentemente son visitas, correos electrónicos o páginas web normales.

2.5. Superficie de ataque

Los elementos que conforman la superficie de ataque de una infraestructura, es la totalidad de elementos susceptibles de tener vulnerabilidades que pueden ser explotadas por un incidente natural o por un ataque deliberado.

Entre los elementos que conforman la superficie de ataque de una infraestructura IT, se tiene a los dispositivos de red como router, switch o firewall, también las computadoras, servidores y sistemas de almacenamiento en red de la infraestructura, así como los sistemas operativos, aplicaciones y firmware implementados en todos esos equipos, incluso las personas que usan y administran toda esa tecnología forman parte de la superficie de ataque de esa infraestructura, ya que tienen sus propias vulnerabilidades, la Figura 11 muestra el detalle de superficie de ataque de la infraestructura de TI .

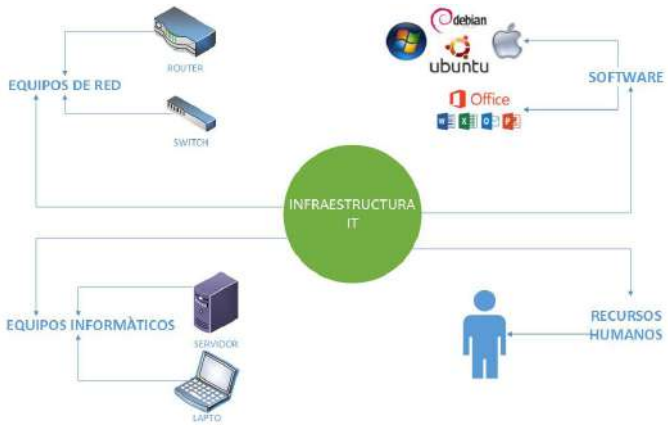

Figura 11. Superficie de ataque en infraestructura de TI**.**
Fuente: elaboración propia.

Cuanto mayor sea la superficie de ataque, es decir cuántos más elementos estén expuestos más probabilidades hay de que existan vulnerabilidades disponibles para un ataque por lo que minimizar esta superficie implica una reducción de los riesgos que pueden causar problemas, además que puede reducirse también la tasación de los riesgos que no se puedan evitar, la Figura 12 muestra los riesgos en la superficie de ataque.

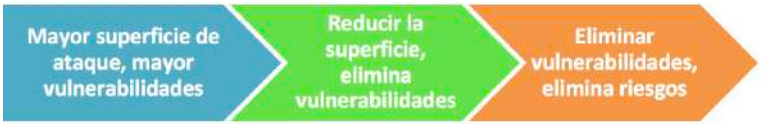

Figura 12. Superficie de ataque vs riesgos**.**
Fuente: elaboración propia.

Al estudiar las diferentes superficies de ataques se dice que hay dos formas de ataque la **pasiva y la activa.**

El **ataque pasivo** consiste en monitorear al sujeto atacado, es un ataque no invasivo ya que no afecta a la infraestructura, pero monitoriza lo que esta puede almacenar o transmitir, incluso información que es directamente pública. Para este tipo de ataques se pueden atizar técnicas de monitorización de tráfico en busca de documentos, contraseñas o fuentes abiertas de información conocidas como **OSINT**.

Los ataques pasivos están orientados exclusivamente a obtener información que puede ser suficiente en sí misma o ser empleada para posteriores ataques activos, es por esto, que identificar un ataque pasivo puede poner en alerta al usuario respecto a uno activo, la Figura 13 muestra los elementos del ataque pasivo.

Figura 13. Fuentes del ataque pasivo**.**
Fuente: elaboración propia.

Los **ataques activos** se caracterizan por acciones directas que tratan de penetrar la infraestructura, e incluso de hacerse estables dentro de ella de forma permanente, los objetivos suelen ser sabotajes, robo de información o despliegue de malware para espionaje o secuestro de equipos para otras actividades de ataque contra terceros objetivos.

Las **vulnerabilidades** son fallas en los sistemas, no son puertas abiertas diseñadas deliberadamente, sino errores de diseño, configuración o implementación que generan oportunidades de ataque, es decir que hacen viable una amenaza.

Por ejemplo, se puede analizar las distintas superficies que se tienen que estudiar para identificar potenciales amenazas y vulnerabilidades como:

Software

Está compuesto de aplicaciones, servicios, ejecutables, páginas web y otros servicios como NFTP, TELNET y otros similares. Las vulnerabilidades en el software son fallas en la programación o compilación de los programas que ejecutan las computadoras a servidores, los ataques a estas vulnerabilidades pueden derivar en un mal funcionamiento del software, acceso a información restringida, fallos de sistema, etc. Para reducir esta superficie de ataque, hay que reducir al mínimo el software instalado en las computadoras y servidores, mantener actualizado el software y aplicar todos los parches de seguridad publicados por los desarrolladores.

ConFigurar el software con la ley de los mínimos privilegios en mente, no utilizar software pirata o de fuentes no confiables y explorar recurrentemente las bases de datos públicas de vulnerabilidades en busca de aquellas que puedan afectar al software.

Hardware

Estadísticamente hablando el hardware es la segunda superficie de ataque a considerar, lo común es que, para atacar a un dispositivo hardware, el atacante necesita tener acceso físico al dispositivo. En este caso es fácil analizar que las amenazas naturales como fallos por envejecimiento de equipos o desastres como robos, incendios o inundaciones, afecta específicamente a esta superficie de ataque.

Los ataques a hardware también pueden producirse a través de la red o afectando al medio físico de transmisión, por ejemplo, los perturbadores de señal pueden interrumpir las comunicaciones de distinto tipo de tecnología inalámbrica mediante la generación de ruido radioeléctrico en la frecuencia y forma correcta. Este tipo de ataques podría anular sistemas de comunicaciones de los que dependen alarmas, sensores o cualquier otro tipo de comunicaciones, ya sean entre dispositivos o personas.

Todo Hardware de la infraestructura está o puede estar expuesto como dispositivo en sí mismo, por sus puertos y protocolos de comunicaciones, aplicaciones e interfaces. Para reducir al mínimo la superficie de ataque, se debe proteger físicamente los equipos frente a incidentes y sabotajes mediante instalaciones seguras con controles de acceso. Se debe conFigurar los equipos cerrando todo puerto innecesario y deshabilitando cualquier protocolo de comunicación no pertinente, en el entorno de red se puede desplegar firewalls, sistemas de detección de intrusión y sistemas de gestión y balanceo de carga de tráfico. Al igual que con el software se debe mantener el firmware actualizado de los equipos y evitar que personal no autorizado pueda manipular su configuración.

Recursos humanos

Por último, esta es la última superficie de ataque correspondiente a los recursos humanos, que pueden actuar contra los intereses de la organización por descontento, error, engaño o coacción. Además de implementar y exigir el cumplimiento de protocolos de actuación, es aconsejable implementar sistemas de registro y auditoría para verificar quién hace qué y cuándo, de este modo al evitar el anonimato se minimiza la probabilidad de éxito de una amenaza de carácter humano, además se debe invertir esfuerzo y recursos en educar y concienciar a los usuarios de nuestros recursos e infraestructuras para que se impliquen a la hora mantener un alto nivel de seguridad.

CAPÍTULO III: LAS VULNERABILIDADES

Este capítulo no tiene como objetivo analizar cuál es la mejor herramienta para el escaneo de vulnerabilidades, tampoco decir cuál es la mejor para Linux, Windows. El objetivo es poder brindar al lector un mayor conocimiento sobre el análisis de las vulnerabilidades, los tipos, las diferentes formas de escaneos y la detección de las diferentes vulnerabilidades y como poder resolverlas.

3.1. Introducción al análisis de vulnerabilidades

Definiendo a muy grandes rasgos que es una vulnerabilidad, una vulnerabilidad de una manera muy general es un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema.

Existen dos tipos de vulnerabilidades que se mencionan a continuación:

- Las lógicas
- Las físicas

3.1.1. Vulnerabilidades físicas

Las vulnerabilidades físicas son las que van a afectar a la infraestructura de la organización de manera física y se pueden mencionar en este tipo de clasificación a los desastres naturales, como ejemplo se podría mencionar una vulnerabilidad alta de este tipo si se vive en una zona de alto riesgo de sismos, ya que puede presentarse una negación en el servicio, una afectación en la disponibilidad y a partir de ahí se podría empezar con problemas. Si la organización está en una zona que generalmente se inunda, se tiene también otro tipo de vulnerabilidad.

Otra de las opciones físicas son los controles de acceso, en muchas ocasiones se tiene los accesos a la infraestructura crítica y no se tiene los accesos pertinentes, cualquier persona podría abrir una puerta, podría entrar y constituye un gran riesgo para la organización porque cualquier usuario podría ingresar con una USB y copiar información, podría infectar la misma infraestructura.

3.1.2. Vulnerabilidades lógicas

Las vulnerabilidades lógicas son las que van a afectar directamente la infraestructura y el desarrollo de la operación de estos, estas pueden ser de:

- Configuración
- Actualización
- Desarrollo

Las de **configuración** en el sistema operativo, pueden ser las configuraciones por defecto del sistema o incluso de algunas aplicaciones del servidor que se tenga expuesta, puede ser también la configuración de algunos firewalls que no está gestionado de una manera correcta y también de infraestructura perimetral.

Las vulnerabilidades de **actualización**, en muchas ocasiones hay empresas que no actualizan sus sistemas, van saliendo las vulnerabilidades y es un punto que se debe tomar en cuenta.

Actualmente, en los equipos XP de Windows no se les está dando soporte y muchas empresas tienen estos sistemas, cuando se realiza un escaneo en una determinada red al no tener soporte estos equipos ya son vulnerables.

Las vulnerabilidades de **desarrollo**, aquí se puede mencionar las inyecciones de código en SQL, Cross Site Scripting, esto puede variar dependiendo del tipo de aplicación, la validación de los datos. Cada escáner de vulnerabilidades utiliza distintas escalas, en estas escalas se va a poder auditar en base a una metodología de pruebas de penetración, de cumplimiento, si se va a auditar una red interna o una aplicación web, es muy distinto el escáner que se va a utilizar.

3.1.3. Escáneres de vulnerabilidades

Existen una gran gama de escáner de vulnerabilidades, muchos son de pago otros son gratuitos y se los puede utilizar sin mayor problema para su ejecución, hay escáneres como **Acunetix** que son muy buenos en la parte web y no sólo permiten escanear, también permiten la explotación real de ciertas vulnerabilidades o incluso la comprobación de estas.

Muchos de los escáneres web trabajan con proxys y a partir de estos se realiza la captura de las tramas de la información y se puede realizar la modificación. Algunos escáneres utilizan métodos que van a permitir listar el contenido del servidor de acuerdo a los directorios más conocidos, uno de esos escáneres es "**Acunetix**", el cual es una herramienta que está diseñada con el objetivo de encontrar agujeros de seguridad en las aplicaciones web, los cuales puedan ser aprovechados por determinados atacantes para accesar a los sistemas y la información.

También hay herramientas escáner como **netsparker** y **ProxyStrike** que permiten detectar vulnerabilidades. El caso de netsparker es un escáner de pago y ProxyStrike es gratuito, el cual permite identificar inyecciones de SQL Y Cross Site Scripting y el escáner "**VEGA**" que vienen incluidos en Kali Linux, al igual que ProxyStrike y a partir de ahí se puede realizar un propio escaneo.

Hay escáner para CMS, esto se debe al número de vulnerabilidades que se han dado a conocer y sobre de eso la posibilidad de explotar inyecciones SQL, la gestión del administrador entre otras cosas.

También existen escáner de vulnerabilidades en lo referente a sistemas operativos y también algunos son utilizados en la parte web, uno de los más completos es Nessus que se puede integrar con sistemas operativos como Android, se puede escanear desde el teléfono Android alguna red, buscando las vulnerabilidades y a partir de allí empezar a gestionar los resultados, tiene incluso opciones para virtualización.

Nexpose es un escáner que viene de la familia de "**Metasploit**", el cual permite realizar un escaneo y en algunos casos se puede exportar en herramientas como Metasploit en su versión pro o exprés y a partir de ahí tener un vector de ataque más puntual.

También hay tipos de escaneos con herramientas como **LanGuard** u **OpenVAS**, que pueden permitir utilizar el escáner sin tener credenciales o con las credenciales

del administrador, aparte de realizar un escaneo, evaluar las políticas tanto del equipo, como las de seguridad e incluso se podría empezar a ver si realmente las áreas de administración están teniendo un cumplimiento de sus políticas internas y analizar los procedimientos para la gestión de los equipos cuando se hace una prueba de penetración.

Estos escáneres funcionan de una manera sencilla, cuando se da a conocer una vulnerabilidad que tenga gran relevancia se desarrollan las firmas que van a validar estas vulnerabilidades, los escáneres se actualizan directamente, bajan las firmas y a partir de allí se puede realizar el escaneo.

3.2. Tipos de vulnerabilidades

Existen algunos tipos de vulnerabilidades que son mecanismos aprovechados por los atacantes para infectar una red o robar información entre los cuales se puede mencionar a los siguientes tipos:

3.2.1. Desbordamiento de buffer

El desbordamiento de buffer ocurre cuando el programador no controla el espacio de memoria del programa, entonces alguna persona puede introducir su propio código en ese espacio de memoria y la máquina lo va a ejecutar antes que cualquier otra tarea, por ejemplo, eso normalmente se da mucho con los payloads, en los cuales se inyectan cierta cantidad de memoria o inclusive dentro de los backdoor o puerta trasera, los cuales inyectan en la memoria RAM un cierto o una cierta cantidad de código, el cual se arranca antes, inclusive de arrancar toda la parte del sistema operativo o de algunos de los archivos dentro del mismo sistema que se utilizan para arrancar de manera normal. La Figura 14 muestra un ejemplo de desbordamiento de buffer.

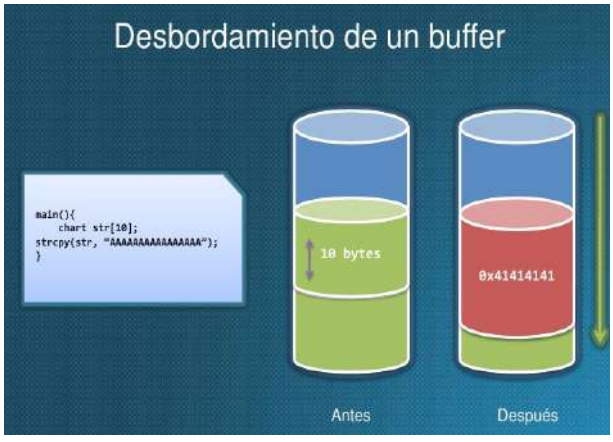

Figura 14. Desbordamiento de buffer.
Fuente: https://www.slideshare.net/RevistaSG/ups-cdigo-inseguro-deteccin-explotacin-y-mitigacin-de-vulnerabilidades-en-software

3.2.2. Errores de configuración

Otra de las principales vulnerabilidades, son los errores de configuración, se puede mencionar, por ejemplo, los password por default, password débiles, usuarios con demasiados privilegios e inclusive la utilización de protocolos de encriptación obsoletos, normalmente una de las cosas más típicas en las organizaciones es que utilizan algún sistema de encriptación web, lo cual con una aplicación de teléfono celular se puede crackear en menos de 10 o 15 segundos o inclusive con una laptop.

Otro error de vulnerabilidad puede ser algún protocolo de SSH que no se haya parchado o actualizado, por ejemplo, con alguna especie de vulnerabilidad se estaría utilizando algún protocolo de encriptación ya sea obsoleto o inseguro, pero normalmente la parte de errores de configuración provienen de la parte del password default, cuando se ingresa a una red con la IP por ejemplo, 198.X.X.X y si se tiene la posibilidad de ingresar a Google y buscar dentro del mismo, lo que sería el usuario y la contraseña por default, se puede cambiar la configuración causando un daño a la empresa.

3.2.3. Errores web

Otros tipos de vulnerabilidades son las WEB, aquí simple y sencillamente se tiene errores de validación de input, Scripts inseguros, errores de configuración de aplicaciones web, entre algunas otras situaciones, que a final de cuenta todos y cada uno de esos errores son los medios para algún ataque de XSS (Cross Site Scripting) o inyección SQL.

Según Cañon Parada (2015), la inyección por SQL es uno de los ataques más utilizados en la actualidad, consiste en acceder a las tablas de la base de datos incluyendo información sobre el usuario y su clave, este ataque está caracterizado porque es fácil de ejecutar porque modifica la cadena de consulta SQL hacia la base de datos.

También Cañon Parada (2015), indica que los ataques tipos Cross Site Scripting consisten en infectar un sitio web mediante scripts maliciosos con el objetivo de obtener acceso a una determinada cuenta de usuario.

3.2.4. Errores de protocolo

Por último, se tiene la parte de las vulnerabilidades de protocolos, existen diversas cantidades de protocolos que normalmente fueron definidos sin la necesidad o sin tener en cuenta precisamente la parte de la seguridad y en muchas veces no se preveo el crecimiento que estos iban a tener y como el internet no estaba preparado para ser tan grande, no se pensó en la parte de la seguridad.

Algunos de los protocolos pueden ser un simple HTTP, el cual no es seguro, dado que realiza solamente la parte de la autenticación, pero sin la encriptación de los datos que a final intercambia, esto puede ser necesario en algunos ambientes, por ejemplo, en las páginas visitadas simple y sencillamente por los usuarios, pero cuando se realizan transacciones bancarias normalmente la parte de este protocolo resultaría muy inseguro, probablemente se requiera de alguna otra acción como

sería algún certificado SSL o TSL, etc. Normalmente el mayor problema es cuando se define el marco de seguridad que tienen las fallas, por ejemplo, alguna especie de utilización de sistema web.

3.2.5. Aprovechamiento de las vulnerabilidades

Normalmente existen dos formas de aprovechar las vulnerabilidades como se muestra a continuación:

- Forma remota
- Ingeniería social

En la forma remota se llega mediante una computadora y se empieza a hacer análisis, ataques a un cierto servidor y tratar de vulnerarlo, si se logra el acceso, quiere decir que ya se hizo alguna explotación remota.

En la parte de la ingeniería social, alguien puede ayudar de manera interna, una persona dentro de la organización puede ayudar a realizar un acceso no permitido.

También existen las partes de ataques directo una vulnerabilidad de forma remota utilizando internet, se aprovecha de que algún software o servicio tiene un puerto abierto volviéndose vulnerable. Otra de las partes es engañando a un usuario, aplicando ingeniería social con alguna memoria o algún archivo infectado se puede aprovechar de alguna vulnerabilidad que se encuentra dentro del mismo sistema.

3.3. Detección de vulnerabilidades

Las vulnerabilidades pueden ser detectadas mediante herramientas de detección, realizar un escaneo de puertos con el objetivo de verificar cuales están abiertos para intentar obtener información sobre el servicio que se encuentre corriendo en ese momento y con esta información buscar vulnerabilidades asociadas precisamente a esos servicios. Se tienen tres formas de detectarse.

1. Escáner de vulnerabilidades.
2. Análisis manuales.
3. Consultando información.

A través del **escáner de vulnerabilidades** se tienen herramientas como Nikto la cual funciona buscando fallos en base a servidores, Nessus, Nmap, etc. Una de las ventajas de la parte del escáner de vulnerabilidades, es que funcionan de manera automática, trabajan ubicando un rango de direcciones IP e inicia el escaneo, la máquina realiza todo el proceso prácticamente sola.

En la parte de los **análisis manuales** es muy importante realizarlos, ya que, todos los análisis automáticos no detectan de forma automática todas las vulnerabilidades que se pueda tener en un sistema, entonces, también es necesario realizar algún análisis manual dentro de las vulnerabilidades encontradas con la finalidad de evitar que se pueda escapar o dejar como tal cabo suelta.

Otra de las partes es **consultar información**, en la parte precisamente de ocultar información se tiene alguna especie de Google hacking por así mencionarlo o algo

por el estilo, utilizar simple servicios, de lo que sería la búsqueda de información en red para poder realizar o encontrar información que pueda servir a la organización, de identificación de algunas vulnerabilidades que puedan tener todos los servicios.

3.4. Métodos de escaneo de vulnerabilidades

Existen varios métodos de escaneo para poder realizar análisis de vulnerabilidades que se mencionan a continuación:

Caja blanca

El método de escaneo de caja blanca tiene una visión total de la red a analizar, así como, acceso a todos los equipos como súper usuario, aquí es donde se tiene la parte de toda la administración de los servicios, la parte de análisis de caja blanca actúa como un usuario legítimo dentro de la red, que puede utilizar los servicios de diversas formas a la que otra persona los pueda estar utilizando. De una manera más detallada, este método utilizará ciertos usuarios con ciertos privilegios dentro de la red y accesando a los servicios, dentro de los productos, dentro de los softwares que se quieren auditar y así poder verificar si se puede realizar alguna acción adicional en base los privilegios que se han brindado.

Caja negra

También existe el método de escaneo de caja negra, aquí es donde normalmente se proporciona información de acceso de red, aquí a los analistas les van a proporcionar sólo información de acceso a red o al sistema, por ejemplo, una sola dirección IP, algún nombre de alguna empresa, etc., a partir de aquí empieza como tal a buscar información, todo lo posible relacionado para la exploración y así poder obtener la mayor cantidad de información posible de dicha dirección IP, del resto de los equipos probablemente que se encuentran dentro de algún rango de direcciones IP asociado, aquí no se realiza ninguna instrucción, solamente se detecta y se documenta la vulnerabilidad.

Hay una diferencia en lo que sería un método de escaneo de análisis vulnerabilidades y un pentesting, en el primero se encuentra las vulnerabilidades y se las documenta, en cambio en el pentesting se busca explotar dichas vulnerabilidades.

3.5. Remediación de vulnerabilidades

En este punto se va a analizar como remediar las vulnerabilidades, se ha analizado en capítulos anteriores las amenazas, como identificar las vulnerabilidades, como clasificar los activos e identificar la amenaza que puede afectar dichos activos, una vez que se ha logrado detectar las vulnerabilidades hay una serie de pasos para tratar de remediarlas que se indican a continuación.

3.5.1. Análisis de activos

Existe un ciclo de vulnerabilidades o de remediación el cual Inicia con la parte de la realización de un inventario y sobre todo la parte importante, la categorización de activos, aquí para corregir dichas vulnerabilidades se debe entender que esos activos

tanto pc, servidores, impresoras, todo lo que podría catalogarse como un activo se realiza para tener un orden de los sistemas, por ejemplo, mantener una lista de direcciones IP que tienen los dispositivos o bien para descubrir, qué equipos se han conectado a la red sin ser detectados, para eso va a servir la parte de la realización de un inventario y la categorización de activos.

3.5.2. Escanear sistemas para detectar vulnerabilidades

Otra de las partes fundamentales dentro del ciclo de remediación de vulnerabilidades, es la parte de escanear los sistemas para detectar fallos, en este paso el escáner normalmente revisará ya sea el software, configuraciones o dispositivos que tenga cada dirección IP y determinará si se tiene alguna vulnerabilidad reportada sobre dicho servicio o software o alguna especie de configuración. Igualmente, si se está haciendo un escaneo de cumplimiento de normas, el escáner revisará el registro de la máquina para detectar las configuraciones que son inseguras. Hay que tomar en cuenta que el escáner necesita tener acceso de administrador a las máquinas que se van a estar escaneando, al terminar dicho escáner va a generar un reporte muy completo de todas las vulnerabilidades detectadas.

3.5.3. Identificar vulnerabilidades

Otro de los puntos muy importantes en la parte del ciclo de remediación de vulnerabilidades, es verificar vulnerabilidades dentro del inventario, una cosa muy importante es escanear los sistemas para detectar vulnerabilidades y otra cosa muy distinta es precisamente verificar vulnerabilidades dentro del inventario de los activos de la empresa. Esto consiste en identificar que las vulnerabilidades que son detectadas por el escáner, primeramente, sean relevantes, generalmente los escáneres pueden generar tener falsos positivos, si un escáner genera demasiados falsos positivos, va a costar muchas horas de trabajo en remediaciones que a final de cuenta no son innecesarias.

3.5.4. Clasificar y priorizar riesgos

Es imposible arreglar todas las vulnerabilidades detectadas, es por eso, que es necesario clasificar y sobretodo priorizar el riesgo que está impondría en la organización. No se puede arreglar todas las fallas encontradas porque se tiene poco tiempo, poco personal y sobre todo poco dinero, por esto la organización se debe enfocar en arreglar primero las vulnerabilidades más graves en sistemas críticos, pero para esto se debe diseñar un esquema de prioridad que combine el nivel de severidad de una vulnerabilidad y qué tan importante es el sistema para la empresa.

Los escáneres inclusive en ocasiones permiten crear un esquema automáticamente como el que se muestra en la Figura 15, que viene a ser una matriz de riesgos.

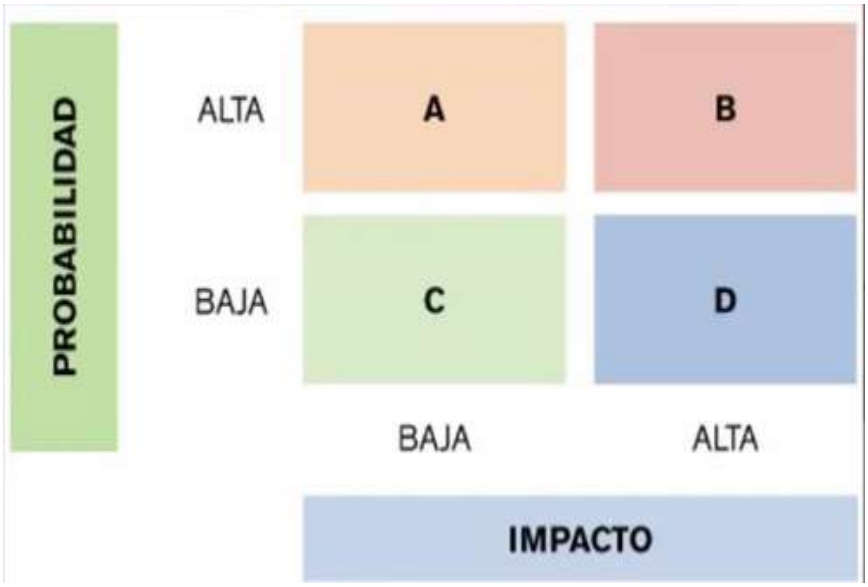

Figura 15. Matriz de riesgos**.**
Fuente: https://www.ics.dait.com.mx

3.5.5. Probar parches y configuraciones

Una vez que se ha detectado las vulnerabilidades dentro del sistema, del inventario y se ha clasificado y priorizado los riesgos que pueden incurrir estas vulnerabilidades, el siguiente paso es probar parches y cambios de configuración. El proceso de parcheo puede poner en riesgo el sistema de la organización, ya que el software parcheado puede traer inclusive errores que aún no han sido detectados.

El parcheo se debe instalar principalmente en una sola máquina y hacer pruebas para verificar si se llega a detectar algún problema, con esto poder evitar al haber instalado en todos los sistemas o en todos los dispositivos que ese error se propague. Hay que tomar en cuenta que el software que está haciendo parchado puede venir con configuraciones por default, ya que probablemente se tendría que ajustarlo nuevamente.

Es importante también descargar los parches de sitios oficiales del fabricante y sobre todo no usar parches de sitios de terceros, como, por ejemplo, up to down o zenet, etc., los cuales al final pueden traer algún software o malware o versiones anteriores con errores.

Los reportes de dicho escáner se incluyen en algunas ocasiones, instrucciones detalladas de cómo proceder con el parcheo o con el cambio de configuración que el sistema requiere para poder estar más seguro.

3.5.6. Aplicar parches y configuraciones

Una vez que ya se ha probado los parches y los cambios de configuración, es necesario aplicarlos, cuando se ha comprobado que dichos partes funcionan correctamente

en una máquina hay que proceder a implementarlos en todas las demás máquinas en la red, dependiendo del tamaño de la red este es el paso más laborioso de la administración de vulnerabilidades, hay soluciones de implementación de manera automáticas de parches que se pueden utilizar, hay que recordar que se tiene que probar primeramente el parche en una sola máquina antes de proceder a instalarlos en las demás.

Algunos escáneres tienen la posibilidad de generar automáticamente tickets para que sean asignados a ingenieros encargados de remediación y se las pueda dar un seguimiento a todo el proceso.

3.5.7. Aplicar parches y configuraciones

Una vez que ya se ha implementado todas las partes, se ha escaneado, clasificado riesgos, buscado los parches, aplicado dichos parches, la última parte es volver a escanear para verificar el parcheo, esto una vez que ya se haya parchado todos los sistemas o se hayan cambiado sus configuraciones inseguras, se debe escanear toda la red de nuevo para asegurarse que los parches estén adecuadamente instalados y no hayan faltado equipos, inclusive con toda esta situación de que se haya realizado un parcheo o una actualización es necesario volver a escanear para verificar si esos parches quedaron debidamente aplicados o bien generaron nuevas vulnerabilidades.

CAPÍTULO IV: METODOLOGÍAS DE ANÁLISIS DE VULNERABILIDADES

El objetivo de este capítulo es implementar una metodología de análisis de vulnerabilidades con la finalidad de tratar de mitigar o bajar los riesgos que se encuentran en determinados sistemas dentro de la organización. Para esto se establecen una serie de pasos para lograr dicho proceso.

4.1. Acuerdo de confidencialidad

En esta sección se explicará los pasos a seguir para llevar a cabo un análisis de vulnerabilidades de manera correcta y sobre todo sin sufrir algún inconveniente, por ejemplo, normalmente es necesario conocer los pasos a seguir durante el análisis de los fallos para formar parte de un desarrollo de seguridad de manera general, donde, el objetivo principal consistirá en hacer conocer el estado actual de la red y los riesgos que éstos tienen.

Una de las tareas principales que se debe verificar, es la parte del acuerdo de confidencialidad entre ambas partes, donde intervienen la empresa y el analista de seguridad. Es importante realizar un acuerdo de confidencialidad entre las dos partes involucradas en el análisis, debido a que, a lo largo de la búsqueda de vulnerabilidades, se puede obtener alguna información crítica para la organización analizada, por ejemplo, nombres de usuario y contraseñas, algunos agujeros de seguridad, documentos que se encuentran expuestos en la red, etc.

Toda la información que sea obtenida a través del análisis debe ser utilizada sólo para fines informativos, de mejora de servicios y seguridad, no podrá ser divulgada como tal a terceras personas o partes que no sean involucradas en la parte de este análisis. Desde el punto de vista de la organización debe de existir la confianza absoluta por parte del analista en este caso, si se está realizando un test de análisis de caja blanca, se deberá abrir como empresa todas las puertas a la red y ofrecerle toda la información que solicite el especialista.

Desde el punto de vista del analizador, el acuerdo de confidencialidad le ofrece un marco legal sobre el cual trabajar, constituyendo un respaldo formal a la labor realizada. La Figura 16 muestra un ejemplo sencillo de un acuerdo de confidencialidad.

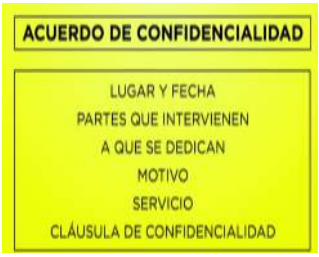

Figura 16. Ejemplo de un acuerdo de confidencialidad.
Fuente: https://www.youtube.com/watch?v=5hfPVX3T2O0

En conclusión, el acuerdo de confidencialidad debe tener un acuerdo muto entre ambas partes, tanto por la empresa como por el analista de seguridad sobre la información que se va a encontrar en el análisis de vulnerabilidad como, nombres de usuario, contraseñas, agujeros de seguridad, documentos expuestos, información crítica, etc. Toda la información que se encuentre debe ser utilizada para lo siguiente:

- Con fines informáticos
- Mejoras de los servicios y seguridad

4.2. Establecimiento de las reglas del juego

Otro de los puntos que se deben de establecer, son las reglas del juego, esto se refiere a todo antes de comenzar con el análisis de vulnerabilidades, ya que es necesario definir cuáles van hacer las tareas que se van a realizar y cuáles serán los límites, permisos y obligaciones que se van a respetar. Es probable que la organización que sea analizada no esté interesada en que sus servicios se suspenden, probablemente por algún ataque de denegación de servicio que sea exitoso por parte del analista. En caso de que esto suceda el experto deberá ser capaz de determinar las vulnerabilidades, durante el análisis se debe de mantener informada a la menor cantidad de personas, de forma de que la utilización de la red por parte del personal sea normal, con la finalidad de evitar cambios en la forma de trabajo de los usuarios de manera regular, ya que, si los usuarios de la red son informados que se va a realizar un cierto análisis, probablemente, lo que van a hacer es modificar algunas prácticas inseguras que normalmente realizan por miedo precisamente a que puedan ser reprendidos, despedidos y si esto sucede el análisis no tendrá el mismo efecto.

En este punto se quiere lograr definir cuáles serán las tareas a realizar, los límites que se deben alcanzar, las obligaciones y permisos que se tienen que cumplir, además se deberá realizar de manera cautelosa el análisis sin informar al personal en lo más mínimo posible para que la utilización de la red fluya de forma normal y realizar un excelente análisis.

4.3. Recolección de información

Otro de los puntos que se debe de verificar, es la parte de la recolección información, así como anteriormente se ha analizado los test de caja negra y caja blanca, el análisis de vulnerabilidades comienza con la obtención de información del objetivo, si se está seleccionando un test de caja negra, el proceso de análisis será muy similar al proceso seguido por un atacante, si se realiza el proceso de caja blanca, este es el momento para recopilar la mayor cantidad de información de acceso a servicios, información y todo lo que se considere necesario al momento de realizar el análisis. Por ejemplo, si se está realizando un test de caja blanca probablemente lo que hay que obtener son direcciones de servidores, nombres de usuarios, contraseñas, servicios que se llegan a brindar, esquemas de redireccionamiento, topologías de red, niveles de privilegios, etc.

Si se realiza un test de caja negra se puede obtener probablemente alguna dirección, nombres de dominio, correos electrónicos, etc. Cuando se realiza este tipo de

análisis para recolectar la información uno de las técnicas de análisis para levantar la información es el llamado OSINT, la Figura 17 muestra el esquema de este método de recolección de información.

Figura 17. Proceso OSINT.
Fuente: https://www.certsi.es/blog/osint-la-informacion-es-poder

Según la Figura anterior este modelo consta de 6 fases que según (CERTSI, 2014) las describe de la siguiente manera.

- Requisitos: En esta fase se establecen todos los requerimientos que se tienen que cumplir, como las condiciones que tienen que cumplirse según los objetivos planteados para resolver el problema.
- Identificación de las fuentes de información: En esta fase se especifican a partir de los requisitos establecidos, todas las fuentes necesarias que serán recopiladas, se deben concretar y especificar las fuentes de información que serán relevantes con el objetivo de optimizar el proceso de adquisición.
- Adquisición: En esta fase se obtiene la información partiendo de los orígenes indicados.
- Procesamiento: Esta fase se basa en dar formato a la información recopilada para que pueda ser analizada.
- Análisis: Aquí en esta fase se genera inteligencia a partir de los datos recopilados y procesados.

- Inteligencia: Se base en presentar la información recopilada de una manera eficaz, útil y comprensible para que pueda ser correctamente explotada.

4.4. Análisis interior

Antes de continuar con el análisis de vulnerabilidad, se debe verificar varios tipos de test, un análisis interior trata de mostrar o demostrar hasta dónde se puede llegar con los privilegios de un usuario típico dentro de la organización, para poder realizarlo se requiere que la organización provea una computadora con un nombre de usuario y una clave de acceso normal de un usuario específico.

Este tipo de test se compone normalmente de varias pruebas entre las cuales se puede mencionar a las siguientes:

La revisión de la privacidad: aquí simple y sencillamente el analista se centra en cómo se gestiona desde el punto de vista ético y legal el almacenamiento, transmisión y control de la información que todos los usuarios típicos o los empleados utilizan día a día.

Testeo de aplicaciones de internet: La parte del análisis de aplicaciones de internet o de aplicaciones web, este estudio se emplea de manera diferente, por ejemplo, se realizan técnicas de análisis de software para encontrar fallas de seguridad en aplicaciones que sean cliente servidor de un sistema desde internet. Cómo se está realizando un análisis interno, se deben probar las aplicaciones que son accedidas por los usuarios dentro de la red.

Testeo de sistema de detección de intrusos: En este tipo de análisis, normalmente se enfoca en la parte del rendimiento de los sistemas de identificación de intrusos, la mayor parte de este análisis normalmente no se puede llevar a cabo de manera adecuada, si no, accediendo a los registros del sistema de identificación de intrusos.

Testeo de medidas de contingencia: En este tipo de análisis se debe medir el mínimo de recursos necesarios que se necesitan en el subsistema, para realizar las tareas y verificar la detección de medidas presentes para la detección de intentos de acceso o recursos protegidos.

Descifrado de contraseñas: Descifrar las contraseñas es el proceso de validar cuan robusta puede ser una clave, a través del uso de herramientas de recuperación de contraseñas de manera automática, dejando normalmente al descubierto las aplicaciones de algoritmos criptográficos débiles y mal implementados o contraseñas débiles debido a factores humanos ya que las personas no se encuentran preparadas lo suficiente como para poder registrar una buena clave de seguridad.

Testeo de denegación de servicios: La denegación de servicio es una situación, donde una circunstancia sea intencional o de manera accidental previene a el sistema de que llegue a funcionar de manera exactamente como se dice lo diseñó. Normalmente se realiza en base alguna carga excesiva, algún alcance que no se llegue a cubrir o que los mismos usuarios abusen de los recursos del sistema, es muy

importante que los test o análisis de denegación de servicios reciban ayuda adicional de la organización ya sea a monitorizar a nivel privado o de algunos otros usuarios que también sean analistas de seguridad.

Evaluación de políticas de seguridad: En la evaluación de políticas, la reducción de riesgos en una organización con la utilización de tipos de específicos de tecnologías, por ejemplo Cisco, existen dos funciones a llevar a cabo, lo primero es el análisis de lo escrito contra el estado actual de las conexiones y segundo asegurar que la política esté incluida dentro de las justificaciones del negocio de la organización, en especial en lo que hace referencia a la parte de una política que está incluida dentro de las justificaciones de negocio, esta se refiere a que esta política vaya ajustada hacia los objetivos, debido a que si se pone una política, por ejemplo de que no se puede utilizar internet y resulta que la empresa para sus ventas hace uso de este recurso la política no tendría sentido, por eso es importante realizar un análisis acerca de las políticas de seguridad que más le benefician a la organización.

4.5. Análisis exterior

En el punto anterior se hizo un análisis interno, también existe el análisis externo, el principal objetivo de este tipo de análisis, es acceder en forma remota a los servidores de la organización y sobre todo obtener privilegios o permisos que no deberían estar disponibles. Este test puede comenzar con técnicas ya sea aplicando ingeniería social para poder obtener alguna información y luego se podría utilizar en algún intento de acceso. Los pasos de este tipo de análisis consisten en los siguientes puntos:

Revisión de la inteligencia competitiva: Esta parte se basa en toda la información recolectada a partir de la presencia en internet de la organización.

Revisión de la privacidad: Esta etapa se basa en un punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente. Por ejemplo, se hace una imaginación que dicha empresa no tiene el control suficiente como para hacer que toda la información o los datos que están manejando los empleados se queden dentro de la organización, lo que pueda a conllevar a que probablemente alguno de los empleados se pueda llevar dicha información.

Análisis de solicitud: Éste es el método para obtener privilegios de acceso a una organización y sus activos, preguntando sencillamente al personal de entrada usando las comunicaciones como algún teléfono, correo, chat, etc., desde una posición privilegiada o de una forma fraudulenta que tiende a ser simplemente un análisis basado en ingeniería social.

Análisis de sugerencia dirigida: Aquí en este método, se intenta lograr que un integrante de la organización ingrese a un sitio o reciba un correo electrónico en este sitio o el correo se podría agregar a herramientas que luego serían utilizadas en el intento de acceso. Técnicamente sería tener un cómplice dentro de la organización que ayude a instalar ciertas herramientas y posteriormente el atacante podría crear una sesión, ya sea con alguna herramienta que le permita gestionar sesiones desde el exterior.

Una vez que se recopila esta información se procede a realizar algunas de las siguientes pruebas que se muestran a continuación:

1. **Sondeo de red:** Sirve como Introducción a los sistemas a ser analizados, aquí se analizan nombres de dominio, nombres de servidores, direcciones IP, mapas de red, información del proveedor de internet, propietarios de sistema y servicios.
2. **Identificación de los servicios de sistemas:** En esta prueba se deben enumerar los servicios de internet activos o sobretodo accesibles, así como, traspasar el firewall con el objetivo de encontrar más máquinas activas, luego es necesario llevar adelante un análisis de la aplicación que escucha, tras dicho servicio. Tras la identificación de los servicios el siguiente paso simplemente es identificar al sistema con el fin de obtener respuestas que pueden dirigir el sistema operativo y su versión, técnicamente realizar un análisis de Fingerprint.
3. **Búsqueda y verificación de vulnerabilidades:** Esta prueba se basa en la identificación, comprensión y verificación de las vulnerabilidades o debilidades, errores de configuración dentro de un servidor o en una red. La búsqueda de vulnerabilidades se realiza mediante herramientas automáticas para determinar agujeros de seguridad existente y niveles de parcheado de los sistemas, pero se debe tener en cuenta nuevas vulnerabilidades que se publican en sitios donde normalmente todavía no incluyen las herramientas automáticas.
4. **Testeo de aplicaciones de internet:** Aquí se emplean diferentes técnicas de análisis de software para encontrar fallos de seguridad en aplicaciones cliente, como se está realizando un análisis externo, se pueden utilizar en este módulo los test de caja negra.
5. **Testeo de relaciones de confianza:** La parte de enrutamiento técnicamente está diseñado para asegurar que sólo aquellos que deben ser expresamente permitidos puede ser aceptado en la red.
6. **Verificación de redes inalámbricas:** Aquí en este caso se menciona la parte del estándar 802.11, que es un método para la verificación del Wireless que normalmente se basa en la parte de la cobertura y el acceso de los Access Point por red ad hoc.

4.6. Documentación e informes

En los puntos anteriores se analizó la parte del análisis interno y externo, ahora se debe realizar un análisis acerca de la parte de la documentación y los informes. Como en la parte de la finalización del análisis de vulnerabilidades se debe presentar un informe, donde se detalle cada uno de los test que se han realizado y los resultados de los mismos. Este informe debe especificar la lista de vulnerabilidades que han

sido probadas, las vulnerabilidades detectadas, lista de servicios y dispositivos vulnerables, el riesgo o el nivel de riesgo que involucra cada vulnerabilidad que ha sido encontrada en cada servicio y dispositivo, como tal se debe incluir los resultados de los programas utilizados.

CAPÍTULO V: HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES

Este capítulo tiene como objetivo mostrar las herramientas más utilizadas para el análisis de vulnerabilidades en los sistemas, los pasos necesarios para interpretar todos los fallos encontrados y sobre todo las posibles soluciones para dichas falencias.

5.1. Introducción a Nessus

Actualmente existen muchas herramientas para el análisis de fallos e inseguridades en el mercado, una de estas aplicaciones tipo escáner más populares es Nessus, esta solución es un escáner de vulnerabilidades desarrollado por la empresa Tenable Network Security, en la actualidad ofrece distintas soluciones no solo de escaneos de redes para encontrar fallos, sino, aplicaciones más completas como Nessus Security Center el cual evalúa las vulnerabilidades de una organización o empresa categorizando estas deficiencias de acuerdo al riesgo, incluso proporciona reportes continuos, datos estadísticos y posee un plugin que genera alertas y notificaciones, también apoya a la organización en el cumplimiento de estándares regulatorios y es posible integrarla con otras soluciones, esto constituye una de las grandes ventajas que tiene esta herramienta. La Figura 18 muestra la página principal de esa herramienta de escaneo de vulnerabilidades.

Figura 18. Sitio web de la herramienta Nessus.
Fuente: https://www.tenable.com/

Una versión más completa de Nessus Security Center es la que se enfoca en el monitoreo constante, este paquete permitirá monitorear continuamente la infraestructura permitiendo recopilar los datos a partir de múltiples sensores que apoyará en el análisis de vulnerabilidades, monitoreo de las amenazas, el tráfico de la red. La diferencia de los servicios que se mencionan va a permitir brindar escaneos activos, permitiendo el uso de conectores inteligentes e incluso el escaneo por medio de agentes. También puede manejar:

- Cumplimiento de estándares

- Detección de Malware, entre otras utilidades
- Escáner de vulnerabilidades

El escáner de vulnerabilidades se divide en 3 secciones como muestra la Figura 19.

Figura 19. Versiones de la herramienta Nessus.
Fuente: https://www.tenable.com/

El **Nessus Cloud** permite realizar escaneos de una manera externa como interna, permite realizar múltiples escaneos personalizando las políticas y delegar los resultados a los posibles responsables de la administración de la infraestructura o del desarrollo, apoya también en el cumplimiento de estándares internacionales y una de sus grandes ventajas es el escaneo por medio de agentes, esto reduce el tiempo en el escaneo y permite reducir los costos y los riesgos.

Nessus Manager, esta versión permite realizar escaneos, gestión de políticas con respecto a reportes y estadísticas de las vulnerabilidades que se hayan detectado en la organización y en la infraestructura. Esta herramienta se actualiza constantemente para trabajar sobre las amenazas avanzadas, vulnerabilidades de día cero y nuevos requisitos en el cumplimiento de estándares. Permite realizar integraciones por medio de su Api con algunos datos de infraestructura de seguridad perimetral como los firewalls, sistemas de virtualización.

Nessus Profesional esta versión permitir escanear múltiples sistemas operativos tanto físicos como virtuales y también las bases de datos se pueden analizar en este tipo de escaneos, así como, n cantidad de infraestructuras. Los escaneos se pueden realizar de una manera múltiple con o sin credenciales de acceso. El escaneo con credenciales de acceso va poder permitir tener una idea más completa de los estándares de cumplimiento que se está evaluando, se puede manejar la parte de las políticas internas y poder gestionar si realmente se tiene los requisitos de acceso para escaneo. Por ejemplo, se puede auditar la complejidad de las contraseñas, si son poli alfabética, si tienen alguna longitud mínima, alguna fecha de caducidad, etc.

De una manera muy general se puede decir que Nessus opera en varios sistemas operativos, no sólo puede en Windows o Linux, se lo podemos integrar sin mayor problema incluso hasta en dispositivos móviles. La instalación es muy simple, lo único que hasta cierto punto se podría decir sería el costo, pero se generó una versión