ITSSAT

Lista de cotejo Protocolo de Investigación

Nombre asignatura: Taller de Investigación **I**

Nombre del proyecto: "Análisis de Vulnerabilidades en el servidor Web del Instituto Tecnológico Superior de San Andrés Tuxtla: Evaluación y Mitigación de riesgos

Nombre del alumno (a): Jonathan Emmanuel Acevedo Mendez

Nombre del docente: Dra. Verónica Guerrero Hernández

Elementos de un protocolo de investigación		60	SI	NO	INDICADOR DE ALCANCE TOTAL 60%
	Título del proyecto				
	Contiene no más de 10 a 15 palabras como máximo, es atractivo y contiene las variables dependiente e independiente	0-1			1
	Generalidades del proyecto				
	Planteamiento del Problema				
	Contiene la situación actual por lo menos con una cita con cifras, datos o porcentajes que demuestran que el problema existe.	0-2			2
	¿Las cifras, datos y porcentajes que se citan, son de fuentes confiables?	0-2			2
	Se identifica y menciona la causa que provoca el problema	0-2			2
	Se menciona un pronóstico como consecuencia (lo malo que sucederá)	0-1			1
	Formulación del Problema				
	La Pregunta de Investigación contiene las variables dependiente e independiente	0-2			2
	El enunciado es en formato de pregunta	0-1			1
	Objetivos				
	El objetivo general contiene las variables dependiente e independiente.	0-1			1

	En el objetivo general el verbo coincide con el nivel de profundidad del trabajo	0-2			2
	El objetivo general es un enunciado claro y preciso	0-2			2
	Los objetivos están redactados con el verbo en infinitivo	0-1			1
	Se redactaron los objetivos específicos	0-2			2
	Los objetivos específicos permiten lograr el objetivo general	0-2			2
	Hipótesis				
	Contiene las variable dependiente e independiente	0-1			1
	Muestra relación de la variable independiente sobre la dependiente	0-1			1
	Redactada como una afirmación	0-1			1
	Justificación				
	Al menos una cita	0-1			1
	Al menos media cuartilla	0-1			1
	Demuestra la magnitud de la investigación (teórica, práctica o metodológica)	0-1			1
Coincide el título, la formulación del problema, el objetivo general y la hipótesis permitiendo una redacción clara del perfil del proyecto.		0-1			1
	Marco teórico				
	La redacción de cada artículo del estado del arte se encuentra en una tabla y contiene el nombre del artículo, la cita, el problema, objetivo y solución propuesta.	0-10			10
	La información corresponde a 5 años atrás	0-1			1
	Se realizaron investigaciones de proyectos similares	0-1			1
	Se adjunta un mapa conceptual con los conceptos relacionados a su tema	0-5			5
	Se adjunta un índice tentativo del marco teórico	0-5			5
	Diseño metodológico				
	Menciona el tipo de enfoque a utilizar para el desarrollo de la investigación	0-1			1
	Menciona el tipo de investigación	0-1			1
	Se describe la población y muestra	0-1			1
	Fuentes de información				
Presenta el listado de todas las referencias consultadas y las presenta de acuerdo con la norma IEEE		0-2			2

Al menos 5 fuentes de información	0-5			5
				60

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA

Asignatura:

Taller 1

Docente:

Verónica Guerrero Hernández

Alumno:

Jonathan Emmanuel Acevedo Mendez

Trabajo:

PROTOCOLO INVESTIGACION

"Análisis de Vulnerabilidades en el servidor Web del Instituto Tecnológico Superior de San Andrés Tuxtla: Evaluación y Mitigación de Riesgos"

Fecha de entrega:

11/12/2023

Grupo: 710 A

Resumen.

Este documento describe un plan para evaluar y mitigar el riesgo de un servidor web en un instituto mediante la realización de un análisis de vulnerabilidad. El plan implica el uso de herramientas de escaneo de vulnerabilidades para identificar posibles vulnerabilidades en el servidor web y luego medir la frecuencia y gravedad de estas vulnerabilidades.

Además, se pueden utilizar encuestas y cuestionarios para recopilar datos sobre las prácticas de seguridad actuales y las necesidades de seguridad del instituto.

Con base en los resultados de la investigación, se puede desarrollar un plan de acción para implementar soluciones de seguridad y monitoreo continuo.

La metodología de investigación utilizada es la investigación cuantitativa, que implica la recolección y análisis de datos estructurados utilizando herramientas estadísticas y matemáticas para cuantificar el problema de investigación.

La población en este caso son todos los servidores web del instituto, mientras que la muestra serán los servidores web seleccionados para el análisis de vulnerabilidad.

Es importante asegurarse de que la muestra sea representativa de la población y se seleccione aleatoriamente o estratificada para evitar sesgos en los resultados del análisis.

Las actividades incluirán la realización de un análisis de riesgos del servidor web, la identificación de amenazas internas y externas y el desarrollo de un cronograma para implementar soluciones de seguridad.

Índice

Introducción.

El análisis de vulnerabilidades en el servidor web de una institución es fundamental para identificar y mitigar riesgos de seguridad. Este proceso implica la identificación de debilidades en la estructura tecnológica, como exploits, fallas y riesgos de seguridad.

Para llevar a cabo este análisis, es recomendable utilizar herramientas de escaneo de vulnerabilidades o software especializado como Kali Linux, Nessus, Nexpose, Nmap y Owasp Zap, que pueda inspeccionar los endpoints en la institución y detectar y gestionar las vulnerabilidades de manera continua.

Asimismo, es importante considerar la implementación de sistemas de seguridad, como firewalls de aplicaciones, y la configuración adecuada de los servicios del servidor web, como Apache y PHP, para mitigar posibles ataques.

Una vez identificadas las vulnerabilidades, es importante desarrollar un plan de acción para implementar soluciones de seguridad y realizar un monitoreo continuo para prevenir posibles ataques cibernéticos.

El análisis de vulnerabilidades protege a la institución a corto y largo plazo, minimizando la probabilidad de presentar problemas de forma anticipada.

En la literatura se pueden encontrar varios trabajos que abordan el análisis de vulnerabilidades en servidores web de instituciones, utilizando herramientas como Kali Linux, Nmap, Nikto, OWASP Zap, entre otras. Además, es importante conocer los tipos de vulnerabilidades y amenazas informáticas que existen, como los ataques DDoS, vulnerabilidades de configuración débil, comunicación insegura entre cliente y servidor, entre otros.

CAPÍTULO I. GENERALIDADES

Antecedentes.

El análisis de vulnerabilidad en servidores web es un tema amplio y en constante evolución.

| Antecedentes| El análisis de vulnerabilidad en servidores web ha sido un tema de interés desde los primeros días de internet. Con el tiempo, ha evolucionado con el desarrollo de nuevas tecnologías y la aparición de nuevas amenazas.

| Evolución| Inicialmente, el enfoque estaba en la detección de vulnerabilidades conocidas. Con el tiempo, se ha avanzado hacia la identificación de vulnerabilidades desconocidas y el análisis de su impacto potencial.

| Conceptos | El análisis de vulnerabilidad en servidores web implica la identificación, evaluación y mitigación de posibles debilidades que podrían ser explotadas por atacantes. Incluye el escaneo de puertos, la detección de software obsoleto, la evaluación de configuraciones erróneas, entre otros.

| Características| - Automatización de procesos de escaneo y detección. - Análisis de riesgos y priorización de vulnerabilidades. - Reportes detallados y recomendaciones de mitigación. - Integración con sistemas de gestión de vulnerabilidades.

| Ejemplos| - Ataques de inyección SQL. - Explotación de vulnerabilidades de desbordamiento de búfer. - Ataques de denegación de servicio (DDoS). - Exposición de información sensible a través de directorios no protegidos.

Actualmente, se están desarrollando y aplicando diversas técnicas y herramientas para el análisis de vulnerabilidades en servidores web, con el fin de proteger la información y los sistemas críticos de organizaciones e instituciones.

Planteamiento del problema.

En la era digital actual, las instituciones dependen en gran medida de sus sitios web como plataformas fundamentales para la interacción con el público, la difusión de información crucial y la realización de transacciones importantes. Sin embargo, este aumento en la dependencia de la tecnología también ha dado lugar a una creciente amenaza de ciberseguridad.

Los sitios web institucionales se han convertido en blancos principales para ataques cibernéticos, con actores malintencionados que buscan explotar vulnerabilidades en la seguridad para acceder, manipular o comprometer datos confidenciales.

El planteamiento del problema radica en la necesidad crítica de realizar un exhaustivo análisis de vulnerabilidades en los sitios web de las instituciones.

A pesar de los esfuerzos de las organizaciones para implementar medidas de seguridad, la naturaleza dinámica de las amenazas cibernéticas y la evolución constante de las tecnologías hacen que los sistemas estén en constante riesgo.

Este proyecto se enfocará en identificar, evaluar y abordar las vulnerabilidades presentes en el sitio web del Instituto Tecnológico Superior de San Andrés Tuxtla, con el objetivo de fortalecer sus defensas y salvaguardar la integridad, confidencialidad y disponibilidad de la información crítica presente.

Este enfoque no solo protegerá la integridad de la información crítica, sino que también fomentará la confianza del público y garantizará que la institución cumpla con los más altos estándares de seguridad en el entorno digital actual.

Formulación del problema

¿Cuáles son las vulnerabilidades específicas más recurrentes y críticas que afectan a los servidores web del instituto superior de san Andrés Tuxtla, y cómo pueden ser mitigadas eficazmente para garantizar la seguridad de la información confidencial y prevenir accesos no autorizados?

Hipótesis.

H1: Un análisis de vulnerabilidades en el servidor web de ITTSAT puede identicar los fallos de seguridad.

H2: Aplicar medidas de mitigación puede reducir impactos a las vulnerabilidades cibernéticas.

Objetivo general y específicos.

Objetivo General:

Evaluar y mitigar los riesgos del instituto tecnológico superior de san Andrés Tuxtla mediante un análisis de vulnerabilidad en el servidor web.

Objetivos Específicos:

- Identificar vulnerabilidades potenciales en el servidor web del Instituto Tecnológico Superior de San Andrés Tuxtla.
- Identificar un plan de acción para implementar las soluciones de seguridad y monitoreo continuo.

Justificación.

En la actualidad, todos los activos de una institución deben ser monitoreados y gestionados con la misma importancia dentro de un período de tiempo regular para garantizar la confidencialidad, integridad y disponibilidad de los mismos.

De esta manera evitar que se materialicen amenazas de seguridad que surjan de vulnerabilidades no atendidas en el tiempo correcto, las cuales deben ser incluidas en un plan de remediación de vulnerabilidades y tratamiento de riesgos con la finalidad de llevar una gestión periódica que garantice los procesos y servicios del servidor web.

La ejecución de un proyecto de análisis de vulnerabilidades en el servidor web del instituto es una respuesta integral a las complejidades del entorno digital actual.

Va más allá de la mera seguridad técnica, buscando asegurar la confidencialidad, integridad y disponibilidad de datos, así como preservar la confianza de la comunidad educativa y posicionar al instituto como líder en prácticas de ciberseguridad en el ámbito educativo.

Su implementación representa una inversión estratégica en la seguridad y resiliencia del instituto ante las amenazas digitales emergentes.

CAPÍTULO II. MARCO TEÓRICO

Estado del arte.

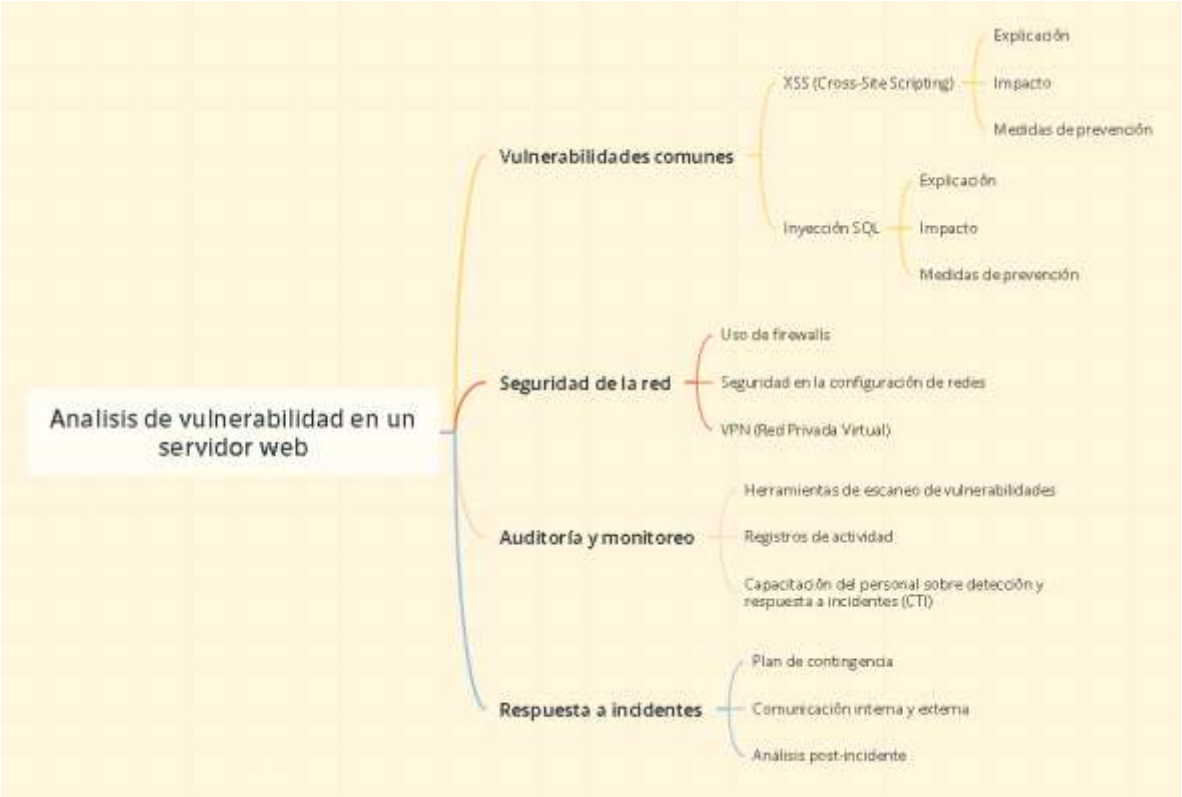
CITA	NOMBRE DEL ARTICULO	PROBLEMA	SOLUCIÓN	RESULTADOS
[1]	ANALISIS DE VULNERABILIDADES EN SITIO WEB DE LA ORGANIZACION INFRAESTRUCTURA TECNOLÓGICA DE COLOMBIA (ETHICAL HACKING)	¿Qué recomendaciones técnicas se pueden dar a las brechas identificadas en el sitio web de la organización en el marco de referencia ISO-27001, y que permita que estos riesgos se mitiguen y puedan ser gestionados?	realizar un proceso de diagnóstico que permita establecer los criterios para proponer una consultoría sobre el estado de la seguridad informática en los procesos que son inherentes y transversales al modelo de negocio, para posteriormente establecer cuáles son las oportunidades de mejora que le permitan a Infraestructura Tecnológica de Colombia SAS cumplir con los requisitos y desafíos en materia de ciberseguridad y Ethical Hackin.	Por medio de las pruebas de pentesting permite hallar y demostrar las vulnerabilidades del sitio web, así mismo permite evaluar y encontrar los riesgos y por último nos permite desde software desarrollados para hacking ético prevenir posibles ataques que se intenten realizar sobre el sitio web de la organización
[2]	IMPLEMENTACIÓN DE UN MARCO DE REFERENCIA PARA EL ANÁLISIS DE VULNERABILIDADES DE LOS SITIOS WEB EN LAS INSTITUCIONES PÚBLICAS DE COSTA RICA	Las entidades públicas de Costa Rica sufren de diversos ataques, esto sin contar los posibles ataques que sufren por usuarios internos, donde existen filtraciones de información.	Elaborar un marco de referencia para el análisis de vulnerabilidades de los sitios web de las instituciones públicas de Costa Rica para construir un ciclo de revisión y mejora de la seguridad.	Al realizar el análisis de vulnerabilidades de los sitios web, para que, de esta forma, una vez detectado, aquellas vulnerabilidades, trabajar sobre ellas, y ver las correcciones que se deben realizar en cada una de las encontradas, esto para que cualquier funcionario de T.I. pueda llevar a cabo sin necesidad de conocimientos extras en ciber seguridad.
[3]	"ANÁLISIS DE VULNERABILIDAD DE UN SISTEMA DE INFORMACIÓN WEB MEDIANTE PRUEBA DE PENETRACIÓN UTILIZANDO LA TÉCNICA OWASP (OPEN WEB APPLICATION SECURITY PROJECT) CON LA FINALIDAD DE COMPROMETER EL ALMACENAMIENTO DE INFORMACIÓN DE LA BASE DE DATOS."	¿Cómo saber la vulnerabilidad que tiene un sistema de información web en los procesos donde se almacena la información y el riesgo que existe de perder o alterar datos importantes de las amenazas de intrusos a través de los ataques informáticos?	El propósito de la propuesta se define en conocer la Metodología de evaluación de riesgos Owasp y las principales técnicas que le ayudará al administrador de sistemas realizar el test de penetración, donde podrá analizar y evaluar la vulnerabilidad que tenga la página de la Carrera de Ingeniería en Sistemas Computacionales, evitando los riesgos de seguridad en la aplicación web.	Se verificó de manera técnica la seguridad en el sistema de información web, observando que el protocolo de transferencia de hipertexto (HTTP) es inseguro, a su vez también configurar directrices de seguridad en la página web. Se instaló OpenSSL habilitando el puerto 443 y se configuro directrices de seguridad de esta manera se obtiene un protocolo seguro de transferencia de Hipertexto (HTTPS) generando un Certificado SSL/TLS.
[4]	DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP 10 DE VULNERABILIDADES MÁS EXPLOTADAS EN 2017 SEGÚN EL MARCO DE REFERENCIA OWASP	¿Cómo debe ser y que características tiene un modelo para el cálculo del nivel de seguridad en un sitio web ayudara a optimizar la evaluación de las vulnerabilidades?	Desarrollar un modelo para calcular el nivel de seguridad en sitios web, basado en el top 10 de vulnerabilidades en 2017 por owasp.	Se analizaron los vectores de ataque según lo reportado por las organizaciones y caso que se tengan establecidos de ataques, se pasó al siguiente paso donde se analiza que debilidad se aprovechó o que controles se traspasaron con el ataque, para finalmente evaluar los impactos que genero este ataque a nivel técnico y del negocio.

[5]	ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN AVANZADA PENTESTING AL SITIO WEB OFICIAL DE LA ALCALDÍA DEL MUNICIPIO DE QUIBDÓ.	¿Cómo se puede realizar una medición de los niveles de seguridad y caracterización de los posibles ataques informáticos, a los que está expuesta la información publicada en el sitio web de la alcaldía del municipio de Quibdó?	Realizar un análisis de vulnerabilidades mediante pruebas de penetración avanzada pentesting al sitio web oficial de la alcaldía del municipio de Quibdó Chocó.	Se logró identificar los diferentes ataques a los que está expuesto el sitio web y los servicios en línea que presta la alcaldía de Quibdó. Se realizaron ataques con: • Paquete Uniscan. No se logró detectar una vulnerabilidad utilizando los diferentes plugins que contiene la herramienta. • Paquete de Software Nikto. Se pudo evidenciar que el servidor no presento vulnerabilidades detectadas por esta herramienta

CITA	NOMBRE DE LA TESIS	PROBLEMA	SOLUCIÓN	RESULTADOS
[1]	IMPLEMENTACIÓN DE UN MODELO DE ANÁLISIS DE VULNERABILIDADES Y RIESGOS PARA LOS SISTEMAS WEB DE LA EMPRESA SOCIAL CAPITAL GROUP.	¿Cómo debe ser una implementación de un modelo de análisis de vulnerabilidades y riesgos para los sistemas web de la empresa Social Capital Group?	implementación de un modelo que detectará, identificará, calificará y evaluará el riesgo de las vulnerabilidades encontradas en los sistemas web de la empresa SCG aplicando el OWASP Risk Rating Methodology, el cual ayudará a determinar la severidad de los riesgos encontrados estimando la probabilidad y el impacto.	Cabe mencionar que en los siguientes resultados se logró cumplir con los 3 objetivos específicos: **Primer Objetivo:** Realizar pruebas de Pentesting para detectar las vulnerabilidades en los sistemas web de la empresa SCG **Segundo Objetivo:** Identificar las vulnerabilidades que se encuentren en los sistemas web de la empresa SCG según el apartado OWASP TOP 10 - 2017. **Tercer Objetivo:** Determinar la severidad de los riesgos encontrados en los sistemas web de la empresa SCG aplicando la metodología de Calificación de Riesgos de OWASP.
[2]	ANÁLISIS DE VULNERABILIDADES DEL PORTAL WEB UTILIZANDO METODOLOGÍAS DE HACKING ÉTICO PARA UN GAD MUNICIPAL DE LA PROVINCIA DE SANTA ELENA	¿Cómo saber las vulnerabilidades que tiene un portal web de un gad municipal de la provincia de santa elena?	Analizar las vulnerabilidades existentes del portal web de un Gobierno Autónomo Descentralizado mediante metodologías de hacking ético para brindar recomendaciones que ayuden a mitigar los riesgos encontrados.	Se obtuvo como resultado final de la comparativa, que la herramienta Nessus es la que lleva la delantera con respecto a tiempo de análisis, interfaz de usuario y contenido de reporte final y legibilidad de este, por lo tanto, sería la herramienta óptima para la detección de vulnerabilidades del portal web. Sin embargo, Nikto por su cantidad de resultados obtenidos sería la segunda opción con respecto a esta investigación, aunque su usabilidad podría ser un poco compleja.
[3]	"ANÁLISIS DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN"	Los sistemas académicos se ejecutan en infraestructura de redes TCP/IP, sin embargo, en dichas redes existen vulnerabilidades que pueden ser explotadas por un atacante malicioso, debido a estas infracciones ejecutadas por los piratas malicioso ha ido en aumento la demanda de personas calificadas y con el cumplimiento del perfil profesional de ellas que pueden ayudar a las universidades a protegerse y mitigar estas amenazas cibernéticas.	Analizar las vulnerabilidades presentes en la red de la Escuela Culinaria utilizando el estándar de seguridad OSSTMM3 para evitar el acceso no autorizado a los procesos del sistema de información académica.	Por medio del análisis de detección de vulnerabilidades en la infraestructura tecnológica del instituto de educación superior se detalló toda la información referente a la red corporativa de la organización académica. Con el uso de herramientas como Maltego, Nmap, Golismero, Nessus, Sparta, TheHarvester y Foca se llevó a cabo exitosamente la ejecución del análisis de una forma correcta para obtener los resultados deseados y con esto se pudo llegar a tener conocimiento de todos los riesgos que pueden acarrearse al no tomar en consideración estos tipos de análisis y desconocer como los atacantes pueden afectar la productividad de los sistemas.
[4]	"ANALISIS DE VULNERABILIDADES EN SISTEMAS INFORMÁTICOS WEB DESDE LA RED DE INTERNET UTILIZANDO HERRAMIENTAS DE HACKING ETICO Y LA METODOLOGÍA OWASP."	¿Cómo contribuye el no uso del hacking ético al aumento de las vulnerabilidades en sistemas informáticos web de la pyme en la ciudad de Guayaquil actualmente?	Establecer la contribución de la no aplicación del hacking ético al aumento de las vulnerabilidades en sistemas informáticos web mediante una investigación documental y de campo de las pymes en la ciudad de Guayaquil en la actualidad.	se analizó las vulnerabilidades en los sistemas informáticos web. Así como se realizó la respectiva revisión de la metodología OWASP y la aplicación de Hacking Ético. Luego de la recopilación de la información y el concerniente análisis se han obtenido conclusiones y recomendaciones que pretenden exponer el estado actual de las Pymes con relación a los servicios, aplicativos y mecanismos que se encuentren vulnerables.

[5]	ANÁLISIS COMPARATIVOS DE LAS AMENAZAS INFORMÁTICAS SUSCITADAS A LOS SITIOS WEB DE LAS ENTIDADES DEL SISTEMA FINANCIERO.	identificar las amenazas informáticas más comunes a las que se enfrentan estas empresas en sus sitios web y compararlas para entender su impacto y frecuencia.	Analizar las amenazas informáticas a las que están expuestas los sitios web de las entidades financieras.	Los resultados del estudio indican durante la revisión sistemática bibliográfica y de los análisis documentales se identificó que los sitios web de las entidades financieras están expuestos a una variedad de amenazas informáticas. Entre las amenazas identificadas se encuentran ataques de phishing, malware, denial of service (DoS), Cross-site scripting (XSS), entre otros. Estos ataques pueden tener consecuencias graves, como la pérdida de información confidencial, la interrupción de los servicios en línea, el robo de identidad y la pérdida financiera.

Marco conceptual.



CAPÍTULO III. DISEÑO METODOLÓGICO.

Enfoque de la investigación.

Para el proyecto de análisis de vulnerabilidades en el servidor web de un instituto, se puede utilizar un enfoque de investigación cuantitativa.

Este enfoque implica la recopilación y análisis de datos numéricos para identificar patrones y tendencias en la seguridad del servidor web.

Se pueden utilizar herramientas de escaneo de vulnerabilidades para identificar posibles vulnerabilidades en el servidor web y luego medir la frecuencia y gravedad de estas vulnerabilidades.

Además, se pueden utilizar encuestas y cuestionarios para recopilar datos sobre las prácticas de seguridad actuales y las necesidades de seguridad del instituto. Con base en los resultados de la investigación, se puede desarrollar un plan de acción para implementar soluciones de seguridad y monitoreo continuo.

Tipo de investigación.

¿Qué es la investigación cuantitativa?

La investigación cuantitativa es un método estructurado de recopilación y análisis de información que se obtiene a través de diversas fuentes. Este proceso se lleva a cabo con el uso de herramientas estadísticas y matemáticas con el propósito de cuantificar el problema de investigación.

En cuanto a su uso en las empresas, la investigación cuantitativa puede ayudar a la mejora de productos y servicios o en la toma de decisiones exactas e informadas que ayuden a conseguir los objetivos establecidos.

De manera general, se trata de pedirle a las personas que den su opinión de manera estructurada para que puedas producir datos y estadísticas concretas que te guíen y de esta manera, obtengas resultados estadísticos confiables.

Población y muestra.

En este caso, el objetivo es evaluar y mitigar el riesgo del instituto mediante un análisis de vulnerabilidad en el servidor web. Por lo tanto, la población serán todos los servidores web del instituto, mientras que la muestra serán los servidores web seleccionados para el análisis de vulnerabilidades. Es importante que la muestra sea representativa de la población y que se seleccione de manera aleatoria o estratificada para evitar sesgos en los resultados del análisis.

Cronograma de actividades.

Cronograma de activades					
Actividad	Agosto	septiembre	Octubre	noviembre	Diciembre
Realizar un análisis de riesgos del servidor web del instituto.					
Identificar amenazas internas y externas.					
Evaluar la vulnerabilidad de los sistemas actuales.					
Desarrollar un plan de acción para abordar las vulnerabilidades identificadas.					
Priorizar las vulnerabilidades según su impacto y probabilidad de explotación.					
Implementar tecnologías para proteger el servidor web, como firewalls, soluciones antimalware y detección de intrusos.					
Realizar pruebas de vulnerabilidad, pruebas de intrusión y pruebas de seguridad de la aplicación.					
Realice un escaneo de vulnerabilidades en el servidor web.					

Implementar un programa de monitoreo continuo del servidor web.					

Fuentes de Información

[1] P. MILAGROS. ""Análisis De Vulnerabilidades En La Infraestructura Tecnológica De Una Empresa, Utilizando Herramientas De Test De Intrusión"". Repositorio Universidad de Guayaquil :: Inicio. Accedido el 1 de diciembre de 2023. [En línea]. Disponible: http://repositorio.ug.edu.ec/handle/redug/24003

[2] C. Cautín García. Universidad Nacional Abierta y a Distancia UNAD. Accedido el 1 de diciembre de 2023. [En línea]. Disponible: https://repository.unad.edu.co/bitstream/handle/10596/26950/%20cacouting.pdf?sequence=1&isAllowed=y

[3] P. E. AVEGNO TENORIO. DSpace Principal. Accedido el 1 de diciembre de 2023. [En línea]. Disponible: http://dspace.utb.edu.ec/bitstream/handle/49000/14157/E-UTB-FAFI-SIST.INF-000096.pdf?sequence=1&isAllowed=y

[4] Y. C. STEVEN. ""Análisis De Vulnerabilidades En La Infraestructura Tecnológica De Una Empresa, Utilizando Herramientas De Test De Intrusión"". Repositorio Universidad de Guayaquil :: Inicio. Accedido el 1 de diciembre de 2023. [En línea]. Disponible: http://repositorio.ug.edu.ec/handle/redug/24003

GUÍA DE OBSERVACIÓN EXPOSICIÓN (40%)

Unidad 3

Nombre asignatura: Taller de Investigación I

Nombre del alumno: Jonathan Emmanuel Acevedo Mendez

Nombre del docente: Dra. Verónica Guerrero Hernández

Criterios	Indicador máximo por criterio	Indicador de alcance total (40%)
a. Capacidad crítica y autocrítica del trabajo	0-5	5
b. Habilidad en el uso de TIC	0-5	5
c. Dominio del tema	0-15	15
d. Utilización de ejemplos acorde al tema explicado.	0-10	10
e. Manejo e inclusión de referencias bibliográficas	0-5	5
Total Indicador	0-40	40

SUPERIOR DE SAN ANDRÉS TUXTLA: EVALUACIÓN Y MITIGACIÓN DE RIESGOS"

INTRODUCCION.

Este trabajo describe un plan para evaluar y mitigar el riesgo de un servidor web en un instituto mediante la realización de un análisis de vulnerabilidad. El plan implica el uso de herramientas de escaneo de vulnerabilidades para identificar posibles vulnerabilidades en el servidor web y luego medir la frecuencia y gravedad de estas vulnerabilidades.

METODOLOGIA.

Para el proyecto de análisis de vulnerabilidades en el servidor web de un instituto, se puede utilizar un enfoque de investigación cuantitativa.

Este enfoque implica la recopilación y análisis de datos numéricos para identificar patrones y tendencias en la seguridad del servidor web.

Se pueden utilizar herramientas de escaneo de vulnerabilidades para identificar posibles vulnerabilidades en el servidor web y luego medir la frecuencia y gravedad de estas vulnerabilidades.

Además, se pueden utilizar encuestas y cuestionarios para recopilar datos sobre las prácticas de seguridad actuales y las necesidades de seguridad del instituto. Con base en los resultados de la investigación, se puede desarrollar un plan de acción para implementar soluciones de seguridad y monitoreo continuo.

RESULTADOS.

- Parra Barzola, LM y Yánez Cedeño, ES (2017). Análisis de vulnerabilidad en la infraestructura tecnológica de una empresa, utilizando herramientas de prueba de intrusión. Tesis de grado, Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Networking y Telecomunicaciones.

EL artículo se centra en la realización de un análisis de vulnerabilidades en la infraestructura tecnológica de una empresa utilizando herramientas de prueba de intrusión, siguiendo la Metodología Abierta de Testeo de Seguridad (OSSTMM).

- El autor menciona que la metodología OWASP está basada en dos fases, pasiva y activa, y su enfoque es "caja negra", preferiblemente con poca o ninguna información conocida. El estudio confirma que ninguna aplicación web es perfectamente segura, pero con la práctica de las herramientas y metodologías necesarias, las vulnerabilidades pueden ser superadas, proporcionando integridad y confiabilidad a la información manejada (López, 2017).

CONCLUSIÓNES.

Los servidores web del ITSSAT son vulnerables a ataques cibernéticos y no se han implementado medidas de seguridad adecuadas para proteger la información confidencial y prevenir accesos no autorizados.

Para abordar este problema se debe Evaluar y mitigar los riesgos del Instituto Tecnológico Superior de San Andrés Tuxtla mediante un análisis de vulnerabilidad en el servidor web.

DATOS ALUMNO.

Instituto Superior de San Andres Tuxtla
Alum: Jonathan E Acevedo Mendez
Doc: Veronica Guerrero Hernandez

BIBLIOGRAFIAS.

[1] D. M.Оформити списки використаних джерел онлайн. Accedido el 2 de diciembre de 2023. [En línea]. Disponible: Lorem ipsum dolor sit amet, consectetur adipiscing elit.

[2]C. P. Repositorio Universidad de Guayaquil :: Inicio. Accedido el 2 de diciembre de 2023. [En línea]. Disponible:https://repositorio.ug.edu.ec/server/api/core/bitstreams/b0d17af0-4885-4d35-8e31-8853ebf609b4/content