UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS COMPARATIVO DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN MEDIANTE METODOLOGÍAS ETHICAL HACKING

SUMBA FAJARDO LESTER OMAR
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS COMPARATIVO DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN MEDIANTE METODOLOGÍAS ETHICAL HACKING

SUMBA FAJARDO LESTER OMAR
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

ANÁLISIS COMPARATIVO DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN MEDIANTE METODOLOGÍAS ETHICAL HACKING

SUMBA FAJARDO LESTER OMAR
INGENIERO DE SISTEMAS

CARTUCHE CALVA JOFFRE JEORWIN

MACHALA, 24 DE FEBRERO DE 2022

MACHALA
2022

Titulación

INFORME DE ORIGINALIDAD

10%	9%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	1library.co Fuente de Internet	4%
2	www.programacionparatodos.com Fuente de Internet	1%
3	paginasnaranja.emprenemjunts.es Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	<1%
5	ria.utn.edu.ar Fuente de Internet	<1%
6	www.dragonjar.org Fuente de Internet	<1%
7	wiki.owasp.org Fuente de Internet	<1%
8	Submitted to Universidad Politecnica Salesiana del Ecuado Trabajo del estudiante	<1%
9	hdl.handle.net Fuente de Internet	

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, SUMBA FAJARDO LESTER OMAR, en calidad de autor del siguiente trabajo escrito titulado ANÁLISIS COMPARATIVO DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN MEDIANTE METODOLOGÍAS ETHICAL HACKING, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 24 de febrero de 2022

SUMBA FAJARDO LESTER OMAR
0106290257

DEDICATORIA

Dedico este trabajo de investigación primeramente a Dios por brindarme un día más de vida, por permitirme tener cerca mío a las personas que más quiero en esta vida, a mis padres Juan Sumba y Dolores Fajardo, en especial a mi madre por haberme inculcado buenos valores desde niño, por su apoyo económico, moral y emocional, sin ellos no sería posible de cumplir esta meta propuesta de llegar a convertirme en un Ingeniero de Sistemas, de la misma manera también agradecer a mis hermanos y tío que siempre estuvieron ahí apoyándome brindándome su mano en momentos difíciles de toda esta trayectoria.

A mis amigos y familiares en general que estuvieron presentes en cada momento y en todo este proceso de convertirme en un profesional de la Republica del Ecuador, así mismo a mis compañeros de curso por brindarme su ayuda cuando la necesite, a mis profesores por aportar con su conocimiento y convertirse en mis amigos.

Sr. Lester Omar Sumba Fajardo

AGRADECIMIENTO

Quiero agradecer infinitamente a Dios por darme la vida, salud, fortaleza, sabiduría, una familia donde puedo ser feliz para así poder cumplir mis metas propuestas a lo largo de mi recorrido por este mundo, a mis padres y en especial a mi madre por ser la fuente de inspiración para no decaer cuando las cosas no salen del todo bien, por ser mis amigos y brindarme los mejores consejos necesario para afrontar problemas de la vida, por su motivación para continuar con mis estudios y convertirme en un profesional.

Agradezco también a mis hermanos por apoyarme en todo este trayecto, tanto emocionalmente como económicamente, siempre estuvieron ahí atentos para ayudarme ante cualquier situación y a mi hermana Cynthia Sumba por ser un ejemplo de superación y motivación.

A la Universidad Técnica de Machala por haberte abierto sus puertas y permitirme tener una educación de calidad totalmente gratuita, a mis profesores que siempre estuvieron ahí compartiendo un poco de sus conocimientos en el aula de clase y por brindarme consejos para ser un buen profesional ético.

De la misma manera a mi tutor el Ing. Joffre Cartuche por ser paciente y guiarme en este proceso de titulación, por brindarme consejos y motivarme para que sea un profesional ético

RESUMEN

Las técnicas, conceptos y metodologías asociadas al pentesting y la mayor parte de dichos avances que ha tenido la tecnología, el crecimiento tan grande que ha llegado a tener el internet y este a su vez tiene un lado oscuro que son los hackers de sombrero blanco que ayudan y los de sombrero negro que tiene como finalidad perjudicar a las empresas a las cuales realizan ataques de robo de información.

La escalada natural de las amenazas ofensivas contra las medidas defensivas ha demostrado cada vez que no existen sistemas que puedan construir y que estos no sean vulnerables a ataques.

Algunos estudios han explorado métodos para realizar pruebas de penetración, se nota una gran escases de estándares que sean flexibles para la realización de la misma. Cuando se habla de ethical hacking muchas de las veces nos referimos a una prueba de penetración que pueda llegar a abarcar absolutamente todo o, dicho de otra manera, no tiene un objetivo determinado o detallado, ya que todo es explotable y no tiene ninguna limitación más allá de la que se haya pactado con el o los clientes para la realización de las pruebas pertinentes.

Dado el crecimiento de ciberataques, la filtración y el uso no adecuado de la información que existe en los computadores por la poca seguridad en la red y los equipos. Hoy en día los niveles de protección y seguridad en los sistemas empresariales y personales se han llegado a convertir en un tema de gran relevancia ya sea por la falta de conocimiento y poca información que existe sobre aquello o también por la falta de recursos en las empresas que esta se la deja a un lado y muchas de las veces olvidada.

Todo esto ha hecho que los hackers éticos se unan para crear metodologías y métodos o scripts novedosos, para poder llegar a evitar o prevenir en un futuro posibles robos, ataques, sustracción y perdida de información.

Entre las funciones más relevantes que tienen los hackers éticos es llegar a dar una solución a los ataques o mitigar un poco el impacto que este pueda llegar a causar en las mimas y así también proteger y prevenir ataques a demás

usuarios, mejorar los procesos de seguridad sobre la importancia de la implementación de un sistema de seguridad para la protección de datos sensibles.

La demanda de tecnologías y nuevos procedimientos para poder hacer la administración de lo que son sistemas de seguridad y almacenamiento, todo esto promovió lo que es el nacimiento del pentesting, uno de los objetivos de estas pruebas es la identificación de las vulnerabilidades de seguridad, mediante el uso de las técnicas y/o herramientas específicas.

En el mundo digital en el que vivimos es de mucha importancia garantizar lo que es la seguridad de la nuestra información ya que la mayoría de las organizaciones se han convertido en un blanco fácil para esto. Es por esa razón que hoy por hoy existen una variedad de metodologías que nos guían y ayudan a muchos de los auditores para poder realizar pruebas y a estas llegar a aplicar métricas con el único fin de analizar, controlar los procedimientos para que verifiquen la seguridad que tienen las empresas. Para la realización de esto se hizo una investigación de la mayoría de las características más notables de las metodologías OSSTMM, OWASP, ISSAF usando lo que es la investigación bibliográfica, de esta manera llegando y encontrando procedimientos, estándares que guíen a la realización efectiva de pruebas de penetración, como resultado se espera que una de las metodologías propuestas cumpla con los estándares y así esta ayude con un aporte hacia los auditores y que sea más completa ya que de esta manera pueden los mismos pueden ir priorizando los niveles de riesgos de incidencias o peligrosidad que estas tenga sobre los objetivos propuestos por la empresa para realizar las pruebas pertinentes.

Palabras clave: Ethical Hacking, vulnerabilidad, pruebas de penetración, metodologías para pentesting, ataques, seguridad.

ABSTRACT

The techniques, concepts and methodologies associated with pentesting and most of these advances that technology has had, the great growth that the internet has had and this in turn has a dark side that are the white hat hackers that help and those of black hat whose purpose is to harm the companies to which they carry out information theft attacks.

The natural escalation of offensive threats against defensive measures has shown each time that there are no systems that can be built and that these are not vulnerable to attack.

Some studies have explored methods to carry out penetration tests, there is a great lack of standards that are flexible for carrying out the same. When we talk about ethical hacking, many times we refer to a penetration test that can cover absolutely everything or, in other words, does not have a specific or detailed objective, since everything is exploitable and has no further limitations. beyond that which has been agreed with the client(s) for carrying out the pertinent tests.

Given the growth of cyberattacks, the filtration and the inappropriate use of the information that exists in the computers due to the lack of security in the network and the equipment. Today the levels of protection and security in business and personal systems have become a highly relevant issue either due to lack of knowledge and little information that exists about it or also due to the lack of resources in companies. that this is left aside and many times forgotten.

All this has led ethical hackers to come together to create innovative methodologies and methods or scripts, in order to avoid or prevent possible thefts, attacks, theft and loss of information in the future.

Among the most relevant functions that ethical hackers have is to provide a solution to attacks or mitigate a little the impact that this may cause in them and thus also protect and prevent attacks on other users, improve security processes

on the importance of implementing a security system for the protection of sensitive data.

The demand for technologies and new procedures to manage what are security and storage systems, all this promoted what is the birth of pentesting, one of the objectives of these tests is the identification of security vulnerabilities, through the use of specific techniques and/or tools.

In the digital world in which we live, it is very important to guarantee the security of our information, since most organizations have become an easy target for this. It is for this reason that today there are a variety of methodologies that guide us and help many of the auditors to be able to carry out tests and to apply metrics with the sole purpose of analyzing, controlling the procedures so that they verify the security they have. the companies. To carry out this, an investigation was made of most of the most notable characteristics of the OSSTMM, OWASP, ISSAF methodologies using what is bibliographic research, in this way arriving and finding procedures, standards that guide the effective realization of tests. of penetration, as a result it is expected that one of the proposed methodologies complies with the standards and thus helps with a contribution to the auditors and that it is more complete since in this way they can prioritize the levels of risk of incidents or danger that these have on the objectives proposed by the company to carry out the pertinent tests.

Keywords: Ethical Hacking, vulnerability, penetration tests, methodologies for pentesting, attacks, security.

CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

INTRODUCCIÓN

En la actualidad el mundo va creciendo digitalmente y las empresas han llegado a la conclusión de trasladar casi toda su información a servidores en la nube, de esta manera es como se ha llegado a producir incrementos y mejoras del uso de las nuevas tecnologías, cloud computing, aplicaciones web,, internet, y esto ha provocado también el incremento de ciberdelincuentes que buscan la manera obtener información sensible, dinero o algún bien de valor que tienen dichas empresas, los ataques de estos son cada vez más sofisticados y mucho más frecuentes. Estos ciberdelincuentes buscan la manera y llegan a valerse de los fallos o vulnerabilidades en las redes o sistemas para llegar a obtener el acceso a dicha información y generar un daño irreparable, pero no solo los sistemas de información se han visto involucrados si no también muchas de las veces las personas ya que por medio de estas resultan ser el eslabón más débil que existe y pueden llegar a tener las empresas.

La seguridad de la información cada día que pasa es uno de los mayores retos y tema de gran importancia para las empresas u organizaciones ya sean estás públicas o privadas.

Las organizaciones tienen la posibilidad de desplegar sus aplicaciones web en la nube estando así expuesto hacia todo el internet, el uso de infraestructuras convencionales en la nube y la presencia de diferentes vulnerabilidades conocidas por mencionar XSS hacen tener una preocupación de seguridad critica[1].

Las aplicaciones web son las más atacadas de hoy en día debido a que están presentes en la capa de aplicación[2], las vulnerabilidades brindan una entrada a los ciberdelincuentes que conducen a la perdida y exposición de datos confidenciales, como puede ser información sobre empleados, datos de tarjetas de crédito[3].

La estructura del presente trabajo se menciona a continuación.

Capítulo I: Se habla sobre el hecho de interés, además se establece los requerimientos que se tiene que cumplir, se detalla la justificación de porque se debe de abarcar el tema propuesto, cual es el problema y las posibles soluciones.

Capitulo II: En este capítulo se desarrolla el proyecto como tal va desde la definición básica del escenario pasando por la fundamentación teórica hasta la implementación del mismo.

Capitulo III: Se crea un plan para evaluar los resultados obtenidos de las pruebas de penetración que se realizó en el escenario propuesto, finalmente las conclusiones que se obtuvieron tras realizar el presente trabajo, y las recomendaciones para futuras investigaciones.

1. CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1 Ámbito de Aplicación: Descripción del contexto y hecho de interés

La seguridad informática al igual que otros campos se basa en minimizar los riesgos asociados al acceso o el uso indebido de la información por lo que es bueno y de vital importancia tener una gestión de riesgos donde se evalúan y cuantificarán los datos sensibles, equipos y el software que está dentro de la empresa u organización donde se tomarán precauciones tales como políticas de seguridad para protegerse contra un ataque y esto tenga lugar a reemplazar, modificar o alterar los datos o la información que se encuentra almacenada.

Para poder hablar de Hacking ético es imprescindible consultar las herramientas existentes de protección y prevención de datos. El hacking ético es adquisición y uso de los conocimientos adquiridos de ciberseguridad para poder hacer pruebas de penetración en redes sistemas o dispositivos que estén conectados a la red para de esta manera encontrar vulnerabilidades para explotar exploits con el único propósito de informarlos para poder tomar las medidas sin poner en peligro los sistemas o la información sensible con la que cuenta. Una de las técnicas o procedimientos usados es la seguridad de cifrado de la información que se utiliza para proteger los datos o información confidenciales transmitidos en los sistemas u otros tipos de redes de comunicación. Este cifrado ayuda a proporcionar una protección aparte o adicional para proteger lo que es la confidencialidad de la base de datos. La información se cifra a través de un algoritmo que este está cifrado de tal manera que ayude a controlar los accesos malintencionados. Los usuarios no autorizados con acceso a datos cifrados tendrán ciertas dificultades para acceder a ellos y poder descifrarlos, pero para esto solo tendrán acceso los usuarios autorizados tendrán los accesos (o claves) de cifrado para poder acceder a la información.

Pentesting es un método para encontrar posibles vulnerabilidades, defectos o brechas en lo que es el área de red. La mayoría de los hackers éticos tienen que ser certificados u otros profesionales de la ciberseguridad de la información suelen realizar las pruebas fuera de la red que estamos utilizando, aunque en ocasiones también están presentes en el sistema. Las pruebas de pentesting extrema que a menudo se realizan, es a ciegas sin tener o conocer las medidas

de la empresa y la supervisión de seguridad que tiene en la red. Un pentesting externo de este tipo puede llegar a infringir la red y esto también puede proporcionar información sobre la validez o eficacia de las medidas de seguridad en caso de infracción. Los pentesting extremos a menudo o casi siempre se realizan a ciegas sin ningún conocimiento de las medidas de la empresa y la supervisión de seguridad de dicha información que tiene en la red. Si un pentesting que por lo general son de este tipo, infringen la red esto también puede proporcionar información que pueda afectar sobre la validez o eficacia de las medidas de seguridad en caso de infracción.

Toda prueba de penetración interna generalmente estos incluyen las medidas de seguridad interna sobre los evaluadores que pueden intentar violar las redes informáticas de los usuarios o llegar utilizar otros métodos para adquirir y evaluar las vulnerabilidades de seguridad interna. Además, los supervisores de red deben ser auditados para evaluar su respuesta a cualquier recha de seguridad que haya ocurrido.

Según [4] en internet existen más de 1.92 mil millones de sitios web, es decir que, de todos los sitios de internet, menos de 200 millones están activos El hito de 1000 millones de sitios webs se llegaron a alcanzar por primera vez en el mes de septiembre del 2014, según lo confirmó NetCraft en una encuesta que se realizó de servidores web de octubre de 2014 y este lo estimó y anunció por primera vez Internet Live Stats (ver el tweet del inventor de la World Wide Web, Tim Berners-Lee).

Según [2] las aplicaciones web son el objetivo de piratas informáticos, esto debido a que están presentes en cada de aplicación, el informe CLUSIT [5] del año 2022 menciona que en el año de la pandemia los ciberataques a nivel mundial aumentaron en un 25% en comparación con el año anterior.

Como trabajo de titulación se propone un análisis de metodologías para pruebas de pentesting usando ethical hacking que nos ayuden para la identificación, explotación y corrección de vulnerabilidades haciendo uso de las metodologías OWASP, OSSTMM, ISSAF.

1.2 Establecimiento de requerimientos

En la actualidad la seguridad en los sistemas informáticos es importante debido a que es el área que se encarga de proteger la información sensible de una empresa u organización, el autor[6] en su investigación realizada menciona que más de la mitad de todos los sitios webs que existen en internet tienen muchas vulnerabilidades de seguridad altas presentes, la gran mayoría fácil de solucionar, y otras que llevan arrasando en la historia por su popularidad, por mencionar a eternal blue que es un exploit desarrollado por la nsa en cual fue filtrado y usado por ciberdelincuentes para usarlo junto con el ramsonware wannacry.

Por esa razón es por la que debe implementar soluciones adecuadas ante esta problemática que afectan disponibilidad, confidencialidad, la integridad y perdida de los datos. Existen muchas empresas que brindan y ofrecen servicios de pruebas de penetración automáticas que en ocasiones revelan falsos positivos sobre las vulnerabilidades, es por ellos que se requiere de la presencia humana, para que así ayude y verifique los hallazgos mediante la implementación de pruebas manuales que ayuden a descubrir que dichas vulnerabilidades sean ciertas.

1.3 Justificación del requerimiento a satisfacer.

Dado que al dia de hoy y en la actualidad los ataques a las empresas u organizaciones han ido aumentado por el crecimiento de la tecnología y de nuevos métodos que van saliendo evolucionando y actualizándose día a día, todas estas técnicas son empleadas por los atacantes para así cometer dichos delitos informáticos, en los que se ven afectados directamente los activos de las mismas ya que a partir de esto empiezan a perder información sin ninguna razón y no tienen control sobre estas ya que al no tener algún método de mitigación o una gestión de riesgos sobre estos ataquen se ven muy vulnerables. Dentro de este estudio comparativo de toma en cuenta de las etapas de las cuales conforman las metodologías y el hacking ético ya que al realizar este estudio se determinará las similitudes, diferencias de las herramientas que existen y de como podemos hacer uso de las mismas mediante pruebas de pentesting. En algunos o gran parte de países que cuentan con empresas grandes se dedican a invertir en mejorar la calidad de seguridad informática con la que cuenta, en

algunos ha crecido de una manera acelerada y rápida, a diferencia de otras partes que han hecho caso omiso a esta y no han tomado en cuenta y el crecimiento a sido lento, pero todo estamos de acuerdo que en este mundo digital en el que estamos viviendo actualmente el activo más importante que se debe de tener en cuenta es la información ya que este es intangible pero de un precio muy valioso pueden llegar a tener las empresas dentro de la misma.

Se ha llegado a la conclusión que la manera más recomendable y efectiva es tomando medidas de contingencia ya sean estas preventivas o predictivas, las cuales ethical hacking nos ofrece a través de sus herramientas y a partir de esto permitir observar las falencias con las que cuentan las instalaciones de una empresa.

Las pruebas de penetración que se realizan a menudo son de vital importancia ya que estas ayudan a llevar un control de la protección de los datos e información con la que contemos y mostrando los puntos débiles de estas que a simple vista muchas de las veces no son evidentes, para esto tenemos a los profesionales que son los hackers éticos encargados en hacer simulaciones como crackers y encontrar fallos en los sistemas vulnerando, explotando y encontrando fallos para así de esta manera poder llegar a mitigarlos y tomar medidas las cuales beneficien a los usuarios que están siendo auditados, todo esto se realiza con el único objetivo de alertar a las organizaciones los riesgos que pueden sufrir sus instalaciones al tener esas brechas abiertas y no tratarlas a tiempo como debería y así prevenir a futuro problemas o inconvenientes.

El proceso que realizan los hackers éticos es de vital importancia pero esto no quiere decir que ya se hayan solucionado todas las vulnerabilidades o problemas de seguridad que se tengan, ya que cada vez los crackers o personas malintencionadas buscan nuevas maneras y formas de robar dicha información, por eso las empresas deben de priorizar el solucionar dichas vulnerabilidades ya sean estas de alto, medio o bajo riesgo de mitigarlos, pero siempre todo esto queda y tiene la ultima palabra el cliente contratante es quien decide si mitigarlos o dejarlos tal y como esta.

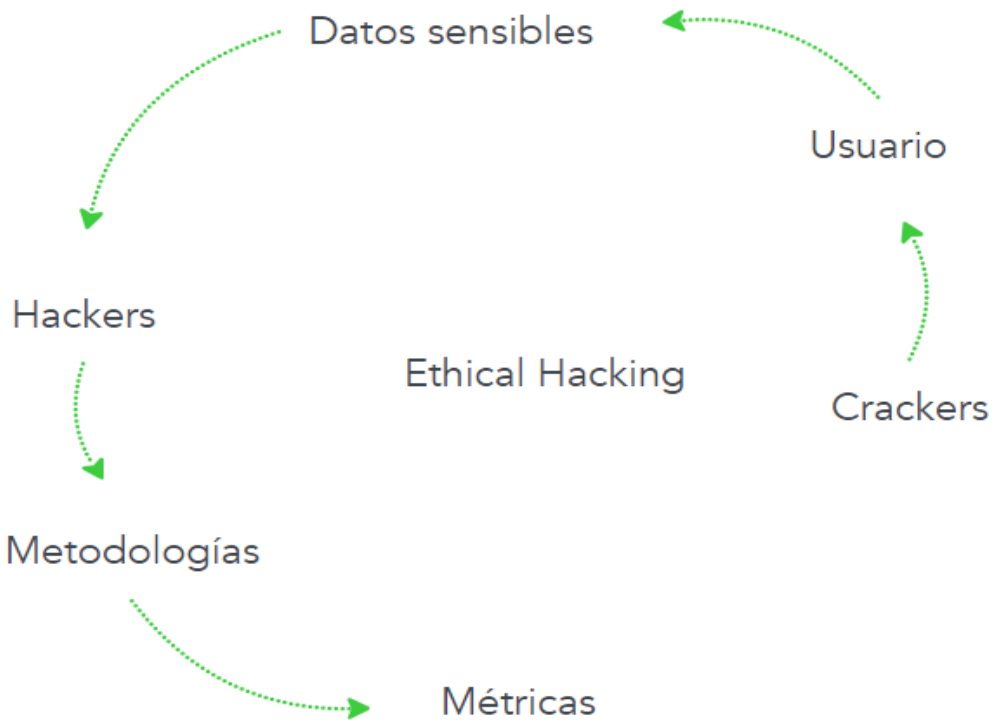
2. CAPÍTULO II. DESARROLLO DEL PROYECTO

2.1 Definición del escenario

En el presente escenario se ha constituido por optar de tres metodologías de lo que es pentesting mediante Hacking Ético. Para la correcta realización del mismo se tomarán de todas las fuentes que haya posibles para poder hacer la comparación de dichas metodologías, con la única finalidad de encontrar antecedentes para poder tener bases de lo que es la investigación y de esta manera poder llegar a tener un buen desarrollo de trabajo propuesto a continuación, de las metodologías para realizar una correcta prueba de penetración en empresas u organizaciones que estas requieran para buscar vulnerabilidades o fallos y proceder a mitigarlos.

La Ilustración muestra cómo actúan las metodologías en un escenario de atacante y víctima y que ventajas se obtiene al hacer uso de las mismas al momento de buscar vulnerabilidades.

Ilustración 1: Metodologías



Fuente: Elaboración propia

2.2 Fundamentación teórica del Escenario

La pandemia que fue generada por el virus covid-19 ha causado cambios en los aspectos cotidianos en la sociedad actual, llegando así a afectar la forma de educación, trabajo, compras, etc. Es a través de las TIC's que dichas actividades aún se siguen realizando, pero cada familia desde sus hogares. Todo esto a llevado a que los riesgos que tengan al robo de información sean mucho mayores por el uso de las tecnologías que se llegaron a intensificar.

La seguridad informática, como cualquier otra área, se enfrasca en la minimización de los riesgos que puedan existir tanto en los accesos o el uso indebido de la información, de esta manera es bueno que las empresas cuenten con una buena gestión de riesgos para así más adelante poder mitigar las vulnerabilidades, donde se llega a valorar mucho la información que existen dentro de las organizaciones, donde se estén usando procedimientos de medidas preventivas las cuales serían de mucha ayuda para así de esta manera poder protegerse contra los ataques y evitar el reemplazo, la alteración y/o modificación de la información que esta almacenada.

2.2.1 Hacking Ético

Hacking ético es la persona o individuo o también llamado sombrero blanco, este hace referencia a la habilidad o modo que tiene esta persona para aplicar sus conocimientos de ciberseguridad en seguridad informática y poder detectar fallos, vulnerabilidades dentro de los sistemas, estos son expertos los cuales irrumpen de manera ética y con el consentimiento de la víctima.

2.2.2 Pruebas de penetración

Las pruebas de penetración o también llamadas pentesting es una práctica que se debe de poner a prueba en lo que son los sistemas informáticos, redes o aplicaciones web para de esta manera llegar a encontrar fallos, vulnerabilidades que un atacante a futuro puede encontrar y explotarlas.

2.2.3 Piratas Informáticos

Las actividades mencionadas como el "teletrabajo, teleducación y el comercio electrónico" han llegado a ser un foco de atención de los piratas informáticos, los cuales intentan comprometer y vulnerar los equipos empresariales aprovechando la digitalización remota de las operaciones institucionales[10], en

vista de que en la mayoría de casos, existe beneficios propios a costa de alterar la integridad de la información.

2.2.4 Ataques Informáticos

Debido a lo que se ha descrito anteriormente, se puede mencionar que un hospital en la Republica Checa se vio obligado a desactivar todos los sistemas informáticos y cancelar todas las operaciones planificadas por el ataque de un virus ransomware[11], por otro lado se puede mencionar el caso de una escuela secundaria en Boston-Massachusetts reporta intrusiones en la clase en línea utilizando l software de teleconferencia Zoom [12].

Los piratas informáticos sustraen datos valiosos, como nombres de usuario y contraseñas, información de tarjetas de crédito y otra información intima de los usuarios. Los atacantes usan la técnica de phishing en tres líneas de ataques: páginas web, correo electrónico y sms. Estas últimas son las más vulnerables por el hecho de la publicidad que la mayoría de páginas web tiene.

2.2.5 Seguridad de la Información

Desde que surgió la era digital la información y más al día de hoy donde la mayoría de las actividades se han digitalizado, la información ha tenido un rol más importante dentro de las empresas por lo que la seguridad de la misma debe de ser una prioridad.

Todo esto conlleva a que la información es de vital importancia y muy valiosa para las empresas ya que de ella dependen mucho, y si se ven afectados por fallos o vulnerabilidades que pueda encontrar algún cracker con malas intenciones entonces puede llegar a afectar los activos de dicha empresa ya que podría generar perdidas y ponerse en peligro al no haber hecho un plan de riesgos contra fallos de seguridad ante ataques a los sistemas.

2.2.5.1 Activa

La seguridad activa es aquella que está compuesta por un conjunto de normas o medidas de defensa que tienen como objetivo primordial la reducción de los constantes riesgos que afectan a un sistema de información. Con la implementación de esta medida se pretende impedir el acceso a información confidencial de los usuarios no autorizados[13].

2.2.5.2 Pasiva

Es aquella que tiene como finalidad la recuperación del sistema después de estar expuesto a ataques y presentar perdidas de información, además de minimizar el riesgo acontecido en el sistema[7].

2.2.6 Vulnerabilidad

Es uno de los puntos débiles de los sistemas, red, o aplicaciones web ya que puede ser usadas para llegar a causar un daño irreparable a empresas grandes o pequeñas. Existen puntos débiles en la informática y estas puede ser mediante el software o hardware las cuales el o los atacantes pueden llegar a comprometer lo que es la integridad de los sistemas o datos que procesan estas, las vulnerabilidades son fallos que se dan por no aplicar procedimientos robustos y estas pueden llegar a ser peligrosas.

2.2.7 Elementos de la seguridad de la información

Para asegurar que la información no pierda su validez se debe priorizar que la seguridad sea efectiva en pro de protegerla de daños, sustracción, hurto o copia de la misma. Debido a esta premisa es que muchos autores mencionan como mínimo tres características principales, en que la información debe poseer en cualquier contexto, estos:

Tabla 1: Elementos más importantes de la seguridad

Integridad	El contenido de los datos no debe ser alterado, a menos de que lo haga el personal autorizado.
Confidencialidad	Es el tipo de información que se debe de tener visible para las personas autorizadas a recibirlas.
Disponibilidad	Es aquella información que debe de estar visible para ser procesada por las personas autorizadas (gerentes o jefes de departamento).

Fuente: [14]

2.2.8 Pentesting

Una prueba de penetración o pentest es un ataque ya sea este simulado y autorizado contra los sistemas informáticos con el objetivo principal de evaluar las seguridades que existen en los sistemas. Durante las pruebas de penetración

que se realizan, se encuentran los posibles fallos que tiene presente un activo y se busca métodos de explotación tal y como lo haría un pirata informático con fines maliciosos y lucrativos con el fin de analizar los posibles escenarios en los cuales puede quedar expuesto dicho sistema.

Existen dos tipos de pentest que se catalogan según desde donde se lo realicen, las pruebas de penetración:

Tabla 2: Tipos de Pentest

Auditoría Externa (Covert Pentest)	Auditoría Interna
La auditoría externa tiene como objetivo identificar el grado de seguridad de la red externa de una empresa u organización.	La auditoría interna tiene como objetivo evaluar el nivel de seguridad presente en un entorno privado de una empresa u organización.

Fuente: [15]

2.2.9 Metodología PTES

El Peenetration testing Execution Standard(PTES) este fue creado por expertos en ciberseguridad para realizar auditorías de seguridad ya que este se ha convertido en un estándar con el cual podemos llegar a completar las auditorias y tener mejores resultados ya que estos cubren todo lo relacionado con las pruebas de penetración y son de vital importancia para la mitigación de errores o fallos, esta es un herramienta requerida ya que con aplicaciones o simplemente con instrucciones se puede ejecutar tareas de una manera mucho más sencilla, también nos ayuda con el análisis de las vulnerabilidades ya que de una manera activa toca el objetivo e identifican puertos ya sea de forma manual o automáticamente de vulnerabilidades existentes en los sistemas [16].

2.2.10 OWASP

El Open Web Application Security Project(OWASP), en una organización benéfica sin fines de lucro con la misión de hacer que la seguridad del software sea visible para el individuo y la organización para ayudarlos a tomar decisiones informadas sobre el riesgo de seguridad de software[17].

2.2.11 OWASP TOP 10

OWASP TOP 10 es un proyecto de seguridad patrocinado por OWASP. Este proyecto publica una lista de lo que considera los 10 principales riesgos de seguridad de las aplicaciones web en todo el mundo. La lista explica la vulnerabilidad con un ejemplo relevante y la forma de evitarla[17], la lista se enumera a continuación:

A1:2017 Inyección

En este tipo de vulnerabilidad se encuentran las inyecciones SQL, NOSQL, LDAP, se producen cuando un usuario manipula parámetros que son enviados a la base de datos como consultas, la base de datos no está preparada para recibir ese tipo de consultas y como resultado ocurren estos errores, como se menciona en la investigación realizada sobre inyecciones SQL, esta categoría de vulnerabilidades es una de las más severas que se dan en aplicaciones que interactúan con base de datos debido a que un atacante puede obtener acceso no autorizado y realizar modificaciones en la base de datos, esto debido a que no se implementó una correcta validación de entrada.

A2: Autenticación rota

Las funciones que se utilizan para la autenticación se implementan de manera incorrectas y esto permite que los atacantes logren capturar contraseñas.

A3: Exposición de datos confidenciales

Esta vulnerabilidad es causada debido a que los programadores de aplicaciones web no protegen datos confidenciales de los usuarios, y pueden ser obtenido desde sus servicios web, lo que permite que atacantes roben esta información y la usen para fines lucrativos o venderlas en fotos de la darknet.

A4: Entidades Externas XML

Es causada por procesadores XML están mal configurados y esto puede exponer archivos internos mediante el manejo de la URI, por dar un ejemplo se puede listar direcciones ip, puertos abiertos.

A5: Control de Acceso Roto

Se debe a que no se restringe de manera correcta a usuarios autenticados a directorios o archivos que no deberían tener acceso, mediante esto un atacante puede ver datos confidenciales, modificar registros de otros usuarios o inclusive volverse administrador del sistema.

A6: Configuración incorrecta de seguridad

Es causada por configuraciones predeterminadas, encabezados http mal implementados y mensajes de error que muestran rutas confidenciales.

A7: Cross Site Scripting

También conocido como XSS se produce cuando no se valida o escapa etiquetas html y JavaScript y son ejecutadas en el navegador web, mediante este tipo de vulnerabilidades un atacante puede obtener cookies de sesión, redirigir a usuarios a otros sitios webs, existen dos tipos de XSS reflejado y almacenado, en la investigación realizada[18] se menciona que son las vulnerabilidades más explotadas en las aplicaciones web.

A8: Deserialización insegura

Esta vulnerabilidad ocurre cuando un atacante utiliza datos que no son de confianza con el fin de aprovechar o abusar de la lógica de una aplicación y esto conduce a ataques más complejos como ejecución remota de comandos o denegación de servicios.

A9: Uso de componente de vulnerabilidades conocidas

Cuando se utilizan bibliotecas o componentes con errores conocidos y estos se ejecutan con los permisos que las aplicaciones, si un atacante kigra vulnerar un activo mediante un componente desactualizado podrá ser un medio de entrada hacia el servidor y control del mismo.

A10: Registro y monitoreo

Es causado debido a que no se implementa un monitoreo de las actividades de ciertos usuarios con el fin de detectar cuentas sospechosas, debido al monitoreo insuficiente que tiene como resultado la mayoría de los incidentes.

2.2.12 Web Application Firewall

Los firewalls de aplicaciones web (WAF) son el principal mecanismo de protección front-end para la infraestructura basada en internet que está constantemente bajo ataque[19].

2.2.13 Fuerza bruta

Este trata de generar todas las contraseñas posibles hasta una cierta longitud y sus hashes asociados[20]. Dado que hay tantas posibilidades, pueden llevar meses descifrar una contraseña. Aunque la fuerza bruta puede llegar a llevar muchísimo tiempo, normalmente lleva mucho tiempo menos que el que especifican la mayoría de las políticas de contraseñas para el cambio de contraseñas.

Los asesores y atacantes a menudo tienen varias máquinas sobre los que puede llegar a distribuir la tarea de ir a descifrar las contraseñas, lo que acorta enormemente el tiempo involucrado.

En consecuencia, las contraseñas que se encuentran durante los ataques de fuerza bruta siguen siendo demasiado débiles. En teoría, todas las contraseñas se pueden descifrar mediante fuerza bruta, con que tenga suficiente tiempo y buena potencia de procesamiento, aunque podría llevar hasta años y llegar a requerir una gran potencia informática.

2.2.14 Web Shell

Según la investigación[21] una Shell web es un programa codificado con un lenguaje de alto nivel como PHP, dichos scripts son cargados por un atacante luego de haber comprometido un servidor con el fin de seguir manteniendo acceso al equipo, sirve en la fase de post explotación en una prueba de penetración.

2.2.15 Contraseñas débiles

Cuando una contraseña cumple a medias las normas de las contraseñas estas son llamadas o consideradas contraseñas débiles. Esto facilita a que el cracker de contraseñas genere rápidamente hashes adicionales hasta que se encuentre con una coincidencia o el evaluador detenga el intento de agrietamiento[22].

2.2.16 Web Shell

Los listados de los directorios por si solos no representan una vulnerabilidad de seguridad. Pero eso no quiere decir que estos mismo no deben estar correctamente controlados por el acceso, que esto conlleva a que no pueda ser accedido por una persona o agente desconocido o no autorizado que conozca o adive la URL.

Muchas de las veces este listado de directorios esta oculto, un atacante puede identificar esta posición de los archivos protegidos con aplicaciones automatizadas.

2.2.17 Auditoria en los sistemas de información

La auditoría consiste en proceder a obtener la información de los equipos de cómputo y la seguridad de los SI, procedimientos, el correcto funcionamiento de los controles o archivos con el único fin de poder garantizar que la información que está entrando sea confiable y de manera segura que no se estén perdiendo en el proceso o no llegue a tener algún fallo o perdida y luego tener problemas.

2.2.18 Nmap

Es una aplicación que ayuda a efectuar rastreos de puertos y que es multiplataforma y es muy utilizado para evaluar los sistemas informáticos y poder descubrir servicios o servidores en una red informática, este envía paquetes que son definidos a otros equipos y hace un análisis de las respuestas.

2.2.19 Metasploit

Un exploits es un de las muchas herramientas que se usa para lo que son las auditorias informáticas de seguridad, con esto se puede probar y crear maquina remota para de esta manera poder probar las vulnerabilidades que tienen dichos sistemas y evitar la piratería.

2.2.20 Exploit

Un exploit es un ataque cualquiera el cual puede aprovechar las vulnerabilidades de la red, aplicaciones o sistemas, por lo que esta toma forma de una software o secuencia de algún código previsto para así poder hacerse del control de las computadoras acceder y robar la información de las mismas.

2.2.21 Crackers

Este puede considerarse como un subgrupo que se dedica a afectar a la comunidad de hackers, ya que se dedican a violar la seguridad de muchos sistemas informáticos de forma similar como lo que haría un hacker, pero con la diferencia que realizan la intrusión con fines de beneficios personal o explícitamente para causar daño a una determinada empresa u organización tocando sus datos sensibles.

2.2.22 Objetivo de evaluación

Un sistema tecnológico, producto o componente que está siendo identificado o sujeto a requerimientos o evaluaciones de seguridad para saber que tan vulnerable es a dichos ataques que puedan llegar a existir.

2.2.23 Inyección SQL

Esta vulnerabilidad se muestra mediante la falta de control en la información que se puede ingresar en una página web. Aplicaciones web que usan contenido dinámico para obtener datos a través de consultas SQL a una base de datos que pueden estar vulnerables si un atacante tiene la posibilidad de ingresar códigos en los parámetros mal configurados[24].

2.3 OBJETIVOS DEL ESCENARIO

2.3.1 Objetivo Principal

Analizar las metodologías para pentesting mediante ethical hacking que se aplicarían dentro de empresas u organizaciones para el control y acceso mal intencionado.1h

2.3.2 Objetivos Específicos

- Comparar las debilidades, fortalezas y en cómo afectan dichas metodologías.
- Analizar el entorno en cómo aplicar las metodologías dentro de las empresas que corren peligro de perdida de información.
- Determinar metodologías de hacking ético para llegar a ser aplicadas en los entornos de los sistemas o tecnologías de la información.

2.4 Escenario para análisis comparativo de las metodologías

El escenario está constituido por tres metodologías para pentesting mediante Hacking Ético. Para poder realizar este trabajo se tomará en cuenta de todas las fuentes posibles que estén relacionadas o enfocadas con los conceptos de Hacking ético, estas metodologías, es con la finalidad de poder llegar a relacionar los antecedentes y así poder llegar a tener un buen entendimiento y bases en lo que es la investigación y así poder dar el desarrollo más adecuado al trabajo que se ha propuesto a lo largo de este tiempo.

Se analizarán las diferentes vulnerabilidades mencionadas en las metodologías antes mencionadas para las pruebas de penetración.

2.4.1 Software de Virtualización

Para elaborar el laboratorio de hacking profesional se utilizó VMware Workstation el cual es un software que opera bajo una licencia, pero además ofrece un periodo de prueba del cual para este caso se hizo uso, la versión que se utilizó para usarla es la 16.0.0.

Se opto por elegir este software debido a que el mismo es de pago y este presenta varias ventajas frente a otros como lo que viene siendo VirtualBox, una de las características más importantes es que compatible con DirectX 11, y gráficos que trabajen con OPENGL versión 4.1[25].

2.4.2 Sistema Operativo

2.4.2.1 Parrot Security OS

Parrot Security OS, tiene el kernel de GNU Linux y esta, está basada en Debian, y se enfoca 100% en pruebas de penetración, cuenta con una amplia suite de herramientas pre instaladas enfocadas en identificar vulnerabilidades en sistemas operativos y aplicaciones web.

2.4.2.2 Kali Linux

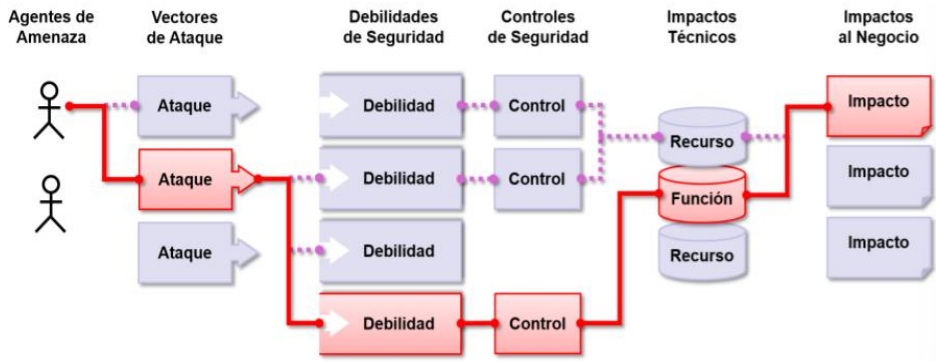
Kali Linux esta es una distribución que es basada en lo que es Debian GNU Linux diseñada principalmente para lo que son auditorias y ciberseguridad, llevar un mejor control de las vulnerabilidades que puedan ocurrir dentro de las organizaciones.

2.4.3 Metodologías

2.4.3.1 Metodología OWASP

Los atacantes pueden potencialmente llegar a usar diferentes rutas que a través de la aplicación pueden perjudicar al negocio u organización en la cual se este ejecutando. Cada camino de estos representa un riesgo en el cual se debe de estar dispuesto a correrlo ya que al momento de encontrar una vulnerabilidad este se tiene que mitigar y puede o no ser suficiente grave para merecer la atención debida o no.

Ilustración 2: Riesgos en seguridad de aplicaciones



Fuente: [8]

Muchas de las veces, estos caminos son fáciles de encontrar, hallar y explotar, mientras que otras ocasiones son extremadamente difíciles el cual requieren de mucha dedicación y constancia.

De esta manera, el peligro y daños causados perjudica de una manera que no pueda llegar a tener consecuencias o a su vez podría llegar a tener serios problemas y perjudicarlo bastante dejando al borde de la quiebra. Con este fin de determinar los riesgos que puede tener una empresa u organización se evalúan lo que son todas las probabilidades que se asocian a cada agente de peligro o amenaza de los ataques y las debilidades de seguridad con las cuales cuenta y combinar este impacto con la organización de negocio ya que estos factores llegan a determinar el riesgo general en el que se encuentran [26].

Tabla 3: Metodología OWASP TOP 10

OWASP TOP 10
A1: Inyección

A2: Autenticación Rota
A3: Exposición de datos confidenciales
A4: Entidades Externas XML
A5: Control de Acceso Roto
A6: Configuración incorrecta de seguridad
A7: Cross Site Scripting
A8: Deserialización insegura
A9: Uso de componente con vulnerabilidades conocidas
A10: Registro y monitoreo

Fuente: Elaboración propia

El OWASP Top 10 se enfoca en identifica los riesgos más peligrosos para un amplio tipo de organizaciones. Para todos estos riesgos se proporcionan una serie de información sobre la probabilidad y el impacto que este puede causar.

A1: 2017 Inyección

Los fallos, daños o vulnerabilidades de inyección, como NoSQL, OS, SQL o LDPA ocurren cuando al momento de enviar muchos de los datos no confiables a un intérprete, como parte ya sea de una consulta o comando. Los datos dañinos del atacante pueden engañar al interprete para que este proceda a ejecutar los comandos de una manera involuntaria y entonces procede a dar acceso a los datos sin ninguna debida autorización[27].

A2: 2017 Perdida de autenticación

Las funciones de las aplicaciones relacionadas a una autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo así de esta manera los atacantes comprometer usuarios y contraseñas, token de sesiones o explotar otras fallas de implementación para asumir la identidad de otros usuarios ya sean estos temporales o a su vez permanentes[17].

A3: 2017 Exposición de datos sensibles

Muchas de las aplicaciones web y APIs no protegen de una manera adecuada los datos sensibles tales como información financiasen, de salud o la información personalmente identificable (PII). Los atacantes pueden modificar o robar este tipo de información que no está debidamente protegida para así poder llevar a

cabo fraudes con tarjetas de créditos, robos de identidad o algunos otros delitos[27].

A4:2017 Entidades Externas XML (XXE)

Muchos de los procesadores XML ya sean estos antiguos o mal configurados evalúan referencias a entidades externas en lo que son documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en los servidores que no están actualizados, escanear puertos de la LAN, ejecutar códigos de una manera remota y realizar ataques de denegación de los servicios.

A5: 2017 Pérdida de control de acceso

Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder de una manera no autorizada a funcionalidades o datos, de cuentas de otros usuarios, llegar a ver lo que son los archivos sensibles, modificar los datos y cambiar los derechos de accesos o permisos que estos tengan y un sin número de más cosas que pueden llegar a hacer estos atacantes[17].

A6: 2017 Configuración de seguridad incorrecta

Una configuración incorrecta en lo que es seguridad es uno de los problemas muy comunes que pueden existir y esto se debe en cierta parte a la configuración manual que suelen hacer, como ad hoc o por omisión (o puede ser directamente por que le falta configurar). Son ejemplos: S3 buckets abiertos, mensajes de error con contenido sensible, cabeceras HTTP mal configuradas, falta de parches de seguridad, frameworks, dependencias o componentes desactualizados, etc[27].

A7: 2017 Secuencia de comandos en sitios cruzados (XSS)

Las secuencias de los comandos en sitios cruzados (XSS del inglés cross-site scripting), estos pueden ocurrir cuando una aplicación esta tomando de cierta manera datos que no son confiables y estos se envían a través del navegador web que permiten a los atacantes colocar parte de códigos maliciosas para así vulnerar la información de los usuarios y obtener los datos sensibles de la misma[26].

A8: 2017 Deserialización insegura

La deserialización insegura de los datos, estos son defectos que llegan a ocurrir de una manera cuando la aplicación tiende a recibir objetos que son serializados, pero de alguna forma dañinos y de esta manera puede ser manipulados o borrados por la persona que está haciendo el ataque, en el peor de los casos la deserialización de manera insegura puede llevar a conducir al atacante a la ejecución remota en el servidor[25].

A9: 2017 Componentes con vulnerabilidades conocidas

Los componentes con vulnerabilidades conocidas, tienen componentes en las bibliotecas, módulos, framework que se ejecutan estos con los mismos privilegios en la aplicación, un componente es vulnerable cuando se lo explota de una manera adecuada y concisa ya que al atacar a este puede provocar una pérdida de datos y esta puede llegar a tomar el control del servidor. Intentar debilitar las defensas de las aplicaciones y permitir diversos ataques estas vulnerabilidades pueden afectar de una manera muy dañina a las organizaciones si no se llega a tener un buen control sobre ellos [28].

A10: 2017 Registro y monitoreo insuficientes

El registro y monitoreo es insuficientes a estos incidentes ya que de alguna u otra manera estos permiten a los atacantes llegar a mantener el ataque en el tiempo para pivotear en otros sistemas y de esta manera poder manipular, destruir o extraer los datos ya que debido a estos estudios se demuestra que a partir de una brecha que haya terceras personas pueden aprovechar y sacarle provecho para así poder acceder a los datos internos de las organizaciones [17].

2.4.3.2 Metodología ISSAF

La metodología ISSAF es un marco de trabajo con el cual se puede evaluar y modelar el nivel de los requisitos y procesos internos en cuanto a seguridad de la información, dicha metodología puede definir en un plan de pruebas que es basada en dominios, estos son los que se van a basar en las pruebas que se lleguen a realizar. Esta metodología empieza a abarcar una cantidad enorme de procesos tecnológicos y SI que sirven para cubrir los procesos de un nivel alto en los asociados a las TICs. Esto principalmente es usado en lo que son las

empresas u organizaciones financieras, de servicios y tecnológicas que existen a nivel mundial. Su fortaleza en los procesos de evaluación es generalmente fundamentada en permitir que las etapas de preevaluación en los procesos que se realicen de auditorías o de pentesting. Los procesos de la evaluación mientras entren a la parte práctica de la aplicación de técnicas propuestas y materialización de muchos aspectos planeados de una manera previa [30].

El ISSAF es un marco de trabajo para evaluación de políticas y procesos de seguridad de la información en las organizaciones. En esta metodología se integran herramientas de gestión las cuales hace en conjunto, un proceso de evaluación completo para las organizaciones. Para este caso se llegan a definir unas herramientas de lista y gestión de control interno[31].

- Evaluación de procedimientos y políticas de seguridad de la información en las organizaciones o empresas para un buen cumplimiento de estándares en TI y normativa legal aplicable en los estándares de seguridad.
- Evaluación e identificación de áreas de comercio de servicios de infraestructuras que se prestan desde las áreas de TI
- Desarrollar análisis de vulnerabilidades y pentesting para poder identificar y que representen algún riesgo potencial o significativo a cualquier activo de información en las organizaciones
- Definir el modelo ideal para la valoración por dominios de seguridad.
    - Detección de las configuraciones que contengan algún problema para de esta manera poder llegar a corregirlos.
    - Detección de riesgos que suelen estar asociadas a las nuevas tecnologías y que luego uno tiene que proceder a tratarlos de una buena manera para un buen manejo de la información.
    - Detección de los riesgos que estén asociados de manera personal y a los procesos de negocio para de esta manera ya empezar a tratarlos.
    - Fortalecer tecnologías y procedimientos existentes en las organizaciones.

Empezar a brindar mejores y más prácticas y procesos para poder salvaguardar la información de los negocios, y estos pueden llegar a ser favorables al momento de aplicar los procesos de normas IEC/ISO 27001 entre otras ya que

ayudan de una u otra manera a poder hacer una buena auditoria o mitigación de las vulnerabilidades[31].

Ilustración 3: Controles ISSAF

Fuente: [29]

2.4.3.3 Metodología OSSTMM

La metodología Open Source Security Testing Methodology Manual (OSSTMM) que en español es el manual de Metodologías abiertas para la verificación de seguridad ya que hoy en día se desarrolla y mantiene por el ISECOM (Institute For Security and Open Methodologies, este de aquí es conocido como un gran manual para el pentesting en ambientes de redes y tecnologías de la información.

Según [23], “The OSSTMM is about operational security. It is about knowing and measuring how well security works. This methodology will tell you if what you have does what you want it to do and not just what you were told it does”. La metodología básicamente se encarga de medir que también este trabajando la seguridad de la organización, validando que sus herramientas hagan lo que deben hacer en varios espacios corporativos.

Dicha metodología ofrece dentro de las ejecuciones la posibilidad de poder realizar procesos evaluativos de seguridad de una forma integral a toda la organización, esta integración se describe como una interconexión entre los procesos de TI que están asociados a lo que es seguridad y que los actores principales de la metodología va a definir puntualmente la relación que existe

entre el personal que está dentro de las empresas ya que los procesos se desarrollan internamente en los sistemas que usan programas o software dentro de la empresa. Esta prueba de seguridad se realiza para las configuraciones que se debe de dar para las soluciones y de esta manera los sistemas de información se pueda garantizar las operaciones que hayan sido logradas o que se estén realizando y estas deben de estar bien hechas para lo que fueron destinada y programadas ya que si no es así entonces se tendría problemas con las auditorias de seguridad que se realicen.[23].

Definición de las secciones que se van a evaluar

De esta manera está definido por secciones en las cuales se ve como se utiliza una evaluación con cada uno de los componentes que se interconectan lo cual ha permitido de esta manera tener una metodología para poder ser ampliamente usada por los profesionales que son los hacker éticos o que alguna persona que tenga las habilidades adecuadas para realizar este tipo de trabajos[23].

Sección A: Seguridad de la información

- Revisión de la inteligencia competitiva
- Revisión de privacidad
- Recolección de Documentos

Sección B: Seguridad de los procesos

- Realizar un test de solicitud
- Realizar un test de sugerencia dirigida
- Realizar un test de las personas confiables

Sección C: Seguridad de las tecnologías de internet

- Determinación de la logística y de control
- Sondeo de la red
- Clasificación de los servicios de TI
- Búsqueda de información de competitividad
- Validación de la privacidad
- Obtener capturar documentos
- Buscar y verificar vulnerabilidades

- Probar aplicaciones que están en internet
- Enrutar redes de datos
- Prueba de sistemas confiados
- Pruebas los controles de acceso
- Pruebas de IDS
- Probar las contingencias
- Desencriptación de password
- Pruebas de DoS, Denia lof services
- Validad políticas de seguridad

Sección D: Seguridad en las comunicaciones

- Pruebas de servidores de telefonía
- Pruebas de mensajes y correos hablados
- Verificación de fax
- Pruebas de modem

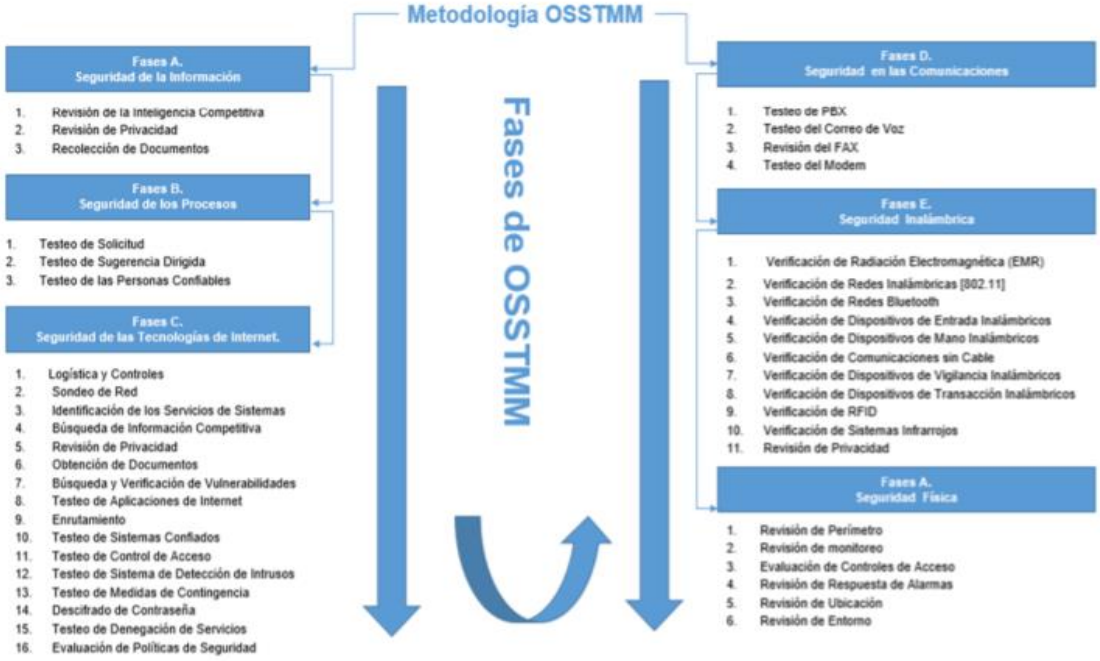
Sección E: Seguridad inalámbrica

- Validación electromagnética
- Validación de redes inalámbricas
- Validación de red de equipos por bluetooth

Sección F: Seguridad Física

- Revisión monitoreos realizados
- Revisión de control de acceso
- Validación de respuestas por alarma
- Validaciones generales del entorno

Ilustración 4: Fases de Metodología OSSTMM



Fuente: [23]

El proceso de análisis de la seguridad

Esta metodología llega a enmarcar un proceso amplio de análisis de seguridad den en un esquema pasos claros para de esta manera conformar y poder llevar a cabo un proceso de análisis de las vulnerabilidades en seguridad, de esta manera estos son conocidos como dimensiones de seguridad [23].

Visibilidad

Es una manera de definir todo aquello que pueda llegar a verse a nivel corporativo para así de esta manera monitorear sin la necesidad de tener y usar algún dispositivo tecnológico.

Acceso

Esta es una manera de definir una entrada a nivel de seguridad informática como puede ser un punto en la red, alguna aplicación web o alguno que nos permita ser definido como un caso público para así poder tener acceso al sistema sin ninguna restricción mientras se tenga la autorización de los administradores.

Confianza

Este se define como el nivel de seguridad que se tiene en cuenta para la integridad de la información y el nivel de acceso que van a tener al mismo en particular.

Autenticación

Esta medida en la con la cual vamos a acceder para realizar cada proceso mediante la autenticación que nos hayan otorgado.

Confidencialidad

Son autorizaciones que se realizan en certeza de que las partes de los interesados estén de acuerdo para así de esta manera le den el acceso a la información sensible.

Privacidad

Esto se refiere únicamente que se le da el acceso de la información a los interesados mientras estos estén de acuerdo en brindarle, ya que esto es un riesgo que se corre.

Autorización

De esta manera este proceso cuenta con el consentimiento y con el visto bueno de las partes interesadas para la ejecución de la misma.

Integridad

De esta manera se tiene la certeza de que el proceso que se está realizando finalmente no puede desviarse para poder modificarlos, ya que de esta manera estaría violando la integridad de la información a la cual se está dando acceso.

3. CAPÍTULO Ⅲ. EVALUACIÓN DEL ESCENARIO

3.1 Plan de evaluación

Se propone analizar tres metodologías para pruebas de pentesting mediante hacking ético, se basa principalmente en el análisis comparativo de distintas metodologías que componen el hacking ético que con esto conlleva a la finalidad de hallar vulnerabilidades y fortalezas en cada una de estas para así al final de todo esto crear un reporte de la aplicación de las metodologías.

Resultados de la evaluación

Durante el análisis y comparación de las principales metodologías de pruebas de pentesting, se hizo un análisis cualitativo respecto a los requerimientos y principales requisitos de seguridad en lo que son las aplicaciones web. Para llegar a profundizar este análisis, se llegó a la finalidad de crear una escala de una evaluación cualitativa de las metodologías, para poder llegar a un análisis de cómo se abordan las vulnerabilidades, perdida de información, peligros que corren las aplicaciones web.

Tabla 4: Comparación Metodologías

Metodologías / **Patrones**	**ISSAF**	**OWASP**	**OSSTMM**
Rigor de metodología	Alta	Muy alta Centrada en lo que es web, pero muy didáctica	Muy alta
Niveles de detalles	Detallada pero sencilla, faltando así elementos de cloud computing y protección de datos.	Muy detallada y su enfoque en la web en demasiado meticulosa. Y orienta muy bien el trabajo del auditor	

Facilidad de uso	Se puede usar con conocimientos medios	Muy técnico y muestra el uso de herramientas, sugiere usos y muestras de varios ejemplos.	Requiere entrenamiento previo y practicar, además de certificaciones.
Ámbitos de aplicación	Organizaciones e instituciones	Para todo tipo de organizaciones con presencia web	Todo tipo de organizaciones pymes, instituciones educativas.
Entorno de aplicabilidad		En todo lo que tenga que ver con aplicaciones enfocadas a la web.	
Uso por los auditores	Es lineal y cobre las etapas típicas de una auditoria con test de intrusión.	Usado frecuentemente en combinación de otras metodologías por la precisión y nivel de detalle con la que cuenta	Es muy usado a nivel general, aunque la tendencia es simplificar, aunque el uso requiere de un poco de conocimiento y tener experiencia.
Ventajas		Facilidad de uso de los controles más conocidos “Top Ten”. Novedoso y bien estructurado, se preocupa de las	Se integra y tiene en cuenta todos los estándares de seguridad de la información. Ofrece.

		auditorias de la web, elementos centrados en el marketing y el negocio.	

Fuente: Elaboración Propia

Tabla 5: parámetros

Valor	Descripción
0	No se hace ni una sola alusión a las vulnerabilidades ni a testing de seguridad o alguna que relacionada con la misma.
1	Se hace mención a las vulnerabilidades, pero este no se describe como hacer los pentesting de seguridad para así detectar a la misma.
2	Se hace mención como realizar un pentesting de seguridad, pero la información presentada no llega a ser suficiente para poder realizar una prueba de seguridad mucho más real.
3	Se describe como realizar la prueba de seguridad con suficientes detalles para así de esta manera ser aplicada directamente en una prueba de detección de vulnerabilidades y seguridad real.

Fuente: Elaboración Propia

Tabla 6: Comparación

Principales Vulnerabilidades	OWASP	ISSAF	OSSTMM
Inyección de código	2	2	1
Secuencia de los comandos en sitios cruzados (XSS)	3	3	0
Perdida de autenticación y gestión de sesiones	3	1	2
Pérdida de control de acceso	3	1	1
Referencia directa insegura a objetos	3	2	1
Ausencia de control de acceso a funciones	3	2	1
Configuración de seguridad incorrecta	2	2	1
Exposición de datos sensibles en distintas aplicaciones web	2	2	1
Falsificación de peticiones en sitios cruzados (CSRF)	3	0	0

Uso de componentes con las vulnerabilidades más notables	3	1	1
Entidades externas de procesadores XML (XXE)	3	0	1
Deserialización de defectos insegura	2	0	0
Registros y monitoreos insuficientes	2	0	0
Riesgos de seguridad de la aplicación	1	1	1
Pruebas de gestión de identidad	3	1	1
Totales	**38**	**18**	**12**

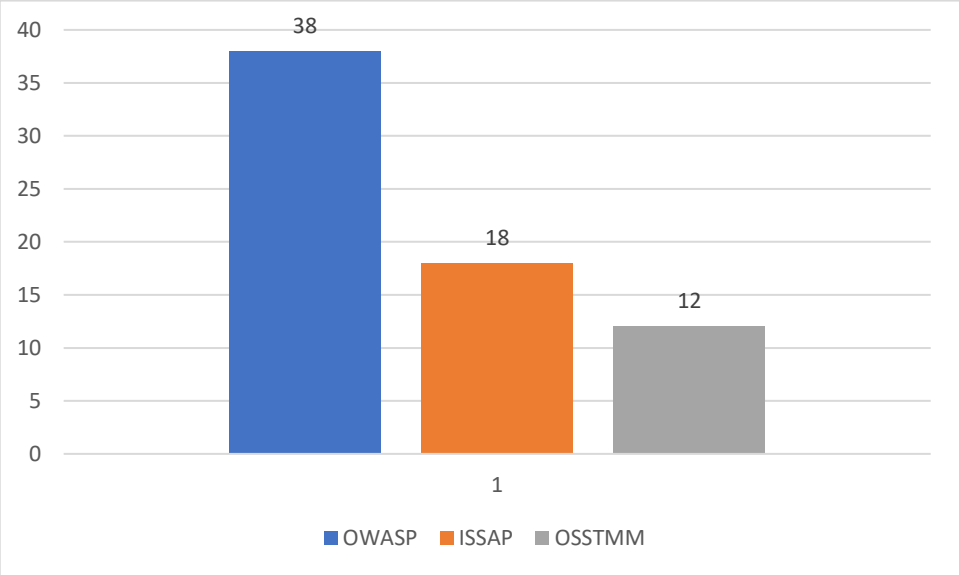
Fuente: Elaboración Propia

¿Estas metodologías de pentesting pueden llegar a ser capaces de evaluar las vulnerabilidades presentes en la actualidad en aplicaciones web?

Como se muestra en la ilustración ninguna de las metodologías abarca la evaluación completa de las principales vulnerabilidades en las aplicaciones web. La guía de pruebas de OWASP es la que presenta un nivel más alto (38), le sigue la metodología ISSAF (18) y la metodología OSSTMM (12), según lo diseñado.

Por lo tanto, puede afirmarse que ninguna de las metodologías de pruebas de penetración analizadas enuncia todas las evaluaciones de seguridad que se requieren para detectar al menos las principales vulnerabilidades en aplicaciones web. Necesitan por tanto un proceso de adaptación y completitud que dependerá de las competencia y experiencias de los equipos de seguridad que tengan la misión de realizarlas.

Ilustración 5: Metodologías de pentesting comparativa



Fuente: Elaboración Propia

CONCLUSIONES

- El análisis de las metodologías pentesting para Hacking ético, nos permite y ayuda a identificar muchos aspectos que sean relevantes para de esta manera poder llegar a tener en cuenta al momento de establecer la seguridad de los datos en las empresas ya sean estas grandes, medianas o pequeñas, ya que todas sin excepción están expuestas a ataques informáticos.
- La administración realizada de una buena manera de la seguridad informática ya sea esta en pequeñas, medianas o grandess empresas, esto nos ayuda en asegurar toda la información, en todos muchos aspectos o en todas las áreas o departamentos con la cual comprende la empresa.
- La ciberseguridad en este caso nos permite analizar las funcionalidades que estas comprenden para tener un buen análisis dentro de las organizaciones. Mediante estas funciones y administraciones de las actividades que se realizan para el procesamiento de los datos en los sistemas donde buscamos la adecuada manera de aplicar las metodologías ya que son de mucha ayuda para las empresas que cuentan con información sensible y se ven expuestas a ataques malintencionados.
- A pesar de que hay un aumento en la demanda del aseguramiento de información sensible por hoy en día haber constantes innovaciones en ataques que realizar los hackers, es de vital importancia tener en cuenta metodologías que nos sean de utilidad y tener el conocimiento de sus fortalezas y debilidades, ya que así nos ayudarían a mejorar la seguridad de nuestra empresa y a tener un mejor control de nuestra información.

RECOMENDACIONES

- Teniendo en cuenta el avance de la tecnología que se visualiza en estos tiempos modernos es correcto que las empresas e instituciones apliquen métodos y técnicas que permitan mantener segura la información que poseen, para ellos deben incluir herramientas de análisis como también aplicar pruebas dinámicas para identificar vulnerabilidades a las que están expuestas sus sitios web.
- Es necesario tomar medidas de seguridad si bien las amenazas continúan evolucionando, las organizaciones deberían de organizar su enfoque de prueba. Todo esto pueden llegar a lograrlos principalmente teniendo conocimiento de las metodologías, herramientas, tecnologías y las posibilidades de llegar a sufrir de algún ataque de su información sensible.
- En las diferentes metodologías siempre se tiene que ser cauteloso en cumplir con lo que se haya especificado en el alcance, ya que esto le puede traer problemas con la empresa a la cual esta realizando alguna prueba de penetración y esto pueda llevarle a problemas legales con la misma.
- Se recomienda que para realizar pentesting usar las metodologías recomendadas y que se ajuste a lo que desee realizar, también lo más recomendable es utilizar los sistemas operativos Parrot Security OS y Kali Linux, ya que estos cuentan con una suite completa de herramientas preinstaladas para que pueda hacer las pruebas pertinentes.
- Gracias a los resultados obtenidos en el análisis comparativo de las metodologías la más recomendable usar para pruebas de penetración en aplicaciones web es OWASP.

REFERENCIAS BIBLIOGRÁFICAS

[1] S. Gupta y B. B. Gupta, «CSSXC: Context-sensitive Sanitization Framework for Web Applications against XSS Vulnerabilities in Cloud Environments», *Procedia Comput. Sci.*, vol. 85, pp. 198-205, ene. 2016, doi: 10.1016/j.procs.2016.05.211.

[2] D. Kaur y P. Kaur, «Empirical Analysis of Web Attacks», *Procedia Comput. Sci.*, vol. 78, pp. 298-306, 2016, doi: 10.1016/j.procs.2016.02.057.

[3] D. Shugrue, «Fighting application threats with cloud-based WAFs», *Netw. Secur.*, vol. 2017, n.º 6, Art. n.º 6, jun. 2017, doi: 10.1016/S1353-4858(17)30059-4.

[4] «Total number of Websites - Internet Live Stats», 18 de enero de 2022. https://www.internetlivestats.com/total-number-of-websites/ (accedido 18 de enero de 2022).

[5] Clusit, «Rapporto Clusit», *Clusit*, 19 de enero de 2022. https://clusit.it/rapporto-clusit/ (accedido 19 de enero de 2022).

[6] I. Muscat, «Web vulnerabilities: identifying patterns and remedies», *Netw. Secur.*, vol. 2016, n.º 2, Art. n.º 2, feb. 2016, doi: 10.1016/S1353-4858(16)30016-2.

[7] R. O. Andrade, I. Ortiz-Garcés, y M. Cazares, «Cybersecurity Attacks on Smart Home During Covid-19 Pandemic», en *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, jul. 2020, pp. 398-404. doi: 10.1109/WorldS450073.2020.9210363.

[8] A. BÎZGĂ, «Mysterious cyberattack cripples Czech hospital amid COVID-19 outbreak», *Hot for Security*, 8 de septiembre de 2021. https://www.bitdefender.com/blog/hotforsecurity/mysterious-cyberattack-cripples-czech-hospital-amid-covid-19-outbreak/ (accedido 7 de septiembre de 2021).

[9] R. Garcia Cano y A. Morisson, «Massachusetts schools, churches have been targeted by hackers on Zoom», *Boston*, 7 de abril de 2020. https://www.boston.com/news/local-news/2020/04/07/massachusetts-schools-churches-zoom-hackers/

[10] «Análisis de vulnerabilidad: el estándar de ejecución de pruebas de penetración», 10 de enero de 2022. http://www.pentest-standard.org/index.php/Vulnerability_Analysis#Testing (accedido 10 de enero de 2022).

[11] «El hacking ético y su importancia para las empresas • ENTER.CO», *ENTER.CO*, 28 de febrero de 2014. https://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/ (accedido 17 de febrero de 2022).

[12] W. V. Velasco, «POLITICAS Y SEGURIDAD DE LA INFORMACION», p. 7.

[13] P. González Pérez, G. Sánchez Garcés, y J. M. Soriano de la cámara, *Pentesting con Kali 2.0*, Móstoles: 0xWORD. Computing S.L, 2015.

[14] «PTEST - High Level Organization of the Standard», 6 de diciembre de 2021. http://www.pentest-standard.org/index.php/Main_Page (accedido 6 de diciembre de 2021).

[15] D. Pandya y P. Nguyen Jaen, «OWASP TOP 10 VULNERABILITY ANALYSES IN GOVERNMENT WEBSITES», *International Journal of Enterprise Computing and Business Systems*, vol. 6, n.º 1, 2016.

[16] B. B. Gupta, «XSS-SAFE: A Server-Side Approach to Detect and Mitigate Cross-Site Scripting (XSS) Attacks in JavaScript Code», *Arab. J. Sci. Eng.*, vol. 41, n.º 3, Art. n.º 3, mar. 2016, doi: 10.1007/s13369-015-1891-7.

[17] S. Prandl, M. Lazarescu, y D.-S. Pham, «A Study of Web Application Firewall Solutions», en *Information Systems Security*, Cham, 2015, pp. 501-510. doi: 10.1007/978-3-319-26961-0_29.

[18] L. Johnson, «System and network assessments», en *Security Controls Evaluation, Testing, and Assessment Handbook*, Elsevier, 2020, pp. 447-469. doi: 10.1016/B978-0-12-818427-1.00010-0.

[19] Y. Li, J. Huang, A. Ikusan, M. Mitchell, J. Zhang, y R. Dai, «ShellBreaker: Automatically detecting PHP-based malicious web shells», *Comput. Secur.*, vol. 87, p. 101595, nov. 2019, doi: 10.1016/j.cose.2019.101595.

[20] K. A. Scarfone, M. P. Souppaya, A. Cody, y A. D. Orebaugh, «Technical guide to information security testing and assessment.», National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-115, 2008. doi: 10.6028/NIST.SP.800-115.

[21] C. C. Urcuqui, M. G. Peña, J. L. Osorio Quintero, y A. Navarro Cadavid, «Antidefacement - State of art», *Sist. Telemática*, vol. 14, n.º 39, Art. n.º 39, dic. 2016, doi: 10.18046/syt.v14i39.2341.

[22] «Descargar VMware Workstation Pro», *VMware*, 7 de enero de 2022. https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html (accedido 6 de enero de 2022).

[23] «OWASP Top Ten Web Application Security Risks | OWASP», 6 de diciembre de 2021. https://owasp.org/www-project-top-ten/ (accedido 6 de diciembre de 2021).

[24] «The Penetration Testing Execution Standard», 6 de diciembre de 2021. http://www.pentest-standard.org/index.php/Main_Page (accedido 6 de diciembre de 2021).

[25] «WSTG - Latest | OWASP», 5 de diciembre de 2021. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/ (accedido 4 de diciembre de 2021).

[26] D. Pandya y D. N. J. Patel, «OWASP TOP 10 VULNERABILITY ANALYSES IN GOVERNMENT WEBSITES», vol. 6, n.º 1, Art. n.º 1, 2016.

[27] B. Rathore, «Information Systems Security Assessment Framework», p. 1264, 2005.

[28] J. Willis, J. Baron, R.-A. Lee, M. Gozza-Cohen, y A. Currie, «Scholarly Knowledge Development and Dissemination in an International Context: Approaches and Tools for Higher Education», *Comput. Sch.*, vol. 27, n.º 3-4, Art. n.º 3-4, dic. 2010, doi: 10.1080/07380569.2010.523883.

[29] B. Rathore, «Information Systems Security Assessment Framework», p. 1264, 2005.

[30] «OSSTMM.3.pdf». Accedido: 18 de febrero de 2022. [En línea]. Disponible en: https://www.isecom.org/OSSTMM.3.pdf