PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS



ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

TÍTULO:

"PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACIÓN EN AMBIENTES VIRTUALES"

LÍNEA DE INVESTIGACIÓN:

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR:

BURBANO ANGULO CAROLINA ALEXANDRA

ASESOR:

ING. EVELIN LORENA FLORES

FECHA:

ESMERALDAS, ABRIL 2019

TRIBUNAL DE GRADUACIÓN

Trabajo de tesis aprobado luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de Grado de la PUCESE previo a la obtención del título de INGENIERO DE SISTEMAS Y COMPUTACIÓN.

……..

Ing. Evelin Flores

Tutor de Tesis

……..……..

Mgt. Jaime Sayago

Lector 1

…….

Mgt. Kleber Posligua Flores

Lector 2

……..…….…….

Mgt. Xavier Quiñonez Ku

Director de la Escuela de Sistemas y Computación

……..

Mgt. Maritza Demera Mejía

Secretaria general PUCESE

Fecha:

AUTORÍA

Yo, CAROLINA ALEXANDRA BURBANO ANGULO portadora de la cédula de identidad No. 0803892017 declaro que los resultados obtenidos en la investigación que presento como informe final son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

……..…….....

Carolina Alexandra Burbano Angulo

C.I. 080389201-7

CERTIFICACIÓN

Ing. Evelin Flores docente investigadora de la PUCESE, certifica que:

La investigación realizada por CAROLINA ALEXANDRA BURBANO ANGULO bajo el título "PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACIÓN EN AMBIENTES VIRTUALES" reúne los requisitos de calidad, originalidad y presentación, además de haber sido incorporadas al documento final, las sugerencias dadas; en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargada de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, marzo del 2019.

Ing. Evelin Flores

ASESORA

AGRADECIMIENTOS

A Dios por rodearme de personas maravillosas que han formado parte de mi vida y a lo largo de esta mi gran meta.

A mis padres por su paciencia, entrega y apoyo incondicional.

A mis hermanos, por todo su apoyo en el transcurso de mi vida.

A todos mis familiares y amigos que estuvieron pendientes y motivándome a no decaer, porque todo en la vida se puede lograr si te aferras a ese sueño.

Gracias totales, es una bendición tenerlos en mi vida.

DEDICATORIA

El presente trabajo de investigación está dedicado a Dios, a mis padres por el apoyo y compresión incondicionalmente durante el desarrollo de mi vida profesional. A mis hermanos y amigos que en cada momento me dieron su apoyo para continuar y salir adelante, gracias eternamente y a mi asesora que con sus conocimientos y aportes se pudo conseguir y finalizar este trabajo de investigación, los ama Lola.

Carolina Burbano

RESUMEN

La presente investigación se realizó con el objetivo de plantear una metodología que permita realizar pruebas de intrusión en ambientes virtuales, haciendo uso de estándares y herramientas que logren asegurar la confidencialidad, integridad y disponibilidad de la información. Durante el desarrollo exploratorio de la investigación, se recolectó información de la problemática mediante el análisis de las mejores prácticas de seguridad informática como es OWASP, OSSTMM, ISSAF, ISO/EC 27001, ISO/EC 27002, además de las herramientas de código libre para la realización de las pruebas de seguridad.

Aplicando la técnica de la observación mediante fichas de observación, se logró obtener resultados que permitieron identificar aquellas amenazas y vulnerabilidades que representan un riesgo considerable en la información del sistema analizado ponderándolas según la métrica de evaluación de vulnerabilidades Common Vulnerability Scoring System (CVSS), información de vital importancia para determinar el nivel de seguridad que incorpora el sistema.

La investigación concluye con la propuesta de una metodología, que contiene: las fases de desarrollo: Planificación, Descubrimiento, Evaluación, Intrusión, Pos-Explotación, Análisis y Reporte, así como también la descripción de herramientas que se utilizan en la ejecución de cada una de ellas y que permitieron identificar vulnerabilidades que fueron analizadas de acuerdo al top 10 OWASP.

Palabras Claves: pruebas de intrusión, seguridad, metodología, sistemas web

ABSTRACT

This research was carried out with the objective of proposing a methodology that allows intrusion tests in virtual environments, using standards and tools that ensure confidentiality, integrity and availability of information. During the exploratory development of the investigation, information of the problematic was collected by means of the analysis of the best practices of computer security as it is OWASP, OSSTMM, ISSAF, ISO/EC 27001, ISO/EC 27002, besides the tools of free code for the accomplishment of the security tests.

Applying the technique of observation by means of observation sheets, it was possible to obtain results that made it possible to identify those threats and vulnerabilities that represent a considerable risk in the information of the system analyzed, weighing them according to the Common Vulnerability Scoring System (CVSS), information of vital importance to determine the level of security that the system incorporates.

The investigation concludes with the proposal of a methodology that contains: the phases of development: Planning, Discovery, Evaluation, Intrusion, Post-Exploitation, Analysis and Report, as well as the description of tools that are used in the execution of each one of them and that allowed to identify vulnerabilities that were analyzed according to the top 10 OWASP.

Keywords: intrusion testing, security, methodology, web systems

ÍNDICE

TRIBUNAL DE GRADUACIÓN ii

AUTORÍA iii

CERTIFICACIÓN iv

AGRADECIMIENTOS v

DEDICATORIA vi

RESUMEN vii

ABSTRACT viii

ÍNDICE ix

ÍNDICE DE FIGURAS xi

ÍNDICE DE TABLA xii

Introducción 1

Presentación del tema de investigación 1

Planteamiento del problema 2

Justificación 3

Objetivos 4

CAPÍTULO I: MARCO TEÓRICO 5

1.1. Bases teóricas-científicas 5

1.1.1. La seguridad de la Información 5

1.1.2. Políticas de Seguridad 6

1.1.3. Mecanismos de Seguridad 8

1.1.4. Vulnerabilidad, Riesgo y Amenaza 8

1.1.5. Ethical Hacking 9

1.1.6. Pruebas de penetración o PenTest 9

1.1.7. Tipos de PenTest 10

1.1.8. Fases del PenTest 11

1.1.9. Metodologías para realizar Pruebas de Penetración 12

1.1.10. Herramientas para realizar Pruebas de Penetración 14

1.2. Antecedentes 17

1.3. Marco Legal 18

CAPÍTULO II: MATERIALES Y MÉTODOS 20

2.1. Tipo de estudio 20

2.2. Definición conceptual y operacionalización de las variables 20

2.3. Métodos 21

2.4. Técnicas y metodologías para realizar pruebas de intrusión 21

CAPÍTULO III: RESULTADOS 24

3.1. Análisis de las mejores prácticas de seguridad informática 24

3.2. Propuesta metodológica para realizar pruebas de intrusión en ambientes virtuales 26

Introducción 26

3.2.1. Planificación 27

3.2.2. Descubrimiento 28

3.2.3. Evaluación 28

3.2.4. Intrusión 31

3.2.5. Post Explotación 33

3.2.6. Reporte 35

3.2.7. Análisis y Validación de la Metodología 38

CAPÍTULO IV: DISCUSIÓN 41

CAPÍTULO V: CONCLUSIONES 42

CAPÍTULO VI: RECOMENDACIONES 42

Bibliografía 43

ÍNDICE DE FIGURAS

Figura 1 Los elementos de la Seguridad de la Información [1]. 5

Figura 2 Etapas del Ciclo de Deming [4]. 7

Figura 3 Tipos de perspectivas del Pent Test [12]. 10

Figura 4 Fases del Pentesting [13]. 11

Figura 5 Guía de Pruebas Metodología OWASP 23

Figura 6. Uso de la herramienta DIG 29

Figura 7. Escaneo de Puertos Nmap 30

Figura 8. Escaneo de Puertos UDP Zenmap 30

Figura 9. Escaneo de Puertos TCP Zenmap 31

Figura 10. Escaneo de puertos Unicornscan 2corintios v3 c4 31

Figura 11. Metasploit 32

Figura 12. Ejecución de Samba 32

Figura 13. Identificación del exploit 33

Figura 14. Acceso root exitoso 33

Figura 15. Unix-Privesc-check 34

Figura 16. Porcentaje de Vulnerabilidades Top 10 OWASP 35

Figura 17. Porcentaje de riesgo para un total de 3 vulnerabilidades identificadas 35

Figura 18. OWAS Top 10 Incorrecta Autentificación 39

Figura 19. OWAS Top 10 Exposición de datos sensibles 39

Figura 20. OWAS Top 10 Referencia Insegura a Objetos Directos 40

ÍNDICE DE TABLA

Tabla 1. Comparación de Metodologías de Pentesting [16] 13

Tabla 2. Comparación de herramientas para realizar pruebas de penetración [23]. 16

Tabla 3. Entornos de prueba 23

Tabla 4. Tipología basada en métricas..... 25

Tabla 5. Clasificación de herramientas en base a la normativa ISO 27000..... 26

Tabla 6. Métrica de evaluación de Vulnerabilidades CVSS [36]. 38

Introducción

Presentación del tema de investigación

Con el despliegue tecnológico de las redes y el internet se han logrado agilizar procesos de la vida diaria del ser humano, dando paso a la consumación de servicios web donde se involucra el uso de información. Lo que conlleva a que las empresas que brindan estos servicios busquen mecanismos que permitan minimizar los riesgos a los que están expuestos constantemente.

La presente investigación expone la importancia de la seguridad en el desarrollo de aplicaciones web y la forma de garantizar un activo primordial como es la información, a través de los principios de la seguridad de la información como es la confidencialidad, integridad y disponibilidad.

El Ethical hacking es realizado por hackers de sombrero blanco, por medio de un acto de intrusión o penetración y con previa autorización de la organización, logra encontrar y explotar debilidades. Aplica métodos y herramientas para descubrir esas vulnerabilidades que pongan en riesgo la información del sistema analizado.

El Éthical hacking tiene la finalidad de informar todas las vulnerabilidades encontradas durante el proceso, para prevenir y fortalecer la seguridad del servicio web y minimizar riegos cuando se presente un acceso no autorizado. Estas pruebas de penetración pueden ser aplicadas tanto para grandes y pequeñas organizaciones, todo dependerá de la necesidad requerida.

En el capítulo I, se presentan conceptos fundamentales de la seguridad de la información, pruebas de penetración, metodologías y herramientas que se utilizan para identificar vulnerabilidades en un sistema web y determinar qué tan seguro es el sistema. En el capítulo II, se presenta la metodología de la investigación, en el capítulo III se detallan los resultados obtenidos concluyendo con los capítulos IV y V correspondientes a conclusiones y recomendaciones.

Planteamiento del problema

Desde que los sistemas funcionan en la web afrontan problemas relacionados con la seguridad de la información debido a las amenazas a las que se enfrentan. Esto ocurre por la falta de aplicación de métodos y políticas de seguridad necesarias que ayuden a evitar posibles amenazas externas.

La seguridad de la información garantiza 3 conceptos principales que son: la integridad, confidencialidad y disponibilidad de la información, preparando a la empresa a la reducción de ataques frente a las posibles amenazas internas y externas, por ejemplo, cerrar el acceso a personas no autorizadas significa que cada trabajador tiene acceso únicamente a la información que le compete.

Cabe recalcar que ningún sistema web es cien por cien seguro, pero, aplicando métodos, herramientas y técnicas especializadas para realizar pruebas de penetración que cumpla con estándares internacionales se garantiza cierto nivel de seguridad y estabilidad del software.

La presente investigación tiene la finalidad de diseñar una propuesta metodológica que permita realizar pruebas de penetración a un sistema web mediante ambientes virtuales, para evaluar, analizar e identificar las debilidades que comprometen la seguridad de los datos. Por ello se plantea la siguiente interrogante: ¿Qué tan importante es realizar pruebas de penetración a sistemas web para asegurar la confidencialidad, integridad y disponibilidad de la información?

Justificación

Con el progreso y evolución de la tecnología, y el acceso a internet, ha cambiado la forma de comunicación y convivencia de los seres humanos, el hecho de poder realizar transacciones en línea, compartir y exhibir datos personales en la red, genera que personas no autorizadas quieran apropiarse de esta información. Estos cambios benefician al usuario, pero a su vez accionan nuevos riesgos, lo que induce a que las empresas e instituciones implementen métodos y políticas de seguridad que protejan la información.

En el desarrollo de software, las pruebas de seguridad y vulnerabilidad forman una parte fundamental para determinar la calidad, estabilidad, confidencialidad e integridad de la información del sistema. Existen organizaciones que establecen estándares internacionales, en las cuales se presentan distintas metodologías para implementar y llevar a cabo pruebas de seguridad enfocadas a evaluar y determinar los niveles de seguridad del software analizado.

Para llevar a cabo pruebas de penetración, se debe definir el entorno en que se va a desarrollar y las herramientas que le permitirán al tester (quien tiene conocimiento y realiza las pruebas de intrusión) optimizar recursos informáticos y económicos.

Por lo tanto, es de prioridad plantear una metodología que acompañe en el desarrollo de la prueba de penetración en un entorno virtual, para determinar, por medio de métricas de evaluación el nivel de seguridad de esta. Por ello, la metodología propuesta además de identificar las vulnerabilidades permitirá generar recomendaciones que serán útil a la organización en el tratamiento y mitigación de riesgo y a la toma de decisiones. Los principales beneficiarios serán aquellas empresas o instituciones que prestan servicios en la web para lograr proteger un activo primordial como es la información de los usuarios que lo utilizan.

Objetivos

General

- Diseñar una propuesta metodológica que permita identificar vulnerabilidades en un sistema web realizando pruebas de intrusión en ambientes virtuales.

Específico

- Analizar las mejores prácticas de seguridad informática para realizar pruebas de penetración en ambientes virtuales.
- Identificar puntos de vulnerabilidad para señalar el nivel de seguridad del sistema web analizado basado en estándares de seguridad informática.
- Describir las técnicas y herramientas utilizadas durante el desarrollo del pentesting.

CAPÍTULO I: MARCO TEÓRICO

1.1. Bases teóricas-científicas

1.1.1. La seguridad de la Información

La seguridad de la información digital depende de tres frentes: el físico, el social, y el lógico, por lo consiguiente las organizaciones deben integrar el ciclo de seguridad para que la información fluya dentro de procesos bien estructurados. Se debe de tener claro qué se entiende por seguro, Barinas, Alarcón y Callejas definen este término como mantener en secreto aquello que no se quiere revelar y que pueda caer en manos del enemigo o mantener estrategias para evitar el riesgo de vulneración; mientras que al hablar de seguridad de la información, se entiende como el proceso en el que se da cabida a un creciente número de elementos tanto en aspecto tecnológico, económico, telecomunicaciones y humanos [1] en la Figura 1 se detallan los elementos de la Seguridad de la información que se deben proteger.



Figura 1 *Los elementos de la Seguridad de la Información* [1].

La seguridad de la información también abarca a los principios de la información que son: Integridad, confidencialidad y disponibilidad. La Integridad hace referencia a la información que no ha sido modificada o alterada, es decir, permite garantizar que esta sea íntegra. La Confidencialidad tiene como propósito asegurar que solo a la

persona que le pertenece la información tenga acceso, y por último la Disponibilidad es la encargada de garantizar que la información llegue al usuario o destinatario en el momento oportuno y que esta información sea útil.

1.1.2. Políticas de Seguridad

Las políticas de seguridad se encargan exclusivamente de asegurar los derechos de acceso a los datos y recursos en base a herramientas y mecanismos de control. La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: este debe incluir copias de seguridad completa y copias de seguridad incrementales. Un buen sistema de respaldo debe contar con ciertas características indispensables: continuo, seguro, remoto y mantención de versiones anteriores de los datos [2].

Las organizaciones a nivel mundial han reconocido la importancia de un activo primordial como es la información y la tecnología que lo acompaña como un elemento diferenciador para lograr ventaja sobre sus competidores. Más de 6600 organizaciones de todo el mundo están implementando un Sistema de Gestión de Seguridad en base a la norma ISO/ IEC 27001 [3].

Considerando las políticas ecuatorianas, establecen las normativas técnicas ISO /IEC 27001:2013 y ISO /IEC 27002:2013 para implementar, operar, monitorear, revisar y mejorar la seguridad en los procesos y servicios de los sistemas de gestión de seguridad de la información (SGSI) de las organizaciones teniendo en cuenta los activos informáticos disponibles y las vulnerabilidades, amenazas y riesgos que puedan presentarse [4].

El sistema de gestión de seguridad de la información (SGSI), tiene como propósito principal identificar los activos tangibles e intangibles y recursos involucrados en los procesos y servicios que presta la organización a través de la gestión de riesgos, para verificar los controles de seguridad que permitan integrar políticas y procedimientos para aminorar los riesgos encontrados. Para la implementación exitosa de un SGSI, es necesario dar a conocer los aspectos y procedimientos de seguridad, la disposición

de las políticas y los mecanismos de medición, por medio del mapeo de las etapas del ciclo de Deming (PDCA).

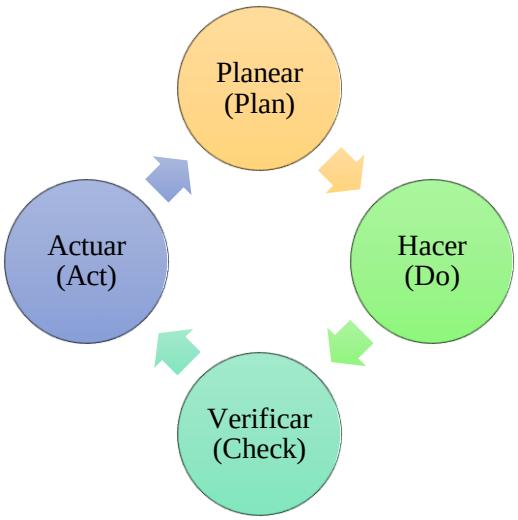


Figura 2 *Etapas del Ciclo de Deming* [4].

En la primera etapa del ciclo que es el plan, se realiza una planificación para establecer el alcance y límites, definir políticas y enfoque para la evaluación de riesgos y realizar un plan de tratamiento de los riesgos [5].

En la segunda etapa hacer, se implementan los controles, programas y procedimientos para gestionar recursos y operación del SGSI [5].

En la tercera etapa verificar, se da seguimiento y revisión de los controles aplicados, esta verificación se debe realizar periódicamente para que en un futuro los impactos que se generen no afecten en la eficiencia del SGSI [5].

En la última etapa actuar, se procede a recopilar lo aprendido y ponerlo en marcha, se pueden realizar observaciones y nuevas recomendaciones que posteriormente pasarán a la etapa inicial del ciclo, esta retroalimentación de resultados logrará acercar más a los objetivos del negocio [5].

1.1.3. Mecanismos de Seguridad

Los mecanismos de seguridad que se pueden implementar en un sistema web pueden ser:

a) Identificación y Autentificación, se identifican las entidades del sistema por medio de filtros para asegurar que el sujeto es quien dice ser.

b) Control de acceso, este establece los tipos de acceso que puede tener el sujeto en el sistema, no todos los sujetos pueden acceder a la misma información.

c) Separación, se establecen para separar objetos dependiendo de los niveles de seguridad que tenga el sistema.

d) Seguridad en las comunicaciones, se encargan de cifrar el tráfico que corre por la red, se utilizan protocolos como SSH, Kerberos, entre otros.

1.1.4. Vulnerabilidad, Riesgo y Amenaza

Las vulnerabilidades en los sistemas de información pueden traer graves problemas. Cada vez las redes están expuestas a virus informáticos, spam, código malicioso, hackers y crackers que penetran los sistemas de seguridad [6], por ello se deben diferenciar los términos amenaza, riesgo y vulnerabilidad.

Una amenaza está relacionada con la posibilidad de que un evento pueda presentarse en cualquier momento y puede provocar un daño sobre los activos informáticos, esta amenaza puede ser cometida por personas internas o externas a la institución, eventos naturales, entre otros [7].

El riesgo está ligado a los problemas presentados por amenazas y vulnerabilidades que pueden afectar potencialmente al negocio si no se tienen las medidas adecuadas [7].

La vulnerabilidad es la posibilidad de que se produzca una amenaza, esta vulnerabilidad puede ser de tipo física, natural, informática, humana, entre otras, provocando un impacto y daños susceptibles a los activos informáticos, infraestructura y sistema de información [7].

1.1.5. Ethical Hacking

En la comunidad informática se ha desarrollado la cultura Hacker, la misma que a través de los años se ha convertido en una sociedad más abierta, y es por ello por lo que existen diferentes tipos de Hackers o piratas informáticos. Están los Hacker de sombrero blanco, Hacker de sombrero gris y hacker de sombrero negro.

Hackers de sombrero blanco buscan, descubren e investigan agujeros de seguridad en el software. Cuando descubren una vulnerabilidad la notifican a la empresa o la hacen pública para que así el agujero pueda ser parcheado. Los hackers de sombrero negro buscan las fallas de seguridad del software y las aprovechan en su propio beneficio, roban datos confidenciales como: contraseñas, emails, números de tarjetas de créditos, entre otros, para después comercializarlas. Los hacker de sombrero gris, están en medio de: sombrero blanco y negro, si descubren fallas en el software y hurtan información pero para vender a los gobiernos, servicios de inteligencia, militares o policía [8].

A través del Ethical Hacking la organización puede evaluar los niveles de seguridad, así como comprobar y clasificar las vulnerabilidades, y por medio de un análisis de riesgo disminuir tiempo y esfuerzos para determinar el impacto que causarían las vulnerabilidades encontradas. El desarrollo de pruebas de penetración ayuda a la organización a tener un panorama de las vulnerabilidades encontradas y con la información recopilada se pueda llegar a establecer medidas preventivas y correctivas [9].

Se deben considerar aspectos importantes en el desarrollo de las pruebas de penetración como es el aspecto legal, este aspecto legal varía según las normas y estándares de cada país. Además, la organización debe de aportar con información verídica para que el resultado de la prueba concluya con datos reales y ayuden a la organización de manera eficaz en la toma de decisiones.

1.1.6. Pruebas de penetración o PenTest

El termino PenTest es como comúnmente se denomina a los "Test de penetración" o en inglés "Penetration Tests", es un procedimiento que se realiza a través de un conjunto de técnicas y métodos que simulan el ataque a un sistema, esto nos sirve para evaluar la seguridad de los sistemas informáticos, redes y aplicaciones [10].

Esta prueba puede realizarse a través de medios físicos utilizando hardware o mediante ingeniería social, existen herramientas de prueba de penetración que simplemente analizan un sistema, así como aquellas que realmente atacan el sistema para encontrar vulnerabilidades. Las pruebas de penetración permiten evaluar vulnerabilidades a través de la identificación de las debilidades, analizar y categorizar las debilidades explotables y prever recomendaciones en base a las prioridades de la organización, para reducir riesgos [11].

1.1.7. Tipos de PenTest

En la figura 3 se explican los tipos de perspectivas de los PenTest, que pueden variar según el enfoque u objetivo de la prueba.

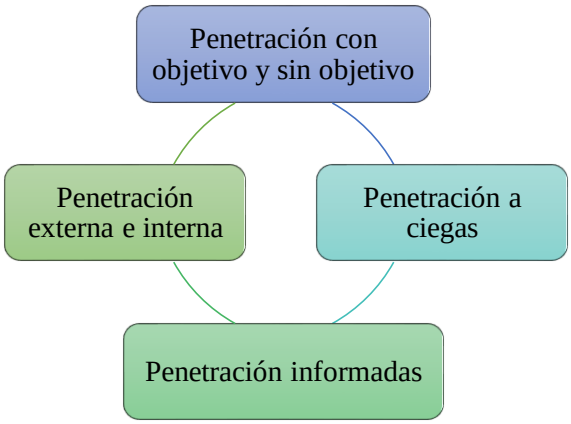


Figura 3 *Tipos de perspectivas del Pen Test* [12].

Las pruebas de penetración pueden buscar las vulnerabilidades en partes específicas o en la totalidad de los sistemas informáticos críticos de la organización. La información que se emplea la dispone la organización de forma pública y privada. El entorno de desarrollo de pruebas de penetración puede ser realizado desde lugares externos o dentro de las instalaciones de la organización con el fin de evaluar sus políticas y mecanismos de seguridad.

Las pruebas de intrusión pueden ser:

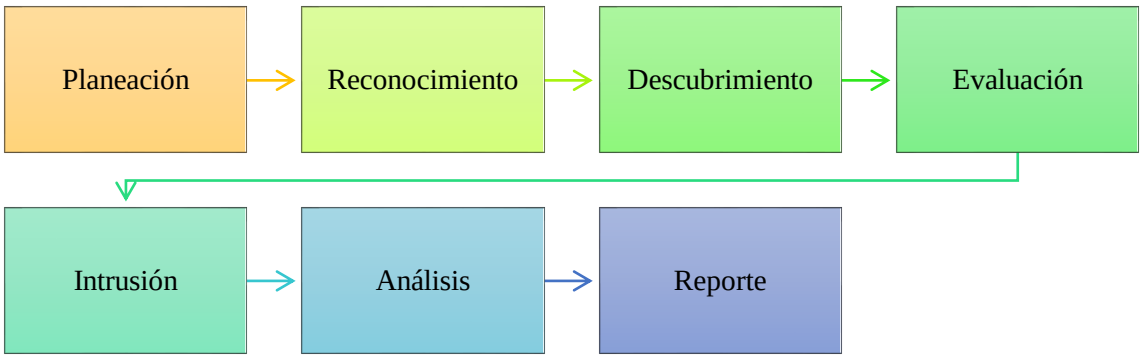
- Caja blanca: el pentester tiene conocimiento de toda la organización, conoce el funcionamiento del sistema, arquitectura de red, sistemas operativos, etc.

Este representa el mejor de los casos puesto que el atacante ya cuenta con información antes de acceder al sistema.

- Caja negra: el pentester no tiene conocimiento del sistema, suele contratarse una empresa externa para que realice el trabajo.
- Caja Gris: el pentester simula ser un empleado de la organización, se le da un usuario y clave de acceso a los sistemas con el objetivo de encontrar posibles problemas que pueden ser aprovechados por usuarios internos.

1.1.8. Fases del PenTest

En la figura 4 se describen las etapas o fases que incluye una prueba de penetración para su desarrollo.



- ***Figura 4*** *Fases del Pentesting* [13].

- Planeación: el pentester y el cliente definen las metas y objetivos de la prueba, de modo que ambas partes estén de acuerdo y comprendan que se desea obtener.
- Reconocimiento: se analiza de forma preliminar la información disponible, esta información debe ser proporcionada y tiene que ser clara y completa.
- Descubrimiento: se realiza la recolección de datos mediante herramientas de análisis, el pentester determinará lo siguiente: rangos de direcciones IP, dirección física de la empresa, datos personales de la empresa: números de teléfonos, nombres del personal y cuentas de correo electrónico y demás información que el pentester considere.

- Evaluación: esta se centra en el análisis de los datos encontrados en fases anteriores para determinar mediante herramientas de scanning los puntos de vulnerabilidad que afectan al sistema evaluado.
- Intrusión: el pentester en esta etapa utiliza el conocimiento adquirido en etapas anteriores para lograr acceder al sistema y obtener información de la misma.
- Análisis: evalúa las vulnerabilidades encontradas en etapas anteriores para determinar riesgos potenciales que afecten a la empresa.
- Reporte: se prepara un informe detallado con todos los procedimientos generales realizados en las pruebas, seguido del análisis de las vulnerabilidades y riesgos, y sugerencias de seguridad futura.

1.1.9. Metodologías para realizar Pruebas de Penetración

Para llevar a cabo pruebas de penetración se debe acompañar de una metodología que se acople a las necesidades de la organización, esta metodología debe emplear procedimientos y técnicas para alcanzar los objetivos deseados. A continuación, se describen metodologías utilizadas en pruebas de penetración:

OWASP: (Open Web Application Security Project) Es un proyecto de código abierto dedicado a identificar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es una organización sin fines de lucro que apoya y administra los proyectos e infraestructura de OWASP. Su enfoque es más para pruebas de penetración de caja negra, se compone de: Fase pasiva: en esta el tester entiende la lógica del sistema evaluado. Fase activa: el tester prueba todas las herramientas recomendadas por la metodología [14].

ISSAF ((Information Systems Security Assessment Framework) Los Sistemas de Información del Marco de Evaluación de Seguridad son una metodología estructurada para el análisis de seguridad en múltiples dominios y detalles específicos de la prueba o de las pruebas para cada uno de ellos. Su objetivo es proporcionar procedimientos muy detallados para la comprobación de sistemas de información que reflejen situaciones reales [14].

OSSTMM: Por sus siglas en inglés, Open Source Security Testing Methodology Manual, es un manual que combina ambición, estudio y años de experiencia de

profesionales en el área de la seguridad. Las pruebas individuales no son particularmente revolucionarios, pero la metodología en conjunto representa un estándar de referencia en el área de testeo de seguridad. Dicho manual es un estándar profesional para el testeo de seguridad en cualquier entorno, desde el exterior al interior. Como cualquier estándar profesional, incluye los lineamientos, la ética del Auditor de Seguridad, la legislación sobre el testeo de seguridad y un conjunto integral de test [15].

Tabla 1. Comparación de Metodologías de Pentesting [16]

ASPECTOS	ISSAF	OSSTMM	OWASP
Permite realizar pruebas y análisis de seguridad	Si	Si	Si
Establece requisitos previos para la evaluación	Si	No	Si
La metodología define un proceso detallado para la realización de pruebas	Si	Si	Si
Define áreas de alcance	Si	No	Si
Contiene plantillas para realizar las pruebas	Si	Si	Si
Detalla técnicas para cada prueba	Si	No	Si
Contiene ejemplos de pruebas y resultados	Si	No	Si
Recomienda herramientas para cada prueba	Si	No	Si
Presenta procesos de análisis y evaluación de riesgos	Si	Si	Si
Define dimensiones de seguridad a evaluar	No	Si	Si
Establece valores o niveles de evaluación de riesgos	Si	Si	Si
Enumera y clasifica las vulnerabilidades encontradas	Si	No	Si
Realiza estimación de impacto	Si	Si	Si
Genera reportes e informes	Si	No	Si
Presenta contramedidas y recomendaciones	Si	No	Si
Contiene referencias a documentación y enlaces externos	Si	No	Si

1.1.10.Herramientas para realizar Pruebas de Penetración

Wireshark: Es un analizador de protocolo de red que satisface los estándares de industrias e instituciones educativas de todo el mundo y, por lo tanto, es una opción preferible para la mayoría de los probadores de penetración para verificar la fortaleza de los sitios frente a ataques de seguridad. Admite cientos de protocolos y no es exclusivo de ningún sistema operativo en particular. La documentación adecuada sobre Wireshark está disponible, lo que ayuda a aprender rápidamente [17].

Nmap: Se usa para escanear en red. Puede encontrar dispositivos finales de redes conectadas, sus puertos abiertos, ejecutar servicios y puede construir un mapa de red. También se pueden encontrar versiones de sistemas operativos, servicios y demonios en ejecución. Esta información se puede usar en combinación con vulnerabilidades bien conocidas que se encuentran en bases de datos de acceso público [18].

Maltego: Es una herramienta de tipo OSINT (inteligencia de fuente abierta), que representa un grupo de herramientas que utilizan fuentes de información disponibles públicamente. La herramienta usa listas de índices y bases de datos para buscar información relevante [18].

Metasploit Framework: Es un proyecto de código abierto que proporciona la infraestructura, el contenido y las herramientas para realizar pruebas de penetración y una amplia auditoría de seguridad. Consta de múltiples componentes que trabajan en conjunto para proporcionarle una herramienta completa de prueba de penetración [19].

Nexpose: Es una solución de gestión de vulnerabilidades que combina la evaluación de vulnerabilidades y controles, la validación de vulnerabilidades y la planificación de remediación [20].

OpenVAS: Es un marco que contiene varios servicios y herramientas forjadas de Nessus, funciona en Linux y Microsoft Windows. Utiliza varios escáneres para descubrir vulnerabilidades en servidores desde una máquina cliente [21].

Acunetix: Es una herramienta comercial especializada en auditar aplicaciones web en busca de vulnerabilidades y fallos que puedan comprometer la integridad de la aplicación y la información que contiene. Ofrece una gran cantidad de características que permiten configurar la herramienta para que la precisión del análisis aumente y así, obtener resultados más fiables en su reporte [22].

Owas Zap: Es una herramienta gratuita de análisis dinámico de vulnerabilidades. Forma parte del grupo de proyectos de la fundación OWASP y es ampliamente utilizado alrededor del mundo. Ofrece gran cantidad de documentación y soporte además permite realizar distintos tipos de análisis y ataques, permitiendo configurar perfiles específicos para ajustarlos a las características de las aplicaciones [22].

Tabla 2. Comparación de herramientas para realizar pruebas de penetración [23].

ASPECTOS	WIRESHARK	KALI LINUX	NMAP	MALTEGO	METASPLOIT	NEXPOSE	OPENVAS	OWAS ZAP	ACUNETIX	NESUS
Facilidad de uso	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Media	Alta	Alta
Requerimientos del sistema	Medio	Medio	Medio	Medio	Alta	Alta	Medio	Media	Media	Medio
Facilidad de instalación	Medio	Medio	Baja	Medio	Compleja	Compleja	Medio	Media	Media	Medio
Interfaz amigable	Alta	Alta	Alta	Alta	Alta	Alto	Alto	Alta	Alta	Alto
Complejidad	Medio	Alta	Alta	Medio	Alta	Alto	Alto	Media	Media	Alto
Legibilidad del reporte final	Alta	Alta	Medio	Medio	Alta	Alta	Alta	Alta	Alta	Alta
Contenido de detección	Alta	Alta	Medio	Medio	Alta	Alta	Medio	Alta	Alta	Medio
Velocidad de detección	Medio	Media	Medio	Baja	Alta	Baja	Medio	Alta	Alta	Medio

1.2. Antecedentes

Los cambios y evolución de la tecnología en los últimos años han generado un progreso en la sociedad, el hecho de poder realizar transacciones en línea, implica que el usuario comparta información personal en la red [24]. Este cambio también incita a que personas no autorizadas quieran apropiarse de esta información, generando ataques informáticos a estos servicios web. Con ello las empresas enfrentan el reto de desarrollar e implementar políticas y normas de seguridad en el desarrollo de software desde sus inicios, para proteger, prevenir y salvaguardar la información.

Como lo menciona Ríos, Reyes, Morales, Sandoya y Miranda, la seguridad informática ha ganado popularidad y ha pasado de ser considerada un gasto, a ser vista como una inversión por parte de los directivos de las empresas y organizaciones a nivel mundial. Además, indican cómo la implementación de tecnologías de virtualización permiten llevar a cabo pruebas de seguridad logrando disminuir el riesgo a equipos y redes en producción, precautelando la información y servicios de las organizaciones [25].

Las páginas web podrían verse comprometidas con diferentes vulnerabilidades, las más representativas son: inyección de SQL, pérdida de autenticación y gestión de sesiones, referencia directa insegura a objetos, configuración de seguridad incorrecta, almacenamiento criptográfico inseguro, falsificación de peticiones en sitios cruzados (CSRF), protección insuficiente en la capa de transporte, entre otros[26].

Estos tipos de ataques de seguridad forjan a que las instituciones públicas y privadas, empresas y organizaciones efectúen mecanismos de seguridad mediante la práctica de tecnologías de virtualización para el desarrollo de pruebas logrando que se disminuyan riesgos y costos en equipos informáticos y redes.

Cabe recalcar que una solución con un cien por ciento de seguridad y efectividad es demasiado difícil de hallar; por lo tanto, la seguridad informática es una línea que requiere de un trabajo continuo a través de nuevas técnicas o herramientas para reducir los riesgos en un sistema [26].

Otra parte esencial en el desarrollo de pruebas de seguridad son los Ethical hacking, como lo afirma Caldwell, estos se han convertido de una parte esencial en la seguridad web, también llamados "sombreros blancos", para distinguirlos de sus malvados homólogos de sombrero negro, cumplen un papel más allá en las pruebas de penetración [27].

A medida que las amenazas cambian, las habilidades de los hackers éticos también cambian. John Stock, consultor de seguridad de Outpost24, dice que se deben hacer tres preguntas claves para garantizar que se realice una prueba efectiva. ¿Qué está tratando de proteger la empresa? ¿De qué está tratando la compañía de protegerse? ¿Y cuánto tiempo, esfuerzo y dinero está dispuesto a gastar la empresa para obtener una protección adecuada? Una vez que todo esto se decida, se debe determinar el método de prueba [27].

1.3. Marco Legal

El delito informático, es un acto ilícito, son acciones ilegales realizadas a través de conocimientos y tecnologías informáticas. En la constitución del Ecuador, el delito informático está tipificado en el artículo 190 del Código Orgánico Integral Penal, aprobado en el año 2014, de acuerdo a lo que se establece como delito “el uso de un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años” [28].

Considerando que la información es el bien más importante de las instituciones públicas y privadas, el Estado Ecuatoriano tomó la decisión de implementar el Esquema Gubernamental de Seguridad de la Información (EGSI), en todas las instituciones públicas, y con fecha 19 de septiembre de 2013, se emitió el Acuerdo Ministerial No. 166, publicado mediante Registro Oficial No. 88 del 25 de septiembre de 2013, en el cual dispone que las entidades de la Administración Pública Central,

Institucional y Dependiente de la Función Ejecutiva (APCID), procedan a su implementación, basado en la Norma Técnica Ecuatoriana INEN ISO/IE C 27002:2009 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información” [29P].

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1. Tipo de estudio

Este proyecto de investigación según los objetivos planteados está orientado a diseñar una propuesta metodológica que permita describir la seguridad informática e identificar las principales vulnerabilidades relacionadas a un sistema web, este estudio se basa en ejecutar pruebas de intrusión y en cada fase del desarrollo del mismo, encontrar los mecanismos necesarios que garanticen la seguridad de la información del sistema analizado logrando protegerlo ante posibles amenazas informáticas, y se considera un estudio mixto de tipo **exploratorio** y **descriptivo.**

2.2. Definición conceptual y operacionalización de las variables

Para el desarrollo de esta investigación se define un diseño exploratorio, puesto que, para llevar a cabo pruebas de penetración, es necesario aplicar las fases del pentesting para lograr determinar el nivel de seguridad del sistema que se analiza. Las fases por realizar son: planeación, descubrimiento, evaluación, intrusión, post explotación, análisis y reporte.

Variable	Definición	Definición operacional	Dimensiones	Indicadores
Nivel de Seguridad	Determina qué tan vulnerable es un sistema web	1. Fase pasiva • Planificación: definición de objetivos y alcance. • Descubrimiento: levantamiento de información. • Análisis: determinar riesgos potenciales. • Reporte: realizar un informe detallando las actividades realizadas. 2. Fase activa	Autentificación del sistema. Acceso a la base de datos. Modificación de información.	Por medio de una ficha de observación, se evaluarán los aspectos principales de la información que son: confidencialidad, integridad y disponibilidad que serán medidos en parámetros de: Alto, Medio, Bajo

		• Evaluación: escaneo de red • Intrusión: ataque al cliente • Post Explotación: limpiar evidencias		

2.3. Métodos

En el siguiente proyecto de investigación exploratorio-descriptivo se hizo uso de los métodos de investigación con enfoque inductivo-deductivo con el fin de fundamentar los procedimientos legales y lógicos mediante la aplicación de diferentes técnicas e instrumentos, para alcanzar una descripción más detallada de la realidad relacionada con la Seguridad Informática y Hacking Ético.

Método Inductivo: El estudio de los conceptos y herramientas para la detección y explotación de vulnerabilidades permitirán determinar el entorno de seguridad del sistema web e identificar amenazas que se conviertan en posibles ataques informáticos.

Método deductivo: Desde un estudio general a particular de las diferentes bases conceptuales, se parte de la situación general de seguridad del sistema web para determinar políticas de seguridad aplicables.

2.4. Técnicas y metodologías para realizar pruebas de intrusión

Para el desarrollo y manejo de datos de esta investigación se aplicó un análisis comparativo de las diferentes metodologías y herramientas para realizar pruebas de penetración, contemplando a OWASP (Proyecto Abierto de Seguridad de las Aplicaciones Web) como procedimiento de guía. Esta es una comunidad mundial libre y abierta enfocada en mejorar la seguridad de aplicaciones de software. Su misión es hacer la seguridad de las aplicaciones visible para que las personas y organizaciones puedan tomar decisiones acerca de los riesgos en la seguridad [30].

OWASP brinda información imparcial, práctica y rentable sobre seguridad en aplicaciones, produce materiales de una manera abierta y colaborativa. El resultado de este proyecto es un marco de pruebas completas. La guía de pruebas describe en detalles generales los tipos de pruebas y las técnicas necesarias para aplicarlas en la práctica [31].

Para determinar el nivel de seguridad del sistema web analizado se utilizará una ficha de observación (Anexo 1), durante la realización del pentesting, para registrar y controlar por medio de indicadores los aspectos principales de la seguridad de la información como son: confidencialidad, integridad y disponibilidad.

Para el procesamiento y análisis de los datos obtenidos en el desarrollo de cada fase de las pruebas de penetración de las vulnerabilidades, se realizó un análisis con el Top 10 OWASP, que es un documento de concienciación para la seguridad de las aplicaciones web. Representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones web. Los miembros del proyecto incluyen una variedad de expertos en seguridad de todo el mundo que han compartido su experiencia para producir esta lista. Incitan a todas las empresas a que adopten este documento de sensibilización dentro de su organización y comiencen el proceso de garantizar que sus aplicaciones web minimicen estos riesgos [32].

La guía de pruebas contiene:

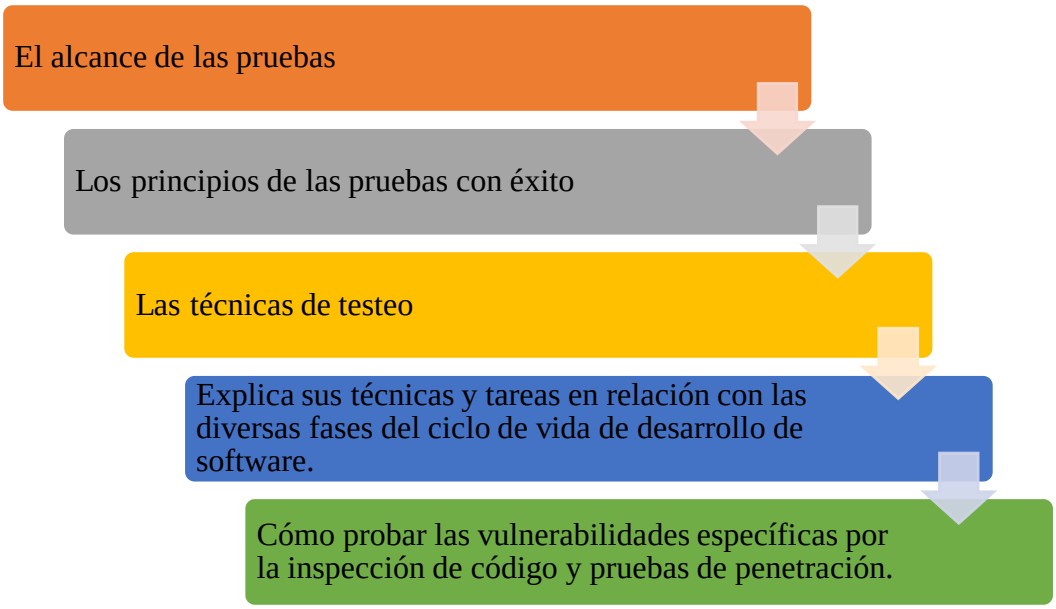


Figura 5 *Guía de Pruebas Metodología OWASP*

Entorno de prueba

Para el proceso de pruebas del proyecto se requiere de la disponibilidad de los siguientes entornos, a saber, en la tabla 3:

Tabla 3. *Entornos de prueba*

	Atacante	**Cliente**
SO	Kali Linux x64	Ubuntu 16.x x64
Hardware	8GB Ram, Intel Core i7 2.7GH	1GB Ram, 1 CPU, (Virtual)
Software	Acunetix, Nmap, Zenmap OWASP ZAP, DIG Metasploit	Apache 2, MySQL

CAPÍTULO III: RESULTADOS

3.1. Análisis de las mejores prácticas de seguridad informática

Hoy, en el internet se puede encontrar información o recurso para realizar una prueba de intrusión, como son sitios web en donde se explican de muchas formas las fases, y algunas técnicas de cómo realizar un pen test, sin embargo, es necesario hacer uso de una guía formal que dicte las mejores prácticas para poder llevar a cabo pruebas de intrusión.

En el capítulo anterior ya se expusieron metodologías para realizar pruebas de intrusión como es OSSTMM, OWASP y ISAFF, en este caso se detalla PTES (Penetration Testing Execution Standard sus siglas en ingles), que consiste en siete secciones principales. Estas cubren todo lo relacionado con un test de intrusión, desde la comunicación inicial hasta la inteligencia de recolección y fases de modelado para poder obtener un mejor entendimiento de la organización que será testeada, a través de la investigación de vulnerabilidades, explotación y post explotación, donde la habilidad técnica de los auditores de seguridad juega un papel importante conjuntamente con el entendimiento y compromiso adquirido con la organización, y finalmente, la fase de informes, que captura el proceso completo, en una forma que tenga sentido para el cliente y provea lo más valioso del test [33].

Así como se pueden aplicar metodologías para realizar pruebas de intrusión también están los estándares o normas para llevarlos a cabo, uno de ellos es la ISO 27001 en donde indica que una prueba de intrusión es un componente esencial de cualquier Sistema de Gestión de Seguridad de la Información ISO 27001, desde las fases iniciales hasta las fases de mantenimiento y mejoramiento continuo. El objetivo de control ISO 27001 A12.6, Gestión de la Vulnerabilidad Técnica, indica: se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado [34].

Es importante como buenas prácticas de seguridad ejecutar las pruebas de intrusión mínimo una vez al año, o cuando se realicen actualizaciones o modificaciones en los sistemas informáticos, con esto la organización verificará que su sistema informático se encuentra seguro y que sus políticas de respuesta a incidentes sean las adecuadas.

Las vulnerabilidades y amenazas identificadas se convertirán en información de punto de partida para una evaluación de riesgo, por ello una vez que son evidenciadas las vulnerabilidades aplicando las diferentes herramientas y técnicas, es necesario clasificarlas y cuantificarlas, para esto el Forum of Incident Response and Security Teams (FIRST), plantea un modelo tipológico basado en métricas cualitativas, temporales y de entorno según se indica en la tabla 4 [35].

Tabla 4. Tipología basada en métricas

GRUPOS	MÉTRICAS	TIPOS
Métricas base	Complejidad de acceso	Baja
Métricas base	Autenticación	Simple
Métricas base	Impacto de la confidencialidad	Alta
Métricas base	Impacto de la Integridad	Alta
Métricas base	Impacto en la Disponibilidad	Alta
Métricas del entorno	Requisitos de Seguridad	Baja

En la Tabla 5. la normativa ISO 27000 considerando los objetivos y actividades de control clasifica varias herramientas de análisis, esto permitirá determinar según los requerimientos de pen test qué herramienta se ajusta a la metodología propuesta.

Tabla 5. Clasificación de herramientas en base a la normativa ISO 27000

OBJETIVOS CONTROL	ACTIVIDADES CONTROL	HERRAMIENTAS
Garantizar la integridad de los sistemas	Instalación del software en sistemas en producción	GMF es un producto de software libre distribuido bajo licencia GPL e incluye módulos de gestión de incidencias (Trouble Ticketing), gestión de inventario, gestión del cambio (Change Management), SLA y reporting.
Evitar la explotación de vulnerabilidades	Restricciones en la instalación de software	Belarc: Belarc Advisor construye un perfil detallado del software y hardware instalado, el inventario de la red, la falta de revisiones en productos de Microsoft, el estado de antivirus, puntos de referencia de seguridad, y muestra los resultados en el explorador Web. Toda la información del perfil del PC se mantiene privada y no se envía a servidores de la web.
Minimizar el impacto de actividades	Controles de auditoría de los sistemas de información	SANS: SIFT Workstation es un Appliance de VMware preconfigurado con todas las herramientas necesarias para llevar a cabo un examen forense detallado digital.

3.2. Propuesta metodológica para realizar pruebas de intrusión en ambientes virtuales

Introducción

Una prueba de intrusión tiene como finalidad generar un informe técnico en el que expongan la identificación de amenazas y vulnerabilidades que generen un impacto de riesgo y la probabilidad de que este ocurra, así como también las medidas correspondientes para que la organización ponga en práctica y ayude a la toma de decisiones.

Existen metodologías que se pueden aplicar para realizar pruebas de intrusión, cada una ajustadas a las especificaciones de trabajo, por ello este trabajo de investigación proporciona una metodología que permite realizar pruebas de intrusión a sistemas web en ambientes virtuales. Las fases de ejecución son: Planificación, Descubrimiento, Evaluación, Intrusión, Post explotación y Reporte, detalladas a continuación.

3.2.1. Planificación

El principal objetivo de este trabajo es esbozar las fases de una prueba de penetración y proporcionar información actual y contrastada de las técnicas y herramientas utilizadas durante un pentest profesional y a qué fase pertenecen cada una de ellas, además, describir las técnicas y herramientas más utilizadas.

Otro de los objetivos es realizar una auditoría para comprobar que la metodología, técnicas y herramientas descritas son correctas, consiguiendo acceso a los tres equipos preparados virtualmente siguiendo en todo momento las fases anteriormente descritas.

Durante la exploración de las fases del pentest se ilustrará, sobre todo, herramientas gratuitas y de código abierto disponibles en la distribución S.O Linux.

Este trabajo no pretende de ningún modo ser una guía definitiva sobre pentest, solo pretende diseñar una metodología para realizar auditoría de seguridad o pentesting profesional.

Para empezar, es esencial establecer una línea de tiempos clara, definir fechas para el inicio que será el 15-09-2018 y finalización de la prueba el 19-11-2018 y también planificar en qué se invertirá exactamente el tiempo o el cronograma de actividades.

Es necesario establecer explícitamente qué rangos de direcciones IP están dentro del alcance de la prueba. Debería verificarse que el cliente posee todos los sistemas a auditar como el servidor DNS, el servidor de e-mail, el servidor en el que está alojada la página web o su sistema de firewall/IDS/IPS.

En este caso se pretende realizar la intrusión al sistema web de CROSOSFTSYSTEM, una pequeña empresa de desarrollo web Esmeraldeña, cuenta con un servidor con dirección IP 142.93.248.176, sin nombre de dominio.

3.2.2. Descubrimiento

En esta fase de la prueba de penetración se pretende obtener la máxima cantidad de información posible sobre el objetivo, para utilizarla en las fases posteriores, aquella información que sea útil para el auditor, como es dirección del sitio web, IP, teléfonos, correos, dirección, etc. Asimismo, debemos fijarnos en apartados como "Noticias" o "Anuncios" ya que las compañías suelen filtrar información de forma no intencionada. También es importante fijarnos en los puestos de trabajo técnico ofertados por la compañía.

- CrosoftSystem: es una empresa que busca convertirse en el socio tecnológico de sus clientes, incrementando su productividad y rentabilidad a través de la implementación de soluciones innovadoras. Realizan páginas web estáticas o dinámicas con la tecnología actual, generan contenido para páginas además de generar mayor tráfico en ellas. También ofrecen asesoramiento en funcionamiento, diseño y presentación de tu página web.
- Dirección IP del sitio web: 142.93.248.176
- Teléfonos: 098 212 2843
- correo electrónico: systemscrosoft@gmail.com
- Redes sociales: https://www.facebook.com/crosoftsystems/

3.2.3. Evaluación

En la fase de evaluación se destacan los barridos ping y el escaneo de puertos. El escaneo de puertos puede realizarse de varias maneras: la más básica es el escaneo TCP. Este consiste en realizar el three-way handshake en cada puerto especificado y luego cerrar la conexión. Si no especificamos ningún puerto, la herramienta realizará el escaneo de los mil puertos más comunes. Es recomendable escanear todos los puertos, ya que cambiar los puertos que utiliza un servicio es una medida de seguridad fácil de implementar por un administrador.

Otra forma de realizar el escaneo de puertos es el escaneo SYN, que es el que Nmap usa por defecto y es más rápido que el escaneo TCP, puesto que en lugar de completar el three-way handshake solo completa los dos primeros pasos del proceso. Además, proporciona un cierto grado de sigilo, ya que al no completar el handshake no suele quedar registrado en la máquina objetivo.

La recogida de información sobre los servicios web consiste en:

- Identificación del servidor web
- Identificación del Content Management System (CMS)
- Identificación de vulnerabilidades y plugins de los CMS

3.2.3.1 DNS

El servicio DNS proporciona información fundamental durante la fase de reconocimiento, gracias a la cual se podrá hacer un primer mapa de la infraestructura de red objetivo, con cadenas de texto, que son más sencillas de recordar.

En la figura 6. se ha empleado la herramienta DIG, la misma que es una herramienta muy flexible para interrogar a los servidores de DNS. Ejecuta búsquedas del DNS y muestra las respuestas devueltas de los nombres de los servidores que fueron requeridos.

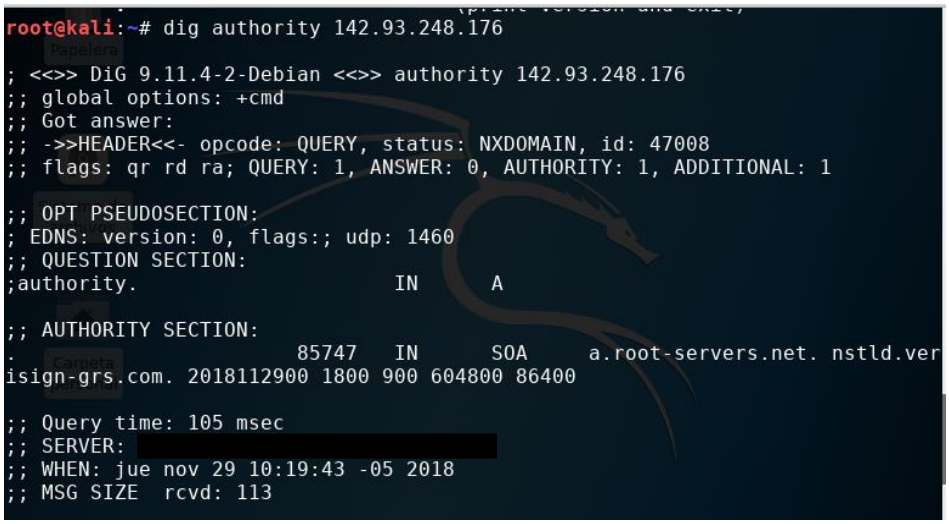


Figura 6. *Uso de la herramienta DIG*

3.2.3.2 Herramientas de escaneo de Puertos

Una de las herramientas que puede utilizarse es nmap, que es una herramienta muy poderosa para realizar escaneos de red. Su funcionalidad es bastante extensa y permite hacer muchos tipos de escaneos diferentes, e incluso ataques. Es una herramienta open source y está disponible para varias plataformas como Windows y Linux.

En la figura 7. Se muestran los puertos abiertos del servidor a explorar.

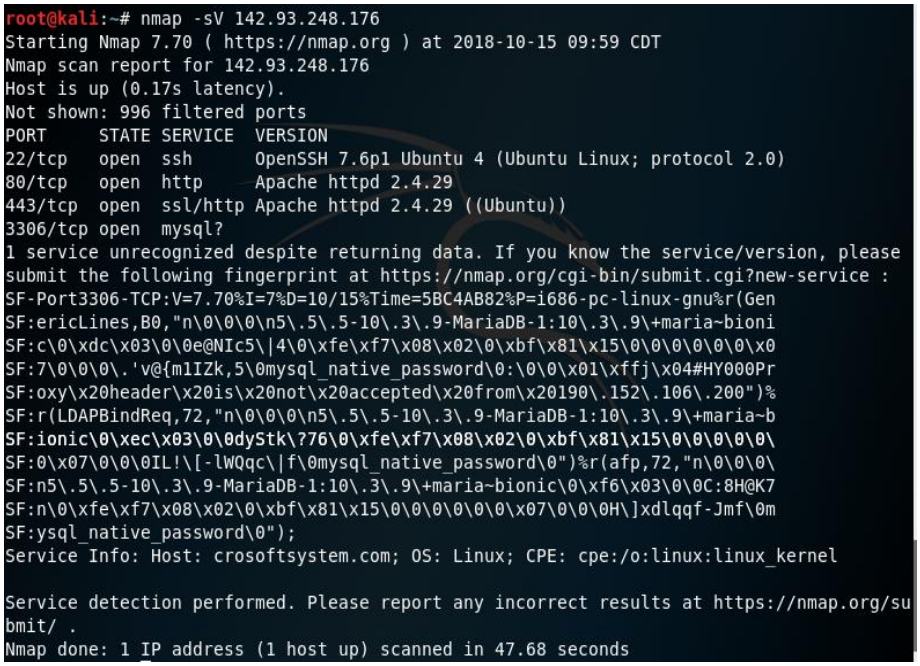


Figura 7. *Escaneo de Puertos Nmap*

En la figura 8 y 9 se muestra la herramienta zenmap para escaneo de puertos UDP y TCP de red. En la figura 10, se utiliza otra herramienta para el escaneo de puertos como es unicornscan.

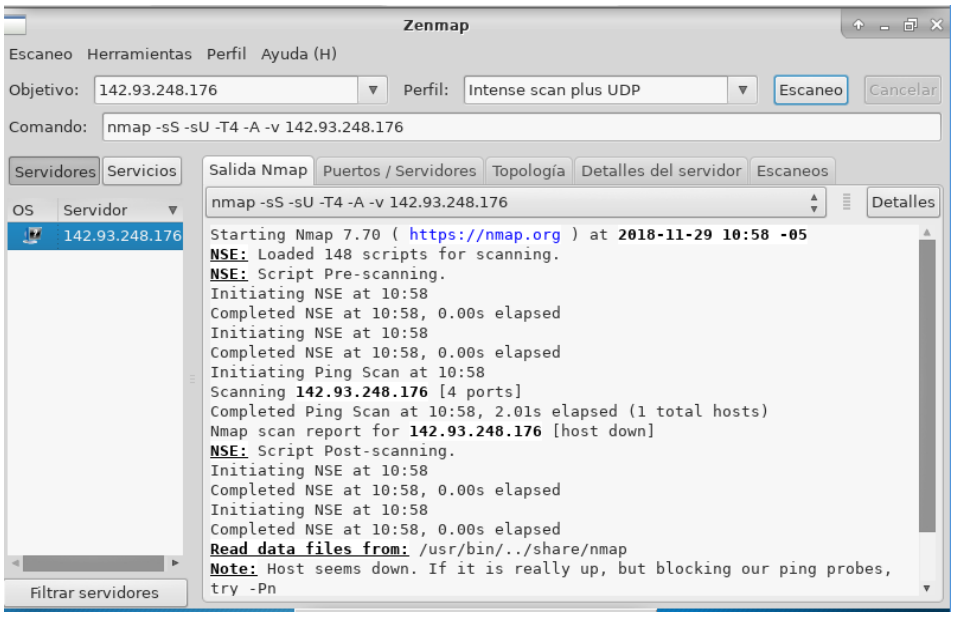


Figura 8. *Escaneo de Puertos UDP Zenmap*

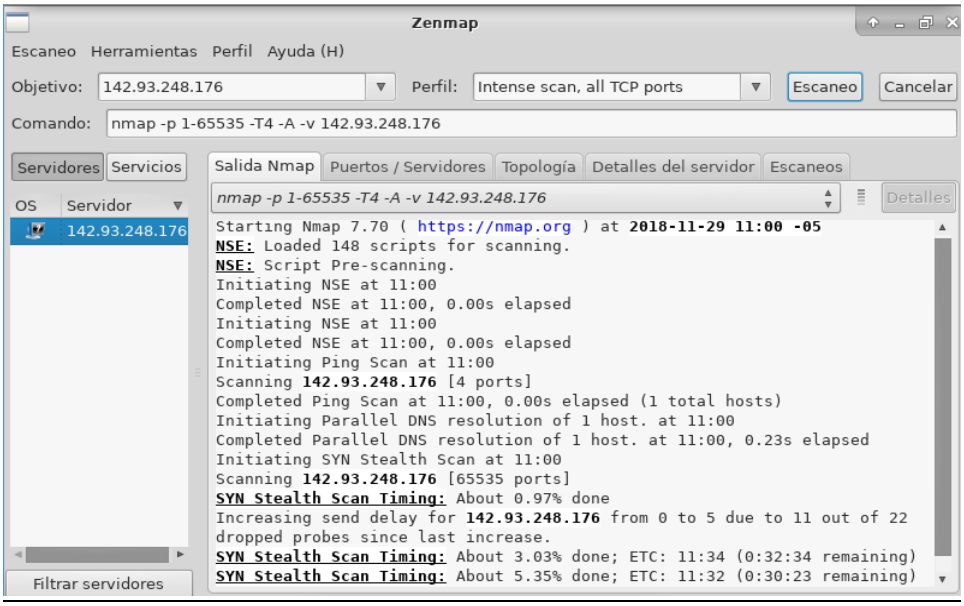


Figura 9. *Escaneo de Puertos TCP Zenmap*

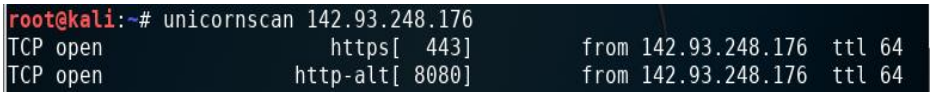


Figura 10*. Escaneo de puertos Unicornscan 2corintios v3 c4*

3.2.4. Intrusión

La fase de explotación se enfoca específicamente en obtener acceso al sistema objetivo traspasando las restricciones de seguridad. Si la fase anterior, de análisis y mapeo de vulnerabilidades se llevó a cabo de manera precisa y adecuada, la fase de explotación deberá resultar en una actividad bien planificada y con resultados certeros y satisfactorios, desde el punto de vista de un atacante.

El objetivo principal de esta fase es identificar la ruta de acceso principal en el sistema objetivo e identificar aquellos activos de mucho valor, desde el punto de vista de la información o accesos que pueden ser obtenidos como resultado de dicha explotación.

3.2.4.1. Metasploit Framework

Metasploit Framework (MSF) es la herramienta de explotación de facto en el mercado. Su núcleo desde su creación ha sido de código abierto, permitiendo que miles de hackers alrededor del mundo puedan contribuir con su desarrollo, desde documentación hasta desarrollo de nuevos módulos o exploits. En la figura 11 se inicia la configuración auxiliar de Metasploit framework. En la figura 12 con la dirección del host se inicia samba para identificar el script de explotación como se evidencia en la figura 13. Y en la figura 14. Se logra obtener acceso remoto del sitio explotado.

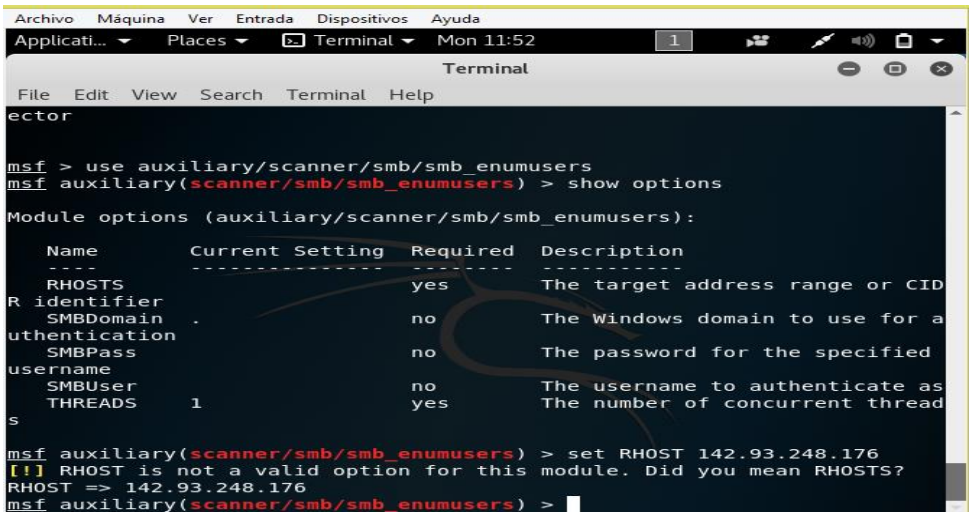


Figura 11. *Metasploit*

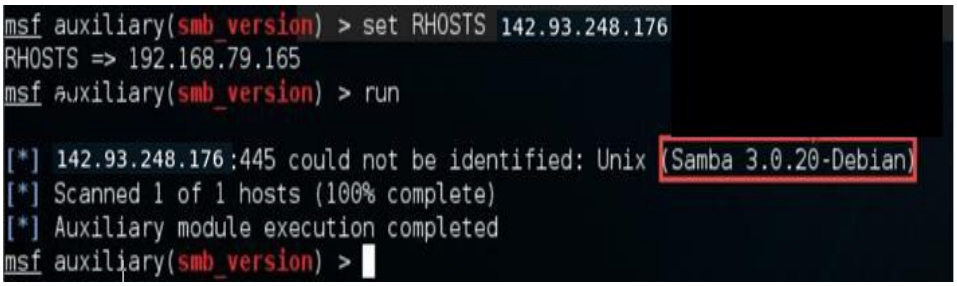


Figura 12. *Ejecución de Samba*

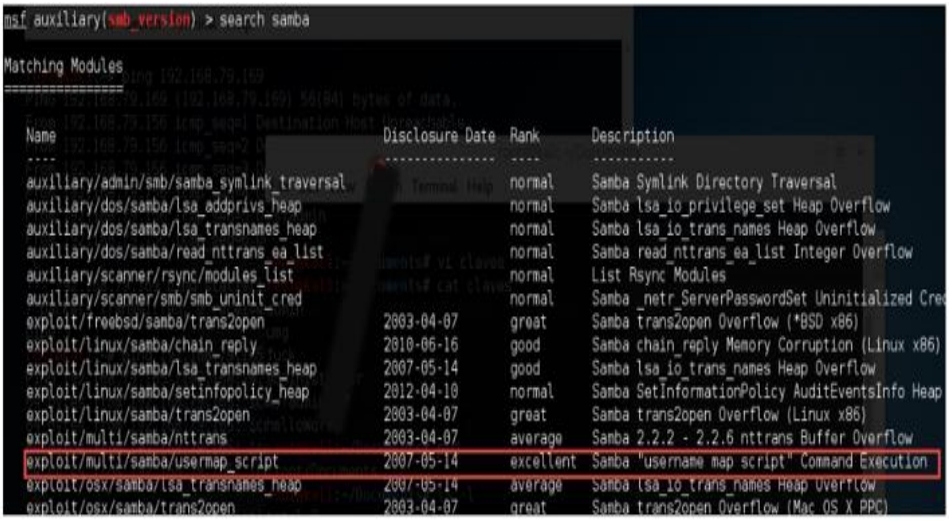


Figura 13. *Identificación del exploit*

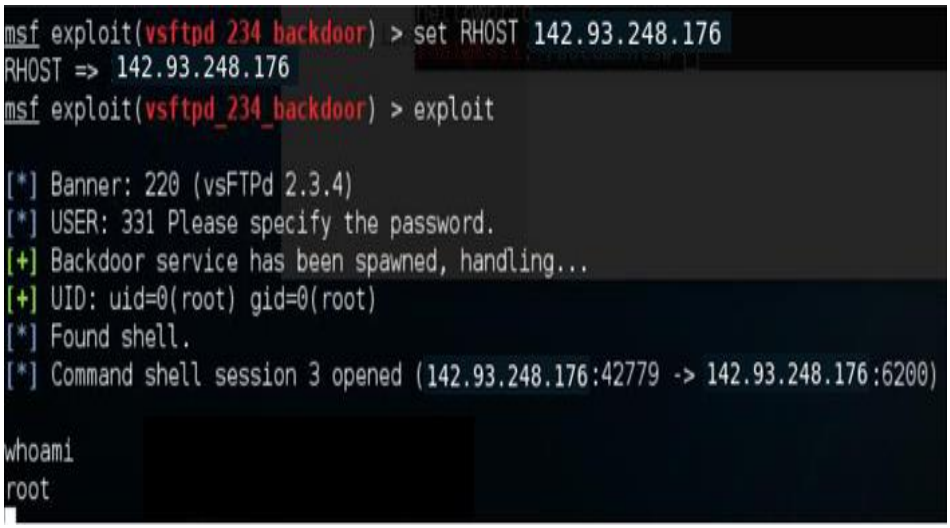


Figura 14. *Acceso root exitoso*

3.2.5. Post Explotación

El proceso de post explotación se lleva a cabo una vez que se ha ganado acceso al sistema objetivo. En esta fase se revisa la información obtenida en la fase de recolección de información de los sistemas que fueron vulnerados, el objetivo de la fase de post explotación es determinar el valor del dispositivo comprometido ante un ataque, y principalmente mantener el control y el acceso futuro. Es común ver en una prueba de intrusión, que esta fase no se lleve a cabo, ya que en muchas ocasiones los clientes no requieren de validar o confirmar métodos para mantener el acceso, sino más bien identificar vectores de ataque y materializar una

explotación específica con el objetivo de vulnerar sus dispositivos principales o extraer información.

En la figura 15 se emplea un script que se ejecuta en sistemas Unix para encontrar configuraciones erróneas que podrían permitir a los usuarios locales sin privilegios escalar privilegios a otros usuarios o acceder a aplicaciones locales.

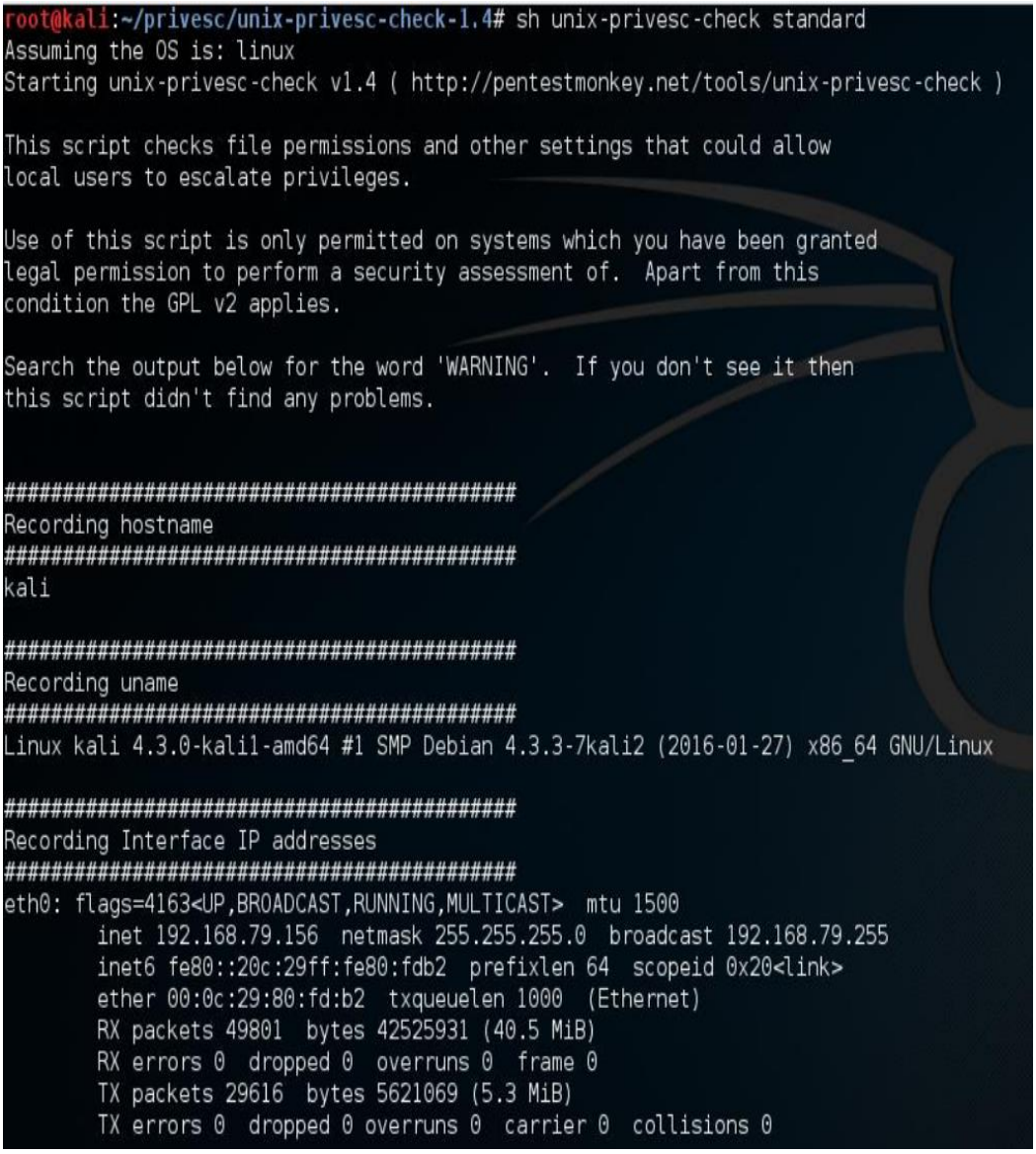


Figura 15. *Unix-Privesc-check*

3.2.6. Reporte

Esta sección provee una sinopsis general de los hallazgos identificados durante la ejecución de la prueba de Intrusión, en un formato estadístico básico. En esta sección se incluyen representaciones gráficas de los dispositivos testeados, resultados obtenidos, procedimientos, escenarios de ataque y algunas otras métricas consideradas e incluidas en la fase de Planificación.

En la figura 17. Se indica el porcentaje que representa la vulnerabilidad con respecto a la métrica de Vulnerabilidades CVSS

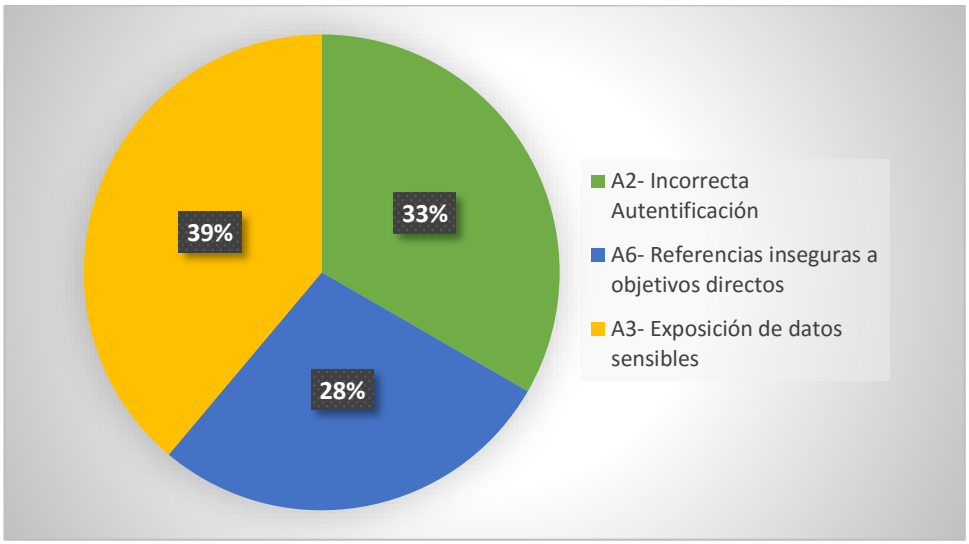


Figura 16. *Porcentaje de Vulnerabilidades Top 10 OWASP*

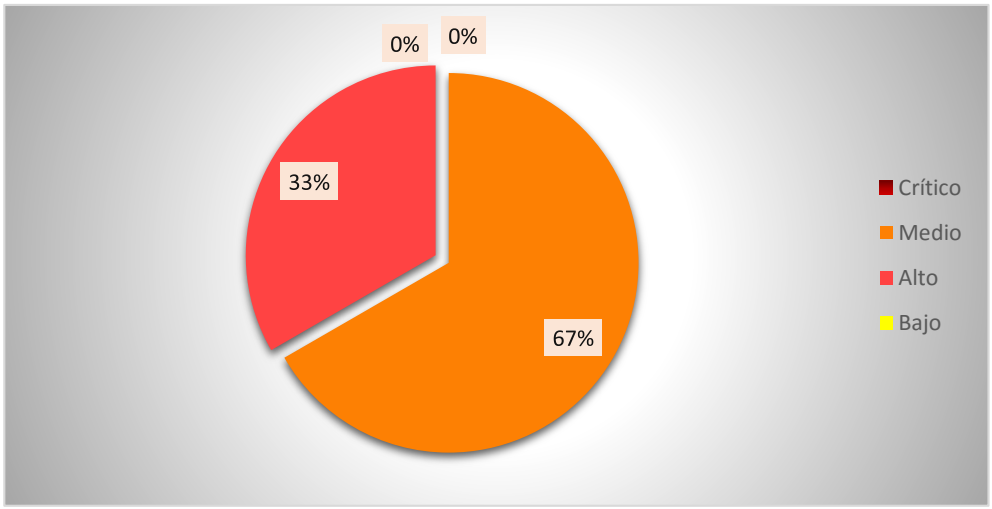


Figura 17. *Porcentaje de riesgo para un total de 3 vulnerabilidades identificadas*

Nª	01
HALLAZGO	Incorrecta Autentificación
NIVEL DE RIESGO	Medio
DESCRIPCIÓN DETALLADA	Se identificó que se está utilizando contraseñas de longitud pequeña, y esto permite que se puedan hacer peticiones y obtener respuestas válidas.
	Se recomienda realizar reglas generales de autentificación como la longitud mínima de 10 caracteres, al menos 1 mayúscula, una minúscula, un carácter especial y un dígito, como también métodos de encriptación.

Nª	02
HALLAZGO	Referencias inseguras a objetivos directos
NIVEL DE RIESGO	Medio
DESCRIPCIÓN DETALLADA	Se identificó que, en la aplicación el usuario tiene el permiso para acceder a un recurso específico, con esta información un atacante podría realizar fraude.
RECOMENDACIÓN DE MEJORA	Se recomienda hacer el uso de un índice o un mapa de referencias que eviten la manipulación de parámetros comprobando el acceso mediante comprobación de control de acceso.

Nª	**03**
HALLAZGO	Exposición de datos sensibles
NIVEL DE RIESGO	Alto
DESCRIPCIÓN DETALLADA	Se identificó que es posible extraer información de todos los usuarios del sistema sin requerir autenticación, esto incluye nombre, email, número de teléfono, entre otros.
RECOMENDACIÓN DE MEJORA	Se recomienda deshabilitar el almacenamiento en cache de datos sensibles, en caso de almacenar información sensible, asegurarse de cifrarlos.

La prueba de Intrusión que se realizó como primer punto se pudo observar que en la aplicación Web no se identificó una vulnerabilidad que permitiese tomar el control de algún servidor o escalamiento de privilegios, pero se encontraron múltiples fallas a nivel de lógica de negocio.

Se recomiendan capacitaciones regulares sobre metodologías y técnicas de desarrollo seguro. Se sugiere puedan tomar como referencia la documentación del proyecto OWASP, la cual incluye múltiples fuentes de recursos de libre acceso para fomentar las buenas prácticas de desarrollo seguro.

Se recomienda la ejecución de al menos una intrusión interna y externa anual, por parte de un profesional externo para validar las mitigaciones y asegurarse que se cumple con las mejores prácticas recomendadas, así como la identificación de nuevas vulnerabilidades. De esta forma lograr reducir el riesgo de fuga de información o intrusiones no autorizadas que resulten en activos comprometidos.

3.2.7. Análisis y Validación de la Metodología

Para cada hallazgo identificado es necesario asignarle una ponderación o escala de riesgo. Esta escala puede variar, pero es responsabilidad del Auditor de Seguridad comprender a cabalidad el entorno donde se realiza la prueba de intrusión, la lógica del negocio y en base a esto etiquetar cada hallazgo. Como referencia, es posible utilizar la calculadora de CVSS (Common Vulnerability Scoring System), que es la herramienta utilizada por todos los fabricantes o investigadores de seguridad, que descubren una vulnerabilidad de algún producto particular [36].

En la tabla 6 indica la correspondencia entre la puntuación CVSS y el valor cualitativo.

Tabla 6. Métrica de evaluación de Vulnerabilidades CVSS [36].

CRITICO 10	Este nivel es el más alto y crítico. Implica pérdidas financieras, legales y de imagen catastróficas.
ALTO 7-9	En este nivel, se encuentran los hallazgos ALTOS que podrían significar una potencial pérdida financiera, legal o de imagen.
MEDIO 4-6	En este nivel, se encuentran los hallazgos que podrían significar una potencial pérdida financiera o de imagen limitada.
BAJO 1-3	En este nivel, se encuentran los hallazgos que no representan ningún impacto negativo. Pueden considerarse como informativo o mejor práctica.

A continuación, se muestra un resumen de los principales hallazgos encontrados y se toma como base el OWASP Top 10:

- A2- Incorrecta Autentificación
- A3- Exposición de datos sensibles
- A6- Referencias inseguras a objetivos directos

A2- Incorrecta Autentificación

En la figura 18 se muestran las funciones de la aplicación relacionadas a la autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente referencia al top 10 OWASP, permitiendo a los atacantes comprometer contraseñas, claves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.

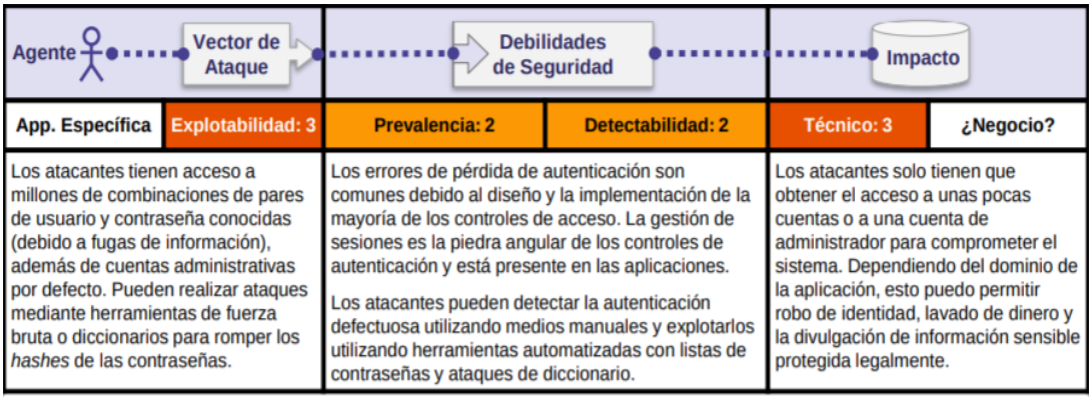


Figura 18. OWAS Top 10 Incorrecta Autentificación

A3- Exposición de datos sensibles

Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito o credenciales de autenticación. Los atacantes pueden robar o modificar tales datos para llevar a cabo fraudes, robos de identidad u otros delitos. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador como lo indica la figura 19.

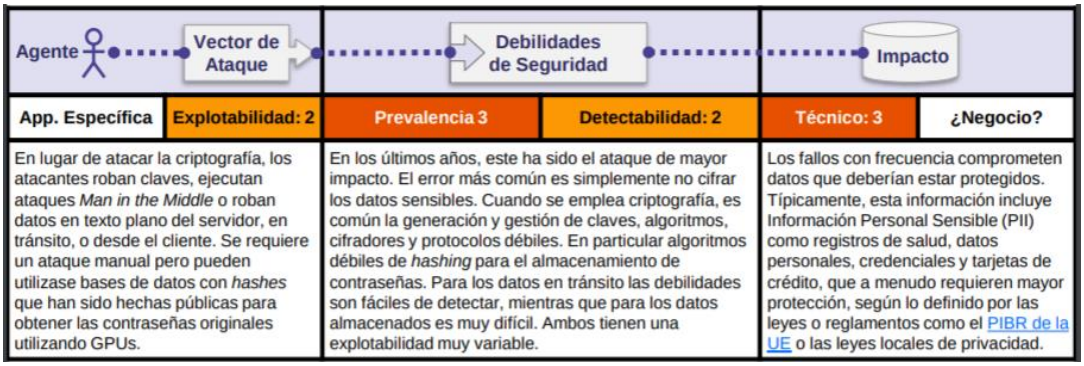


***Figura 19**. OWAS Top 10 Exposición de datos sensibles*

A6- Referencias inseguras a objetivos directos

Una referencia insegura a objetos directos ocurre cuando un programador expone una referencia hacia un objeto interno de la aplicación, tales como un fichero, directorio, registro de base de datos, o una clave tal como una URL o un parámetro de formulario web. Un atacante podría manipular este tipo de referencias en la aplicación para acceder a otros objetos sin autorización. En la figura 20 se indica cómo actúa la vulnerabilidad A6 en el sistema web.

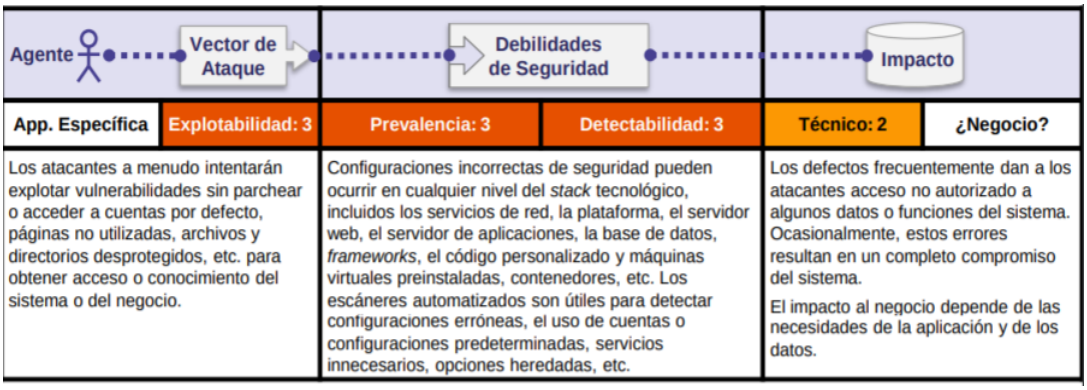


Figura 20. *OWAS Top 10 Referencia Insegura a Objetos Directos*

Una vez acabada la prueba de intrusión se puede comprobar que con las herramientas y técnicas de la propuesta metodológica se pudo evaluar, analizar e identificar amenazas y vulnerabilidades que comprometen la seguridad de los datos, permitiéndole a la organización situar el nivel de desempeño del sistema de información para la mitigación del riesgo y toma oportuna de decisiones.

Se lograron identificar un total de tres vulnerabilidades puntuados en un nivel medio para dos vulnerabilidades y alta para una vulnerabilidad según la escala CVSS, donde se puede situar el nivel medio de seguridad del sistema web con respecto a las métricas utilizadas de autentificación, confidencialidad e integridad y a la técnica y ficha de observación empleada durante el desarrollo exploratorio de la investigación.

CAPÍTULO IV: DISCUSIÓN

El avance tecnológico de las redes y el internet a logrado agilizar procesos de la vida diaria del ser humano, dando paso a la consumación de servicios web donde se implica el uso de datos personales. Lo que conlleva a que las empresas que brindan estos servicios busquen mecanismos que permitan minimizar los riesgos a los que están expuestos constantemente. Como lo indica ESET en su reporte de seguridad en Latinoamérica, se hace evidente que al menos tres de cada cinco empresas en la región sufrieron por lo menos un incidente de seguridad, estando en el top la infección con códigos maliciosos (45%). La mitad de ellos aparecen relacionados al ransomware, es decir, que al menos una de cada cinco empresas encuestadas en toda Latinoamérica fueron víctimas del secuestro de información siendo Ecuador el que tiene un mayor índice de infecciones de ransomware [37].

Por ello es de vital importancia que las empresas empleen en sus sistemas mecanismos y políticas de seguridad que permitan proteger un activo primordial como es la información. ESET en el apartado de control de seguridad indica que apenas un 58% de las empresas más pequeñas cuentan con una política de seguridad, en oposición a casi la totalidad de empresas grandes (78%) y Enterprise (84%) que sí cuentan con este tipo de controles. En el caso de las empresas medianas, tres cuartas partes de las encuestadas cuentan con políticas de seguridad [37].

En esta investigación se da a conocer cómo una pequeña empresa de desarrollo puede ser víctima de fraude o robo de información a su sistema web, acorde a los hallazgos encontrados durante la aplicación de la metodología propuesta. En el trabajo realizado por Palacios y Pérez se logran identificar vulnerabilidades y generar un reporte de hallazgo aplicando las fases del PenTest [16], lo que no le permite obtener a la organización una visión más clara sobre el impacto del riesgo de las vulnerabilidades con respecto a la organización, por ello la metodología propuesta en esta investigación además de identificar vulnerabilidades, en la fase de análisis permite ponderar el impacto del riesgo y emplear sugerencias que ayudan al tratamiento de riesgo y el proceso de mejoramiento continuo como lo indica la ISO 27001, que una prueba de intrusión es un componente esencial de cualquier Sistema de Gestión de Seguridad de la Información, desde las fases iniciales hasta las fases de mantenimiento y mejoramiento continuo. En donde la prueba de Intrusión contribuye significativamente, como parte del: Proceso de

Evaluación de Riesgos, Plan de Tratamiento de Riesgos y Procesos de Mejoramiento Continuo. Asegurando que los controles continúen funcionando como sean requeridos y que las nuevas amenazas y vulnerabilidades emergentes sean identificadas y sea posible lidiar con ellas [34].

CAPÍTULO V: CONCLUSIONES

Terminado el trabajo de investigación se puede concluir:

- Mediante el análisis de las mejores prácticas de seguridad informática y la adecuada utilización de técnicas y herramientas de intrusión fue posible diseñar una propuesta metodológica que permitiese ejecutar de manera satisfactoria una prueba de Intrusión en un ambiente virtual, en el cual se pudo incluir tecnologías de código abierto.
- Con la aplicación de la metodología propuesta a un sistema web se logró identificar vulnerabilidades que representan un impacto de riego medio a los activos de información de la organización.

CAPÍTULO VI: RECOMENDACIONES

- Capacitación al equipo técnico de la organización sobre las mejores prácticas de seguridad informática puesto que una prueba de intrusión además de proveer información sobre puntos débiles debe ser tomado como base para una línea de conocimiento por parte del equipo técnico de la organización.
- Se recomienda ejecutar una prueba de intrusión de manera periódica, al menos una vez por año, puesto que la identificación oportuna y manejo adecuado de vulnerabilidades permite la ejecución de acciones preventivas de forma proactiva y no reactiva ya que cada día pueden descubrirse nuevas vulnerabilidades y amenazas, o se implementan nuevas soluciones tecnológicas.
- Se recomienda documentar detalladamente la identificación de cada uno de los hallazgos y explotación donde sea posible proveer recomendaciones generales y oportunas sobre cómo puede mitigarse el riesgo asociado a cada uno de los activos vulnerados.

Bibliografía

[1] A. Barinas, A. Alarcon, and M. Callejas, "Vulnerabilidad de ambientes virtuales de aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus," *Ventana Informática*, vol. 30, Manizales, p. 247–26 0, Jul-2014.

[2] A. Orejuela, "Elaboración e implementación del manual de políticas y normas de seguridad informática para la empresa eléctrica regional norte s.a. EmelNorte," *repositorio UTN*, 2015. [Online]. Available: http://repositorio.utn.edu.ec/bitstream/123456789/3730/4/04 ISC 311 Artículo Científico.pdf. [Accessed: 30-May-2018].

[3] J. A. Monsalve Pulido, F. A. Aponte Novoa, and D. F. Chaves-Tamayo, "Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia)," *Facultad de Ingeniería*, vol. 23, no. 37, Universidad Pedagógica y Tecnológica de Colombia, Boyacá, pp. 65–72, Jun-2014.

[4] F. Solarte, E. Enriquez, and M. Benavides, "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001," *Rev. Tecnológica ESPOL – RTE*, vol. 28, no. 5, p. 492–507, 2015.

[5] R. J. Martelo, J. E. Madera, and A. D. Betín, "Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)," *Inf. tecnológica*, vol. 26, no. 2, pp. 129–134, 2015.

[6] C. Dussan, "Políticas de seguridad informática," *Entramado*, vol. 2, no. 1, pp. 86–92, 2006.

[7] G. García Pierrat and M. J. Vidal Ledo, "La informática y la seguridad. Un tema de importancia para el directivo. Informatics and security: an important topic for managers. Gonzalo," *Infodir (Revista de Información para la Dirección en Salud)*, vol. 12, no. 22, [s.n.], pp. 47–58, 08-Feb-2016.

[8] K. Zetter, "Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?," *Wired*, 2016. [Online]. Available: https://www.eldiario.es/tecnologia/hackers-llevan-sombrero-blanco-negro_0_505349668.html. [Accessed: 30-May-2018].

[9] S. Al-Sharif, F. Iqbal, T. Baker, and A. Khattack, "White-hat hacking framework for promoting security awareness," in *2016 8th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2016*, 2016.

[10] J. Luis and R. Ramos, "Pruebas de penetración o pent test."

[11] M. Denis, C. Zena, and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," in *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*, 2016.

[12] L. G. Carolina Pinzón -Mihdí Badí Talero M -John A Bohada, L. G. Carolina

Pinzón, M. M. Talero, and J. A. Bohada, “Pruebas de intrusión y metodologías abiertas.”

[13] T. Guarda, W. Orozco, M. F. Augusto, G. Morillo, S. A. Navarrete, and F. M. Pinto, “Penetration Testing on Virtual Environments,” in *Proceedings of the 4th International Conference on Information and Network Security - ICINS ’16*, 2016.

[14] R. López, “Pruebas de penetración en aplicaciones web usando hackeo ético,” *Rev. Tecnológica*, vol. 10, pp. 13–19, 2017.

[15] Y. Gavilánez Cruz, “METODOLOGÍA OSSTMM PARA LA DETECCIÓN DE ERRORES OPERATIVOS DE 64 BITS A NIVEL DE USUARIO FINAL,” ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO INSTITUTO DE POSGRADO Y EDUCACIÓN CONTINUA, 2016.

[16] A. J. Palacios Quispe and D. E. Pérez Vinueza, “Propuesta metodológica para realizar pruebas de penetración en ambientes virtuales,” Universidad de las Fuerzas Armadas ESPE, 2016.

[17] S. Sandhya, S. Purkayastha, E. Joshua, and A. Deep, “Assessment of website security by penetration testing using Wireshark,” in *2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017*, 2017.

[18] F. Holik and S. Neradova, “Vulnerabilities of modern web applications,” in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 2017, pp. 1256–1261.

[19] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, “Effective penetration testing with Metasploit framework and methodologies,” in *CINTI 2014 - 15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings*, 2014.

[20] A. L. Hernández Saucedo and J. Mejia Miranda, “Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web,” *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica*, vol. 1, Guadalajara, 2015.

[21] M. I. Abdullah, “TCP/IP Attacks, Defenses and Security Tools,” *Int. J. Sci. Mod. Eng.*, vol. 1, no. 10, pp. 42–47, 2013.

[22] E. Alejandro, A. Vega, F. Román Muñoz, L. Javier, and G. Villalba, “Herramientas de análisis dinámico de aplicaciones web con snort.”

[23] D. A. Franco, J. L. Perea, and L. C. Tovar, “Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios,” vol. 24, no. 5, pp. 13–22, 2013.

[24] P. Dip, “Tecnología e Informática: ÉTICA Y SEGURIDAD INFORMÁTICA,” *20/11/2008*, 2008. [Online]. Available:

http://latecnologiavirtual.blogspot.com/2008/11/tica-y-seguridad-informtica.html. [Accessed: 30-May-2018].

[25] N. R. Ríos Tirado, J. D. Reyes Ramos, L. E. Morales Álvarez, D. S. Sandoya Carreño, and M. Miranda Quintana, "Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas," *Rev. Publicando*, vol. 10, pp. 462–473, 2017.

[26] O. Mondragón, A. Mera, C. Urcuqui, and A. Navarro, "Security control for website defacement," *Sist. Telemática*, vol. 15, no. 1541, pp. 45–55, 2017.

[27] T. Caldwell, "Ethical hackers: Putting on the white hat," *Netw. Secur.*, 2011.

[28] J. Zambrano Mendieta, K. I. Dueñas Zambrano, and L. Macías Ordoñez, "Delito Informático Procedimiento Penal en Ecuador," *Rev. Cient. Dominio las Ciencias*, vol. 2, pp. 204–215, 2016.

[29] C. De la Torre and M. De la Torre, "Planteamientos básicos para la implementación de las normas ISO 27001," *scprogress*, 2017. [Online]. Available: http://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf. [Accessed: 30-May-2018].

[30] A. D. De León Velásquez, "Test de penetración 'pentesting' aplicado en entornos gnu/linux en una empresa Guatemalteca," Universidad Mariano Gálvez de Guatemala Facultad de Ingeniería en Sistemas de Información y Ciencias de la Computación, 2017.

[31] M. C. Castillo Jaramillo and C. J. Herrera Riofrío, "Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la editorial Don Bosco, mediante un test de intrusión de caja blanca," Universidad Politécnica Salesiana Sede Cuenca, 2015.

[32] OWASP, "OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks," *Owasp*, 2017. [Online]. Available: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf. [Accessed: 07-Jul-2018].

[33] E. Rodríguez, "PROCESO DE AUDITORÍA INTERNA Y ETHICAL HACKING," Colombia, 2016.

[34] R. C. Lema Vinlasaca and D. F. Donoso Gallo, "Implementación de un sistema de gestión de seguridad de información basado en la norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa Lockers S.A," ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS, 2018.

[35] A. F. Sánchez Sánchez and R. E. Rodríguez Rodríguez, "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," 2018.

[36] A. López, “Métricas de evaluación de vulnerabilidades: CVSS 3.0 | INCIBE-CERT,” *Instituto Nacional de Ciberseguridad de España*, 2015. [Online]. Available: https://www.incibe-cert.es/blog/cvss3-0. [Accessed: 10-Jan-2019].

[37] ESET, “Eset Security Report Latinoamérica 2018,” *we live security*, 2018. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf. [Accessed: 13-Jan-2019].

Anexos

Anexo 1. Ficha de Observación

FICHA DE OBSERVACIÓN

Fase:

Entorno Virtual:

Nombre del Sistema:

Fecha:

Aspectos que Observar		**Escala**		
		Impacto		
		Alta	Media	Baja
Integridad de Datos	Modificación			
	Validación			
	Destrucción			
Confidencialidad	Gestión de claves			
	Autentificación de Usuario			
Disponibilidad	Información Disponible			