PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

"DESARROLLO DE UNA GUÍA TÉCNICA ESTÁNDAR PARA APLICAR HERRAMIENTAS DE ETHICAL HACKING EN REDES DE DATOS, DIRIGIDO A PYMES"

AUTOR:

OSWALDO ALEJANDRO TAMAYO VEINTIMILLA

DIRECTOR:

Ing. ANDRÉS JIMENEZ

QUITO, JUNIO 2016

RESUMEN

El concepto de hacking apareció prácticamente en los años sesenta, que, en esa época, tenía otro significado, el de una persona preparada y que domina todas las ramas de la informática. Sin embargo, a partir de los años ochenta, se reportaron varios crímenes cibernéticos que, hicieron que el término hacker cambiara de bando y se lo relacionara con el crimen tecnológico.

A partir de los años 90, aparece una disciplina que trata de combatir el crimen cibernético, con sus mismas armas, el ethical hacking si bien, ataca las redes de datos de las organizaciones, previene de futuros ataques y fortalece a las empresas que contrataron los servicios de personas que dominan esta disciplina. Los ethical hackers como se los conoce son, entonces profesionales que actúan como delincuentes informáticos a favor de la protección de la información.

A partir de esa década, ambos bandos, tanto el criminal, como el preventivo se nutrieron de nuevas iniciativas. Es por ello que el ethical hacking ha crecido hasta en la actualidad situarse en un aliado para las empresas, y en este caso de las pequeñas y medianas, que al no tener un presupuesto alto como las grandes, quieren protegerse de alteración de su información y robo. Desde ese entonces, muchas metodologías se han desarrollado con diferente orientación, pero con el fin de cuidar los datos.

En la actualidad, es crucial protegerse ya que la información se ha convertido en un bien intangible de gran valor, y perderla o ver como se altera la misma, puede ser causa de inclusive ir a la banca rota.

En la presente disertación se tratarán temas como: que es un hacker sus valores y las diversas metodologías y herramientas usadas, hasta el reporte final al cliente.

DEDICATORIA

La presente disertación de grado, se la dedico enteramente a mamá y papá, son mi todo, el apoyo incondicional que todo hijo desearía y que afortunadamente lo tengo. Son mi ejemplo a seguir y los que están ahí en todo.

También va para mi segunda madre mi abuela que a pesar de que ya no está conmigo físicamente, sé que ha estado siempre desde que inicié la carrera.

AGRADECIMIENTOS

Quiero dar las gracias a mi pa y ma que son la razón por la cual puedo alcanzar mis objetivos trazados a lo largo de mi vida. Su apoyo es trascendental para mí. Además, agradecerles a mis amigos y compañeros de clase a lo largo de mi carrera, sin ellos la vida universitaria no hubiera sido la misma.

También, quiero agradecer a mi director de tesis, Andrés, gracias infinitas por las enseñanzas en esta etapa y en la carrera, a mis correctores por sus sugerencias y enseñanzas, y a mis profesores que a lo largo de la carrera impartieron su conocimiento.

Finalmente, y no menos importante por ello, agradezco a mi universidad la PUCE por todo lo logrado.

TABLA DE CONTENIDO

INTRODUCCIÓN 1

Antecedentes 1

Justificación 3

Objetivos 4

1.1.1. Objetivo General 4

1.1.2. Objetivos Específicos 4

Alcance 4

Metodología 4

MARCO TEÓRICO 5

2.1. Seguridad informática 5

2.1.1. Objetivos de la seguridad informática 5

2.1.2. Principales técnicas para evaluar vulnerabilidades 6

2.2. Ethical Hacking 8

2.2.1. Definición 8

2.2.2. Hacker 9

2.2.3. Tipos de Hacker 10

2.2.4. Clases de hacker ético 12

2.2.4.1. Hacker de sombrero negro reformado 12

2.2.4.2. Hacker de sombrero blanco 14

2.2.4.3. Consultorías 14

2.2.5. Ética del hacker 14
2.2.6. Valores de la ética del hacker 15
2.2.7. Modo de actuación de un hacker 15
2.2.8. Beneficios de Ethical Hacking 19
2.3. PYMES 19
2.3.1. Definición 19
2.3.2. Características 20
2.3.3. Situación actual del manejo y control de la información 21
2.3.4. Legislación vigente 22
ANÁLISIS DE METODOLOGÍAS Y HERRAMIENTAS 27
3.1. METODOLOGÍAS DEL ETHICAL HACKING 28
3.1.1. OWASP 28
3.1.2. PTES (PENETRATION TESTING EXECUTION STANDARD) 37
3.1.3. ISSAF 43
3.1.4. OSSTMM (Open Source Security Testing Methodology Manual) 48
3.1.5. Análisis comparativo de las metodologías analizadas 54
3.2. Herramientas del hacker ético 57
3.2.1. Footprinting 57
3.2.2. Scanning 59
3.2.3. Keyloggers (Grabadores de escritura de teclado) 60
GUIA PARA APLICAR ETHICAL HACKING EN PYMES 61

4.1. Procesos comunes en Ethical Hacking 62

4.2. Reporte final 65

4.2.1. Estructura del reporte de Ethical Hacking 65

CONCLUSIONES Y RECOMENDACIONES 70

Conclusiones 70

Recomendaciones 71

BIBLIOGRAFÍA 74

ANEXOS 78

Anexo 1: Glosario de siglas y términos 78

ÍNDICE DE TABLAS:

TABLA 1: TÉCNICAS DE VULNERABILIDADES INFORMÁTICAS 7

TABLA 2: HERRAMIENTAS DE LA FASE INFORMATION GATHERING 29

TABLA 3: HERRAMIENTAS DE LA FASE "CONFIGURATION MANAGEMENT TESTING" 30

TABLA 4: HERRAMIENTAS DE LA FASE "AUTHENTICATION TESTING" 31

TABLA 5: CANALES Y SECCIONES DE OSSTMM 52

TABLA 6: COMPARATIVA DE METODOLOGÍAS DE ETHICAL HACKING 54

TABLA 7: PROCESO DE PRUEBAS DE ETHICAL HACKING 64

TABLA 8: FASES COMUNES DE ETHICAL HACKING 67

ÍNDICE DE FIGURAS:

FIGURA 1. EMBLEMA HACKER ____ 10

FIGURA 2. SÍMBOLO DE LA METODOLOGÍA OWASP ____ 28

FIGURA 3. SÍMBOLO DE PTES ____ 37

FIGURA 4 INTERACCIONES PRE COMPROMISO ____ 38

FIGURA 5. THREAT MODELLING 40

FIGURA 6. FASES DE EVALUACIÓN ISSAF 47

FIGURA 7. CANALES Y SECCIONES DE LA METODOLOGÍA ISSAF 51

FIGURA 8 PÁGINA WEB DE NETCRAFT 58

FIGURA 9 PÁGINA WEB IP-ADRESS 58

CAPÍTULO 1

INTRODUCCIÓN

Alrededor del mundo las computadoras son víctimas constantes de ataques de hacker que pueden manipular e inclusive dañar un sistema y sobre todo ser la causa de espionaje y robo de información en tan solo unos instantes. Es por ello que es de gran importancia conocer si los sistemas informáticos y las redes pueden ser vulnerables o estar protegidas a todo tipo de intrusos.

Es por ello que el Ethical Hacking aparece como una práctica en la cual, con el consentimiento de la empresa a ser evaluada, se realiza una serie de pruebas o test que permitirán determinar qué tan robusta o no es la seguridad de sus redes, y poder realizar acciones de prevención ante un probable ataque por parte de los mencionados hackers. Estas pruebas simulan ataques de diferente índole, es por ello que resulta recomendable escoger una de las metodologías de Ethical Hacking que se diferencian en los pasos, formas y herramientas que utilizan para vulnerar las seguridades de las redes y de los sistemas.

Por lo tanto, resulta necesario determinar metodologías, qué herramientas utilizar, ya sean pagadas o libres, y las técnicas fundamentales para probar la vulnerabilidad de los sistemas de información y de las redes instaladas.

Antecedentes

El creciente uso de equipos tecnológicos como computadoras de escritorio, laptops, equipos móviles, servidores, entre otros por parte de instituciones ya sea públicas o privadas para la automatización de sus procesos internos, externos o combinados, además de la

información que cada una de estas contiene, aumenta considerablemente de valor debido al potencial uso que se puede hacer con ella, ya sea beneficioso o perjudicial.

Es por esta razón que existen una o más personas u organizaciones que juntan esfuerzos para vulnerar las diferentes seguridades informáticas de las empresas o instituciones, robando información para sus diferentes fines delictivos, generando grandes pérdidas muchas de ellas incalculables para dichas empresas.

El objetivo primordial del Ethical Hacking, es brindar ayuda a las empresas para que de esta forma tomen acciones preventivas en contra de estas acciones maliciosas; las medidas de prevención en las que se basa el Ethical Hacking son test de intrusión, los cuales examinan y evalúan la seguridad técnica de los sistemas de información, las redes de computadoras, servidores, aplicaciones web o móviles etc. Estos test simulan ataques controlados a las diferentes áreas de la infraestructura de la empresa.

El término hacking está asociado a actividades criminales sin embargo puede ser un aliado de las organizaciones. Un claro ejemplo sucedió en 1970 (ComputerFutures, 2016: web) cuando el gobierno de Estados Unidos dio luz verde a un grupo de expertos en seguridad a atacar su sistema de computación, de esta forma se aseguró el nivel de la misma, es por ello que en la actualidad la idea de probar un sistema atacándolo no suena tan descabellada; cabe destacar que gracias a esta práctica se basa el concepto del Ethical Hacking.

En la actualidad existen diferentes metodologías de hacking ético que permiten a los funcionarios de las TICs determinar las diferentes vulnerabilidades que tienen sus equipos tecnológicos y sus configuraciones respectivas.

Por todo lo mencionado previamente es que la razón de esta investigación es analizar las metodologías y herramientas que mejor se acoplen a las PyMES en Ecuador y elaborar la respectiva guía. Además de que la idea de implementar Ethical Hacking en el país madure para permitir controlar los diferentes ataques informáticos y prevenirlos en un futuro.

Justificación

En la actualidad, la mayoría de empresas ya sean grandes, medianas o pequeñas han optado por automatizar su información, para que de esta manera manipular grandes volúmenes de datos, mejorar la ejecución de los procesos y mejorar la calidad de atención a clientes. Conjuntamente con la automatización, está la compra de equipos tecnológicos, los cuales deben soportar todo lo mencionado previamente. Es por ello que es fundamental en las organizaciones proteger la información almacenada, y solucionar problemas como la manipulación o robo de datos por parte de terceros. La manera más recomendable es tomar medidas preventivas usando las diferentes metodologías y herramientas que el Ethical Hacking ofrece, permitiendo observar falencias y fortalezas de la infraestructura de las diferentes empresas.

Para ello se realizará un análisis comparativo tanto de las metodologías existentes como de las herramientas de Ethical Hacking, con el objetivo de descubrir cuál de ellas abarca mejores soluciones o más cercanas y adecuadas para la protección de redes de datos enfocado a PyMES.

Además de brindar las medidas preventivas mencionadas, la presente investigación ayudará a resolver problemas dentro del campo tratado y así complementar nuevos conocimientos teniendo como objetivo un mejor manejo de información. Cabe destacar que el desarrollo de técnicas de Ethical Hacking favorecerá a una mejor toma de decisiones por parte de los encargados de la seguridad de las PyMES, lo cual incluye personal experto en seguridad informática, equipos y sistemas robustos para garantizar la integridad de la información y sus inmediatas relaciones.

Objetivos

1.1.1. Objetivo General

Desarrollar una guía técnica estándar para aplicar herramientas de Ethical Hacking en redes de datos, enfocada a PyMES.

1.1.2. Objetivos Específicos

- Analizar la situación actual sobre el manejo y control de la información en las empresas medianas y pequeñas.
- Realizar un análisis comparativo entre las principales herramientas para aplicar Ethical Hacking e identificar los beneficios, ventajas, desventajas de las mismas.
- Desarrollar una guía estándar para aplicar Ethical Hacking.

Alcance

El presente proyecto de disertación de grado, culminará con la entrega de un documento con el análisis, selección de herramientas, ejecución y evaluación de resultados de las herramientas y desarrollo de la guía metodológica para aplicar hacking ético en redes de datos de PyMES.

Metodología

Para el presente proyecto se aplicará una metodología lógico deductiva la cual indica que "en esta se aplican los principios descubiertos a casos particulares, a partir de un enlace de juicios" (Saldaño, 2009, p.6). Es decir, está relacionada con búsqueda y personalización de casos de estudios enfocados a PyMES adecuados a la práctica de Ethical Hacking que se relacionan a la investigación de vulnerabilidades informáticas.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Seguridad informática

La seguridad informática (Galdámez, 2003: web) al igual que en diferentes áreas, se basa en la minimización de riesgos que están asociados al acceso y uso de un sistema o sistemas en general de forma no autorizada y sobre todo malintencionada, es por ello que es necesario la gestión de riesgo; es decir evaluar y cuantificar los bienes informáticos como los datos, equipos y software de una organización que permiten almacenar y automatizar la información, y mediante el análisis realizado, implementar acciones preventivas como políticas de seguridad que prevengan la alteración, modificación o reemplazo de datos almacenados en los mencionados sistemas de información de la organización.

2.1.1. Objetivos de la seguridad informática

El objetivo más importante de la seguridad informática es, cabe recalcar asegurar la integridad de los recursos informáticos valiosos de la organización principalmente de la información, la cual es la razón de que exista hardware y software; también es primordial la disponibilidad de uso que tiene el personal, sin que afecte su uso; y finalmente la confidencialidad para evitar la filtración de información.

Según López (2007: web), los elementos primordiales de la seguridad informática son:

- Integridad: los componentes del sistema no son alterados excepto por personal autorizado.
- Disponibilidad: los usuarios tienen al alcance todos los componentes del sistema y en correcto funcionamiento.

- Confidencialidad: solo pueden acceder a los distintos componentes del sistema por usuarios autorizados.
- Autenticación: asegurar que solo los usuarios asignados tengan acceso a los diferentes recursos.
- Trazabilidad: determina qué, cuándo, cómo y quién realiza acciones al sistema.

2.1.2. Principales técnicas para evaluar vulnerabilidades

Debido a la complejidad actual de las Tecnologías de información, se han incrementado los ataques a las diferentes redes de datos y sistemas tanto de organizaciones de cualquier índole, como a cualquier usuario. Según Hernández y Mejía (2015: web) un estudio de McAfee conocida por ser una importante empresa dedicada a la seguridad informática, los principales ataques aprovechándose de las vulnerabilidades se encuentran:

- SQL injection estructurado que es un método en el que se infiltra el código del hacker, también llamado Inyección en lenguaje de consulta de Sistemas operativos.
- Cross –site scripting o secuencia de comandos en sitios cruzados. (XSS), en la que un extraño puede insertar código JavaScript o similar en las páginas web de mayor frecuencia de visitas del usuario.
- Falsificación de petición en sitios cruzados donde se puede forzar al navegador de un usuario envía una petición a una aplicación web con debilidades de seguridad, que realiza la acción requerida por la víctima. Es un tipo de exploit o pedazos de código para aprovecharse de las vulnerabilidades en los programas (CSRF o cross-site request forgery).

La mejor forma de evitar ataques como los mencionados y otros, es la prevención, y para ello existen técnicas y herramientas para la detección de vulnerabilidades. Estas técnicas tienen diferentes enfoques como

- Black Box
- White Box
- Análisis estático de código
- Análisis dinámico de código
- Pruebas de penetración
- Pruebas pasivas
- Pruebas activas
- Fuzz testing (Prueba de la caja negra)

En la siguiente, se analiza a detalle cada una de las técnicas mencionadas.

Tabla 1: Técnicas de vulnerabilidades informáticas

Técnica	Descripción
Black Box	Permite detectar vulnerabilidades en aplicaciones web, basándose en un enfoque real, el del atacante.
White Box	En ésta técnica, se tiene acceso al código fuente, a las credenciales válidas, a la configuración y datos técnicos del servidor.
Análisis estático de código	Se analiza el código fuente directamente, para poder determinar vacíos de seguridad
Análisis dinámico de código	Al hacer el análisis, se comunica con la aplicación mediante front-end, para identificar debilidades de la arquitectura de la aplicación.
Pruebas de penetración	Simula ataques de delincuentes informáticos. Se analiza el sistema en busca de vulnerabilidades las cuales pueden ser de configuración, falla de hardware o software, errores operativos en proceso o contramedidas técnicas.
Pruebas pasivas	Analizan el tráfico de telecomunicaciones. Su característica es detectar fallas mediante un examen

	de livetrafficor log files o paquetes capturados. (Mammar, Cavalli, Jiménez, 2011)
Pruebas activas	Se usa un programador de subprocesos para verificar si las advertencias reportadas en un análisis predictivo del programa son errores reales
Fuzz testing o pruebas de caja negra	En una prueba al sistema usa datos aleatorios o alterados para detectar fallas en el comportamiento del sistema

Autor: Oswaldo Tamayo, marzo 2016.

La mayoría de las técnicas mencionadas tienen certificaciones que serán mencionadas en capítulos posteriores; además son certificaciones de Ethical hacking.

2.2. Ethical Hacking

2.2.1. Definición

Ethical Hacking es una herramienta de la seguridad informática que permitirá evaluar de la mejor forma las diferentes amenazas y ataques por parte de los delincuentes informáticos o "hacker", es un procedimiento en el que se actúa como uno de ellos, para de esta forma realizar las diferentes acciones de prevención si es el caso. En el Ethical Hacking, el personal a cargo tiene la capacidad de reportar las vulnerabilidades que tenga el sistema y prevenirlas ante inminentes ataques.

Ethical Hacking es el acto de anticiparse a los delitos usando conocimiento informático y herramientas de software; con las cuales realizará pruebas para encontrar fallas, que luego serán enviadas como reporte para tomar medidas preventivas. No se dañará la red y su acción correctiva será inminente.

Esta serie de pasos y pruebas mencionadas se denominan "pruebas de penetración" (403lab, 2016: web), las cuales simulan un ataque a la red de la infraestructura o aplicaciones de las empresas; el gran objetivo de las pruebas de penetración es determinar a qué pueden los hackers acceder y al violar la seguridad qué problemas podrían ocasionar.

Para poder garantizar que las redes de la infraestructura de una organización son "seguras", se requieren de herramientas, métodos y sistemas creados para la protección de la información, es en este instante donde el Ethical Hacking es importante para la toma de decisiones luego de ser reportadas las vulnerabilidades. El Ethical Hacking más que una herramienta pasa a ser una disciplina de la seguridad informática que usa varios métodos para hacer test, estos incluyen a la ingeniería social, usa herramientas de un hacker, y demás tácticas y artimañas que sirvan para violar la seguridad y entrar a las áreas más sensibles de las organizaciones.

Otro concepto (Manikandan, 2013: web) define al Ethical Hacking como una técnica utilizada para evaluar y gestionar el riesgo informático de una red, sistema o aplicación. Esta técnica la realizan expertos en seguridad que simularán acciones de un "cracker" para tener acceso no autorizado a un sistema, además cabe señalar que estos expertos usan las mismas herramientas que los delincuentes informáticos.

Como conclusión y concepto propio, el Ethical Hacking además de ser una técnica y disciplina como muchos expertos la definen; es una medida preventiva usada por las organizaciones para evaluar que tan "segura" es la red de datos, aplicaciones y sistemas de la misma, y si presenta vulnerabilidades, tomar medidas preventivas y dar soluciones específicas con el fin de proteger la información de la institución.

2.2.2. Hacker

La palabra Hacker ha sido malinterpretada desde sus inicios, durante los años 90 se lo asoció con el término "cracker" que significa una persona que desempeña alguna forma de sabotaje o avería en sistemas computacionales, es decir para ser un "efectivo" cracker se necesita ser un "buen" hacker.

Sin embargo, a pesar de la mala fama dada al término según Villacorta (2005) su significado es el de "una persona con profundos conocimientos sobre una tecnología. Esta puede ser la informática, electrónica o comunicaciones. El verdadero hacker es alguien que tiene ansias por saberlo todo, le gusta la investigación y sobre todo lo que resulta más fácil descifrar" (p.141).

Además, Villacorta (2005) señala que "entre las muchas variantes de hacker podemos distinguir dos: los crackers y los lamers. El cracker es aquel hacker fascinado por su capacidad de romper sistemas y software y que se dedica única y exclusivamente a crackear sistemas. El cracker, a diferencia del hacker, rompe sistemas y se aprovecha con fines ilícitos de la información obtenida" (p.141).

Por todo lo señalado previamente se puede definir a los hackers, como expertos en tecnologías de la información que muchas veces que basan sus conocimientos en autoaprendizaje y que disfrutan del proceso de aprendizaje y de ampliar sus capacidades sin la obligación de hacerlo.

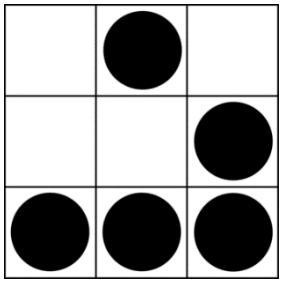


Figura 1. Emblema Hacker

Fuente: catb.org, marzo 2016

2.2.3. Tipos de Hacker

- **Cracker o hacker de sombrero negro**

Son los hackers maliciosos es decir personas que violan la seguridad de un equipo, una red e inclusive crean virus informáticos para sus fines. Estos crackers como los definí previamente, buscan constantemente maneras para romper la seguridad; por lo general

buscan maneras de menor resistencia. Su principal motivación es el valor monetario que pueden conseguir. (Giménez, 2011: web).

- **Hacker de Sombrero blanco**

Son profesionales que tienen gran conocimiento en hacking y los usan con fines preventivos, es decir actúan con las técnicas de los crackers, pero en lugar de usarla para sus propios beneficios, elaboran reportes y medidas preventivas en la mejora de las seguridades que hayan identificado como amenazas. Sus principales amenazas son los hackers de sombrero negro. (Giménez, 2011: web)

- **Hacker de Sombrero gris**

Este tipo de hacker tiene ética ambigua es decir de acuerdo la circunstancia pueden actuar como hacker de sombrero negro buscando como violar la seguridad de las redes de datos, y en otras actúan como hacker de sombrero blanco, es decir ayudando a las organizaciones mediante acciones preventivas. Son los más peligrosos ya que las empresas pueden confiar en sus servicios sin embargo al no tener una ética definida pueden actuar a su beneficio. (Giménez, 2011: web).

- **Ethical hacker**

Son profesionales que, al ser contratados por las diferentes organizaciones, gozan de la confianza total de los empleadores. Al realizar las diferentes pruebas del sistema, este profesional deberá tener total confidencialidad para con su cliente, además si se filtra cualquier información mal manejada puede causar que delincuentes informáticos quebranten el sistema causando pérdidas desde financieras, alteración y destrucción de datos. (Giménez, 2011: web).

Durante las pruebas el “hacker ético” tiene todo acceso a los diferentes sistemas de la organización para la que presta su servicio, es por ello que su profesionalismo y ética son trascendentales y funcionan como garantía de su labor. Cabe destacar que la información que se maneja durante los test o pruebas requiere medidas de seguridad altas. (Giménez, 2011: web).

Cuando el ethical hacker realiza un análisis de seguridad, puede requerir varias horas y días de trabajo ya que en ciertas ocasiones su horario laboral será en horas pocos usuales como madrugadas o fuera de la jornada de trabajo de la organización ya que tendrá dos beneficios: no habrá interferencia en alguna actividad, y se puede simular algún ataque en horas no esperadas.

2.2.4. Clases de hacker ético

Como se definió previamente, los hackers éticos trabajan a favor de fortalecer las seguridades de las diferentes organizaciones para las que son contratados, debido a que poseen gran conocimiento en seguridad informática, programación, redes entre otras ramas. Y sobre todo su profesionalismo los avala para ser contratados.

Los “hackers éticos” se los puede clasificar como:

- Ex hacker de sombrero negro (former black hats)
- Hacker de sombrero blanco (White hats)
- Consultorías

2.2.4.1. Hacker de sombrero negro reformado

También denominados ex “crackers”, son personas que antes se dedicaban a atacar las vulnerabilidades de los sistemas y que ahora se dedican a la protección de los mismos. Debido a su pasado, conocen los problemas de seguridad y pueden localizar la información

en las redes usando su metodología. Por causa de su pasado su credibilidad puede ser causa de desconfianza por parte de sus clientes.

La razón por la que se los contrata es por su notable dominio en cuanto a penetración de sistemas informáticos, que en muchos casos es superior a la de un hacker de sombrero blanco. Su moral es la principal duda en si contratarlos o no; sin embargo, a lo largo de la historia hay muchos ejemplos en los que en ocasiones demuestran estar del lado del "bien" y en otras del opuesto. A continuación, hay algunos ejemplos en los que este grupo de hackers actuaron a favor de mejorar la seguridad.

- En el 2000 un grupo de hackers accedieron al sitio apache.org el cual es un servidor http; ellos decidieron informar dichas vulnerabilidades.
- En el 2010 revelaron una falla de seguridad de AT&T, dicha falla permitía conseguir las direcciones de correo electrónico, ellos notificaron a la prensa de la vulnerabilidad.
- En el 2011 un grupo de hackers descubrieron que la generación del iPhone e iPad de aquel año registraban lo que el usuario visitaba. Por esa razón Apple declaró que solo registraba las torres donde el teléfono podía tener acceso. (Zarza, 2015: web).

Debido a que muchas empresas necesitan de su conocimiento, la mejor forma en la que estos hackers estén del lado del bien, es pagarles una gran cantidad de dinero para que de esta manera estén en su equipo. Por ejemplo, Microsoft paga hasta $150000 por encontrar y arreglar una vulnerabilidad en sus productos. (ArturoGoga, 2013: web).

Otro ejemplo es el de Jack Whitton el cual encontró una falla en la mensajería de Facebook en la que exponía el número de teléfono de los usuarios y por esta razón le pagaron $20000. (SecurityWeek, 2013: web).

2.2.4.2. Hacker de sombrero blanco

Como se los definió previamente, usan las mismas técnicas y tienen habilidades similares que los crackers o hacker de sombrero negro. Pueden trabajar externamente (consultorías) o pertenecer a una empresa en particular.

2.2.4.3. Consultorías

Son empresas dedicadas a la seguridad informática y son contratadas por las organizaciones para trabajos específicos. Por lo general tienen certificaciones y credenciales de seguridad que avalan su trabajo. Sin embargo, dentro de sus empleados pueden estar hacker de sombrero gris, hacker de sombrero negro reformados o hacker de sombrero blanco.

2.2.5. Ética del hacker

Debido a la creciente industria relacionada con la computación e informática, la ética hacker es relativamente nueva comparada con la de otras ramas y ciencias, y está aplicada a comunidades virtuales, pero no de manera exclusiva.

La ética hacker es atribuida a Steven Levy quien relata en su libro "Hacker: Heroes of the Computer Revolution" acerca del incremento de hacker en Estados Unidos, además describe y define los principios de la ética hacker. Estos se los puede generalizar como el acceso libre a la información y que las ciencias computacionales e informáticas pueden mejorar la calidad de vida de los seres humanos; basados en estas dos ideas se han fomentado las bases de las definiciones que se describirán posteriormente.

Pekka Himanen (2001: web) señala que en la era de la tecnología de la actualidad existen hacker los cuales los define como personas apasionadas a la programación y que para ellos el compartir y desarrollar software gratuito es una forma de ser. No se los debe relacionar con los crackers que su objetivo es introducirse en un sistema o crear virus para dañar. Por

ello la ética hacker es una disciplina filosófica que desafía a la ética protestante del trabajo debido a que se basa en la creatividad y combina libertad y pasión. El valor monetario queda de lado y su beneficio se basa en objetivos clave como el valor social, la transparencia y el libre acceso, entre otros.

2.2.6. Valores de la ética del hacker

Según Himanen (2001: web) los valores orientados a la vida del hacker son:

- Pasión: relacionada a la búsqueda intrínseca
- Libertad: debido a que los hackers organizan su jornada de trabajo como flujo dinámico entre el trabajo creativo y el juego
- Conciencia social: relacionada en computación como satisfacer necesidades de confidencialidad de las organizaciones y sobre todo proteger al individuo de estas organizaciones como gobiernos y empresas
- Verdad
- Anticorrupción
- Igualdad social
- Curiosidad
- Creatividad

2.2.7. Modo de actuación de un hacker

Cabe destacar que todos los sistemas al ser desarrollados por humanos son inseguros; incluso los sistemas bancarios, de los organismos de seguridad e inclusive de la NASA.

El problema de las computadoras surge cuando se les conecta a Internet y se asigna un número de IP para identificarse a una determinada red.

Cabe destacar que es posible atacar la seguridad de un equipo de cómputo desconectado de la red. Un grupo de investigadores israelíes desarrollo un malware llamado “AirHopper” que mediante señales electromagnéticas puede infectar un computador. Este malware extrae datos de manera remota mediante las pequeñas señales electromagnéticas de la tarjeta gráfica del equipo con el monitor a modo de antena cada vez que se teclea. Además, es necesario un teléfono inteligente con receptor de radio FM para recibir las pulsaciones. (Giménez, 2011: web).

En ese instante el computador es un elemento más de las diferentes redes. Debido a la gran demanda de servicios de red, además de una dirección IP, se especifican estos servicios mediante puertos. Por ejemplo, cuando se requiere una página web, por ejemplo, la solicitud se realiza mediante un determinado puerto del ordenador a un puerto del servidor web. En la actualidad (Giménez, 2011: web) el número de puertos es de más de 65000 y es por la causa de estos que suceden intromisiones por los hackers, razón por la cual estos puertos deben permanecer cerrados, es decir solo tener el puerto que se usará, y los demás tenerlos desactivados.

Además, es importante destacar que debido al despliegue global de IPv6, sería imprudente creer que un ataque por esta vía es poco probable; la realidad es diferente ya que todos los equipos Windows Vista, Windows 7, Windows 8, Windows server 2008,2008 R2 y 2012 vienen configurados por defecto; en los entornos actuales es muy probable que IPv4 esté en “convivencia” con IPv6. Uno de los ataques en redes de datos IPv6 por su sencillez es el Neighbor Spoofing. Según Alonso (2012: web) es habitual que una computadora envíe un mensaje de Neighbor Solicitation NS a una dirección multicast cuando vaya a comunicarse con otro, y el equipo que tenga la dirección IPv6 responda al mensaje multicast con un mensaje unicast de Neighbor Advertisement NA con su propia dirección física MAC; el receptor del mensaje NA guardará en la tabla de vecinos la dirección IPv6 con la respectiva

MAC asociada. Sin embargo, al igual que en IPv4 con el protocolo ARP un atacante puede enviar un mensaje NA sin haber recibido el mensaje previo de NS y hacer que la caché de la tabla de vecinos se almacene en el registro. (Giménez, 2011: web).

Los pasos para un buen ataque hacker consta de los siguientes:

a) Introducirse en el sistema objetivo

Es decir, identificar el objetivo, por lo general este puede ser elegido al azar o identificado previamente, al tenerlo identificado se infiere que el hacker tiene la dirección IP de la máquina objetivo. El siguiente paso es obtener información adicional como la topología de red, su sistema operativo, algo de información de la organización etc. Se explora además información de los puertos usando herramientas (Giménez, 2011: web) como netcat o nmap, estas permiten detectar los puertos abiertos o disponibles de una máquina, es decir qué servicios están activos. Después de esto el hacker tiene su fuente de datos sobre su objetivo como: la topología de red, versión y tipo de sistema operativo que tienen los servidores y si tiene firewall o cortafuegos, los servicios de internet en ejecución, información de la organización, sus usuarios etc. El hacker ahora deberá tener la capacidad analítica de estudiar la información que posee para identificar vulnerabilidades, los accesos y puertas de escape. En este punto inicia el ataque.

Los hackers harán uso de servicios como telnet, ssh o ftp para entrar a otros equipos, sin embargo, deben tener un usuario y una contraseña. Cabe destacar que los servidores tienen sistemas operativos como Unix y sus derivados (Linux, AIX) o Windows NT, en donde los usuarios tienen diversos privilegios, dependiendo de su labor en la empresa, alguno de estos usuarios tendrá acceso a cambiar la configuración de ésta.

Los hackers para poder entrar al sistema tienen que conseguir la carpeta o fichero dependiendo el S.O. llamado passwd que contiene información de la contraseña y del

nombre de usuario de todos los que pertenecen al sistema a vulnerar. Por esto buscan inmiscuirse en el sistema y buscan puertos vulnerables conocer los protocolos y sus versiones, con el fin de ejecutar bugs o falencias de programación y que sirvan para hacer la "entrada" más fácil. Estos bugs son fallas de los sistemas operativos o de las aplicaciones que corren en los servidores que al ser desarrollados no han sido corregidos y que al ser atacados de diversas formas permiten el acceso a un sistema. Las aplicaciones pueden ser servidores de páginas web o puertos de red mal configurados como http, smtp, ftp, que son las llamadas puertas traseras o backdoors.

Supongamos que el hacker ha obtenido el fichero o carpeta passwd, por lo general este archivo está encriptado, su siguiente paso será descifrarlo para obtener la contraseña y el usuario respectivo. En la actualidad, existe un método que hace invisibles las contraseñas denominado "shadow", sin embargo, según (Giménez, 2011: web) no es una protección segura ya que cualquier hacker con conocimientos al respecto y con paciencia puede ser capaz de romper esa seguridad extra.

b) Obtener privilegios de administrador

Al ser administrador de un sistema, se tiene potestad de alterar o "tener privilegios" de hacer cualquier cosa en el sistema sin ningún problema al respecto.

Es por ello que cuando el hacker ha conseguido entrar al sistema usando un usuario cualquiera, buscará ahora ser un usuario root. En el área de computación un usuario root es aquel que tiene absoluto poder en un sistema, es decir puede revisar el correo de los usuarios, instalar programas de cualquier tipo y demás. Al haber ingresado al sistema como un usuario cualquiera, el hacker usa exploits, que según Albors (2014: web) son programas o códigos de ejecución que sacan ventaja de un agujero de seguridad en un sistema, de esta forma el atacante saca ventaja, es decir es como una llave maestra que permite abrir cualquier puerta que tenga una falla de su cerradura.

c) Borrar las huellas

Cuando el hacker ha accedido al sistema como usuario root, es común que deje un mensaje al administrador en tono jocoso, ya que consiguió violar las seguridades de su sistema. Además, es importante borrar los registros logs, que indican el instante en que fue alterada la seguridad.

2.2.8. Beneficios de Ethical Hacking

Antes de saber los beneficios que conllevan aplicar Ethical Hacking en una organización, es importante saber su funcionalidad y la prevención que significa.

Los principales beneficios son:

- Evitar la pérdida de información y por ende la protección de los diversos recursos que tienen las organizaciones.
- Informar acerca de los problemas de seguridad encontrados durante los diversos test aplicados para tomar acciones preventivas y correctivas.
- Actualizar los sistemas que son vulnerables por falta de las mismas
- Evitar tener configuraciones mal instaladas o de erróneo funcionamiento en equipos o software, como switches, routers, firewalls que podrían causar fallas de seguridad.

2.3. PYMES

2.3.1. Definición

Según el sitio web del Servicio de Rentas Internas (SRI, 2015: web) PYMES es la denominación que se le da al conjunto de pequeñas y medianas empresas, debido a su volumen de ventas, capital social, cantidad de trabajadores, y el nivel de producción o activos.

Según el grupo Enroke (2014: web), el concepto varía de acuerdo a la economía de un país, es decir si la empresa tiene un volumen de venta de unos $10000000 al año, se considera pequeña o mediana empresa en un determinado país, pero en otro puede ser una empresa grande. De igual forma una empresa que solo tiene un trabajador puede generar más ingreso que la que tenga 20 o más. En el país una pequeña o mediana empresa se mide de acuerdo a volumen de ventas, número de trabajadores, activos, pasivos y niveles de producción.

Es decir, una empresa es pequeña o mediana si tiene una cantidad limitada de personal, un presupuesto reducido para su medio y además el gobierno local da asistencia o ayuda.

En el país existen 3 tipos de negocios: las microempresas, las PyMES y las empresas grandes. La gran diferencia es que las microempresas tienen un volumen de venta que no supera los $15000 anuales; las empresas grandes según la revista Vistazo o Líderes, tienen un volumen de venta en el país que va desde los $20 millones hasta los $1000 millones anuales. Con estos parámetros una pequeña y mediana empresa en el Ecuador en términos de volúmenes de venta es aquella que va entre los $15000 y $20 millones anuales. (Enroke, 2014: web).

2.3.2. Características

- Recursos limitados
- Reciben asistencia del gobierno o subsidios.
- Son administradas por sus propietarios
- Varios de sus empleados pueden pertenecer a la familia del propietario.
- La organización y políticas de gestión son simples sin cargas burocráticas.
- Poca capacidad de negociación

Además de las características señaladas, según Morales (2012: web) en el país las PYMES tienen las siguientes fortalezas y debilidades:

Fortalezas de las PYMES

- Generan empleo en un porcentaje del 60%
- Alta flexibilidad frente a cambios
- Amplio potencial redistributivo
- Su estructura empresarial es horizontal
- Participan de un 50% de la producción

Debilidades de las PYMES

- Insuficiente capacitación al recurso humano
- Insuficiente cantidad productiva
- Inadecuada e insuficiente tecnología y/o maquinaria para la fabricación de productos.
- Costos elevados por desperdicio de materia prima
- Se requiere exigencias de calidad, técnicas y legales.

2.3.3. Situación actual del manejo y control de la información

La situación actual acerca de la gestión en las PyMES, se asemeja al contexto de la región; ya que existen factores internos y externos que en el país son similares a los de Latinoamérica. Los factores externos serían:

- Características de la industria
- Políticas nacionales en lo económico, comercial y tecnológico.

En cambio, los internos, responden a la capacidad de la empresa y de su persona como:

- Experiencia tanto de la empresa como de sus empleados en el uso de TIC´s
- Estrategias relacionadas a la productividad, rentabilidad y competitividad.

CONQuito, realizó una encuesta a 202 empresas manufactureras de Quito, sus condiciones y costos, políticas de seguridad y proyectos desarrollados en el país. Respecto a los resultados, se concluye que los sistemas de información no son aún el eje de gestión en las PyMES, pero que de a poco, especialmente las grandes y medianas empresas están mejorando sus prácticas. Cabe destacar que varias empresas familiares atraviesan un cambio generacional para lograr incorporar a la tecnología para sus objetivos. (Corporación de Promoción Económica CONQuito, 2007).

Si bien la idea de ethical hacking aplicado a empresas, se basa en asistir a empresas grandes, con un costo elevado, hoy en día todas las empresas pequeñas y medianas, usan aplicativos diversos como: correo electrónico, archivos en la nube, o página web, es muy probable que si requieren asistencia de un analista de sistemas para una rápida evaluación de seguridad sería conveniente para ambas partes el pago de mucho menos de lo que cobra una empresa de ethical hacking. Este podría ofrecer sus servicios para proteger a la empresa, recomendando incluir políticas de seguridad, y siguiendo los pasos de alguna de las metodologías.

2.3.4. Legislación vigente

En el Ecuador, las leyes no incluyen a los delitos informáticos en la seguridad estatal. Por ello se puede realizar mucho daño a las instituciones públicas, al poder alterar su información y por ende al ciudadano común. A pesar de esto, en el 2002 se creó la ley de comercio electrónico y mensajes de datos con la cual se agrega al código penal artículos referentes a los delitos electrónicos.

- El artículo 201.1 señala que: “Delitos contra la información protegida. - El que, empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en

sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica." *(Yar, 2015: web).*

Esta ley lo que indica es el castigo para las personas que quieran obtener passwords usando cualquier mecanismo ya sea físico o virtual. La pena puede ser prisión y multa dependiendo la gravedad del delito a ser juzgado.

Además, este artículo tiene los siguientes ítems:

- *"Si la información obtenida se refiere a seguridad nacional, o secretos comerciales e industriales, la pena será de uno a tres años de prisión y una multa de 1000 a 1500 dólares." (Páez, 2009: web).* El castigo señalado en este ítem, no indica que el delincuente haya divulgado la información sino, que la tiene sin haber sido demostrado que haya difundido.
- "*La divulgación o utilización fraudulenta de la información confidencial, así como los secretos comerciales o industriales serán sancionados con pena de reclusión menor de 3 a 6 años y una multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica." (Páez, 2009: web).* En este caso, el delincuente si divulgó lo que encontró usando técnicas particulares para obtener la información.
- *"Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, estas serán sancionadas con pena de reclusión menor de seis a nueve años y una multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica." (Páez, 2009: web).* Este caso en cambio, sucede cuando el personal a cargo de la seguridad informática de la institución, difunde

información privada, al ser condenado, es el caso que mayores años de prisión tiene en el país.

El artículo 202 se rige para los casos en que, ya sea la forma en que obtuvieron la información, sea esta cedida por el dueño u obtenida de forma ilegal, no pueden difundirla sin previa autorización. Este artículo textualmente dice lo siguiente:

- "*Obtención y utilización no autorizada de información. - La persona o personas que obtuvieron información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionados con una pena de prisión de 2 meses a 2 años y una multa de 1000 a 2000 dólares".* (Páez, 2009: web)

El siguiente artículo en cambio, indica el caso en que el acusado haya eliminado información importante y trascendental para la empresa, cabe destacar que esta data está a su cargo o responsabilidad.

- "*Art. (262).- Destrucción Maliciosa de documentos.- Serán reprimidos con 3 a 6 años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo."* (Páez, 2009: web).

- "*Art. (353.1).- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la*

información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho." (Páez, 2009: web). Este caso, detalla la falsificación de mensajes como correos, o editar archivos para lucrar en perjuicio de una tercera parte. Estas falsificaciones pueden ser modificaciones, simulaciones o intervenciones erróneas.

- "*Art (415.1). - Daños informáticos. - el que dolosamente de cualquier modo o utilizando cualquier método destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de 6 meses a 3 años y multa de sesenta a ciento cincuenta dólares. "(*Páez, 2009: web). Finalmente, este artículo, indica castigar por la destrucción o alteración de información reflejada en bases de datos, mensajes o información almacenada en repositorios.

Es importante señalar que, si bien las leyes contra el delito informático existen een el país, su penalización es leve comparada a la de otros países en los que el delito informático se juzga con igual magnitud a la de los delitos conocidos.

CAPÍTULO 3

ANÁLISIS DE METODOLOGÍAS Y HERRAMIENTAS

Como se mencionó en el capítulo previo, existen varias certificaciones internacionales de ethical hacking, cada una de ellas se basa en una metodología propia, sin embargo, cabe resaltar que todas ellas realizan un test de intrusión el cual, dependiendo la certificación, la metodología variará. Es por ello que se enmarcará en un concepto general de seguridad de la información.

Al momento de escoger una de ellas es común preguntarse: ¿Cuál escoger?, ¿cuál es la más adecuada?, ¿cuáles se aplican en la actualidad?, y sobre todo ¿cuál de ellas se adapta mejor a las necesidades de las empresas? Según una de las metodologías más importantes como es la OWASP (2016: web), realizar un test de intrusión o pentest, nunca es una ciencia exacta, ya que existen un sinnúmero de factores y diversos problemas y riesgos que deben ser revisados o analizados previamente a la prueba de intrusión.

Las metodologías que se analizarán a mayor detalle, son procesos de larga duración que estarán en función de las necesidades y al alcance de cualquiera, ya que son de libre uso. Estas ofrecen una posibilidad de usarlas tanto para beneficio propio o de la empresa a cargo como para realizar aportes a una comunidad de internet. Por lo general, las personas que ponen en práctica estas metodologías poseen una preparación precisa, sino que también prudencia moral y madurez lo cual garantizará la objetividad, ética e independencia.

En el capítulo previo se definió a las principales metodologías para realizar ethical hacking; en este capítulo se detallarán las fases de éstas para poder tener como referencia al analizarlas y compararlas.

En el capítulo también se incluye un apartado de las herramientas más importantes del ethical hacking, las cuales son facilitadores para su trabajo, el cual consiste en buscar

vulnerabilidades orientadas a pequeñas y medianas empresas. Cabe destacar que, si son usadas para perjudicar a personas u organizaciones, pueden causar pérdidas incuantificables si se pueden usar.

3.1. METODOLOGÍAS DEL ETHICAL HACKING

3.1.1. OWASP



Figura 2. Símbolo de la metodología OWASP

El método de aplicación que usa OWASP se basa en una aproximación de tipo "Caja negra"; es decir el hacker ético no conoce nada o tiene muy poca información sobre la aplicación a ser evaluada. Esta metodología se basa en dos fases:

Fase Pasiva:

Según Pérez (2012: web) la fase pasiva trata en hacer pruebas en la cual analiza a la aplicación en su parte lógica, la cual está en etapa de prueba, además se puede comprobar si lanza algún dato que signifique una puerta abierta u oportunidad para de esta forma, mejorar el análisis, el cual será más persuasivo.

Fase Activa:

El hacker ético prueba los procesos recomendados de ésta metodología que costa de 9 subcategorías y 66 procesos:

Configuration Management Testing o Pruebas de gestión de la Configuración (Recopilación de información- Gestión de configuración)

- Pruebas de autenticación o Authentication Testing
- Pruebas de acceso o autorización -Authorization testing
- Pruebas de gestión de sesiones o Session Management Testing
- Pruebas de lógica de negocio o Business Logic Testing
- Pruebas de datos reales Data Validation Testing
- Pruebas de negación de servicio o Denial of Service Testing
- Pruebas de los servicios web o Web Services Testing
- Pruebas Ajax- Ajax Testing

i. Information Gathering o Recopilación de información

En esta fase se almacena o recopila la mayor cantidad de información acerca del objetivo o de lo que busca el cliente. Se puede hacer el procedimiento con herramientas públicas y/o software libre. Lo que se busca es forzar a la aplicación a mostrar una o varias debilidades. (Pérez, 2012: web).

Algunas de las mencionadas, están en la tabla mostrada a continuación:

Tabla 2: Herramientas de la fase Information Gathering

Herramientas	Descripción
Pruebas: spiders, robots, y rastreadores o crawlers (owasp-ig-001)	Recuperan una página web y luego recursivamente a través de hipervínculos, los usan para recuperar el contenido web. Este comportamiento es especificado en el archivo robots.txt el cual está el directorio web root.
Search engine discovery/reconnaissance o Descubrimiento y reconocimiento de motores de búsqueda (owasp-ig-002)	Tiene elementos directos e indirectos para buscar en los motores de búsqueda. Los directos realizan la búsqueda en índices y contenido en las caches. Los indirectos recabar o buscar información del diseño e información de configuración usando foros de búsqueda y sitios web de licitación.
Identify application entry points o Identificación de los puntos de login o entrada de la aplicación (owasp-ig-003)	Enumera la aplicación y la superficie de ataque, es decir la describe superficialmente lo cual es clave antes de cualquier prueba más específica, ya que permite que el tester identifique áreas de posible debilidad.
Testing for web application fingerprint o Pruebas fingerprint enfocadas en aplicaciones web (owasp-ig-004)	Permite conocer la versión y tipo del servidor web, es fundamental para los siguientes pasos.
Application discovery o Descubrimiento de aplicaciones (owasp-ig-005)	Permite saber las aplicaciones y el tipo de estas que corren sobre un determinado servidor, entre los cuales puede ser apache tomcat, jboss,swat etc.

Analysis of error codes o análisis en los errores de código(owasp-ig-006)	Es común que las aplicaciones indiquen las vulnerabilidades que tienen, muchas de ellas detallan inclusive el sistema operativo, el puerto y el protocolo de seguridad que usa, lo cual facilitará el ataque. Por ejemplo, el error 404 da el siguiente mensaje: Not found: que indica que la página web en esa dirección no fue encontrada The requested URL /page.html was not found on this server. Aqui especifica lo que se mencionó, ésta página web no existe en el determinado servidor. Apache/2.2.3 (Unix) mod_ssl/2.2.3 OpenSSL/0.9.7g DAV/2 PHP/5.1.2 Server at localhost Port 80: y aquí provee información como el nombre del servidor y su versión (Apache 2.2.3) el sistema operativo, a pesar de que no especifica que partición de Unix es, el protcolo que usa openssl, el lenguaje de programación de la aplicación que es php y el puerto 80.

Autor: Oswaldo Tamayo, mayo 2016.

ii. Configuration Management Testing o Gestión de pruebas de configuración

En esta fase se pueden observar fallas de configuración y sobre todo de la topología o la forma de la infraestructura de la aplicación, además aparecen fallas derivadas de la poca consistencia en el desarrollo de la aplicación.

Las herramientas a utilizar se describen en la siguiente tabla:

*Tabla 3**: Herramientas de la fase "Configuration Management Testing"***

Herramientas	Descripción
SSL/TLS Testing o Pruebas SSL/TLS (OWASP-CM-001)	Permite verificar que tan robusto es el cifrado de la aplicación a la que se estudiará.
DB Listener Testing o Pruebas a los puertos de la Base de datos (OWASP-CM-002)	Permite verificar la configuración de la base de datos del objetivo, como los puertos, el servidor etc.
Infrastructure Configuration Management Testing o Pruebas de Gestión de configuración de infraestructura (OWASP-CM-03)	Analiza los fallos de infraestructuras web, uno muy simple puede dejar al descubierto a la infraestructura, esto puede ser el sistema operativo, los puertos y protocolos de seguridad usados.
Application Configuration Management Testing o Gestión de pruebas de configuración de la aplicación (OWASP-CM-004)	Al estudiar el código fuente de las aplicaciones, se puede quedar en evidencia algunos datos sobre los procesos de configuración.
Testing for File Extensions Handling o Pruebas de extensión de archivos de manipulación (OWASP-CM-005)	Existen archivos con extensiones php, asp, jsp entre otros, que revelan que servidor trabaja en las aplicaciones y sus probables conexiones
Old, Backup and Unreferenced Files (OWASP-CM-006)	Todos los archivos que se puedan descargar o sean legibles, copias de seguridad entre otros, pueden indicar rutas de instalación, nombres de usuario o passwords.
Infrastructure and Application Admin Interfaces (OWASP-CM-007)	La mayoría de aplicaciones web, por lo general tienen una interfaz administrativa la cual puede ser atacada, o tener una configuración dada en la instalación. Eso facilitará el ingreso, puede ser el caso de routers que tienen interfaz web para facilitar el uso a usuarios con poco conocimiento.
Testing for HTTP Methods and XST o Pruebas de métodos HTTP y XST (OWASP-CM-008)	Prueba que el servidor objetivo, permita o no el uso de comandos xst y http

Autor: Oswaldo Tamayo, mayo 2016

iii. Authentication testing O Pruebas de Autenticación

Indica el perfil y a que usuario pertenece. Las principales herramientas según Pérez (2012: web) se mencionan en la siguiente tabla:

Tabla 4: Herramientas de la fase "Authentication testing"

Herramientas	Descripción
Credentials transport over an encrypted channel (OWASP-AT-001)	Permite identificar si se usan protocolos seguros o no, los cuales pueden proteger de ataques
Testing for user enumeration (OWASP-AT-002)	Pruebas de resistencia a ataques de fuerza bruta como querys en el registro de datos, y entrada al sistema por extraños.
Pruebas para invitados con cuentas de usuario o Testing for Guessable (Dictionary) User Account (OWASP-AT-003)	Permite encontrar cuentas de usuarios existentes por defecto.
Brute Force Testing o Pruebas de fuerza bruta (OWASP-AT-004)	Si falla el encontrar cuentas de usuario en el ataque mencionado previamente, garantizar otro mediante intentos de fuerza bruta, como atacar la autenticación con cuentas falsas para que el servidor colapse.
Testing for bypassing authentication schema o Pruebas para saltarse el Sistema de autenticación (OWASP-AT-005)	Es común que existan recursos no protegidos, pero no por ello se los debe descuidar ya que se puede acceder a ellos sin utilizar el proceso de login (bypass)
Testing for vulnerable remember password and pwd reset o Pruebas para recuerdo de contraseñas (OWASP-AT-006)	Se relaciona con la función de recordar la contraseña en los navegadores, es importante tener precaución al respecto
Testing for Logout and Browser Cache Management (OWASP-AT-07)	Analiza si se salió o no del sistema correctamente usando la función log-out.
Testing for CAPTCHA o Pruebas para Captcha (OWASP-AT-008)	Existen versionas de captcha que son vulnerables lo cual permite que los bots de registro masivo y ataque ddos sea más fácil..
Testing Multiple Factors Authentication o Pruebas de factores multiples de autenticación (OWASP-AT-009)	Sirve para realizar pruebas a dispositivos que tienen certificados para autenticación y que son legítimos.
Pruebas en condiciones reales o Testing for Race Conditions (OWASP-AT-010)	Son difíciles de desarrollar e instalar. Los resultados son improbables y muestran impacto en otras tareas. Ej. Aplicaciones mutihilo.

Autor: Oswaldo Tamayo, mayo 2016

iv. Session management testing o Pruebas de Gestión de sesiones

Se gestiona la gestión de sesiones, es decir desde el ingreso del usuario autenticándose al sistema hasta que finaliza la sesión.

Según la página web de OWASP (web: 2014) las principales herramientas en esta fase son:

- Testing for Session Management Schema (OWASP-SM-001)

  Sirve para entender el mecanismo de gestión de sesiones. Se puede probar haciendo un bypass de sesión.

- Testing for Cookies attributes (OWASP-SM-002)

  Usualmente, se ataca a las cookies, las cuales para evitarlo deben estar protegidas. Si se intercepta una, se podría autenticar un sistema, o ingresar en él.

- Testing for Session Fixation o Pruebas de fijación de sesión (OWASP-SM_003)

  Si no se renuevan las cookies de la sesión, estas pueden servir para ser reutilizadas.

- Testing for Exposed Session Variables o Pruebas para variables de sesión expuesta (OWASP-SM-004)

  Si es posible replicar los tokens de la sesión, es un hecho que se puede ingresar al sistema.

- Testing for CSRF o Pruebas para falsificación de petición en sitios cruzados (OWASP-SM-005)

  Se forzará a un usuario víctima que esté autenticado o dentro del sistema a realizar algo no previsto sobre una aplicación web.

v. Authorization Testing o Pruebas de autorización

En la metodología OWASP autorización significa acceder y usar todo dentro de un sistema que se está registrado. Además, los roles de usuario y los niveles de autorización o de acceso que tienen.

(OWASP; 2014; web). Las principales herramientas, según Pérez (2014: web) son:

- Testing for Path Traversal o Prueba de ruta transversal (OWASP-AZ-001)

Esta prueba permite acceder a información confidencial a través del ataque de ruta transversal.

- Testing for bypassing authorization schema o Pruebas para evitar el esquema de autorización (OWASP-AZ-002)

Como se desarrolló cada rol de usuario y que privilegio tiene en el sistema para acceder a información privada.

- Testing for Privilege Escalation o Pruebas de escala de privilegios (OWASP-AZ-003)

Se debe revisar que no es posible modificar los roles de usuario y los privilegios de este dentro del sistema.

vi. Business Logic testing o Pruebas de Lógica de Negocio (owasp-bl-001)

Es una forma que se basa en la creatividad del hacker para acceder a un sistema web. No solo se utilizan formas técnicas sino cualquier forma es aceptable. Existen muchas maneras, pero lo que se establece en esta fase es "pensar de manera única y creativa". (OWASP, 2014: web).

vii. Data Validation Testing o Pruebas de validación de datos

Son técnicas estables y conocidas para atacar a sistemas como croos site scripting o XSS, sql injection y otros. Las principales técnicas según Pérez (2012: web) son:

- Testing for Reflected Cross Site Scripting o Pruebas de cross site scripting reflejado o mirror (OWASP-DV-001)
- Testing for Stored Cross Site Scripting o Pruebas de cross site scripting en data almacenada (OWASP-DV-002)

- Testing for DOM based Cross Site Scripting o Pruebas para DOM basadadas en xss (OWASP-DV-003)
- Testing for Cross Site Flashing o Pruebas de xsf o csf (OWASP-DV004)
- SQL Injection o Inyección de código sql (OWASP-DV-005)

  Se inyectan a través de una consulta a la Base de datos
- LDAP Injection (OWASP-DV-006)
- Code Injection o Ejecución de código (OWASP-DV-012)

  Código malicioso que pueda se puede lanzar o ejecutar
- OS Commanding (OWASP-DV-013)

  Se lanzará una secuencia de comandos del sistema usando una búsqueda http.
- Buffer overflow o Desbordamiento de Buffer(OWASP-DV-014)
- Testing for HTTP Splitting/Smuggling o Pruebas HTTP usando splitting o smuggling (OWASP-DV-016)

viii. Denial of Service Testing o Pruebas de negación de servicio

En esta fase se trata de desestabilizar al servidor de la organización mediante tráfico que no se puede procesar. (OWASP; 2014: web). Las herramientas usadas en la fase son:

- ***Testing_for_SQL_Wildcard_Attacks o Pruebas de ataque con wildcards SQL (OWASP-DS-001)***
- ***D Locking Customer Accounts o Bloquear cuentas de usuarios (OWASP-DS-002)***
- ***Buffer Overflows o Desbordamiento buffer (OWASP-DS-003)***

- ***User Specified Object Allocation o Asignación de objeto especificado por el usuario (OWASP-DS-004)***
- ***User Input as a Loop Counter o Entrada de usuario como un Contador de bucle (OWASP-DS-005)***
- ***Writing User Provided Data to Disk o Usuario de escritura suministrando datos en el disco (OWASP-DS-006)***
- ***Failure to Release Resources o Falla en la liberación de recursos (OWASP-DS-007)***
- ***Storing too Much Data in Session o Exceso de almacenamiento de datos en una sesión (OWASP-DS-008)***

ix. Web Service testing o Pruebas del Servicio Web

Se realizan pruebas a los servicios web de la aplicación y se puede encontrar vulnerabilidades dentro de esta, se realizan técnicas de inyección como la de SQL.

- ***WS Information Gathering o Recopilación de información (OWASP-WS-001)***
- ***Testing WSDL o Pruebas de Web service description language(OWASP-WS-002)***
- ***XML Structural Testing Pruebas de estructura XML (OWASP-WS-003)***
- ***XML Content-level Testing Pruebas sobre el contenido XML (OWASP-WS-004)***
- ***HTTP GET parameters/REST Testing o Pruebas de HTTP GET y parámetros REST (OWASP-WS-005)***
- ***Naughty SOAP attachments o Archivos adjuntos SOAP dañados (OWASP-WS-006)***

- ***Replay Testing o Pruebas de repetición (OWASP-WS-007)***

x. Pruebas Ajax

Ajax significa xml y javascript no sincronizadas o Asynchronous JavaScript and XML, la cual es una técnica usada para determinar si se tiene respuesta de dos servidores de forma dinámica. Se basa en dar al usuario experiencias similares de uso de escritorio. Son de gran utilidad, sin embargo, desde un punto de vista de un atacante, ofrecen una amplia superficie de vectores de ataque. (Pérez; 2014: web).

- ***AJAX Vulnerabilities o Vulnerabilidades AJAX (OWASP-AJ-001)***

Se combinan técnicas de ataque como: SQL injection, XSS y otros.

- ***How to test AJAX o Como realizar pruebas AJAX (OWASP-AJ-002)***

xi. Escribiendo reportes para valorar los riesgos de la empresa

Es la forma en la que se va a presentar el informe al cliente. Es una tabla con una imagen que refleje la evaluación hecha la cual debe ser lo más exacta posible.

¿Cómo evaluar el riesgo real?

Las fallas encontradas son importantes, sin embargo, son solo de referencia de los riesgos asociados con la información expuesta. Se debe hacer un enfoque de severidad de los riesgos encontrados.

La fórmula para describir a un riesgo y sus impactos es:

R = probabilidad de que suceda * impacto.

Lo que significa que, si algo pasa, se puede despreciar el riesgo siempre y cuando este no afecte la continuidad, tomando medidas correctivas.

Los pasos para realizar esta metodología son los siguientes:

1. Identificar el o los riesgos.

2. Que factores o datos ese usó para determinar la probabilidad del riesgo o de q suceda.

3. Factores o datos para estimar qué impacto tendrá en el negocio.

4. Determinar el grado del riesgo, es decir si este afecta o no la continuidad. (valoración numérica).

5. Decidir qué corregir.

6. Adaptar el moldeo de valoración del riesgo con medidas propias. (Perez; 2012: web).

3.1.2. PTES (PENETRATION TESTING EXECUTION STANDARD)



Figura 3. Símbolo de PTES

Según la página del penetration testing execution standard (web: 2014), es una guía de metodologías, guías y pruebas existentes. Su objetivo es unir lo mejor de los analistas y expertos de seguridad y realizar una guía estándar que favorezca los procesos de auditoría de seguridad más recurrentes. Usa como soporte a la metodología OSSTMM mencionada previamente, sin embargo, no depende exclusivamente de ella. Para utilizar esta metodología, el test de intrusión se realiza en 7 fases que se detallan a continuación.

- **Pre-engagement Interactions:**

Se define el alcance que tendrá el test de intrusión. Además de tendrá un acuerdo con el cliente de la profundidad o grado de impacto que tendrán las pruebas a realizar, si el test será caja negra, gris o blanca y demás puntos a destacar. (Pérez; 2012: web)

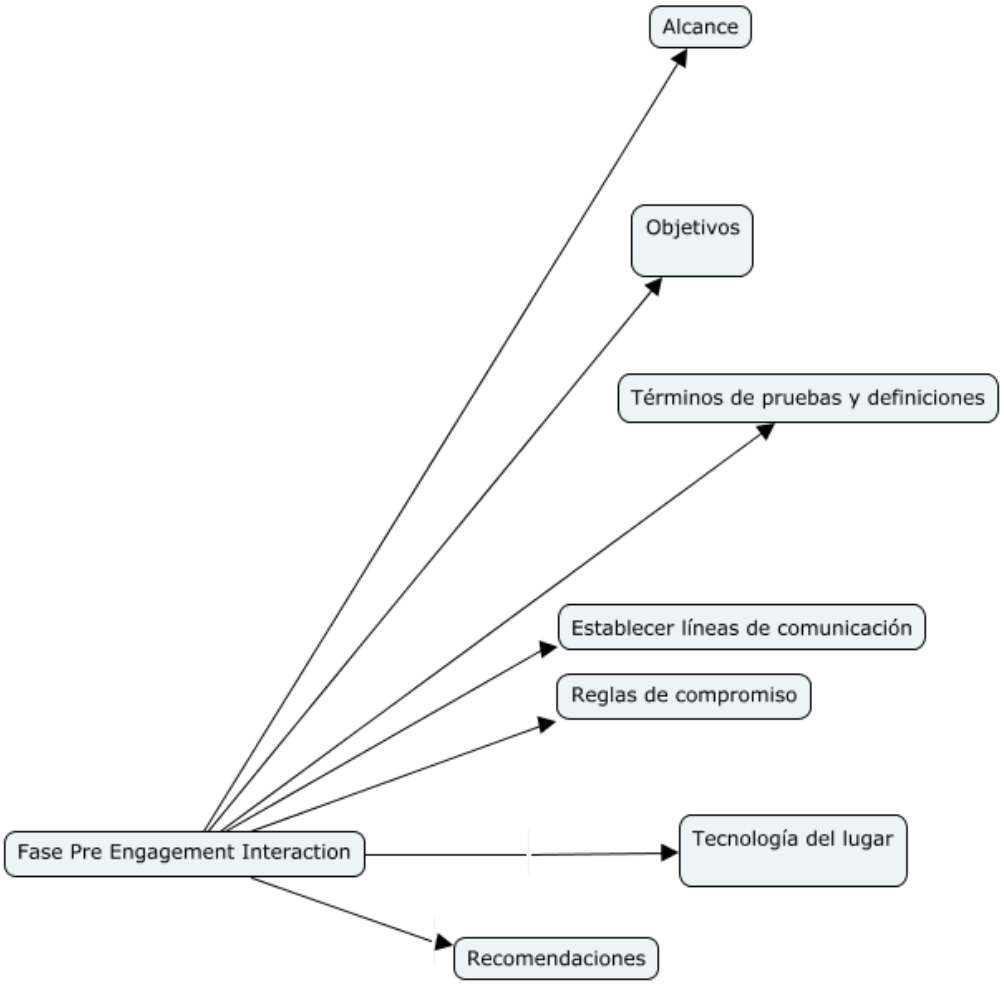


Figura 4 Interacciones pre compromiso

Autor: Oswaldo Tamayo, mayo 2016.

- **Intelligence Gathering**

Se recopilará información de inteligencia competitiva publicada en motores de búsqueda que permitirá conocer que se está estudiando y de los recursos de la empresa. Además,

incluye información del sistema, planificación de la organización, Se analiza e identifica interna y externamente a los servicios, mapeo, VoIP, protocolos que estén disponibles. Se puede profundizar en perfiles de usuario, e inclusive localización física de los empleados, uso de redes sociales. Se puede incluir aspectos competitivos como planes de marketing o visión de productos. (Pérez; 2012: web).

- **Threat Modeling**

Al obtener la información previa en las dos fases previas, se procede a definir las líneas de negocios existentes, la importancia de los activos IT que están visibles en el estudio realizado para poder definir vectores de ataques posteriores. (Pérez; 2012: web).

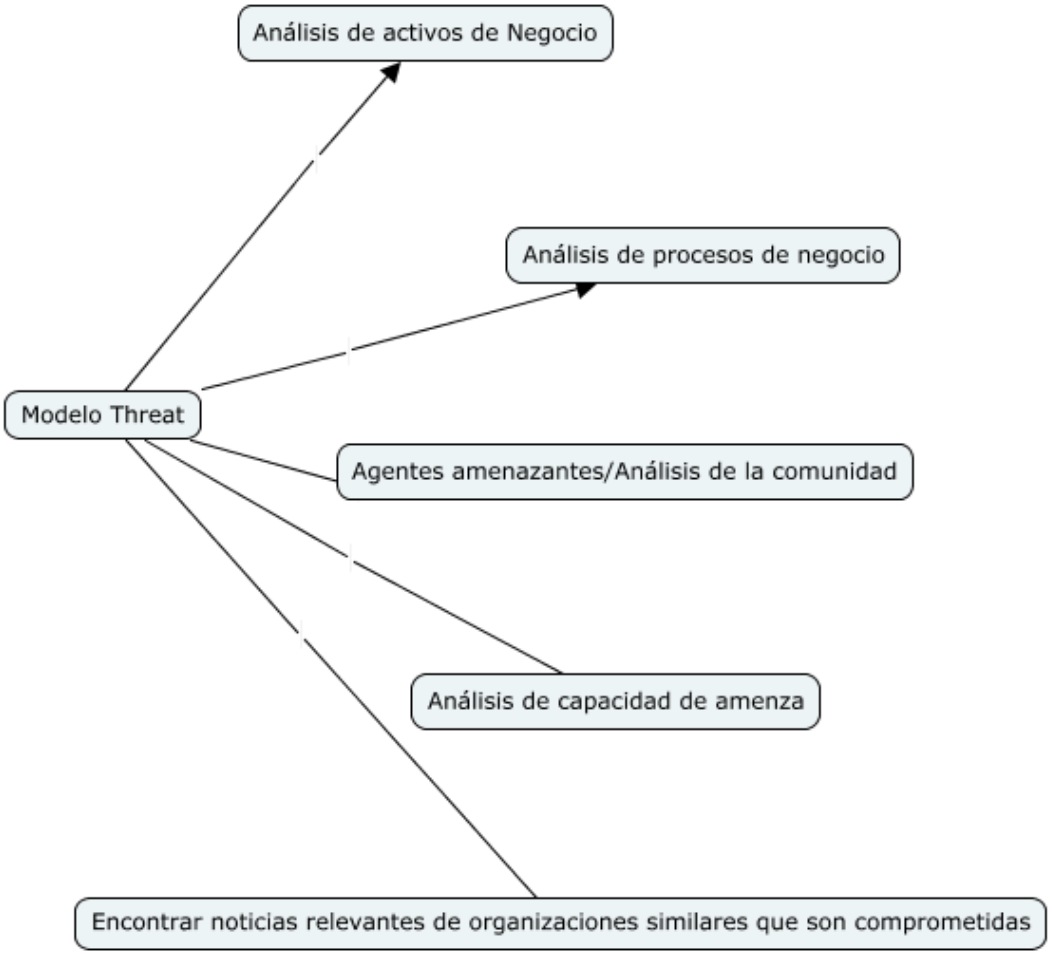


Figura 5. Threat modelling

Autor: Oswaldo Tamayo, mayo 2016.

- **Vulnerability Analysis:**

El nombre de esta fase indica que se analizarán las vulnerabilidades, de forma activa y "manipulando" el objetivo", se identifican los puertos y servicios que existen en la organización para buscar de forma manual y automática las vulnerabilidades existentes. Esta fase se divide en pruebas activas y pasivas, validación e investigación. Se recopila la información que hace referencia a servicios, redes y web scanner, VoIP entre otros. Una vez que se identifican los puertos, se analizan posibles ataques y se validan las opciones reales a

atacar y se comprueba que se puede realizar incluyendo el riesgo que esto conlleva. Existe una sub-fase de Investigación en la que se revisa todo lo encontrado en internet sobre las brechas de seguridad y vulnerabilidades.

Un consejo profesional que se debe hacer es el de la réplica del entorno de pruebas o simular pruebas en un ambiente real lo cual garantizará que toda la infraestructura no se tocará hasta asegurarse totalmente de la viabilidad y verdadero alcance de la auditoría., o que es lo mismo, se tendrá total seguridad de las medidas preventivas tomadas (Pérez; 2012: web).

- **Exploitation:**

En esta fase se incluye la evasión de host intrusión detection system o HIDS y de network intrusión detection system o NIDS, ambos son programas cuya funcionalidad es la detección de accesos no autorizados al computador y a la red respectivamente, de antivirus y demás contramedidas existentes a nivel de red o endpoint.

Se harán revisiones a todo lo probable, es decir desde el acceso físico como USB, hasta las redes Wireless, se asegurarán contramedidas de bypass una vez detectadas, cabe destacar que esto dependerá de los servicios activos que tiene la empresa. (Pérez; 2012: web).

- **Post exploitation**

La fase sirve para recopilar o almacenar ´pruebas y como poder calificarlas en el punto de vista de intrusión y hasta donde se puede “maniobrar” en el sistema comprometido.

Se analiza el borrado de huellas y se hace persistente el ataque (puertas traseras, rootkits, conexión inversa). Son demasiados los riesgos que se corre al tener una red vulnerable, es por ello que se debe hacer la pregunta: ¿Qué se pueden llevar de mi organización? Es por ello que tanto desde el área de auditoría de sistemas como de la gerencia se deben centrar esfuerzos en reforzar la infraestructura de red, asegurar elementos para restringir la salida de datos (voz, video, cintas, discos, USB), realizar backups periódicos a la documentación, etc.

Hay que prestar mayor atención a los ataques que están dirigidos a directamente al negocio como lista de clientes, copias de seguridad borradas o discos dañados, etc. Es importante tener conciencia y no escatimar recursos en la protección de elementos críticos como los mencionados. Además, la auditoría que se realizará usando esta metodología deberá ser limpia, es decir, no dejar rastro; garantizar que todo sistema sea recuperable. (Pérez; 2012: web).

- **Reporting:**

En esta fase, contiene los reportes tanto ejecutivo como técnico que se entrega al finalizar el estudio de la organización.

Los puntos relevantes en el reporte deben ser las razones por las cuales la organización solicitó el test. Después deben ir los riesgos clasificados por prioritarios. Después las métricas usadas y contramedidas propuestas para los riesgos estudiados.

A continuación, se detalla la información obtenida o robada en el estudio. Se evalúan las vulnerabilidades encontradas, y se confirman que dichas fallas fueron explotadas, junto con las contramedidas propuestas y probadas incluyendo otras contramedidas derivadas. Analizar el grado de exposición que tienen los activos de la empresa es decir si están al alcance o no de terceras personas, y calcularlo en función de su magnitud, frecuencia y riesgos derivados.

Finalmente se debe incluir un informe, el cual como se mencionó previamente debe ser técnico señalando los puntos indicados, y un informe ejecutivo, dirigido al gerente o CEO de la organización o empresa.

3.1.3. ISSAF

Esta metodología ha sido creada para evaluar o probar una red, sistemas y aplicación de controles, según Pérez (2013: web) los controles mencionados abarcan IEC/ISO 27001:2005(BS7799).

El objetivo de ISSAF es proporcionar procedimientos que sean detallados para realizar las pruebas de sistemas de información que reflejan situaciones reales.

Según Pérez (2013: web) esta metodología es usada en su mayoría para cumplir con los requisitos de evaluación en las empresas, además de que se la usa como referencia al momento de realizar nuevas implementaciones relacionadas a la seguridad en la información.

Además, se menciona en el sitio web que tiene criterios de evaluación bien definidos, los cuales han sido puestos en revisión por expertos globales de la materia.

Esta metodología usa un enfoque que en la práctica se realiza en 3 etapas o fases y se analiza o evalúa en 9 pasos. Las etapas son:

- Planificación y preparación
- Evaluación
- Informe, limpieza (borrado de rastros) y destrucción de "dispositivos".

Planificación y Preparación

Sirve para la preparación del entorno de trabajo. Antes de la planificación, cabe mencionar que se firmará con el cliente un contrato profesional en el cual se delimitan las responsabilidades y funciones. Se establece un acuerdo legal de Protección legal mutua en la que ambas partes la contratada y la contratante tienen "mutuas garantías". Se realizan reuniones de trabajo para definir el alcance del test, su enfoque y que metodología o

metodologías usar, se limitan las pruebas y se dan rutas de escalamiento y se establecen las pruebas del test. (Pérez; 2012: web).

Evaluación

En esta fase se realiza el test de penetración o intrusión definido anteriormente; este test está enfocado por capas en donde cada una de ellas tiene un nivel a detalle mayor de los activos. Estas capas se las puede definir como:

- *Information Gathering (Obtención de información)*

  En esta capa se exploran las posibilidades de ataques, los cuales podrían ser dentro de la red o fuera de ella. Es válido cualquier documento, que podría comprometer los sistemas; se sugiere inclusive: emails, teléfonos, información personal, empleados, socios de negocio, implementación de tecnologías, bloqueo de propiedad de IP (de manera que se desconozcan los datos precisos sobre los dueños de dominios).

  Tiene gran similitud con OWASP y con PTES, pero ISSAF además de detallar las capas, explica ejemplos de herramientas de posible uso muchas de las cuales son recomendadas por expertos (dig, nslooup, nmap etc.). (Pérez; 2012: web).

- *Network Mapping (Análisis de la red de datos)*

  Es una de las capas más técnicas de las mencionadas, el denominad mapeo de red incluye análisis de topologías de red, routers, dispositivos de red, firewalls, nombre de los hosts, servidores y puertos activos en los ordenadores, Netbios, que uso determinado tienen, los sistemas operativos de uso, las cuentas y privilegios de estas, entre otros factores.

- *Vulnerability Identification (Identificación de vulnerabilidades)*

  En esta fase se profundiza más acerca de los sistemas que son objetivos. Es decir, todas las herramientas y técnicas de intrusión masiva como nikto, nessus, opnevas, whisker entre otras, estarás preparadas para el despliegue. (Pérez; 2012: web).

Entre la planificación entran los siguientes ítems dados en el siguiente orden:

- Servicios vulnerables
- Ajuste de scanner a vulnerabilidades
- Identificación de fallas desconocidas o errores en las vulnerabilidades
- Listas de vulnerabilidades
- Medidas inmediatas de minimización de fallos
- Clasificación de riesgos técnicos en función de las vulnerabilidades encontradas.
- Impactos probables

Una de las recomendaciones de la metodología ISSAF es clasificar las vulnerabilidades de acuerdo a su riesgo, y asignarlas un color, por ejemplo:

Si es de riesgo bajo: color azul, riesgo medio: color naranja y si el riesgo es considerable o alto será de color rojo.

Después de haber clasificado las vulnerabilidades, es recomendable realizar una matriz en la que se establece el riesgo por color y el impacto que se supone tendría en los activos de la empresa. (Pérez; 2012: web)

- *Penetration (Penetración o entrada)*

  En esta fase se realizan pruebas de concepto para, las cuales son hechas a la medida por el hacker ético usando código y herramientas señaladas.

- *Gaining Access and privilege escalation (Obtener acceso y escalado de privilegios)*

  Se ganan u obtienen privilegios de usuario, los cuales van desde el más elemental hasta el usuario root, ya que de esta forma se pueden controlar y manipular los archivos de los sistemas y a los mismos. Es por ello que se prueban todos los usuarios posibles.

- *Enumerating further (Lista de objetivos)*

En esta fase se realizan ataques a las contraseñas, se capturan los paquetes del tráfico de red y se analiza con las "cookies" o el historial de búsqueda, también se incluyen a direcciones de correo, routers y redes.

- *Compromise remote users/sites (Sitios y usuarios remotos comprometidos)*

  El auditor tratará de manipular todos los sistemas al tener el mayor número de contraseñas, esto lo realizará dentro o fuera de la red objetivo. En esta fase, se usará firewall en escritorios remotos de los usuarios para de esta forma evitar tener vía libre a cualquier parte de la red. (Pérez; 2012: web)

- *Maintaining Access (Mantenimiento de los privilegios y accesos obtenidos)*

  El objetivo es que el control a los sistemas comprometidos sea eficaz y sobre todo pase desapercibido para el resto de los usuarios y/o administradores. Se usan canales disimulados o secretos. Para elegir la forma de comunicación encubierta, se usará SSL túneles, proxys, ssh entre otros. La forma más general de control oculto de varias máquinas es mediante troyanos, backdoors, rootkits. (Pérez; 2012: web).

- *Covering Tracks (Borrado de huellas)*

  Un crimen nunca es perfecto, pero por lo menos intentarlo vale la pena, es por ello que en esa fase se trata de cubrir todas las pistas, se usan los métodos de ocultación de pruebas, de keyloggers, herramientas, exploits, archivos etc. Se ocultan carpetas en los sistemas Windows y GNU/Linux. Se limpian los logs si es que no están replicados, o se los manipula. (Pérez; 2012: web).

  La siguiente imagen, muestra las áreas que hay que tomar en cuenta en la fase de evaluación. Cabe destacar que es son cíclicas e iterativas.

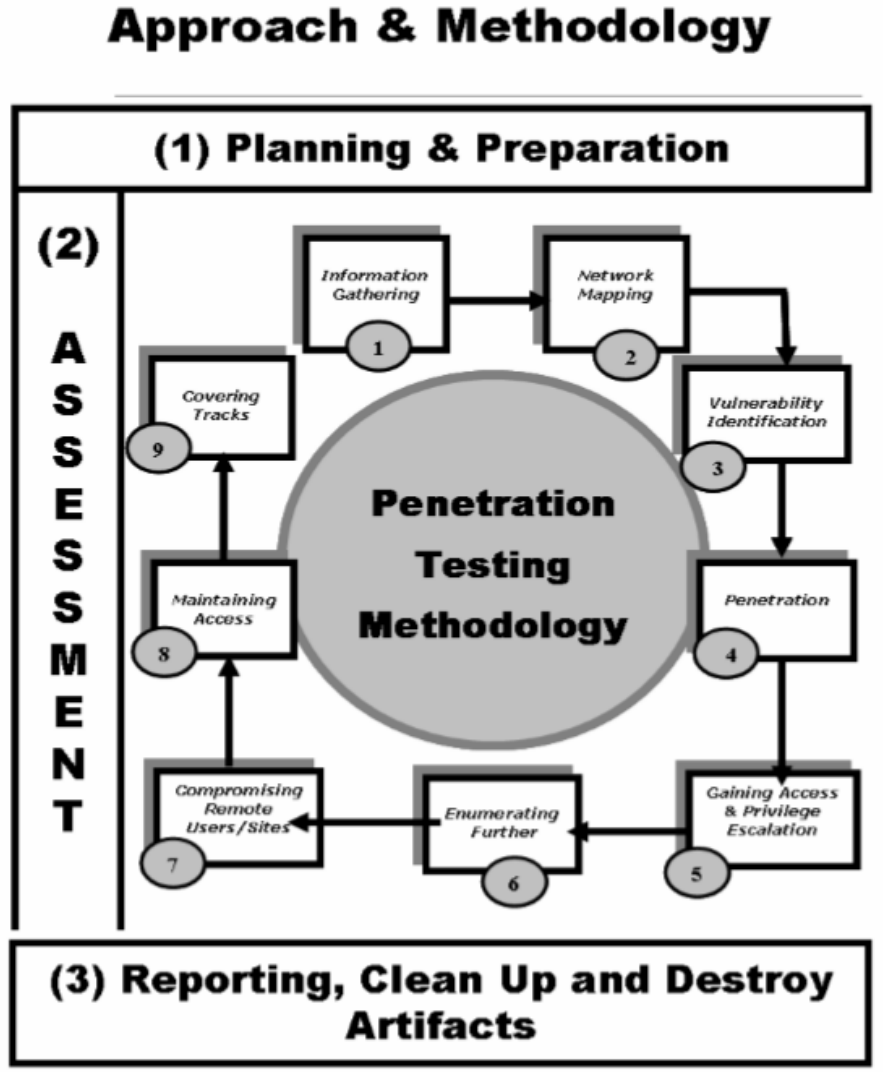


Figura 6. Fases de evaluación ISSAF

Fuente: dataceta.unad.edu.co

Informe, limpieza (borrado de rastros) y destrucción de "dispositivos"

Es la fase final de la metodología en la cual se deben realizar dos tipos de informes:

- Verbal

  Solo se informa si existe una o varias vulnerabilidades graves, es decir que afectan considerablemente la línea de negocio de la organización. (Pérez; 2012: web)

- Informe final

  Es una descripción detallada en la cual van apartados como:

  - Resumen del trabajo llevado a cabo.

- Alcance global del proyecto.
- Herramientas utilizadas
- Fechas de los test a los sistemas incluyendo las horas.
- Conclusiones respecto a los test diseñados
- Informe especifico de las vulnerabilidades encontradas
- Medidas preventivas relacionadas con las vulnerabilidades mencionadas.
- Listado de los puntos de intervención. Tanto de las mejoras como de futuras propuestas de solución.

3.1.4. OSSTMM (Open Source Security Testing Methodology Manual)

Es una metodología considerada un manual debido a que es muy detallada a pesar de no ser tan extensa. Es constantemente actualizada, y su última versión es la 4ta, sin embargo, la 3ra es la que se usa debido a su estabilidad. Cabe destacar que no existe una traducción oficial al idioma castellano.

Según su página oficial (OSSTMM, 2016: web) su diseño se pueda repetir varias veces, además ofrece al mismo tiempo estrategia, test de evaluación, medidas de riesgo y valoraciones intrínsecas en función de resultados de los test.

PASOS PARA DEFINIR UN TEST DE SEGURIDAD:

Son 7 los pasos para definir las pruebas que realizará el analista, definidas a continuación:

- Definir los mecanismos de control los cuales son controles que, pondrán a prueba los activos que se quiere proteger.
- En esta metodología existen “zona de acuerdos”, alrededor de ésta, existen procesos, mecanismos y servicios que protegen los activos, es por ello que es primordial identificarla.

- Definir la zona externa la cual es necesaria para proteger las operaciones de los activos. Es decir, definir el alcance del test.
- Definir el alcance del test, si este interactuará dentro o fuera de la empresa. Los vectores indicarán las direcciones de la interacción, los cuales pueden ser dentro-fuera o viceversa, dentro-dentro o fuera-fuera. A cada vector se lo debería realizar pruebas por separado y de poca duración.
- Tomar decisiones acerca de que equipamiento es necesario en cada test a realizar. En La interacción entre vectores puede pasar en varios niveles; los cuales pueden ser varios, pero se han separado a 5 canales por función, y cada canal deberá ser probado separadamente por cada vector.
- Hacer un plan acerca de que información se quiere extraer en cada prueba. Y se realiza un plan de los test que se realizarán.
- Asegurarse que las pruebas que se realizarán, cumplan las reglas de Acuerdos o contratos previos, ya que es importante no crear malos entendidos o falsas expectativas.

Tipos de test de Seguridad:

Según la página de la OSSTMM, (2016: web), elegir el tipo de test de seguridad no significa que será orientada solo para esta metodología, es decir en la práctica se puede individualizar las pruebas. Es decir que, para seguir la metodología, su aplicación y su técnica, se reflejará en el tipo de test que se haya elegido. Estos podrían ser:

- Blind (a ciegas): es cuando el ethical hacker o auditor, interactuará con el objetivo sin tener conocimiento de las defensas, canales (vías de acceso) o activos. El tipo de test será un desafío para el propio auditor ya que dependerá de su nivel de preparación.

- Double blind: o técnica black box, ya que no se tiene idea de lo que se puede encontrar. Se desconoce todo del objetivo y se lo probará de forma brusca varias veces. Igual que el tipo de test previo, depende mucho del nivel de preparación del auditor.
- Gray box: en este tipo de test, el hacker conoce todo acerca de los canales (vías de acceso). Es posible determinar el alcance del test. La eficacia de este test radica en la calidad de información que ha aportado el auditor, inclusive antes de finalizar las pruebas.
- Double gray box: o White box, en la cual el auditor, tiene conocimiento limitado de las defensas y activos, pero tiene un conocimiento total de los canales. Se diferencia del test previo en que no solo depende de la calidad de información recibida, sino del grado de recepción del objetivo.
- Tándem: el auditor forma parte del equipo de seguridad y de control de procesos. Tanto el cliente como el auditor saben los términos de la auditoría. Se probarán los controles aplicados, así como proteger el objetivo con test reales. El éxito depende de la meticulosidad en la que se preparan los test para tener una visión general de estos y de sus respuestas.
- Reversal o reversible: en este test, el proceso dependerá del grado de creatividad y conocimientos del hacker. Este además tiene conocimiento completo de toda la operación de la empresa. Además, el cliente no sabe en qué momento como ni con qué y cuándo se realizarán las auditorías.

  El hacker ético deberá informar en un reporte sobre el o los test que utilizó. (OSSTMM, 2016: web)

Alcance (Scope):

Son 3 las vías de acceso o canales que comprende el alcance, las cuales son posibles valga la redundancia, vías de actuación e interacción:

Seguridades de comunicaciones o COMSEC, Seguridades físicas o PHYSSEC, y las Seguridades Espectro o SPECSEC.

Si se requiere una auditoría meticulosa, se deberá profundizar en los 3 canales, es decir dependerá de la pericia del auditor y su equipamiento y medios. La metodología profundiza estos 3 canales en 5 secciones lógicas:

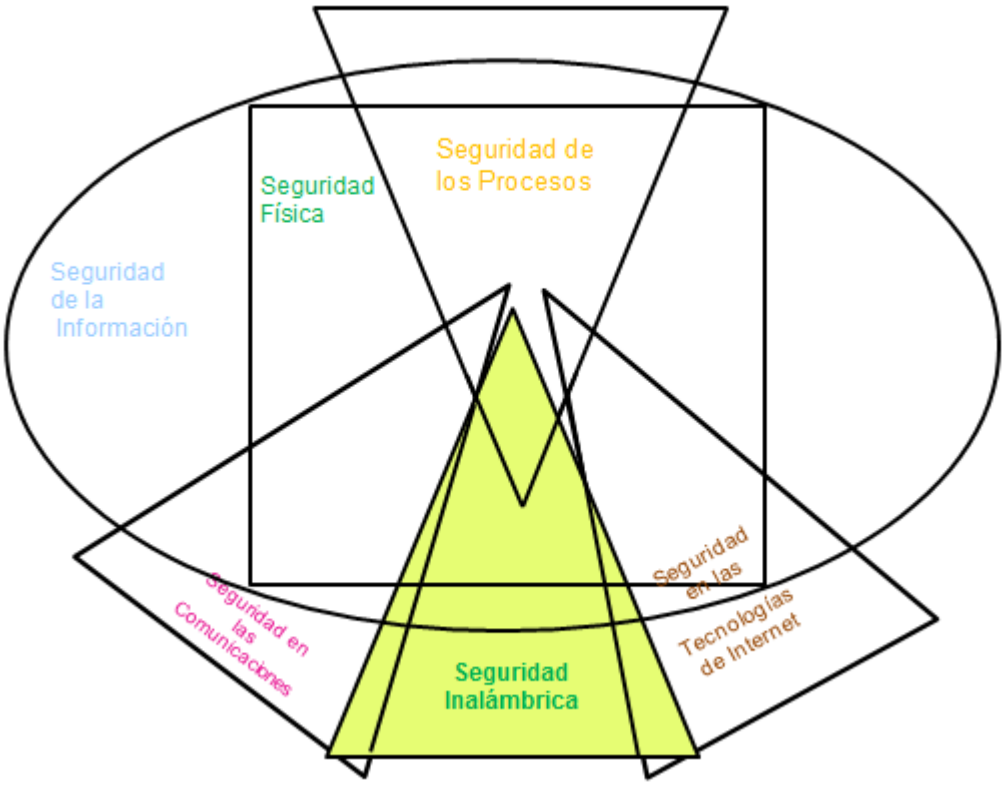


Figura 7. . Canales y secciones de la metodología ISSAF

Fuente: datateca.unad.edu.ec

A continuación, se detalla a mayor nivel los canales y las secciones referidas:

Tabla 5: Canales y secciones de OSSTMM

CANAL	SECCIÓN	DESCRIPCIÓN
Entorno físico	Humano	Es la parte de la interacción con el usuario, la cual puede ser física o psicológica.
	Físico	Son elementos tangibles donde se requiere del trabajo físico o de un transmisor de energía para la manipulación. Se realizan pruebas de seguridad física a los canales los cuales son físicos y no electrónicos. (OSSTMM, 2016: web) (OSSTMM, 2016: web)
Entorno inalámbrico	Comunicaciones inalámbricas	Son de 3 tipos: - ELSEC que son comunicaciones electrónicas. - SIGSEC o comunicación por señales - EMSEC o aplicar técnicas que evitan emanación de señales de radiofrecuencia.
Entorno de comunicaciones	Redes de datos	Conformada por todos los sistemas y redes de datos cableadas.
	Telecomunicaciones	Comunicaciones telefónicas, analógicas o digitales sobre redes de líneas.

Autor: Oswaldo Tamayo, junio 2016

Contratos o Reglas de Acuerdos:

En este apartado, esta metodología es bastante prolija al respecto debido a su ética en cada detalle; es decir los requerimientos detallados en el contrato no ofrecen más de lo necesario tanto para el cliente como para el auditor.

El alcance del trabajo debe estar definido perfectamente antes de realizar la auditoría. Además, la planificación de cada prueba debe ser hecha para cada uno de los miembros del equipo de trabajo o si es el caso del auditor encargado.

Resultados de los test:

Estos resultados van acompañados de las soluciones recomendadas. Algunas empresas de ethical hacking las usan como valores añadidos en el trabajo, pero no son obligatorias. Inclusive, el dar soluciones no forma parte de realizar auditorías en la metodología OSSTMM.

Según esta metodología y su página web (OSSTMM; 2016: web), para elegir el test más adecuado para cada empresa, es importante comprender como están diseñados los módulos para trabajar. Depende el tipo de negocio de la organización, el tiempo disponible, los requerimientos de la auditoría, es entonces que después de tener en cuenta todos estos puntos, el auditor podrá planificar y distribuir detalles de la auditoría por fases.

La metodología tiene 4 fases de ejecución:

- ✓ **Fase regulatoria**

Se toma la decisión de qué tipo de pruebas se realizarán, teniendo en cuenta los límites de la auditoría, requerimientos del cliente, las restricciones y lo que se quiere alcanzar.

- ✓ **Fase de definiciones**

Definido lo que se quiere alcanzar, se tiene constancia real de la definición precisa y clara del alcance que tendrá la auditoría.

- ✓ **Fase de información**

La mayoría de las auditorías se realizan o cubren información no contemplada. Se sacará a relucir en esos casos a los activos mal ubicados, desatendidos y mal gestionados.

- ✓ **Fase interactiva de prueba de controles**

Por lo general es la fase final de los test. En ella se asegura el grado de las perturbaciones o ataques, el efecto de la información extraída, la cual no puede ser dada a conocer hasta

que otras fases hayan sido llevadas a cabo. Además, se debe verificar que las conclusiones son reales.

3.1.5. Análisis comparativo de las metodologías analizadas

Después de haber analizado a mayor detalle las distintas metodologías que existen, es importante poder compararlas para de esta forma tener más claro que ofrece cada una de ellas, sus ventajas, desventajas, organizaciones a las que están enfocadas, facilidad y otros puntos que serán reflejados a continuación:

Tabla 6: Comparativa de Metodologías de Ethical hacking

Métodos \ Patrones (Ítems)	ISSAF	PTES	OWASP	OSSTMM
Niveles de detalle	No tiene elementos de cloud computing y protección de datos. Es muy detallada pero a la vez muy sencilla	Sus procesos están detallados y definidos correctamente, sin embargo desde su última actualización no se tienen novedades.	Ayuda al auditor en la ejecución de su trabajo, a pesar de estar enfocada al ámbito web, eso no le quita meticulosidad	No es tan detallada como las anteriores, ya que se basa en la formación previa del auditor antes de la ejecución como tal de los requerimientos
Rigor de la metodología	Desactualizada, última versión 2006. Alto rigor	Desactualizada, última versión 2008. Alto rigor	Muy alto rigor, en constante actualización, a pesar de ser enfocada a web, sirve como instructivo.	Actualizada constantemente, alto rigor.
Facilidad de uso	Se puede utilizar con conocimientos medios. De fácil uso	Alta facilidad de uso, requiere de capacitación previa	A pesar de ser muy técnica, existen varios ejemplos prácticos. Alta facilidad de uso.	Su facilidad de uso es media. Requiere que el auditor tenga entrenamiento y certificaciones., es muy técnico.
Entornos de aplicabilidad	Aplica más en servidores IBM, sin embargo es genérico.	Al combinarse con la metodología OWASP resultaría ideal	Se enfoca a servidores web. Debido a la orientación de esta metodología.	Debido a ser una metodología dinámica, se aplica a servidores inclusive inexistentes.
Ámbitos de aplicación	Aplicada a PYMES	Organizaciones financieras complejas y PYMES orientadas a finanzas	Aplica a todas las organizaciones que usen aplicaciones web	En general para organizaciones grandes y PYMES.
Uso por los hackers éticos	Es de fácil aprendizaje, además de cubrir las principales etapas de una auditoría usando test de intrusión. Respeta los modelos NIST.	No es usado por la mayoría de profesionales por sí solo, sino lo combinan con otras metodologías.	Es de gran uso, sobre todo para complementarlo con otras metodologías. Lo importante de esta metodología es que está en constante revisión y mejoramiento.	Quizás la metodología más usada, sin embargo, varios profesionales la modifican para su propio uso, simplificándola. Por lo general su uso supone alto conocimiento y experiencia en el tema.
Ventajas	Su fase de evaluación es conocida. Permite la facilidad en la creación del informe en función de los pasos seguidos y la data obtenida. Además recomienda herramientas para la evaluación.	Su similitud hace que se la relacione mucho con la metodología ISSAF. Están muy bien definidos los controles en el test de intrusión.	Gran facilidad en el uso de los más conocidos controles. Es bien estructurada y está al tanto de auditorías de la web centradas en el marketing del negocio. Al culminar la auditoría, propone le uso de herramientas. Inclusive al ser una metodología práctica, sirve como modelo de aprendizaje de fundamentos de pentesting.	Posee mucha documentación, y soporte de una comunidad a nivel global. Además, tiene guías de uso. Pone gran énfasis en los estándares de seguridad de información. Además de su alto grado de calidad en los resultados.
Desventajas	- No tiene límites de uso en los test, por ende, los acuerdos de uso con el cliente tienen alto déficit. - Al no tener estabilidad en sus test de intrusión, su nivel de desarrollo es inmaduro en cuanto a la práctica en sí. - No está actualizado.	Sirve como metodología de consulta sin embargo al no ser un proyecto consolidado ni completo no proporciona mayores ventajas.	Al no existir otras metodologías orientadas a auditorías web, es difícil compararla. Además cabe destacar que los servidores e infraestructura web no es auditada.	- No permite combinarse con otras metodologías. - Se basa más en la experiencia del hacker debido a que no hace referencia el tipo de objetivo de cada test.
Opinión personal	Su uso es fácil y cualquier hacker con o sin experiencia puede usarla, sin embargo, no está actualizada. Es una	Tiene un buen nivel de precisión de vulnerabilidades, que al ser combinada con otra metodología se	De las estudiadas en el capítulo, es la menos agresiva y como consecuencia sus test de penetración menos intrusivos. Se	Al contrario de la metodología ISSAF, sus límites aplicados en los acuerdos con los clientes permiten tener límites en su uso. Es muy agresiva

	metodología agresiva por ende intrusiva en alto nivel.	incrementa. Es muy detallada y al igual que la metodología OWASP, es muy buena para el aprendizaje.	pueden borrar las huellas al aplicarla muy fácil.	e intrusiva. No propone un listado de herramientas sugeridas.

Autor: Oswaldo Tamayo, junio 2016.

3.2. Herramientas del hacker ético

Cada una de las herramientas analizadas a continuación, tiene su software utilizado, y método de uso, las más importantes se mencionan a continuación.

3.2.1. Footprinting

Según PeritoIT (2012: web), footprinting es el análisis de la seguridad de la empresa, en el caso a estudiar serán las pequeñas y medianas empresas, pero se aplica para todo tipo; para realizar footprinting, no es necesario basarse en una sola metodología, escenario que resulta ideal si no se domina una de las mencionadas, usando esta herramienta, el hacker podrá llegar a su objetivo de diversos modos, pero de forma prolija, al finalizar su uso, se puede encontrar información perteneciente a varias capas de red como detalles del dominio, su nombre, direcciones de red, servicios de red algunas direcciones IP específicas entre otras.

Es tan amplia la herramienta, que usa otras herramientas valga la redundancia. Según Calles y González (2011: web), éstas pueden ser:

- ✓ **DNS stuff**

  Sirve para realizar búsquedas en la base de datos de la herramienta whois, que se estudiará a continuación, para poder encontrar data de la empresa a analizar, como los puntos de contacto.

  Además, se pueden hacer consultas, mediante dirección IP para usar información de división de subredes.

- ✓ **Whois**

  Es un tipo de protocolo TCP, que se basa en preguntas y respuestas para de ésta forma consultar datos como nombre de un dominio, hasta una dirección IP. Estas consultas se realizan mediante líneas de comando. Existen varias páginas web que se prestan para esta técnica como

✓ **Netcraft**



Site report for www.[redacted].com

Site	http://www.[redacted].com	Last reboot	unknown Uptime graph
Domain	[redacted].com	Netblock owner	Prima S.A.
IP address	201.212.[redacted]	Site rank	unknown
Country	AR	Nameserver	ns1.afraid.org
Date first seen	April 2008	DNS admin	dnsadmin@afraid.org
Domain Registrar	unknown	Reverse DNS	mail.[redacted].com
Organisation	unknown	Nameserver Organisation	Joshua Anderson, 4120 Douglas Blvd #306-199, Granite Bay, 95746, United States
Check another site:			

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
Prima S.A. Buenos Aires	201.212.[redacted]	unknown	Apache/1.3.34 Debian mod_accounting/0.5 PHP/5.2.0-8etch16 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	27-Oct-2012
Prima S.A. Buenos Aires	201.212.[redacted]	Linux	Apache/1.3.34 Debian PHP/5.2.0-8 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	6-Sep-2010
Prima S.A. Buenos Aires	201.212.[redacted]	Linux	Apache/1.3.34 Debian PHP/5.2.0-8 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	10-Jun-2010
Prima S.A. Buenos Aires	201.212.[redacted]	Linux	Apache/1.3.34 Debian PHP/5.2.0-8 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	16-Dec-2009

Figura 8 Página web de Netcraft

Fuente: Calles y González (2011: web)

✓ **IP-Adress**

Se puede conocer la dirección IP que está asociada a un dominio.



[redacted].com website research report available below. Detailed information includes the server IP Address is 201.212.[redacted] and [redacted].com resides on Prima S.A. in Rosario, 21, Argentina. The domain [redacted].com was first registered on 09/28/2007 which was 5 years and 2 months ago!

[redacted].com whois shows that the registrar is DATTATEC COM DE IRAZOQUI VERONICA PALMIRA - but a full analysis for [redacted] is below.

The official title of [redacted].com is: [redacted]

Feel free to comment on this [redacted] website report using Facebook below!

[redacted].com Whois

Registrar
[redacted] COM DE IRAZOQUI VERONICA PALMIRA

Whois Server
whois.[redacted].com

Referral URL
http://www.[redacted].com

Status
ok

Contact Email
supacha5818[redacted].com.ar

Creation Date
09/28/2007

Updated Date
11/02/2012

Expiration Date
09/28/2017

Figura 9 Página web IP-Adress

Fuente: Calles y González (2011: web)

3.2.2. Scanning

Es el escaneo de puertos, el cual sirve para reunir información posible de los puertos abiertos. Según Giménez (2011: web), es una de las herramientas más usadas para el reconocimiento que usan todo tipo de hackers. Los puertos pueden ser clasificados en tres tipos:

- ✓ Del 0 al 1023 son conocidos
- ✓ Del 1024 al 49151 son registrados
- ✓ Del 49152 al 65535 son privados o dinámicos

Si bien es probable escanear puertos 65635 los atacantes no se enfocan en ellos sino en los denominados “conocidos”.

Por lo general el proceso se refiere a puertos de tipo TCP, el cual es un protocolo de estado de la conexión que reconoce o provee información valiosa al atacante. Gregg en su libro” The network security test lab” (2015: web) destaca que una de las desventajas de escanear un puerto, es la generación de un log de error de aplicación por cada puerto escaneado, o lo que es lo mismo que se genera un reporte debido a que detectan una conexión entrante, sin embargo, no reciben ningún dato del atacante. Así mismo Gregg (2015: web) destaca a los principales complementos de scanning:

- Pinger
- THC Scan, THC Amap
- Ping
- NMap (Network Mapper)
- Nessus, NeWT (Nessus Window Technology)
- LANguard
- VLAD

3.2.3. Keyloggers (Grabadores de escritura de teclado)

Son dispositivos que pueden ser software o hardware los cuales monitorean todo tipo de actividades. Si son hardware, se instalan como complemento del teclado, es decir, tranquilamente pueden estar instalados en la parte posterior del computador sin poder detectarse. Si es un software, estarán ubicados entre el teclado y el sistema operativo, su modo de operación es enviar al correo todo lo que se digite, esta dirección estará preestablecida. (Giménez, 2011: web).

CAPÍTULO 4

GUIA PARA APLICAR ETHICAL HACKING EN PYMES

Basados En las características de las PyMES, donde la información manejada depende mucho de cuanto está dispuesta la empresa en invertir, crecer y de su manejo de las TIC´s, es recomendable aplicar ethical hacking guiándose de los siguientes pasos, cabe destacar que, son los pasos más comunes, tomando el ejemplo en la empresa no quiere invertir mucho en Tics y que no cuenta con un personal especializado en tecnología, dicho esto los pasos serían:

1. Aplicar los procesos comunes:

   1.1. Preparación del equipo de trabajo necesario y cronograma de actividades.

   1.2. Elaboración del test en el tiempo estimado.

   1.3. Análisis de resultados y preparación del reporte

2. Entrega del reporte.

   Este puede ser de dos tipos:

   - Técnico
   - Gerencial.

Después de realizar el análisis de la empresa cliente, independientemente de la metodología que se use, como se mencionó previamente, es importante elaborar dos tipos de informes, los cuales corresponderán al cliente, el uno sería técnico enfocado al jefe o gerente de tecnología de la organización, y el segundo a nivel gerencial, sin tanto tecnicismo, sino resumido en las soluciones a tomar. Cabe destacar que ambos informes, se centrarán en el listado de las vulnerabilidades encontradas y de las posibles soluciones a tomar, desde el punto de vista de un hacker.

El informe a nivel de gerencia, deberá ser preciso y sin muchos tecnicismos, sino siendo preciso en lo que se requiere mejorar y solucionar. A diferencia del informe técnico en el

que se resaltarán configuraciones erróneas, protocolos de seguridad vulnerados, tipos de sistemas operativos a utilizar y demás componentes de seguridad.

Lo trascendental en el informe, será la confidencialidad debido al contenido del mismo, si este cae en manos de la ciberdelincuencia, puede llegar a ser motivo de pérdidas económicas importantes y de bienes intangibles irrecuperables como lo es la información. Por ello al momento de firmar el contrato, ambas partes deberán acordar como realizar la entrega del informe.

El capítulo sirve para indicar la estructura y características de un informe, para que el resultado mostrado y entregado cumpla con las exigencias del cliente y sirva como base de protección. Además, se incluyen los procesos comunes de ethical hacking.

4.1. Procesos comunes en Ethical Hacking

Existen procesos generales que independientemente de la metodología escogida o usada, los cuales son:

- Preparación del equipo de trabajo necesario y cronograma de actividades.

  Es necesario tener el equipo de trabajo listo con el cual se va a brindar el servicio, el mismo deberá tener la experiencia requerida y brindar las prestaciones requeridas para desarrollar el análisis de vulnerabilidades. Dependiendo de la necesidad y de que tan grande sea el proyecto, dependerá el número de recursos humanos y tecnológicos a utilizar, el personal comúnmente está conformado por un líder técnico que sirve como guía en el proceso, dando cargos a los demás miembros y asignando responsabilidades o tareas.

- Reuniones previas con el cliente destacando las necesidades del test.

  Sirve para analizar los principales inconvenientes y se tomará una decisión de cómo se trabajará. No se realizará una reunión técnica sino una explicación práctica para todos

los integrantes de la junta. Se definirá el alcance del proyecto, dando relevancia a los principales puntos. Además, se estimarán los tiempos de finalización de los entregables si entran en el caso, o del informe final.

- Preparación y elaboración de acuerdo de confidencialidad y autorizaciones.

Al iniciar el proyecto, es clave la realización de un documento de garantías necesarias para ambas partes. El cual detalla el alcance de la evaluación, las tareas a realizar durante el proyecto. Este documento deberá estar al alcance del ethical hacker para prevenir inconvenientes con el personal de la empresa.

- Elaboración del test en el tiempo estimado.

Depende del acuerdo entre el cliente y la empresa contratada, la cual deberá regirse a los tiempos que se establecieron entregarse los resultados parciales y el informe final. Debido a que siempre existen retrasos en las entregas, es importante la comunicación con el cliente, explicando las causas de la demora. Es importante tener una constancia en la comunicación y motivos; por ello es recomendable usar el correo electrónico.

- Análisis de resultados y preparación del reporte.

Esta etapa es interna, ya que el equipo de trabajo realizará su diseño análisis y reportará al jefe o líder del grupo para que este consolide todas las tareas en las cuales se encuentran las fallas encontradas y prepare el informe final que será entregado al cliente.

- Entrega del reporte.

En el reporte deben constar todos los entregables previos destacando el alcance que se estableció en la primera reunión y en el acuerdo firmado por ambas partes. Además, se detalla la forma en que se manejará la confidencialidad de la información y los tiempos estimados que tomará la realización de cada ítem del análisis.

AL finalizar el proyecto, se entregará un informe con los resultados obtenidos, que se lo entregará a la empresa contratante, detallando las vulnerabilidades y sus soluciones detalladas, para evitar fallos de seguridad a corto y largo plazo.

A continuación, se muestran los pasos para realizar pruebas de ethical hacking en la siguiente tabla:

Tabla 7: Proceso de pruebas de ethical hacking

PROCESO PARA REALIZAR PRUEBAS DE ETHICAL HACKING		
Nro.	Nombre del proceso	Descripción
1	Firma del contrato	Requisito indispensable para elaborar las pruebas, se muestran fechas de inicio y finalización
2	Establecimiento de reglas de operación	Un ejemplo puede ser: -no ejecutar pruebas maliciosas o que causen daño en la organización. -No instalar software de puertas traseras en los equipos. -No cubrir las huellas después de ejecutar algún acceso no autorizado.
3	Planificación del ataque	Fecha en que se realizarán las pruebas de intrusión
4	Recopilación de información	Se recopilaron datos mediante uso de herramientas como Footprinting
5	Scanning	Se utilizaron herramientas asociadas al Scanning como Nmap entre otras.
6	Obtención de acceso	Mediante herramientas de Windows hacking
7	Cubrimiento de huellas	Depende del acuerdo en la firma de contrato, por lo general se establece que se borre o no las huellas de las pruebas realizadas.
8	Elaboración del informe final	Presentación de vulnerabilidades encontradas, seguido de posibles soluciones

Autor: Oswaldo Tamayo, mayo 2016

4.2. Reporte final

Es la parte final, en la que la empresa o persona contratada después de analizar la situación de la empresa contratante en ámbitos de seguridad informática, entrega un informe con las vulnerabilidades que se encontraron, desde el punto de vista de hackers.

Como se mencionó al inicio del capítulo pueden ser dos tipos dependiendo el caso, uno para el administrador de seguridad, y otro a nivel gerencial, siendo más preciso en lo que se debería buscar solucionar. Destacando siempre la confidencialidad debido a la sensibilidad de la información.

4.2.1. Estructura del reporte de Ethical Hacking

- ✓ **Datos del responsable**

  En esta sección del informe se colocan los datos personales de la empresa y del analista responsable, así como puesto en que se desempeña. El formato puede ir en el siguiente orden:

  - Nombre de la empresa
  - Nombre del analista responsable
  - Dirección de la empresa y número telefónico.

- ✓ **Tiempo establecido**

  Se relaciona directamente con las fechas de inicio y finalización del test realizado en la empresa cliente. Los tiempos se quedaron establecidos salvo algún cambio importante en el que estén de acuerdo ambas partes. Los datos que pueden ir en el informe al respecto serían:

  - Fecha de inicio del análisis
  - Fecha de inicio por requerimientos o tareas específicas.
  - Fecha de finalización del análisis.

- ✓ **Tipo de test realizado**

  Debido a que existen diferentes tipos de test, es común que en la estructura del reporte se mencione que tipo de test se realizó, el cual como se mencionó en el capítulo 2, puede ser:

- ✓ Caja negra
- ✓ Caja blanca
- ✓ Caja gris

- ✓ **Metodología utilizada**

  Este ítem, depende mucho de la metodología de trabajo que la empresa que realiza ethical hacking, la cantidad de especialistas que disponga en determinada metodología, si domina o no dicha metodología y la experiencia en trabajar con ella. Es importante, además, definir la metodología junto con el acuerdo de trabajo ya que en este documento se puede saber la orientación del test, ya sea a una aplicación web o las diferentes redes de datos.

  Las metodologías pueden ser:

  - OWASP
  - PTES
  - ISSAF
  - OSSTMM

  Como se mencionó en el capítulo previo, las metodologías tienen las siguientes fases, dependiendo de cada una de ellas las denominan de diferentes formas, sin embargo, son las siguientes como se muestra en la siguiente tabla:

Tabla 8: Fases comunes de ethical hacking

FASE	DESCRIPCIÓN
Reconocimiento	Obtención de la mayor cantidad de data del objetivo, la cual puede ser activa o pasiva. La manera activa es el análisis de tráfico y de forma pasiva es realizar el proceso de ingeniería social sobre empleados de la empresa
Escaneo	Se identifican los sistemas que se ejecutan y que están activos en el sistema. Se obtiene información de los usuarios, carpetas compartidas que por lo general se usan en las pequeñas empresas, el objetivo es un mapa detallado de los usuarios, servicios, máquinas y privilegios.
Obtención de Acceso	Se aprovechan las vulnerabilidades que se encontraron en los pasos previos, acceder a la red de datos de la empresa y alterar su información.
Mantenimiento de Acceso	Para poder acceder al sistema nuevamente, se carga un software malicioso. Es similar a instalar una puerta trasera en una casa.
Borrado de Huellas	En esta fase se borra o esconden las modificaciones en los archivos del sistema, ya que si son rastreados, los administradores de red pueden aumentar las seguridades de la empresa e impedir la culminación del test.

Autor: Oswaldo Tamayo, junio 2016.

- ✓ Resumen Ejecutivo

  Debido a su orientación, la cual es a los gerentes de las compañías, debe ser preciso, claro y sin mucha terminología técnica, no muchas personas tienen conocimientos informáticos.

  - Ventajas

Se destacan los procesos, formas de instalación y componentes del sistema que se manejan de manera correcta, tanto en desempeño e instalación siempre relacionada con las medidas de seguridad.

- Desventajas

  Las debilidades o desventajas, van de la mano de las vulnerabilidades encontradas, debido a que representan riesgos para la empresa, es importante que el personal las conozca para que no sean de un mayor riesgo.

✓ Resumen técnico

- **Ámbito del test**

  Se basa en las pruebas realizadas a la empresa cliente durante la etapa de análisis, las cuales podrían ser:

  - Pruebas al servidor FTP.
  - Ataque de fuerza bruta
  - Ataques de diccionario
  - Pruebas de ingeniería social
  - Pruebas hacia servidores web
  - Pruebas a puertos abiertos

- **Análisis del Objetivo**

  Se estudian todos los tipos de conexiones que se usaron para obtener información, así como data relevante, estas pueden ser:

  - Encriptaciones encontradas
  - Número de sistemas operativos encontrados y características
  - Configuración de hardware y software
  - Tipo de conexiones utilizadas en las pruebas.

- **Vulnerabilidades analizadas**

Son los errores por diferente motivo que fueron encontrados en las aplicaciones. Por lo general se destacan:

- Vulnerabilidades en la base de datos
- Errores en los servidores web
- Fallas en la transferencia de archivos
- Vulnerabilidades en la red interna
- Vulnerabilidades a nivel de contraseñas

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El hacking ético, es una solución real, preventiva y que usa pruebas de casos reales para poder encontrar diversas vulnerabilidades posibles en las redes de datos o sistemas de las empresas de cualquier índole, que pueden estar expuestas a cualquier delito informático.
2. Formar hackers de sombrero blanco, tiene como fin combatir la delincuencia informática, para que de esta forma las vulnerabilidades posibles no sean explotadas sino mitigadas. Cabe destacar que la formación de este hacker ético, debe ser constante debido al cambio constante del área de seguridad; cabe destacar que no solo se debe impartir formación en el área sino también de la parte ética.
3. Las políticas de seguridad en la organización cliente, sirven como instructivo para que el personal de la misma, se rija a los procedimientos establecidos después de la auditoría contratada. Sirven de base para que los empleados sigan el estándar implementado.
4. Las metodologías estudiadas, tanto las actualizadas como las que no están, sirven como guía de construcción de una solución de ethical hacking, como para ejecutar las pruebas de penetración, además se rigen a un plan con lineamientos establecidos para evitar la improvisación y posibles fallos en las pruebas.
5. Realizar pruebas anunciadas son modos eficientes de controlar la seguridad ya que la actitud laboral se orienta a la seguridad, el personal experimentará directamente la posible intrusión de un delincuente y el personal de tecnología de la

organización, (en el caso de PyMES es probable que el área sea establecida por una persona o ninguna) ayuda a la empresa auditora a centrar su trabajo en determinados puntos críticos.

6. Realizar pruebas sorpresa, son prácticamente de caso real ya que el analista intentará encontrar objetivos y violar la seguridad de la empresa. La prueba será de mayor valor que una que fue anunciada ya que se analizarán todos los componentes desde una visión hacker.
7. A pesar de las ventajas y del crecimiento tecnológico, en la región, aún no son mayoría las empresas que utilizan las tecnologías de información para verse favorecidas, esto puede deberse a la falta de capacitación a nivel gerencial y de sus trabajadores, falta de confianza en la tecnología y/o falta de inversión.
8. Las PyMES a comparación de las grandes corporaciones, no poseen el movimiento económico de estas, es por ello que, al momento de realizar el estudio y la firma de acuerdo del contrato, estimar el presupuesto acorde a la empresa que se analizará, ya que el desarrollo sería menos complejo y de menor tiempo, y la cantidad de recursos sería menor.
9. Debido a la situación en la región de las medianas y pequeñas empresas, las auditorías de seguridad serán de gran ayuda como consultorías más que en medidas preventivas, es decir el estudio se enfocaría dependiendo el caso en el uso de TIC´s desde 0, desde el uso de políticas de seguridad, capacitación al personal, instalación recomendada de servidores, red de datos etc.

Recomendaciones

1. Planificar periódicamente auditorias de seguridad para la detección de intrusos es una crucial práctica que debe ser evaluada en el cronograma de las empresas de

cualquier índole para proteger su información. Un mínimo descuido por parte del área administrativa en este asunto podría provocar pérdidas de recursos.

2. Es importante actualizarse constantemente acerca de las herramientas de seguridad y de las nuevas vulnerabilidades encontradas. Todos los días se escuchan nuevas formas de violar la seguridad o casos exitosos de hacking a empresas, es por ello que resulta importante desarrollar mecanismos para mantener la seguridad de la red de datos o del sistema actualizado.
3. A pesar de que la metodología OWASP y PTES son desactualizadas comparadas con el resto de metodologías estudiadas, es importante usarlas como material de consulta debido a que muchos de sus procesos son macro, y pueden ser aplicados en las diferentes etapas.
4. Los administradores de sistemas deben estar alerta y ser prudentes acerca del uso de las herramientas mencionadas en el presente documento, debido a que la parte ética es muy sensible; y sobre todo realizar la ejecución de tareas apegándose al marco legal.
5. Resulta crucial que las organizaciones de cualquier tipo difundan a sus empleados sus políticas de seguridad y hagan controles periódicos sobre el tema para evitar pérdidas, robo o difusión de información sensible.
6. Es adecuado para el medio, crear planes económicos para el estudio de seguridad enfocado a pequeñas empresas y para medianas, ya que muchas de ellas, no tienen como prioridad las Tics o su presupuesto no se centra en ellas. Razón por la cual, el uso de diferentes metodologías y herramientas de software libre es de gran importancia, en la firma de contratos.

7. Si la pequeña o mediana empresa no tiene establecido como prioridad el uso de Tics, pero quiere incorporarlas a su empresa, las recomendaciones puntuales por parte de la consultora de ethical hacking serían:
    - Implementar políticas de seguridad acordes a la cantidad de empleados y el tipo de empresa.
    - Compra e instalación de antivirus y antispyware en todos los equipos.
    - Instalación de firewalls en los ordenadores.
    - Realizar copias de seguridad especialmente a los datos considerados de mayor relevancia.
    - Asegurar el acceso inalámbrico a las redes de trabajo usando passwords fuertes.
    - Limitar los accesos a los empleados que se crea que no son importantes en su área.
    - Capacitar a los empleados con respecto a las políticas de seguridad.
    - Evitar que personas ajenas al personal utilicen los ordenadores de la empresa, ya que es común que familiares o amigos utilicen los equipos en las PyMES.

BIBLIOGRAFÍA

- ✓ ComputerFutures (Sitio web). *Los riesgos del hacking ético.* Internet. http://www.computerfutures.com/en/news/articles/the-rise-of-ethical-hacking. Acceso: (04 de febrero de 2016).
- ✓ SALDAÑO, Osmar. (s.f.) *Tesis de grado. Metodología de la investigación.* Recuperado de: http://www.mailxmail.com/curso-tesis-investigacion/tesis-planteamiento-problema. Acceso: (04 de febrero de 2016).
- ✓ GALDÁMEZ, Pablo. (s.f.). *Seguridad informática*. Recuperado de: http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf. Acceso: (20 de febrero de 2016).
- ✓ LOPEZ. (2007) *Seguridad Informática. Recuperado de: http://www.uv.mx/personal/llopez/files/2011/09/presentacion.pdf. Acceso: (20 de febrero de 2016).*
- ✓ HERNANDEZ, Laura & MEJIA, Jezreel. (2015) RECIBE: Revista electrónica de computación informática, biomédica y electrónica. *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web.* Recuperado de: http://recibe.cucei.udg.mx/beta/revista/es/vol4-no1/computacion05.html. Acceso: (21 de febrero de 2016).
- ✓ 403labs (Sitio Web). *Pruebas de penetración.* Internet. http://www.403labs.com/es/professional_services/penetration_testing. Acceso: (26 de febrero de 2016).
- ✓ MANIKANDAN, Jayanthi. (2016). *Role of an Ethical Hacker – What exactly does an Ethical Hacker do?* Internet. http://www.simplilearn.com/roles-of-ethical-hacker-article. Acceso: (26 de febrero de 2016).

- ✓ VILLACORTA, Alberto. (2005). *Enredados. El mundo de la Internet.* Recuperado de: https://books.google.com.ec/books?id=u0ZeCjcr2S0C&printsec=frontcover#v=onepage&q&f=false. Acceso (01 de marzo de 2016).
- ✓ GIMENEZ, Vicente Miguel. (2011). *Hacking y ciberdelito.* Recuperado de: https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1. Acceso: (01 de marzo de 2016).
- ✓ Zarza (Sitio web). *Gray hacking, Los de ética ambigua.* Internet. https://zarza.com/gray-hat-hacking-los-de-la-etica-ambigua/. Acceso: (01 de marzo de 2016).
- ✓ ArturoGoga. (Sitio web). *MICROSOFT PAGA HASTA $100,000 DÓLARES POR ENCONTRAR UN BUG EN WINDOWS 8.1.* Internet. *https://www.arturogoga.com/microsoft-paga-hasta-100000-dolares-por-encontrar-un-bug-en-windows-8-1/. Acceso: (01 de marzo de 2016).*
- ✓ SecurityWeek. (Sitio web). *Facebook Pays Out $7,500 Bounty for Account Hijacking Flaw*. Internet. http://www.securityweek.com/facebook-pays-out-7500-bounty-account-hijacking-flaw. Acceso: (01 de marzo de 2016).
- ✓ HIMANEN, Pekka. (2001*). La ética del hacker y el espíritu de la era de la información.* Recuperado de: https://docs.google.com/document/d/1ONaAn_UPB-mahPaIfdnHOtdZGTHAgaXhqrXzsGIvuKg/edit. Acceso: (01 de marzo de 2016).
- ✓ ALBORS, Josep. (2014). *¿Sabes qué es un exploit y cómo funciona?* Recuperado de: http://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan Acceso: (01 de marzo de 2016).
- ✓ SRI. (Sitio web). *PYMES*. Internet. http://www.sri.gob.ec/de/32. Acceso: (02 de marzo de 2016).

- ✓ Enroke. (Sitio web*). ¿Qué son las PYMES?* Internet. http://www.grupoenroke.com/index.php/proyecto-pymes/46-que-son-las-pymes. Acceso: (04 de marzo de 2016).
- ✓ CEH (Sitio web). *Certified Ethical Hacking Training Program.* Internet. https://www.eccouncil.org/Certification/certified-ethical-hacker. Acceso: (08 de marzo de 2016).
- ✓ UNAD. (Sitio web). *Lección 29: ISSAF*. Internet. http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_29_issaf.html. Acceso: (Acceso 08 de marzo d 2016).
- ✓ OSSTMM. (Sitio web). *Open Source Security Testing Methodology Manual (OSSTMM). Internet*. http://www.isecom.org/research/. Acceso: (08 de marzo de 2016).
- ✓ OWASP. (Sitio web). *About The Open Web Application Security Project. Internet*. https://www.owasp.org/index.php/About_OWASP#The_OWASP_Foundation. Acceso: (09 de marzo de 2016).
- ✓ PEREZ, Maximiliano. (2012). *Módulo 3: Auditorías y Seguridad. Tema 4: Comparativa Metodologías Auditorías y Pentesting*. Recuperado de: http://docslide.us/documents/metodologias-mas-usadas-en-pentesting-estudio-comparativo.html#. Acceso: (29 de junio de 2016).
- ✓ PeritoIT (Sitio web*). Footprinting informático, primer paso del Pentest o Test de Intrusión. Internet.* https://peritoit.com/2012/06/18/footprinting-informatico-primer-paso-del-pentest-o-test-de-intrusion/. Acceso: (13 de junio de 2016).
- ✓ CALLES, Juan & PEREZ, Pablo. (2011). *La Biblia del Footprinting.* Recuperado de: https://la-biblia-del-

footprinting.googlecode.com/files/La_Biblia_del_Footprinting.pdf. Acceso: (14 de junio de 2016).

- ✓ Corporación de Estudios y Publicaciones. (2011). *Código Penal, Legislación Conexa, Concordancias, Jurisprudencia.* Editorial Corporación de Estudios y Publicaciones, edición 2011, 2011.
- ✓ CONQUITO. (2007). *Las tecnologías de la información y las comunicaciones en la competitividad de Quito.* Recuperado de: http://www.infodesarrollo.ec/documentos/files/original/459293435d2d451ec86dcbf029627341.pdf. Acceso: (19 de junio de 2016).
- ✓ YAR, Ronier. (2015). *Infracciones informáticas.* Internet. http://comunidad.todocomercioexterior.com.ec/profiles/blogs/infracciones-inform-ticas-2 . Acceso: (29 de junio de 2016).
- ✓ PÁEZ, Juan. (2009). *Peritaje e infracciones Electrónicas.* Internet. http://www.derechoecuador.com/utility/Printer.aspx?e=35278. Acceso: (29 de junio de 2016).

ANEXOS

Anexo 1: Glosario de siglas y términos

A

- **Amenaza:** acción que puede significar peligro en la seguridad de información de un determinado sistema o red de datos.
- **Ataque:** accionar que viola la seguridad de la empresa.
- **Ataque dirigido:** ataques realizados de manera sigilosa cuyo objetivo puede ser una organización o una persona.
- **Auditor:** persona que realiza pruebas, para verificar, comprobar o reportar algún procedimiento.

B

- **Base de datos:** conjunto de ficheros que contienen información para gestionar la estructura y forma en la que estos se almacenan.
- **Backdoor:** técnica que permite entrar a un sistema sin la forma común como con un usuario y contraseña.

C

- **Cache:** Memoria que tienen las computadoras la cual funciona de manera similar a la RAM, es de menor tamaño y de accesibilidad más rápida, la usa el CPU lo cual permite reducir tiempos de acceso a datos ubicados en la memoria principal que se usan con frecuencia.
- **Contraseña:** combinación de caracteres para restringir o permitir el ingreso de usuarios a un determinado sistema o fichero.
- **Cracker:** persona que le interesa violar la seguridad de un sistema informático para robar información.

D

- **Ddos:** ataque de negación de servicios que se realiza en igual tiempo desde varias computadoras contra un servidor.
- **DNS:** facilita la conexión entre computadoras a una red y su ubicación.

E

- **Escáner de puertos:** monitoreo de puertos de comunicaciones o direcciones IP de una computadora, obtener su estado y localización.
- **Exploit:** secuencia de comando que se usa para quebrantar la seguridad de sistemas usando una vulnerabilidad encontrada.

F

- **Firewall:** software cuya funcionalidad es bloquear o monitorear el tráfico de red hacia un sistema determinado.
- **FTP:** mecanismo que permite la transferencia de archivos a través de conexión TCP/IP.

H

- **Hacking:** ingreso a sistemas ajenos sin conocimiento de los implicados, puede ser virtual o físicamente
- **Honeypot:** software o hardware que simula ser un objetivo vulnerable, sirve como pruebas de ataques y evaluación de técnicas utilizadas por los hackers.

I

- **Ingeniería Social:** es una técnica que su objetivo es convencer al usuario usando técnicas de engaño para obtener información que permita ingresar a un determinado sistema de forma no autorizada.

K

- **Keylogger:** Hardware o software que registra las digitaciones que se realiza al teclado.

L

- **Log:** Archivo que recoge un registro de actividades del sistema para su difusión.

M

- **Malware:** Software que causa diversos tipos de daños a los usuarios.

O

- **OWASP:** metodología de ethical hacking de código abierto que tiene como objetivo determinar y prevenir las causas que hacen que el software sea inseguro.

S

- **Script:** archivo que tiene órdenes de ser ejecutado en secuencia.
- **Spyware:** es un software espía que su objetivo es enviar información confidencial de los propietarios de la máquina.
- **Servidor:** Gran computadora que presta todos o algunos servicios y recursos a otras computadoras conectadas en red

V

- **VoIP:** Tipo de recurso que permite que la señal de la voz viaje mediante internet utilizando el protocolo IP.