ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

IMPLANTACIÓN DE TÉCNICAS Y ADMINISTRACIÓN DE LABORATORIO PARA INVESTIGACIÓN DE ETHICAL HACKING

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR:

SANDOVAL MENDEZ LUCÍA CAROLINA

VACA HERRERA ANDREA ESTEFANÍA

SANGOLQUÍ, MAYO DEL 2013

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por las Srtas. SANDOVAL MENDEZ LUCÍA SANDOVAL y VACA HERRERA ANDREA ESTEFANÍA como requerimiento parcial a la obtención del título de INGENIEROS EN SISTEMAS E INFORMÁTICA.

Mayo, 2013

_____

ING. MAURICIO CAMPAÑA

DEDICATORIA

A Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mi familia que siempre estuvo apoyándome especialmente a mi madre Marcia Méndez, por darme la vida, quererme mucho, creer en mí, hacer todo lo posible para que estudiara y porque este era uno de tus mayores sueños. Mamá gracias por darme una carrera para mi futuro, todo esto te lo debo a ti.

A mis sobrinos quienes me han tomado como su ejemplo a seguir, los quiero mucho y nos los defraudare.

A mis maestros por su gran apoyo y motivación para la culminación de mis estudios profesionales, por ayudar a formarme no solo como una excelente profesional sino como una gran persona.

A mis amigos con los que pase de las aulas al trabajo y a pesar de eso siempre me han ayudado, gracias por apoyarme y motivarme a seguir, no sé qué sería de mí sin ustedes.

Lucía Carolina Sandoval Méndez

DEDICATORIA

A mi amigo más fiel que de un día para el otro se fue sin poder regresar, el mismo que me ayudó a no darme por vencida en ningún momento y que desde el cielo me sigue dando ánimos para continuar con mis sueños y anhelos.

A mis padres quienes con su esfuerzo me ayudaron a tener prioridades en la vida y a no dejarme caer por ningún obstáculo poniendo la cara a los problemas.

A todos mis profesores que compartieron sus conocimientos y me dieron la oportunidad de crecer no solo profesionalmente sino también como persona.

A mis amigos quienes estuvieron apoyándome con mi mal genio y estrés, nunca me abandonaron sino más bien me apoyaron.

Andrea Estefanía Vaca Herrera

AGRADECIMIENTO

El presente trabajo de tesis primeramente me gustaría agradecerte a ti Dios por bendecirme para llegar hasta donde he llegado, por hacer realidad este sueño anhelado.

A la Escuela Politécnica del Ejército por darme la oportunidad de estudiar y ser una profesional.

A mi familia por todas las veces que tuve que faltar a reuniones familiares, viajes o fiestas, por realizar la tesis, muchas gracias por su comprensión y apoyo los quiero mucho.

Al Ingeniero Mario Ron, por su esfuerzo y dedicación, quien con sus conocimientos, experiencia, paciencia y motivación nos ayudó a terminar nuestros estudios con éxito

A mis amigos por ser un constante apoyo y paciencia durante esta etapa de mi vida en la que entre el trabajo y mi tesis no he tenido tiempo mucho tiempo para ellos.

A mi compañera de tesis, de aula y sobretodo una de mis mejores amigas, Andrea esta tesis es el resultado de nuestro esfuerzo y dedicación, gracias por compartir conmigo este sueño.

También me gustaría agradecer a mis profesores durante toda mi carrera profesional porque todos han aportado con un granito de arena a mi formación.

Lucía Carolina Sandoval Méndez

AGRADECIMIENTO

Agradezco a Dios por su apoyo incondicional, por darme lo que más quiero en esta vida, mi familia y amigos. Por ser ese apoyo incondicional y estar en todos los años de mi vida. A mis padres que me han tenido la paciencia más grande del mundo, por ayudarme a ver la vida de una forma diferente, por los consejos que algunas veces solo escuchaba pero ellos hacían lo mejor que podían.

Agradezco a un persona incondicional que a pesar de no estar a mi lado sé que desde el cielo me protege y desea que me vaya de lo mejor tanto personal o como laboral. Agradezco sus consejos de que si alguna vez me caiga levantarme y empezar de nuevo, a ti Mauricio Machado te agradezco puesto que desde arriba sé que me proteges y me sigues apoyando en todo lo que realizo.

A mis amigos quienes me entregaron y confiaron sus vidas, por tenerme paciencia en todas las cosas que he dicho y he hecho. Sin ellos no habría llegado a donde estoy.

Al Ingeniero Mario Ron quien aparte de ser un profesor fue un pilar, quien nos guio por el camino para alcanzar el éxito más grande de una persona profesional.

A mi compañera, amiga de tesis por la constancia al realizar este trabajo, a la paciencia y conocimientos que hemos compartido puesto que sin compartir los mismos no hubiéramos logrado llegar hasta este momento.

Andrea Estefanía Vaca Herrera

ÍNDICE DE CONTENIDOS

LISTADO DE TABLAS

LISTADO DE FIGURAS

GLOSARIO

Buena Practicas Conjunto coherente de acciones que han rendido buen o excelente servicio en un determinado contexto

Proceso Conjunto estructurado de actividades diseñadas para conseguir un objetivo específico.

Rol Conjunto de responsabilidades, actividades y autoridades concedidas a una persona o a un equipo.

Servicio Una forma de proporcionar valor a los clientes facilitando los resultados que los clientes quieren alcanzar

Incidente Interrupción no planificada de un servicio de TI o una reducción de la calidad de un servicio de TI.

Diseño Actividad o proceso que identifica los requisitos y luego define la solución que sea capaz de satisfacer tales requisitos.

Ciclo de Vida Las diferentes etapas en la vida de un servicio de TI, un elemento de configuración, un incidente, un problema, un cambio, etc.

Catálogo de Servicios Una base de datos o un documento estructurado con información sobre todos los servicios de TI

Acuerdo de Nivel de Servicio Describe el servicio de TI, documenta las metas de niveles de servicio y especifica las responsabilidades del proveedor de servicios de TI y del cliente

Acuerdo de Nivel de Operación Ofrece soporte a la prestación por parte del proveedor de servicios de TI de los servicios de TI a los clientes.

Prioridad Categoría usada para identificar la importancia relativa de un incidente, un problema o un cambio. La prioridad se basa en el impacto y urgencia.

Impacto Categoría usada para identificar la importancia relativa de un incidente, un problema o un cambio. La prioridad se basa en el impacto y urgencia

Problema La causa de uno o más incidentes

Victimas Personas que sufren un daño o perjuicio

Ataques es un método donde un individuo, mediante un sistema informático, intenta tomar el control.

Hackers Persona capaces de comprometer un sistema, robar todo lo valioso y borrar completamente la información en pocos minutos

Ethical Hacking Disciplina que se encarga de encontrar vulnerabilidades ya sea en la red como en las aplicaciones y usar estas a beneficio de la empresa u organización.

Internet es un conjunto descentralizado de redes de comunicación interconectadas.

Seguridad Informática consiste en un conjunto de métodos, formas y estándares que permiten asegurar que las políticas de una organización

Metasploits Es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para Sistemas de Detección de Intrusos

Vulnerabilidades Son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo.

Método Delphi Es la consecución de un consenso basado en la discusión entre expertos.

Delitos Informáticos Es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet

Test de Intrusión Es un paso previo a todo análisis de fallas de seguridad o riesgo para una organización.

Amenazas hecho que puede producir un daño provocado por un evento informático.

Accesos no autorizados Incluye tanto los servicios profesionales vinculados a la instalación, mantenimiento, desarrollo, integración de software, como los de soporte técnico de hardware.

Telnet Es el nombre de un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

Puerto Es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir

Red Conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos.

Sistema Operativo Programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación.

Password Es una palabra secreta o una cadena de caracteres que son usados para la autentificación del usuario o para el acceso a un recurso.

Backdoor Es un método que permite autentificar a un usuario.

LAN Es una red de computadoras que se conectan en un área limitada como casas, escuelas, entre otros.

Log Es un registro oficial de eventos durante un rango de tiempo en particular

Topología Familia de comunicación usada por los computadores que conforman una red para intercambiar datos.

Métrica es una metodología de planificación, desarrollo y mantenimiento de sistemas de información

ACRÓNIMOS

ITIL Biblioteca de Infraestructura de Tecnologías de Información

IT Tecnologías de Información

ESPE Escuela Politécnica del Ejército

TICs Tecnologías de Información y la Comunicación

SLA Acuerdo de Nivel de Servicio

OLA Acuerdo de Nivel de Operación

IP Internet Protocol

RESUMEN

El presente proyecto pretende diseñar en base a ITIL, los servicios que prestará un laboratorio de investigación en Ethical Hacking.

La inseguridad y pérdida de información en organizaciones y empresas en los últimos años, es consecuencia de su falta de preocupación respecto a la seguridad de la Información en los servicios que estas ofrecen, lo que da lugar a vulnerabilidades que requieren ser descubiertas por personal y servicios especializados en Hacking Ético; esto ha motivado la creación del Laboratorio de Ethical Hacking de la ESPE el cual ofrece servicios de educación, consultoría e investigación orientado a estudiantes, docentes y comunidad en general para ayudarlos a la concientización de los peligros que existen en los sistemas informáticos, donde las personas evitan ser víctimas poniéndose en el lugar del atacante.

El proyecto de tesis presenta el diseño de los servicios del Laboratorio describiendo la implantación de nuevas técnicas basadas en Ethical Hacking y la propuesta de los servicios que el Laboratorio brindará, utilizando las tres primeras fases de ITIL que son: Estrategia del Servicio, Diseño del Servicio y Transición del Servicio de los cuales los dos primeros se realiza por completo mientras de que el ultimo se llega al plan de transición de los servicios diseñados. Para asegurar un proceso adecuado, el diseño es validado por expertos en el tema, utilizando el método Delphi.

CAPÍTULO 1

INTRODUCCIÓN

Las computadoras alrededor del mundo están siendo víctimas constantemente de ataques de hackers (piratas informáticos), capaces de comprometer un sistema, robar todo lo valioso y borrar completamente la información en pocos minutos. Por esta razón resulta de vital importancia conocer si los sistemas informáticos y redes están protegidos de todo tipo de intrusos.

Precisamente el objetivo fundamental de Ethical Hacking, es, brindar ayuda a las organizaciones para que tomen todas las medidas preventivas en contra de agresiones maliciosas, valiéndose para ello de los test de intrusión, que evalúan la seguridad técnica de los sistemas de información, redes de computadoras, aplicaciones web, servidores. El servicio consiste en la simulación de ataques hostiles controlados y la realización de actividades propias de delincuentes informáticos, esta filosofía resulta de la practica probada: "Para atrapar a un ladrón debes pensar como un ladrón"[1].

Es necesario, por tanto, determinar las herramientas y técnicas necesarias para probar la vulnerabilidad de los sistemas de informaciçón ya implantados. De ahí el hecho de madurar la idea de implementar ética hacking en el Ecuador como mecanismo investigativo que permita controlar los diferentes ataques informáticos que en los últimos años se vienen presentando.

[1] http://www.sadvisor.com/servicios/servicios_masinfo.php?id=71&secc=servicios

1.1- Antecedentes

El uso indebido de las Tecnologías de la Información y Comunicación por gente inescrupulosa que realiza ataques en contra de la integridad de sistemas computacionales o redes, ha causado no solo enormes pérdidas económicas sino la aprensión de personas inocentes que han sido víctimas de dichos ataque informáticos, o que se ha detectado el mal uso de los recursos tanto redes sociales como de Internet.

Para el análisis y tratamiento de este tipo de incidentes se encuentra Ethical Hacking, que consiste en la simulación de posibles escenarios donde se producen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos.

Para garantizar la seguridad informática se requiere de un conjunto de sistemas, métodos y herramientas destinados a proteger la información, es aquí donde entran los servicios del Ethical Hacking , la cual es una disciplina de la seguridad informática que echa mano de una gran variedad de métodos para realizar sus pruebas, estos métodos incluyen tácticas de ingeniería social, uso de herramientas de hacking , uso de Metasploits que explotan vulnerabilidades conocidas, en fin son válidas todas las tácticas que conlleven a vulnerar la seguridad y entrar a las áreas críticas de las organizaciones.

Por esta razón se desea implementar los laboratorios para así dar conciencia a los estudiantes sobre los diversos ataques informáticos que hoy en día existen y a la vez poder contar con el personal capacitado, dentro de la justicia ecuatoriana en conjunto con los profesionales informáticos, para sancionar el mal uso de las TICs y combatir esta clase de infracciones.

La Policía Nacional del Ecuador se encuentra limitada en los procesos de investigación de delitos informáticos, porque no cuenta con suficiente personal capacitado en el uso de herramientas informáticas y metodologías de recolección de evidencia digital.

En la Carrera de Ingeniería de Sistemas de la ESPE, se piensa implementar los laboratorios de Ethical Hacking, para todas las personas que se encuentren interesadas en la seguridad informática puesto que hoy en día los ataques informáticos son los más sonados y más vistos.

Se halla en etapa de recepción los equipos del laboratorio de Ethical Hacking, del Departamento de Ciencias de la Computación que será utilizado por los programas de pregrado y posgrado, así como por cursos de vinculación con la Comunidad.

1.2- Justificación

La masificación del uso de las computadoras y el acceso al servicio del internet, ha hecho que los usuarios cometan delitos informáticos de manera voluntaria o involuntaria, pero las autoridades se han envuelto en el tema sin dar solución por falta de infraestructura, equipamiento y de personal capacitado.

La solución a esto es la Implantación de un Laboratorio de Ethical Hacking en la Escuela politécnica del ejercito el mismo que fomentara la investigación y uso de herramientas de hacking para poner a prueba la seguridad de los sistemas de información, además de educar a la comunidad en general sobre los peligros a los que están expuestos mediante demostraciones de ataques.

Esto permitirá capacitar con cursos prácticos a los estudiantes de educación formal y continua de la Carrera de Ingeniería en Sistemas e Informática de la

Escuela Politécnica del Ejército, aprovechando el conjunto de recursos de hardware, software, infraestructura y sobre todo personal capacitado.

Con el desarrollo de las técnicas de Laboratorio de Ethical Hacking se favorecerá la prestación de los servicios profesionales a la ciudadanía, realizando un adecuado análisis del campo descrito, empleando un equipo multidisciplinario, que incluya personas expertas en seguridad informática, con la finalidad de garantizar la integridad de la información y de su sistema.

1.3- Objetivos

1.3.1- Objetivo General

Implantar técnicas para el uso del laboratorio de Ethical Hacking diseñados en base a ITIL V3 de seguridad informática, el cual se instalará en la Escuela Politécnica del Ejército, a través de prácticas de laboratorios para la educación continua y formal de la comunidad en general para su correcta administración y funcionamiento en la Carrera de Ingeniería en Sistemas e Informática que permitirá brindar dicho servicio

1.3.2- Objetivos Específicos

- Plantear el uso de ITIL V3 para la propuesta de servicios que podría tener el Laboratorio de Ethical Hacking, describiendo las tres primeras fases del ciclo de vida del mismo.
- Crear guías prácticas que describan de manera ordenada y secuencial la utilización de las herramientas seleccionadas.
- Describir los pasos que se deben realizar para poder acceder a los diferentes servicios.

- Usar el método Delphi para validar la propuesta de los servicios que se presentará en este proyecto.

1.4- Alcance

El presente proyecto cubre las tres primeras fases de ITIL V3 que son Estrategia, Diseño y Transición del Servicio, cumpliendo por completo las dos primeras fases mientras que la tercera solo se llegará al plan de transición de los servicios diseñados.

La Estrategia del Servicio es la primera etapa donde se proyecta la efectividad operativa y rendimiento dando a conocer:

- Que se va hacer
- Por qué se va hacer
- Para quien se va hacer
- Y cuánto debe costar

El Diseño del Servicio planteará temarios, guías prácticas y los formatos de contratos de prestación de servicios.

La Transición del Servicio se describe un plan de transición en el que se especifica que se debe hacer para poner en funcionamiento el laboratorio.

1.5- Metodología

Se aplicará una metodología, relacionada con la búsqueda y generalización de casos de estudio adecuados a la práctica de Ethical Hacking, relacionados con la enseñanza y con la investigación profesional de vulnerabilidades informáticas.

La calidad de la propuesta de servicios que el laboratorio de Ethical Hacking brindará, será demostrada mediante el método DELPHI, el mismo que consiste en la

selección de un grupo de expertos los cuales evaluarán a la misma de acuerdo a ciertos indicadores.

Características:

- ANONIMATO: no debe existir contacto entre los participantes.
- ITERACIÓN: se pueden manejar tantas rondas como sean necesarias.
- RETROALIMENTACIÓN CONTROLADA: los resultados totales de la ronda previa no son entregados a los participantes, sólo una parte seleccionada de la información circula.
- RESULTADOS ESTADÍSTICOS: la respuesta del grupo puede ser presentada estadísticamente (promedios y grado de dispersión).

El método Delphi se encuentra establecido en cuatro fases:

- **Fase 1:** Formulación del problema.
- **Fase 2:** Elección de expertos.
- **Fase 3:** Elaboración y lanzamiento de los cuestionarios.
- **Fase 4:** Desarrollo práctico y explotación de resultados

CAPÍTULO 2

MARCO TEÓRICO

2.1- Seguridad Informática

Los sistemas de información incluyen todos los datos, equipos y software de una organización que le permiten almacenar y hacer circular información, al ser esto un proceso crítico todos estos elementos deben ser protegidos y es aquí donde aparece la seguridad informática.

La Seguridad Informática consiste en un conjunto de métodos, formas y estándares que permiten asegurar que las políticas de una organización sean utilizadas de la manera en que fueron planeadas previniendo la alteración, modificación o reemplazo de los datos, contenidos en los recursos de información, por personas o entidades no autorizadas. Además se encarga de garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

2.2- Objetivos de la Seguridad Informática

La seguridad informática en lo general tiene cinco objetivos principales:

- **Integridad:** garantizar que los datos sean los que se supone que son.
- **Confidencialidad:** asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **Disponibilidad:** garantizar el correcto funcionamiento de los sistemas de información.
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.

- **Autenticación:** asegurar que sólo los individuos autorizados tengan acceso a los recursos.

2.3- Los Delitos Informáticos.

El avance de la tecnología que ha vivido y está viviendo la sociedad, se observa una evolución tan grande en la forma de infringir la ley, debido a esta situación las respectivas autoridades se ven en la necesidad de tomar la decisión de diferenciar o no los delitos informáticos del resto de delitos y definir su tratamiento dentro del marco legal.

Wikipedia[2], define a los delitos informáticos como “es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.”

Rafael Fernández Calvo [3] al "delito Informático" como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando en elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española.".

Muchos expertos y organismos a los delitos informáticos los denominan como delitos electrónicos, delitos relacionados con la computadora, delincuencia relacionada con la computadora, crímenes por computadora, por lo que denota que no existe una definición de carácter universal propia del delito informática, pero sin

[2] http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico
[3] http://www.angelfire.com/la/LegislaDir/Defin.

embargo que cada una de las definiciones de los expertos, son basadas en la experiencia que han obtenido mediante el debido proceso de tratamiento de los delitos informáticos.

El Delito Informático implica actividades criminales susceptibles a ser sancionadas, que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Como todo delito, el informático tiene un sujeto activo y otro pasivo:

- **SUJETO ACTIVO**: En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación, también conocido como atacante.
- **SUJETO PASIVO**: en el caso del delito informático pueden ser: individuos, instituciones de crédito, gobiernos, en fin entidades que usan sistemas automatizados de información, también conocido como víctima.

2.3.1- Tipos De Delitos Informáticos

Existen varios autores y organizaciones que clasifican los delitos de varias maneras. A continuación se detallan los tipos de delitos informáticos según las Naciones Unidas:

- Fraudes cometidos mediante manipulación de computadoras:
  - Manipulación de datos de entrada.
  - Manipulación de programas.

- Manipulación de los datos de salida.

- Falsificaciones informáticas:
  - Cuando se alteran datos de los documentos almacenados en forma computarizada.
  - Cuando se usan las computadoras para efectuar falsificaciones de documentos de uso comercial.
  - Daños o modificaciones de programas o datos computarizados:
  - Sabotaje informático mediante: virus, gusanos, bomba lógica o cronológica.
  - Acceso no autorizado a servicios y sistemas informáticos.
  - Piratas informáticos o hackers.
  - Reproducción no autorizada de programas informáticos de protección legal.

En la siguiente tabla se describe los delitos informáticos que otros autores describen:

Tabla 2.3: Delitos Informáticos

DELITO	DESCRIPCIÓN
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.
Bomba lógica o cronológica	Son difíciles de detectar antes de que exploten, poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente.

Acceso no autorizado a servicios y sistemas informáticos	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, el delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad.
Protección al menor	Producción, distribución y posesión de pornografía infantil.
Fraudes en Internet	Estafas, subastas ficticias y ventas fraudulentas.
Phising	Redirección mediante correo electrónico a falsas páginas simuladas trucadas (común en las mafias rusas)
Seguridad lógica	Ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico. Delitos de injurias, calumnias y amenazas a través del e-mail, noticias, foros.
Propiedad intelectual	Piratería de programas de ordenador, de música y de productos cinematográficos, robos de código

2.4- Informática Forense.

La Informática forense es una ciencia que trata sobre el proceso de investigar dispositivos no solo informáticos, utilizando métodos y técnicas aplicables a la investigación de delitos con el fin de descubrir y de analizar información disponible, suprimida, u oculta que puede servir como evidencia en un asunto legal.

Aplica técnicas no solo científicas sino también analíticas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

La Informática Forense recolecta y utiliza la evidencia digital para casos de delitos informáticos y para otro tipo de crímenes usando técnicas y tecnologías. No solo recupera información, sino que también la descubre ya que esta pudo haber sido borrada, adulterada o encubierta con o sin intensión y el trabajo del informático forense es utilizar todas las herramientas que tenga a su alcance para tenerla devuelta sin alteración alguna.

La Informática Forense se puede utilizar para descubrir un fraude, uso no autorizado de computadoras, una violación de políticas de compañías, historial de chats, archivos y navegación o cualquier otra forma de comunicaciones electrónicas, donde la escena del crimen es el computador y la red a la cual éste está conectado.

2.4.1- Objetivos

Los objetivos de Informática Forense son:

- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia a través de las siguientes preguntas.

- ¿Qué sucedió?
- ¿Dónde?
- ¿Cuándo?
- ¿Cómo?
- ¿Por qué?

2.4.2- Fases de la Informática Forense

La Informática Forense se resume tradicionalmente en cuantos procesos secuenciales que son las siguientes:

- Identificación
- Análisis
- Preservación
- Presentación

La informática forense hace uso entre otras herramientas al Ethical Hacking como uno de sus principales respaldos al momento de obtener y recuperar información.

2.4.3- Áreas de Aplicación

Esta ciencia como se la conoce, tiene 3 diferentes áreas en donde puede desenvolverse una investigación:

o Área policial (Policía Digital): La policial digital generalmente se divide en 3 departamentos donde utilizan la informática forense para sus investigaciones:

- ✓ Departamento de Pornografía Infantil.- donde se realiza patrullajes cibernéticos para la investigación y captura redes de pedofilia.
- ✓ Departamento de Investigaciones y Delitos Financieros.- realiza investigaciones de fraudes financieros además de investigar delitos especiales como correos electrónicos maliciosos.
- ✓ Departamento de Análisis de evidencias digitales.- se encarga del análisis y búsqueda de evidencia digital dentro de las unidades de almacenamiento de los equipos utilizados para el cometimiento del delito o que fueron causa del mismo.

- Área judicial (Peritaje Informático Forense): realiza la búsqueda y presentación de pruebas útiles dentro de un proceso legal.
- Área privada (Oficinas de Investigación Privada): se basa en empresas que brindan servicios forenses para una investigación extra judicial.

En conclusión Informática Forense es una ciencia que se basa en un análisis de pruebas donde se recolecta y se utiliza la evidencia digital para casos de delitos informáticos y para otro tipo de crímenes usando técnicas y tecnologías avanzadas ya sea hardware o software especializado para así llegar a la causa del delito.

2.5- Ethical Hacking

2.5.1- Introducción

Hace algún tiempo, cuando algunas de las organizaciones apenas comenzaban a incrementar los procesos informatizados dentro de su sistema de información, sus propios administradores y analistas técnicos eran los encargados de buscar claras falencias o brechas de seguridad en el escenario para solucionarlas como podían.

En ese entonces, la mayoría no tenía una noción madura acerca de la seguridad de la información o de las intrusiones de terceros no autorizados en sus sistemas. A medida que pasó el tiempo, estas organizaciones se multiplicaron de manera notable y se informatizaron aún más, incluso tomando a Internet como plataforma de sus movimientos de información. De ese modo, se hicieron fluidas las comunicaciones interpersonales, inter-sucursales, transacciones o flujo digital de todo tipo y nivel de importancia, dejando, al mismo tiempo, muchos más datos expuestos a terceros, como nunca antes había sucedido.

Como resultado de ello y debido a que grandes casos de intrusión se dieron a conocer al público en general a través de los medios de prensa (aunque muchos no

salen a la luz para salvaguardar una imagen institucional de organización confiable), se hizo evidente la falta de algún servicio profesional que imitara esos ataques o capacitara a su personal con las mismas metodologías que utilizaba el intruso. De manera que se puedan evaluar las reales condiciones de seguridad en las que se encontraba una organización y, de existir vulnerabilidades en el sistema, descubrirlos y solucionarlos de forma preventiva.

Los accesos no autorizados, junto a una gama de vulnerabilidades y todo tipo de amenazas relacionadas o dirigidas hacia la información, estaban a la orden del día. Desde algunos años antes, muchos especialistas ligados a la seguridad informática han estudiado y practicado metodologías de intrusión en sus trabajos, laboratorios o casas.

Así, comenzaron a brindar a las organizaciones un servicio a modo de proveedores externos o contratados y, para darle un nombre medianamente formal, lo llamaron Ethical Hacking.

2.5.2- Definición

Ethical Hacking es una disciplina de la seguridad informática que se sustenta en que la mejor forma de evaluar las amenazas que representan los llamados “hackers” o piratas de la información, es conocer cómo actúan y operan. Este esquema es similar a tener un auditor verificando los “libros” de la empresa. En el caso de seguridad de computadoras, los “hackers éticos” usarán las mismas herramientas y técnicas que utilizan los intrusos. Ellos están en capacidad de reportar las vulnerabilidades que encuentren y la forma de remediarlas.

Ethical Hacking es una forma de referirse al acto de una persona que a través de sus conocimientos de informática y seguridad realiza pruebas en redes y encuentra

vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño, es decir, tener el conocimiento de cuales elementos dentro de una red son vulnerables y corregirlo antes que ocurra hurto de información.

Estas pruebas se llaman "pruebas de penetración", en donde se intenta de múltiples formas burlar la seguridad de la red para robar información sensitiva de una organización, y así reportarlo a la misma para mejorar su seguridad.

Alejandro Reyes Plata[4], resume a Ethical Hacking en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso".

Para garantizar la seguridad informática se requiere de un conjunto de sistemas, métodos y herramientas destinados a proteger la información, es aquí donde entran los servicios del Ethical Hacking , la cual es una disciplina de la seguridad informática que hecha a mano de una gran variedad de métodos para realizar sus pruebas, estos métodos incluyen tácticas de ingeniería social, uso de herramientas de hacking, uso de Metaexploits que explotan vulnerabilidades conocidas, en fin son válidas todas las tácticas que conlleven a vulnerar la seguridad y entrar a las áreas críticas de las organizaciones.

Técnica utilizada en la evaluación del riesgo informático de una red, sistema o aplicación. Consiste en la simulación de acciones que realizaría un “cracker” para tener acceso no autorizado a un sistema, información o generar Ethical Hacking autorizado a un sistema. Está técnica es realizada por expertos en seguridad internos y externos usando las mismas herramientas que los atacantes reales.

[4] http://www.seguridad.unam.mx/descarga.dsc?arch=2776

Metodología adoptada por hackers éticos para descubrir las vulnerabilidades existentes en los ambientes de operación de sistemas computacionales se refiere generalmente a los test de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración de un proyecto.

En conclusión Ethical Hacking es una disciplina de la seguridad informática que se sustenta en que la mejor forma de evaluar las amenazas que representan los llamados “hackers” o piratas de la información, es conocer cómo actúan y operan, a través de Ethical Hackers quienes están en capacidad de reportar las vulnerabilidades que encuentren y la forma de remediarlas, toman este nombre debido a que las técnicas y metodologías usadas son similares a las empleadas por los hackers, pero el único objetivo es comprobar el estado real y actual de la seguridad.

2.5.3- Hacker.

Desde que se usó por primera vez la palabra Hacker, ésta ha sido mal interpretada y catalogada en un contexto erróneo, por las operaciones que vienen realizando grupos de hackers como Anonymous y AntySec, aclarando que el termino Hacker no tiene que ver con actividades delictivas, si bien muchos Hackers las realizan su definición no tiene que ver con ellas.

Definición 1: “El término hacker, se utiliza para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal sin intentar causar daños.”[5]

[5] Flamix. Hackers. Taringa. Recuperado de: http://www.taringa.net/posts/info/6113810/Hackers.html

Los hackers son personas que disfrutan de aprender independientemente de los sistemas de computación y como ampliar sus capacidades sin sentirse obligado a hacerlo, es decir, programar por gusto.

2.5.4- Tipos de Hacker.

✓ Hacker de sombrero Negro o crackers.

Los Hackers de Sombrero Negro son los hackers maliciosos, mejor identificados en el mundo informático como crackers, son personas que rompen la seguridad de una Computadora, una red o crean Virus de Computadora.

Estas personas continuamente buscan la forma de entrar o romper la seguridad de lo que quieren. Estos Hackers a menudo buscan el camino de menor resistencia, ya sea por alguna vulnerabilidad, error humano, vagancia o algún nuevo método de ataque. La motivación número uno de un Hacker de Sobrero Negro es el dinero.

✓ Hackers de Sombrero Gris

Los Hackers de Sombrero Gris son personas que no se ubican ni entre los hackers de sombrero blanco ni en los de sombrero negro ya que por momentos, trabajan de manera ofensiva y otros de manera defensiva, dependiendo de la circunstancia, ocasionalmente traspasa los límites de la legalidad. Una gran cantidad de personas transita durante mucho tiempo en esta categoría pero luego se identifican como Hackers de sombrero negro o blanco.

✓ Hacker de sombrero Blanco.

Los White Hat Hackers o hackers de sombrero blanco son personas con grandes conocimientos de hacking y los utilizan con fines defensivos. Aprovechan su saber para localizar vulnerabilidades e implementar contramedidas. Se dedican al hacking ético para ayudar con la seguridad informática a compañías y organizaciones para

proteger a los sistemas de los Hackers de Sobrero Negro. Su creencia es que se debe examinar su propia red en la misma manera que lo haría un cracker para entender mejor sus vulnerabilidades.

✓ Ethical Hacker.

Profesionales que poseen una gran colección de habilidades. Ante todo, deben ser completamente merecedores de confianza. Al probar la seguridad de los sistemas de un cliente, el Ethical Hacker puede descubrir información acerca del cliente que se debe mantener en secreto, cualquier filtrado de información mal manejada, podría conducir a que los delincuentes informáticos irrumpieran en sus sistemas, conduciendo así a una posible pérdida financiera, robo de información o destrucción de datos.

Durante una evaluación, el Ethical Hacker maneja “las riendas” o “llaves” de la compañía, y por tanto esta persona debe ser absolutamente profesional y ética ya que manejara información sensible. La sensibilidad de la información manejada durante la evaluación exige que sean tomadas fuertes medidas de seguridad, para el manejo de las mismas:

- laboratorios de acceso restringido con medidas de seguridad física,
- conexiones múltiples de acceso a Internet,
- caja fuerte para sustentar la documentación en papel de los clientes,
- criptografía reforzada que proteja los resultados electrónicos,
- redes aisladas para el proceso de experimentación.

Los Ethical hackers normalmente tienen conocimientos avanzados en programación y dominan el tema de instalación, mantenimiento y configuración de varios sistemas operativos, además de los distintos tipos de hardware.

Esta anotación permite entender que no solo es necesario tener conocimientos en software, o en seguridad, sino que es necesario conocer y dominar el mayor tipo de conocimientos sobre sistemas informáticos y todo su entorno.

Estas personas deben tener un alto grado de paciencia y serenidad, el trabajo de los Ethical hackers exige largas jornadas de tiempo y persistencia, así mismo como los Delincuentes Informáticos esperan, y monitorean por días y semanas los sistemas esperando una oportunidad para penetrar en ella, aprovechando un descuido de su administrador.

Un análisis profesional de un Ethical Hacker puede requerir varios días de trabajo y dedicación, ya que hay tareas que son difíciles de automatizar. Algunas de estas actividades deben realizarse fuera de la "jornada" laboral, para así evitar el retraso o la interferencia en tiempo real de alguna actividad, o para simular un ataque verdadero en horas no esperadas. Cuando es analizado un sistema poco familiar o poco conocido por los Hackers Éticos, estos tendrán que pasar largo tiempo estudiando y analizando este sistema, tratando de encontrar sus vulnerabilidades y debilidades.

2.5.5- Clases de hacker ético

- Former Black Hats (Sombreros Negros Reformados): este grupo está conformado por crackers reformados que se han pasado del ataque a la defensa de sistemas. Están mejor informados sobre problemas relacionados con la seguridad y saben cómo ubicar la información en las redes con metodología usada por los hackers, no ganan mucha credibilidad ni confianza, debido a su pasado, si tienen alcance a información importante podrían pasarla inadvertidamente a través de una red insegura, poniendo en riesgo al lugar donde laboran.

- Sombreros Blancos (White Hats): Se los describió con anterioridad. Son personas con habilidades similares a las de los crackers, debido a sus ideales y forma de trabajo son considerados como verdaderos hackers éticos, normalmente trabajan como consultores de seguridad.
- Empresas de Consultoría (Consulting Firms): Son empresas de consultoría informática que con la creciente demanda de evaluaciones de seguridad, ofrecen a sus clientes pruebas de su seguridad mediante técnicas hacker avalándose mediante un sin número de credenciales y certificados. Pueden poseer en su personal a hackers de sombreros reformados y hackers de sombreros grises.

2.5.6- Ética del hacker

La ética hacker es una nueva ética surgida de y aplicada a las comunidades virtuales o ciber comunidades, aunque no exclusivamente. La expresión se suele atribuir al periodista Steven Levy en su ensayo seminal Hackers[6], donde describe y enuncia con detalle los principios morales que surgieron a finales de los años cincuenta en el Laboratorio de Inteligencia Artificial del MIT y, en general, en la cultura de los aficionados a la informática de los años sesenta y setenta. Aquellos principios que se resumen en el acceso libre a la información y en que la informática puede mejorar la calidad de vida de las personas han constituido la base de la mayor parte de definiciones que se han elaborado posteriormente. Uno de sus mentores actuales ha sido el finlandés Himanen.

Pekka Himanen[7], *"En el centro de nuestra era tecnológica se hallan unas personas que se autodenominan hackers. Se definen a sí mismos como personas que se dedican a programar de manera apasionada y creen que es un deber para*

6 Heroes of the Computer Revolution, 1984

7 La ética del hacker y el espíritu de la era de la información

ellos compartir la información y elaborar software gratuito. No hay que confundirlos con los crackers, los usuarios destructivos cuyo objetivo es el de crear virus e introducirse en otros sistemas: un hacker es un experto o un entusiasta de cualquier tipo que puede dedicarse o no a la informática. En este sentido, la ética hacker es una nueva moral que desafía la ética protestante del trabajo, tal como la expuso hace casi un siglo Max Weber en su obra La ética protestante y el espíritu del capitalismo, y que está fundada en la laboriosidad diligente, la aceptación de la rutina, el valor del dinero y la preocupación por la cuenta de resultados."

En comparación a la moral presentada por Weber, la ética del trabajo para el hacker se funda en el valor de la creatividad, y consiste en combinar la pasión con la libertad. El dinero deja de ser un valor en sí mismo y el beneficio se cifra en metas como el valor social y el libre acceso, la transparencia y la franqueza.

2.5.7- Valores fundamentales

La ética hacker es una ética basada en una determinada serie de valores. Himanen rescata algunos fundamentales, a saber:

- Pasión
- Libertad
- Conciencia social
- Verdad
- Anti-corrupción
- Lucha contra la alienación del hombre
- Igualdad social
- Libre acceso a la información (conocimiento libre)
- Valor social (reconocimiento entre semejantes)

- Accesibilidad
- Actividad
- Preocupación responsable
- Curiosidad
- Creatividad
- Interés

2.5.8- Principios Éticos

- **Principio de Accesibilidad**. El sujeto de un registro electrónico tiene el derecho de acceder al registro y a exigir la exactitud del mismo con relación a su precisión, integridad y relevancia.
- **Principio de Privacidad y Disposición de la Información.** Todas las personas poseen el derecho fundamental a la privacidad y, en consecuencia, a ser informadas y ejercer el derecho de autorizar la recolección, almacenamiento, acceso, uso, comunicación, manipulación y disposición de la información sobre sí mismas.
- **Principio de Transparencia.** La recolección, almacenamiento, acceso, uso, comunicación, manipulación y disposición de información personal debe ser revelado en tiempo y forma apropiados al sujeto de esos datos.
- **Principio de Seguridad.** Todas las personas tienen el derecho a que la información que ha sido legítimamente recolectada sobre sí, sea debidamente protegida, mediante todas las medidas disponibles, razonables y apropiadas tendientes a evitar pérdidas, degradación, así como la destrucción, el acceso, uso, manipulación, modificación o difusión no autorizada.

- **Principio de Garantía.** El derecho fundamental sobre el control de la recolección, el almacenamiento, acceso, uso, manipulación, comunicación y disposición de la información personal, está condicionado sólo por las necesidades legítimas, apropiadas y relevantes de información en una sociedad libre, responsable y democrática, así como por los correspondientes derechos iguales y competentes de otras personas.
- **Principio de la alternativa menos invasora**. Cualquier acción legítima que deba interferir con los derechos del individuo a su privacidad o al control sobre la información relativa a ésta, deberá sólo ser efectuada de la forma menos invasora posible, tal que garantice el mínimo de interferencia a los derechos de las personas afectadas.
- **Principio de Responsabilidad.** Cualquier interferencia con los derechos de privacidad de un individuo o del derecho de tener control sobre la información relativa a su persona, debe ser justificada a tiempo y de manera apropiada ante la persona afectada.

2.5.9- Modalidades de Ethical Hacking.

- Red Teaming: Es una prueba encubierta, es decir que sólo un grupo selecto de ejecutivos sabe de ella. En esta modalidad son válidas las técnicas de "Ingeniería Social" para obtener información que permita realizar ataque. Ésta obviamente es más real y evita se realicen cambios de última hora que hagan pensar que hay un mayor nivel de seguridad en la organización.
- Blue Teaming: El personal de informática conoce sobre las pruebas. Esta modalidad se aplica cuando las medidas tomadas por el personal de seguridad

de las organizaciones ante un evento considerado como incidente, repercuten en la continuidad de las operaciones críticas de la organización.

- Hacking Ético Externo (Caja Blanca): Se facilita información para poder realizar la intrusión. Se analiza en profundidad y extensión todas las posibles vulnerabilidades de seguridad al alcance de un atacante de los sistemas de comunicaciones sometidos a estudio.
- Hacking Ético Externo (Caja Negra): Es esencialmente lo mismo que en el de Caja Blanca con la dificultad añadida de que no se facilita ningún tipo de información inicial.
- Hacking Ético Interno: El ámbito de esta auditoría es la red interna de la empresa, para hacer frente a la amenaza de intento de intrusión.
- Hacking de Aplicaciones Web: Se simulan los intentos de ataque reales a las vulnerabilidades de una o varias aplicaciones determinadas, como pueden ser: sistemas de comercio electrónico, de información, o de acceso a bases de datos.
- Hacking Ético de Sistemas de Comunicaciones: esta auditoría se analiza la seguridad de las comunicaciones tales como:

✓ redes de datos,
✓ hardware de red,
✓ comunicaciones de voz,
✓ fraude en telecomunicaciones

Principalmente para estudiar la disponibilidad de los sistemas, la posibilidad de una interceptación o introducción no autorizada de información.

- Hacking Ético VozIP: los ataques que pueden sufrir los sistemas VozIP son múltiples: robo de servicio, interceptación de comunicaciones, denegación de

comunicaciones telefónicas, entre otros, por lo que identifica los puntos débiles en la infraestructura de comunicaciones para minimizar estos riesgos.

- Test de Denegación de Servicio (DoS): este test refleja el grado de solidez o resistencia de un servicio ante la agresión de un atacante local o remoto que intente deshabilitarlo.

2.5.10- Etapas del Ethical Hacking

✓ Reconocimiento

El reconocimiento se refiere a la fase preparatoria donde el hacker obtiene toda la información necesaria de su objetivo o victima antes de lanzar el ataque. Esta fase también puede incluir el escaneo de la red que el Hacker quiere atacar no importa si va a ser interno o externo. Esta fase le permite crear una estrategia.

Este período puede incluir la Ingeniería Social, buscar en la basura (Dumpsterdiving), buscar que tipo de sistema operativo y aplicaciones usa el objetivo o víctima, cuales son los puertos que están abiertos, donde están localizados los routers (enrutadores), cuales son los [8]host más accesibles, buscar en las bases de datos del Internet (Whois) información como direcciones de Internet (IP), nombres de dominios, información de contacto, servidores de email y toda la información que se pueda extraer de los [9]DNS .

Esta fase le puede tomar bastante tiempo al Hacker ya que tiene que analizar toda la información que ha obtenido para lanzar el ataque con mayor precisión. Así poder demostrar a la empresa las debilidades de seguridad que poseen y tener ya sea una ganancia personal, económica, o de satisfacción, con el hecho de dañar a la organización.

8 terminales, computadoras
9 Domain Name Server.

✓ Escaneo

Esta fase se la realiza antes de lanzar un ataque a la red (network). En el escaneo se utiliza toda la información que se obtuvo en la Fase del Reconocimiento (Fase 1) para identificar vulnerabilidades específicas. Por ejemplo, si en la Fase 1 se descubrió que el objetivo o víctima usa el sistema operativo Windows XP entonces se busca vulnerabilidades específicas que tenga ese sistema operativo para saber por dónde atacarlo.

También se hace un escaneo de puertos para ver cuáles son los puertos abiertos y saber por cual puerto va entrar, se usa herramientas automatizadas para escanear la red y los host en busca de más vulnerabilidades que permitan el acceso al sistema.

Objetivos

- Detectar sistemas vivos en la red
- Descubrir puertos activos
- Descubrir el sistema operativo
- Descubrir los servicios ejecutándose y presentes en el sistema
- Descubrir direcciones IPs

Tipos

- Escaneo de puertos: Es comprobar los servicios corriendo en el objetivo enviando una secuencia de mensajes en un intento de entrar.
- Escaneo de Red: Es el proceso de identificar host activos en la red
- Escaneo de Vulnerabilidades

✓ Ganar acceso (Gaining Access)

Esta es una de las fases más importantes para el Hacker porque es la fase de penetración al sistema, en esta fase el Hacker explota las vulnerabilidades que encontró en la fase 2. La explotación puede ocurrir localmente, offline (sin estar conectado), sobre el LAN (Local Area Network), o sobre el Internet y puede incluir técnicas como [10]buffer overflows, denial-of-service (negación de servicios), sesión hacking (secuestro de sesión), y password cracking (romper o adivinar claves).

Los factores que ayudan al Hacker en esta fase a tener una penetración exitosa al sistema dependen de cómo es la arquitectura y de cómo está configurado el sistema objetivo o víctima, otro factor a tener en cuenta es el nivel de destrezas, habilidades y conocimientos sobre seguridad informática y redes que tenga el Hacker y el nivel de acceso que obtuvo al principio de la penetración (Fase 3).

✓ Mantener el Acceso (maintaining access)

Una vez que el Hacker gana acceso al sistema objetivo (Fase 3) su prioridad es mantener el acceso que gano en el sistema. En esta fase el Hacker usa sus recursos y los del sistema, usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas que quiere atacar, también usa programas llamados sniffers para capturar todo el tráfico de la red, incluyendo sesiones de telnet y FTP[11].

En esta fase el Hacker puede tener la habilidad de subir, bajar y alterar programas e información, el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema y hace uso de Backdoor[12] y Troyanos para

10 Desbordamiento del buffer
11 File Transfer Protocol.
12 puertas traseras

ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. También usan los Troyans[13] para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito almacenadas en el sistema.

✓ Cubrir las huellas (Covering Tracks)

En esta fase el Hacker trata de destruir toda la evidencia de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el Hacker podrá seguir penetrando el sistema cuando quiera, además borrando sus huellas evita ser detectado y ser atrapado por la policía o los Federales.

Las herramientas y técnicas que usa para esto son caballos de Troya, Steganography, Tunneling, Rootkits y la alteración de los “log files” (Archivos donde se almacenan todos los eventos ocurridos en un sistema informático y permite obtener información detallada sobre los hábitos de los usuarios), una vez que el Hacker logra plantar caballos de Troya en el sistema este asume que tiene control total del mismo. Los objetivos de cubrir las huellas son: mantener escondido el acceso al sistema, modificar los logs del sistema donde se encuentren evidencias y esconder los archivos que se usará para el hacking.

13 caballos de Troya

2.5.3.2- Beneficios de Ethical Hacking.

- Ofrecer un panorama acerca de las vulnerabilidades halladas en los sistemas de información, lo cual es de gran ayuda al momento de aplicar medidas correctivas.
- Deja al descubierto configuraciones no adecuadas en las aplicaciones instaladas en los sistemas (equipos de cómputo, switches, routers, firewalls) que pudieran desencadenar problemas de seguridad en las organizaciones.
- Identificar sistemas que son vulnerables a causa de la falta de actualizaciones.
- Disminuir tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización.

2.5.3.3- Laboratorios de Ethical Hacking

Las máquinas virtuales son una de las muchas tecnologías de la información utilizados para apoyar sistemas avanzados de información y educación de aseguramiento. Su despliegue en la educación tiene el potencial de apoyar un mayor número de estudiantes con hardware significativamente menor y los recursos financieros necesarios.

Las topologías de máquinas virtuales más utilizadas en laboratorios de Ethical Hacking se basan en la estructura de NETLAB+[14], ya que fueron diseñados por el Centro de Sistemas de Garantía de la seguridad y de la Información (CSSI) y el Grupo de Desarrollo de Red (NDG), financiado por (NSF) Educación Avanzada de la Fundación Nacional de Ciencias Tecnológicas (ATE) del Departamento de Educación del programa de Pregrado (DUE) No. 0702872 y 1002746.

2.5.3.4- Topología CNSS 4011 Pod

14 Dispositivo de servidor con todas las herramientas de software precargados para las instituciones académicas que alberga equipos de laboratorio real, máquinas virtuales y los programas necesarios para los alumnos.

Esta topología consiste en 5 máquinas virtuales unidas entre sí a través de redes virtuales, estas máquinas virtuales proporcionan el entorno para que un estudiante o equipo pueda realizar los laboratorios de Seguridad de la Información CNSS 4011[15].

Requerimientos

- Al menos 55 gigabytes de almacenamiento para el CNSS 4011 pod.
- 15 gigabytes para almacenamiento por estudiante.

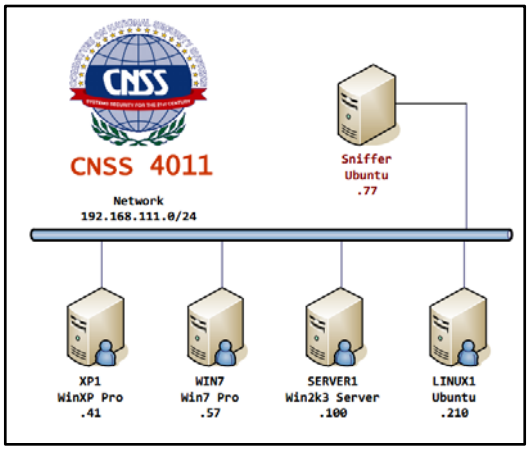

Figura 2.5.2: Topología CNSS 4011

Tabla 2. 1 Topología CNSS 4011

Máquina Virtual	**Rol**
XP1	Microsoft Windows XP Professional
WIN7	Microsoft Windows 7 Professional
SERVER1	Microsoft Windows 2003 Server
LINUX1	Ubuntu v10.10
Sniffer	Ubuntu v10.10

15 Certificación del Comité de Sistemas de Seguridad Nacional 4011

Requerimientos de máquinas virtuales:

1. CNSS 4011 Master LINUX1

a. Memoria– 1 GB

b. Disco Duro – 10 GB

c. Sistema Operativo – Ubuntu 32-bit

2. CNSS 4011 Master LINUX2

a. Memoria – 1 GB

b. Disco Duro – 10 GB

c. Sistema Operativo – Ubuntu 32-bit

3. CNSS 4011 Master XP1

a. Memoria – 1 GB

b. Disco Duro – 10 GB

c. Sistema Operativo – Windows XP 32-bit

4. CNSS 4011 Master WIN7

a. Memoria – 1 GB

b. Disco Duro – 15 GB

c. Sistema Operativo – Windows 7 32-bit

5. CNSS 4011 Master SERVER1

a. Memoria – 1 GB

b. Disco Duro – 10 GB

c. Sistema Operativo – Windows Server 2003 32-bit

Programas instalados en las máquinas

- SlavaSoft HashCalc
- CrypTool
- ophcrack
- Zenmap
- Wireshark
- Eraser
- Restoration
- PuTTY

2.5.3.5- Seguridad Multipropósito (MSEC) Pod

Esta topología consiste en 8 máquinas virtuales unidas entre sí a través de redes virtuales, estas máquinas virtuales proporcionan el entorno para que un estudiante o equipo pueda realizar los laboratorios de Seguridad de la Información.

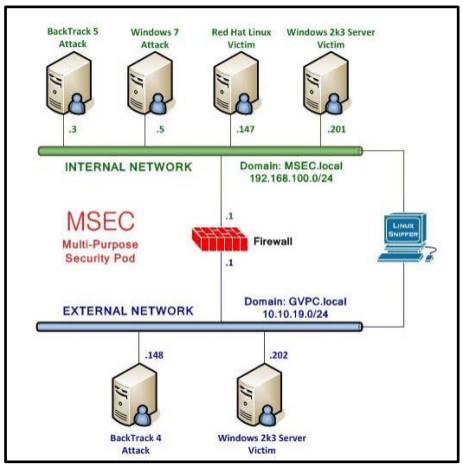

Figura 2. 1 Topología MSEC

Tabla 2. 2 Topología MSEC

Máquina Virtual	**Rol**
BackTrack 5 Attack	BackTrack 5
Windows 7 Attack	Microsoft Windows 7 Professional
Red Hat Linux Victim	Microsoft Windows 2003 Server
Windows 2k3 Server Victim	Microsoft Windows 2003 Server (internal network)
pfSense Firewall	Firewall
Sniffer	Linux based Sniffer
BackTrack 4 Attack	BackTrack 4
Windows 2k3 Server Victim	Microsoft Windows 2003 Server (external network)

Requerimientos:

- Al menos 28 gigabytes de almacenamiento para el pod.
- 15 gigabytes para almacenamiento por estudiante.

2.6- Test de intrusión

A través del Ethical Hacking es posible detectar el nivel de seguridad interno y externo de los sistemas de información de una organización, esto se logra determinando el grado de acceso que tendría un atacante con intenciones maliciosas a los sistemas informáticos con información crítica.

Las pruebas de penetración son un paso previo a los análisis de fallas de seguridad o riesgos para una organización.

Estas pruebas dejan al descubierto las vulnerabilidades que pudieran ser vistas y explotadas por individuos no autorizados y ajenos a la información como: crackers, hackers, ladrones, ex-empleados, empleados actuales, entre otros. Las pruebas de penetración, están totalmente relacionadas con el tipo de información que cada organización maneja, por tanto según la información se determina la estructura y las herramientas de seguridad.

Estas pruebas de penetración permiten:

- Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.
- Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Proveer recomendaciones en base a las prioridades de la organización.

La realización de las pruebas de penetración está basada en las siguientes fases:

1. Recopilación de información
2. Descripción de la red
3. Exploración de los sistemas
4. Extracción de información
5. Acceso no autorizado a información sensible o crítica
6. Auditoría de las aplicaciones web
7. Elaboración de informes
8. Informe final

2.7- Tipos de Ethical Hacking.

Las pruebas de penetración se enfocan principalmente en las siguientes perspectivas:

- Pruebas de penetración con objetivo: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos de la organización.
- Pruebas de penetración sin objetivo: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización.
- Pruebas de penetración a ciegas: en estas pruebas sólo se emplea la información pública disponible sobre la organización.
- Pruebas de penetración informadas: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada.
- Pruebas de penetración externas: son realizas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- Pruebas de penetración internas: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

2.8- Metodologías

2.8.1- OSSTMM 3

Esta metodología se encuentra realizada por ISECOM (Institute for Security and Open Methodologies), una organización sin ánimo de lucro de dedicada al desarrollo de metodologías de libre utilización para la verificación de la seguridad, la programación segura, la verificación de software y la concientización en seguridad.

Es una metodología científica para la exacta caracterización de la seguridad operacional (OPSEC), mediante el examen y la correlación de los resultados de las pruebas en una manera consistente y confiable. Esta metodología es adaptable a casi cualquier tipo de auditoría, incluyendo las pruebas de penetración, hacking ético, las evaluaciones de seguridad, evaluaciones de vulnerabilidad. Está escrito como un documento de investigación sobre la seguridad y está diseñado para la verificación de la seguridad objetiva y presentación de indicadores en un nivel profesional.

Uno de sus objetivos es proporcionar directrices que, si se siguen correctamente, le permitirán al analista realizar una auditoría de certificación OSSTMM. Estas directrices existen para asegurar lo siguiente:

1) La prueba se realizó a fondo.
2) La prueba incluyó a todos los canales necesarios.
3) La postura de la prueba de cumplimiento con la ley.
4) Los resultados son medibles de forma cuantificable.
5) Los resultados son consistentes y repetibles.
6) Los resultados contienen sólo los hechos que se deriven de las mismas pruebas.

El modelo de seguridad completo puede ser dividido en secciones administrables para las pruebas. Cada sección puede a su vez ser vista como una colección de módulos de test con cada módulo dividido en un conjunto de tareas.

La metodología fluye desde el módulo inicial hasta completar el módulo final, permite la separación entre recolección de datos y tests de verificación. El flujo también determina los puntos precisos de cuando extraer e insertar estos datos. Al definir la metodología de análisis no se restringe la creatividad del analista

introduciendo estándares excesivamente formales e inflexibles que la calidad de los tests sufra.

Cada módulo tiene una relación con el anterior y posterior. Cada fase tiene aspectos interrelacionados a otros módulos y algunos se interrelacionan con todas las otras secciones. Normalmente, los análisis de seguridad comienzan con una entrada que corresponde a las direcciones de los sistemas a ser analizados. El análisis de seguridad finaliza con el inicio de la fase de análisis y la construcción del informe final. Esta metodología no afecta la forma, tamaño, estilo o contenido del informe final ni especifica como los datos deben ser analizados. Esto es responsabilidad del analista de seguridad o la organización.

Las secciones son el modelo total de seguridad dividido en porciones manejables y analizables. El módulo requiere una entrada para ejecutar las tareas del módulo y de otros módulos en otras secciones. Las tareas son los tests de seguridad a ejecutarse dependiendo de la entrada del módulo. Los resultados de las tareas pueden ser inmediatamente analizados para actuar como un resultado procesado o se pueden dejar en bruto (sin analizar). De cualquier modo, estos son considerados la salida del módulo. Esta salida es a menudo la entrada para el siguiente módulo o en algunos casos, como equipos recién descubiertos; pueden ser la entrada para un módulo anterior.

Si se lo dividiría en etapas sería de la siguiente manera:

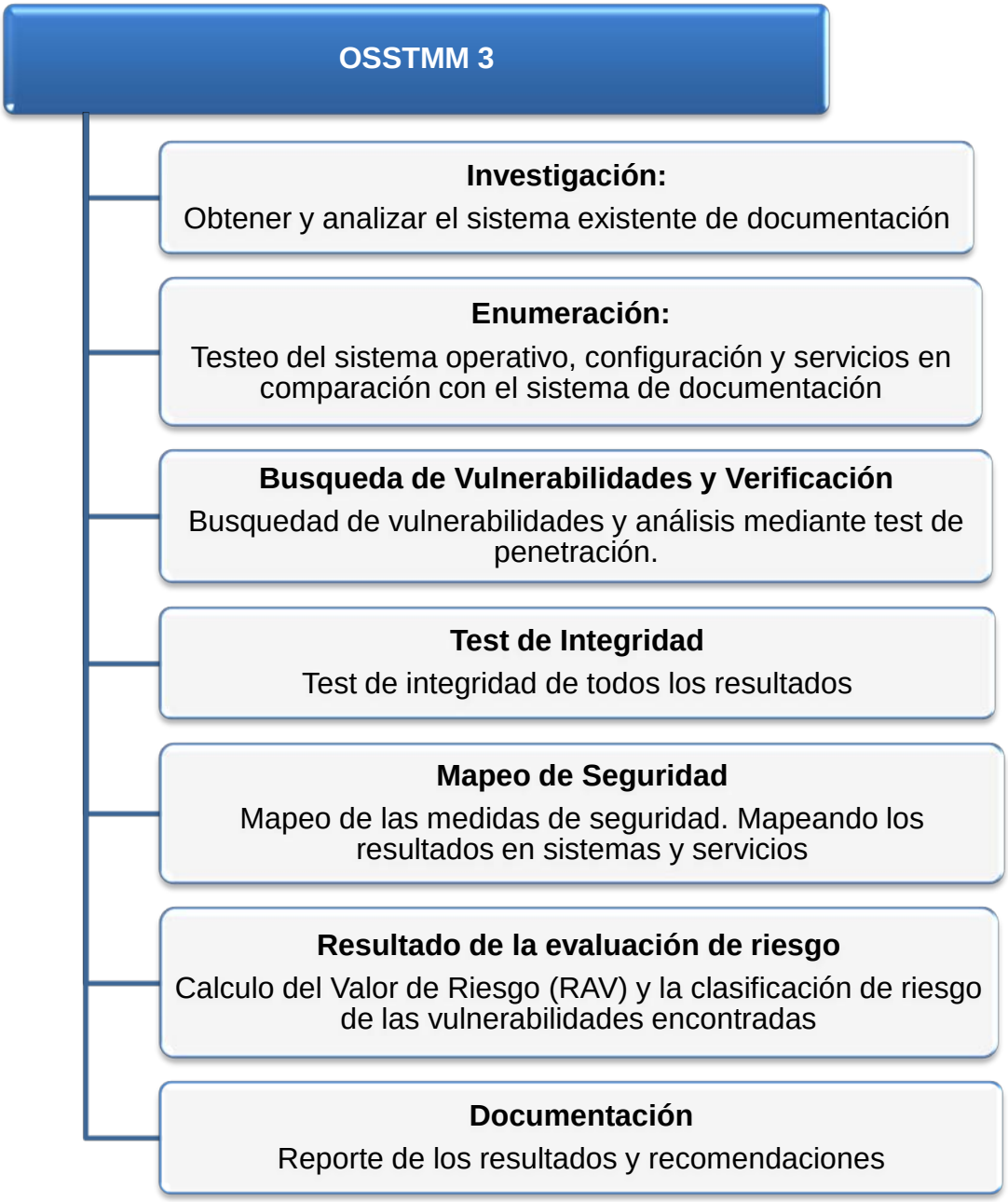

Figura 2.8: OSSTMM3

Se compone de las siguientes secciones:

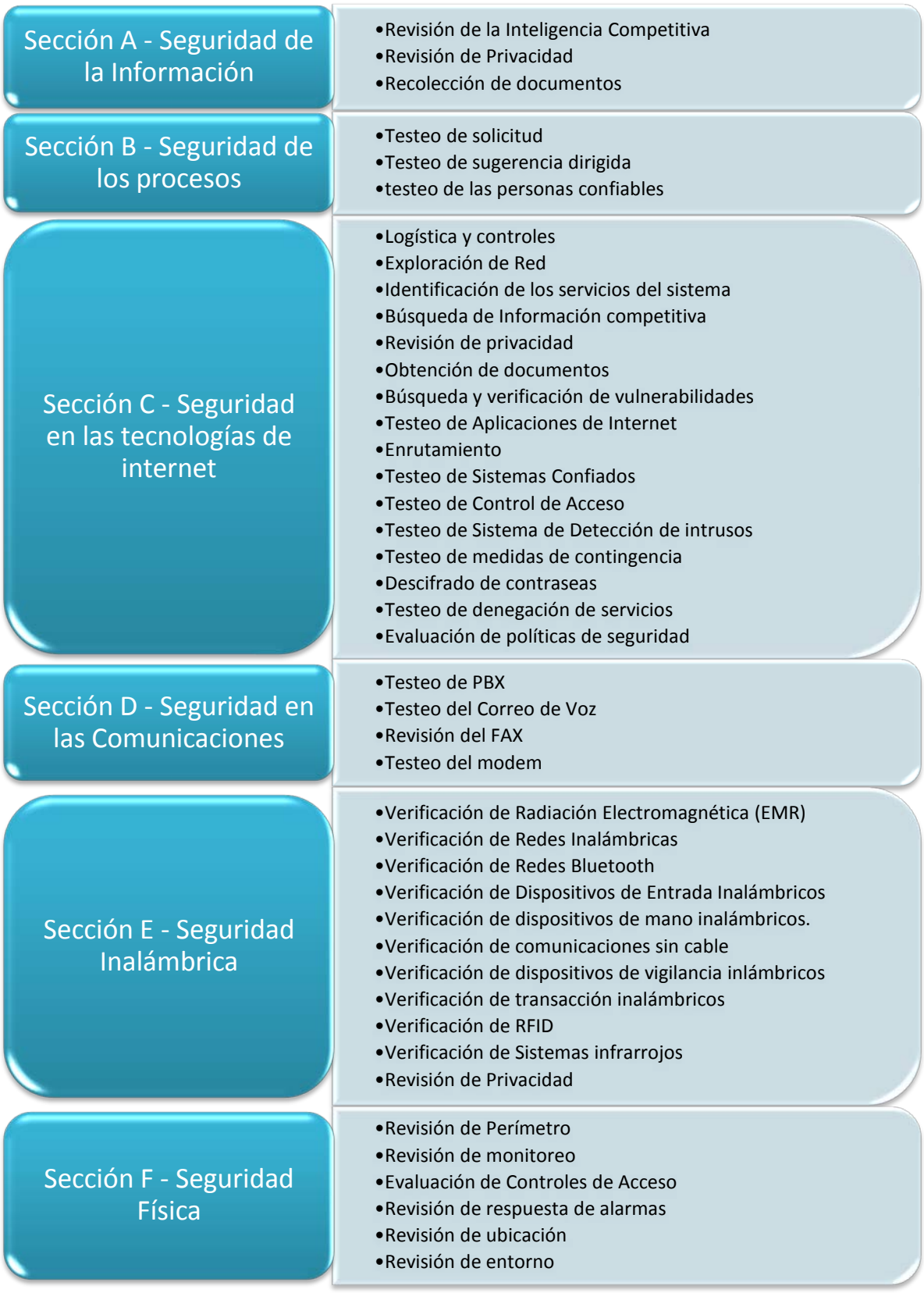

Figura 2.8.1: Secciones OSSTMM3

2.8.2- P r o c e s o

El proceso de un análisis de seguridad, se concentra en evaluar las siguientes áreas, que reflejan los niveles de seguridad presentes, siendo estos el ambiente definido para el análisis de seguridad. Estos son conocidos como las Dimensiones de Seguridad:

- ✓ **Visibilidad:** Es lo que puede verse, registrarse, o monitorearse en el nivel de seguridad con o sin la ayuda de dispositivos electrónicos.
- ✓ **Acceso:** Es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física.
- ✓ **Confianza:** Es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.
- ✓ **Autenticación:** Es la medida por la cual cada interacción en el proceso está privilegiada.
- ✓ **No-repudio:** Provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.
- ✓ **Confidencialidad:** Es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.
- ✓ **Privacidad:** implica que el proceso es conocido únicamente por los sistemas o partes involucradas.
- ✓ **Autorización:** Es la certeza que el proceso tiene una razón o justificación de negocios y es administrado responsablemente dando acceso permitido a los sistemas.

- ✓ **Integridad:** Es la certeza que el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reversado sin el conocimiento de los sistemas o partes involucradas.
- ✓ **Seguridad:** Son los medios por los cuales un proceso no puede dañar otros sistemas, o procesos incluso en caso de falla total del mismo.
- ✓ **Alarma:** es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad.

2.9- Herramientas de Ethical Hacking

2.9.1- Footprinting

El Footprinting es el primer paso que es tomado por los Harkers, consiste en la búsqueda de toda la información pública, bien porque haya sido publicada a propósito o por desconocimiento que pueda haber sobre el sistema objetivo, es decir, se buscan todas las huellas posibles, como direcciones IP, servidores internos, cuentas de correo de los usuarios, nombres de máquinas, información del registrador del dominio, tipos de servidores, ficheros con cuentas y/o credenciales de usuarios, impresoras, cámaras IP, metadatos, entre otros.

Las herramientas más comunes de Footprinting son:

a) *Dnsstuff*: Página web creada por SolarWinds. Herramienta que al ingresar a la misma permite conocer la IP del visitante, su proveedor de Internet y su país, además se puede hacer todo tipo de consultas como por ejemplo: trazar rutas, pings, localizar ciudad y país de una IP, información de dominios, whois, test de velocidad de DNS, Spam Database entre otros.

URL: www. dnsstuff.com

b) *Traceroute*: [16]*Es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host. Se obtiene además una estadística del RTT o latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación. Esta herramienta se llama traceroute en UNIX, Mac1 y GNU/linux, mientras que en Windows se llama tracert.*

c) Whois*:* Es un protocolo TCP que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet. Las consultas se las realiza normalmente utilizando línea de comandos, pero actualmente existen páginas web que permiten realizarlas.

2.9.2- Fingerprinting:

Se refiere a la detección del sistema operativo de la computadora víctima – destino. Es muy importante para un atacante determinar el tipo de sistema operativo de su víctima ya que cada sistema operativo responde de manera diferente al mismo mensaje ICMP (Protocolo de Mensajes de Control de Internet), también se pueden llevar a cabo ataques ya que el agresor sabe sobre las vulnerabilidades de los sistemas operativos.

Existen cuatro firmas que se ven para determinar el sistema operativo

- TTL(Time To Live): Tiempo de vida de un paquete de salida que es establecido por el sistema operativo
- Tamaño de ventana
- DF: si el sistema operativo establece el bit de fragmento
- TOS (Technical Operating System): si el sistema operativo establece el tipo de servicio.

[16] http://es.wikipedia.org/wiki/Traceroute

Técnicas

- Activo de SO: Examina el comportamiento de la fila del protocolo TCP/IP
- Análisis de vulnerabilidades: es un análisis que busca identificar e informar fallas en los dispositivos y en los procesos tecnológicos de las vulnerabilidades que posee.
- Explotación de vulnerabilidades
- Generación de informes.

2.9.3- Escaneo de Puertos:

El escaneo de puertos permite descubrir puertos abiertos, los mismos que son usados para encontrar las vulnerabilidades del sistema. Durante este proceso, se puede encontrar el host, los sistemas operativos involucrados, firewalls, sistemas de detección de intrusos, servidores / servicios, dispositivos perimetrales, enrutamiento y la topología de red en general (disposición física de la red), que forman parte de la organización de destino.

2.9.4- Enumeración

Es la recopilación y compilación de nombre de usuario, nombres de equipos, recursos de red, recursos compartidos y servicios, y también involucra a las conexiones activas de los sistemas y las preguntas dirigidas.

El objetivo principal de enumeración consiste en identificar las cuentas de usuario, nombres de equipos, recursos de red, recursos compartidos y servicios, y también involucra a las conexiones activas de los sistemas y los recursos del sistema menos protegidos.

En este proceso los hackers se conectan a los equipos de la red del objetivo usando las herramientas de hacking para encontrar los detalles de seguridad y así obtener la información.

- **Pasos para la Enumeración**

1. Extraer los nombres de usuario que utilizan enumeración.
2. Recopilar información sobre el host mediante sesiones nulas.
3. Realizar enumeración de Windows utilizando la herramienta [17]Superscan(es una potente aplicación muy útil y fácil de emplear que permite cambiar la IP del PC o computadora sin tener que reiniciar el módem o router.).
4. Adquirir las cuentas de usuario mediante la herramienta getacct ([18]*muestra fugas de información al abrir una sesión anónima y presenta información como: enumeración de usuarios, cuentas de usuarios, entre otras*).
5. Realizar el escaneo de puertos SNMP ([19]*es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento*).

2.9.5- Ingeniería Social

El término Ingeniería Social hace referencia al arte de manipular personas para evitar los sistemas de seguridad. Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador u otra persona de confianza o de mayor rango, para que revelen sus contraseñas u otra información, a través de las debilidades propias de una implementación y mantenimiento de un sistema.

La ingeniería social puede llevarse a cabo a través de una serie de medios:

- Por teléfono
- Por correo electrónico

[17] http://recursosenweb.com/superscan-un-programa-que-cambia-tu-ip/
[18] http://www.hackguide4u.com/2010/02/enumeration-tools.html
[19] http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

- Por correo tradicional
- Por mensajería instantánea

- **Los métodos**

Para usar la ingeniería social se pueden usar varios métodos:

- Demanda directa: a un individuo se le pide completar su tarea directamente, la víctima está enterada de lo que el atacante quiere exactamente que haga.
- Situación simulada: es ejecutado indirectamente, esto no significa que las situaciones no tienen que ser basadas en hechos reales sino que cuando menos falsas sean, mayor la factibilidad de que el individuo en cuestión juegue el papel que le fue designado.

Una de las herramientas esenciales usadas para la ingeniería social es una buena recolección de los hábitos de los individuos.

- **Fases**

En general, los métodos de la ingeniería social están organizados de la siguiente manera:

- Una fase de acercamiento para ganarse la confianza del usuario.
- Una fase de alerta, para desestabilizar al usuario y observar la velocidad de su respuesta.
- Una distracción, es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre en el alerta.

La ingeniería social se dirige a los individuos con menos conocimientos, dado que los argumentos y otros factores de influencia tienen que ser construidos generando una situación creíble que el individuo ejecute.

2.10- ITIL

"ITIL (Biblioteca de Infraestructura de Tecnologías de Información), es un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI, que tiene como objetivo mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrece soluciones con el menor impacto y a la mayor brevedad posible."

ITIL v3 ayuda a las organizaciones a adoptar un punto de vista más estratégico que abarca todo el ciclo de vida del servicio. Este tipo de enfoque reporta algunas ventajas:

- Favorecer la integración de la estrategia de negocio con la estrategia de servicios de TI
- Facilitar la implantación y gestión de servicios adaptados a unas necesidades de negocio dinámico, volátil, altamente cambiante y de alto riesgo.
- Identificar las oportunidades de mejora y cambio a lo largo de todo el ciclo de vida del servicio.

2.10.1- Definición de Servicio según ITIL:

Es un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados.

Para definir un servicio es fundamental, conocer los requerimientos que se pretende atender, un servicio optimiza el rendimiento y reduce las limitaciones, mejora las probabilidades de éxito de una tarea, proyecto, proceso o actividad, un servicio que no resuelve un requerimiento es simplemente una idea.

2.10.2- El ciclo de vida de los servicios TI

ITIL constan de cinco fases, etapas o ciclos orientados a mejorar la vida de los servicios y mantiene ciertos principios como pilares. Los procesos ITIL v3 siguientes definen las políticas, estándares, guías de actuación, actividades e instrucciones de trabajo necesarias para una correcta gestión de los servicios TI.

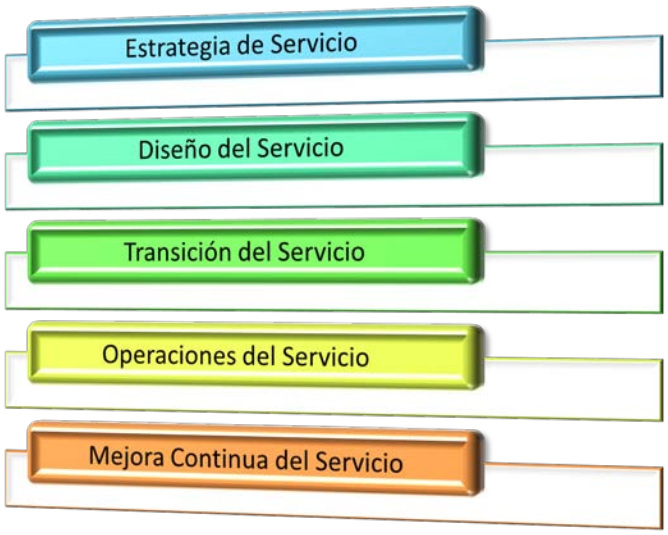

Figura 2. 2 Ciclo de Vida del Servicio

2.10.3- Estrategia del Servicio

Se enfoca en el estudio de mercado y posibilidades mediante la búsqueda de servicios innovadores que satisfagan al cliente.

Una correcta Estrategia del Servicio debe:

- Servir de guía a la hora de establecer y priorizar objetivos y oportunidades.
- Conocer el mercado y los servicios de la competencia.
- Armonizar la oferta con la demanda de servicios.
- Proponer servicios diferenciados que aporten valor añadido al cliente.
- Gestionar los recursos y capacidades necesarios para prestar los servicios ofrecidos teniendo en cuenta los costes y riesgos asociados.

- Alinear los servicios ofrecidos con la estrategia de negocio.
- Elaborar planes que permitan un crecimiento sostenible.
- Crear casos de negocio para justificar inversiones estratégicas.

La fase de Estrategia del Servicio es el eje que permite que las fases de Diseño, Transición y Operación del servicio se ajusten a las políticas y visión estratégica del negocio.

La Estrategia del Servicio debe responder a las siguientes preguntas tales como:

- ¿Qué servicios se debe ofrecer?
- ¿Cuál es el valor?
- ¿Cuáles son los clientes potenciales?
- ¿Cuáles son los resultados esperados?
- ¿Qué servicios son prioritarios?
- ¿Qué inversiones son necesarias?
- ¿Cuál es el retorno a la inversión o ROI?
- ¿Qué servicios existen ya en el mercado que puedan representar una competencia directa?
- ¿Cómo se puede diferenciar la competencia?

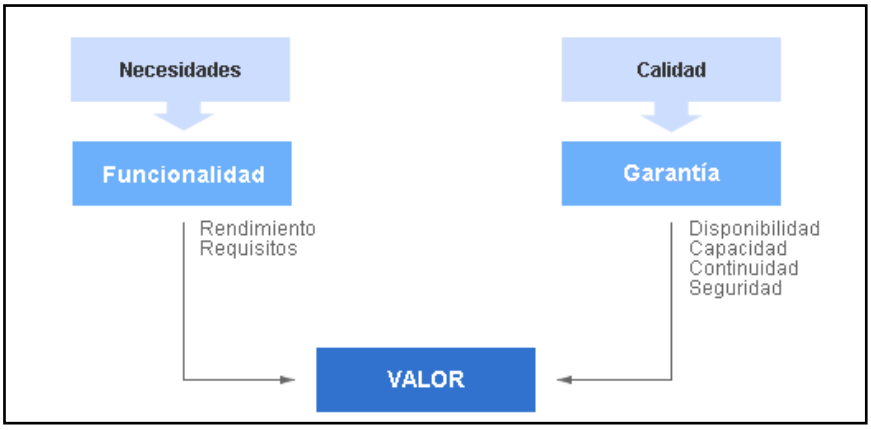

Figura 2.10.3: Valor del Servicio

2.10.4- Activos del servicio

Para que una organización TI pueda ofrecer valor en forma de servicios debe hacer buen uso de sus recursos y capacidades.

Los recursos son la "materia prima" necesaria para la prestación del servicio e incluyen el capital, las infraestructuras, aplicaciones e información.

Las capacidades representan las habilidades desarrolladas a lo largo del tiempo para transformar los recursos en valor a través de la gestión, la organización, los procesos y el conocimiento.

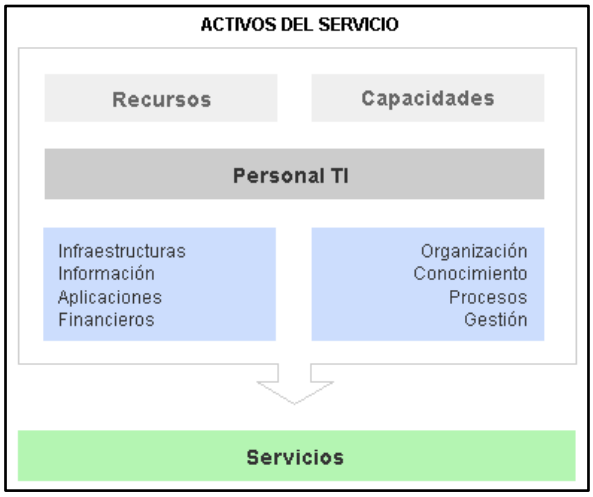

Figura 2.10.4: Activos del Servicio

2.10.5- Proveedores de servicios

ITIL considera tres tipos diferentes de proveedores de servicios:

- Tipo I o proveedor de servicios interno: los servicios prestados forman parte esencial en el posicionamiento estratégico de la organización.
- Tipo II o unidad de servicios compartidos: presta servicio a diferentes unidades de negocio que operan bajo un paraguas común.
- Tipo III o proveedores de servicio externos: ofrecen sus servicios en el mercado a diferentes clientes que frecuentemente serán competidores entre sí.

2.10.6- Procesos

Los procesos asociados directamente a la fase de Estrategia son:

a) Gestión Financiera: responsable de garantizar la prestación de servicios con unos costes controlados y una correcta relación calidad-precio.
b) Gestión del Portafolio de Servicios: responsable de la inversión en servicios nuevos y actualizados que ofrezcan el máximo valor al cliente minimizando a su vez los riesgos y costes asociados.
c) Gestión de la Demanda: responsable de la armonización de la oferta de los servicios ofrecidos con las demandas del mercado.

2.10.7- Diseño del Servicio

Diseñar nuevos servicios o modificar los ya existentes para su incorporación al catálogo de servicios y su paso al entorno de producción.

El Diseño del Servicio debe seguir las directrices establecidas en la fase de Estrategia y debe a su vez colaborar con ella para que los servicios diseñados:

✓ Se adecuen a las necesidades del mercado.
✓ Sean eficientes en costes y rentables.
✓ Cumplan los estándares de calidad adoptados.

El Diseño del Servicio debe tener en cuenta:

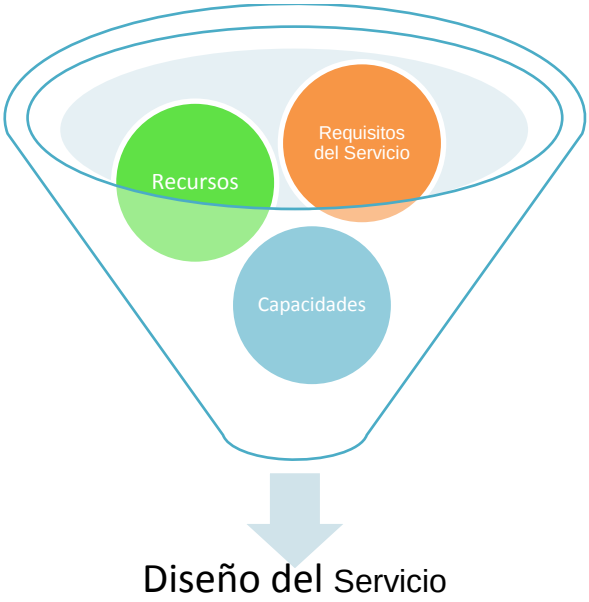

Figura 2.10.7: Diseño del Servicio

Una correcta implementación del Diseño del Servicio debe ayudar a responder cuestiones tales como:

- ✓ ¿Cuáles son los requisitos y necesidades de nuestros clientes?
- ✓ ¿Cuáles son los recursos y capacidades necesarias para prestar los servicios propuestos?
- ✓ ¿Los servicios son seguros, ofrecen la disponibilidad necesaria y se garantiza la continuidad del servicio?
- ✓ ¿Son necesarias nuevas inversiones para prestar los servicios con los niveles de calidad propuestos?
- ✓ ¿Están todos los agentes involucrados correctamente informados sobre los objetivos y alcance de los nuevos servicios o de las modificaciones a realizar en los ya existentes?

- **Diseño de soluciones de servicio**

Debe incluir de forma estructurada todos los elementos clave del nuevo o modificado servicio:

✓ Requisitos de negocio

✓ Requisitos de servicio (SLR)

✓ Adecuación a la estrategia del servicio

✓ Análisis funcional

✓ Estudios de los servicios prestados para ver si existen módulos reutilizables de otros servicios en cartera

✓ Análisis de costes (TCO) y retorno a la inversión

✓ Estudio de los recursos y capacidades involucradas

✓ Estrategias de contratación con los proveedores externos (si estos se consideraran necesarios)

- **Diseño del Portfolio de Servicios**

Incluye información sobre todos los servicios ofrecidos, los servicios en fase de desarrollo y los servicios retirados en términos de valor para el negocio.

El Portfolio de Servicios debe contener información sobre:

✓ Los objetivos del servicio

✓ Su valor: funcionalidad y garantía

✓ Su estado

✓ Los SLAs asociados

✓ Capacidades y recursos utilizados

✓ Sus costes y retorno esperado

✓ Los controles o métricas de calidad asociados

✓ Los responsables del mismo

✓ Servicios relacionados

✓ Proveedores externos involucrados (OLAs y UCs)

- **Diseño de la arquitectura del servicio**

La arquitectura debe tener en cuanto todos los elementos necesarios para la Gestión del Servicio así como la interrelación entre ellos y el mercado. Debe ofrecer una guía para el diseño y evolución del servicio teniendo en cuenta:

✓ La alineación entre la tecnología y el negocio.

✓ La infraestructura TI necesaria.

✓ La Gestión de las aplicaciones.

✓ La Gestión de los datos y la información.

✓ La Documentación y Gestión del Conocimiento.

✓ Los Planes de Despliegue del servicio.

- **Diseño de procesos**

La gestión basada en procesos es una de las señas de identidad de ITIL. En la fase de diseño del servicio se han de definir los procesos involucrados con una descripción detallada de sus actividades, funciones, organización, entradas y salidas.

- **Diseño de métricas y sistemas de monitorización**

Es imprescindible diseñar sistemas de medición y seguimiento que permitan evaluar tanto la calidad de los servicios prestados como la eficiencia de los procesos involucrados.

Existen cuatro tipos principales de métricas a considerar:

a) Progreso: cumplimiento de los calendarios previstos

b) Cumplimiento: adecuación a las políticas y requisitos predefinidos.

c) Eficacia: calidad de los resultados obtenidos.

d) Rendimiento: productividad de los procesos y gestión de los recursos utilizados.

- **Transición del Servicio**

La misión de la fase de Transición del Servicio es hacer que los productos y servicios definidos en la fase de Diseño del Servicio se integren en el entorno de producción y sean accesibles a los clientes y usuarios autorizados.

Sus principales objetivos se resumen en:

✓ Supervisar y dar soporte a todo el proceso de cambio del nuevo (o modificado) servicio.

✓ Garantizar que los nuevos servicios cumplen los requisitos y estándares de calidad estipulados en las fases de Estrategia y la de Diseño.

✓ Minimizar los riesgos intrínsecos asociados al cambio reduciendo el posible impacto sobre los servicios ya existentes.

✓ Mejorar la satisfacción del cliente respecto a los servicios prestados.

Para cumplir adecuadamente estos objetivos es necesario que durante la fase de Transición del Servicio:

a) Se planifique todo el proceso de cambio.

b) Se creen los entornos de pruebas y preproducción necesarios.

c) Se realicen todas las pruebas necesarias para asegurar la adecuación del nuevo servicio a los requisitos predefinidos.

d) Se establezcan planes de roll-out (despliegue) y roll-back (retorno a la última versión estable).

e) Se cierre el proceso de cambio con una detallada revisión post-implementación.

- **Procesos**

✓ Planificación y soporte a la Transición: responsable de planificar y coordinar todo el proceso de transición asociado a la creación o modificación de los servicios TI.

- ✓ Gestión de Cambios: responsable de supervisar y aprobar la introducción o modificación de los servicios prestados garantizando que todo el proceso ha sido convenientemente planificado, evaluado, probado, implementado y documentado.
- ✓ Gestión de la Configuración y Activos del Servicio: responsable del registro y gestión de los elementos de configuración (CIs) y activos del servicio. Este proceso da soporte a prácticamente todos los aspectos de la Gestión del Servicio
- ✓ Gestión de Entregas y Despliegues: Responsable de desarrollar, probar e implementar las nuevas versiones de los servicios según las directrices marcadas en la fase de Diseño del Servicio.
- ✓ Validación y pruebas: responsable de garantizar que los servicios cumplen los requisitos preestablecidos antes de su paso al entorno de producción.
- ✓ Evaluación: responsable de evaluar la calidad general de los servicios, su rentabilidad, su utilización, la percepción de sus usuarios, etcétera
- ✓ Gestión del Conocimiento: gestiona toda la información relevante a la prestación de los servicios asegurando que esté disponible para los agentes implicados en su concepción, diseño, desarrollo, implementación y operación.

- **Operación del Servicio**

En este punto se monitoriza activa y pasivamente el funcionamiento del servicio, se registran eventos, incidencias, problemas, peticiones y accesos al servicio.

Los principales objetivos de la fase de Operación del Servicio incluyen:

- ✓ Coordinar e implementar todos los procesos, actividades y funciones necesarias para la prestación de los servicios acordados con los niveles de calidad aprobados.
- ✓ Dar soporte a todos los usuarios del servicio.
- ✓ Gestionar la infraestructura tecnológica necesaria para la prestación del servicio.

- ✓ Uno de los aspectos esenciales en la Operación del Servicio es la búsqueda de un equilibrio entre estabilidad y capacidad de respuesta.

- **Procesos**

- ✓ Gestión de Eventos: responsable de monitorizar todos los eventos que acontezcan en la infraestructura TI con el objetivo de asegurar su correcto funcionamiento y ayudar a prever incidencias futuras.
- ✓ Gestión de Incidencias: responsable de registrar todas las incidencias que afecten a la calidad del servicio y restaurarlo a los niveles acordados de calidad en el más breve plazo posible.
- ✓ Petición de Servicios TI: responsable de gestionar las peticiones de usuarios y clientes que habitualmente requieren pequeños cambios en la prestación del servicio.
- ✓ Gestión de Problemas: responsable de analizar y ofrecer soluciones a aquellos incidentes que por su frecuencia o impacto degradan la calidad del servicio
- ✓ Gestión de Acceso a los Servicios TI: responsable de garantizar que sólo las personas con los permisos adecuados pueda acceder a la información de carácter restringido.

- **Mejora Continua del Servicio**

Se utilizan herramientas de medición y feedback para documentar la información referente al funcionamiento del servicio, los resultados obtenidos, problemas ocasionados, soluciones implementadas, entre otros. Para ello se debe verificar el nivel de conocimiento de los usuarios respecto al nuevo servicio, fomentar el registro e investigación referentes al servicio y disponer de la información al resto de los usuarios. Pero este objetivo de mejora sólo se puede alcanzar mediante la continua

monitorización y medición de todas las actividades y procesos involucrados en la prestación de los servicios TI:

- ✓ Conformidad: los procesos se adecúan a los nuevos modelos y protocolos.
- ✓ Calidad: se cumplen los objetivos preestablecidos en plazo y forma.
- ✓ Rendimiento: los procesos son eficientes y rentables para la organización TI.
- ✓ Valor: los servicios ofrecen el valor esperado y se diferencian de los de la competencia.

Los principales objetivos de la fase de Mejora Continua del servicio se resumen en:

- ✓ Recomendar mejoras para todos los procesos y actividades involucrados en la gestión y prestación de los servicios TI.
- ✓ Monitorizar y analizar los parámetros de seguimiento de Niveles de Servicio y contrastarlos con los SLAs en vigor.
- ✓ Proponer mejoras que aumenten el ROI y VOI asociados a los servicios TI.
- ✓ Dar soporte a la fase de estrategia y diseño para la definición de nuevos servicios y procesos/ actividades asociados a los mismos.
- ✓ Los resultados de esta fase del ciclo de vida han de verse reflejados en Planes de Mejora del Servicio que incorporen toda la información necesaria para:
- ✓ Mejorar la calidad de los servicios prestados.
- ✓ Incorporar nuevos servicios que se adapten mejor a los requisitos de los clientes y el mercado.
- ✓ Mejorar y hacer más eficientes los procesos internos de la organización TI.

- **Beneficios de ITIL**

- ✓ Dirige los servicios de TI con los requerimientos actuales de la organización y de sus clientes.
- ✓ Aumenta la rentabilidad y eficacia del suministro de los servicios TI.

- ✓ Sirve de guía para los procesos, la terminología, los roles y procedimientos adecuados que se deben adoptar para una óptima gestión de servicios TI.
- ✓ Aumenta la satisfacción del cliente ofreciendo mayor calidad en el servicio.
- ✓ Alinea la tecnología al negocio por medio de una gestión del servicio TI basada en procesos.
- ✓ Mejores prestaciones de manutención de cambios dentro de TI.
- ✓ Reducción de costos de TI
- ✓ Alineación entre TI y Negocios.

CAPÍTULO 3

PROPUESTA DE SERVICIOS DEL LABORATORIO DE ETHICAL HACKING BASADO EN ITIL V3

3.1- Estrategia del servicio

Teniendo en consideración el ciclo de vida de un servicio que presenta ITIL V3, se empieza con la fase de estrategia del servicio, en la cual se define un conjunto de reglas y normas que aseguran una decisión optima y especifica de los objetivos, perspectivas de desempeño para los servicios que ofrecerá el laboratorio de Ethical Hacking, asegurando así el aprendizaje de nuevas herramientas y técnicas a través

del servicio Educativo que este laboratorio ofrecerá tanto a los estudiantes de la Escuela Politécnica del Ejército como a la Comunidad en general.

3.1.1- Gestión Financiera

Proceso necesario que gestiona recursos económicos para evaluar y controlar los costos asociados a los servicios que garantizarán la efectividad y la calidad del laboratorio de Ethical Hacking.

En este proceso se realiza un análisis financiero donde se presenta cotizaciones de los recursos necesarios, asociados a los servicios.

3.1.2- Análisis Financiero de los Servicios

A continuación se realizará un análisis del costo para la adquisición de equipos, muebles y suministros necesarios para implementar el servicio

3.1.3- Costos de la Inversión

Se establece un presupuesto que contempla el equipamiento, tanto en hardware como software, en los que se incluye la instalación y capacitación; estos valores son estimados a la fecha actual.

- Hardware
- Software

Tabla 3.1.3: Costo Hardware

Requerimientos	Especificación	Cant.	Costo Unit.	Costo Total
Computadores escritorio	Core i7, disco 500GB memoria DDR3, monitor 18.5”	32	1000	25000,00
Computador portátil	Core i7, disco 500 GB, Monitor de 14”	2	1500	3000,00

Video proyectores	3.13 kg (6.97lb) Reproducción de colores 16,7 millones de colores	2	1500	3000,00
Servidor Dread Nought Digital Store	Servidor para aplicaciones password Cracking con Software Elcom, maltego	1	8000	8000,00
Total Aproximado de la inversión				**39000,00**

Tabla 3.1.3: Costo Software

Requerimientos	**Especificación**	**Cantidad**	**Costo Unit**	**Costo Total**
Backtrack Software		1	375	375,00
Software para análisis y recuperación de archivos	WinHex Specialist	1	490	490,00
Total Aproximado de la Inversión				**865,00**

3.1.4- Ganancias

A continuación se describirá las posibles ganancias que se obtendrá de cada se servicio ofrecido por el Laboratorio de Ethical Hacking.

- Educación: el precio va incluido en la matrícula del estudiante.

- Seminario:

  Estudiantes ESPE: $ 80.00

  Profesores: $ 120.00

  Público en General: $135

  Cupo máximo: 40 personas

- Prestación de Servicios:

  Por hora de laboratorio $20

  Por prueba de vulnerabilidades, el precio variaría por la complejidad del caso: los precios estarían en un rango de $300- $2000.

3.1.5- Gestión de la Demanda

Proceso en el que se realiza un análisis de la demanda y factibilidad para crear, mejorar o implementar servicios que soliciten los clientes.

3.1.5.1- Análisis de la Demanda.

Para determinar los servicios que necesitan ser implementados se realizó un estudio de campo mediante encuestas dirigidas a docentes, estudiantes de la Escuela Politécnica del Ejército y comunidad en general.

3.1.5.2- Segmentación de los Clientes del Laboratorio de Ethical Hacking.

Se ha considerado tomar como población a los estudiantes de la Escuela Politécnica del Ejército, Campus-Sangolquí, así como también a la población de Pichincha comprendida entre las edades de 15 a 34 años, ya que serán los principales beneficiarios de la implantación de los Servicios del Laboratorio de Ethical Hacking.

Cálculo de la muestra:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Dónde:

Z = Valor obtenido mediante niveles de confianza.

N = tamaño de la población.

σ =Desviación estándar de la población.

e = Límite aceptable de error muestral.

n = el tamaño de la muestra.

Z= 95% equivale a 1,96

N= 1’735.658

σ =0,5

e= 5%= 0.05

n= ?

$$n = \frac{1735658 * 0{,}5^2 * 1{,}96^2}{(1735658 - 1)0{,}05^2 + 0{,}5^2 * 1{,}96^2}$$

$$n = \frac{1735658 * 0{,}25 * 3{,}8416}{(1735657)0{,}0025 + 0{,}25 * 3{,}8416}$$

$$n = \frac{1666925{,}9432}{4339{,}1425 + 0{,}9604}$$

$$n = \frac{1666925{,}9432}{4340{,}1029}$$

n= 384,07

Con el objetivo de establecer una demanda real, se ha realizado un estudio utilizando técnicas de segmentación del mercado con una muestra de 384 personas entre las que se encuentran estudiantes, docentes de la ESPE y comunidad en general, tomando en cuenta los resultados del análisis de la población global.

Ver Anexo A: Encuesta Servicios

Ver Anexo B: Resultados de Encuesta de Servicios

3.1.6- Gestión de Portafolio de Servicios

El portafolio de servicios muestra una lista completa de los servicios ofrecidos por el laboratorio, para ser gestionados correctamente y determinar su factibilidad funcional dentro de la institución.

3.1.6.1- Visión

Proporcionar servicios informáticos de alta calidad para los estudiantes de la Escuela Politécnica del Ejército y comunidad en general ampliando el desarrollo tecnológico-académico-científico de alumnos y profesores, para servir como apoyo en el cumplimiento de los objetivos de la Seguridad Informática.

3.1.6.2- Misión

Fortalecer y difundir el conocimiento con las herramientas necesarias a los estudiantes para implantar una cultura tecnológica y ética orientada a la seguridad informática para así posicionar a la Carrera de Ingeniería en Sistemas como líder en la investigación y desarrollo del Hacking ético a nivel nacional.

3.1.6.3- Objetivos del Laboratorio de Ethical Hacking

Objetivo General

- Ofrecer técnicas, tácticas y herramientas utilizadas en el hacking ético para que los estudiantes y la comunidad en general puedan identificar las posibles amenazas que puede sufrir un sistema informático y establecer los mecanismos de protección adecuados que garanticen la seguridad del mismo.

Objetivos Específicos

- Apoyar al alumno en el desarrollo de habilidades para la creación, diseño, implantación, mantenimiento de herramientas y mecanismos de Ethical Hacking, impartiéndoles los conceptos y enfoques necesarios y así difundir la investigación en la Escuela Politécnica del Ejército.
- Conformar un grupo de profesores-investigadores interesados en este campo del conocimiento para desarrollar actividades encaminadas a docencia, investigación, creación y desarrollo de proyectos que generen nuevo conocimiento y que el trabajo conjunto sea encaminado a enriquecer cada proyecto con distintas visiones y aprovechar las capacidades y talentos de cada uno de los integrantes del laboratorio.

3.1.6.4- Portafolio de Servicios

A continuación se describirá los diferentes servicios que serán ofrecidos en el Laboratorio de Ethical Hacking, estos serán dirigidos por personal capacitado referente a Ethical Hacking.

3.1.6.4.1- Servicio de Educación de Ethical Hacking

Programas orientados a la profundización o actualización en el Ethical Hacking, cuya oferta académica se actualiza periódicamente de acuerdo con las nuevas exigencias y tendencias de la Seguridad Informática.

- Educación Formal: materia optativa para los estudiantes de Ingeniería en Sistemas e Informática que permitirá a los estudiantes tener conciencia sobre la Seguridad Informática y como vulnerarla.
- Educación Continua: curso intensivo ofrecido por la Escuela Politécnica del Ejército al alumnado y a la comunidad general para la obtención del diploma respectivo.

- Seminarios Temporales: capacitación activa diseñada exclusivamente para una organización solicitante o para la comunidad en general en la que se mezcla la docencia con la investigación sobre el Ethical Hacking.

3.1.6.4.2- Servicio de Investigación y Vinculación de Ethical Hacking

Ofrece el uso del Laboratorio de Ethical Hacking lo que incluye hardware y software para llevar a cabo exploraciones de vulnerabilidades de manera apropiada y legal.

Prestación del Laboratorio de Ethical Hacking a docentes y a estudiantes para la investigación de nuevas técnicas y herramientas con el objetivo de prevenir delitos informáticos.

3.1.6.4.3- Prestación de Servicios del Laboratorio de Ethical Hacking

Servicio orientado al sector público y privado, así como a la comunidad y las entidades relacionadas con la Seguridad Informática.

- Servicio de Consultoría: servicio en el que se ofrece el uso del Laboratorio de Ethical Hacking, el conocimiento y la experiencia de los expertos en el tema para asesorar y ayudar a organizaciones o a personas particulares con problemas de Seguridad Informática mediante la detección de vulnerabilidades.
- Servicio de Prestación de Laboratorio: ofrece el uso de la instalación del Laboratorio de Ethical Hacking con su respectivo Hardware y Software a entidades externas a la institución.

3.2- Diseño del Servicio

La siguiente fase del ciclo de vida de un servicio de ITIL V3 es el diseño del mismo, donde se plantean nuevos servicios y se mejoran los existentes, además de crear documentos y políticas para el diseño adecuado de servicios TI y soluciones que permitan cumplir los objetivos presentes y futuros del mismo.

3.2.1- Gestión de Catálogo de servicios

Al definir el catálogo de servicios se aporta una visión general de lo que oferta este laboratorio puesto que el catálogo de servicios es la clave principal para que una organización ahorre tiempo y dinero al proponer servicios a sus clientes.

3.2.1.1- Servicio de Educación de Ehtical Hacking

Ofrece un estudio de nuevas herramientas y técnicas no solo para estudiantes sino también para docentes y comunidad en general, ayudando a motivar a los mismos el estudio de la seguridad informática.

Destinatarios: Estudiantes de la Escuela Politécnica del Ejército y comunidad en general**,** para que los usuarios puedan acceder al servicio de educación, deben seguir las siguientes indicaciones:

- **Educación formal**

✓ Encontrarse legalmente matriculado en la ESPE modalidad presencial.

✓ Completar cierto número de créditos para poder matricularse que la materia optativa de Ethical Hacking.

✓ Los estudiantes pertenecientes a la Escuela Politécnica del Ejército y que estén matriculados en esta materia harán uso de los laboratorios en el horario correspondiente, 4 horas semanales.

- **Educación Continua**

✓ Encontrarse matriculado en la Unidad de Educación Continua de la ESPE.

✓ Los estudiantes de esta modalidad harán uso de los laboratorios en el horario correspondiente, 40 horas durante dos semanas aproximadamente.

- **Seminarios**

✓ Cumplir con los requisitos del seminario.

✓ Encontrarse inscrito.

- ✓ Presentar una solicitud formal al Departamento de Ciencias de la Computación indicando la duración, los equipos y el motivo por el cual requieren ocupar el laboratorio de Ethical Hacking.
- ✓ Los estudiantes que asistan al seminario deben presentar algún documento válido que identifique la pertenencia al seminario.
- ✓ Se debe dejar una garantía equivalente al precio del alquiler más un 50%, este se debe pagar quince días antes del evento.
- ✓ El ingreso de los estudiantes a la institución será indicando el comprobante de inscripción de la respectiva institución que organiza el seminario.

- **Temario de la cátedra**

✓ **Educación formal**

Ver Anexo C: Syllabus de la Cátedra de Ethical Hacking

✓ **Educación Continua**

Contenido

Introducción al Hacking Ético

1. Identificación de huellas – footprinting
2. Escaneo de redes
3. Enumeración
4. Sistema de hacking
5. Troyanos y backdoors
6. Virus y gusanos
7. Sniffers
8. Ingeniería social
9. Sesión hijacking
10. Hacking de servidores web

11. Hacking de aplicaciones web
12. Inyección SQL
13. Hacking de Redes Inalámbricas
14. Evadir IDS, Firewalls and Honeypots
15. Buffer Overflows
16. Criptografía
17. Test de Penetración

Observación: Cada parte del contenido tiene su laboratorio correspondiente

Seminarios

Contenido

Módulo I

✓ Situación Actual

✓ Tendencias Actuales. Dónde Apuntan los ataques hoy

✓ Riesgos y Componentes asociados.

✓ Nuevos Riesgos

Módulo II: Metodologías de Penetration Testing - Ethical Hacking

✓ Conceptos Generales

✓ Tipos de Test. Detalles y alcances

✓ Etapas metodológicas

✓ Metodologías Internacionales camino al Estándar

Módulo III: Hacking

✓ Tipificación de perfiles

- ✓ La amenaza Interna
- ✓ Anatomía de un ataque

Módulo IV: Ataques: Análisis de los ataques más conocidos y sus medidas de seguridad:

- ✓ BackDoors
- ✓ Rootkits
- ✓ Port Scanning
- ✓ Wipping Trace
- ✓ DOS/DDOS
- ✓ Escalamiento de privilegios
- ✓ Exploit Code
- ✓ Wireless Hacking (802.11 y bluetooth)
- ✓ Ingeniería Social
- ✓ Spoofing
- ✓ Mobile Code.Java Applets, Activex
- ✓ Key logging
- ✓ Man in the middle
- ✓ Phishing y Pharming
- ✓ Password Craking
- ✓ Proxy attack
- ✓ Port redirection
- ✓ Sql Injection
- ✓ Sniffing
- ✓ XSS

✓ Trojan Horses

✓ Virus/Worms

Módulo V: Práctico

✓ Information Gathering

✓ Reconocimiento

✓ Enumeración Superficial y en Profundidad

✓ Captura de Tráfico

✓ Ataque Puro

✓ Borrado de Rastro y consolidación

Laboratorios

Ver Anexos D: Prácticas de Laboratorios

Evaluaciones

Ver Anexos E: Evaluaciones

3.2.1.2- Servicio de Investigación de Ethical Hacking

Ofrece el uso del laboratorio de Ethical Hacking lo que incluye hardware y software para llevar a cabo una exploración de vulnerabilidades de manera apropiada y legal.

Destinatarios

Comunidad en General

Para que los usuarios puedan acceder al servicio de investigación, deben seguir las siguientes indicaciones:

- Firma de contrato de prestación de servicios.
- Pago del 50% en el momento de la firma del contrato y el otro 50% al momento de entregar el informe detallado de los resultados.

- El contratante utilizara el laboratorio en los horarios estipulados en el contrato.

3.2.1.3- Prestación de Servicio de Ethical Hacking

Servicio orientado al sector público y privado, así como a la comunidad y las entidades relacionadas con la Seguridad Informática.

- Servicio de Consultoría: servicio en el que se ofrece el uso de las instalaciones del laboratorio de Ethical Hacking y la asesoría de personal especializado.
- Servicio de Prestación de Laboratorio: ofrece el uso de la instalación del Laboratorio de Ethical Hacking con su respectivo Hardware y Software a entidades externas a la institución.

Destinatarios

Sector Público y privado

Para que los usuarios puedan acceder a la prestación de Servicio de Ethical Hacking, deben seguir las siguientes indicaciones:

- ✓ Firma de contrato de prestación de servicios.
- ✓ Pago del 50% en el momento de la firma del contrato y el otro 50% al momento de entregar el informe detallado de los resultados.
- ✓ El contratante utilizara el laboratorio en los horarios estipulados en el contrato.

3.2.2- Gestión de Niveles de Servicio

En este proceso se definirá el nivel de servicio de los Laboratorios Generales, en el que se asegurará la calidad de los servicios TI, mediante Acuerdos de Nivel de Servicio (SLA), Acuerdos de Nivel Operacional (OLA).

Entradas

- Retroalimentación de los clientes
- Información de otros procesos
- Reuniones de Seguimiento

- Cambios en los requisitos de servicios

Actividades

- Determinar, negociar y acordar requisitos para nuevos servicios
- Supervisar y medir el funcionamiento de los servicios
- Promover planes de mejora de servicios
- Recopilar, medir y mejorar la satisfacción del cliente.
- Registrar y gestionar las quejas y reclamos.
- Proporcionar la información adecuada para ayudar a la gestión
- Revisar OLAs y SLAs

Salidas

- Informes de Servicio
- Plan de Calidad de Servicios
- Acciones de mejora priorizada
- SLAs
- OLAs

Ver Anexo F: Diseño de Formato SLA, OLA para el Laboratorio de Ethical Hacking

3.2.3- Gestión de la capacidad

Tabla 3.2.3: Capacidad de Laboratorio

	NOMBRE DEL SERVICIO	Nº DE AULA/ OFICINA	ÁREA M2 POR AULA	ÁREA TOTAL
Recursos Físicos:	Servicio de Educación en Ethical Hacking	1	17.34	17.34
	Servicio de Investigación y vinculación en Ethical Hacking			
	Prestación de Servicio de			

	Ethical Hacking			

Observación: Todos los servicios se prestan en el Laboratorio de Ethical Hacking.

Tabla 3.2.3: Recursos Tecnológicos

	Nombre del servicio	**Nombre**	**Nº**	**Características Técnicas**
Recursos tecnológicos:	Servicio de Educación	Computadoras de Escritorio	32	Core i7, disco 500GB memoria DDR3, monitor 18.5’
	Servicio de Investigación	Portátiles	2	Core i7, disco 500 GB, Monitor de 14’
	Prestación de Servicio de Ethical Hacking	Video Proyectores	2	Características Físicas Ancho: 34.5 cm Profundidad: 26.3 cm Altura: 9.3 cm Peso: 3.13 kg (6.97lb) Reproducción de colores 16,7 millones de colores Distancia de proyección 30" a 300" a una distancia de 0.9m - 10.8m Resolución nativa XGA 1024x768 Pixeles
		Servidor	1	Procesadores: Intel Core i7 3930K 3.2GHz (Unlocked CPU for Extreme Overclocking) Mainboard: ASUS Sabertooth X79 (Intel X79 Chipset) (Features USB 3.0 and SATA 6Gb/s) RAM: 16 GB
		Software	1	Software con el que se puede realizar: Test intrusión Ingeniería Social

				Entre otras técnicas de Ethical Hacking

Tabla 3.2.3: Recursos Humanos

Recursos Humanos	SERVICIO	Nº RRHH	GRADO
	Servicio de Educación	1	Docente
	Servicio de Investigación	1	Laboratorista
	Prestación de Servicio de Ethical Hacking	1	Docente

3.2.4- Organigrama

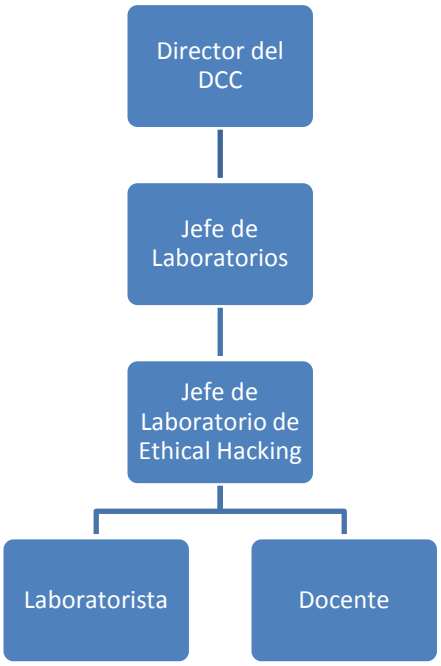

Figura 3.2.4: Organigrama

3.2.4.1- Perfil de los Recursos Humanos del Laboratorio de Ethical Hacking

Es de gran importancia definir el perfil adecuado para el personal que formará parte del Laboratorio de Ethical Hacking para garantizar el éxito en el desempeño de

sus funciones, se tomará en cuenta ciertos parámetros como: el nivel de estudios, experiencia y competencias personales.

3.2.4.2- Funciones del Jefe de laboratorio

- Implementar normas de seguridad para el correcto funcionamiento y utilización de los equipos.
- Planificar y supervisar las actividades del personal a su cargo.
- Realizar un análisis técnico y económico para la prestación de servicios que se encomiende al laboratorio.
- Entregar semestralmente el detalle de las necesidades del laboratorio, para el normal desenvolvimiento de sus actividades, previo el inicio de cada período de clases y/o cursos que se realice.
- Aprobar o negar el préstamo del laboratorio a entidades externas para la realización de cursos y/o seminarios
- La entrega y recepción del laboratorio se efectuará de acuerdo con el inventario que debe ser debidamente legalizado con su firma.
- Realizar el plan de actividades de los laboratorios, tomando en cuenta el horario de usos de los laboratorios, el horario de limpieza de las instalaciones y el cronograma de mantenimiento de los equipos.

3.2.4.3- Funciones del Laboratorista

- Poner en ejecución las normas y medidas previstas para la seguridad y buen funcionamiento de los equipos.
- Informar al jefe del laboratorio cuando haya necesidad de mantenimiento correctivo.
- Efectuar el mantenimiento rutinario del equipo de laboratorio.

- Ser responsable directo de la seguridad del laboratorio y reportar cualquier novedad en forma inmediata al jefe de laboratorio.
- Llevar el inventario de cada uno de los equipos.
- Colaborar con el control de la disciplina de los alumnos que se encuentran en las dependencias del laboratorio.
- Está a cargo del mantenimiento y conservación del equipo y los materiales del laboratorio.
- Responder ante el jefe de laboratorio por daños y pérdidas de repuestos, accesorios, elementos y demás enseres a él encomendados.

3.2.4.4- Perfil para Docente de Ethical Hacking

Conocimientos:

- Manejo de Sistema Operativos :Windows, Linux, Unix
- Criptografía
- Protocolos de Seguridad: IPSec
- Manejo de herramientas de seguridad: scanners, firewalls, IDS
- Lenguajes de programación
- Análisis de vulnerabilidades
- Conocimientos de estándares: ITIL, ISO27000
- Computo forense
- Manejo de herramientas de ethical hacking

Deberes y responsabilidades

- Cumplir con el temario de la cátedra
- Llegar puntual a las clases
- Cumplir con las normas de la Escuela Politécnica del Ejército.

- Responder a las dudas de los alumnos
- Incentivar la investigación y autoeducación en los alumnos.
- Inculcar valores de ética y responsabilidad.
- Permitir que los estudiantes se focalicen en el aprendizaje y la resolución de problemas.
- Difundir el conocimiento del Ethical Hacking a través del uso de herramientas y aplicación de técnicas.
- Conocer y aplicar los estándares y/o protocolo de seguridad.

3.2.5- Gestión de Disponibilidad.

En este proceso se define los horarios de disponibilidad y el responsable del servicio para que funcione ininterrumpidamente y de manera fiable.

Tabla 3. 1 Disponibilidad de Laboratorio

SERVICIO	DISPONIBILIDAD	RESPONSABLE
Educación Presencial	Lunes – Viernes 6 hrs	Laboratorista, docente
Educación Continua	Lunes – Viernes 4 hrs	Laboratorista, docente
Seminarios Temporales	Lunes – Viernes 6 hrs Sábados y Domingos 5 hrs	Jefe de Laboratorio y Laboratorista
Servicio de Investigación	Lunes – Viernes 6 hrs Sábados y Domingos 5 hrs	Jefe de Laboratorio

3.2.6- Gestión de la Continuidad del Servicio

Este proceso tiene como objetivo garantizar la recuperación del servicio después de un incidente crítico, para lo que es necesario definir y establecer estrategias, políticas y procedimientos que eviten en lo posible la interrupción del servicio.

Durante las operaciones normales de negocio existe la probabilidad de pérdidas potenciales o interrupciones no programadas asociadas con un desastre o contingencia mayor, por lo que es importante el desarrollo de un plan viable y factible de recuperación que asegure la continuidad de las operaciones del laboratorio de Ethical Hacking de la Escuela Politécnica del Ejército.

El planeamiento adecuado, la preparación, y la comunicación son los ingredientes necesarios para un exitoso plan de recuperación en caso de contingencia o desastre. En el caso de una situación de contingencia o desastre, es importante disponer de una estrategia de recuperación que pueda proveer el reinicio del negocio en un tiempo razonable y predeterminado.

3.2.6.1- Definición de contingencia

Una contingencia se define como cualquier evento no planeado que hace que las actividades de negocio no sean operadas normalmente durante un determinado periodo de tiempo, para la cual existe una solución que permite la recuperación en un tiempo razonable. Las contingencias comunes se deben normalmente a los eventos como:

- Falla de la red.
- Falta de suministro de corriente eléctrica.
- Fallas humanas en la operación de la red o equipos de cómputo.

Esto implica que deben existir equipos de repuesto, redes de datos alternas o suministro in-interrumpido de fluido eléctrico para minimizar el impacto de una

contingencia. El plan de recuperación en caso de contingencia o desastre considera el disponer de mecanismos para reanudar las actividades de negocio mientras exista dicha contingencia.

3.2.6.2- Definición de desastre

Un desastre se define como cualquier evento no planeado que hace un lugar inoperable o inaccesible. Diversos tipos de desastre pueden ocurrir y varían de:

1. Comunes:

a. Fallos masivos.

b. Daños accidentales.

2. Extraordinarios:

a. Robo.

b. Destrucción del laboratorio.

c. Incendio.

d. Atentado Terrorista

3. Naturales:

a. Terremoto.

b. Inundación.

c. Erupción volcánica.

3.2.6.3- Objetivos

Los objetivos del plan de recuperación en caso de desastre incluyen, pero no están restringidos a:

- Minimizar los efectos de una contingencia o desastre en las funciones críticas al proveer de un conjunto de procedimientos y tareas a ser usados en el evento.
- Responder a una situación de contingencia o desastre rápida y efectivamente.

- Reunir al personal necesario para reactivar el proceso con las interrupciones menores respecto al servicio al cliente.

3.2.6.4- Suposiciones

El Departamento de Ciencias de la Computación de la Escuela Politécnica del Ejército es responsable de:

- Soportar el acceso local a la red global de datos.
- Mantener un Plan de Contingencias y Recuperación en caso de Desastre local actualizado.
- Entrenar al personal clave para llevar a cabo las funciones definidas dentro del plan.

3.2.6.5- Procedimiento para atención de fallas en infraestructura

Notificación del incidente

El jefe de laboratorio notificará al personal si una situación de desastre ocurre en el departamento, el mismo que determinará si un desastre necesita ser declarado y las actividades de reanudación necesitan ser activadas.

Tabla 3. 2 Procedimiento de atención a fallas

Categoría	**Estrategia de recuperación de hardware**	**Localidad de recuperación**
Servidor	Se enviará el servidor o las partes que se requieran al proveedor del mismo para que lo repare. El laboratorista se encargará de reinstalar el sistema operativo y el software específico.	

Comunicaciones de datos	Se poseerá en inventario por lo menos: 1 modem, 10 metros de cable de datos. Cuando se dañe alguno de estos equipos serán reemplazados por los que se tengan en bodega.	El laboratorista es quien hará la instalación del nuevo equipo.
PCs	Se enviará a los computadores al servicio técnico pertinente. El laboratorista se encargará de reinstalar el sistema operativo y el software específico.	
No hay acceso al servidor	Revisar entorno de red. Si no hay acceso intranet o el problema es la conexión con el servidor, reportar al jefe de laboratorios.	
No hay acceso a la red de datos.	1. Determinar si el usuario está conectado a la red. 2. Corregir problemas de nivel físico, conectores, LAN Jack, Switch. 3. Si se determina que el problema es una avería que va a ser resuelta por más de 2 horas, habilitar puntos de red de emergencia.	Puntos de red de emergencia
No energía eléctrica	Conectarse al generador de la universidad. Duración: máximo 2 horas	

3.2.7- Gestión de la seguridad de la Información

La gestión de la seguridad de la información se encuentra activa y se involucra durante todo el ciclo de vida del servicio, es por esto que es la encargada de que todos los servicios se encuentren disponibles, manteniendo la información completa, actualizada e integra.

Todo el procedimiento de test de intrusión y la información obtenida será manejada mediante la metodología OSSTMM el cual no solo alcanza los ámbitos técnicos y de operación de seguridad tradicionales, sino que se encarga de fijar estándares respecto de aspectos tales como: las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado desde el inicio mismo de su ofrecimiento de cara al cliente, la forma en la que los resultados del mismo deben ser presentados, las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar el test y los tiempos que deberían ser tenidos en cuenta para cada una de las tareas. Todos y cada uno de estos puntos, se encuentran claramente definidos a lo largo de la metodología por lo que garantiza cuidar las tres características de la información (confidencialidad, disponibilidad e integridad).

3.2.8- Gestión de los Proveedores

El Laboratorio de Ethical Hacking forma parte de una institución pública por ende el comité de adquisiciones de la ESPE es el encargado de realizar las adecuaciones necesarias tanto en infraestructura como en inmuebles y tecnología.

Este comité está constituido por los siguientes miembros:

- Rector de la ESPE o su delegado
- Oficial Superior en servicio activo
- Asesor Jurídico
- Director Financiero
- Técnico de la institución, especialista en el tema de la contratación

CAPÍTULO 4

METODOLOGÍA

4.1- Método Delphi

El método Delphi es una técnica de investigación social que tiene como objetivo la obtención de una opinión grupal fidedigna a partir de un grupo de expertos, en este caso sirve como herramienta para obtener información y determinar la conveniencia de la implantación de ITIL en el Laboratorio de Ethical Hacking.

4.2- Desarrollo del trabajo

El desarrollo del proceso se inicia con la selección de evaluadores quienes serán los encargados de realizar las revisiones y de ser necesarios efectuar las correcciones pertinentes a la Propuesta de Servicios del Laboratorio de Ethical Hacking.

4.3- Selección de Evaluadores (expertos)

Para garantizar que la selección de los expertos sea la más eficiente y eficaz se generaron criterios de formación académica y experiencia laboral, quienes son expertos universitarios de reconocido prestigio y profesionales que laboran en el área de las Seguridades Informáticas, Ethical Hacking e ITIL.

Inicialmente se convocó a 4 expertos, a los cuales se les solicito su perfil profesional a fin de analizarlos y determinar quienes cumplen con el perfil para la evaluación requerida:

- **Ing. Víctor Paliz**
- **Ing. Jairo Navarro**
- **Ing. Ramiro Pulgar**

- **Ing. Edgar Álvarez**

4.3.1- Perfil de Selección

- Título de Tercer Nivel en Ciencias de la Computación.
- Título de Cuarto Nivel en Seguridades Informáticas.
- Certificado en ITIL V3.
- Experiencia Laboral – mínimo dos años.
- Calidad de su actividad docente e investigadora (opcional).

Mediante las Hojas de Vida de cada uno de los expertos se pudo hacer la selección.

Ver Anexo G: Hojas de Vida

Del análisis de los perfiles profesionales propuestos, designó a tres profesionales:

- ✓ **Ing. Víctor Paliz**
- ✓ **Ing. Jairo Navarro**
- ✓ **Ing. Edgar Alvares**

- El 75% de los profesionales analizados tienen estudios universitarios de tercer nivel.

- Un 100% de ellos dispone además de estudios complementarios, tales como maestrías.

- Todos los candidatos proceden de especialidades afines y que tienen relación directa con el ámbito de las nuevas tecnologías y de las profesiones técnicas.

- La selección de estos dos candidatos se realizó por la experiencia en ITIL y en Ethical Hacking como en herramientas de Seguridad Informática.

4.4- Revisión de la Propuesta de Servicios del Laboratorio de Ethical Hacking

Los resultados obtenidos permiten reflejar las observaciones grupales cuantitativos remitidos por los expertos, los mismos que determinan cierta asertividad y ciertas correcciones a ser realizadas en las Prácticas de Cátedra propuestos en los puntos que se detallan a continuación:

4.4.1- Estrategia del Servicio

Tabla 4.4.1: Resultados obtenidos en correcciones-Estrategia del Servicio

Actividades	Completo	Falta por Definir	Conciso	Observaciones
Gestión Financiera	98%	-	100%	-
Gestión de la Demanda	98%	-	100%	-
Gestión del Portafolio del Servicio	90%	Especificar más claramente los servicios	90%	

4.4.2- Diseño del Servicio

Tabla 4.4.2: Resultados obtenidos en correcciones Diseño del servicio

Actividades	Completo	Falta por Definir	Conciso	Observaciones
Gestión de Catálogo del Servicio	80%	15%	90%	
Gestión de Nivel de Servicio	70%	20%	90%	Se debería proponer unos SLA mínimos, los mismos que deben constar en el catálogo de servicios.
Gestión de la Capacidad	50%	50%	75%	La gestión de la capacidad su objetivo es que la infraestructura de TIC´S sea capaz de asegurar el procesamiento presente y futuro, para lo cual se requiere análisis de uso de los recursos tecnológicos y tendencias de incremento en el tiempo.

Gestión de la Disponibilidad	90%	5%	98%	
Gestión de la Continuidad de Servicios de TI	95%	2%	97%	
Gestión de Seguridad	75%	10%	80%	
Gestión de los Proveedores	90%	5%	97%	

4.5- Evaluación de la Propuesta de Servicios del Laboratorio de Ethical Hacking.

Se describirá en forma gráfica los porcentajes que los expertos expusieron en la Propuesta de servicios del Laboratorio de Ethical Hacking.

4.5.1- Estrategia del Servicio

En la propuesta de Servicios del Laboratorios Estrategia del Servicio se puede destacar que la Gestión Financiera es una de las que posee un alto porcentaje en el criterio Completo, esta actividad es una de las importantes del ciclo de vida de ITIL V3 puesto que se relaciona los servicios con el mercado actual.

En el segundo criterio la única actividad que presenta observaciones es la Gestión del Portafolio del Servicio, ya que se debe especificar y ordenar por prioridad a cada uno de los servicios que prestará el Laboratorio de Ethical hacking.

El tercer criterio existe que se refiere a Conciso, la actividad que menos porcentaje posee es la Gestión del Portafolio del Servicio puesto que al inicio no se tenía conocimiento de todos los servicios que el laboratorio iba a ofrecer. Tal como se indica en la Figura 4.5.1

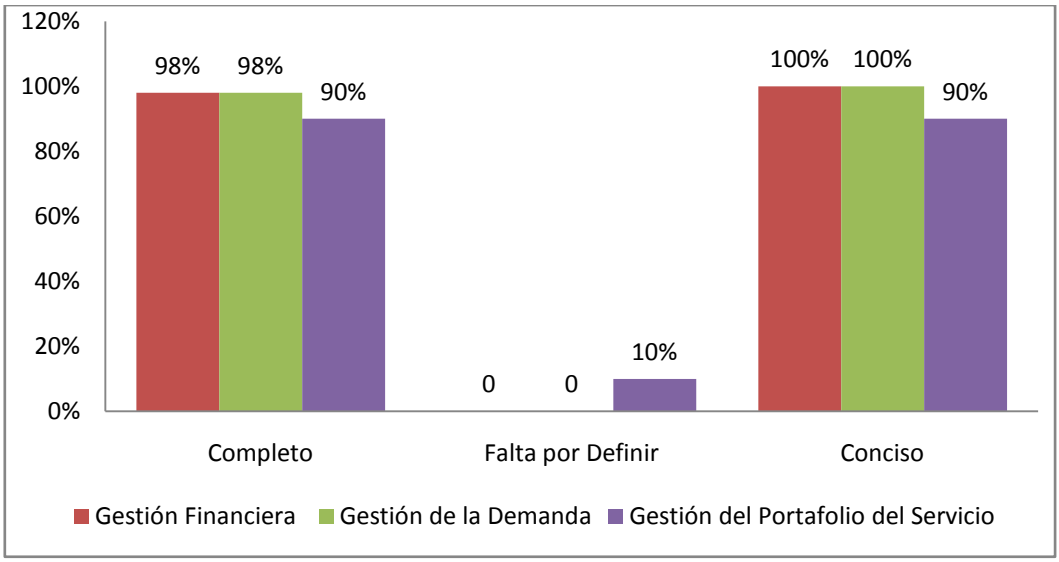

Figura 4.5.1: Diagrama de evaluación la Propuesta de Servicio del Laboratorio-Estrategia del Servicio

4.5.2- Diseño del Servicio

El porcentaje más alto del criterio Completo, es el de la Gestión de la Continuidad de Servicios de TI puesto que este criterio habla de todos los posibles incidentes y lo que se podría hacer en caso de que estos se puedan presentar en el Laboratorio de Ethical Hacking.

El peso más elevado del criterio Falta por Definir, es la Gestión de Capacidad puesto que en la Propuesta de Servicios del Laboratorio de Ethical Hacking no presenta una definición clara de lo que está ofreciendo y de lo que va ofrecer en un futuro.

La mayoría de actividades poseen un porcentaje razonable en el criterio Conciso, puesto que la mayoría de ellos posee un concepto claro y entendible. Tal como se indica en la Figura 4.5.2

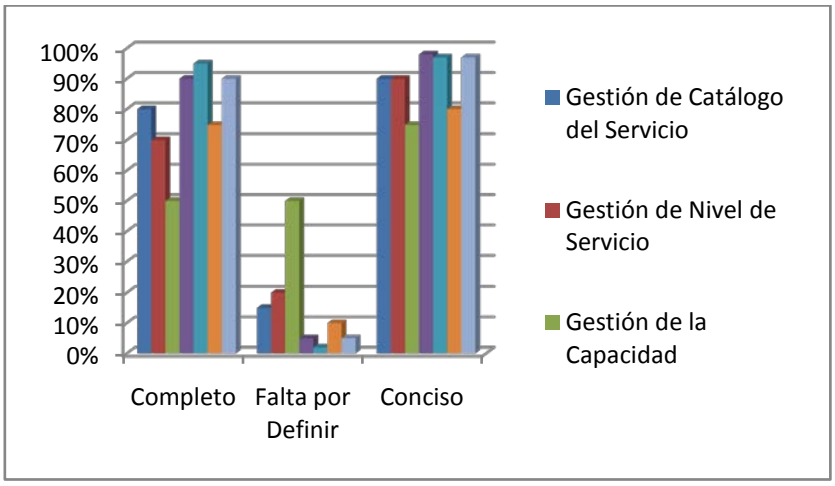

Figura 4.5.2: Diagrama de evaluación la Propuesta de Servicio del Laboratorio de Ethical Hacking- Diseño del Servicio

Cabe mencionar que las prácticas que se encuentran adjuntas a este proyecto tienen tanto puntos débiles como puntos fuertes, los mismos que tienen una breve descripción del por qué sus porcentajes, los mismos que se presentan en la Figura 4.5.2

a) Puntos fuertes con un 70%

- Las prácticas poseen los conocimientos básicos que una persona debe conocer para proceder con las mismas.
- Permite medir el nivel de conocimiento adquirido a través de las prácticas que se realizan y sus respectivas evaluaciones.
- Ayuda a la investigación de nuevas prácticas o de nuevos temas referentes a Ethical Hacking.

- Estimula al estudiante y al docente a la investigación de temas referentes a la Seguridad Informática y a sus derivados.

b) Puntos débiles con un 30%

- Carencia de imágenes en las prácticas
- A pesar de que la práctica guie al estudiante, este no legue al objetivo de la misma.
- Falta de conocimiento del uso de normas que se pueda usar en el tema de Ethical Hacking. Puesto que en el mercado últimamente todo se basa en normas y reglas.

Figura 4.5.2: Diagrama de Puntos Fuertes y Puntos Débiles

4.6- Rediseño e Instalación.

Después de un análisis de las observaciones y correcciones que los expertos han emitido en la Propuesta de Servicios del Laboratorio de Ethical Hacking, se logró que las dos etapas del ciclo de vida de ITIL V3 logren plantear los servicios del laboratorio en función del negocio no solo de la Universidad sino del país. Las

prácticas y evaluaciones, que forman parte de la propuesta anteriormente mencionada, son una estimulación para el estudiante y el docente para continuar un estudio más profundo y así lograr objetivos que nunca pensaron en lograr.

4.7- Plan de Transición del Servicio

El plan de transición del servicio representa el proceso que se debe seguir para poner a los servicios, que brindará el Laboratorio de Ethical Hacking no solo a los estudiantes sino a los docentes y comunidad en general, en acción, lo que significa describir las tareas que se realizarán, el costo de estas y el tiempo que tomará llevarlas a cabo.

4.7.1- Tareas

Describen cada uno de los pasos que se van a realizar para poner al laboratorio y a los servicios que ofrece en funcionamiento.

4.7.1.1- Instalación

En este paso se realiza la instalación del software así como también de los equipos que compondrán el laboratorio.

En la instalación física es necesario realizar un cableado estructural con 40 puntos de red funcionales, que dispongan de internet. El equipamiento como computadoras y servidores son transportados e instalados por personal de departamento de ciencias de la computación.

El software utilizado en los laboratorios es instalado por el laboratorista encargado.

Los pasos para instalar el software que se va a utilizar en el laboratorio, BackTrack 5 y Winhex, se describe a continuación:

4.7.1.1.1- Instalación BackTrack 5

a) Descargar backtrack 5 desde: http://www.backtrack-linux.org/downloads/

b) Escoger la versión de backtrack a instalar

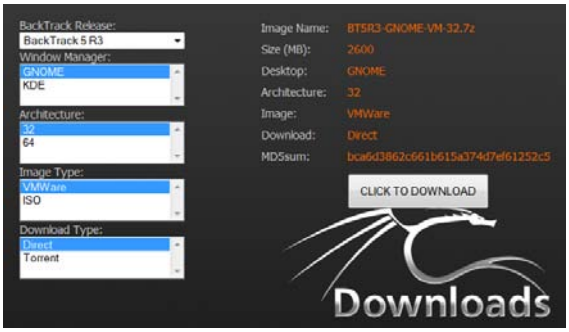

Figura 4.7.1.1.1: Versión BackTrack

c) Grabar la distribución de backtrack sobre un cd o flash USB e iniciar la computadora, cuando se inicie la instalación aparecerá la siguiente pantalla, mientras se carga.

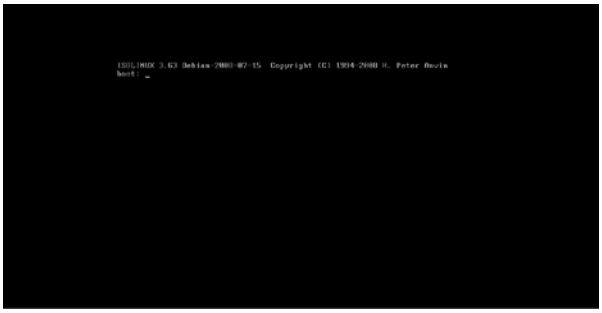

Figura 4.7.1.1.1: Grabación BackTrack en un CD o Flash

d) En las opciones de instalación escoger la opción default boot text mode

Figura 4.7.1.1.1: Opciones de Instalación

e) Después de unos pocos minutos aparece una consola

Figura 4.7.1.1.1: Consola de BackTrack

f) Para manejar la interfaz gráfica escribir startx

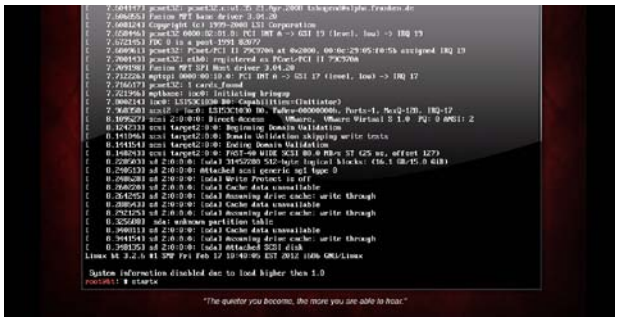

Figura 4.7.1.1.1: Interfaz Gráfica

g) Aparecerá el escritorio de backtrack, para instalar este SO en el disco duro dar doble clic sobre install BackTrack

Figura 4.7.1.1.1: Instalación Backtrack

h) Escoger el idioma: Español y dar clic en adelante

Figura 4.7.1.1.1: Idioma de instalación

i) Escoger la región: Ecuador y la zona horaria: Ecuador (Guayaquil) y dar clic en adelante

Figura 4.7.1.1.1: Opción de región

j) En la distribución del teclado escoger: Latino América – Latinoamerica Include dead tilde

Figura 4.7.1.1.1: Opciones de Teclado

k) Seleccionar en que parte y cuando espacio de disco duro utilizará backtrack

Figura 4.7.1.1.1: Selección de disco duro

l) Una vez escogidas todas las opciones anteriores dar clic en el botón Instalar

Figura 4.7.1.1.1: Instalación-1

m) La instalación durará algunos minutos

Figura 4.7.1.1.1: Instalación-2

n) Para terminar la instalación habrá que reiniciar el equipo

Figura 4.7.1.1.1: Reinicio del equipo

o) Una vez reiniciado el equipo nos pedirá un usuario y la contraseña, las que son root y toor respectivamente.

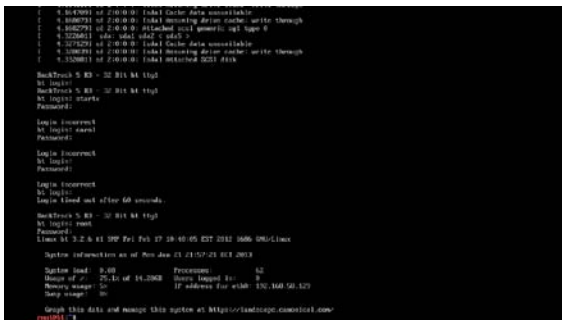

Figura 4.7.1.1.1: Ingreso de usuario y contraseña

p) Después de esto escribir startx para cambiarse al modo gráfico.

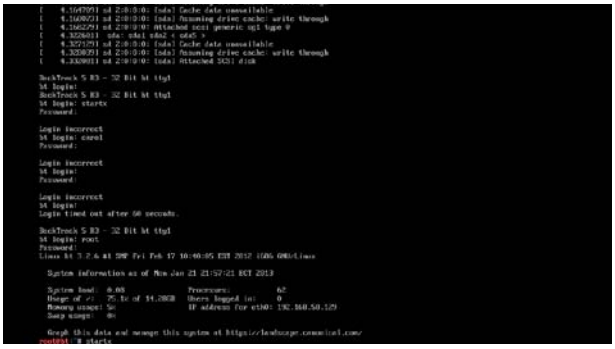

Figura 4.7.1.1.1: Cambio al modo gráfico

4.7.1.1.2- Instalación del Winhex

q) Descargar winhex

Figura 4.7.1.1.2: Ícono de instalación

r) Hacer doble clic en el ejecutable

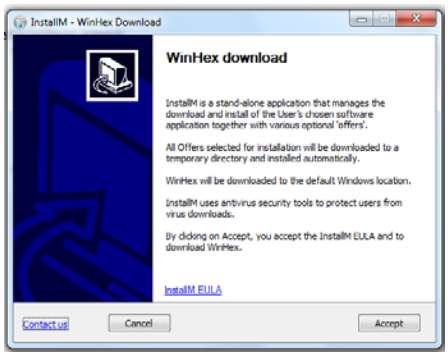

Figura 4.7.1.1.2: Descarga de Winhex

s) Colocar Aceptar

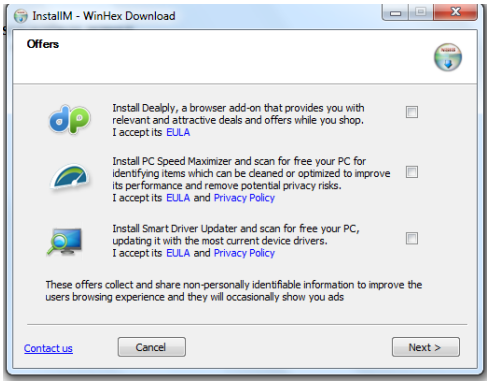

Figura 4.7.1.1.2: Opciones de Instalación

t) Colocar la instalación que viene por defecto en la aplicación

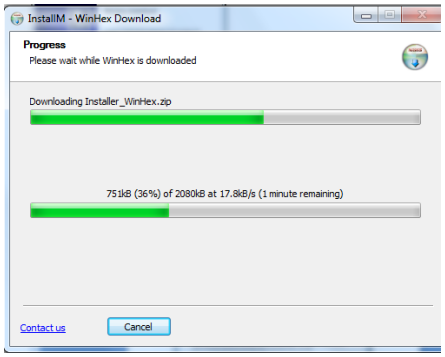

Figura 4.7.1.1.2: Procedimiento de Instalación

u) Al terminar la instalación se abrirá una ventana donde se encontrara el ejecutable Winhex. Hacer doble clic y continuar con su instalación

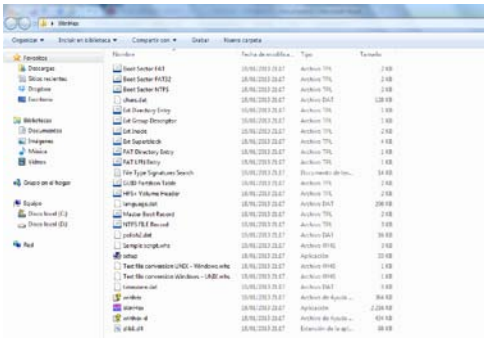

Figura 4.7.1.1.2: Ejecutable de Winhex

v) Al dar clic aparece la siguiente ventana donde se elige el idioma del programa.

Figura 4.7.1.1.2: Elección de Idioma de Winhex

w) Después de elegir el idioma, se continúa con algunas propiedades como poner acceso directo al programa, o crear una carpeta donde se guarde los documentos recuperados o documentos que se han modificado por la aplicación.

Figura 4.7.1.1.2: Elección de componentes

Figura 4.7.1.1.2: Elección de Íconos directos

x) Después de cambiar la configuración básica del aplicativo, este, está listo para ser ejecutado y probado.

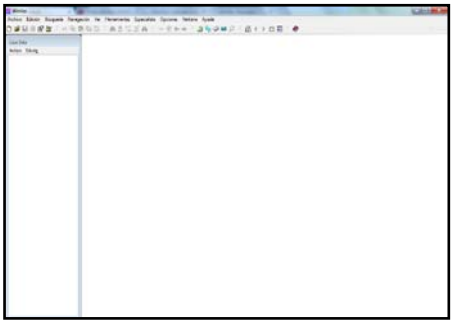

Figura 4.7.1.1.2: Interfaz

4.7.1.2- Poner a Disposición

Esta fase describe todos los servicios que el Laboratorio de Ehical hacking ofrecerá no solo a los estudiantes de la Escuela Politécnica del Ejercito sino también a la comunidad en general.

La actividad publicitaria se pondrá a vista de todo el público, empezando con la población politécnica utilizando los recursos del área de Marketing de la Escuela Politécnica del Ejército como son: la radio escape y las pantallas informativas que se encuentran en la universidad, así como también se colocará en las redes sociales la información principal de los diversos cursos y seminarios que se vayan a desarrollar.

Se generarán trípticos y carteles publicitarios, con el propósito de llamar la mayor cantidad de gente para que se capacite en Ethical Hacking y las herramientas que utiliza.

4.7.1.3- Selección de Personal

En esta actividad se debe convocar a un concurso de méritos interno, en el que se analice las hojas de vida de los docentes y cumplan con el perfil definido por el departamento y ciertas responsabilidades.

Al realizar el análisis de las Hojas de Vida, las personas que cumplan con todo lo requerido anteriormente mencionado, serán las personas que realizaran la capacitación.

4.7.1.4- Capacitación

En esta fase participarán todos los docentes que han cumplido con el perfil anteriormente mencionado, se les capacitará sobre fundamento teórico de la materia en general, los valores que deben inculcar en los estudiantes, las herramientas tanto de software y hardware que se deberán manejar para llevar a cabo las prácticas, así como también las consultorías que podrían asesorar.

4.7.1.5- Evaluar

Las personas que hayan asistido a la capacitación deberán presentar una evaluación escrita, sobre los temas impartidos sobre la misma. Después de obtener los resultados de la evaluación, se escogerá al personal correcto el cual se reunirá

para desarrollar el respectivo syllabus de materia optativa y el temario de los cursos o seminarios.

4.7.1.6- Puesta del servicio

Se integra la materia en la malla curricular de la carrera de Ingeniería en Sistemas e Informática para el próximo semestre académico, así como también se comienza a planificar las fechas y temarios para la realización de cursos y seminarios.

Se difunde la publicidad diseñada para los diferentes servicios que ofrece el laboratorio.

4.7.2- Cronograma

El proyecto se pretende realizar en un periodo de 4 meses, incluyendo la compra de tanto del software como el hardware y su propia instalación, se anexa el cronograma con las actividades previstas y el tiempo que estas tomarán.

Ver Anexo H: Cronograma

4.7.3- Costos

En el proyecto se establece un presupuesto que contempla el equipamiento, tanto en hardware como software descrito en la Tabla 3.1 y Tabla 3.2 respectivamente, en los que se incluye la instalación y capacitación; estos valores son estimados a la fecha actual.

CAPÍTULO 5

5.1- Conclusiones

- El hacking ético representa una solución para la seguridad informática a través de pruebas las cuales tienen como objetivo encontrar todas las vulnerabilidades posibles que tiene un sistema o aplicación web para así poder prevenir cualquier delito informático.
- Los hackers éticos son personas que prestan servicios para realizar test de intrusión en un sistema; estas personas ayudan a que los clientes entiendan mejor las vulnerabilidades que tienen y que criterios de seguridad en su información deben aplicar para prevenirlos.
- El Laboratorio de Ethical Hacking permitirá al estudiante trabajar en un equipo orientado a la seguridad de la información, donde podrá experimentar pruebas en los sistemas y hacer que estos se encuentren en los momentos más críticos para así evitar que sus propios sistemas posean estas falencias y sean más seguros.
- Los expertos en ITIL V3 concluyeron que Ethical Hacking es una materia que no debe ser opcional sino esencial puesto que hoy en día la seguridad informática es tomada muy en cuenta en las empresas, y es necesario que la gente estudie sobre estas nuevas tendencias. Por esta razón, el servicio que ofrecerá el Laboratorio de Ethical Hacking es súper importante puesto que no solo vela por los intereses de los estudiantes y docentes de la Universidad sino del país.

5.2- Recomendaciones

- Es necesario concientizar a los administradores de sistemas acerca del uso o mal uso que se puede dar a las herramientas utilizadas en este proyecto de titulación, dado que la ética es algo muy importante para no caer en lado de los hackers criminales y realizar actividades al margen de la ley.
- Cada vez existen muchos ataques informáticos por lo que se debería desarrollar mecanismos para mantener actualizadas las herramientas de seguridad que se encontrarán en el laboratorio para así conservar tanto a los docentes como a los estudiantes al día.
- Ethical Haking es una rama de la Seguridad Informática y es así por lo que se debe integrar en la malla curricular de la Carrera de Ingeniería de Sistemas como una materia obligatoria.
- Es necesario concienciar a las autoridades que Ethical Hacking puede dar apertura a varias técnicas y herramientas, las mismas que pueden tener un buen uso así como un malo, por esto hay que inculcar los valores que un Ethical Hacking debe poseer.
- Incentivar y crear mecanismos para que el profesorado comience a fomentar la investigación y desarrollo de habilidades en otros ámbitos de la Seguridad Informática.
- Dotar con herramientas actualizadas al laboratorio para que los estudiantes se sientan incentivados y pueden tener mejores resultados.
- Los docentes que vayan a impartir la cátedra de Ethical Hacking deben ser personas que no solo hayan tenido experiencia en consultoría, auditoria sino también cursos sobre el tema, practicas con ciertas herramientas y que tengan conocimientos realistas y cercanos con lo que hoy en día sucede.

BIBLIOGRAFÍA

Delincuencia del Consejo de Europa. (s.f.). Obtenido de Agpd: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Delitos Informáticos. (s.f.). Obtenido de Cabinas: http://www.cabinas.net/informatica/delitos_informaticos.asp

Delitos Informáticos. (s.f.). Obtenido de Seguridad: http://www.seguridad.unam.mx/descarga.dsc?arch=2776

Delitos Informáticos. (s.f.). Obtenido de Nebrija: http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf

Ethical Hacking. (s.f.). Obtenido de Slideshare: http://www.slideshare.net/YulderBermeo/introduccion-hacking-etico

Ethical Hacking. (s.f.). Obtenido de Scribd: http://es.scribd.com/doc/58565986/Ethical-Hacking

Ethical Hacking. (s.f.). Obtenido de Cert.uy: http://www.cert.uy/archivos/ISEC_PRESENTACION_AGESIC_2009_MARTIN_VILA_JULIO_BALDERRAMA.pdf

Ethical Hacking. (s.f.). Obtenido de Comunidad: http://comunidad.dragonjar.org/f152/ethical-hacking-4660/

Ethical Hacking. (s.f.). Obtenido de Plusformación: http://www.plusformacion.com/Recursos/r/Ethical-hacking-Test-intrusion-Principales-metodologias

Ethical Hacking. (s.f.). Obtenido de Slideshare: http://www.slideshare.net/mfrayssinet/etical-hacking

Ethical Hacking. (s.f.). Obtenido de Darkjrof.Wordpress: http://darkjrof.wordpress.com/2011/01/28/introduccion-al-hacking-etico/

Ethical Hacking. (s.f.). Obtenido de Introducción al Ethical Hacking: http://don/introduccion-al-ethical-hacking#

Ethical Hacking. (s.f.). Obtenido de Monografías: http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtml

itSME. (2009). "Fundamentos de Gestión de Servicios TI basados en ITIL".

Juan Antonio Calles García. (2013). "La biblia del Footprinting".

Metodología Delphi. (s.f.). Obtenido de Echalemojo: http://www.echalemojo.com/uploadsarchivos/metodo_delphi.pdf

Metodología Delphi. (s.f.). Obtenido de Scribd: http://es.scribd.com/doc/94271885/metodo-DELPHI

Prácticas. (s.f.). Obtenido de Jbercero: http://www.jbercero.com/index.php?

Prácticas. (s.f.). Obtenido de Labs.dragonjar: http://labs.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-enumeracion-del-objetivo-ii

Prácticas. (s.f.). Obtenido de Cibersociedad: http://www.cibersociedad.net/congreso/g11_t1.pdf

Seguridad Informática. (s.f.). Obtenido de Definicion ABC: http://www.definicionabc.com/tecnologia/seguridad-informatica.php

Seguridad Informática. (s.f.). Obtenido de Wps.Prehnhall: http://wps.prenhall.com/bp_security_2006_1/

Seguridad Informática. (s.f.). Obtenido de Kioskea: http://es.kioskea.net/contents/secu/secuintro.php3.

Tori, C. (s.f.). Hacking Etico.