IMPLANTACIÓN DE TÉCNICAS Y ADMINISTRACIÓN DEL LABORATORIO PARA INVESTIGACIÓN DE ETHICAL HACKING DEL DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN DE LA ESPE

Lucía Sandoval Méndez, Andrea Vaca Herrera, Ing. Mauricio Campaña, Ing. Mario Ron Egas

Escuela Politécnica del Ejército, Quito Ecuador, lucerok_89@hotmail.com

Escuela Politécnica del Ejército, Quito Ecuador, aevaca2@espe.edu.ec

Escuela Politécnica del Ejército, Quito Ecuador, emcampania@espe.edu.ec

Escuela Politécnica del Ejército, Quito Ecuador, mbron@espe.edu.ec

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 y para este efecto se describe la implantación de técnicas y la propuesta de los servicios que el Laboratorio brindará no solo a los estudiantes y docentes de la Escuela Politécnica del Ejército sino a la comunidad en general.

Esta publicación presenta el diseño de los servicios del Laboratorio utilizando ITIL en sus tres primeras fases hasta llegar a un 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.

Palabras Clave: Seguridad Informática, Ethical Hacking, Informática Forense, Técnicas.

ABSTRACT

This project pretends design services based on ITIL, which ones will be offered by an Ethical Hacking Investigation Lab.

The insecurity and information lost in organizations and companies in the last years are consequences of their lack of concern about safety information in the services that they offered, which leads to vulnerabilities that need to be discovered by personal and specialized services in Ethical Hacking; this gives rise to create an Ethical Hacking Lab of ESPE University and this describes the implementation of techniques and the propose of Lab services, that it provides, not only for students and teachers of Escuela Politécnica del Ejército Univerity, but also general community.

This publication presents a design of Laboratory services using the three first phases of ITIL to reach a transition plan of the services designed. To ensure an appropriate process, the design is validated by experts, using Delphi's method.

KeyWords: Information Security, Ethical Hacking, Computer Forensics, Techniques

1. INTRODUCCIÓN

Las computadoras alrededor del mundo están siendo víctimas sistemáticamente 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.

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 práctica probada: "Para atrapar a un ladrón debes pensar como un ladrón".

Es necesario, por tanto, determinar las herramientas y técnicas necesarias para probar la vulnerabilidad de los sistemas de información ya implantados. De ahí 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 han presentado.

2. METODOLOGÍA

Se aplica una metodología, relacionada con la búsqueda y generalización de casos de estudio adecuados a la práctica de Ethical Hacking, en concordancia con la educación y con la investigación profesional de vulnerabilidades informáticas.

La propuesta de Servicios del Laboratorio de Ethical Hacking basada en ITIL V3, cumple con las tres primeras fases del ciclo de ITIL que tiene las siguientes características que se muestra en la Figura 1.

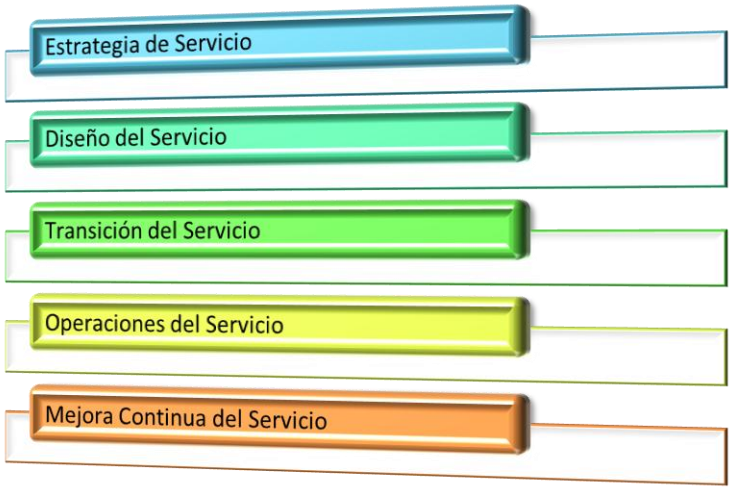

Figura 1. Ciclo de vida del servicio

Todas las fases de ITIL son importantes para establecer servicios, sin embargo para este proyecto se emplean las tres primeras:

- ✓ Estrategia del Servicio, que responde a las siguientes preguntas:
  - ¿Qué servicios debemos ofrecer?
  - ¿Cuál es su 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 de la competencia?
- ✓ Diseño del Servicio, que sigue las directrices establecidas en la fase de Estrategia y colabora 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.
  - Aporten valor a clientes y usuarios.
- ✓ 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.
  - Comunicar el cambio a todos los agentes implicados.

Para el desarrollo de las tres primeras etapas del ciclo de vida de ITIL V3, se usa herramientas de investigación, primarias y secundarias, que permiten obtener resultados útiles para realizar la propuesta de los Servicios que el Laboratorio de Ethical Hacking ofrece.

La calidad de las prácticas de Ethical Hacking es demostrada mediante el método DELPHI, que consiste en la selección de un grupo de expertos, quienes evalúan las prácticas de acuerdo a ciertas características que se detallan a continuación:

- 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

3. DISEÑO E IMPLEMENTACIÓN

3.1. Estrategia del Servicio

La Propuesta de Servicios en el Laboratorio de Ethical Hacking basado en ITIL V3, se realiza mediante una oferta de servicios orientados al negocio, a través de la gestión financiera, gestión de la demanda y la gestión de portafolio, los que permiten comparar los requerimientos de los clientes con el mercado y saber si los servicios que se oferta tendrán una acogida en la Universidad.

3.2. Diseño del Servicio.

Se establece la gestión del Catálogo del Servicio, gestión de niveles de servicio, gestión de la capacidad, gestión de la disponibilidad, gestión de la continuidad del servicio, gestión de la seguridad de la información y gestión de los proveedores las que apoyan al diseño de los servicios propuestos. Estos procesos ayudan a que el servicio sea de calidad porque mide los riesgos que pueden presentar cuando estén en operación y las posibles soluciones que se pueden establecer.

Una vez elaborada la propuesta de los Servicios del Laboratorio de Ethical Hacking, se realiza un análisis de la misma con expertos en ITIL V3, usando el método DELPHI. Los expertos realizan modificaciones, sugerencias y determinan que las prácticas que diseñadas para el Laboratorio de Ethical Hacking son útiles, no solo para los estudiantes y docentes de la Escuela Politécnica del Ejército sino también para la comunidad en general.

3.3. Transición del Servicio

El plan de transición del servicio detalla el proceso a seguir, para instalar los servicios que brinda el Laboratorio de Ethical Hacking; describe las actividades que se realizan para brindar los servicios y que cumplan con todos los requerimientos que ITIL V3 establece.

4. RESULTADOS

A continuación se presenta los resultados obtenidos en cada una de las actividades del Diseño e Implementación descrito anteriormente:

4.1. Estrategia del Servicio

La Estrategia del Servicio permite conocer los requerimientos no solo de los estudiantes sino de los docentes y comunidad en general. En Gestión de la Demanda se obtuvo los siguientes resultados que son mostrados en la Figura 2.

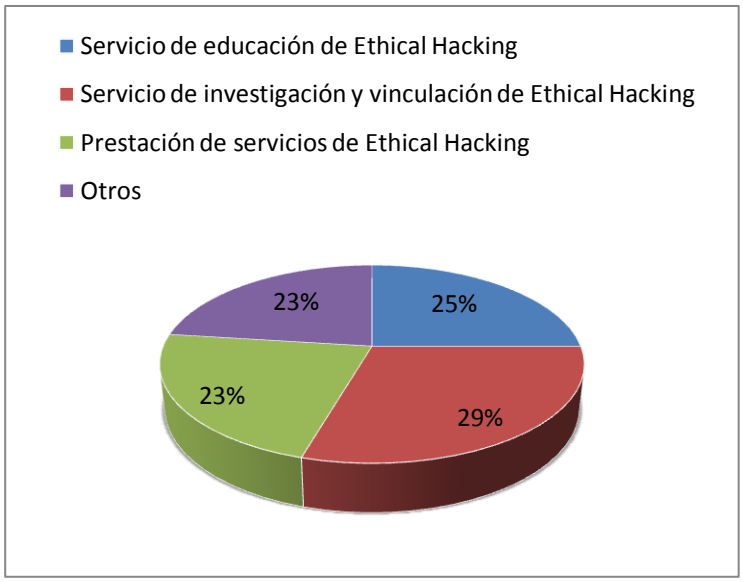

Figura 2. Resultados de Servicios

A través de las encuestas realizadas a una población de 384 personas se definen los principales servicios que el Laboratorio de Ethical Hacking debe ofrecer, tanto a la comunidad politécnica como a la comunidad en general.

En esta fase se obtiene una propuesta de los servicios del Laboratorio que debe ser analizada con la utilidad que puede tener la Universidad al ofrecer los servicios que se señalan en la figura 2. Esa estrategia debe convencer a quien toma decisiones, que no solo es una inversión para la Universidad sino para el país.

4.2. Diseño del Servicio

En esta etapa de ITIL V3 se presenta el diseño de prácticas que serán desarrolladas por los estudiantes, docentes y comunidad en general en las instalaciones del Laboratorio de Ethical Hacking. Las siguientes tablas representan la capacidad del laboratorio, el personal que participa y su disponibilidad.

Tabla 1. 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	1	17.34	17.34
	Prestación de Servicio de Ethical Hacking	1	17.34	17.34

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

Tabla 2. 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	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 Mainboard: ASUS Sabertooth X79 (Intel X79 Chipset) (Features USB 3.0 and SATA 6Gb/s) RAM: 16 GB Discos Duros: • 120GB Solid State (SATA 6Gbps) • 1TB WDCaviar (7200 RPM)
		Software **(**Backtrack, WinHex)	1	Software con el que se puede realizar: • Test intrusión • Ingeniería Social • Spidering • SQL Injection • Man in the Middle • Phising • Pharming • Entre otras técnicas de Ethical Hacking

Tabla 3 Recursos Humanos

	Servicio	Nº	Grado
Recursos Humanos	Servicio de Educación	1	Docentes
	Servicio de Investigación	1	Laboratorista
	Prestación de Servicio de Ethical Hacking	1	Docentes

Tabla 4 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

El Laboratorio de Ethical Hacking consta de un espacio físico de 17.34 metros cuadrados con la capacidad para 32 estudiantes quienes reciben la cátedra Ethical Hacking, para lo cual se dispone de 16 mesas dobles, 32 sillas y un escritorio para el docente. En cuanto al equipamiento tecnológico el laboratorio consta de: un proyector instalado en el techo, un sistema de cableado estructurado conectado a un switch, 2 servidores y 32 computadoras. En este espacio se desarrolla prácticas y estudio de Ethical Hacking, donde se usa el hardware y software respectivo anteriormente descrito desarrollando así diferentes habilidades del estudiante.

4.3. Transición del Servicio

El alcance del presente trabajo cumple únicamente hasta el plan de transición del servicio que se detalla a continuación:

Plan de Transición del Servicio

- Tareas:

1. Realizar 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.

2. Poner a disposición: La actividad publicitaria es puesta 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 presenta en las redes sociales la información principal de los diversos cursos y seminarios que se vayan a desarrollar.

   Se generan 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.

3. Seleccionar 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.

4. Capacitación: En esta fase participan todos los docentes que han cumplido con el perfil anteriormente mencionado, se les capacita 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 debe manejar para llevar a cabo las prácticas, así como también las consultorías que se puede asesorar.

5. Evaluación: Las personas que hayan asistido a la capacitación deben presentar una evaluación escrita, sobre los temas impartidos sobre la misma. Después de obtener los resultados de la evaluación, se escoge al personal correcto el cual desarrolla el respectivo syllabus de materia y el temario de los cursos o seminarios.

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.

- 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 presenta un cronograma con las actividades previstas.

- Costos

En el proyecto 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:

Tabla 5: Costo Hardware

Requerimientos	Especificación	Cantidad	Costo Unitario	Costo Total
Computadores escritorio	Core i7, disco 500GB memoria DDR3, monitor 18.5'	32	1000	32000,00
Computador portátil	Core i7, disco 500 GB, Monitor de 14'	2	1500	3000,00
Video proyectores		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				**46000,00**

- Software:

Tabla 6: Costo Software

Requerimientos	Especificación	Cantidad	Costo Unitario	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**

5. TRABAJOS RELACIONADOS

En el país aun no existen Universidades que ofrezcan los servicios del Laboratorio de Ethical Hacking de la ESPE. Estos servicios tienen la particularidad de estar orientados a los estudiantes y profesores en general, tanto en docencia como investigación; además brinda a la comunidad la oportunidad de participar en proyectos de vinculación relacionados con el tema.

Existe un proyecto de conformación del centro de investigación científica del Departamento de Ciencias de la Computación, que se encuentra en desarrollo al que integrará este proyecto.

6. CONCLUSIONES Y TRABAJO FUTURO

El hacking ético representa una solución para la seguridad en internet a través de pruebas que tienen un objetivo importante: encontrar las vulnerabilidades posibles que tiene un sistema o aplicación web para prevenir delitos informáticos.

El laboratorio de ethical hacking permite al estudiante trabajar en un equipo orientado a la seguridad de la información, donde puede realizar pruebas en los sistemas y hacer que estos alcancen situaciones críticas que pongan en riesgo la integridad del sistema, para definir entonces, medidas de seguridad y evitar accesos no permitidos.

Las herramientas seleccionadas para el uso en el laboratorio de ethical hacking, permiten al estudiante conocer las diferentes formas de prevenir las vulnerabilidades de los sistemas y aplicaciones web.

Se pretende incrementar el equipamiento y servicios del laboratorio e iniciar una red de investigadores que utilicen el laboratorio en esos fines.

7. REFERENCIAS

LIBROS

- Calles García, J.A. & Pérez González P., "La Biblia del Footprinting", Edición 2013, pp. 4
- itSMF, "Fundamentos de Gestión de Servicios TI basados en ITIL", Edición 2009
- Tori C.,"Hacking Ético", Edisión 2008, cap. I, pp. 15

WEB

Metodología Delphi

- Dozal Rodriguez S. "Investigación del Método Delphi";

http://es.scribd.com/doc/94271885/metodo-DELPHI

Seguridad Informática

- "Seguridad Informática";

http://www.definicionabc.com/tecnologia/seguridad-informatica.php

- "Introducción a la Seguridad Informática";

http://es.kioskea.net/contents/secu/secuintro.php3.

Delitos Informáticos

- Salellas L. "Delitos Informáticos-Ciberterrorismo";

http://www.cabinas.net/informatica/delitos_informaticos.asp

- Convenio de Cyber-delincuencia del Consejo de Europa Estados miembros del Consejo de Europa y otros Estados – Budapest 2001

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Ethical Hacking

- Maladón C. "Hacking Ético";

http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf

- Reyes Plata A. "Ethical Hacking";

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

- Menendez Méndez M. "Ethical hacking: Test de intrusión. Principales metodologías";

http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtml

- Yulder F. Bermeo “Introducción al Hacking Ético” ;

http://www.slideshare.net/YulderBermeo/introduccion-hacking-etico

ITIL V3

http://itilv3.osiatis.es/