UNIVERSIDAD POLITECNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERIA DE SISTEMAS

Tesis previa a la obtención del título de:

INGENIERO DE SISTEMAS

TEMA:

ESTUDIO DE LA UTILIZACIÓN DE SOFTWARE LIBRE PARA PERITAJE INFORMÁTICO PARTIENDO DE CASO REAL EN LA CIUDAD DE GUAYAQUIL

AUTORA:

RAQUEL ESTEFANIA MONTENEGRO SALTOS

DIRECTOR:

ING. GALO VALVERDE

Guayaquil, abril del 2015

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DE TRABAJO DE GRADO

Yo Raquel Estefania Montenegro Saltos autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

……

Raquel Estefania Montenegro Saltos

CC: 0923745731

DEDICATORIA

A Dios por darme la fuerza y la sabiduría para culminar una de mis principales metas.

A mi padre quien ha estado conmigo siempre, para él va éste logro ya que fue una de mis motivaciones para seguir adelante.

A mi madre que me enseñó desde pequeña a ser responsable en mis estudios y gracias a ella mi meta se cumple.

AGRADECIMIENTO

A Dios por guiarme en el buen camino y contar con él cuando me sentía sola.

A mi padre Pablo Montenegro quien ha sido mi ejemplo de superación y apoyo en mi carrera universitaria.

A mi madre Raquel Saltos quien marcó mi infancia enseñándome a ser responsable desde niña.

A mi hermana Geovanna Montenegro quien me daba consejos y ánimos para continuar con mi tesis.

A mi esposo Gianpaolo Dìaz quien estuvo en toda mi etapa universitaria y me apoyo incondicionalmente dándome fuerza para cumplir mi meta.

A mi tutor el Ing. Galo Valverde por la guía y apoyo en el proceso de tesis.

INDICE GENERAL

INDICE DE ILUSTRACION

INDICE DE TABLAS

INDICE DE ANEXOS

RESUMEN

El presente tema de tesis tiene como objetivo el uso de software libre partiendo de un caso real ocurrido en la ciudad de Guayaquil, mediante el diseño de un esquema que cuente con procedimientos, funciones y requerimientos mínimos para combatir los mismos.

Para el análisis de la información se utilizó varios software libres para tabular los datos y presentar información en forma gráfica. Se devela durante la investigación la inexistencia de acciones procedimentales, planes bien establecidos para resolver los casos de delitos informáticos y la falta de conocimiento sobre software libre que se pueden adquirir, preservar y recuperar evidencias digitales, además que los jueces no tienen adiestramiento para manejar las evidencias. Lo cual confirma la importancia de la propuesta del uso de un software libre para el procedimiento de peritaje informático, establecer los requerimientos mínimos necesarios para que la entidad pueda ejercer sus actividades de una manera eficiente, contando con funciones bien definidas según las necesidades y con los recursos con los que se cuentan, estableciendo también procesos y procedimientos que permitan controlar las funciones del peritaje informático.

La importancia científica de esta propuesta es la de aportar a la administración de justicia que permitan planificar, motivar y gestionar rápidamente la indagación de delitos informáticos.

ABSTRACT

The current thesis topic has an objective the use of open source based on a real case occurred in the city of Guayaquil, by designing a scheme that has procedure, functions and minimum requirements to attack them.

For information analysis, software was used to tabulate the data and present information in graphical form. It reveals during the investigation in surveys and interviews the lack of procedural actions, well-established plans for dealing with IT crime cases and the lack of knowledge about open source to acquire, preserve and recover digital evidences, moreover, that judges are not trained to handle these evidences. This confirms the importance of the proposal of the use an open source for the procedure of computer expertise, establishing the minimum necessary requirements for the entity to perform its activities efficiently, counting with well-defined functions according to current needs and the resources that they have, establishing processes and procedures that allow controlling functions of computer expertise.

The scientific importance of this proposal is to contribute to the justice administration guidelines for planning, motivating and quickly handle the investigation of IT crime.

INTRODUCCIÓN

El presente proyecto de tesis es una propuesta que sirve para poder implementar un nuevo esquema para el procedimiento de indagación de los delitos informáticos, en conjunto con las regulaciones existentes (leyes) para el manejo de los mismos.

Haciendo conocer el procedimiento y funciones que se debe realizar en el peritaje informático, y que estos puedan resolverlos de un manera ágil y precisa. Que cuenten con la preparación y pericia requerida para identificar, recoger, analizar y reportar evidencia digital como participantes en la administración de justicia en la sociedad ecuatoriana.

Este trabajo está dividido en 4 capítulos.

En el Capítulo 1, se revisa el planteamiento del problema, presentando la situación actual del procedimiento de peritaje informático, la justificación y objetivos de la investigación.

En el Capítulo 2, se describe el concepto y clasificación del delito informático, formulación de hipótesis y las variables de acuerdo a la información obtenida.

En el Capítulo 3, se detalla la metodología de investigación realizada para obtener la información y los mecanismos para el tratamiento de la misma.

En el Capítulo 4, se presenta el manual de procesos, funciones y requerimientos mínimos para indagar y resolver los delitos informáticos, se muestra ejemplos de delitos informáticos

CAPÍTULO 1

1.1 ANTECEDENTES DE LA INVESTIGACION

Muchas personas se han dedicado a desarrollar sistemas de computación para solucionar los problemas que tiene la sociedad o para el cumplimiento de actividades ilícitas.

La sociedad a nivel mundial ha sido perjudicada por ésta clase de delitos que a menudo son cometidos por personas que están inmersas en el campo de la informática y con elevadas posibilidades de que no lleguen a descubrirlos. Por lo tanto, se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

El término delito informático se acuñó a finales de los años noventa, a medida que internet se expandió por toda norteamérica. Después de una reunión en Lyón, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por lo que migraron a internet. El "Grupo de Lyón" utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos.

Al mismo tiempo, y guiado por los participantes en el grupo de Lyón, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático. Este tratado, que fuera presentado a la opinión pública por primera vez en el año 2000, incorporó una nueva gama de técnicas de vigilancia que las agencias encargadas de la aplicación de la ley consideraban necesarias para combatir el "delito informático". (Perrin, 2006)

En la actualidad el uso de la red mundial de información permite realizar negocios por vía telemática, realizar transferencias de fondos y utilización de datos en forma rápida, casi inmediata. Este desarrollo permite que también aparezcan nuevas formas de delinquir. Los perjudicados estafados por usar los servicios informáticos de las instituciones acusan a éstas de no tener las suficientes seguridades informáticas en sus páginas web.

La Fiscalía registra entre el año 2010 y abril del 2011, 2006 robos informáticos. Además explica que la "institución, al omitir su deber de protección, no le informa al cliente de los riesgos que existen al usar el servicio de banca en línea".

Las instituciones bancarias, son las mayores afectadas, según indagación de la Fiscalía.

Según experto de la fiscalía, el total en robos realizados por internet llega a $ 3 millones, de los que debería recuperar el 80% (aproximadamente $ 2,4 millones).

La cifra fue la más alta desde el 2009 cuando se registraron 168 casos; cantidad que se incrementó al siguiente año, en el 2010, con 1.099 quejas por "apropiación ilícita utilizando medios informáticos", como describe el delito la entidad. (El Universo, 2012).

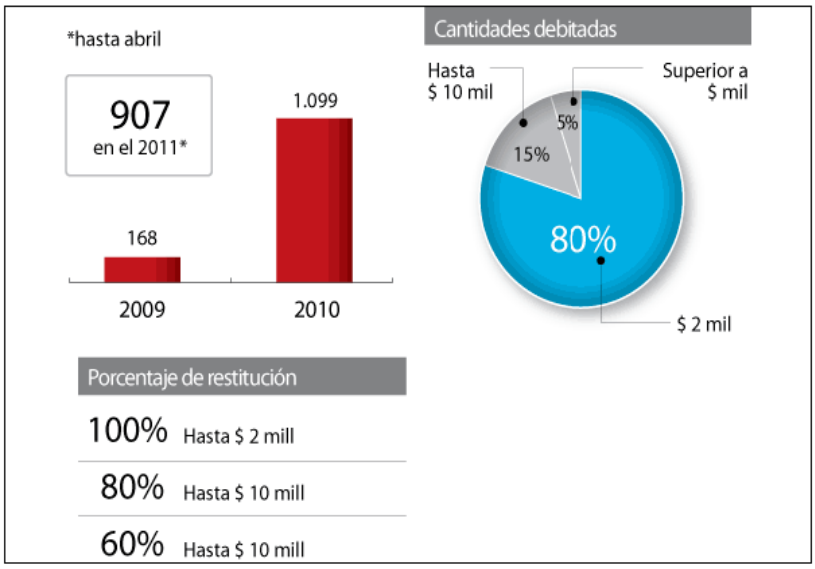

Figura 1.1 Delitos por Internet

Fuente: Fiscalía General y Superintendencia de Bancos, 2010

La falta de una política o un diseño efectivo en cuanto al uso de TICS, seguirá generando aumento en los casos de robos informáticos, por lo que los servicios informáticos no cuentan con la suficiente protección, para brindar seguridad a sus usuarios.

1.2 PROBLEMA DE INVESTIGACION

1.2.1 Planteamiento del problema

Los especialistas en peritaje informático actualmente están capacitados para realizar identificación y recolección de evidencias en medios magnéticos, comprensión y prácticas en procedimientos de revisión y análisis forense, comprensión de los diferentes sistemas de archivos asociados con sistemas operativos, acceso a archivos temporales, de cache, de correo electrónico, de web, etc.

Todas estas actividades se las realiza ya sea de manera manual como con el uso de herramientas que en su totalidad sus licencias son pagadas en altos costos y con buenos resultados. El procedimiento se realiza dependiendo del tipo de delito informático que se posee.

Se requiere entonces de una investigación en el cual proporcione herramientas de software libre efectivas con los mismos o mejores resultados que las que se poseen las herramientas licenciadas. Estas herramientas ayudarán al especialista agilitando el proceso de búsqueda de pruebas ya que muchas de estas aplicaciones son portables y compatibles con sistemas operativos usados.

La investigación se orientará dependiendo del tipo de delito real que se tiene para aprovechar las ventajas de uso que brinde el software libre.

1.2.2 Formulación del problema

¿Cuáles serían las herramientas de software libre que ayuden agilitando el proceso de peritaje informático partiendo de un caso real?

1.3 Objetivos de investigación

1.3.1 Objetivo General

Identificar el mejor uso de herramientas de software libre para el peritaje informático partiendo de un tipo de caso real de delito informático.

1.3.2 Objetivos Específicos

- Investigar y tipificar delitos informáticos denunciados en la Fiscalía General del Estado con jurisdicción en la ciudad de Guayaquil.
- Analizar a detalle uno de los casos denunciados para establecer cuáles serían las características en las herramientas de software a investigar.
- Identificar a detalle las características que brindan las herramientas investigadas.
- Analizar el funcionamiento de las herramientas de software libre investigadas.

1.4 Justificación de la investigación

La investigación propuesta se llevará a cabo con el objetivo de conocer nuevas herramientas sin costo con buenos resultados que ayuden a mejorar el proceso de recolección de evidencias, procedimientos para llegar a conocer pruebas concisas en cuanto a delitos informáticos se refiere.

La necesidad de investigar nuevas aplicaciones de software libre surge ante la actual situación en la que el perito informático tiene que recurrir a pagar por el uso de tecnología que lo ayude a realizar su informe detallado de la información recolectada.

El estudio permitirá dar a conocer nuevas aplicaciones que se pueden usar dependiendo del tipo de delito informático que se tenga. Este uso agilitará el análisis ya que los resultados serán los mismos que los que brinda una herramienta licenciada.

CAPÍTULO 2

2.1 MARCO TEORICO

2.1.1 Delitos Informáticos

Las tecnologías de la información y comunicación están cambiando la sociedad en todas partes del mundo aumentando la productividad, acelerando el tiempo de respuesta, mejorando los procesos en las entidades, pero este desarrollo viene acompañado con nuevas formas de delincuencia informática.

La delincuencia informática es difícil de comprender y conceptualizar plenamente. A menudo, se la considera una conducta proscrita por la legislación y/o jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito, se dirige a las propias tecnologías de la computación y las comunicaciones, o incluye la utilización incidental de computadoras en la comisión de otros delitos (Congreso de las Naciones Unidas, 2005)

Conocer el comportamiento de cómo los incidentes de seguridad, las vulnerabilidades y la criminalidad informática, es vital para el análisis de los delitos informáticos, ya que han tenido un repunte a los largo de los últimos años, por ello, se requiere analizar la tendencia de dichos componentes.

El organismo que realiza investigaciones de este nivel es el CERT (Computer Emergency Response Team), que publica una variedad de estadísticas relacionadas con las vulnerabilidades, que se han catalogado basados en informes de fuentes públicas y reportes que son directamente comunicados mediante su sistema web. Tal como se puede observar en la figura 2.1, se concluye que la tendencia sobre las vulnerabilidades tiene un crecimiento significativo a lo largo de los años que se han analizad.

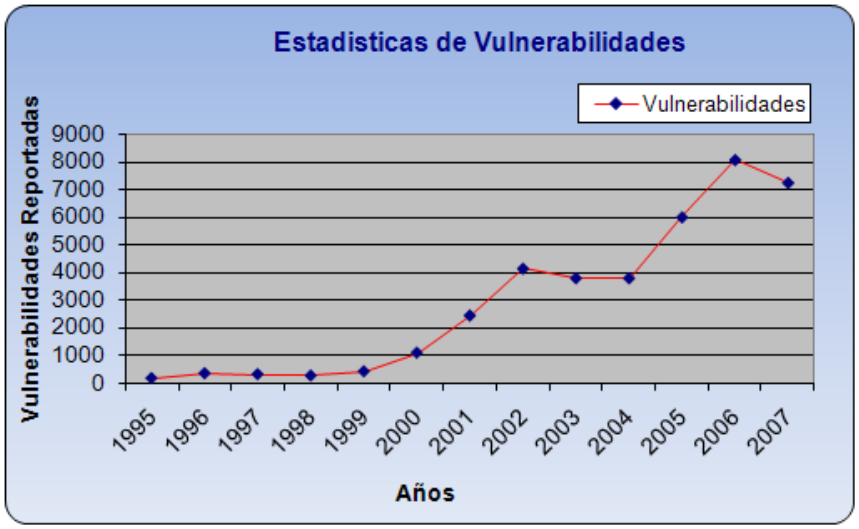

Figura 2.1 Estadísticas de Vulnerabilidad
Fuente: CERT – Informe de vulnerabilidades reportadas 2007

Delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin. (Lima, 2013)

2.1.2.1 Tipos de delincuencia Informática

2.1.2.1.1 Virus Informáticos

Atacan a las propias tecnologías de la información y las comunicaciones, como los servidores y sitios Web, causan considerables perjuicios a las redes comerciales y de consumidores.

Un virus informático son pequeños programas diseñados para propagarse de una computadora a otra e interferir con el funcionamiento de las mismas.

Un virus podría dañar o borrar los datos de su computadora, utilizar su programa de correo electrónico para transmitirse a otros equipos o incluso borrar todo su disco duro.

Los virus informáticos se propagan a menudo a través de documentos adjuntos en mensajes de correo electrónico o de mensajería instantánea. (Microsoft, 2012)

La manera de funcionar de un virus en la siguiente:

- Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario.

- El código del virus queda residente en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse.

- El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución.

- Se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa. (Security, 2010)

2.1.2.1.2 Vandalismo electrónico y la falsificación profesional

Los avances tecnológicos en materia de seguridad informática que las empresas han implantado para evitar las infiltraciones a sus sistemas computacionales y el robo de información, el descuido de los empleados sigue representado el factor primordial por el que los “vándalos informáticos” siguen teniendo éxito.

Estas debilidades son continuamente aprovechadas por los delincuentes dentro de lo que es la "ingeniería social", una habilidad utilizada en el mundo de la informática y por la que se manipula al personal de las empresas para así obtener información confidencial o simplemente provocar problemas.

Con la ingeniería social hay "miles" de maneras para perpetrar y robar información empresarial o personal; además, los ataques se pueden realizar con equipos que cuestan unos cuantos dólares. (Mundo Contact, 2010)

2.1.2.1.3 Falsificación

La falsificación es un acto consistente en la creación o modificación de ciertos documentos, efectos, productos (bienes o servicios), con el fin de hacerlos parecer como verdaderos, o para alterar o simular la verdad. (Mundo Contact, 2010)

2.1.2.1.4 Sabotaje informático

Todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Básicamente, se puede diferenciar dos grupos de casos, por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

- **Conductas dirigidas a causar daños físicos:** El primer grupo comprende todo tipo de conductas destinadas a la destrucción "física" del hardware y el software de un sistema.

- **Conductas dirigidas a causar daños lógicos:** El segundo grupo más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos "lógicos", o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático. (Campos, 2010)

2.1.2.1.5 Ingeniería social

Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permita realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgos o abusos.

Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Via internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas "cadenas", llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. (Barrios, 2011)

- **Pishing.-** Es la construcción de mensajes de correo electrónico con páginas web correspondientes diseñadas para aparecer como sitios de consumidores existentes. Se distribuyen millones de estos mensajes fraudulentos de correo electrónico, que anuncian como provenientes de bancos, subastas en líneas u otros sitios legítimos para engañar a los usuarios a fin de que comuniquen datos financieros, datos personales o contraseñas.

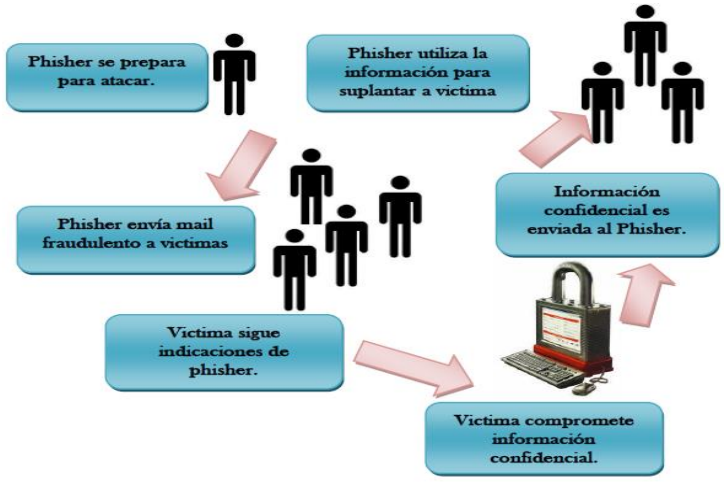

Figura 2.2 Funcionamiento de Pishing

Fuente: Autor

Habitualmente los kits de creación de phishing que facilitan la creación de páginas falsas de distintas entidades, están contenidas en tres partes:

- La réplica de la página web que pretende ser simulada. Esta consta a su vez de páginas HTML, JavaScript, etc. que normalmente son colgadas en cualquier servidor y se debe incitar al usuario a visitarla. Es muy sencillo de obtener puesto que vale con "descargar" con algún programa la web legítima.

- La lógica del robo de contraseñas. Normalmente es un programa PHP que, o bien envía las contraseñas de formulario por correo electrónico, o bien las almacena en un archivo en el propio servidor y el atacante las obtendrá de ahí más adelante. Suelen ser apenas unas líneas de código muy sencillas. En el kit, lo deja todo preparado para que el usuario solo deba modificar la dirección a la que quiere que vayan a parar las contraseñas robadas.

- Un correo que, con cualquier excusa, invita al usuario a visitar la web simulada. Suele contener un logotipo y será enviado de forma masiva a miles de cuentas de

correo. Se suelen utilizar programas específicos para el envío masivo de correos o programas también en PHP que se aprovechan del motor de correo de páginas de terceros. (Hispasec, 2011)

- **Scamming.-** por el contrario, la típica labor que conducen a una estafa. Por lo general empieza con una carta enviada en forma masiva con el nombre del destinatario, y al cual le pueden ofrecer una serie de oportunidades de ganar dinero, premios, préstamos a bajo interés, etc.

    - Oportunidad del cobro de una suma de dinero en algún país lejano como resultado de una resolución judicial.

    - Una persona "amiga" en el extranjero lo refirió para el sorteo de un viaje en crucero durante 7 días, para dos personas.

    - Préstamos de dinero o refinanciamiento de deudas a muy bajo interés.

    - Comunicación de haber ganado un premio en una Lotería.

    - Apelar al dolor humano para contribuir a una causa noble. Puede estar combinado con el Pishing.

    - Venta de software por Internet, supuestamente legal y licenciado. (Informatica juridica, 2010).

- **Pharming.-** método utilizado para enviar a la víctima a una página web que no es la original solicitada. (Todoecommerce, 2011)

- **Skimming.-** robo de la información que contiene una tarjeta de crédito. (ConsumidorGov, 2010)

- **Sniffing.**- la habilidad de un agresor de escuchar a escondidas las comunicaciones entre hosts de la red. (RoboyFraude, 2012)

2.1.2.2 Fundamentación Legal

En la Legislación del Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías , tales como:

1. Ley Orgánica de Transparencia y Acceso a la Información Pública
2. Ley de Comercio Electrónico Firma Electrónicas y Mensajes de Datos.
3. Ley de Propiedad Intelectual
4. Ley Especial de Telecomunicaciones
5. Ley de Control Constitucional (Habeas Data)

Figura 2.9 Legislación - Ecuador
Fuente: Autor

2.2 MARCO CONCEPTUAL

Software.- Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. (Real Academia Española, 2015).

Bit.- Unidad de medida de información equivalente a la elección entre dos posibilidades igualmente probables. (Microsoftbusiness, 2010).

Linux.-Es un sistema operativo: un conjunto de programas que le permiten interactuar con su ordenador y ejecutar otros programas. (Debian, 2010).

Atm.-Máquina conectada informáticamente con un banco que permite efectuar al cliente ciertas operaciones bancarias mediante una tarjeta o libreta magnéticas que tienen asignada una clave personal. (Segu-info, 2007).

Fraude Informática.- Cualquier cambio no autorizado y malicioso de datos o informaciones contenido en un sistema de información. (Debian, 2010)

HTML.- Es un lenguaje de programación que se utiliza para el desarrollo d páginas de internet. Se trata de la sigla que corresponde a Hyper Text Markup Language, es decir lenguaje de marcas de hipertexto. (Definicion, 2008)

Informática Forense.- Se considera el uso de técnicas analíticas y de investigación para identificar, recopilar, analizar y preservar las pruebas/información que se almacena magnéticamente o codificado. (Audoria, 2011)

Auditoria Informática.- Es la revisión técnica, especializada y completa que se realizan a los sistemas informáticos, redes, instalaciones, comunicaciones y todo el entorno computacional, a fin de analizar, evaluar, verificar y recomendar asuntos relativos a la planificación, control eficacia, seguridad y adecuación del servicio informático en la empresa. (Audoria, 2011)

2.3 FORMULACIÓN DE HIPÓTESIS Y VARIABLES.

2.3.1 Hipótesis General

El uso que se obtendrá de las herramientas software libre es una opción más conveniente al momento de realizar un peritaje. Se conseguirá los mismos o mejores resultados que usando una herramienta licenciada.

2.4 VARIABLES INDICADORES.

2.4.1 Dependientes

- ✓ Tipos de delitos informáticos
  - **Indicador**
    - Denuncias de delitos informáticos realizadas en la ciudad de Guayaquil

- ✓ Herramientas de peritaje existentes
  - **Indicador**
    - De tipo licenciadas y de software libre.

- ✓ Características de herramientas
  - **Indicador**
    - Servicios que brindan las herramientas

2.4.2 Independientes

- ✓ Tiempo al realizar el peritaje informático.
  - **Indicador**
    - Uso de la herramienta para el peritaje.

CAPÍTULO 3

ANÁLISIS DE SISTEMAS PARA PERITAJE INFORMATICO

3.1 HACKING ETICO

El hacking ético se refiere a la acción de efectuar pruebas de intrusión controladas sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker, para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole - en algunos casos - acceso al sistema afectado inclusive; pero siempre en un ambiente supervisado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización cliente.

Es importante enfatizar que aunque es indudable que el pentester debe poseer conocimientos sólidos sobre tecnología para poder efectuar un hacking ético, saber de informática no es suficiente para ejecutar con éxito una auditoría de este tipo. Se requiere además seguir una metodología que permita llevar un orden en el trabajo para optimizar tiempos en la fase de explotación, además de aplicar el sentido común y experiencia. (Astudillo, Hacking Etico 101, 2013)

3.2 FASES DE AUDITORIA INFORMATICA

Las fases a seguir al momento de realizar una auditoria informática son los siguientes:

- **Reconocimiento.-** Fase preparatoria en la que el ataque busca reunir tanta información como sea posible acerca del objetivo de la evaluación antes de iniciar el ataque. (Seguridad web, 2010)

- **Escaneo.-** Fase en el cual el atacante utiliza toda la información que obtuvo en la Fase del Reconocimiento (Fase 1) para identificar vulnerabilidades específicas. Por ejemplo, si en la Fase 1 el atacante descubrió que su objetivo o su víctima usa el sistema operativo Windows XP entonces el buscara vulnerabilidades específicas que tenga ese sistema operativo para saber por dónde atacarlo. También hace un escaneo de puertos para ver cuáles son los puertos abiertos y usa herramientas automatizadas para escanear la red y permita el acceso al sistema. (Seguridad web, 2010)

- **Obtener acceso.-** Fase de penetración al sistema, en ésta 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 buffer overflows (desbordamiento de buffer), denial-of-service (negación de servicios), sesión hacking (secuestro de sesión), y password cracking (romper o adivinar claves usando varios métodos como: dictionary attack y brute forcé attack). (Seguridad web, 2010)

- **Mantener acceso.-** Fase en el cual su prioridad es mantener el acceso que gano en el sistema. En esta fase el Hacker usa sus recursos y recursos del sistema 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 (File Transfer Protocol), también puede tener la habilidad de subir, bajar y alterar programas y data. (Seguridad web, 2010).

- **Escribir informe.-** La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración del informe es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor. (Astudillo, Hacking Etico 101, 2013)

- **Presentar informe final.-** El último paso de esta metodología es presentar formalmente el informe y el dictamen de la auditoria al más alto de los directivos de la empresa, donde se informa de los resultados de la auditoría. Tanto el informe como el dictamen deben presentarse en forma resumida, correcta y profesional. La presentación de la misma se hace en una reunión directiva y por eso es indispensable usar un lenguaje claro tanto en el informe como en la exposición del mismo. (Datateca, 2004)

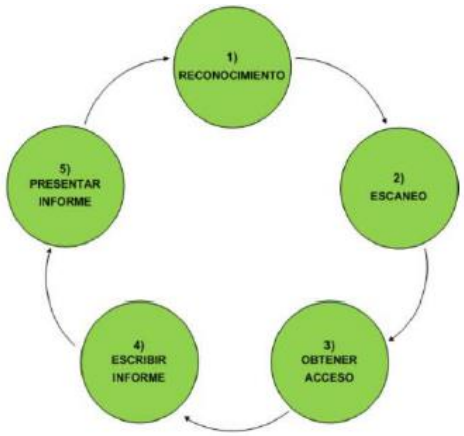

Figura 3 Fases de Auditoria Informática
Fuente: Etical Hacking, 2013

3.3 MODALIDAD DEL HACKING

Dependiendo de la información que el cliente provea al consultor, el servicio de hacking ético se puede ejecutar en una de tres modalidades:

- Black-box hacking
- Gray-box-hacking
- White-box-hacking

3.3.1 Black box hacking

También llamado hacking de caja negra. Esta modalidad se aplica a pruebas de intrusión externas. Se llama de este modo porque el cliente solamente le proporciona el nombre de la empresa a auditar al consultor, por lo que éste obra a ciegas, la infraestructura de la organización es una caja negra para él.

Si bien este tipo de auditoría se considera más realista, dado que usualmente un agresor externo que elige una víctima X no tiene más información al inicio que el nombre de la organización a atacar, también es cierto que requiere una mayor inversión de tiempo y por ende el costo incurrido es superior. Adicionalmente se debe notar que el hacker ético – a diferencia del cracker - no cuenta con todo el tiempo del mundo para efectuar las pruebas de intrusión, por lo que la fase preliminar de indagación no puede extenderse más allá de lo que en términos prácticos sea posible para el cliente en razón del costo/tiempo/beneficio. (Astudillo, Hacking Etico 101, 2013)

3.3.2 Gray box hacking

También llamado hacking de caja gris. Esta modalidad suele utilizarse como sinónimo para referirse a las pruebas de intrusión internas. Para algunos auditores también le llaman gray-box-hacking a una prueba externa en la cual el cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como la dirección IP y el tipo/función del equipo (router, web-server, firewall, etc.).

Cuando el término se aplica a pruebas internas, se denomina así porque el consultor recibe por parte del cliente solamente los accesos que tendría un empleado de la empresa, es decir un punto de red para la estación de auditoría y datos de configuración de la red local (dirección IP, máscara de subred, gateway y servidor DNS); pero no le revela información adicional como por ejemplo: usuario/clave para unirse a un dominio, la existencia de subredes anexas, etc. (Astudillo, Hacking Etico 101, 2013)

3.3.3 White box hacking

También denominado hacking de caja blanca. Esta modalidad se aplica a pruebas de intrusión internas solamente y se llama de ésta forma porque la empresa cliente le da al consultor información completa de las redes y los sistemas a auditar.

Es decir, que además de brindarle un punto de red e información de configuración para la estación de auditoría, como en el hacking de caja gris, el consultor recibe información extensa como diagramas de red, listado detallado de equipos a auditar incluyendo nombres, tipos, plataformas, servicios principales, direcciones IP, información de subredes remotas.

Debido a que el consultor se evita tener que averiguar esta información por sí mismo, este tipo de hacking suele tomar menos tiempo para ejecutarse y por ende reduce costos también. (Astudillo, Hacking Etico 101, 2013)

3.4 SOFTWARES LIBRE PARA PERITAJE INFORMATICO

A continuación se revisarán herramientas de software que no sólo ahorran tiempo en el reconocimiento del delito informático, sino que además facilitan la escritura del informe, gracias a que cuentan con interfaces gráficas amigables que muestran la información recolectada de forma ordenada y, en algunos casos, cuentan inclusive con opciones para generar reportes que resultan muy útiles para ser incluidos como anexos en la documentación.

3.4.1 Tracke Route Visual

Durante la ejecución de un hacking externo de caja negra resulta útil conocer la ubicación geográfica de un determinado objetivo. Por ejemplo se determinó los nombres del servidor de correo y del servidor web del cliente y se quiere saber si estos servicios están alojados en la red pública administrada por dicha empresa o si por el contrario están ubicados en un hosting externo como Yahoo Small Business, Gator, o similares.

¿Por qué se desea conocer esto? Muy simple, si resulta que están alojados en un hosting externo, en el hipotético evento de que se logre ingresar a dichos equipos, en realidad se estaría vulnerando al proveedor de hosting.

Debido a ésto es conveniente realizar un trazado de ruta que facilite conocer la ubicación geográfica de un nombre de host o de una dirección IP. De ese modo se sabrá si tiene sentido o no tratar de vulnerar dicho equipo.

Existen en el mercado diversas aplicaciones de traceroute visual, por mencionar algunas: Visual IP Trace, Visual Route. Algunas de ellas son gratuitas o tienen versiones pagadas que tienen características adicionales como emisión de reportes en formato html.

Además de las aplicaciones que se instalan en el PC existen utilidades web para tracerout visual disponibles para uso gratuito en internet como por ejemplo, la provista por la empresa You Get Signal. Estos aplicativos web tienen como ventaja su simplicidad, pero su debilidad es que no generan informes, por lo que corresponde al investigador realizar capturas de pantalla para incluirlas como evidencia dentro de la documentación. (Astudillo, Hacking Etico 101, 2013).

A continuación un ejemplo en el cuál se puede observar las utilidades que tiene la herramienta:

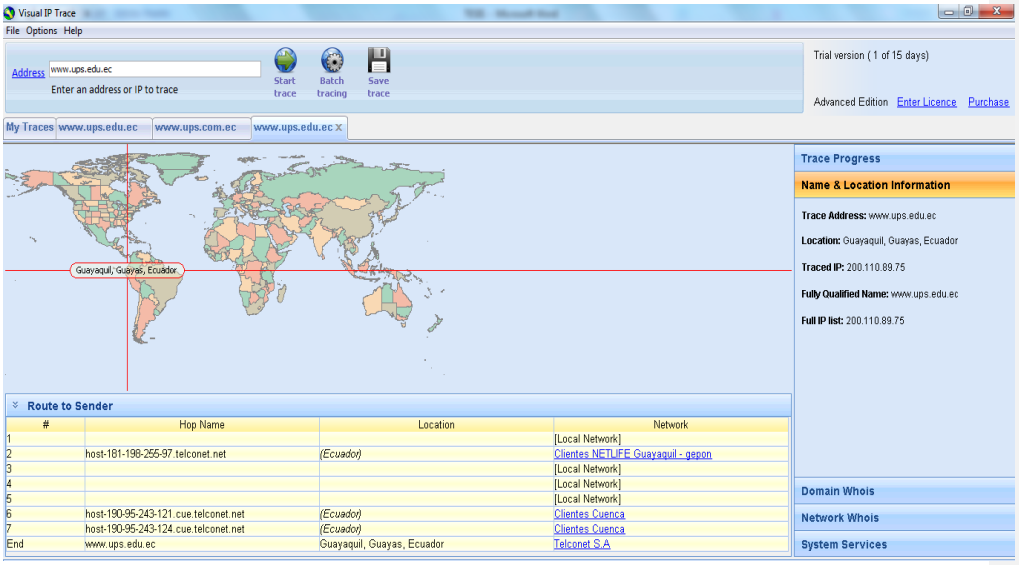

Figura 4 Trazado visual de www.ups.edu.ec en Visual IP Trace

Fuente: Autor

Como se observa en el gráfico la información que se obtiene es la ubicación del host y la IP. Adicionalmente se obtiene toda la información del proveedor del host www.ups.edu.ec.

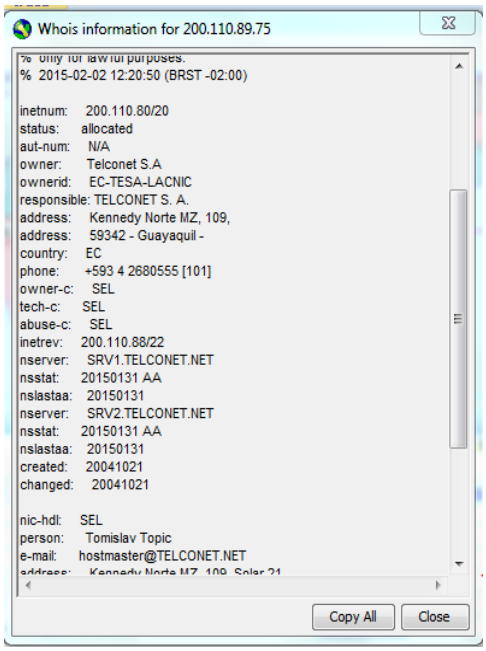

Figura 5 Información de Proveedor
Fuente: Auto

3.4.2 Visualroute

Visualroute es un programa que combina una interfaz gráfica de control de software más popular de la red: Ping, Traceroute y Whois. Analiza la situación de la interconexión de los distintos nodos de internet, que muestra la ruta de un servidor a otro en un mapa geográfico. (VISUALROUTE, 2012).

A continuación se detallará un ejemplo en el cuál se podrá observar las utilidades que posee la herramienta VISUALROUTE.

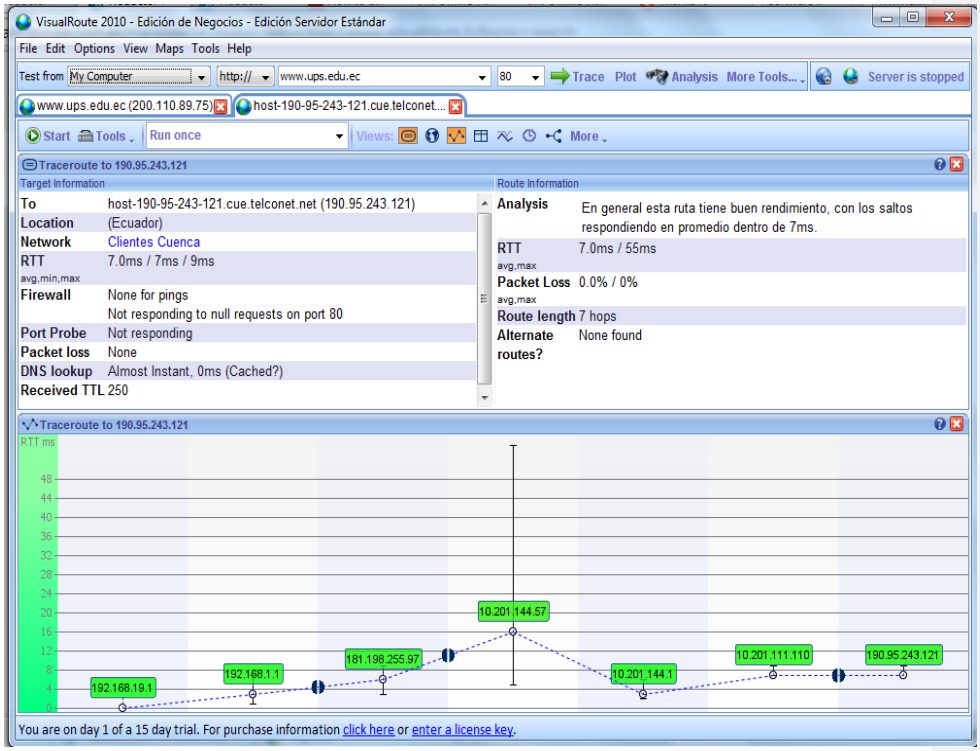

Figura 6 Información UPS en VisualRoute
Fuente: Autor

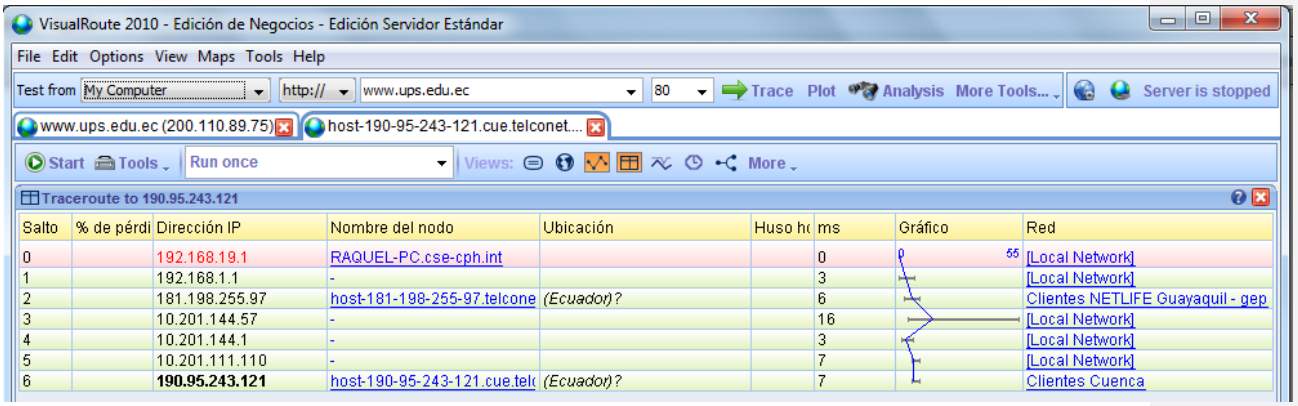

Figura 7 Traceroute dominio www.ups.edu.ec
Fuente: Autor

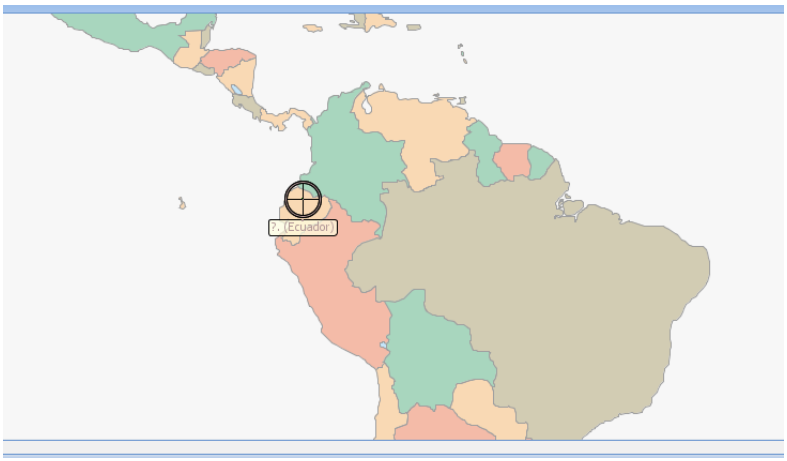

Figura 8 Ubicación Geográfica de www.ups.edu.ec
Fuente: Autor

Como se muestra en la gráfica se identifica la dirección IP del dominio www.ups.edu.ec la cual está ubicada en Ecuador, de ahí la importancia de determinar la ubicación geográfica de un host descubierto en un hacking externo antes de pasar a las fases de escaneo y explotación.

3.4.3 Email Tracker Pro

Es una herramienta fácil de usar para el análisis de encabezados de correo electrónico a revelar (o de spammer) la ubicación del remitente original. También puede enviar quejas de spam correctamente y fácilmente con eMailTrackerPro.

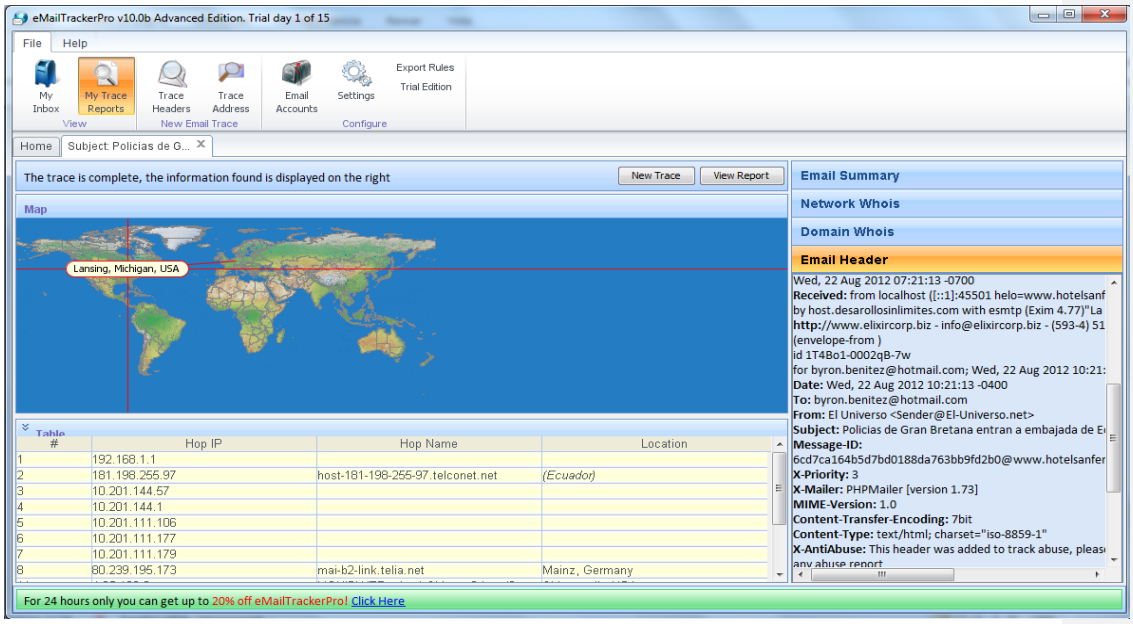

Figura 3.6 Email Tracker Pro
Fuente: Autor

3.4.3.1 Caso diario El Universo analizado por Elixircorp

En el año 2012 en el mes de Agosto circuló de forma masiva un correo electrónico sobre un supuesto ingreso forzado de los policías de Gran Bretaña a la Embajada del Ecuador para capturar a Julian Assange.

El correo electrónico decía provenir de diario El Universo, el diario ecuatoriano de mayor circulación nacional, por lo que muchos usuarios pensaron que se trataba de un correo

legítimo y lo abrieron e hicieron clic en el enlace que les mostraba el supuesto video del ingreso forzado a la embajada.

Por supuesto se trataba de una noticia falsa, distribuida con el ánimo de infectar con malware los computadores de los usuarios que ingenuamente descargaban el archivo sin sospechar que era de origen malicioso.

Esto generó una controversia entre los usuarios que por desconocimiento acusaban a **diario El Universo** de propagar noticias falsas y virus. Por ello, personal de sistemas del mencionado diario acudió a la empresa Elixircorp para solicitar que realicen un análisis del correo electrónico y de esta forma dar a conocer a los usuarios la verdad al respecto. (Astudillo, Elixircorp, 2012)

3.4.3.1.1 Análisis de correo diario El Universo

1. **CORREO ELECTRÓNICO MASIVO RECIBIDO POR LOS USUARIOS**


Date: Wed, 22 Aug 2012 10:21:13 -0400
To: byron.benitez@hotmail.com
From: Sender@El-Universo.net
Subject: Policias de Gran Bretana entran a embajada de Ecuador

EL UNIVERSO

Policias de Gran Bretaña entran a embajada de Ecuador.

Policias de Gran Bretaña entran a la **embajada de Ecuador** a capturar a **Julian Assange** en un operativo nunca antes visto en el ultimo tiempo...para ver más detalles de la noticia vea el video de lo acontecido.

Clic en el enlace para ver el video de la noticia:

http://www.eluniverso.com/servidor_videos/index.html?Wikileaks_Video

Figura 9 Email enviado por El Universo
Fuente: Hacking Ético 101

2. ANÁLISIS DEL CORREO ELECTRÓNICO

Como se puede observar fácilmente en el cuerpo del mensaje posicionando el puntero del mouse sobre el supuesto enlace hacia diario El Universo, que en realidad es una redirección a otro sitio web con url: http://www.lene-kinesiolog.dk/templates/stripes2/images/eluniverso.php?Wikileaks_Video

Figura 10 Cuerpo del correo
Fuente: Elixircorp

Como se puede ver en la imagen, el sitio al que se redirecciona pertenece a otro dominio en internet, diferente al del diario El Universo. De este primer hallazgo se puede hacer una primera conclusión ya que es un caso típico de PHISHING. (Astudillo, Análisis de correo caso Diario El Universo, 2012)

3. ANÁLISIS CON EL SOFTWARE LIBRE EMAIL TRACKER PRO

A continuación el reporte del análisis de cabeceras del correo electrónico en mención, generado con la herramienta E-Mail Tracker Pro:

From: Sender@El-Universo.net
To: byron.benitez@hotmail.com
Date: Wed, 22 Aug 2012 10:21:13 -0400
Subject: Policias de Gran Bretana entran a embajada de Ecuador
Location: Lansing, Michigan, USA

Misdirected: Yes (Possibly spam)
Abuse Address: abuse@liquidweb.com

Abuse Reporting: To automatically generate an email abuse report click here
From IP: 67.227.252.136

Header Analysis:

This email contains misdirection (The sender has attempted to hide their IP). The sender claimed to be from host.desarollosinlimites.com but lookups on that name shows it doesn't exist.

System Information:

- The system is running a mail server (*ESMTP Exim 4.84 #2*) on port 25. This means that this system can be used to send email.
- The system is running a web server (*Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 mod_jk/1.2.35 PHP/5.3.24*) on port 80 (click here to view it). This means that this system serves web pages.
- The system is running a secure web server (*Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 mod_jk/1.2.35 PHP/5.3.24*) on port 443 (click here to view it). This means that this system serves encryped web pages. It therefore probably handles sensitive data, such as credit card information.
- The system is running a file transfer server (*will be disconnected after 15 minutes of inactivity*) on port 21 (click here to view it). This means users are able to upload and download files to this system.

Código de campo cambiado

Código de campo cambiado

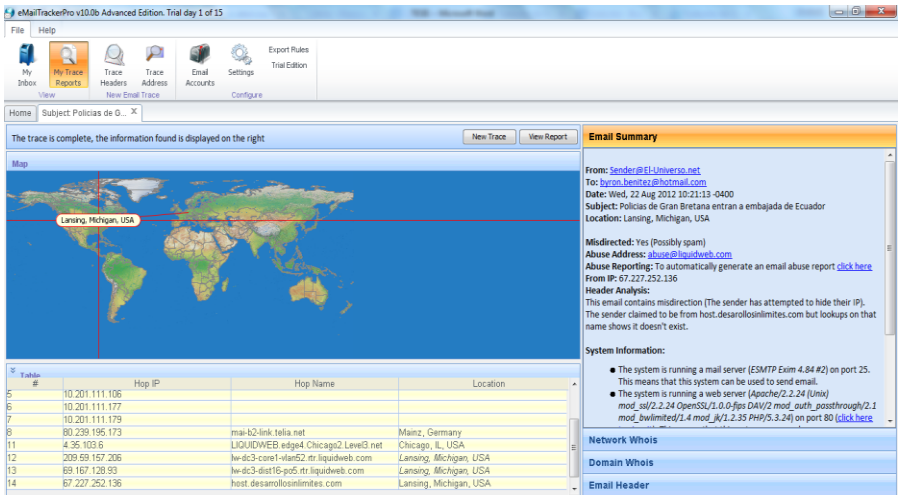

Figura 11 Consulta de correo en Email Tracker Pro
Fuente: Autor

Como se puede observar que el correo electrónico no se originó desde el dominio del diario El Universo, sino que su fuente es el host con dirección IP **67.227.252.136**, ubicado físicamente en la ciudad de Lansing en el estado de Michigan en Estados Unidos. Esto permite realizar una segunda conclusión y es que se trata de un mail forjado, es decir falso, que fue enviado con el ánimo de hacer creer al receptor que era una noticia legítima proveniente del diario El Universo.

3.4.4 Software libre de tcp-ping

Este tipo de software emula la función de un ping, en el sentido de que permite determinar si un host está activo, pero haciendo uso del protocolo TCP en lugar del acostumbrado ICMP (echo-request). Para ello se realiza una conexión a uno o más puertos bien conocidos en el equipo remoto esperando recibir respuesta; si el host analizado responde la solicitud de conexión, entonces es porque evidentemente se encuentra activo. (Astudillo, Hacking Etico 101, 2013)

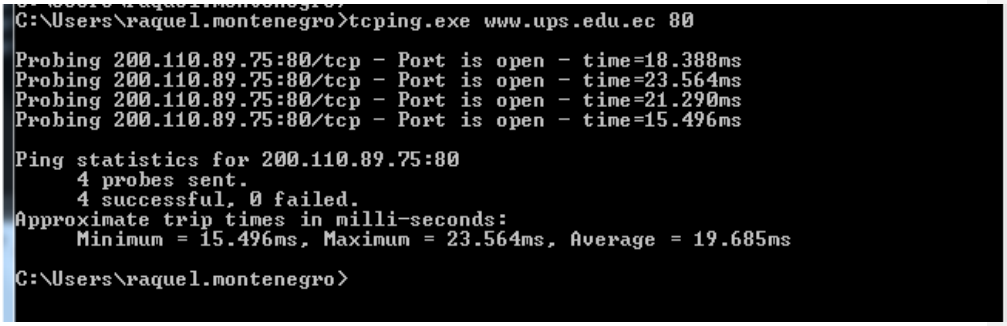

Figura 12 Ping TCP
Fuente: Autor

3.4.4.1 Estados de puertos

Para comprender mejor cómo funcionan los métodos de escaneo es importante conocer primero los posibles estados de un puerto.

Las definiciones de los estados abierto, filtrado y cerrado son comunes entre muchas herramientas de escaneo, pero dependiendo del aplicativo pueden usarse diferentes nombres para referirse a un mismo estado. Por lo consiguiente, se basará en las definiciones de estados de puertos de la herramienta de escaneo más popular: NMAP. (Astudillo, Hacking Etico 101, 2013)

- **Abierto:** Un puerto en este estado está disponible y escuchando por conexiones hacia el servicio asociado en dicho puerto.

Por ejemplo un webserver público podría tener abiertos los puertos TCP/80 (HTTP), TCP/443 (HTTPS), UDP/53 (DNS) y otros más. (Astudillo, Hacking Etico 101, 2013)

- **Cerrado:** Por el contrario un puerto cerrado aunque es accesible, no tiene una aplicación o servicio asociado que responda a solicitudes de conexión. (Astudillo, Hacking Etico 101, 2013)

- **Filtrado:** Un puerto filtrado no es posible de ser accesado porque existe un dispositivo filtrador de paquetes de por medio que impide al escáner determinar si dicho puerto está abierto o cerrado. El dispositivo intermedio puede ser un router con ACL's implementadas o bien un firewall. (Astudillo, Hacking Etico 101, 2013)

- **No-filtrado:** Un puerto en este estado es accesible pero no puede determinarse a ciencia cierta si está abierto o cerrado. Este estado es específico de una técnica de escaneo descrita más adelante en esta misma sección denominada escaneo ACK. (Astudillo, Hacking Etico 101, 2013)

- **Abierto | Filtrado:** Es un estado ambiguo en el cual el escáner no pudo determinar si el puerto se encuentra abierto o filtrado y es factible de obtenerse cuando se usa una

técnica de escaneo en la cual un puerto abierto puede no responder. (Astudillo, Hacking Etico 101, 2013)

- **Cerrado | Filtrado:** Se da cuando el escáner no puede concluir si el puerto está cerrado o filtrado. (Astudillo, Hacking Etico 101, 2013)

3.4.5 Nmap

NMAP es sin duda el escáner de puertos más popular entre los profesionales de redes y seguridad informática, en parte por su facilidad de uso, pero principalmente debido a su versatilidad para escanear.

Con NMAP se pueden aplicar las técnicas de escaneo descritas anteriormente y otras adicionales que pueden revisarse en la Guía de Referencia en el sitio web oficial del proyecto, http://www.nmap.org/.

Otra de las ventajas de este escáner es la posibilidad de ejecutarlo desde la línea de comandos además de la interfaz gráfica. De hecho inicialmente se desarrolló para Linux y se ejecutaba exclusivamente en un shell, pero posteriormente se agregó la interfaz gráfica Zenmap y se portó a la plataforma Windows. (Astudillo, Hacking Etico 101, 2013)

A continuación alguna de las opciones más utilizadas de NMAP:

Sintaxis: nmap [tipo(s)_de_escaneo] [opciones] {red|host_objetivo}

Opciones:

-sn : ping scan

-sS : syn/half scan

-sT : tcp/connect scan

-sA : ack scan

-sN : null scan

-sU : udp scan

-sF : fin scan

-sX : xmas scan

-sV: detección de versión de servicios

-O: detección de sistema operativo

-T<0-5>: temporizador, el valor más alto es más rápido

-v: salida detallada

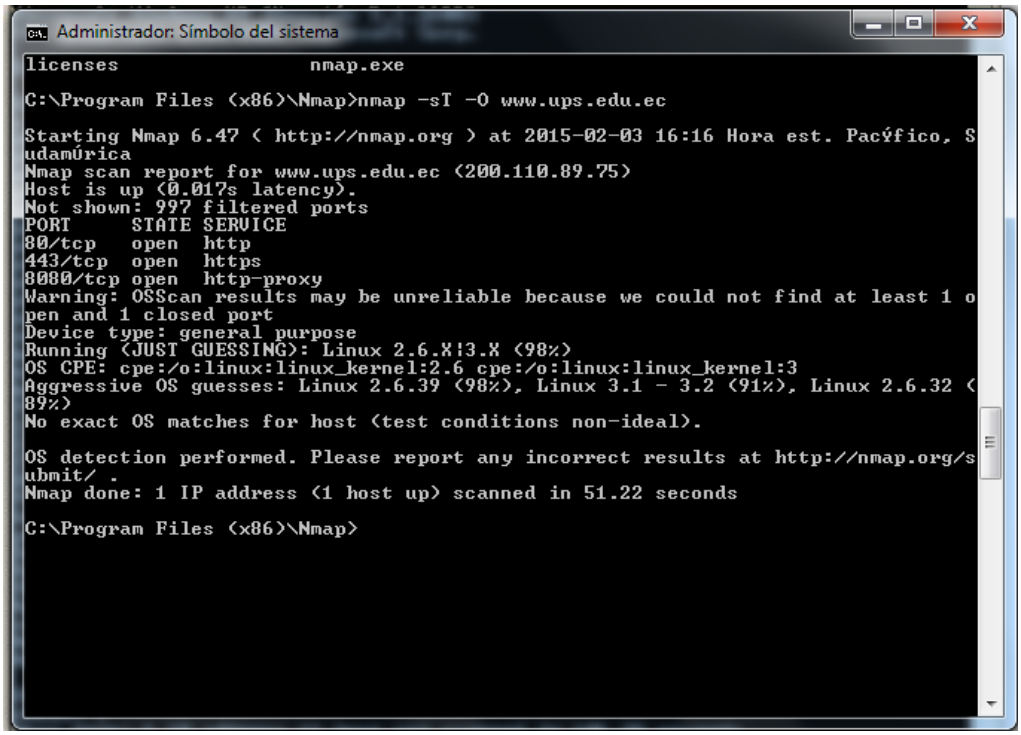

Figura 13 Nmap desde el cmd de Windows
Fuente: Autor

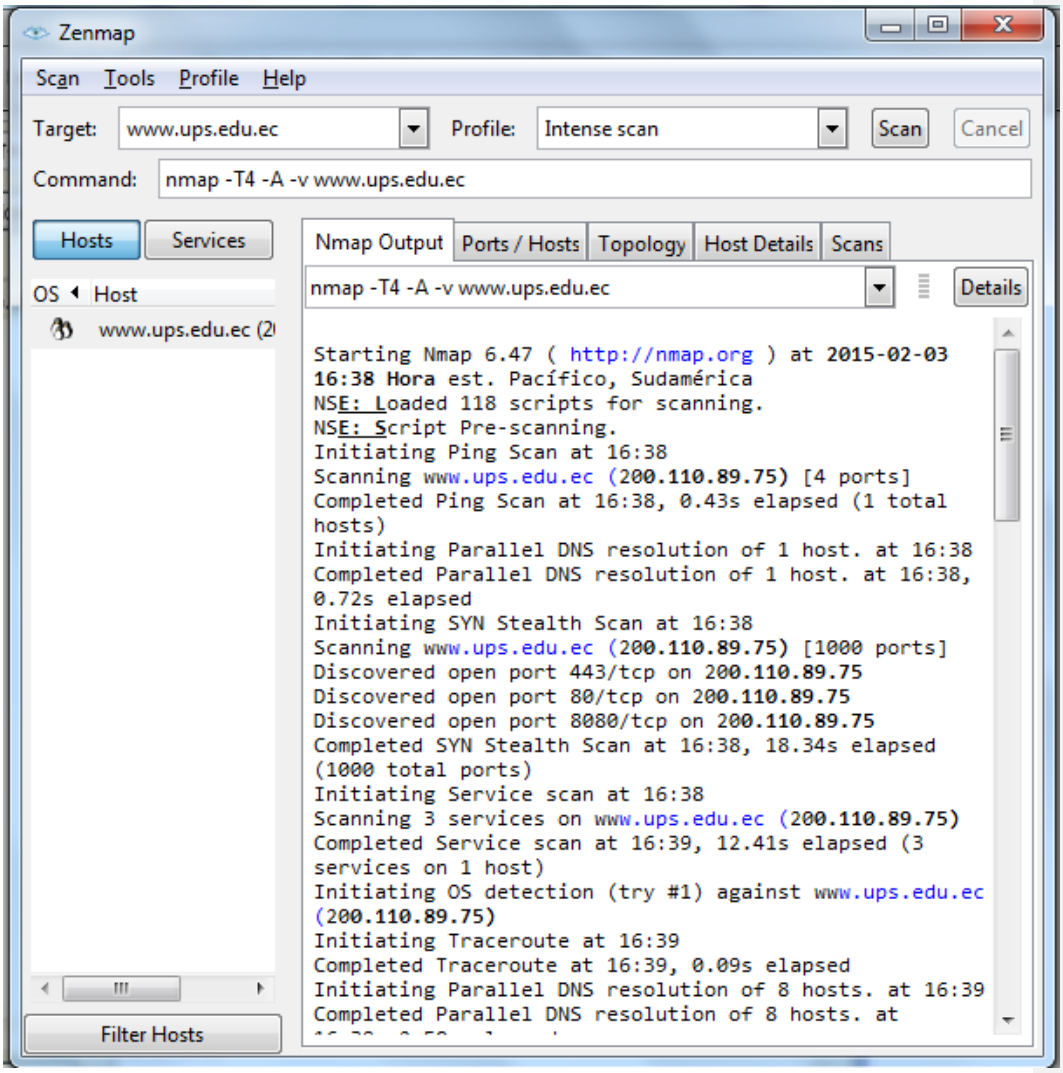

Figura 14 Interfaz gráfica Zenmap, escaneo intensivo a www.ups.edu.ec
Fuente: Autor

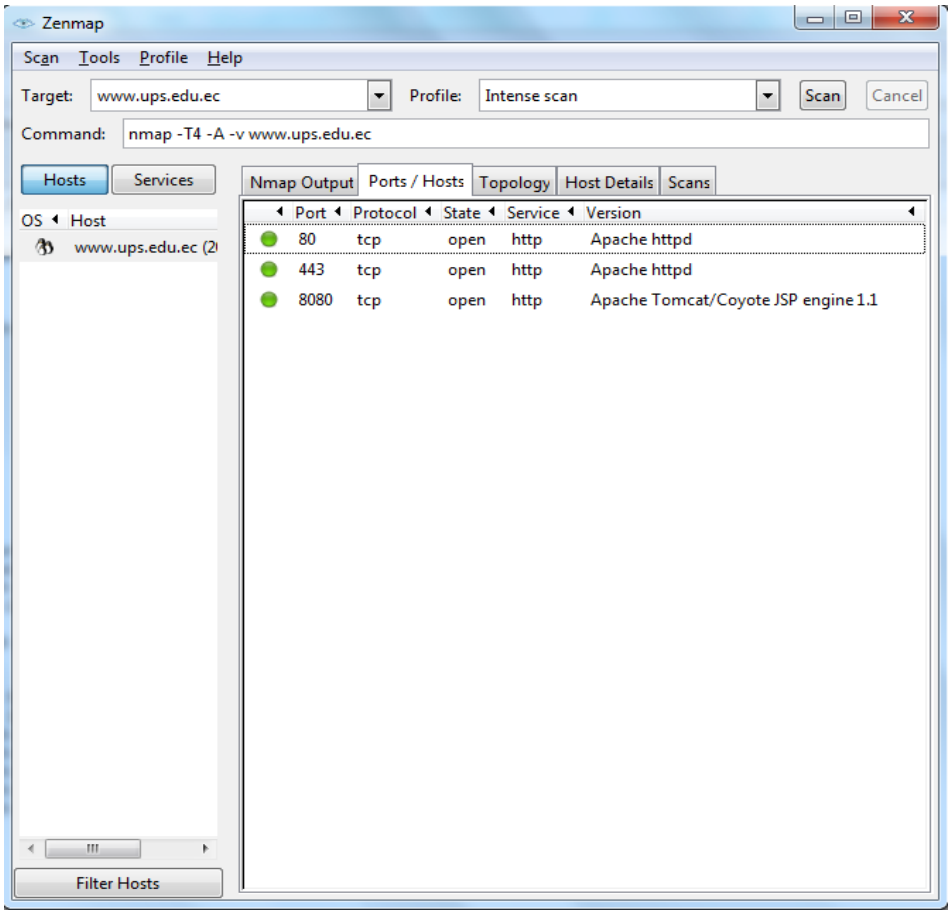

Figura 15 Puertos descubiertos y versiones de servicios en Zenmap
Fuente: Autor

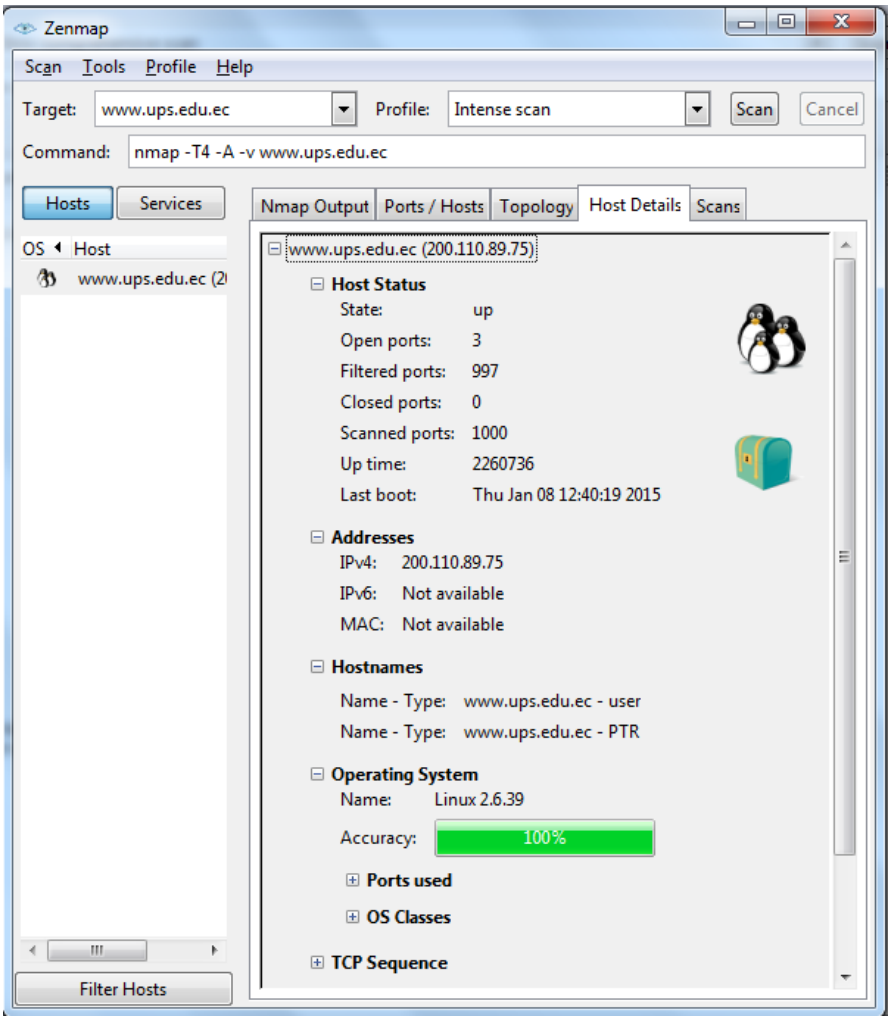

Figura 16 Detección de sistema operativo en Zenmap
Fuente: Autor

Como se puede observar en las figuras previas (Figuras 16 a 19), los resultados de los escaneos coinciden de 3 puertos descubiertos, debido a que se usaron técnicas distintas. Adicionalmente se detecta que la versión de sistema operativo detectada es Linux.

3.4.6 Casos de Delitos Informáticos En Guayaquil.

3.4.6.1 Caso Banco Guayaquil

Mediante mensajes de correo electrónico redirecciona a los usuarios a páginas falsas para el robo de información bancaria de los usuarios.

A través del uso de un Troyano el cual trabaja en segundo plano sin modificar el funcionamiento del computador.

Una vez que el usuario realiza la transacción, el virus toma copia de pantallas de cada movimiento y clic dado por el usuario. Así, se tiene un álbum completo con imágenes que permite ver la información del cliente.

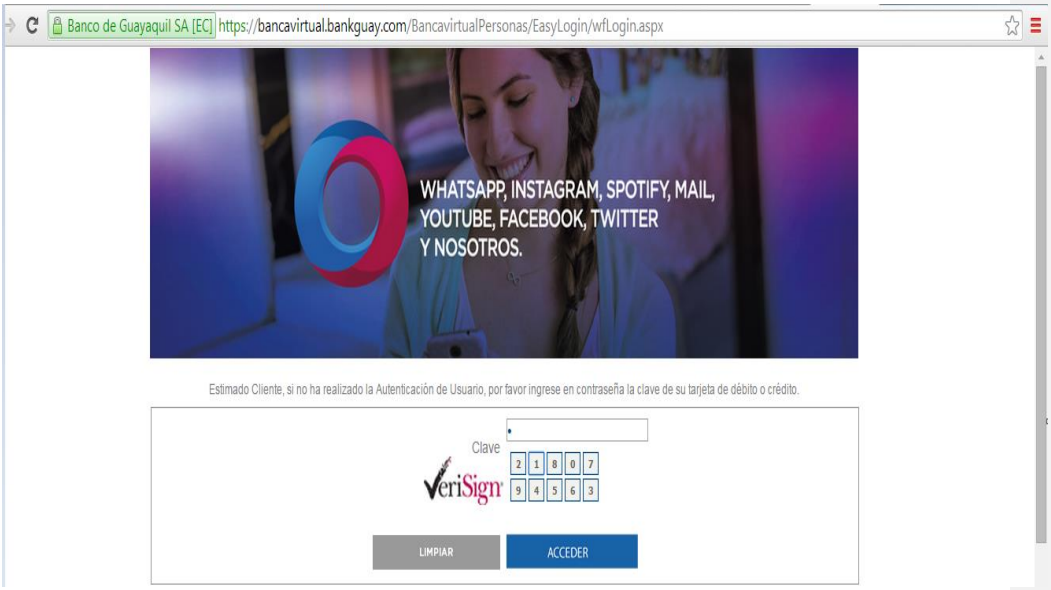

Figura 3.15 Pishing- Banco Guayaquil
Fuente: Autor

3.4.6.2 Caso Banco Pichincha

Como en el caso anterior a menudo llegan correos supuestamente de los portales bancarios en el que se esgrime un tema para pescar al cliente incauto. En este caso el supuesto "bloqueo de la cuenta". Por supuesto todo es falso con el objetivo de robar los datos bancarios de la víctima.

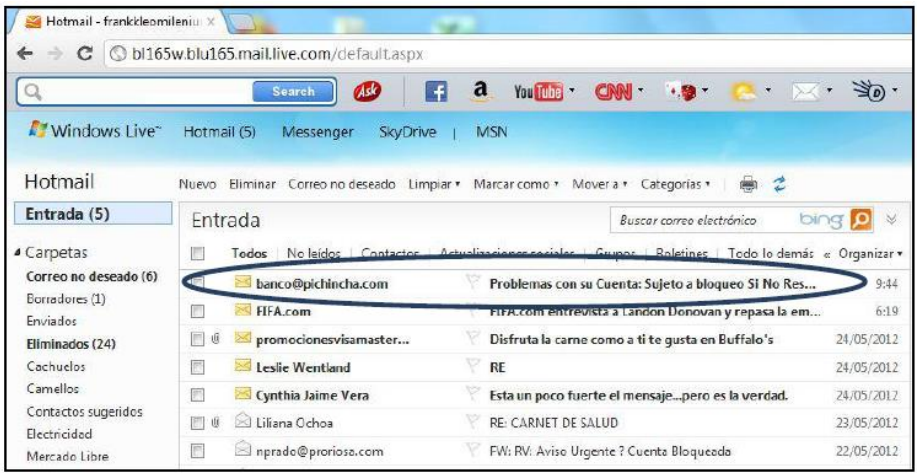

Figura 3.16 Pishing – Mensaje con su cuenta
Fuente: Autor

En el mensaje indican que se debe ingresar un link para supuestamente desbloquear la cuenta.

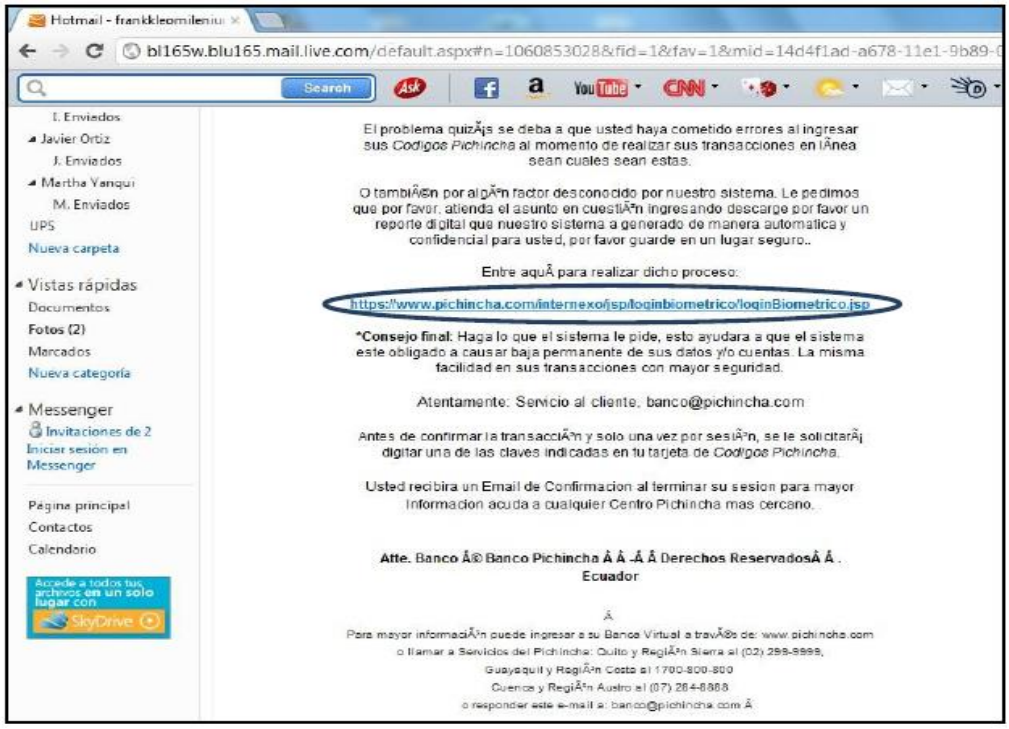

Figura 3.17 Enlace a página falsa
Fuente: Autor

Al visitar ese sitio falso aparece una réplica de la página original, el cual indica colocar los datos.

Figura 3.18 Pishing- Ingreso de datos
Fuente: Canal Tecnológico

Una vez ingresado los datos se muestra el mensaje que el sistema no está disponible por el momento.

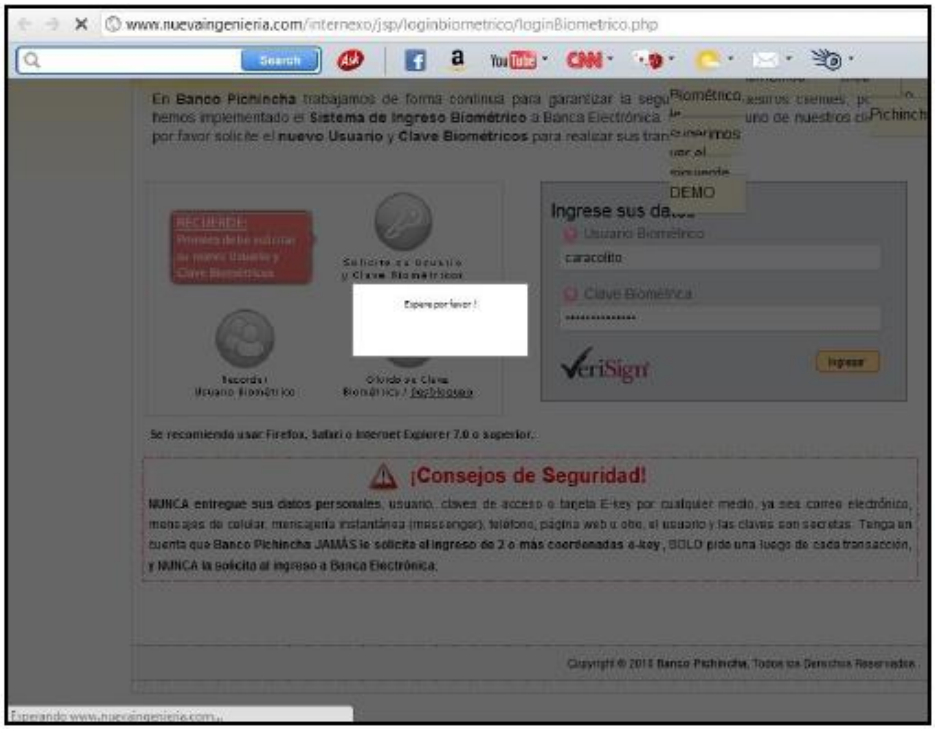

Figura 3.18 Captura de Información
Fuente: Autor

Figura 3.19 Mensaje de error
Fuente: Autor

CAPÍTULO 4

4.1 METODOS DE LA INVESTIGACION

De acuerdo a la investigación que se realizó y la propuesta que se quiere presentar, se va a utilizar el siguiente método de investigación:

- **Plan de Procesamiento y Análisis de Datos**

La información recolectada se procesará para llegar a la hipótesis planteada con la ayuda de las variables y los indicadores que aportarán en la investigación.

Se realizarán estadísticas generales de los tipos de delitos informáticos que arroje la investigación, así como también del estudio del software libre con características para ser utilizado en el peritaje informático.

4.2 ESTADÍSTICAS DE DELITOS INFORMÁTICOS

La Fiscalía del Guayas recibió 877 denuncias por delitos informáticos en el año 2014 entre los meses de Enero a Mayo.

Cada semana la Fiscalía del Guayas recepta entre seis y 10 denuncias sobre delitos informáticos, que consisten en la revelación ilegal de base de datos, su interceptación, la transferencia electrónica de dinero obtenido de forma ilegal (pishing), el ataque a la integridad de sistemas informáticos (skiming) y los accesos no consentidos a un sistema telemático o de telecomunicaciones.

La cifra más alta fue en el 2009 cuando se registraron 3129 casos, los delitos con mayor frecuencia son el Pishing y Skiming.

En el proyecto de Reformas al Código Penal Integral que se trata en la Asamblea Nacional, también se han incluido sanciones para los delitos informáticos que van de uno a siete años de privación de la libertad, dependiendo del delito.

Los delitos informáticos que constan son:

- La revelación ilegal de base de datos,
- Los daños informáticos,
- La obtención de información no autorizada,
- Modificación e inutilización de programas,
- Los delitos contra la información pública empleando diversos medios informáticos para su ilegal obtención, manipulación o distribución para fines ilícitos

Un estudio realizado por las empresas GMS y Kaspersky ubicó las pérdidas económicas por delitos informáticos en el Ecuador en un millón de dólares entre 2012 y 2013.

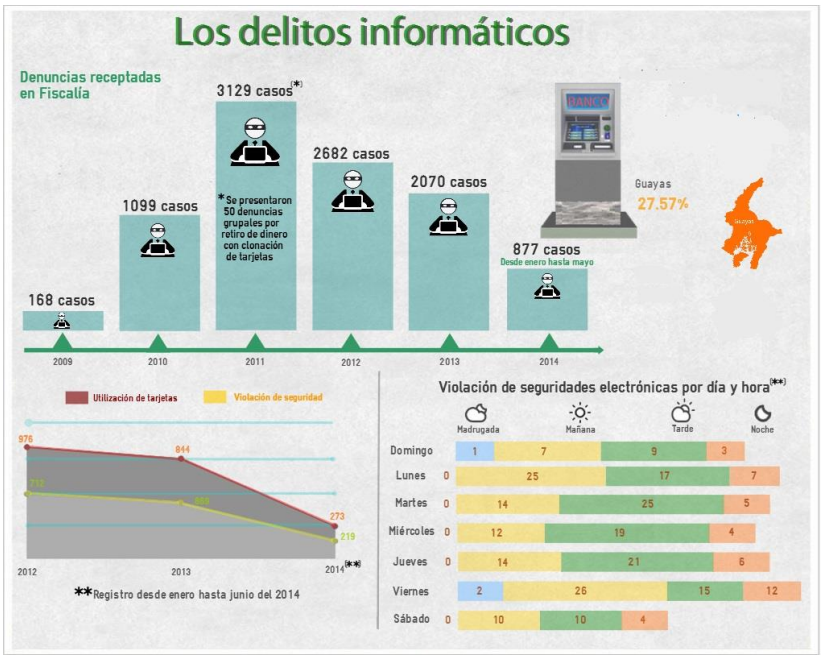

Figura 4.1 Estadística de Delitos Informáticos
Fuente: El Universo/Fiscalía del Guayas

4.3 PASOS PARA LA CREACION DE DOCUMENTO DE AUDITORIA INFORMATICA

1. Crear una carpeta para el proyecto
2. Llevar una bitácora
3. Capturar imágenes / video
4. Usar una plantilla para el informe

4.3.1 Crear una carpeta para el proyecto

Es un paso muy importante y quizás el más obvio, pero en los foros se lee que la mayoría de las personas no crean carpetas para el proyecto a auditar ni llevan un orden en su trabajo, es por eso que a continuación se detalla una sugerencia de cómo pueden llevar un orden en sus carpetas y evitar la pérdida de información.

1. Crear carpeta principal con el nombre del cliente que se va a auditar.
2. Crear subcarpetas para Hacking Externos y otra para el Hacking Interno.
3. Dentro de la carpeta de cada tipo de hacking, crear subcarpetas de bitácora, imágenes capturadas, reportes y datos obtenidos.
4. La subcarpeta de imágenes dividir en fases y herramientas.
5. La subcarpeta de reportes y datos dividirlas en fases y herramientas.
6. Finalmente en la carpeta principal colocar el documento del informe con los datos del cliente.

4.3.2 Llevar bitácora

Llevar una bitácora puede ser tan simple como editar un archivo de texto plano y listar las tareas que se han ejecutado día a día durante el hacking ético, o tan complejo como usar una suite para documentación de auditoría.

Independientemente de la opción que se elija lo importante de este paso es escribir las tareas ejecutadas todos los días, en el momento que se las realiza. De este modo no se olvidará nada importante en el cual se deba mencionar en el informe.

Es usual incluir dentro de la bitácora un resumen de los hallazgos encontrados durante el día, pero el detalle de los mismos debe llevarse aparte en un registro de hallazgos. (Astudillo, Hacking Etico 101, 2013)

Existen aplicaciones específicas para organizar documentos, muy útiles en una auditoría, como por ejemplo:

Linked Notes (http://www.linkednotes.com/)

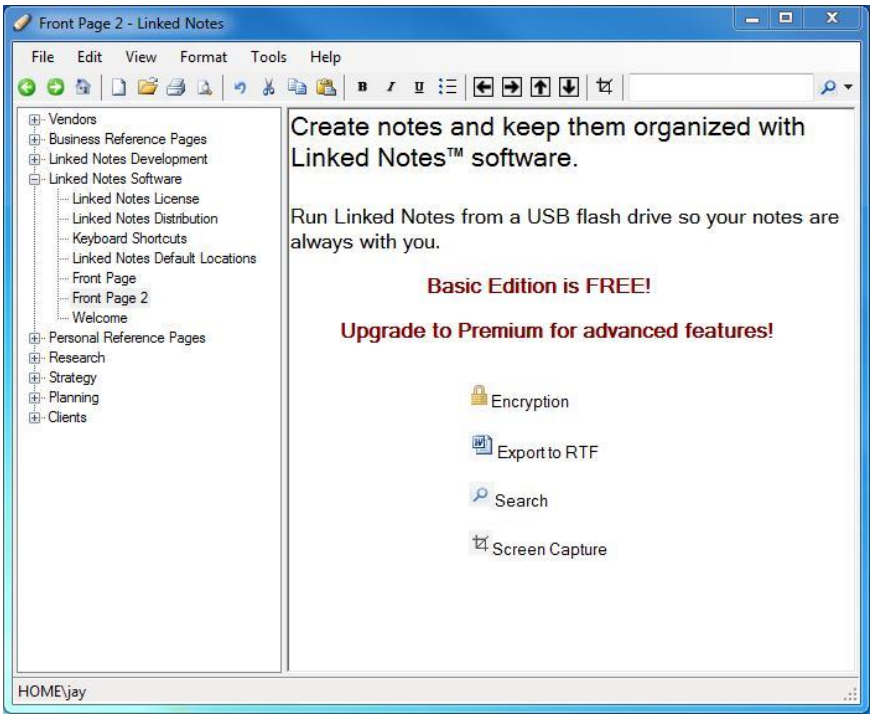

Figura 174.2 Linked Notes
Fuente: LinkedNotes Page

La ventaja de utilizar ésta aplicación versus llevar la bitácora en un archivo de texto simple, es que con ella es posible enlazar información relacionada como: imágenes, video, archivos anexos, etc. La estructura que genera ésta herramienta es tipo árbol, lo que hace más fácil la organización y en muchos casos, existe también la posibilidad de exportar a diferentes formatos útiles como por ejemplo HTML. (Astudillo, Hacking Etico 101, 2013)

4.3.3 Capturar imágenes/videos

El registro de imágenes y/o video durante una auditoría es vital para dejar constancia al cliente de lo actuado, además de servir al consultor como recordatorio de eventos

importantes como el hallazgo de una vulnerabilidad grave, el ingreso exitoso a un sistema o la captura de datos.

Si utilizan Linux como plataforma de hacking, este incluye una herramienta de captura de imágenes que se invoca fácilmente presionando el botón Printscreen del teclado; si usan Windows por otro lado, dependiendo de la versión, pueden pegar lo capturado en Paint o usar la herramienta de Recortes (Snipping Tool) que se incluye a partir de Vista y Windows 7.

Cualquiera sea el caso, lo importante en este punto es acostumbrarse a llevar un registro gráfico de lo que se hace y mantenerlo de forma organizada, asignando nombres que luego sean fáciles de asociar para poder incluirlos fácilmente en el informe, sin necesidad de visualizar previamente la imagen, ahorrando así tiempo valioso durante la fase de documentación. (Astudillo, Hacking Etico 101, 2013)

Para grabar videos hay diversas aplicaciones disponibles que son open source tanto para Windows como para Linux

Para Windows:

- Camstudio
- Camtasia Studio

Para Linux:

- Cinelerra
- Kino
- RecordMyDesktop

4.3.4 Usar plantilla de informe

El uso de plantillas ahorra tiempo al momento de armar el informe final y permite despreocuparse de elementos necesarios pero intrascendentes como la numeración de las secciones y los formatos, para concentrarse en lo realmente importante: transmitir de forma precisa pero comprensible los hallazgos, las conclusiones y las recomendaciones.

Se debe recordar que el informe va a ser leído no sólo por el personal de sistemas de la organización cliente, sino también por altos directivos, que no necesariamente manejan la jerga tecnológica. Es por lo tanto importante, que el documento tenga una estructura congruente y que incluya una sección de “resumen ejecutivo”.

1. Carátula
2. Tabla de contenido
3. Lista de ilustraciones y tablas
4. Antecedentes
5. Alcance de la auditoria
6. Metodología utilizada
7. Resumen ejecutivo
8. Bitácora de actividades
9. Conclusiones y recomendaciones
10. Anexos

4.4 CERTIFICACIONES DE SEGURIDAD RELEVANTES

En el mercado existen diferentes certificaciones internacionales sobre seguridad informática. A continuación se cita algunas certificaciones:

Tabla 4.1 Certificaciones de Seguridad Informática

Certificación	Organización
Certified Information System Security Professional (CISSP)	ISC^2
System Security Certified Practitioner (SSCP)	ISC^2
Certified Information Security Manager (CISM)	ISACA
Global Information Assurance Certification (GIAC)	GIAC
Information Security Security	Brainbench

Elaborado por: Raquel Montenegro

Tabla 4.2 Certificaciones de Seguridad de Redes

Certificación	Organización
Network Security+	CompTIA
Cisco Certified Network Associate (CCNA)	Cisco System
Cisco Certified Security Professional (CCSP)	Cisco System
Network Security	Brainbench

Elaborado por: Raquel Montenegro

Tabla 4.3 Certificaciones sobre Auditoria de Sistemas y Cómputo Forense

Certificación	Organización
Certified Information System Auditor (CISA)	ISACA
Certified Hacking Forensic Investigator (CHFI)	EC- Council
Certified Forensic Analyst (GCFA)	GIAC
Computer Forensics US	Brainbench

Elaborado por: Raquel Montenegro

CONCLUSIONES

En el Ecuador ya se ha manifestado una gran cantidad de delitos informáticos, en el que cual se detalla la tipificación de los delitos que constan en la Fiscalía General del Estado.

- La revelación ilegal de base de datos
- Los daños informáticos
- La obtención de información no autorizada, modificación e inutilización de programas
- Los delitos contra la información pública empleando diversos medios informáticos para su ilegal obtención, manipulación o distribución para fines ilícitos.

La propuesta de varios software libres y sus características que se menciona en capítulos anteriores sirven para el procedimiento de indagación y auditoria de delitos informáticos en Ecuador.

La metodología que se realiza de acuerdo a la investigación es el plan de procesamiento y análisis de datos el cual consiste en seguir una serie de fases para llegar al objetivo que es la entrega del informe final a la organización que se vaya a auditar.

La presencia de delitos informáticos no debe impedir que éstas se beneficien de todo lo que proveen las tecnologías de información, sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos a robustecer los aspectos de seguridad, controles, integridad de la información.

Se espera generar un aporte a la sociedad en materia de diferenciar los delitos informáticos del resto y de definir de una manera eficaz los procedimientos necesarios para la resolución a tiempo de los delitos informáticos.

RECOMENDACIONES

Para investigación y sanción de los delitos informáticos es preciso implementar y mejorar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte de los involucrados en la Administración de Justicia. Por lo que se recomienda lo siguiente:

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnología de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

El avance tecnológico y la necesidad de establecer procesos que permitan la indagación y resolución de delitos informáticos establece la importancia de contar con una nueva generación de profesionales que den respuesta a la creciente necesidad de la sociedad de contar con una buena administración de justicia, que sea capaz de brindar sustento y respaldo legal a cada uno de los procesos planteados para de una forma más rápida y segura indagar y resolver los delitos informáticos.

- Poner en práctica los procesos y software libres planteados para la indagación de los delitos informáticos.

- El perito informático puede obtener una Maestría de Seguridad Informática debido a que muchas organizaciones han comenzado a demandar especialistas con conocimientos del más alto nivel de Seguridad informática.

- Para las estadísticas de delitos informáticos no existe un ente el cual registre los diferentes tipos de delitos que ocurre en Guayaquil y en el Ecuador, lo cual fue complejo dar una estadística real de los casos que ocurren en la ciudad

- Los profesionales informáticos se mantengan a la vanguardia en tecnologías, técnicas y procedimientos.

Por otro lado es primordial propiciar la integración entre la justicia y los ciudadanos. Se necesita se eduque a la ciudadanía de los distintos tipos de delitos informáticos que existe, como la ley los protege y lo que necesitan hacer para realizar la denuncia respectiva, ya que para que inicie el proceso de indagación es primordial que las personas comuniquen inmediatamente cuando hayan sido blanco de delitos informáticos

BIBLIOGRAFÍA

Arreaga, L. L. (2009). *RETOS A SUPERAR EN LA ADMINISTRACIÓN DE JUSTICIA ANTE LOS DELITOS INFORMÁTICOS EN EL ECUADOR.* Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/5792/5/TESIS%20-%20DELITOS%20INFORMATICOS%20EN%20ECUADOR%20Y%20ADMINISTRACION%20DE%20JUSTICIA.pdf

Astudillo, K. (25 de 08 de 2012). *Análisis de correo caso Diario El Universo.* Obtenido de Análisis de correo caso Diario El Universo: http://www.elixircorp.biz/files/Analisis-Correo-Diario-El-Universo-Julian-Assange.pdf

Astudillo, K. (25 de 08 de 2012). *Elixircorp*. Obtenido de http://blog.elixircorp.biz/diseccion-de-un-correo-sobre-supuesto-ingreso-forzado-a-la-embajada-ecuatoriana-en-uk-para-sacar-a-julian-assange/

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

Audoria. (2011). Obtenido de http://es.slideshare.net/jonbonachon/conceptos-generales-auditora-y-evaluacin-de-sistemas

Baez, L. (2003). Obtenido de http://profesores.elo.utfsm.cl/~agv/elo330/2s03/projects/Tomcat/

Barrios, J. (18 de 03 de 2011). *Alcance libre*. Obtenido de www.alcancelibre.org/staticpages/index.php/ingenieria-social-malos-habitos-usuarios

Bedriñana, A. (2000). *LAS TECNOLOGÍAS WORKFLOW EN LA GESTIÓN EMPRESARIAL*. Obtenido de http://sisbib.unmsm.edu.pe/: http://sisbib.unmsm.edu.pe/bibvirtual/publicaciones/administracion/v03_n6/tecnologias.htm

blog.cjavaperu.com. (2013). *http://blog.cjavaperu.com/*. Obtenido de http://blog.cjavaperu.com/wp-content/uploads/2013/04/Aplicaciones-Web-con-ZK-Framework.pdf

Cáceres, J. (2012). Obtenido de http://www2.uah.es/jcaceres/capsulas/DiagramaCasosDeUso.pdf

Campos, J. S. (13 de 09 de 2010). *Tipificación de los delitos informáticos*. Obtenido de Tipificación de los delitos informáticos: www.emagister.com

CARRION, H. D. (Julio de 2011). *http://www.segu-info.com.ar*. Obtenido de http://www.segu-info.com.ar/delitos/tiposdelito.htm

Compañías, S. d. (2012). *Superintendencia de Compañías*. Obtenido de http://www.supercias.gob.ec/portal/

Congreso de las Naciones Unidas. (25 de Abril de 2005). Obtenido de http://www.unis.unvienna.org/pdf/05-82113_S_6_pr_SFS.pdf

ConsumidorGov. (2010). Obtenido de https://www.consumidor.gov/articulos/s1015-evitar-el-robo-de-identidad

Datateca. (2004). Obtenido de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_27_fases_de_la_auditora_informtica_y_de_sistemas.html

Debian. (2010). Obtenido de https://www.debian.org/releases/stable/i386/ch01s02.html.es

Definicion. (2008). Obtenido de http://definicion.de/html/

desarrolloweb.com. (2012). *desarrolloweb.com*. Obtenido de http://www.desarrolloweb.com/wiki/mvc-modelo-vista-controlador.html

Díaz, M. (2013). Obtenido de http://www.usmp.edu.pe/publicaciones/boletin/fia/info49/articulos/RUP%20vs.%20XP.pdf

Dlerus. (2009). Obtenido de http://www.clerus.org/clerus/dati/2009-12/14-999999/software_libre.html

EcuRed. (2011). *EcuRed*. Obtenido de http://www.ecured.cu/index.php/Eclipse,_entorno_de_desarrollo_integrado

El Universo. (26 de Agosto de 2012). Obtenido de http://www.eluniverso.com/2012/08/26/1/1422/un-promedio-siete-delitos-informaticos-registran-dia.html

ESPOL. (s.f.). *http://www.icm.espol.edu.ec*. Obtenido de http://www.icm.espol.edu.ec/delitos/

Estadísticas, C. d. (Febrero de 2014). *PRINCIPALES DELITOS CONTRA LAS PERSONAS Y CONTRA LA PROPIEDAD.* Obtenido de http://www.icm.espol.edu.ec/delitos/Archivos/reporte%20anual/Informe_ANUAL%202013.pdf

FMBR. (s.f.). Obtenido de 2011: http://ccia.ei.uvigo.es/docencia/SCS/1112/transparencias/Tema5-1.pdf

García Perez, A. (2010). *www.adictosaltrabajo.com*. Obtenido de http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=eclipseHelios

Guerrero, J. M. (2005). *http://seguridad.internautas.org*. Obtenido de http://seguridad.internautas.org/html/451.html

HERRAMIENTAS Y EQUIPOS PARA EL ANÁLISIS FORENSE. (s.f.). Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/546/6/CAPITULO5.pdf

HerramientasInformaticas. (s.f.). Obtenido de http://www.ordenadores-y-portatiles.com/herramientas-informatica-forense.html

Hispasec. (03 de 02 de 2011). Obtenido de www.unaaldia.hispasec.com/2011/02/video-kit-de-creacion-de-phishing.html

http://www.dosideas.com/. (2009). Obtenido de http://www.dosideas.com/noticias/java/718-framework-zkoss-ya-en-espanol.html

http://www.eldia.com.ar. (14 de Septiembre de 2012). Obtenido de Delitos informáticos: crece el robo de identidad por Internet : http://www.eldia.com.ar/edis/20120914/delitos-informaticos-crece-robo-identidad-internet-informaciongeneral3.htm

http://www.javatutoriales.com. (2010). Obtenido de http://www.javatutoriales.com/2010/09/spring-parte-1-introduccion.html

http://www.nuestraseguridad.gob.ec. (13 de Mayo de 2014). Obtenido de http://www.nuestraseguridad.gob.ec/es/articulo/ciberseguridad-escenarios-y-recomendaciones

http://www.ordenadores-y-portatiles.com. (s.f.). Obtenido de http://www.ordenadores-y-portatiles.com/herramientas-informatica-forense.html

IMBAQUINGO, D. H. (2011). Obtenido de LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE IMBABURA: http://repositorio.utn.edu.ec/bitstream/123456789/1175/1/PG%20235-TESISHUGOIMBAQUINGO.SEP9.pdf

Informática Forense. (s.f.). Obtenido de http://www.dspace.ups.edu.ec/bitstream/123456789/546/5/CAPITULO4.pdf

Informatica juridica. (16 de 04 de 2010). Obtenido de http://informaticajuridicauapgrupo.blogspot.com/

Lima, M. d. (2013). *criminalistica*. Obtenido de criminalistica: http://www.criminalistica.com.mx/areas-forenses/seguridad-publica/548-delitos-informcos

Marco, D. (2011). Obtenido de http://www.davidmarco.es/articulo/introduccion-a-ejb-3-1-i

Masip, D. (2002). Obtenido de http://www.desarrolloweb.com/articulos/840.php

Microsoft. (10 de Junio de 2011). Obtenido de http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=123

Microsoft. (2012). Obtenido de http://www.microsoft.com/es-xl/security/pc-security/virus-whatis.aspx

Microsoftbusiness. (2010). Obtenido de http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=121

Mundo Contact. (18 de 05 de 2010). Obtenido de www.mundocontact.com

orales.wordpress.com. (2009). Obtenido de http://orales.wordpress.com/2009/07/21/hablemos-un-poco-de-oracle-database-10g/

Perrin, S. (27 de fEBRERO de 2006). *vecam.or*. Obtenido de http://vecam.org/article659.html

Pesquera, C. (2014). Obtenido de http://carlospesquera.com/que-es-un-pojo-ejb-y-un-bean/

Pino, D. S. (s.f.). *Delitos Informáticos: Generalidades.* Obtenido de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Ramírez, J. (25 de Marzo de 2013). *BPM y Workflow para la gestión de procesos*. Obtenido de http://www.r2sistemas.com: http://www.r2sistemas.com/noticias/2013/03/25/workflow-bpm/

Real Academia Española. (2015). Obtenido de http://lema.rae.es/drae

RoboyFraude. (2012). Obtenido de http://roboyfraude-informatico.blogspot.com/

rupmetodologia.blogspot.com. (2012). Obtenido de http://rupmetodologia.blogspot.com/2012/06/principios-de-desarrollo-de-la.html

Security. (s.f.). Obtenido de http://www.pandasecurity.com/ecuador/homeusers/security-info/classic-malware/virus/

Segu-info. (Noviembre de 2007). Obtenido de http://blog.segu-info.com.ar/2007/11/qu-es-el-skimming.html

Seguridad web. (2010). Obtenido de http://jzseguridadweb.blogspot.com/p/fases-de-un-ataque-informatico.html

Todoecommerce. (2011). Obtenido de http://www.todoecommerce.com/ataques-informaticos.html

U. Alicante, S. (2011). Obtenido de http://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html

Universo, D. E. (26 de Agosto de 2012). *http://www.radioviva.com.ec*. Obtenido de http://www.radioviva.com.ec/web/?p=6421

Villamarín, A. (2013). Obtenido de http://ant.onio.org/2013/04/10/modelo-vista-controlador-adaptado-a-la-web.html

VISUALROUTE. (2012). Obtenido de VISUALROUTE: http://www.visualroute.it/

www.aiteco.com. (2011). Obtenido de www.aiteco.com: http://www.aiteco.com/que-es-un-diagrama-de-flujo/#_ftnref1

www.alegsa.com.ar. (2011). Obtenido de http://www.alegsa.com.ar/Dic/framework.php

www.alegsa.com.ar. (2011). *www.alegsa.com.ar.* Obtenido de http://www.alegsa.com.ar/Dic/back-end.php

www.alegsa.com.ar. (2011). *www.alegsa.com.ar*. Obtenido de http://www.alegsa.com.ar/Dic/metadato.php

www.dosideas.com. (17 de Sept. de 2009). *Framework ZK ya en español*. Obtenido de Dos Ideas: http://www.dosideas.com/noticias/java/718-framework-zkoss-ya-en-espanol.html

www.ecured.cu. (s.f.). *EcuRed*. Obtenido de EcuRed: http://www.ecured.cu/index.php/Eclipse,_entorno_de_desarrollo_integrado

www.internetglosario.com. (2013). Obtenido de http://www.internetglosario.com/letra-e.html

www.tiposdeinvestigacion.com. (2013). *http://www.tiposdeinvestigacion.com/*. Obtenido de http://www.tiposdeinvestigacion.com/

Zambrano, R. (2012). *DELITOS INFORMÁTICOS CONTEMPLADOS EN LA LEY ECUATORIANA*. Obtenido de /www.cec.espol.edu.ec: http://www.cec.espol.edu.ec/blog/rzambrano/files/2012/08/DELITOS-INFORM%C3%81TICOS-CONTEMPLADOS-EN-LA-LEY-ECUATORIANA.pdf

ANEXOS

Anexo 1 Reporte Visual IP Trace

Este anexo se aplica para indicar la ip, ubicación, dns y network del dominio www.ups.edu.ec

IP	LOCATION	DNS	NETWORK WHOIS	DOMAIN WHOIS
200.110.89.75	Guayaquil-Guayas-Ecuador	www.ups.edu.ec	% Joint Whois - whois.lacnic.net % This server accepts single ASN, IPv4 or IPv6 queries % LACNIC resource: whois.lacnic.net % Copyright LACNIC lacnic.net % The data below is provided for information purposes % and to assist persons in obtaining information about or % related to AS and IP numbers registrations % By submitting a whois	

			query, you agree to use this data % only for lawful purposes. % 2015-02-02 12:20:50 (BRST -02:00) inetnum: 200.110.80/20 status: allocated aut-num: N/A owner: Telconet S.A ownerid: EC-TESA-LACNIC responsible: TELCONET S. A. address: Kennedy Norte MZ, 109, address: 59342 - Guayaquil - country: EC phone: +593 4 2680555 [101] owner-c: SEL tech-c: SEL abuse-c: SEL inetrev: 200.110.88/22 nserver: SRV1.TELCONET.NET nsstat: 20150131 AA	

			nslastaa: 20150131 nserver: SRV2.TELCONET.NET nsstat: 20150131 AA nslastaa: 20150131 created: 20041021 changed: 20041021 nic-hdl: SEL person: Tomislav Topic e-mail: hostmaster@TELCONET.NET address: Kennedy Norte MZ, 109, Solar 21 address: 59342 - Guayaquil - country: EC phone: +593 4 2680555 [101] created: 20021004 changed: 20100921 % whois.lacnic.net accepts only direct match queries. % Types of queries are: POCs, ownerid, CIDR blocks, IP % and AS numbers	

			% LACNIC resource: whois.lacnic.net % Copyright LACNIC lacnic.net % The data below is provided for information purposes % and to assist persons in obtaining information about or % related to AS and IP numbers registrations % By submitting a whois query, you agree to use this data % only for lawful purposes. % 2015-02-02 12:20:50 (BRST -02:00) inetnum: 200.110.80/20 status: allocated aut-num: N/A owner: Telconet S.A ownerid: EC-TESA-LACNIC responsible: TELCONET S. A. address: Kennedy Norte MZ,	

			109, address: 59342 - Guayaquil - country: EC phone: +593 4 2680555 [101] owner-c: SEL tech-c: SEL abuse-c: SEL inetrev: 200.110.88/22 nserver: SRV1.TELCONET.NET nsstat: 20150131 AA nslastaa: 20150131 nserver: SRV2.TELCONET.NET nsstat: 20150131 AA nslastaa: 20150131 created: 20041021 changed: 20041021 nic-hdl: SEL person: Tomislav Topic e-mail: hostmaster@TELCONET.NET address: Kennedy Norte MZ, 109, Solar 21	

			address: 59342 - Guayaquil - country: EC phone: +593 4 2680555 [101] created: 20021004 changed: 20100921 % whois.lacnic.net accepts only direct match queries. % Types of queries are: POCs, ownerid, CIDR blocks, IP % and AS numbers	

Anexo 2 Reporte Visual Route

Hops	Loss	IP	Name	Location	Tzone	Avg ms	Min ms	Max ms	Network
0	0	192.168.19.1	RAQUEL-PC.cse-cph.int	-	-	0.0	0	0	[Local Network]
1	0	192.168.1.1	-	-	-	9.0	1	31	[Local Network]
2	0	181.198.255.97	host-181-198-255-97.telconet.net	(Ecuador)	-	9.0	6	13	Clientes NETLIFE Guayaquil - gepon
3	0	10.201.144.57	-	-	-	7.0	3	10	[Local Network]
4	0	10.201.144.1	-	-	-	2.0	2	3	[Local Network]
5	0	10.201.111.110	-	-	-	10.0	8	12	[Local Network]
6	0	190.95.243.121	host-190-95-243-121.cue.telconet.net	(Ecuador)	-	7.0	7	8	Clientes Cuenca
7	0	190.95.243.124	host-190-95-243-124.cue.telconet.net	(Ecuador)	-	8.0	7	10	Clientes Cuenca