UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CARRERA DE SISTEMAS INFORMATICOS

“INVESTIGACIÓN Y ELABORACIÓN DE UN INSTRUCTIVO SOBRE LAS HERRAMIENTAS HACKER MÁS UTILIZADAS EN EL ÁMBITO INFORMÁTICO”

Estudiante
Diana Lucia Méndez Ávila

Tutor
Ing. Diego Fajardo.

Cuenca – Ecuador
Noviembre 2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

DECLARACIÓN DE AUTORÍA

El documento de tesis con título “Investigación y elaboración de un instructivo sobre las herramientas hacker más utilizadas en el ámbito informático” ha sido desarrollado por Diana Lucia Méndez Ávila con C.C. No. 010475195-3 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Tnlgo. Diana Lucia Méndez Ávila

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICACIÓN DE AUTORÍA

Que el presente trabajo de investigación "Investigación y elaboración de un instructivo sobre las herramientas hacker más utilizadas en el ámbito informático", realizado por la Srta. Diana Lucia Méndez Ávila con C.C. No. 010475195-3, egresado de la Facultad de Ingeniería de Sistemas, se ajusta a los requerimientos técnico metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 30 de noviembre del 2011.

_____

Ing. Diego Fajardo.

DIRECTOR DE TESIS

AGRADECIMIENTO

A la Universidad Tecnológica Israel por permitirme realizar esta tesis previa a la obtención del título de Ingeniería de Sistemas Informáticos.

A los señores profesores que han contribuido en el proceso educativo forjando un futuro mejor.

A mi familia por brindarme todo el apoyo necesario para llegar a esta etapa de mi vida.

DEDICATORIA

Al cumplir un reto más en mi vida estudiantil dedico esta tesis como recuerdo de mi agradecimiento a toda mi familia, en especial a mi padre y hermanas que con mucho entusiasmo y sacrificio me han ayudado moral y económicamente para salir adelante en mi vida.

Tabla de Contenido

Lista de Figuras

RESUMEN

La seguridad informática enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos medios de ataques y de nuevas modalidades delictivas.

Cada día se descubren nuevos puntos débiles, Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos.

Pero para lograr atenuar de manera eficaz el impacto provocado por los ataques informáticos, es de esencial importancia conocer de qué manera atacan y cuáles son los puntos débiles de un sistema comúnmente explotado en los que se deben enfocar los esfuerzos de seguridad.

Por lo tanto, el presente trabajo de tesis pretende ofrecer un instructivo de las herramientas hacker más utilizadas en el ámbito informático.

Palabras Claves: herramientas hacker, seguridad informática

SUMARY

The computer science security focuses in the protection of the computer infrastructure and all that with this. For it a series of standards exists, protocols, methods, conceived rules, tools and laws to diminish the possible risks to the infrastructure or the information.

The computer science security includes software, data bases, metadata, archives and everything what the organization values and means a risk if this one arrives at the hands of other people. This type of information is known like privileged or confidential information.

Throughout the time, the advance of technological means and communication has brought about the sprouting of new means of attacks and new criminal modalities.

Every day new weak points are discovered, under this stage scene where the main actors are the organizations of any magnitude and heading, the information systems, the computer science money and delinquents; one becomes really necessary and fundamental to devise security strategies that allow establishing defensive barriers oriented to mitigate external attacks indeed as much internal.

But to manage to attenuate of effective way the impact brought about by the computer science attacks, it is of essential importance of knowing how they attack and which are the weak points of a system commonly operated in which is due to focus the security efforts.

Therefore, the present thesis work tries to offer an instructive one of the tools to hacker more used in the computer science scope.

Key words: tools to hacker, computer science security.

CAPITULO I.

1. INTRODUCCIÓN

Este tema de tesina está enfocado al área de la seguridad informática, específicamente a las herramientas hacker más utilizadas en el ámbito informático.

En primer lugar abordaremos la seguridad informática y los hacker en la cual se habla sobre el concepto, objetivo, amenazas y vulnerabilidades de la seguridad informática, al igual que las técnicas de seguridad y etapas de un ataque informático.

Luego se realizará la clasificación y caracterización las herramientas hacker de forma holística en donde trataremos el concepto, métodos y utilidades de las herramientas hacker, para realizar un análisis mediante la aplicación de una matriz de comparación y así determinar las herramientas hacker más utilizadas en el ámbito informático.

Mediante esta investigación se podrá obtener toda la información necesaria para encontrar las herramientas hacker más utilizadas en el ámbito informático, a través de medios comparativos que facilitara la identificación de dichas herramientas.

Con la aplicación de las técnicas de investigación adecuadas se realizara la comparación utilizando criterios para determinar las herramientas sobresalientes y así establecer las características de cada una de ellas.

Con la realización de esta tesina se pretende desarrollar un manual sobre las herramientas hacker más utilizadas en el ámbito informático debido a que el problema radica en la gran existencia de herramientas hacker y por lo tanto provocando vulnerabilidad en la seguridad informática.

1.1. Planteamiento del Problema

1.1.1. Antecedentes

Como en todos los ámbitos de la vida, cualquiera de las creaciones o de los avances de la humanidad siempre se termina empleando para fines negativos, el mundo de la informática y como no, el de las redes (Internet, por ejemplo), ha caído en este tipo de aplicaciones, todos sabíamos que era tan sólo una cuestión de tiempo. Ahora, se nos habla de los hackers, “la guerrilla electrónica”, de gente que defrauda y chantajea con información digital de

empresas multinacionales, de virus, de complots del gobierno, de chicos que violan nuestra intimidad y roban nuestro dinero con un ordenador… y a todo esto se le ha llamado “la cyber guerra”. Pero la sociedad ha creado sus propios mitos, sus monstruos y también miedos, en un terreno del que nos llega poca información, y muchas veces manipulada.

Se puede fechar que el inicio de este fenómeno ocurrió en 1961, y debido al progresivo avance tecnológico y contantes ataque a redes que causan los Hackers en el ámbito informático; hoy en día ha surgido la necesidad de implementar sistemas de protección más seguros, especialmente en el ámbito gubernamental, financiero etc.

1.2. Sistematización

1.2.1. Diagnóstico

1.2.1.1. Causa- Efecto

a) Causas

El problema que se presenta es la vulnerabilidad en los sistemas informáticos, y a través del diagrama causa y Efecto (o Espina de Pescado) que es una técnica gráfica ampliamente utilizada, que permite apreciar con claridad las relaciones entre un tema o problema y las posibles causas que puedan estar contribuyendo para que él ocurra.

b) Efectos

En las causas se puede visualizar a la tecnología que avanza cada día, la variedad de programas hacker, el uso incorrecto, la existencia de hacker, otra causa son los trabajadores ya que tienen un conocimiento bajo sobre herramientas hacker, presentan defectos en los planes de contingencia.

En los efectos se toman decisiones equivocadas por lo que se baja la seguridad informática, produciéndose así vulnerabilidad en las redes, ataques hacker, violación a la información privada.

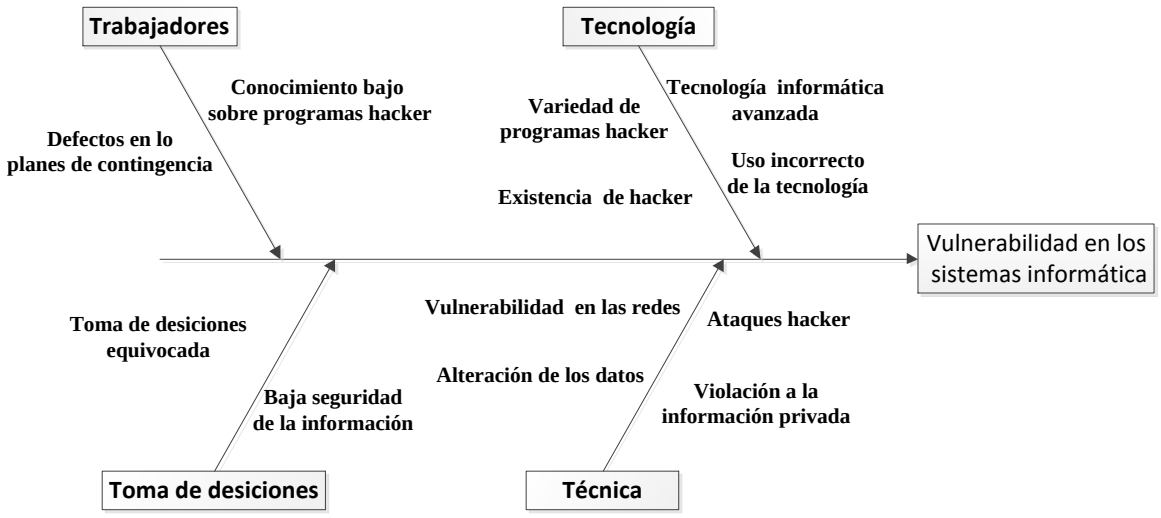


FIGURA 1Espina de pescado

1.2.1.2. Pronóstico

El desconocimiento de herramientas hacker más utilizadas en el ámbito aumenta la vulnerabilidad y peligro de ataques a las redes por parte de personas sin escrúpulos que utilizando medios informáticos, afectan de forma grave las redes.

1.2.1.3. Control de Pronóstico

Se pretende entregar a la sociedad los resultados de la Investigación sobre herramientas hacker dando a conocer los posibles s ataques que pueden sufrir las redes de cualquier tipo, incitando a los encargados de las redes tener más seguridad sobre ellos.

Los resultados de esta investigación se reflejarán en una explicación sobre las herramientas hacker que pueden ser utilizadas para filtrarse en las redes.

1.3. Objetivos

1.3.1. Objetivo General

Elaborar un instructivo informativo sobre las herramientas hacker más utilizadas en el ámbito informático.

1.3.2. Objetivos Específicos

- Investigar sobre las herramientas hacker más utilizadas en el ámbito informático.
- Definir qué herramientas son las más usadas.
- Diseñar un instructivo sobre las herramientas hacker.

1.4. Justificación

1.4.1. Justificación Teórica

Las amenazas de seguridad que enfrentan las redes de datos son suficientes para pensar en las posibles soluciones que disponen en la actualidad para enfrentar dichas amenazas.

Estas infracciones realizadas con la utilización de programas hacker pueden ser detenidas siempre y cuando las organizaciones conozcan la descripción de dichos programas y definan e implementen de una manera clara sus opciones en seguridad perimetral, esto en concordancia con las políticas de seguridad previamente establecidas.

En un alto porcentaje las organizaciones, carecen de conocimientos en el tema de herramientas hacker por tal razón permanentemente están expuestas tanto amenazas internas originadas desde el interior de la organización por medio de

sus empleados, como a amenazas externas originadas por fuera de la organización, esto último se presenta especialmente cuando una organización se interconecta con otras organizaciones o con la Internet.

El proyecto propuesto busca, mediante la investigación de herramientas hacker; dar a conocer de manera holística a las organizaciones la descripción de cada una de las herramientas, para que así puedan prevenir ataques.

1.4.2. Justificación Práctica

De acuerdo con los objetivos de investigación el proyecto de tesis será un instructivo que informara sobre los herramientas hacker más utilizadas en el ámbito informativo, para que las organizaciones se puedan proveer de métodos de protección a posibles ataques a la red.

Este instructivo será una base para que las organizaciones que deseen tener un conocimiento básico sobre la existencia de dichos herramientas que atentan a la integridad de seguridad de las redes.

1.4.3. Justificación Metodológica

Para lograr el cumplimiento de objetivos de estudio se utilizara los métodos:

Descriptivo, que se utiliza para recoger, organizar, resumir, presentar los resultados de la investigación; este método implica la recopilación y presentación sistemática de datos para dar una idea clara de una determinada situación. Las ventajas que tiene este estudio es que: la metodología es fácil, de corto tiempo y económica.

Analítico, consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, comprender mejor su comportamiento.

El resultado de esta investigación servirá para dar a conocer las herramientas hacker más utilizadas en el ámbito informático a todas aquellas organizaciones que deseen informarse sobre los tipos de ataques que pueden sufrir sus redes.

1.5. Alcance y Limitaciones

1.5.1. Alcance

Dentro de este proyecto se contemplara una investigación sobre los programas hacker existentes en el ámbito informático, además se elaborara un instructivo sobre la descripción de dichos programas, que ayudara a las organizaciones a tener un conocimiento global sobre el tema.

1.5.2. Limitaciones

El instructivo se elaborara solo de las herramientas identificadas como, las más utilizadas en el ámbito informático.

1.6. Estudio de Factibilidad

1.6.1. Factibilidad Económica

Análisis costo / beneficio

El análisis costo/beneficio del proyecto está realizado para el primer año, luego de haber aplicado la propuesta, obteniendo la estimación de los siguientes resultados:

COSTO	Precio	BENEFICIO	Precio
Internet	50,00	Venta el instructivo	**200**
Papel	15,00		
Copias	5,00		
Cartuchos	15,00		
Transporte	50,00		
Costo total =	**135,00**	**Beneficio total =**	**200,00**

A.C.B. =	**BENEFICIOS / COSTOS**	200,00 / 135,00	=1,48

FIGURA 2Tabla de análisis costo- beneficio

Los cálculos demuestran un beneficio substancial para el primer año, con una relación de beneficios a costos de $1,48 de retorno por cada dólar gastado. Lo que representa un retorno positivo; por lo tanto, en base a los resultados obtenidos, se puede deducir que este proyecto es económicamente realizable.

CAPITULO II.

2. MARCO DE REFERENCIA

2.1. Marco Teórico

2.1.1. Ataques Informáticos

"Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización." (Jorge Mieres (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas).Recuperado de https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

2.1.2. Códigos maliciosos

"Los códigos maliciosos, o malware, constituyen también una de las principales amenazas de seguridad para cualquier Institución u Organizaciones y aunque parezca un tema trivial, suele ser motivo de importantes pérdidas económicas. Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los

programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.”

(Jorge Mieres (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas).Recuperado de https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

2.1.3. Cracker

“Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obsceno propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web, tales como rutinas des bloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.

Un cracker también puede ser el que se dedica a realizar esos pequeños programas que destruyen los datos de las PC, sí los Virus Informáticos...

Los mismos crackers, pueden usar herramientas (programas) hechas por ellos mismos o por otros crackers, que les sirven para des-encriptar información, "romper" los passwords de las PC, e incluso de los programas y compresores de archivos; aunque si estos programas no son manejados por malas manos, pueden ser muy útiles para los técnicos o para uno mismo...claro con los archivos y ordenadores de cada quien.” (Carlos Iván Paredes Flores. Hacking) Recuperado de http://www.residentmugen.cjb.net/

2.1.4. Delitos Informáticos

El delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan intereses protegidos como la intimidad, el patrimonio económico, la fe pública, la seguridad, etc., como aquellas que recaen sobre herramientas informáticas propiamente dichas tales como programas, computadoras, etc.

2.1.5. Hacker

"Un Hacker es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento, es alguien

que es capaz de hacer algo raro con cualquier aparato electrónico y lo hace actuar distinto, alguien que no tiene límites para la imaginación y busca información para después compartirla, es alguien al que no le interesa el dinero con lo que hace, solo le importa las bellezas que pueda crear con su cerebro, devorando todo lo que le produzca satisfacción y estimulación mental... Un hacker es aquel que piensa distinto y hace de ese pensamiento una realidad con diversos métodos. Es aquel que le interesa lo nuevo y que quiere aprender a fondo lo que le interesa."

“El Hacking se considera una ofensa o ataque al Derecho de gentes, y no tanto un delito contra un Estado concreto, sino más bien contra la humanidad. El delito puede ser castigado por los tribunales de cualquier país en el que el agresor se halle. La esencia del Hacking consiste en que el pirata no tiene permiso de ningún Estado soberano o de un Gobierno en hostilidades con otro. Los HACKERS son considerados delincuentes comunes en toda la humanidad, dado que todas las naciones tienen igual interés en su captura y castigo.”(Carlos Iván Paredes Flores. Hacking) Recuperado de http://www.residentmugen.cjb.net/

Ética Hackers

"Son profesionales que poseen una gran colección de habilidades y completamente merecedores de confianza .Durante una evaluación, el Ethical Hacker maneja "las riendas" o "llaves" de la compañía, y por tanto esta persona debe ser absolutamente profesional y ética ya que manejara información latamente sensible. La sensibilidad de la información manejada durante la evaluación exige que sean tomadas fuertes medidas de seguridad para el manejo de la misma: laboratorios de acceso restringido con medidas de seguridad física, conexiones múltiples de acceso a Internet, caja fuerte para sustentar la documentación en papel de los clientes, criptografía reforzada que proteja los resultados electrónicos, redes aisladas para el proceso de experimentación."(Joomla 1.5 Template, web hosting. Valid XHTML and CSS. TICS - Tecnologías de la Información y las Comunicaciones). Recuperado de http://www.tics.org.ar/index.php?option=com_content&view=article&id=97:conceptos-de-hacking-etico&catid=14:seguridad-informca&Itemid=31

2.1.6. Lamer

"Un Lamer es simple y sencillamente un tonto de la informática, una persona que se siente Hacker por haber bajado de Internet el Net bus, alguien a quien le guste bajar virus de la red e instalarlos en la PC de sus amigos, aunque más

bien podría decírsele como un Cracker de pésima calidad; en general alguien que cree que tiene muchos conocimientos de informática y programación, pero no tiene ni la más mínima idea de ello." (Carlos Iván Paredes Flores. Hacking) Recuperado de http://www.residentmugen.cjb.net/

2.1.7. Phreacker

"El phreaker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos." (Carlos Iván Paredes Flores. Hacking) Recuperado de http://www.residentmugen.cjb.net/

2.1.8. Seguridad Informática

"Medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la

misma. La información es un recurso de valor estratégico para las empresas y como tal debe ser debidamente protegida.

Las políticas de seguridad de la información protegen de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos. Es importante que los principios de la política de seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas autoridades de la compañía para la difusión y consolidación de las políticas de seguridad."(Zacarías Leone. Delitos Informáticos) Recuperado de http://www.zacariasleone.com.ar/docs/presentacionppt1.ppt

2.2. Marco Espacial

El estudio se realizara en el ámbito informático (empresas, gobierno, hogares) de las herramientas hacker más utilizadas en este ámbito.

2.3. Marco Temporal

Para la ejecución de este estudio y elaboración del instructivo informático se tendrá un lapso de 2 meses en la planificación y desarrollo de resultados.

2.4. Marco legal

Se realizara un enfoque a las leyes en el ecuador como son las multas o sanciones planteadas para las personas hacker.

INFRACCIONES INFORMATICAS	REPRESIÓN	MULTAS
Delitos contra la información protegida(CPPArt.202) 1.Violentando claves o sistemas 2.Seg.nacional o secretos comerciales o industriales 3.Divulgación o utilización fraudulenta 4.Divulgación o utilización fraudulenta por custodios 5.Obtención y uso no autorizados	 6 m. -1 año 3 años 3 a 6 años 9 años 2 m. -2 años	 $500 a $1000 $1.000 - $1500 $2.000 - $10.000 $2.000 - $10.000 $1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	6 años	---
Falsificación electrónica (CPP Art. 353)	6 años	---
Daños informáticos (CPP Art. 415) 1.Daño dolosamente 2.Serv. público o vinculado con la defensa nacional 3.No delito mayor	 6 m. -3 años 5 años 8 m. -4 años	 $60 – $150 $200 - $600 $200 - $600
Apropiación ilícita(CPPArt.553) 1.Uso fraudulento 2. Uso de medios (claves, tarjetas magnéticas, etc.)	6 m. -5 años 5 años	$500 - $1000 $1.000 - $2.000

Estafa(CPPArt.563)	5 años	$500 - 1.000

Título II: DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL. Cap. V. De los Delitos Contra la inviolabilidad del secreto.

Art. 202 A):- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares.

Art. 202 B) Obtención y utilización no autorizada de información. La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares.

TITULO III. DE LOS DELITOS CONTRA LA ADMINISTRACION PÚBLICA. Cap.V. De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad.

Art...- 262. Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

Título IV. DE LOS DELITOS CONTRA LA FE PUBLICA.- Cap. III. De las Falsificaciones de Documentos en General

Art.353. A) Falsificación electrónica. Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos,

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

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

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

3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

4.- El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

Titulo V. DE LOS DELITOS CONTRA LA SEGURIDAD PÚBLICA. Cap. VII:- Del incendio y otras Destrucciones, de los deterioros y Daños

Art.415 A) Daños informáticos. El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art.415 B) Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares.

Cap. II. Del Robo.

Art.553 A) Apropiación ilícita. Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. 553 B) La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Titulo X. De los Delitos Contra la Propiedad. Cap. V De las Estafas y otras defraudaciones.

Segundo Inciso del Art. 563.- Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

TITULO I. CAP. III. DE LAS CONTRAVENCIONES DE TERCERA CLASE.

A continuación del numeral 19 del artículo 606 añádase el siguiente:

“Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos."

CAPITTULO III.

3. METODOLOGÍA

3.1. Metodología de la Investigación

3.1.1. Tipo de investigación

El tipo de investigación es analítico descriptivo, de tal forma que nos permite conoce la caracterización de las herramientas más utilizadas en el ámbito informático.

3.1.1.1. Método descriptivo.

Con este método se podrá llegar a conocer las situaciones, actitudes y funciones de todas las herramientas hacker más utilizadas en el ámbito informático.

La finalidad de este método a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables.

La investigación se expone y resume la información de manera cuidadosa y luego se analizan los resultados a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

Etapas:

Examinar las características de cada herramienta hacker.

Definir cada herramienta hacker.

El objetivo del estudio es describir con una base bibliográfica, las herramientas hacker más utilizadas en el ámbito informático con los siguientes aspectos: nombre, funcionamiento y principales características de cada una de las herramientas hacker.

En base al objetivo de estudio el método es netamente descriptivo ya que se buscara información sobre el tema para encontrar datos que serán útiles para desarrollar los capítulos propuestos.

3.1.1.2. Método comparativo.

Mediante el procedimiento de comparación se realiza un cotejo sistemático de casos de análisis que en su mayoría se aplica con fines de generalización empírica y de la verificación de hipótesis.

La comparación va a ser utilizado para determinar y cuantifica mediante una matriz con criterios y características específicas las herramientas hacer más utilizadas en el ámbito informático.

3.1.2. Técnicas de investigación

La técnica a utilizarse es la recolección de información, esto ayudará a obtener una investigación de datos selecta e importante para desarrollar el tema planteado.

También se utilizara la técnica matriz de análisis que facilitará a localizar y visualizar las herramientas hacker más utilizadas en el ámbito informático.

En la matriz se usa la siguiente formula:

Riesgo=Probabilidad de Amenaza x Magnitud de Daño

La probabilidad de amenaza y magnitud de daño pueden tomar los valores y condiciones respectivamente.

3.1.3. Herramientas de investigación

La herramienta a utilizarse son las fuentes bibliográficas de donde se obtendrá la información necesaria.

CAPITULO IV.

4. DESARROLLO

4.1. Seguridad informática y los hackers

4.1.1. Concepto de seguridad informática

FIGURA 3Seguridad Informática

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

4.1.2. Objetivos de la seguridad informática

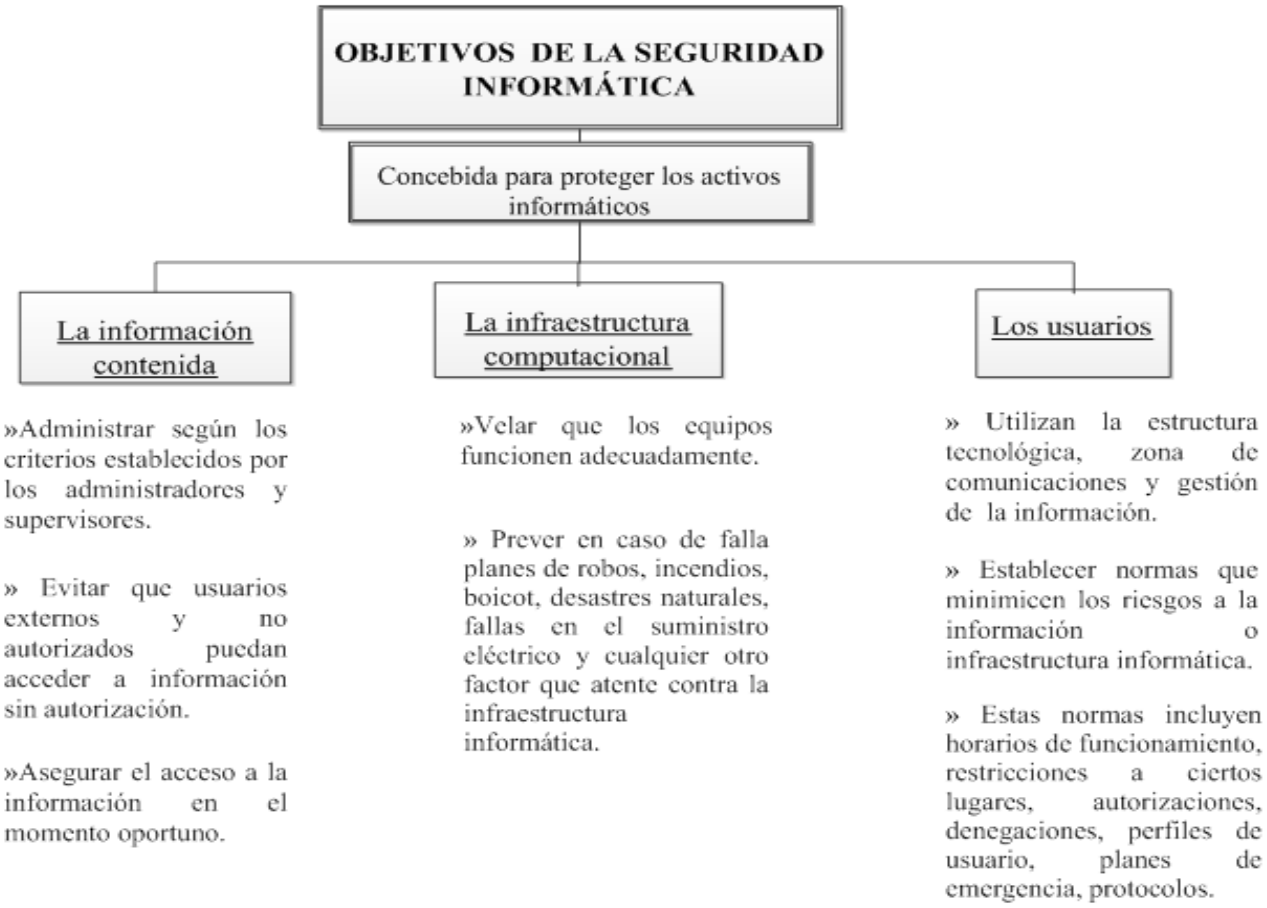


FIGURA 4 Objetivos de la Seguridad Informática

4.1.3. Las amenazas y vulnerabilidad de la seguridad informática

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los

datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

FIGURA 5 Usuario

•El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).

FIGURA 6 Programas

•Programas maliciosos: destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por intención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

FIGURA 7 Intruso

•Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o cript boy, viruxer, etc.).

•Un siniestro (robo, incendio, inundación): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

FIGURA 8 Robo

•El personal interno de Sistemas. Las pujas de poder que llevan a separaciones entre los sectores y soluciones incompatibles para la seguridad informática.

FIGURA 9 Personal

La vulnerabilidad es la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

Las políticas deberán basarse en los siguientes pasos:

- ✓ Identificar y seleccionar lo que se debe proteger (información sensible).
- ✓ Establecer niveles de prioridad e importancia sobre esta información.
- ✓ Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles.
- ✓ Identificar las amenazas, así como los niveles de vulnerabilidad de la red.
- ✓ Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla.
- ✓ Implementar respuesta a incidentes y recuperación para disminuir el impacto.

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los sistemas y datos a proteger.

4.1.4. Técnicas de seguridad informática

•Codificar la información: Cristología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.

FIGURA 10Codificar la información

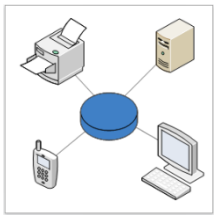


FIGURA 11Red

•Vigilancia de red.

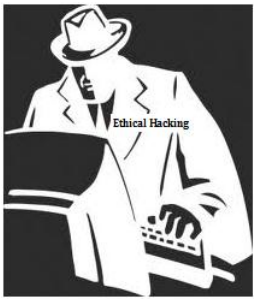
•Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

FIGURA 12 Tecnologías Protectoras

•Sistema de Respaldo Remoto. Servicio de backup remoto.

FIGURA 13 Respaldo

4.2. Ethical Hacking



Es un área de la seguridad informática que se respalda en que la mejor forma de evaluar las amenazas que representan los llamados “hackers” o piratas de la información es conocer cómo actúan y operan.

FIGURA 14 Ethical Hacking

Ethical Hacking también conocida como prueba de la penetración o la piratería sombrero blanco incluye las mismas herramientas, trucos y técnicas que los hackers utilizan, pero con una importante diferencia: hacking ético es legal, ellos están en capacidad de reportar las vulnerabilidades que encuentren y la forma de remediarlas.

Un hacker ético posee las habilidades, el modo de pensar, y las herramientas de un hacker, pero también es digno de confianza, porque tendrá “las riendas” o “llaves” de la compañía, y por tanto esta persona debe ser absolutamente

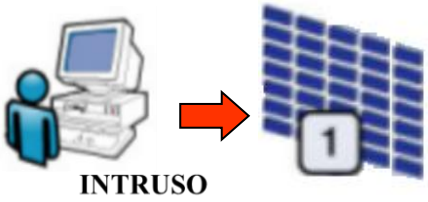
profesional y ética ya que manejara información latamente sensible, la intención de hacking ético es descubrir vulnerabilidades desde la perspectiva de un hacker lo que los sistemas pueden ser mejor asegurados.

4.2.1. Medidas de seguridad para el manejo de la información:

- Laboratorios de acceso restringido con medidas de seguridad física.
- Conexiones múltiples de acceso a Internet.
- Caja fuerte para sustentar la documentación en papel de los clientes.
- Criptografía reforzada que proteja los resultados electrónicos.
- Redes aisladas para el proceso de experimentación.

4.3. Etapas de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender, comprender y analizar la forma en que los hacker llevan a cabo un ataque.



Fase 1: Reconocimiento Se obtiene la información de la potencial víctima que puede ser una persona u organización, se recurre a diferentes recursos de Internet como Google. Algunas de las técnicas utilizadas son la Ingeniería Social, el Dumpster Diving, el sniffing.

FIGURA 15 Fase 1

Fase 2: Exploración Se utiliza la información obtenida en la fase 1 para tratar de obtener información sobre el sistema víctima como direcciones IP[1], nombres de host, datos de autenticación, entre otros. Las herramientas que un atacante puede emplear son network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

FIGURA 16 Fase 2

Fase 3: Obtener acceso Comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración. Algunas de las técnicas para atacar Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

FIGURA 17Fase 3

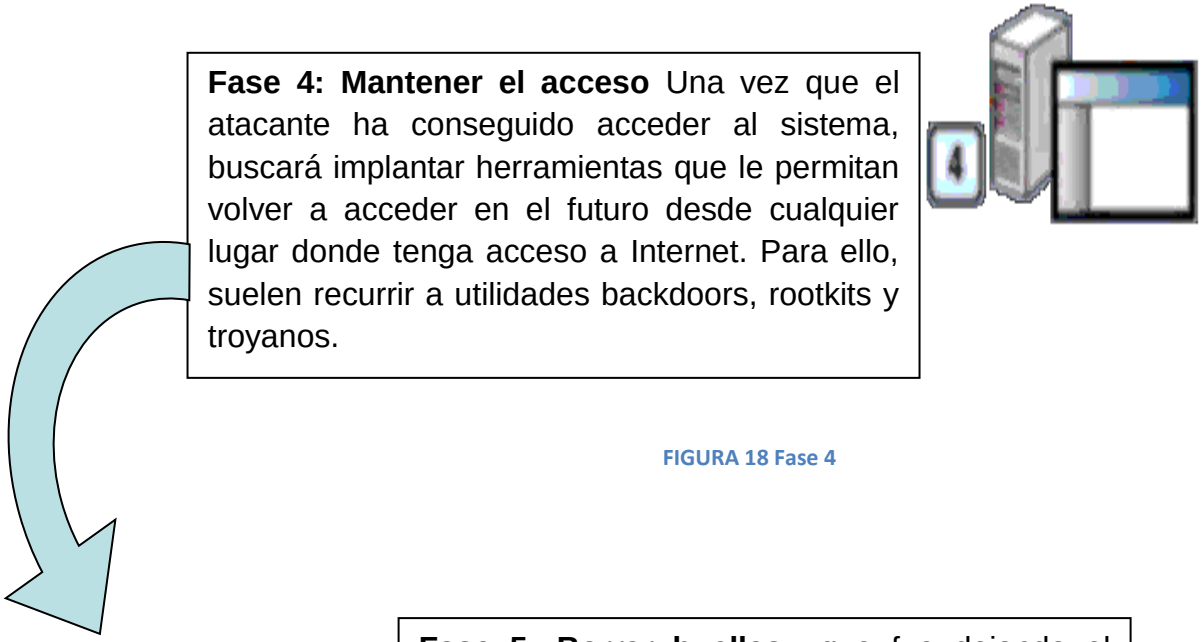


FIGURA 18 Fase 4

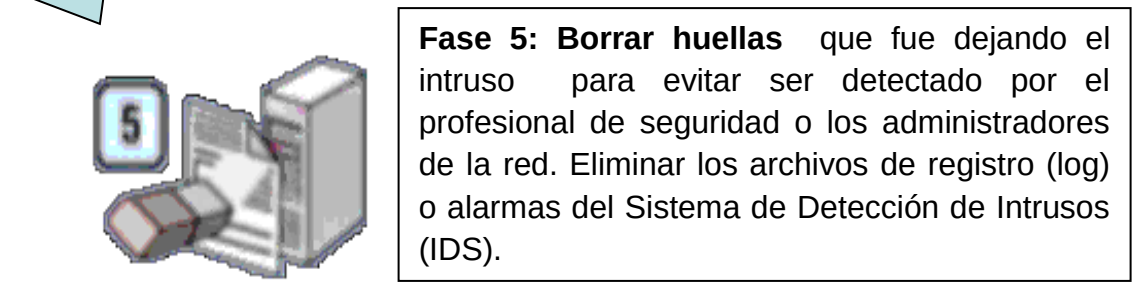


FIGURA 19 Fase 5

4.4. Perfil de un hacker.

Apariencia general: Inteligente. Despeinado. Intenso. Abstracto. Sorprendentemente para una profesión sedentaria, hay más hackers delgados que gordos, Visten vagamente camisetas, vaqueros y zapatillas deportivas. Pelo largo, barba y bigotes son comunes. Alta incidencia de camisetas con slogans intelectuales o humorísticos. Una substancial minoría prefiere ropa de campo: botas de excursión, ropa caqui, camisetas de leñador y cosas por el estilo.

Hábitos de lectura: Normalmente incluye mucha ciencia y ciencia-ficción. Los hackers tienen una diversidad de temas de lectura que dejan a la gente atónita, pero no tienden a hablar demasiado de ello. Muchos hackers pasan mucho tiempo libre leyendo mientras los ciudadanos medios lo queman viendo TV, y a menudo mantienen montones de libros bien cuidados en sus hogares.

Otros intereses: Algunos hobbies son ampliamente compartidos y reconocidos por toda la sociedad. Ciencia-ficción. Música. Medievalismo. Ajedrez, juego de rol e intelectuales de todo tipo, Puzzles lógicos. Otros intereses que pueden correlacionarse menos pero positivamente con el mundo del hacker incluyen lingüística y técnicas teatrales.

Actividad física y deportes: Muchos, quizás la mayoría, de hackers no practican o hacen ningún tipo de deporte y son determinadamente anti físicos. Más aún, los hackers evitan los deportes de equipo. Los deportes del hacker son casi siempre auto competitivo teniendo que ver con la concentración, y habilidades de equilibrio: Artes marciales, ciclismo, carreras de coches, caminar, escalada, navegar, esquí, patinaje sobre hielo y sobre ruedas.

Educación: Aproximadamente todos los hackers que han pasado la adolescencia son universitarios o autodidactas hasta un nivel equivalente. El hacker autodidacta es muchas veces considerado (al menos por otros hackers) como mejor motivado, y puede ser más respetado que su compañero con título de estudios. Las áreas académicas desde las que la gente gravita en el mundo del hack incluyen ciencias informáticas, ingeniería eléctrica, física, matemáticas, lingüistas y filosofía.

Cosas que los hackers detestan y evitan: IBM mainframes, pitufos, Ewoks, y otras formas de animación que consideran ofensivas. Burocracias. Gente estúpida. Música fácil de escuchar.

Género y Etnias: El hack es todavía predominantemente masculino. Aunque el porcentaje de mujeres es claramente mayor que el típico bajo porcentaje en las profesiones técnicas, las hackers son generalmente respetadas y tratadas con igualdad.

Características de la Personalidad: Las características comunes más obvias de la personalidad de los hackers son la gran inteligencia, curiosidad que les consume y facilidad en las abstracciones intelectuales. Además, a la mayoría de los hackers les atrae lo nuevo, y son estimulados por ello (especialmente la

novedad intelectual). La mayoría son además relativamente individualistas y anticonformistas. Los hackers generalmente están solo motivados débilmente por recompensas convencionales como aprobación social o dinero. Tienden a estar atraídos por desafíos y excitados por juguetes interesantes, y a juzgar el interés del trabajo de otras actividades en términos de los desafíos ofrecidos y los juguetes que hacen para jugar.

Debilidades de la personalidad hacker: Habilidad relativamente pequeña para identificarse emocionalmente con otra gente. Esto puede ser porque los hackers no son mucho como esa 'otra gente'. Sin duda, hay también una tendencia a la auto-absorción, arrogancia intelectual, e impaciencia con la gente y tareas que creen malgasta su tiempo. Como resultado, muchos hackers tienen dificultad en establecer relaciones estables.

4.5. Los diez mandamientos del hacker

I. Nunca destroces nada intencionalmente en la Computadora que estés crackeando.
II. Modifica solo los archivos que hagan falta para evitar tu detección y asegurar tu acceso futuro al sistema.
III. Nunca dejes tu dirección real, tu nombre o tu teléfono en ningún sistema.

IV. Ten cuidado a quien le pasas información. A ser posible no pases nada a nadie que no conozcas su voz, número de teléfono y nombre real.

V. Nunca dejes tus datos reales en un BBS, si no conoces al sysop, déjale un mensaje con una lista de gente que pueda responder de ti.

VI. Nunca hackees en computadoras del gobierno. El gobierno puede permitirse gastar fondos en buscarte mientras que las universidades y las empresas particulares no.

VII. No uses BlueBox a menos que no tengas un servicio local o un 0610 al que conectarte. Si se abusa de la bluebox, puedes ser cazado.

VIII. No dejes en ningún BBS mucha información del sistema que estas crackeando.

IX. No te preocupes en preguntar, nadie te contestara, piensa que por responderte a una pregunta, pueden cazarte a ti, al que te contesta o a ambos.

X. Punto final. Puedes pasearte todo lo que quieras por la WEB, y mil cosas más, pero hasta que no estés realmente hackeando, no sabrás lo que es.

4.6. Clasificación y caracterización de herramientas hacker

4.6.1. Concepto de herramientas hacker

Son programa que puede ser utilizado por un hacker para causar perjuicios a los usuarios de un ordenador (pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc).

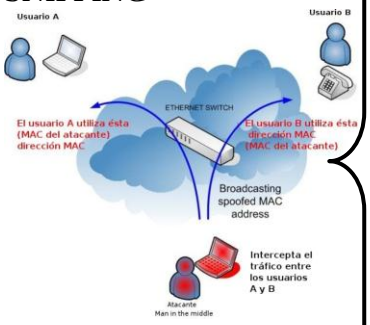
4.6.2. Métodos y herramientas hacker

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar debilidades en el diseño, configuración y operación de los sistemas. Esto permite a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hacker" bulletin boards y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras.

- EAVESDROPPING Y PACKET SNIFFING



Significa escuchar secretamente, se ha utilizado tradicionalmente para escuchas telefónicas.

En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados.

El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, a un equipo router o a un gateway de Internet.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, capturar números de tarjetas de crédito y direcciones de e-mail entrante y saliente.

FIGURA 20 EAVESDROPPING

- SNOOPING Y DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

FIGURA 21 SNOOPING

- TAMPERING O DATA DIDDLING

FIGURA 22 TAMPERING

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos.

Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información.

El administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

- SPOOFING

FIGURA 23SPOOFING

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering.

Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro.

Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.

- CABALLOS DE TROYA

FIGURA 24 Caballos de Troya

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto

Por ejemplo: Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

- JAMMING Ó FLOODING

FIGURA 25 JAMMING

Este tipo de ataques desactivan o saturan los recursos del sistema.

Muchos proveedores de Internet, han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP.

El atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing).

- BOMBAS LÓGICAS

FIGURA 26 Bombas Lógicas

Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos.

Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

- DIFUSION DE VIRUS

FIGURA 27 Difusión de virus

Es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo o través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Una característica propia es su auto reproducción.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc) y los sectores de boot-particion.

El ataque de virus es el más común para la mayoría de las empresas u organizaciones.

- OBTENCIÓN DE PASSWORDS, CÓDIGOS Y CLAVES

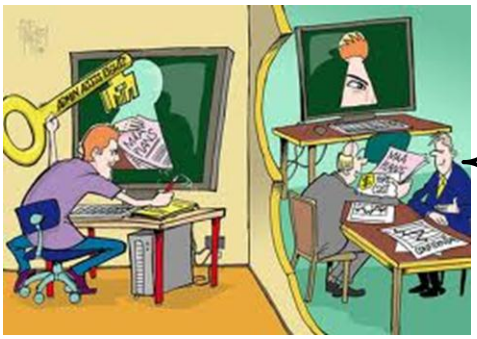


FIGURA 28 Obtención de Passwords

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia.

En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

- INGENIERA SOCIAL

Básicamente convencer a la gente de que haga lo que en realidad no debería.

Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente.

Esto es común cuando en el Centro de Cómputo los administradores son amigos o conocidos.

FIGURA 29 Ingeniería Social

- ELIMINAR EL BLANCO

Ping mortal. Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo.

Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino se cuelgue.

Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par de años.

FIGURA 30 Eliminar el Blanco

4.6.3. Utilidades de herramientas hacker

4.6.3.1. Hack General

HERRAMIENTA	UTILIDAD
Brutus AE v2.0	Crackeador de password por fuerza bruta.
Cain 2.0	Crackea pwl, sniffer, etc...
Crack - FTP	Crackea FTP
NTFS - DOS	Convierte NTFS (nt) a dos (fat)
HEdit 1.2	Editor hexadecimal. Windows.
Phonetag v 1.3	Muy buen war dialer, muy fácil de manejar y configurar.
Toneloc 1.10	Para muchos el mejor war dialer. W95/DOS.
MicroBest Cracklock 3.5	Contra las limitaciones de tiempo de muchas versiones trial shareware o comerciales.
Disaster v 1.0	Interactive Disassembler. DOS.
Netcat NT	Herramienta muy útil para varias tareas de red.

FIGURA 31Tabla Hack General

4.6.3.2. Scanners

HERRAMIENTA	UTILIDAD
Essential Net Tools 3.1	Conjunto de herramientas de red para diagnosticar redes y visualizar las conexiones de red de una computadora.
Languard Network Scanner	Scanner que te permite analizar la red e identificar posibles agujeros de seguridad.
Asmodeus	Scanner y Sniffer. W95/NT
ChaOscan	IP scanner. W9x.
NMap 1.3.1	Sin duda, uno de los mejores scanners de puertos. (Versión para Windows).
NMap (linux)	Este scanner en su última versión para Linux.
SuperScan 3.0	Scanner de puertos muy rápido. (simple pero potente)
CGI - Scan	Scaneador de vulnerabilidades CGI.
FTPScan	FTP Scanner. W95. Linux
NScan	Necrosoft Nscan.
HC Portscan	Scanner de puertos.
Imaniac	Internet Maniac. Whois, Traceroute, Scanner, etc..

SMBScanner v1.0	A partir de una IP busca carpetas y máquinas compartidas.
Wingate Scan	Wingate Scanner. W9x.

FIGURA 32Tabla Scanners

4.6.3.3. Anonimato

HERRAMIENTA	**UTILIDAD**
SocksCap 2.2 Crack	Socksificador que te permite ser anónimo en cualquier conexión (IRC, FTP, Scanners, etc...). Utiliza socks 4 o 5.
AA Tools	Multitud de herramientas relacionadas con la anonimidad (gestión de proxy, más concretamente)
Multiproxy 1.2	Puede ocultar tu IP por completo conectando dinámicamente a servidores proxy públicos no transparentes.
SocksChain	Programa que te permite encadenar proxy.
ProxyChecker	Checkea los proxys (Velocidad, Anonimato, etc...)
WinBouncer	Programa que instala un Bouncer (BCN) en un servidor para usarlo a

	través de una shell.
Stealther	Permite el uso de proxys cruzados, haciéndote prácticamente indetectable e intachable.

FIGURA 33 Anonimato

4.6.3.4. Nukers

HERRAMIENTA	**UTILIDAD**
NS Nuke	Nukeador para la Netbios.
Nuke - IT	Un gran nukeador.
Win - Nuke	Version 4.0 de este nukeador.
Internet Packet Tools	Generador de paquetes DoS. W95.
Panther Modem	Denial of Service Attack. W95.
IRC Kill	Flood Attack. W95.
Klone - X	Flooder
Winsmurf	Potente nuker.
NsBot	Programa para poder conectar clones masivamente a un server de irc.
S Slap	Bitch Slap v. 2.0

FIGURA 34Tabla Nuker

4.6.3.5. Mail Anónimo

HERRAMIENTA	UTILIDAD
Ghost Mail	Uno de los mejores programas para mandar mails anónimos.
Sabotage	Mail anónimo muy sencillo de usar.
Ubi Anonymous Mail	Otro programa para mandar mails anónimos.
Avalanche	Buen programa para mail anónimo. También sirve como mail bomber.

FIGURA 35Tabla Mail Anónimo

4.6.3.6. Keyloggers

HERRAMIENTA	UTILIDAD
BagKeys	Captura las teclas pulsadas y las envía a un fichero. DOS.
HC Dialup Account Ripper	Busca todos los passwords del acceso telefónico a redes y los guarda en un fichero de texto. W9x.
Teclass	Uno de los mejores keyloggers.
Keylog95	Capturador de teclado para W95.
Fatal Network Error	Muestra un cuadro de dialogo de error solicitando el nombre y el password.

	Esta información es guardada en un archivo. W9x.
Phantom	Buen Keylogger
SC Key Log2	Keylogger que permite él envió de los logs capturados por mail.
GOD	Buen keylogger que envía los logs a través de los firewalls.
Perfect Keylogger 1.4.0.0	Puede volcar los logs a una cuenta de e-mail. Loguea también las **URL** visitadas y captura las pantallas con alta resolución. (En castellano).
Tiny Keylogger	Minúsculo keylogger, que corre totalmente invisible en el PC víctima.
2Spy	Programa que monitoriza, intercepta y almacena todo lo ocurrido en tu sistema.

FIGURA 36Tabla Keyloggers

4.6.3.7. Sniffer

HERRAMIENTA	**UTILIDAD**
Ettercap	Sniffer MultiPlataforma v0.6.6.6
Ethereal	Popular sniffer, para entornos Unix y Windows.

Tcpdump 3.7.2	El Sniffer por excelencia.
WinSniffer	Versión 1.22 de otro popular Sniffer.
Snort 2.0.0	Gran sniffer y logger.
Sniffa	Otro sniffer mas.

FIGURA 37Tabla Sniffers

4.6.3.8. Mail Bombers

HERRAMIENTA	UTILIDAD
McSpammer	Mail Bomber, muy fácil de manejar, solo colocas el mail de la víctima, el mensaje, y la cantidad de mensajes a enviar.
Yaemb v1.6	Mailbomber con gran cantidad de opciones como conectarse a proxis, mandar por server propio y más...
Xmas 2000	Buen programa para bombardear y mandar mails anónimos.

FIGURA 38Tabla Mail Bombers

4.6.3.9. Software para crear Virus

HERRAMIENTA	UTILIDAD
Virus Creation Labs	Famoso software que te permite la creación de virus masivos.
Satanic Brain Virus Tools	Sencillo programa creador de software maligno como virus nukers, etc...
Instant Virus Production Kit	Software que permite la creación de virus intruders.
Lavi	Software muy simple de usar para la creación de virus.

FIGURA 39Software para crear Virus

4.6.3.10. Bouncers

HERRAMIENTA	UTILIDAD
NSBNC	Típico Bouncer para Linux.
ProBNC	Bouncer para Windows destinado al IRC.

FIGURA 40Tabla Bouncers

4.7. Análisis de herramientas hacker

4.7.1. Metodología

La metodología que se utilizara es el descriptivo, con la técnica de la matriz de análisis que contendrá criterios q servirá para determinar las herramientas hacker más utilizadas en el medio informático.

4.7.2. Matriz de análisis

La Matriz de análisis ayudara a localizar y visualizar las herramientas hacker más utilizadas en ámbito informático, para posteriormente detallar los daños que puede ocasionar y como combatir dicha herramienta.

La Matriz es la basé en el método de Análisis con un gráfico usando la fórmula:

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente

4.7.3. Criterios

Nivel de impacto: Daño que puede causar en un sistema.

Tiempo de acceso: Retardo temporal entre una petición a un sistema electrónico y la finalización de la misma o la devolución de los datos solicitados.

Discreción: Reserva o cautela para ingresar y obtener información de un sistema.

Actúa en 2 o más sistemas operativos: Compatibilidad de funcionamiento en diferentes sistemas operativos.

Tipo de información extraída: Diferente tipo de información que puede extraer de un sistema.

4.7.4. Elaboración de la matriz de análisis

Matriz de Análisis	Amenaza [1 = Insignificante,			2 = Baja, 3= Mediana, 4 = Alta]			
Datos e Información	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Nivel de impacto	Tiempo de acceso	Discreción	Actúa en 2 más sistemas operativos	Tipo de información extraída	Total
Brutus	3	3	4	3	3	3	48
Crack	2	2	1	2	1	2	16
Cain	4	3	3	3	3	4	64
MicroBest Cracklock	3	3	4	3	3	4	51
Disaster	2	2	1	2	3	1	18
ProxyChecker	3	3	2	1	2	1	27
Essential Net Tool	4	3	3	3	3	3	60
SN Nuke	2	3	2	2	2	1	20
Languard Network Scanner	4	3	3	3	3	3	60
Nmap	4	4	4	3	4	4	76
SuperScan	3	4	4	3	3	3	51
Klone -X	3	2	1	3	2	3	33
FTPscan	3	3	3	4	4	4	54
Ethereal	3	4	3	4	4	4	57
SC Key Log2	3	3	3	4	4	3	51
Sabotage	3	2	3	2	3	1	33
Imaniatic	3	3	2	2	1	2	30
Tcpdum	2	2	2	1	1	3	18
Snort	3	4	3	4	3	3	51
Ettercap	4	3	4	3	4	4	72
Teclass	3	3	2	2	2	3	36
Toneloc	3	2	3	2	1	2	30
Winsmurf	2	3	2	2	3	1	22

FIGURA 41Tabla Matriz de Análisis

4.8. Diseño del instructivo

Mediante la matriz de comparación se ha podido determinar las herramientas hacker más utilizadas en el ámbito informático, con las cuales se elaborará el instructivo informático.

4.8.1. ETTERCAP

- Configurar correctamente las SSL.
- Analizar el tráfico de la red que tengan Hub o switch o cualquier otro dispositivo.
- Ejecutar los permisos de root.
- Analizar los paquetes mediante los filtros.
- Detectar del sistema operativo remoto.
- Cerrar todas las conexiones.
- Escanear periódicamente LAN: hosts, puertos abiertos, servicios.
- Buscar envenenamientos en la red.

4.8.1.1. DEBILIDADES

- ✓ Debe ser instalado para su funcionamiento.
- ✓ Susceptibles a un desbordamiento de búfer

4.8.2. NMAP

- Bloquear los puertos abiertos de la máquina.
- Realizar el inventario y el mantenimiento del inventario de computadores de una red.
- Auditar de la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte.
- Evadir los Sistema de detección de intrusos (IDS).

4.8.2.1. DEBILIDADES

- ✓ La instalación se realiza con privilegios especiales o root.

4.8.3. ESSENTIAL NETTOOLS

- Visualizar las conexiones de tus equipos y los puertos abiertos.
- Escanear los puertos TCP, para chequear la seguridad de la LAN y monitorizar las conexiones externas a tus recursos compartidos.
- Realizar Ping, para conocer en cualquier momento el estado de una red.

4.8.3.1. DEBILIDADES

- ✓ Debe ser instalado para su funcionamiento.

4.8.4. LANGUARD NETWORK SECURITY SCANNER

- Realizar la administración de actualizaciones de seguridad.
- Recopilar toda la información posible acerca de las vulnerabilidades.
- Encontrar servicios rufianes y puertos TCP y UDP abiertos.
- Detectar dispositivos inalámbricos.
- Bloquear recursos compartidos abiertos con claves y enumera quién tiene acceso a estos recursos junto con sus permisos.
- Enumerar los dispositivos, usuarios, servicios, etc.

4.8.4.1. DEBILIDADES

- ✓ Debe ser instalado para su funcionamiento.

4.8.5. CAIN

- Combinar contraseñas con caracteres numéricos, alfanuméricos, letras, símbolos.
- Bloquear puertos abiertos.
- Modificar passwords de protocolos: FTP, SMTP, POP3, HTTP, MySQL, ICQ, Telnet.

4.8.5.1. DEBILIDADES

- ✓ Para su funcionamiento debe ser instalado sus dos partes Caín y Abel.

4.8.6. SUPER SCAN

- Proteger las direcciones IP.
- Cerrar los puertos abiertos.
- Combinar contraseñas con caracteres numéricos, alfanuméricos, letras, símbolos.

4.8.6.1. DEBILIDADES

- ✓ Debe ser instalado para su funcionamiento.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

a) La seguridad informática es fundamental para la privacidad y manejo de información privada.
b) Es necesario profundizar en el conocimiento de las herramientas hacker.
c) Las herramientas hacker se ha convertido en una amenaza para la vulnerabilidad se sistemas informáticos.
d) Las herramientas determinadas como más usada en el ámbito informático tienen un nivel de ataque alto.

5.2. Recomendaciones

a) Dentro de la ejecución de este proyecto es recomendable incentivar a las empresas informarse más sobre las amenazas para los sistemas informáticos.
b) A los integrantes de los centros de cómputo actualizarse cada día sobre la aparición de herramientas hacker.
c) A las organizaciones tener planes de contingencia en caso de ataques informáticos.

Bibliografía

- Carlos Iván Paredes Flores. Hacking) Recuperado de http://www.residentmugen.cjb.net/
- Joomla 1.5 Template, web hosting. Valid XHTML and CSS. TICS - Tecnologías de la Información y las Comunicaciones). Recuperado de http://www.tics.org.ar/index.php?option=com_content&view=article&id=97:conceptos-de-hacking-etico&catid=14:seguridad-informca&Itemid=31
- Jorge Mieres (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas).Recuperado http://proton.ucting.udg.mx/tutorial/hackers/hacking.pdf
- Zacarías Leone. Delitos Informáticos) Recuperado de http://www.zacariasleone.com.ar/docs/presentacionppt1.ppt
- Gonzalo Álvarez Marañón. Herramientas y Técnicas de Hacking y Cracking y cómo protegerse ante ellas.)Recuperado de http://www.iec.csic.es/gonzalo/descargas/HerramientasTecnicasHackingCracking.pdf
- Seguridad informática. Recuperado de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- Nmap Recuperado de http://es.wikipedia.org/wiki/Nmap
- Superscan. Recuperado de http://www.zeroprogramas.com/programas/superscan-3-0.asp

- Dr. Juan José Páez Rivadeneira(2009) Recuperado de http://www.derechoecuador.com/index2.php?option=com_content&do_pdf=1&id=5174

UNIVERSIDAD TECNOLÓGICA ISRAEL

DIRECCIÓN DE POSGRADOS

AUTORIZACIÓN DE EMPASTADO

DE: Ing. Tania Mayorga.

PARA: Msc. Luis Andrés Chávez Ing.

DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

ASUNTO: Autorización de Empastado

FECHA Quito, 1 de diciembre del 2011

Por medio de la presente certifico que la pregradista Srta. Diana Lucia Méndez Ávila con CI No. 010475195-3 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **INVESTIGACIÓN Y ELABORACIÓN DE UN INSTRUCTIVO SOBRE LAS HERRAMIENTAS HACKER MÁS UTILIZADAS EN EL ÁMBITO INFORMÁTICO**, del título de ingenieros en sistemas informáticos

Atentamente

_____

Ing. Tania Mayorga.

UNIVERSIDAD TECNOLÓGICA ISRAEL

DIRECCIÓN DE POSGRADOS

AUTORIZACIÓN DE EMPASTADO

DE: Ing. Juan Pérez.

PARA: Msc. Luis Andrés Chávez Ing.

DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

ASUNTO: Autorización de Empastado

FECHA Quito, 1 de diciembre del 2011

Por medio de la presente certifico que la pregradista Srta. Diana Lucia Méndez Ávila con CI No. 010475195-3 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **INVESTIGACIÓN Y ELABORACIÓN DE UN INSTRUCTIVO SOBRE LAS HERRAMIENTAS HACKER MÁS UTILIZADAS EN EL ÁMBITO INFORMÁTICO**, del título de ingenieros en sistemas informáticos

Atentamente

_____

Ing. Juan Pérez.

UNIVERSIDAD TECNOLÓGICA ISRAEL

DIRECCIÓN DE POSGRADOS

AUTORIZACIÓN DE EMPASTADO

DE: Ing. Pablo Ochoa.

PARA: Msc. Luis Andrés Chávez Ing.

DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

ASUNTO: Autorización de Empastado

FECHA Quito, 1 de diciembre del 2011

Por medio de la presente certifico que la pregradista Srta. Diana Lucia Méndez Ávila con CI No. 010475195-3 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **INVESTIGACIÓN Y ELABORACIÓN DE UN INSTRUCTIVO SOBRE LAS HERRAMIENTAS HACKER MÁS UTILIZADAS EN EL ÁMBITO INFORMÁTICO**, del título de ingenieros en sistemas informáticos.

Atentamente

_____

Ing. Pablo Ochoa.