INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO

DE TECNOLOGÌA

UNIDAD ACADÉMICA DE EDUCACIÓN COMERCIAL, ADMINISTRACIÓN Y CIENCIAS

CARRERA: TECNOLOGÍA EN ANÁLISIS DE SISTEMAS

TESIS PREVIO A LA OBTENCION DEL TITULO DE TECNOLOGÍA EN ANÁLISIS DE SISTEMAS

TESIS:

ESTUDIO DE LOS SISTEMAS OPERATIVOS DE HACKING ÉTICO PARA PRUEBAS DE AMENAZAS Y VULNERABILIDADES Y RIESGOS EN LA RED WIFI DEL INSTITUTO TECNOLÓGICO BOLIVARIANO DE TECNOLOGÍA

AUTOR:

GONZABAY LÓPEZ FÉLIX EMILIO

TUTOR:

ING. JULIO SUÁREZ DIOSES

Guayaquil, Ecuador

2017

Dedicatoria

A mis padres, a mi familia y a todas las personas

Que conozco porque de una u otra manera han

Aportado para lograr mis metas.

Agradecimiento

Agradezco a Dios y a mis padres, abuelitos por darme apoyo y Confianza en toda esta etapa académica en el Instituto Superior Tecnológico Bolivariano de Tecnología.

Índice General

Capítulo III

3. Metodología

Capítulo IV

4. Análisis e Interpretación de Resultados

Índice de Gráficos

Índice de Tablas

Resumen

La mayoría de vulnerabilidades encontradas no se refiere al mal funcionamiento de equipos tecnológicos sino a la incorrecta configuración de los sistemas inalámbricos.

Las actividades de dichas instituciones que no cuentan con las políticas dónde se explique el buen uso/manejo de los dispositivos y de la red inalámbrica o sobre la configuración del dispositivo inalámbrico, indican que existe un cierto desconocimiento del personal interno de la institución en cuanto a la seguridad informática y los riesgos que puedan existir en la red inalámbrica al no contar con dichos reglamentos.

Día a día nuevas noticias y publicaciones en los sitios web sobre las nuevas vulnerabilidades en la red inalámbrica, logran los hackers encontrar. Toda institución que presta servicios y que cuenta con alta cantidad de clientes, tiene como responsabilidad social y profesional asegurar la información no sea Hackeada por personal que no está autorizado.

La nueva tecnología por establecer un sistema de hacking ético para tener la seguridad de la información. El elevado porcentaje de redes inalámbricas son instaladas sin tener la seguridad convirtiendo a sus redes en redes abiertas (o inicialmente vulnerables ante el intento de acceder a ellas por terceras personas).

La razón de la siguiente investigación se da por las frecuentes amenazas, riesgos y vulnerabilidad de datos por terceras personas en el Instituto Tecnológico Bolivariano.

Vulnerabilidades

Hackeada

Seguridad

Abstract

The majority of vulnerabilities found do not refer to the malfunction of technological equipment but to the incorrect configuration of the wireless systems.

The activities of those institutions that do not have policies explaining the good use / management of the devices and the wireless network or the configuration of the wireless device, indicate that there is a certain lack of knowledge of the internal staff of the institution in terms of computer security and the risks that may exist in the wireless network in the absence of such regulations.

Every day new news and publications on websites about new vulnerabilities in the wireless network get the hackers to find. Every institution that provides services and that has a high number of clients has as social and professional responsibility to ensure the information is not hacked by personnel who are not authorized.

The new technology to establish an ethical hacking system to have the security of information. The high percentages of wireless networks are installed without security making their networks open (or initially vulnerable to the attempt to access them by third parties).

The reason for the following investigation is given by the frequents threats, risks and vulnerability of data by third persons in the Bolivarian Technological Institute.

Vulnerabilities

Hacked

Security

Capítulo I

EL PROBLEMA

Planteamiento del problema

Ubicación del problema en un contexto

Los código informático son complejos, existen muchas probabilidades de que existan algunas vulnerabilidades, sobre todo el servicio que contiene es muy popular o valioso y despierta el interés de los hackers, un término con el que deben hacer distinciones, ya que pueden tener intereses de diferentes tipos: económicos, de prestigio y reputación o bien con mero interés de conocimiento y estudio de la seguridad informática. Esta última finalidad se utilizan incluso para conseguir un trabajo, y son una de las mejores formas de reclutamiento. Se conoce como hacking ético, y es útil tanto para los profesionales como para las empresas.

La mayoría de vulnerabilidades encontradas en ciertas redes wifi de instituciones no se refieren al mal funcionamiento de equipos tecnológicos sino a una incorrecta configuración de los dispositivos inalámbricos.

Actividades como no contar con políticas que expliquen el buen uso/manejo de los dispositivos de la red inalámbrica o sobre la configuración del dispositivo inalámbrico, indican que existe un cierto desconocimiento del personal interno de la institución en cuanto a la seguridad informática y los riesgos en que la red inalámbrica pueda estar expuesta al no contar con estos reglamentos.

Cada semana aparecen nuevas publicaciones en la web sobre las amenazas de una red inalámbrica, que logran los hackers hallar.

Toda institución que ofrece sus servicios que tienen una alta cantidad de clientes, tiene como obligación social y profesional asegurar que la información no sea manipulada por ciertas personas que no están autorizadas.

Situación Conflicto

El INSTITUTO TECNOLÓGICO BOLIVARIANO en la actualidad presenta anomalías en la red Wifi lo que ocasiona problemas al momento de:

- Falencias en el cobro de las cuotas mensuales.
- Demora en la carga de la plataforma.
- Lenta respuesta por parte del personal encargado del área de redes inalámbricas.
- Disminución en el Área de Cobranza.

De lo antes mencionado se puede decir que si la institución no toma medidas para estas falencias, la institución tendría consecuencias en su utilidad, rentabilidad, perjudicando al personal administrativo y estudiantes.

Delimitación del problema

Aspecto: Sistemas Informáticos

Campo: Instalación Sistema operativo

Área: Software de hacking ético

Período: 2017

Formulación del problema

¿Cómo evitar el hackeo de la información con este sistema de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red wifi del Instituto Tecnológico Bolivariano de la ciudad de Guayaquil?

Variable de la investigación

Variable independiente: Ejecución e ingreso a la red para verificar las vulnerabilidades.

Variable dependiente: Sistema de hacking ético a utilizar.

Objetivos

Objetivo general

Se Implementará un sistema o software para la ejecución de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red Wifi del Instituto Tecnológico Bolivariano.

Objetivos específicos

- Determinar los requerimientos informáticos y operativos para la implementación de un sistema de hacking ético, que optimice la prueba de amenazas, riesgos y vulnerabilidades en la red wifi del instituto tecnológico bolivariano de la ciudad de Guayaquil.
- Demostrar la factibilidad técnica, la seguridad y funcionamiento operativo del sistema operativo de hacking para controlar la determinación de amenazas, y vulnerabilidades en la red wifi.
- Brindarle al Instituto tecnológico bolivariano un sistema operativo de hacking ético para asegurar la información contra las amenazas de riesgos de hurto de información que se presentan en dicha institución.
- Analizar las técnicas de Hacking Ético aplicadas a las redes Wifi.
- Definir una guía de referencia para asegurar el acceso a la red inalámbrica Wifi.

Justificación de la Investigación

En las justificaciones interesará a los usuarios cómo funcionan los diferentes sistemas operativos que han sido detallados en el Análisis Comparativo en el cual permite, de alguna manera realizar el hacking ético para tener de forma segura la información del Instituto y así beneficiar a los usuarios de manera general con una difusión de la información ya que se incluirán las medidas correctivas para brindar un informe detallado sobre la investigación. De poder prevenir y solucionar los problemas de hackeo de la forma rápida y eficaz sin tener que realizar una inversión gigante.

Dentro del transcurso de la investigación, se analizarán las características acerca de todos los sistemas, software del hacking ético para determinar qué sistema nos convendrá utilizar para realizar las pruebas necesarias para de tal forma asegurar la red inalámbrica del Instituto Tecnológico Bolivariano. El cual servirá para proteger la seguridad de la información de los estudiantes y del personal que labora en la Institución. En un ente como lo es el Instituto Tecnológico Bolivariano, se vuelve necesario que cuenten con un sistema de hacking ético que determine las amenazas, riesgos y vulnerabilidades de la red con el fin de llevar acabo las actividades de manera segura.

Relevancia Social

En el siguiente planteamiento se pone a prueba un sistema operativo de hacking ético que permitirá en tiempo real el escaneo de las redes wifi del Instituto para el ingreso a verificar las vulnerabilidades que se encuentran en la red inalámbrica. Así mismo dicho sistema le permite al personal evitar el robo o hackeo de la información de la Institución en este caso al Tecnológico Bolivariano.

Utilidad práctica

En la siguiente investigación buscamos dar solución a las amenazas, vulnerabilidades de las redes wifi para su correcta configuración y puesta en marcha para evitar el plagio, robo y hackeo de la información.

Utilidad Metodológica

Con la Instalación del sistema de hacking ético se busca inicialmente la ejecución concreta del programa al Instituto Tecnológico Bolivariano de Tecnologías (ITB) en específico, el mismo sistema podrá ser adaptado a requerimientos de otras instituciones, compañías u entidades que desean realizar un escaneo de vulnerabilidades en las redes wifi.

Capítulo II

Marco Teórico

Fundamentación Teórica

En este capítulo se específica las técnicas que usan los cibercriminales para tomar el control de los sistemas. Esto te permitirá proponer contramedidas para mitigarlas y proteger tu red frente a ataques a la Seguridad de la Información.

El mundo informático ha evolucionado a gran escala, permitiendo hacer más fácil la vida del hombre, esta investigación pretende aplicar esta novedad a una institución haciendo más amigable la función administrativa.

Antecedentes históricos

Origen y definición del Hacking Ético

El hacking ético analiza los sistemas y programas informáticos corporativos, asumiendo el rol de un ciberdelincuente y simulando ataques a la empresa con el objetivo de evaluar el estado real de si seguridad TI. Para llevar a cabo este hacking ético es imprescindible contar con la autorización expresa de la empresa, plasmada en un contrato donde se indiquen las obligaciones que debe cumplir el auditor (confidencialidad, integridad, secreto profesional, límites de la auditoría, etc.). El resultado final indica los puntos débiles de la empresa y que pasos se deben realizar para eliminar dichas debilidades o mitigarlas caso de no ser posible su eliminación.

El objetivo es proporcionar el conocimiento para identificar cuáles elementos dentro de una red son indefensos y corregirlo antes que se convierta en una alternativa muy sencillo para hurtar información.

A estos modelos le denominamos "pen test" o "penetration test" en inglés. En español se conocen como "pruebas de penetración", cuyo objetivo es eludir las diferentes maneras en que se puede llegar a la seguridad de la red para sustraer información sensitiva de una entidad, y después informarlo a esa institución y lograr que necesiten mejorar sus sistema de seguridad.

Sistemas Operativos de Hacking ético

Un sistema operativo centrado en la seguridad es el mejor aliado de un hacker, ya que proporciona las técnicas para localizar las deficiencias de los sistemas informáticos o redes de ordenadores.

Las tecnologías informáticas en la actualidad están presentes en todos los aspectos de la sociedad. Esta presencia de la implementación de la informática, exige de control y dominio de la información que genera y utiliza sociedad contemporánea. Así pues, el objetivo es enseñar ejemplos prácticos de cómo tener acceso a ordenadores con diferentes sistemas operativos sin conocer las contraseñas de los mismos. Para lograr este objetivo, se desarrolló un análisis de los principales elementos que intervienen para acceder de forma eficiente a los sistemas operativos más socializados.

Los sistemas operativos indicados están basados en el kernel de Linux por lo que todos los sistemas operativos son libres.

Kali Linux

Kali Linux mantenido y financiado por Offensive Security Ltd. el primero en la lista. Kali Linux es una distribución Linux derivada de Debian está diseñada para examinar los foros digitales y pruebas de penetración. Fue desarrollado por Mati Aharoni y Devon Kearns de Ofensiva de Seguridad a través de la reescritura de BackTrack, tiene como propósito específico la retirada de la

compatibilidad y portabilidad de los dispositivos Android específicos, llamado Kali Linux NetHunter. Se convirtió en una plataforma de pruebas de penetración abierto Android Fuente para los dispositivos Nexus, creado como una forma de brindar seguridad en conjunto entre los miembros de la comunidad Kali “BinkyBear” y ofensivo de Seguridad. Es compatible con Wireless 802.11 inyección marco, de un solo clic configuraciones MANA Evil punto de acceso, teclado HID (Teensy como ataques), así como los ataques MITM Mala USB.

Características: BackTrack (predecesor de Kali) contenían una forma conocida como modo forense. Esta capacidad se llevó a Kali a través de arranque en vivo. Esta forma es muy común por distintas razones, como muchos usuarios de Kali ya tienen una unidad USB de arranque Kali o CD, además esta opción nos proporciona las herramientas para permitirnos la aplicación de este programa a un trabajo forense. Por otro lado, existen diferentes correcciones en este modo (forense) de la forma en cómo actúa de manera regular del sistema, como resultado del modo forense sabemos que no ejecuta el disco duro o espacio de intercambio y el montaje automático se anula. Así también, se sugiere que si Kali se va a utilizar para el análisis forense del mundo real que estas cosas se probaron en ese entorno.

Grafico 1: sistema operativo Kali Linux

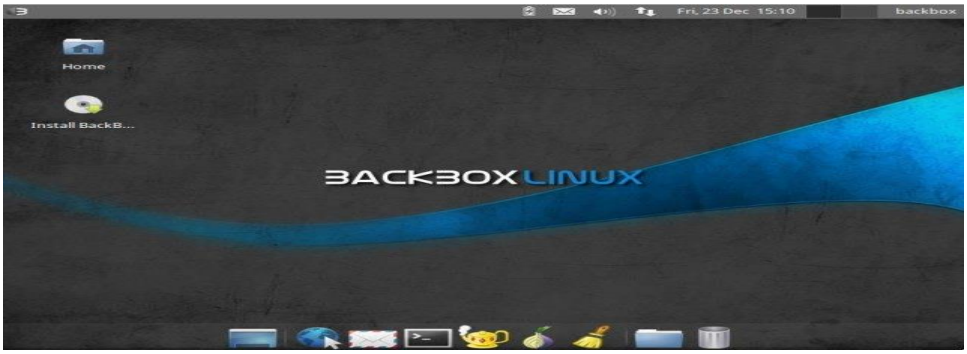
Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Back Box

Back Box se define como una valoración de tentativas de distribución de Linux y la seguridad basada en Ubuntu, la misma que está dirigida a brindarnos una comparación de sistemas informáticos de la red y kit de herramientas. Entorno de escritorio, caja posterior incluye un completo conjunto de herramientas necesarias para el hacking ético y pruebas de seguridad.

Características: Nos brinda unas implementaciones de seguridad y argumentación de las herramientas de Linux más usados, con el objetivo de incrementar una gran gama de información de los objetivos, los cuales inician en el análisis de las aplicaciones web hasta la misma red de análisis, todo esto después de realizar pruebas de resistencia a la instalación; así también, se debe incluir la evaluación de vulnerabilidades, análisis forense informático y explotación. Debemos tener en cuenta la importancia del poder de esta distribución, ya que se deriva de su núcleo repositorio Launchpad, constantemente actualizado a la última versión estable de las herramientas de hacking ético más conocidos y utilizados. La integración y el desarrollo de nuevas herramientas en la distribución sigue la comunidad de código abierto, en particular los criterios de Debian Directrices de Software Libre.

Grafico 2: sistema operativo Back Box



Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

OS Security Parrot

OS Security Parrot se denomina así a la distribución GNU / Linux que tiene como fundamento en Debian. Inicialmente, fue elaborado con la finalidad de realizar pruebas de penetración (seguridad informática), la inseguridad de Evaluación y Mitigación, Informática Forense y Anonymous Surfing, se ha desarrollado por el equipo de Frozenbox.

Loro tiene como sustento la rama estable (Jessie) de Debian, con un Linux 4.1 kernel endurecido personalizado con una rama grsecurity parcheado disponible. Por tal razón se continúa con un camino de desarrollo de Rolling. The es MATE, tenedor de Gnome 2, y el gestor de pantalla por defecto es LightDM. Esta idea está certificada ser usado sobre máquinas que tienen 265MB de RAM como mínimo y es adecuado tanto para 32 bits (i386) y 64 bits (amd64), la cual tiene una edición particular que funciona en máquinas de 32 bits de edad (486). Además, el proyecto está a la disposición para Armel y armhf arquitecturas, inclusive nos brinda una edición (tanto de 32 bits y 64 bits) desarrollado para los servidores solamente para realizar pentesting nube.

Características: OS Seguridad Parrot es un sistema operativo orientado a la seguridad diseñado para Pentesting, Forense Informática, Ingeniería inversa, Hacking, pentesting Nube, privacidad / anonimato y la criptografía.

Grafico 3: sistema operativo Os Security Parrot

Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Live Hacking OS

Vivo de Hacking OS es una distribución de Linux, el cual está lleno de herramientas y utilidades para hacking ético, pruebas de penetración y verificación contramedida. Proporciona la interfaz gráfica de usuario incorporado GNOME. Hay una segunda variación disponible que sólo tiene la línea de comandos, y requiere mucho menos requisitos de hardware.

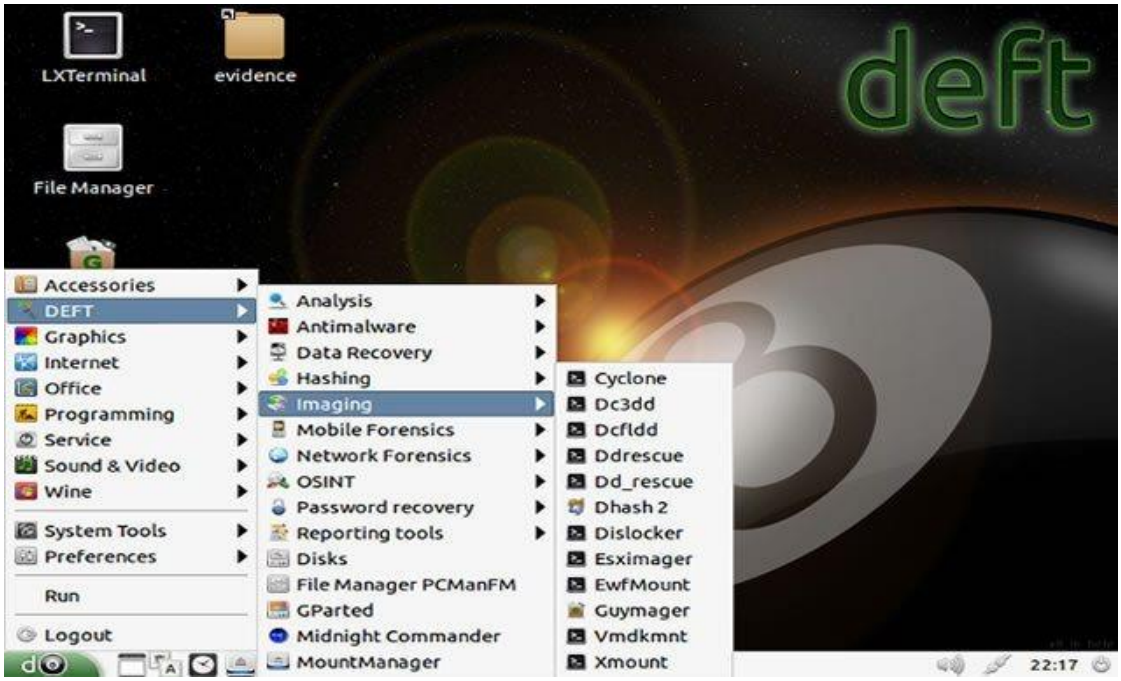
Grafico 4: sistema operativo Live Hacking Os

Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

DEFT Linux

DEFT siglas que quieren decir Evidencia Digital y Forensic Toolkit, no es otra cosa que una asignación de código abierto de Linux elaborada alrededor del DART software (Kit de herramientas de Respuesta Avanzada Digital) y tiene como finalidad el sistema operativo Ubuntu. Se elaboró desde un inicio para dar uno de los mejores análisis forenses informáticos de código abierto y opciones de respuesta para incidentes que pueden ser usados por cualquier persona, los auditores de TI, los investigadores, los militares y la policía.

Grafico 5: sistema operativo Deft Linux

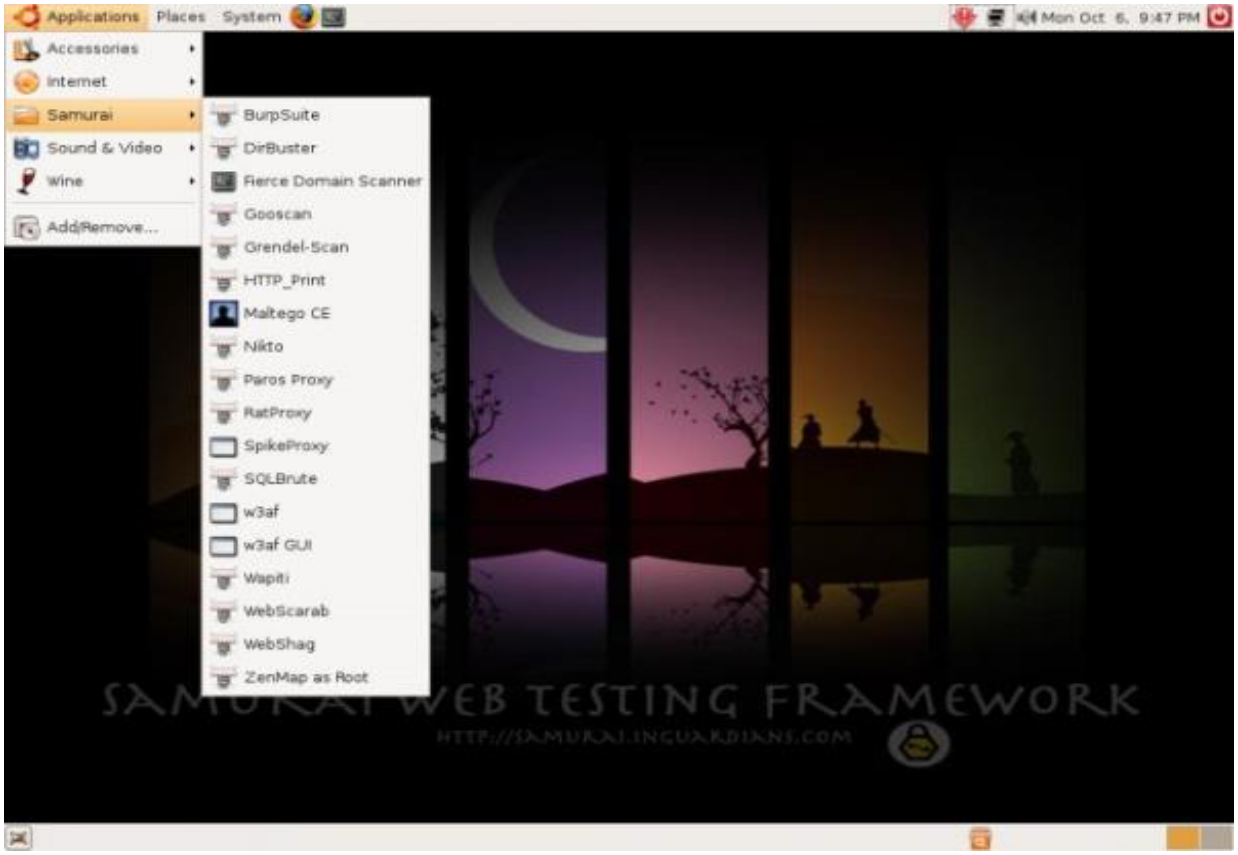


Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Samurai Web Testing Framework

La Web Testing Framework Samurai se origina en un entorno Linux en vivo, el cual ha sido pre-elaborado para funcionar como un entorno web pen-Testing. El CD nos brinda el código abierto más sobresaliente, además de instrumentos gratuitos, los cuales se basan en pruebas y los sitios web que afectan. Por lo tanto su entorno, se basa en nuestra opción de mecanismos que se van a utilizar en la práctica de seguridad. Hemos incluido las herramientas utilizadas en los cuatro pasos de un pen-test web.

Grafico 6: sistema operativo Samurai Web Testing



Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Network Security Toolkit

El kit de herramientas de seguridad de red (NST) es un Live CD que tiene su base en Linux y nos brinda un conjunto de herramientas de seguridad informática y de redes de código abierto, eso no brinda la certeza diaria y seguimiento. La distribución se puede usar como un análisis de seguridad de la red, la validación y la herramienta de monitoreo de servidores de alojamiento de máquinas virtuales.

Características: Algunas de las características que podemos realizar en el NST están disponibles a través de una interfaz web llamada NST WUI. Así tenemos algunas herramientas que se podemos usar a través de esta interfaz son nmap supervisión de puertos serie y características WPA PSK management.Other incluyen la visualización de los datos ntopng, ntop, Wireshark, traceroute, NetFlow y kismet por geo localizar las direcciones de host, dirección IPv4 conversación, datos traceroute y puntos de acceso inalámbricos y mostrarlas a través de una imagen de mapa de bits Mundial Mercator Google Earth o , un paquete de captura y el protocolo de sistema de análisis, el cual tiene como finalidad usar un navegador capaz de monitorizar hasta cuatro interfaces de red usando Wireshark, así como un sistema de detección de intrusiones basado en Snort con un backend “colector” que almacena incidentes en una base de datos MySQL. Para los desarrolladores web, también hay una consola de JavaScript con una biblioteca incorporada de objeto con funciones que ayudan al desarrollo de páginas web dinámicas.

Grafico 7: sistema operativo Network Security Toolkit

Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Bugtraq

Bugtraq es una lista de correo electrónico que se utiliza para descifrar temas de seguridad informática. En-topic donde encontramos tópicos acerca de las inseguridades, las noticias relacionados con la seguridad de los proveedores, las formas de explotación, y cómo solucionarlos. Se trata de una lista de correo de gran volumen, y casi se discuten todas las nuevas vulnerabilidades equipo there. Bugtraq es freaks y desarrolladores experimentados, está disponible en Debian, Ubuntu y openSUSE en 32 y 64 bits arquitecturas.

Grafico 8: sistema operativo Bugtraq

Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

NodeZero

NodeZero se define como un conjunto de códigos abiertos Linux cuya finalidad está basada en el núcleo operativo que nace de la distribución más popular del mundo de Linux, Ubuntu, y diseñado para utilizarse en operaciones de pruebas de penetración. Es sencilla y la podemos descargar como una imagen ISO de DVD en vivo de doble arco, que se desarrollará también en los equipos que soportan tanto de 32 bits (x86) y 64 bits (x86_64) conjunto de instrucciones. Por otra parte, nos ayuda a empezar el sistema en vivo, el menú de inicio tiene algunas opciones avanzadas, tales como la facilidad de realizar una prueba de diagnóstico de memoria del sistema, arrancar desde un disco local, inicie el instalador directamente, así como para arrancar en modo gráfico seguro, en modo texto o en modo de depuración.

Predeterminado entorno de escritorio gráfico de NodeZero es impulsado por GNOME, que utiliza la interfaz de GNOME clásico. Cuenta con un diseño de dos paneles, y usa los repositorios de software por defecto de Ubuntu. Lo importante es no olvidar que primero debe iniciar sesión en la sesión en vivo con el NodeZero nombre de usuario y sin password. With NodeZero usted tendrá acceso instantáneo a más de 300 herramientas de pruebas de penetración, así como un conjunto de servicios básicos que se necesitan en la penetración operaciones de prueba. Aplicaciones por defecto incluyen el navegador Mozilla Firefox Web, F-Spot gestor de fotos, reproductor de música Rhythmbox, editor de vídeo PiTiVi, Transmisión torrent downloader, Empatía multiprotocolo de mensajería instantánea, y la suite ofimática OpenOffice.org.

Grafico 9: sistema operativo NodeZero

Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Gentoo

Pentoo es un CD Live y Live USB el cual nos ayuda a realizar evidencias de penetración y la evaluación de la seguridad. Teniendo como principio Gentoo Linux, Gentoo se ofrece tanto como 32 y 64 bits livecd instalable. Pentoo además se puede encontrar como una superposición de una instalación Gentoo existente. Nos proporciona, además, conductores de inyección de paquetes parcheados wifi, software de craqueo GPGPU, y una serie de sistemas para pruebas de penetración y la evaluación de la seguridad. El kernel Pentoo incluye grsecurity y PAX endurecimiento y parches adicionales – con binarios compilados a partir de una cadena de utensilios endurecido con las más modernas versiones nocturnas de algunas herramientas disponibles.

Grafico 10: sistema operativo Gentoo

Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Caine:

Caine es una asignación que está dirigida a la seguridad basada en Ubuntu y la encontramos como un disco en vivo. Es sinónimo de Computer Aided y la podemos ejecutar desde el disco duro después de la instalación. Esta distribución de Linux, además, trae una gran gama de herramientas para ayudarle en el sistema.

La repartición de hacking ético nos brinda aplicaciones muy sencillas, como navegadores web, clientes de correo electrónico, editores de documentos, etc., para los propósitos de computación habituales. (Ordoñez, 2016)

Grafico 11: sistema operativo Caine

Fuente: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Internet

Una serie de elementos descentralizado de redes de comunicación interconectadas que usan la familia de protocolos TCP/IP, esto nos garantiza que, las redes físicas heterogéneas de las que está compuesta se unan para formar una red lógica única de alcance mundial. Se inició en 1969, cuando se realizó la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California (Estados Unidos).

El servicio de mayor éxito que se ha producido en internet ha sido la World Wide Web (WWW o la Web), de tal forma que relacionan ambos términos hasta confundirlos. La WWW son elementos de protocolos que ayudan de una forma muy particular, consultar remota de archivos de hipertexto. Esta fue un desarrollo posterior (1990) y utiliza internet como medio de transmisión.

Hacking

Al referirnos a la palabra "Hacking" imaginamos que nos estamos refiriendo a una persona que tiene mucha experiencia en equipos que realizan funciones de cómputo y que, por otra parte, son individuos que hacen cosas "improbables" o poco comunes para otros individuos. Además nos imaginamos seres capaces de ejecutar grandes estafas a gran escala sobre bancos y/o grandes multinacionales, eso es para la sociedad moderna, es un hacker.

Al parecer lo antes expuesto puede resultar un poco perturbador, la realidad es que el Hacking es un ente discriminado por la sociedad y se ha ido diluyendo de forma paulatina la esencia de lo que significa realmente la palabra "Hacker".

Todo esto es el resultado de la información que tergiversan los medios de comunicación en donde terminan confundiendo al delincuente con un hacker, llegando a tal punto de convertirlo en un "pirata" siendo un término muy soez y subjetivo.

Hacking ético

El Hacking ético inicialmente es la manera de nombrar a quienes utilizan sus destrezas en informática y seguridad para vulnerar las seguridades en las redes y encontrar mala seguridad, y de esta forma las informan de estas anomalías y buscar que se solucionen inmediatamente.

Lo más importante en saber centro de una red, cuáles son los elementos más fáciles de violentar y buscar la forma de solucionar el problema antes de que sea presa fácil para el robo de información, por ejemplo.

lo primero que se debe hacer es sugerir a la entidad que contrate a una empresa que brinde servicios de hacking ético, por supuesto que la misma esté certificada por organizaciones que posean un grado de reconocimiento a nivel mundial.

Un proyecto ha sido contratado por una empresa y con él se pretende mostrar a toda la dirección de la compañía el *status* actual de la seguridad de la compañía frente a todas las amenazas que hay hoy en día en Internet, centrando sus esfuerzos tanto en el factor humano como en el dimensionamiento y configuración de sus sistemas.

¿Qué se quiere decir con esto? Pues esto es un proyecto habitual de *hacking ético*. No se debe confundir con la ética hacker o con la ética informática, aunque todos estos temas van muy de la mano.

Definición

El hacking ético es una herramienta muy profesional, la cual está sumergida en el campo de la seguridad informática, y nos ayuda a evaluar el nivel de seguridad y riesgo que tienen los sistemas informáticos o los activos de una organización.

Esto ha sido impuesto por la sociedad, para diferenciar el comportamiento ético hecho por un profesional del de las acciones ilegales no autorizadas realizadas por alguien con peores intenciones.

Objetivo

Principalmente, el principio de un proceso de Ethical Hacking es la de reconocer, investigar y explotar las seguridades que posee un sistema de interés.

Además debemos sobresalir lo que posea interés, ya que si la información que contiene ese sistema tiene menos valor que el tiempo que llevaría a un hacker acceder a ella; es decir, después de algún tiempo nadie la querría.

¿Quiénes son los encargados de llevar a cabo este tipo de procesos?

Además de hackers éticos se los denomina como pentesters, y son los que están destinados a hacer pruebas de penetración o intrusión a los sistemas.

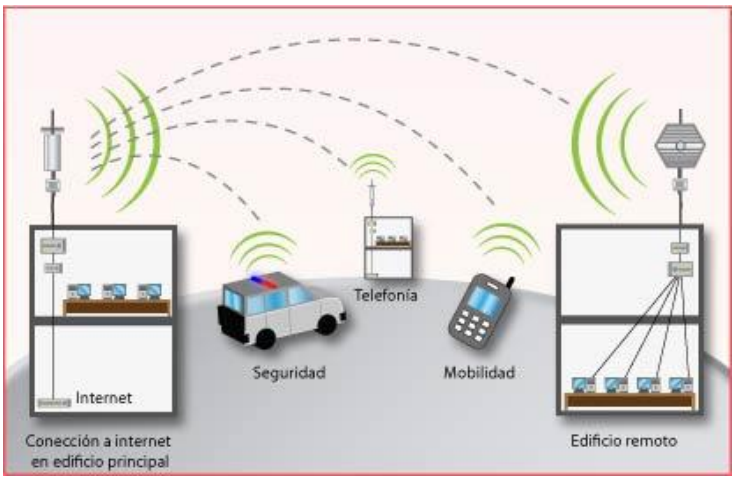
A estos hackers se les suele denominar de sombrero blanco, ya que en las películas del oeste el bueno siempre suele llevar un sombrero blanco. Otro nombre puede ser el de samurái, los cuales investigan casos sobre los derechos de privacidad. La diferencia entre estos y los de sombrero negro, es que el ataque lo hacen en nombre de sus clientes, siempre y cuando ataquen activos de estos.

Que es una Red Wifi?

Red Wifi es la realización de un sistema de red que debe tener como principio el uso y aplicación de tecnología inalámbrica **Wifi** (802.11a - 802.11b - 802.11g - 802.11n) como herramienta para que los equipos se conecten entre sí y a internet.

Otro concepto podría ser la conexión a un enchufe de red en cualquier punto dentro de la zona de **cobertura Wifi**.

Grafico 12: Esquema de una red wifi



Fuente: http://www.redeswifi.info/

Que utilidades tiene una Red Wifi?

Las Redes Wifi suele tener algunos usos prácticos para todo tipo de entidades, empresas o negocios.

- Desde cualquier punto se puede tener acceso a una red empresarial.
- Podríamos acceder a Internet sin necesidad de cables.
- Conectarse sin cables con un pc, un portátil, una pda, un teléfono móvil o videoconsola con conexión WIFI.
- Servicio de HotSpot para acceso restringido por tiempo o volumen.
- Acceder a servicios de VoIP sin cables.

Grafico 13: Antenas para Redes Wifi

Fuente: http://www.redeswifi.info/

Tipos de Redes Inalámbricas WI-FI

Las redes inalámbricas WI-FI se pueden conectar, básicamente, de 2 maneras muy diferentes:

- **Red WIFI de Infraestructura**
  Esta arquitectura se basa en 2 elementos: uno, o más Puntos de Acceso y Estaciones Cliente (fijas o móviles) que se conectan al servidor a través del Punto de Acceso
- **Red WIFI Ad-Hoc**
  Esta arquitectura se basa en 1 sólo elemento: Estaciones cliente (fijas o móviles). Estas se conectan entre sí para intercambiar información de manera inalámbrica (Ibersystems)

Caos en la seguridad Wifi: un repaso a las vulnerabilidades de WEP, WPA, y WPA2

La conexión a **redes Wifi** nos ha proporcionado unas prestaciones extraordinarias a la hora de disfrutar de todo tipo de contenidos en internet. Por fin podíamos decir adiós a los cables... o casi. Y sin embargo, esa comodidad ha estado siempre **comprometida por la seguridad de esas conexiones**, que una y otra vez ha demostrado ser insuficiente.

Las vulnerabilidades en los distintos protocolos de seguridad inalámbricos han ido apareciendo de forma sistemática, y a la desastrosa seguridad del

protocolo WEP se han sumado las vulnerabilidades que también afectaron al protocolo WPA y, por último, al protocolo WPA2 que parecía protegernos de forma razonable. **Así es como nuestras redes Wifi han ido cayendo** unas detrás de otras.

WEP, casi un juego de niños para los hackers

El lanzamiento del estándar IEEE 802.11 para conexiones inalámbricas que se ratificó en 1997 incluyo un apartado para la seguridad de esas conexiones: el llamado Wired Equivalent Privacy (WEP) curioso que el acrónimo haga uso de la palabra “Wired” y no “Wireless”, por cierto planteaba un algoritmo de seguridad para proteger la confidencialidad de los datos de forma similar a la que se proporcionaba a redes de cable.

Gráfico 14: Wired Equivalent Privacy (WEP)

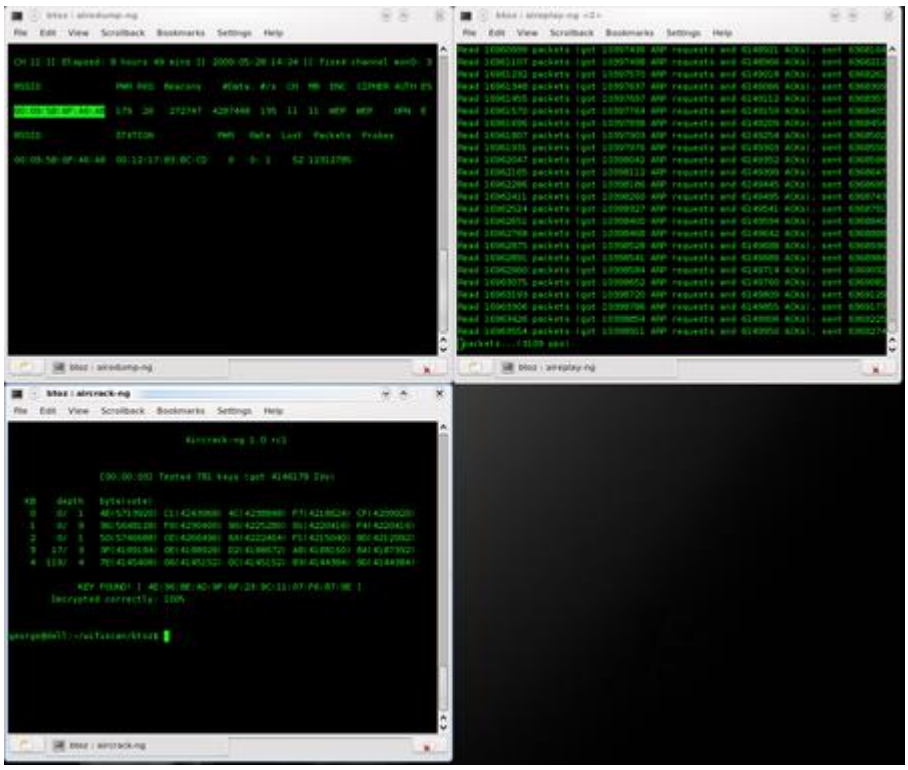
Fuente: https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2

El protocolo WEP podía hacer uso del cifrado RC4 y del mecanismo CRC-32 para la integridad, y el sistema estándar de 64 bits hacía uso de una clave de 40 bits que se concatenaba con un vector de inicialización (IV) de 24 bits para conformar la clave RC4. A cualquiera que haya usado este protocolo **le resultarán familiares esas clave WEP de 64 bits**, pero en formato hexadecimal, que hacían que al conectarnos a una red WiFi con esa seguridad

tuviésemos que introducir esos diez caracteres hexadecimales (números del 0 al 9, letras de la A la F).

En esta forma se logró informar la debilidad en 2001, cuando Scott R. Fluhrer, Itsik Mantin y Adi Shamir expresaron en un informe los estudios realizados sobre los problemas del cifrado RC4 y cómo descubrir esas claves era muy fácil y lo más impactante, es que era realizado en poco tiempo. Haciendo una investigación sobre estas conexiones e inspeccionando los paquetes que se iban intercambiando un cliente conectado a un punto de acceso. Es más, si la navegación era limitada, era posible **inyectar y "estimular" paquetes de respuesta** que servían p se hacía posible lograr que la cantidad de IVs permitiese luego encontrar la clave de acceso Wifi.

Grafico 15: archiconocida aircrack-ng



Fuente: https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2

Así fue como esta forma de ataque se convirtió en uno de los clásicos de los aficionados al hacking WiFi, y suites de seguridad como la **archiconocida aircrack-ng** que produjo crackear una conexión WiFi con el protocolo WEP en un tiempo muy corto.

Sin embargo, era muy conocida las inseguridades y, aun así las **operadoras mantuvieron su validez durante años**, predefiniendo redes WiFi en los routers que distribuían el servicio a los clientes en las que se usaba el protocolo WEP por defecto.

El propio FBI fue capaz de demostrar la facilidad que tenía violar la seguridad esas redes en 2005, pero **el verdadero detonante del caos WEP** fue la brecha de seguridad en TJ Maxx, uno de los gigantes comerciales de Estados Unidos.

En este caso un hacker llamado Albert González —capturado y condenado a 20 años de cárcel— pudo sustraerse más de 100 millones de cuentas de usuario, lo que produjo pérdidas estimadas que rondaron los 1.000 millones de dólares.

Esta situación se convirtió en el colmo del cinismo, y la industria y los usuarios lograron concienciar del peligro para empezar a limitar el uso se comenzó a del protocolo WEP por parte de fabricantes de equipos de comunicaciones y operadoras. Esta inseguridad se trató de arreglar con claves más largas de hasta 256 bits o **variaciones como WEP2 o WEPplus**, sin embargo, el protocolo que trataría de atajar los problemas —sin lograrlo— ya estaba funcionando desde hacía años. WPA se notaba a simple vista que sería la solución a nuestros problemas, finalmente se comprobó que era un error.

Redes Inalámbricas

¿Qué es una red inalámbrica?

Se denomina red inalámbrica a una red en la que dos o más terminales (ordenadores portátiles, agendas electrónicas, etc.) los cuales se pueden comunicar sin la necesidad de una conexión por cable. La característica principal de la red inalámbrica, es que las personas podemos seguir conectados aun cuando nos desplazamos dentro de una determinada área geográfica. Esta es la causa por la que usamos el término movilidad cuando se trata este tema.

Estas redes tienen como principio un enlace que usa ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías particulares que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas nos dan la facilidad que los dispositivos remotos se conecten sin ningún problema, ya se encuentren a unos metros de distancia como a varios kilómetros. Por otra parte, la instalación de estas redes no necesita alguna modificación en la infraestructura existente como pasa con las redes cableadas. Esto ha Hecho que el uso de esta tecnología se extienda con rapidez.

Sin embargo, hay algunas opciones que se deben regular en cuestión de la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida. Por este motivo, un hacker puede, con facilidad, escuchar una red si los datos que se transmiten no están codificados. Por lo

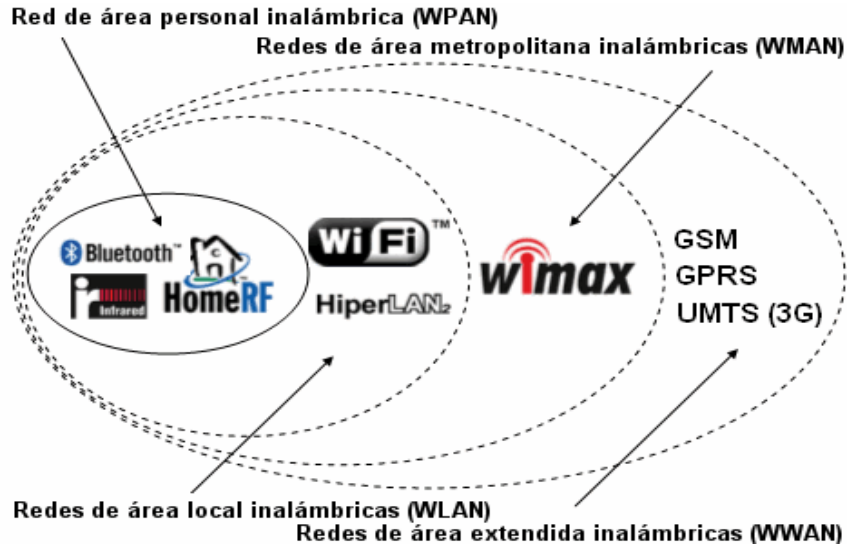
tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

Tipos de redes inalámbricas

Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red (denominada **área de cobertura** (CCM), 2017)

ax

Grafico 16: Tipo de redes



Fuente: http://es.ccm.net/contents/818-redes-inalambricas

Ventajas de las Redes Inalámbricas

- **Flexibilidad**

  Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo Por ejemplo, para hacer esta presentación se podría haber colgado la presentación de la web y haber traído simplemente el portátil y abrirla desde Internet incluso aunque la oficina en la que estuviésemos no tuviese rosetas de acceso a la red cableada.

- **Poca planificación**

  Con respecto a las redes cableadas. Antes de cablear un inmueble o unas oficinas se debe pensar mucho sobre la colocación física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas permanezcan dentro del ámbito de cobertura de la red.

- **Diseño**

  Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.

- **Robustez**

  Ante eventos de improviso que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede soportar bastante mejor este tipo de percances inesperados.

Hacker

Un hacker en el medio de la informática, es un beneficiario muy entusiasmado, curioso, dedicado, libre, arduo en el aprendizaje con enormes deseos de mejorar las habilidades y conocimientos.

Hay casos, no solamente en el área de la informática, espíritu de cultura se extiende en cualquier área del conocimiento humano donde la creatividad y la investigación son importantes.

Existen diferentes clasificaciones de "Hackers" en la medida que esta cultura se ha ido consolidando y dando a conocer, estas son:

Black hats:

Es un hacker dedicado a la obtención y explotación de vulnerabilidades en sistemas de información, base de datos, redes inalámbricas, sistemas operativos, determinados productos de software, etc.

Son también conocidos como atracadores de sistemas y especialistas en hackear la seguridad de sistemas para diversos fines (normalmente en busca de sus propios beneficios).

White hats:

Dedicado a la corrección de vulnerabilidades en el software, definición de métodos, medidas de seguridad y defensa de sistemas por medio de distintas herramientas, son aquellas personas que se dedican a la seguridad en aplicaciones, sistemas operativos y resguardo de datos sensibles, garantizado de esta forma a la confidencialidad de la información de los usuarios.

Gray hats:

Es un hacker que tiene como objetivo obtener toda la información de seguridad y detección de aspectos vulnerables para lograr defender los sistemas, así pues, se puede afirmar que un Gray hat, está nombrado como un hacker con excelentes habilidades y que sus actividades se encuentran en algún punto entre las rescatadas por los White hat hackers y los black hat hackers.

En otro término con que se suele asociar un hacker y es el de Cracker, se trata de aquellas personas que obtienen el acceso a sistemas por medio de dispositivos agresivos, como ataques de fuerza bruta para la creación de cuenta de usuario o incluso técnicas mucho más sofisticadas, como análisis y rompimiento de algoritmos de cifrado, esto entre otras cosas.

FUNDAMENTACIÓN LEGAL LEY DE PROPIEDAD INTELECTUAL DE LOS DERECHOS DE AUTOR Y DERECHOS CONEXOS

Art. 4. Se reconocen y garantizan los derechos de los autores y los derechos de los demás titulares sobre sus obras.

Art. 5. El derecho de autor nace y se protege por el solo hecho de la creación de la obra, independientemente de su mérito, destino o modo de expresión.

Art. 7. Para los efectos de este Título los términos señalados a continuación tendrán los siguientes significados.

Programa de ordenador (software): Toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un dispositivo de lectura automatizada, ordenador, o aparato electrónico o similar con capacidad de procesar información, para la realización de una función o tarea, u obtención de un resultado determinado, cualquiera que fuere su forma de expresión o fijación. El programa de ordenador comprende

también la documentación preparatoria, planes y diseños, la documentación técnica, y los manuales de uso.

Marco Legal del Software libre en Ecuador

Esta es una recopilación del marco legal correspondiente a la implementación de Software libre en el Estado Ecuatoriano. Claro está que este documento puede ser tomado por cualquier lector, revisado, observado, mejorado y utilizado como crea pertinente.

Decreto 1014

En Ecuador, se emitió el decreto No. 1014 en abril del 2008, basado en los siguientes ejes centrales.

1. Cumplimiento de recomendaciones internacionales.

* La Carta Iberoamericana de Gobierno Electrónico aprobada por la "IX Conferencia Iberoamericana de Ministros de Administración Pública y reforma del Estado", que recomienda el uso de estándares abiertos y software libre como herramientas informáticas.

2. Con los objetivos fundamentales de:

- Alcanzar la soberanía y autonomía tecnológica.
- Alcanzar un ahorro significativo de recursos públicos.

3. Plan Nacional de Gobierno electrónico (PNGE)

Este documento, en base a la Carta Iberoamericana de Gobierno electrónico del año 2007, formula 12 principios que precautelan el derecho de los ciudadanos a relacionarse con el Estado electrónicamente. Entre uno de ellos está el principio 7 de “Adecuación tecnológica” que recomiendo el uso de estándares abiertos y de software libre en razón de la seguridad, sostenibilidad a largo plazo y la socialización del conocimiento.

“Principio de adecuación tecnológica: Garantiza que las administraciones elegirán las tecnologías más adecuadas para satisfacer sus necesidades, por lo que se recomienda el uso de estándares abiertos y de software libre en razón de la seguridad, sostenibilidad a largo plazo y la socialización del conocimiento.”

CAPÍTULO III

METODOLOGÍA

Datos Principales de la Institución

Nombre completo de la Institución

Instituto Superior Tecnológico Bolivariano de Tecnología

Fecha de inicio de actividades

25 de septiembre

Política de calidad

Somos una Institución de Educación Superior acreditada, inclusiva, reconocida por su liderazgo, comprometida con la calidad académica y la excelencia en la formación de profesionales técnicos y tecnólogos críticos, innovadores y responsables con el desarrollo del entorno, el progreso económico y el bienestar social del Ecuador.

Misión

Formar profesionales técnicos y tecnólogos que aportan con excelencia académica al crecimiento global sostenible, capaces de satisfacer competencias laborales que demandan los sectores productivos y sociales.

Visión

Ser una Institución de Educación Superior acreditada con bases filosóficas, propositivas, científicas e innovadoras; formando profesionales emprendedores con sólidos conocimientos tecnológicos que aporten al desarrollo global, sustentable y protección al medio ambiente.

Estructura Organizativa

Grafico 17: Organigrama Institucional

Fuente: http://www.itb.edu.ec/organigrama

Antecedentes

El Instituto Superior Tecnológico Bolivariano de Tecnología es una Institución de Educación Superior, con Registro Institucional Nro. 09-030 otorgado por el CONESUP, de derecho público, con personería jurídica propia, y capacidad de autogestión administrativa y financiera.

Inicia con la cesión de derechos que realiza el Sr. Antonio Gregorio Gutiérrez Peñafiel del Instituto Técnico Superior Particular Mastercomp con sede en la ciudad de Milagro, creado por resolución 2763 del Ministerio de Educación y Cultura del 24 de junio de 1996 al Lsi. Manuel Roberto Tolozano Benites, posteriormente la Dirección Provincial de Educación y Cultura en acuerdo No. 0068 del 12 de octubre de 1999 autoriza el cambio de nombre a Instituto Técnico Superior Particular Megacompu.

Luego la Subsecretaria Regional de Educación con acuerdo No. 0474 del 28 de junio del 2000 reconoce el acuerdo No. 0068 expedido por la Dirección Provincial de Educación y Cultura del 12 de octubre de 1999; la cesión de derechos a favor del señor Lsi. Manuel Roberto Tolozano Benites; y, autoriza el cambio de domicilio del cantón Milagro a la ciudad de Guayaquil; reconociendo al señor Lic. Gonzalo Enrique Jarrín Mora como rector.

El 11 de diciembre del año 2001 la Junta General de Directivos y Profesores acepta la renuncia presentada por el Lic. Gonzalo Enrique Jarrín Mora a su cargo de Rector y nombra en su lugar al Lsi. Manuel Roberto Tolozano Benítez, documento que se hizo llegar al CONESUP.

El 25 de septiembre, el CONESUP con resolución RCP.S21. No.368.08 autoriza el cambio de nombre de Instituto Superior Tecnológico Megacompu a Instituto Superior Tecnológico Bolivariano de Tecnología.

Su domicilio civil es en la ciudad de Guayaquil y su ámbito en el área de docencia es la provincia del Guayas y en los de Ciencia y Tecnología y Vinculación con la Comunidad su ámbito es nacional.

Grafico 18: Ubicación

Fuente: http://www.itb.edu.ec/antecedente

Filosofía Institucional

Misión

Somos una Institución de Educación Superior acreditada, inclusiva, reconocida por su liderazgo, comprometida con la calidad académica y la excelencia en la formación de profesionales técnicos y tecnólogos críticos, innovadores y responsables con el desarrollo del entorno, el progreso económico y el bienestar social del Ecuador.

Visión

Ser una institución caracterizada por su autonomía de pensamiento y de desarrollo interno como elementos distintivos de su posicionamiento dentro del Sistema de Educación Superior del Ecuador que:

- Sea reconocida como un aliado estratégico de instituciones educativas, empresas y otros actores sociales para avanzar conjuntamente en los procesos de formación, investigación, innovación y vinculación con la sociedad.

- Implemente políticas de atracción y formación para consolidar su claustro académico y su equipo de trabajo.
- Promueva actuaciones en términos de accesibilidad, igualdad de oportunidades, políticas de acción afirmativa, sostenibilidad y cooperación internacional para el desarrollo.

Himno al ITB

I

JUVENTUD ESTUDIOSA PRESENTE

AHORA Y SIEMPRE POR LA PATRIA INMORTAL

EL FUTURO NOS GRITA MÁS FUERTE:

¡BOLIVARIANOS ESTUDIAR ES TRIUNFAR!

EL FUTURO NOS GRITA MÁS FUERTE:

¡BOLIVARIANOS ESTUDIAR ES TRIUNFAR!

II

NUESTRA PATRIA RECLAMA EL PROGRESO

Y EL PROGRESO SERÁ REALIDAD

SI ESTUDIAMOS CON FE Y MÁS ESFUERZO

CON AHÍNCO, CON PASIÓN Y VOLUNTAD

III

ADELANTE QUE EL TRIUNFO YA ES NUESTRO

DIOS NOS GUÍA EN NUESTRO CAMINAR

ADELANTE VALOR... TRIUNFAREMOS

¡BOLIVARIANOS ESTUDIAR ES TRIUNFAR!

ADELANTE VALOR... TRIUNFAREMOS

¡BOLIVARIANOS ESTUDIAR ES TRIUNFAR!

IV

JUVENTUD ESTUDIOSA PRESENTE

AHORA Y SIEMPRE POR LA PATRIA INMORTAL

EL FUTURO NOS GRITA MÁS FUERTE:

¡BOLIVARIANOS ESTUDIAR ES TRIUNFAR!

ADELANTE VALOR... TRIUNFAREMOS

¡BOLIVARIANOS ESTUDIAR ES TRIUNFAR!

Carreras

Técnico Superior en Enfermería

Técnico superior en Podología

Técnico Superior en Gerontología

Técnico Superior en Contabilidad y Auditoria

Técnico Superior en Administración de Empresas

Técnico Superior en Análisis de Sistemas

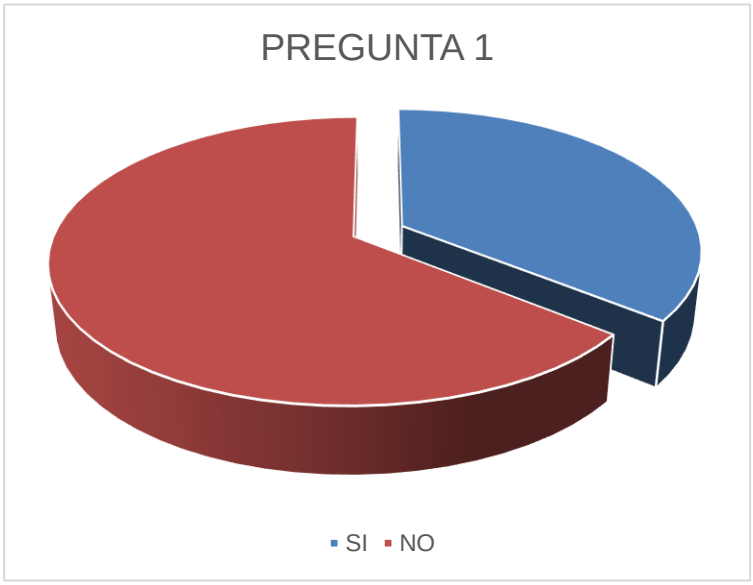
Conduce Ecuador

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

1.- ¿En qué se basa el Hacking Ético?

RESPUESTAS	*Frecuencia*	*%*
SI	25	35,71
NO	45	64,29
TOTAL	70	100



Descripción del resultado

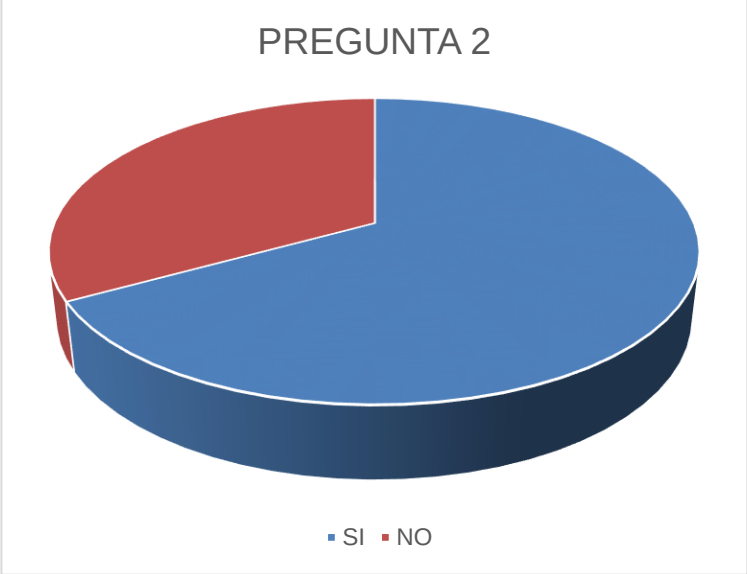
Según los 25 estudiantes encuestados dijeron que es: seguridad informática los otros 45 estudiantes no acertaron a la pregunta sobre hacking ético.

Conclusión

Según los resultados obtenidos el 35,71% que equivale a 25 personas si acertaron a la pregunta sobre que es hacking ético y el no obtuvo un 64,29% equivalente a 45 personas.

2.- ¿Cuál de los sistemas operativos investigados sea el indicado para realizar pruebas de hacking ético?

RESPUESTAS	***Frecuencia***	***%***
SI	75	66,96
NO	37	33,04
TOTAL	112	100



Descripción del resultado

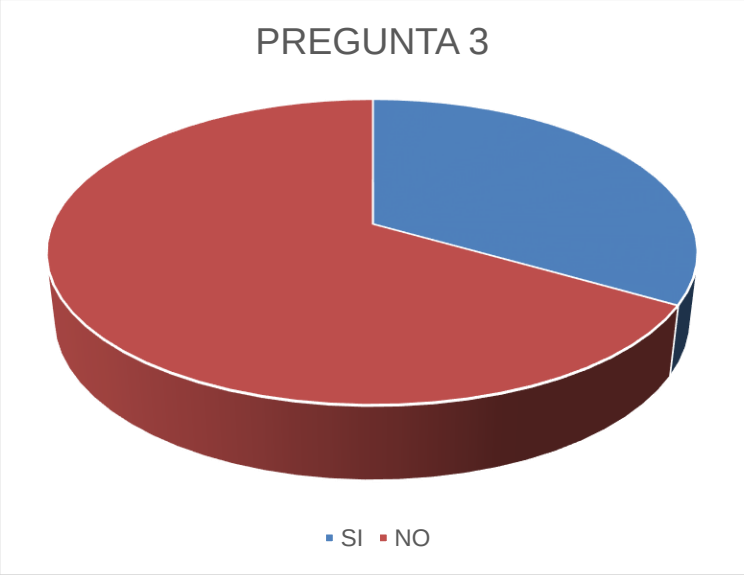
Según los datos obtenidos los 75 encuestados dicen que Kali Linux es el indicado, las 37 personas siguientes aseguraron que el resto de sistemas operativos pueden ser un poco regular.

Conclusión

El Si obtuvo un 66,96% equivalente a 75 personas que estuvieron de acuerdo con Kali Linux que es el mejor para realizar pruebas de hacking ético, en tanto que el No obtuvo un 33,04% equivalente a 37 personas que no estuvieron de acuerdo.

3.- ¿Cree usted que con el sistema operativo instalado sirva para facilitar la seguridad de los datos del estudiante?

RESPUESTAS	***Frecuencia***	***%***
SI	30	33,33
NO	60	66,67
TOTAL	90	100



Descripción del resultado

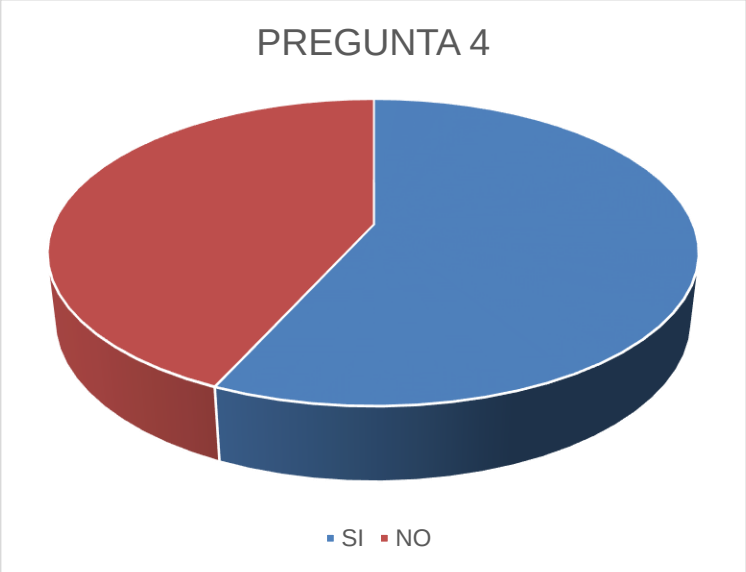
Según los datos analizados de las 30 personas entre ellas estudiantes que fueron encuestados dicen que no se sienten satisfechos con la seguridad informática que posee dicha Institución, pero las 60 personas restantes aseguraron que se sienten satisfechos con la seguridad que posee la Institución al momento de realizar algún trámite, con el sistema operativo implementado por el Tecnológico Bolivariano.

Conclusión

El 66,67% no estuvo de acuerdo con el sistema operativo instalado porque afirman que no gozan de una herramienta informática segura para dar seguridad a la información personal de dicho estudiante o empleado del tecnológico Bolivariano.

4.- ¿Cómo considera usted la visualidad del sistema operativo instalado por los administradores del Instituto Bolivariano?

RESPUESTAS	***Frecuencia***	***%***
SI	21	56,76
NO	16	43,24
TOTAL	37	100



Descripción del resultado

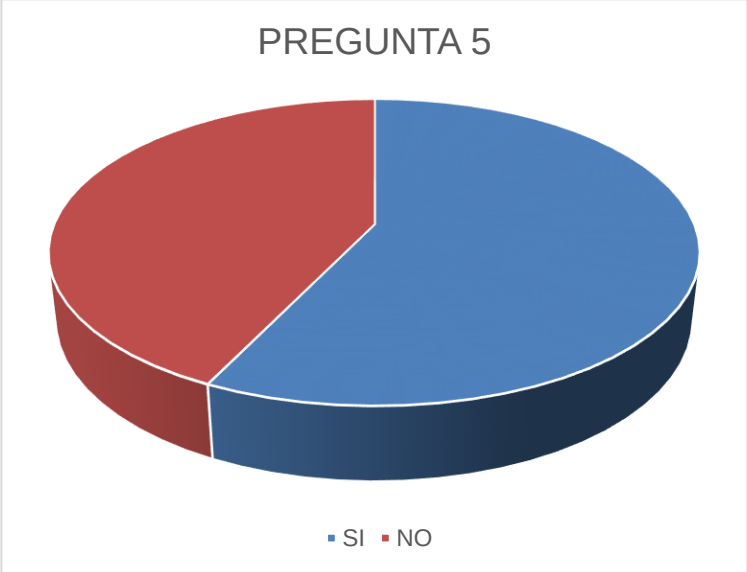
Según los 21 usuarios encuestados dicen que la visualidad es muy buena, y los 16 restantes aseguran que es malo.

Conclusión

El 56,76% estuvo de acuerdo con la visualidad del sistema instalado por el tecnológico bolivariano, mientras que el 43,24% no estuvo de acuerdo.

5.- ¿Cree usted que al momento de realizar un hackeo de la información se le brinda al estudiante o usuario toda la información completa?

RESPUESTAS	***Frecuencia***	***%***
SI	40	57,14
NO	30	42,86
TOTAL	70	100



Descripción del resultado

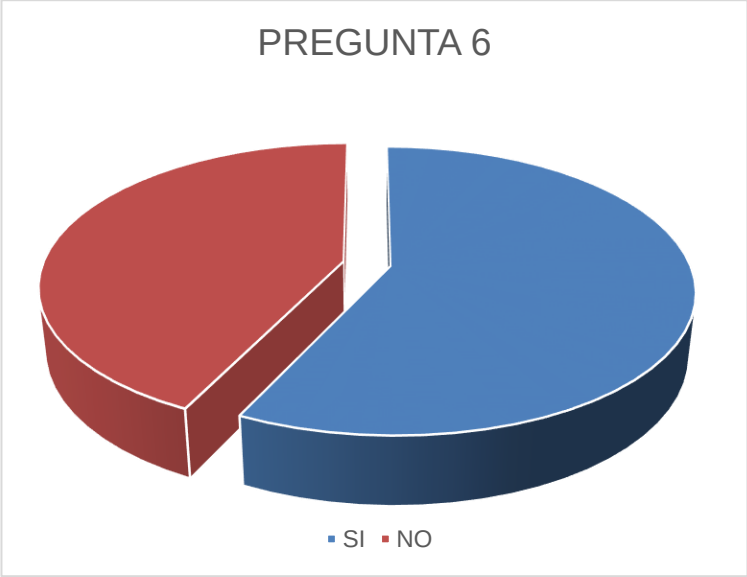
Las 70 personas que fueron encuestadas 40 de ellas estuvieron de acuerdo con dicha pregunta en tanto que las 30 personas restantes no estuvieron de acuerdo porque mencionaron que en algunas ocasiones faltaba información.

Conclusión

El SI obtuvo un 57,14% de aceptación en dicha pregunta refiriéndose al mejor servicio de información que brinda el tecnológico con este nuevo sistema operativo.

6.- ¿Cómo ayuda la parte del Internet al momento de ejecutar el sistema para realizar las pruebas correspondientes al hacking ético?

RESPUESTAS	***Frecuencia***	***%***
SI	20	57,14
NO	15	42,86
TOTAL	35	100



Descripción del resultado

Al momento de realizar la instalación las 15 personas aseguran que no es necesario contar con internet, luego el 20 restante de personas dijo que si es probable contar con internet porque sin Wifi el sistema no podría ejecutar.

Conclusión

El 57,14% dijo que si es necesario contar con conexión a internet porque si no el sistema no empezaría a funcionar al momento de ir a realizar el hacking ético.

7.- ¿Qué es una red inalámbrica?

RESPUESTAS	***Frecuencia***	***%***
SI	25	38,46
NO	40	61,54
TOTAL	65	100

Descripción del resultado

Las 65 personas encuestadas las cuales 25 dicen que es una red en la que dos o más terminales se pueden comunicar sin la necesidad de una conexión

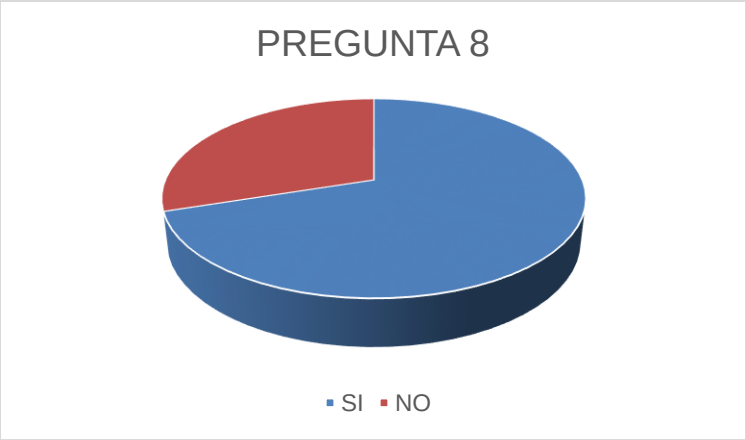
por cable, y las 40 restantes aseguran que se debe contar con una conexión por cable.

Conclusión

El sí obtuvo un 38,46% que confirman que no es necesario una conexión por cable.

8.- ¿Qué es un Hacker?

RESPUESTAS	***Frecuencia***	***%***
SI	70	70,00
NO	30	30,00
TOTAL	100	100



Descripción del resultado

Se realizó la encuesta a todo un curso de 100 estudiantes 70 de ellos sugieren que un hacker es un usuario muy curioso, dedicado, libre, comprometido al aprendizaje con enormes deseos de habilidades y conocimientos.

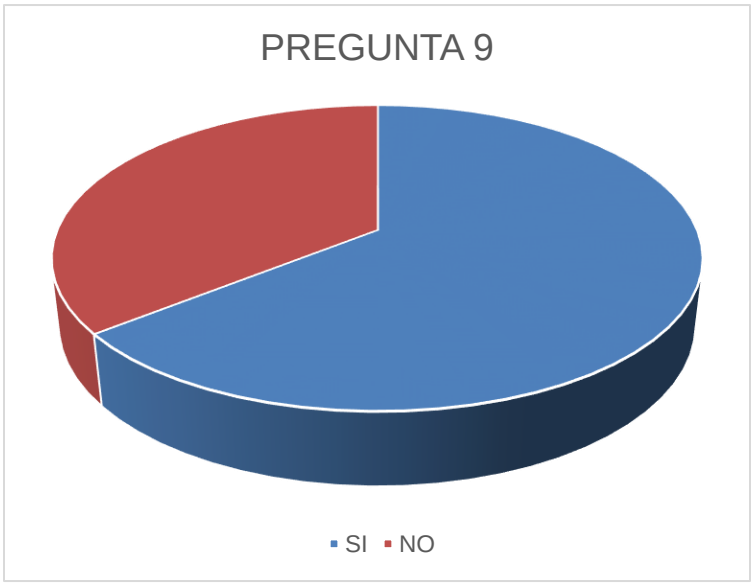
Los 30 estudiantes restantes aseguraron que es una persona que se dedica a robar información, cuentas de bancos, etc.

Conclusión

Al arrojar los resultados el SI con un 70% acertaron con la pregunta puesto que un hacker es un usuario comprometido al aprendizaje con deseos de habilidades y conocimientos.

9.- ¿Cuál es el objetivo de un Hacking ético?

RESPUESTAS	***Frecuencia***	***%***
SI	45	64,29
NO	25	35,71
TOTAL	70	100



Descripción del resultado

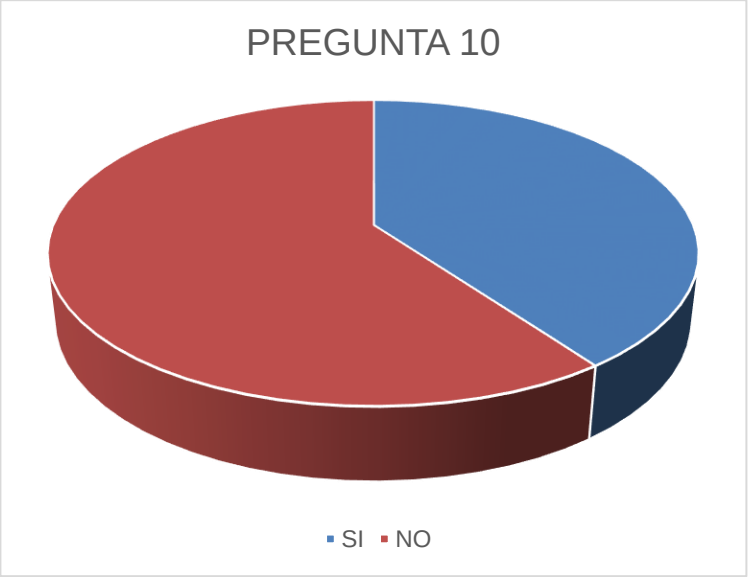
Según los 70 estudiantes encuestados 45 aseguraron que es: es la de detectar, investigar y explotar las vulnerabilidades existentes en un sistema de interés y el otro 25 dicen no saber cuál es el objetivo principal.

Conclusión

Dados los resultados se determinó que el 35,71% no sabían cuál era el objetivo principal del hacking ético

10.- ¿Cuáles son las ventajas de una red inalámbrica?

RESPUESTAS	*Frecuencia*	*%*
SI	20	40,00
NO	30	60,00
TOTAL	50	100



Descripción del resultado

Según los 50 usuarios encuestados 20 dicen que son: flexibilidad, poca planificación, diseño, el otro 30 decían no saber cuáles eran las ventajas principales de la red inalámbrica.

Conclusión

Los resultados obtenidos de esta pregunta fue un 60% a favor del NO cuyas 30 personas no supieron cuáles eran las ventajas principales de una red inalámbrica.

PLAN DE MEJORAS

DESCRIPCIÓN DE LA PROPUESTA

Se Implementará un sistema o software para la ejecución de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red Wifi del Instituto Tecnológico Bolivariano.

Plan de Ejecución

Tabla 1: Plan de Ejecución

No.	Tareas Especificas	Tareas	Recursos
1	Recolección de Información	Entrevistas al personal de Caja y secretaria	Preguntas para la encuesta
2	Realización de Gráficos	Gráficos Estadísticos según las encuestas	Microsoft Word
3	Análisis de la Encuesta	Análisis de la encuesta a los estudiantes y terceras personas	Evaluación

4	Realización de Diagramas	Diagramas de Flujo de procesos	Microsoft Word
5	Diagrama de Gantt	Detalle de actividades	Microsoft Excel

Elaborado: Félix Gonzabay

Determinación del Requerimiento

Existiendo este sistema operativo para la implementación del hacking ético se necesita una máquina virtual de

datos con las siguientes características:

- Bloqueo ante hackers falsos
- Base
- Proceso (paso a paso)

Asimismo los requerimientos mínimos para un ordenador son:

- Navegador como: Google Chrome, Mozilla e Internet Explorer.
- Disco Duro 2 GB disponibles
- Memoria RAM de 1 GB (800 MHz)

Cuadro de Costos

Tabla 2: cuadro de costos

DESCRIPCIÓN	COSTO	TIEMPO
Hackeador	$500	1 vez
Programador	$400	1 vez
Mantenimientos e implementaciones	$700	Al año
Internet	$75	Al mes
Transporte	$20	2 meses
Computadora	$280 c/u	1 vez
Tablet o Celular Smart	$160 c/u	1 vez
TOTAL	**$2135**	

Tabla: Cuadro de Costos del proyecto

Elaborado: Félix Gonzabay

Cronograma de Actividades

Tabla 3: Cronograma de actividades

Id	Nombre	Duración	Comienzo	Fin
1	**Fase 1: Análisis del proyecto**	31d		
2	**Definición del Tema**	6d		
3	Creación del tema con su situación en conflicto	2d		
4	Creación de la formulación del problema	4d		
5	**Seminario**	22d		
6	Creación de la caratula	1d		
7	Creación de los Antecedentes	2d		
8	Creación de la justificación	1d		
9	Creación de los Objetivos y Formulación	4d		
10	Creación de marco teórico	4d		
11	Creación de metodología	4d		
12	Creación de cronograma	4d		
13	Creación de recursos y bibliografía	2d		
14	**Asignación de tutor**	1d		
15	Tutor Asignado	1d		
16	**Fase 2 Diseño Trabajo Investigativo**	25d		
17	**Capítulo 1**	3d		
18	Desarrollo Formulación del Problema	2d		
19	Desarrollo de situación Actual	2d		
20	Desarrollo Delimitación del Problema	2d		
21	Desarrollo de formulación	2d		
22	Desarrollo de objetivos	1d		
23	Desarrollo de Justificación	2d		
24	**Capítulo 2**	6d		
25	Desarrollo de Marco Teórico	6d		
26	Desarrollo de Fundamento Teórico	2d		
27	Desarrollo de Fundamento Legal	3d		
28	**Capítulo 3**	7d		
29	Desarrollo de Metodológica	2d		
30	Desarrollo de Métodos de investigación	4d		
31	Población	2d		

32	Muestra	1d
33	Metodologías para propuesta	2d
34	**Capítulo 4**	14d
35	Análisis e interpretación de los resultados	3d
36	Diagramas y M.E.R	5d
37	Descripción de Pantallas	4d
38	Conclusión y Recomendaciones	2d
39	Correcciones y Mejoras	2d
40	Entrega de Proyecto	1d

Elaborado: Félix Gonzabay

Cuadro Comparativo

Tabla 4: comparación de los sistemas operativos

características	**Kali Linux**	**Back Box**	**Os Security Parrot**	**Deft Linux**	**Live Hacking**
Amplio apoyo a dispositivos inalámbricos	X				
Árbol de código abierto	x				
Facilidad a la hora de activar o reiniciar todo tipo de servicios con implicaciones.		x			
cuadro de búsqueda que rápidamente se va convirtiendo en el estándar de las distribuciones que usan este tipo de entorno		x			
proporciona una mejor experiencia con las pruebas de seguridad e intrusión			x		
Basada en Ubuntu 11.10				x	
está diseñado para la piratería ética					x

Características	Bugtraq	Samurai Web	Gentoo	NodeZero	Network Security
Tiene una amplia gama de penetración, forense y herramientas de laboratorio.	x				
Entorno de trabajo basado en GNU/Linux Ubuntu, que ha sido pre-configurado para llevar a cabo test de penetración a aplicativos Web.		x			
Es que las versiones de software se actualizan de forma continua, a diferencia de otras distribuciones donde los paquetes pasan meses en pruebas.			x		
Diseñado como un sistema operativo completo que también puede ser utilizado para pentesting				x	
Está diseñado para realizar pruebas de hacking ético					x

CONCLUSIONES

Se logró mejorar la seguridad de la información de los estudiantes del Instituto Tecnológico Bolivariano y del personal que labora en dicha institución, para así brindarle un mejor servicio al momento de requerir información o de realizar cualquier trámite que necesite el estudiante o terceras personas.

Utilizando el sistema operativo Kali Linux para asegurar los datos, información que posee el Instituto; además usamos métodos de investigación para centrarnos en el objetivo de acuerdo a la necesidad así como fue la encuesta realizada a estudiantes y personas que se encontraban al momento de llevar a cabo dicha encuesta.

Con la implementación del sistema operativo se cumplió con los requerimientos del alumno, además gracias a la instalación del sistema se brinda un seguimiento seguro y oportuno desde cualquier tipo de computadora y en cualquier hora.

Toda acción de un ser humano, acarrea diferentes perspectivas éticas, malas y buenas; Por lo tanto, es imprescindible que el Hacker posea una éticaque brinde otro punto de vista en las personas que dedican su vida profesional a vulnerar sistemas de información, para convertir esto en un método de protección, permitiendo a todas las organizaciones atacarse y poder mejorar sus soluciones.

Es importante darle un giro a la perspectiva que se tiene de los hackers, ya que no todos quieren realizar cosas negativas, ni hacerles daño a las personas. Más bien son personas que pueden solucionar muchos de nuestros problemas de tal forma que ese conocimiento sea utilizado de forma positiva para la sociedad.

RECOMENDACIONES

Se recomienda leer y entender la presente documentación ya que hemos dado especificaciones de la propuesta como el plan de ejecución para seguir con el proceso de la mejora, además se debe seguir implementando lo necesario para ir mejorando el sistema de hacking ético.

Para el correcto funcionamiento del sistema es indispensable entender la organización expuesta dando los correctos pasos para ingreso de datos. Es provechoso ejecutar el proyecto y luego realizar encuestas adjuntando el nombre de proyecto con el fin de tener la trazabilidad de toda la gestión realizada con el Instituto Tecnológico Bolivariano.

No se puede descuidar el mantenimiento del sistema para el correcto funcionamiento del sistema, además analizando las últimas actualizaciones para poderlas implementar seguida de las debidas capacitaciones al personal del Instituto y al que le competa saber el funcionamiento del sistema.

Por último, es esencial ingresar absolutamente todas las gestiones realizadas ya que mientras más datos se incluyen al sistema, más información oportuna nos brindará.

Es necesario darles la importancia que merecen las personas que se especializan en los temas de seguridad de información, ya que sobresalen a las otras ramas de la tecnología. En toda institución que se dedica a la información se debe marcar como objetivo primordial el cuidado de los sitemas que se utilizan, brindar un valor agregado a proteger sus datos, ya que son recursos muy valiosos para cada empresa.

Reconocer y auspiciara a este tipo de personas sería de gran valor y a lo largo del tiempo podría convertirse en una gran rama de la tecnología y porque no la más importante de todas.

ANEXOS

Anexo 1. PREGUNTAS PARA LA ENCUESTA

1.- ¿En qué se basa el Hacking Ético?

SI

NO

2.- ¿Cuál de los sistemas operativos investigados sea el indicado para realizar pruebas de hacking ético?

SI

NO

3.- ¿Cree usted que con el sistema operativo instalado sirva para facilitar la seguridad de los datos del estudiante?

Rápida

Tardía

4.- ¿Cómo considera usted la visualidad del sistema operativo instalado por los administradores Instituto Bolivariano?

Si

No

5.- ¿Cree usted que al momento de realizar un hackeo de la información se le brinda al estudiante o usuario toda la información completa?

Si

No

CITAS BIBLIOGRÁFICAS

Bibliografía

(es.ccm.net), C. (Noviembre de 2017). *CCM.* Obtenido de CCM: http://es.ccm.net/contents/818-redes-inalambricas

Calderon, S. (24 de mayo de 2012). *blogspot.* Obtenido de blogspot: http://hackinge.blogspot.com/2012/05/conclusiones-y-recomendaciones-sobre.html

CCM), S. C. (noviembre de 2017). *CCM.* Obtenido de CCM: http://es.ccm.net/contents/818-redes-inalambricas

CHECA, S. (3 NOVIEMBRE de ACTUALIZADO 3 NOVIEMBRE, 2017 de 2017). *locura informatica digital.* Obtenido de locura informatica digital: https://www.locurainformaticadigital.com/sistemas-operativos-hacking-etico-y-pentesting/3/

Ibersystems. (s.f.). *Ibersystems.* Obtenido de Ibersystems: http://www.redeswifi.info/

Interesante, M. (s.f.). *Muy interesante.* Obtenido de Muy interesante: https://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-una-red-wi-fi

Itb-Tics, i. A. (2015). *Instituto Tecnológico Bolivariano.* Obtenido de Instituto Tecnológico Bolivariano: http://www.itb.edu.ec/

Ordoñez, I. (17 de 03 de 2016). *Taringa.* Obtenido de Taringa: https://www.taringa.net/posts/ciencia-educacion/19336781/Top-10-sistemas-operativos-favoritos-de-los-hackers.html

Sánchez, I. (s.f.).

solutecsa. (s.f.). *glosario de informatica.* Obtenido de glosario de informatica: http://www.internetglosario.com/1131/hackingetico.html

WordPress.com. (s.f.). *Seguridad en sistemas y tecnicas del hacking*. Obtenido de Seguridad en sistemas y tecnicas del hacking: https://thehackerway.com/about/