TRABAJO ESPECIAL DE GRADO

PROPUESTA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA RED (DETECCIÓN DE INTRUSOS – REDES DE TRAMPA) CASO: INSTITUTO DE LAS ARTES ESCÉNICAS Y MUSICALES (IAEM). 2008 - 2009

Presentado ante la Ilustre
Universidad Central de Venezuela
para optar al Título de
Especialista en Comunicaciones y Redes de Comunicación de Datos

Por el Ing. César E. Vallez S.

Caracas, Agosto 2011

TRABAJO ESPECIAL DE GRADO

PROPUESTA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA RED (DETECCIÓN DE INTRUSOS – REDES DE TRAMPA) CASO: INSTITUTO DE LAS ARTES ESCÉNICAS Y MUSICALES (IAEM). 2008 - 2009

Tutor Académico: Msc. Vicenzo Mendillo

Presentado ante la Ilustre
Universidad Central de Venezuela
para optar al Título de
Especialista en Comunicaciones y Redes de Comunicación de Datos
Por el Ing. César E. Vallez S.

Caracas, Agosto 2011

CONSTANCIA DE APROBACION

Caracas, Agosto 2011

Los abajo firmantes, miembros del Jurado designado por el Consejo de Postgrado de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Ing. Cesar E. Vallez S., titulado:

“PROPUESTA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA RED (DETECCIÓN DE INTRUSOS – REDES DE TRAMPA) CASO: INSTITUTO DE LAS ARTES ESCÉNICAS Y MUSICALES (IAEM). 2008 – 2009”

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Especialista en Comunicaciones y Redes de Comunicación de Datos, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO (y obtuvo la Mención “_____”.)

_____ _____

Jurado Jurado

_____

Prof. Vicenzo Mendillo

Tutor Académico

Vallez S., César E.

PROPUESTA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA RED (DETECCIÓN DE INTRUSOS – REDES DE TRAMPA) CASO: INSTITUTO DE LAS ARTES ESCÉNICAS Y MUSICALES (IAEM). 2008 – 2009.

Tutor Académico: Vicenzo Mendillo. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Comisión de Postgrado. Especialista en Comunicaciones y Redes de Comunicación de Datos. Institución: IAEM. 2011. 100 h. + anexos.

Palabras Claves: Seguridad informática, Redes de datos, Seguridad en redes de datos, Sistemas de detección de intrusos, trampas en la red de datos, Honeynet, HoneyPot, Seguimiento ataques informáticos.

Resumen. Los dogmas estratégicos de la Seguridad Informática consisten en defender la infraestructura de la información, detectar posibles fallos en las redes de datos y reaccionar a esos fallos proactivamente. Esta investigación realiza una propuesta para la seguridad de la red, específicamente con herramientas de detección de intrusos, utilizando los honeynet como sistema aplicativo para el levantamiento y auditoría de la información. Esta tecnología ha evolucionado de manera acelerada, convirtiéndose en un poderoso instrumento de seguridad de la red en nuestra actualidad. Honeynet es un sistema que provee de servidores con información falsa, posicionándolos estratégicamente en una red, para que sean atacados por intrusos que pretendan ingresar a la red de datos, logrando así el sistema recolectar la información necesaria para proteger el resto de la red. El objetivo de esta investigación es desarrollar un estudio que describa las herramientas para implementar los honeynet y este se convierta en el apoyo a los gerentes de tecnología para entregar sus informes pertinentes. Se toma como caso de estudio una Institución del sector público que como prioridad de servicio requiere manejar información de reportes de seguridad. Metodológicamente la investigación se realiza bajo la modalidad de proyecto factible con una investigación de campo de carácter descriptivo, con una población de 10 personas para recabar la información, aplicando la técnica de la encuesta y determinando así las necesidades del caso de estudio. Para la implementación se realiza un método estructurado y paso a paso, para desarrollar la propuesta se utilizan los estándares abiertos del software libre como fundamento para su ejecución. Finalmente los resultados obtenidos, se reflejan en la documentación y registro de auditoría que son necesarios para cualquier empresa, demostrando así la factibilidad de los honeynet como herramienta para la seguridad de datos dentro de las redes de las organizaciones.

DEDICATORIA

Le dedico este Trabajo Especial de Grado a los seres más hermosos y especiales en mi vida Jeannelys de la Caridad (hija), Scarlet de los Angeles (hija), Natasha Alais (hija) y a Juleima del Carmen (esposa). Parte de mis logros son gracias a ellos.

"Como amo la libertad tengo sentimientos nobles y liberales, y si suelo ser severo, es solamente con aquellos que pretenden destruirnos."

(Carta a Juan Jurado, 8 de diciembre de 1814)

Simón Bolívar.

Capitán General de los Ejércitos y Libertador de Venezuela

RECONOCIMIENTO Y AGRADECIMIENTOS

Le agradezco a Dios Todo Poderoso.

Al alma de mi Padre en el cielo y a mi Madre por hacer de mi la persona que soy.

A Juleima (mi esposa) por apoyarme, tenerme paciencia y brindarme la virtud de su belleza, cariño, amor y comprensión.

A Flor (mi tía) por ofrecerme su apoyo y amor incondicional de madre.

A Adilia (hermana) por siempre estar en los momentos más oportunos.

A mi familia y mis amigos (los que estuvieron y los que están).

A mi tutor y profesor Vicenzo Mendillo, por su valiosa colaboración, constante asistencia y el hacer legible este documento.

A todos los profesores y especialistas técnicos que me proporcionaron las herramientas y conocimientos aquí aplicados.

Mi más sincero respeto y cordial saludo...

César Vallez. Autor

ÍNDICE GENERAL

LISTAS DE TABLAS

TABLA Pág.

LISTAS DE FIGURAS

INTRODUCCION

El uso creciente de los sistemas informáticos ha incrementado el problema de los accesos no autorizados y la manipulación de los datos. Es por esto que surgen los sistemas de detección de intrusos, como uno de los campos desde el punto de vista de la seguridad de datos, más investigados de los últimos años.

Sin duda alguna, muchas organizaciones consideran hoy por hoy, que las Tecnologías de la Información representan la espina dorsal de su estructura operativa, debiendo estar a la vanguardia de sus procesos de cambio, debido a que disponer de información confiable y a tiempo constituye una ventaja fundamental en el logro de sus objetivos. La identificación de los riesgos a los cuales está sujeta la información corporativa o de la empresa es de vital importancia para asegurar la integridad, usabilidad y utilidad de la misma.

La primera regla de seguridad que debemos tener en cuenta, es evitar las vulnerabilidades. Todo administrador de la red, debe tener instalado en sus sistemas los últimos parches de seguridad, deshabilitar todos los servicios que no necesite y mantener una configuración cuidadosamente estudiada para hacerle el trabajo más difícil a los posibles atacantes de la red, sin embargo en ocasiones esto no es suficiente para los hackers que logran burlar los dispositivos de seguridad de la red penetrando y haciendo estragos con la información contenida en los servidores de distintas organizaciones. Es justamente allí, donde otra herramienta sale a la luz para su implementación y utilidad llamada honeynet que se hace efectiva justo cuando el atacante piensa haber ingresado a la red en cuestión y es engañado por estos servicios de conexión.

Los honeynet han demostrado su valor como herramienta de investigación en el área de la seguridad de la información. Es así como en las siguientes páginas de esta

investigación, comenzando por el capítulo I, donde se plantea el problema que dio pie a este trabajo de grado, su justificación, los objetivos, su importancia y limitaciones, para luego continuar con el capítulo II, donde se dará a conocer los antecedentes en relación a este tema y su parte teórica, es decir, los conceptos, características, tipos, funcionamiento y tecnologías implementadas para el manejo eficiente convirtiéndose en un sistema confiable para la seguridad de los servidores y un señuelo lo suficientemente engañoso para atrapar el "comportamiento" de un hacker una vez que él ha pensado haber burlado un sistema de seguridad. El capítulo III se contempla el marco metodológico, en el cual se muestra el diseño de la investigación, la población y la muestra, las técnicas e instrumentos de recolección de datos, la validez y confiabilidad de los instrumentos elaborados y la planificación temporal proyectada para la realización de este trabajo de grado.

Adicionalmente, el capítulo IV se contempla desde el punto de vista práctico, para demostrar la efectividad de las honeynet, la herramienta será instalada en un servidor Linux, el cual administrará un sistema emulador de servidores, tomando en consideración las siguientes premisas: Control de datos, captura de datos y análisis de datos. Ya para finalizar esta investigación se continúa con las conclusiones, recomendaciones, la bibliografía consultada y los anexos respectivos.

Esta investigación se realiza enfocada en un caso práctico el cual puede ser representado tanto en el sector público como privado. No obstante, la recomendación principal para todos los lectores de este documento es que se debe tener presente como prioridad principal la seguridad en la red donde accionara la factibilidad de este proyecto a fin de resguardar los servicios y los datos o activos digitales de dicha organización.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

En la actualidad existen una gama de organizaciones empresariales del sector público y privado, en las cuales las redes de tecnología son una herramienta imprescindible para la generación de sus procesos; lo que significa que alguna falla en los sistemas, puede ocasionar grandes pérdidas desde el punto de vista económico o de producción. Muchas de estas fallas se producen por falta de planificación, desde el punto de vista de la seguridad de la información y son atribuidas a los ataques informáticos en la red originados desde el interior de la organización o fuera de ella. Por esto, los equipos de trabajo en el área de tecnología han desarrollado herramientas que sirven para prevenir o detectar estos ataques que interfieren con la productividad de la red lo cual implica el entorno de la empresa.

Estos conflictos son precisamente parte del problema en las Instituciones del Estado Venezolano, donde en ocasiones se descuidan los procesos relativos a la seguridad de la información y vemos comprometida la integridad de la red, desde los servicios de navegación, como lo son las páginas web y los correos electrónicos, hasta la propia red de área local (LAN) de las Organizaciones.

Parte de esta problemática se aborda de manera específica en esta investigación, analizando determinadas herramientas de seguridad de la red, para entender el comportamiento, funcionamiento y características esenciales para su implementación. Esto generará posteriormente el análisis de una red simulada que sea semejante a la red de datos de la Institución objeto de estudio.

Por otra parte, el Instituto de Artes Escénicas y Musicales (IAEM), tiene

como una de sus metas la de ofrecer a las comunidades culturales organizadas para la música, la danza, el teatro y circo, el acompañamiento institucional que promueva e incentive estos valores de identidad nacional fortaleciendo de esta forma el desarrollo y crecimiento de la actividades culturales en nuestro país, con una política de Estado Cultural donde se pretende llevar dichas expresiones artísticas dentro y fuera de nuestras fronteras. El IAEM desde el año 2008, está poniendo en marcha un proyecto para fortalecer las herramientas tecnológicas, que permita aligerar los procesos de información y comunicación de los datos, comenzando con su sede en Caracas y con planes de expansión hacia todo el territorio nacional. En tal sentido, dicho proyecto debe enfocarse en los procesos tecnológicos para obtener resultados eficientes en cuanto a los siguientes términos:

(a) Intercambio de datos confiables y de manera segura en los aspectos relacionados con la música, la danza, el teatro y circo cultural venezolano.

(b) Integrar con el uso de herramientas tecnológicas de código abierto y de comunicaciones de datos las distintas comunidades a fines de promover la música, la danza, el teatro y circo cultural venezolano.

(c) La operatividad de las redes aplicando políticas de seguridad.

(d) Desarrollar e implementar una herramienta que permita supervisar la plataforma tecnológica desde el punto de vista de la seguridad de la red, a fin de evitar ataques o daños en la información y en caso de su ocurrencia poder determinar los factores claves que produjeron tal hecho.

En vista del alto desempeño que busca la Institución, la implementación y ejecución del proyecto tecnológico, en relación a la prestación de servicios informáticos para acompañar a las comunidades dedicadas a incrementar los valores culturales de identidad nacional, se pretende con esta investigación fortalecer los

procedimientos de seguridad informática con la implementación de varias herramientas, como por ejemplo, los Sistemas de Detección de Intrusos (IDS), los cuales se han convertido en parte esencial de las configuraciones de los sistemas de redes, ya que estos buscan detectar anomalías que signifiquen un riesgo potencial en la red de datos, como son los casos de: Escaneadores de puertos, ataques de denegación de servicios, entre otros. Adicionalmente, se indagó con el personal adscrito al área tecnológica de la Institución en función de obtener información en cuanto a las premisas siguientes:

(a) La red o plataforma de tecnología de la Institución, cuenta con sistemas instalados para el resguardo de la información contra ataques externos que pueden producirse en cualquier momento.

(b) Existen nuevos sistemas de seguridad informática, que pueden ser implementados para ayudar a proteger los datos de la red tecnológica de la Institución.

(c) La documentación de los sistemas es de carácter fundamental y obligatorio para todas las organizaciones, por lo tanto todos los sistemas de seguridad informática deben estar bien documentados a fin de resolver rápidamente en caso de que algún incidente ocurra.

Para que la red tecnológica de cualquier organización incluyendo el caso de estudio, obtenga siempre resultados eficientes, debe tener presente los riesgos informáticos latentes en el ambiente, ya sean internos o externos de la red, para poder aplicar así controles adecuados que permitan minimizar o mitigar dichos riesgos tecnológicos. De esta manera, la investigación pretende contribuir a los lineamientos estratégicos de cualquier organización, desde el punto de vista tecnológico, definiendo una metodología particular en cuanto a la detección de intrusos informáticos se refiere,

para apoyar de esta forma en la ejecución eficiente de las redes donde se implementen.

Se abordó el tema siguiendo una metodología de análisis estructurada, donde en principio se realizó una exploración para identificar los esquemas de seguridad de las redes implementadas en las Empresas, luego se determinó y evalúo los potenciales riesgos tecnológicos, a los que están expuestos los organismos, sean de carácter público o privado. Seguidamente, se levantó la información donde se identificó la estructura de red del IAEM, tomando en cuenta sus parámetros de confidencialidad, para finalizar con un estudio de las diferentes redes de trampa, en cuanto a su existencia e implementación como proyecto en distintas partes del mundo, dando así como resultado una posible solución para su implementación junto a los sistemas de seguridad dentro de la red del IAEM.

OBJETIVOS

Objetivo general

Desarrollar una propuesta que permita implementar un sistema de red de trampa (HoneyNet-Señuelo) para la seguridad de la red de datos, basada en Software Libre y que cumpla con los estándares exigidos para la seguridad informática de las empresas públicas y privadas, partiendo inicialmente del Instituto de las Artes Escénicas y Musicales (IAEM) .

Objetivos específicos

(a) Diseñar una red de trampa (HoneyNet) que permita realizar informes pertinentes y constantes para la gerencia de Tecnología de la Información de

Instituto de Artes Escénicas y Musicales (IAEM).

(b) Implementar una red de trampa (HoneyNet) en un sistema de red externo al caso de estudio a fin de ser presentado en el IAEM para su implementación.

(c) Documentar el diseño obtenido de la red de trampa (HoneyNet) en un ambiente externo para ser presentado en el IAEM para su implementación.

JUSTIFICACION

Los sistemas de red de la Institución que incluye servicios como: Página Web, correo institucional, sistemas administrativos, dominio, seguridad entre otros, necesitan estar disponibles durante las 24 horas del día, los 365 días del año, debido a que son usados por una población de usuarios finales, que involucran empleados del organismo como personas externas que tienen que ver a diario con la Institución; lo que significa que una falla en el sistema debe ser corregida de manera inmediata, a fin de seguir con la continuidad y prestación del servicio. Esto obliga a tener una administración de la red permanente que vigile y controle el sistema, a través de normas y políticas de seguridad informática y que estén enmarcados dentro de los objetivos y metas establecidas por la gerencia de tecnología de la Institución.

En este sentido, se desarrollará una herramienta de detección de intrusos para la red, que permita proteger los activos reales de la información digitalizada, tomando como premisa que la Institución objeto de estudio por pertenecer al Estado venezolano, puede ser víctima de ataques en función de retrasar, desprestigiar o incluso sabotear los objetivos y las metas de este ente gubernamental. Esto puede traer como consecuencia, el no permitir la utilización de las herramientas de tecnología instaladas para los usuarios internos o externos de la red. Recientemente, en febrero de 2011, fue víctima de un ataque informático la página web del Ministerio del Poder

Popular para la Cultura (Ver Anexo 1), lo que trajo como consecuencia la paralización del servicio web por escasas horas. Los WebMaster de dicho Ministerio una vez informados del evento procedieron de inmediato a levantar los respaldos de la página web, sin embargo no quedo información alguna de cómo o por donde ingresaron a la red de datos para influenciar negativamente el sitio web del Ministerio. Con esto el Autor pretende decir, que herramientas como los honeynet (redes de trampa) pueden ser muy efectivas a la hora de reconstruir o investigar un ingreso no autorizado, además de poder realizar informes gerenciales que permitan mantener informados a los niveles superiores de la administración de cualquier Institución o empresa que así lo solicite. En la mayoría de los casos el honeynet servirá también de señuelo para engañar al enemigo del otro lado de la red y poder analizar los medios en que estas personas acceden a los datos.

En este sentido, la labor del investigador se basó fundamentalmente en realizar una propuesta, donde se aplicarán técnicas específicas de análisis y diseño de sistemas de información, usando metodologías inherentes al campo de las comunicaciones y redes de datos y procesos analíticos precisos del área científica, lo cual representa la plataforma estructural de la carrera de ingeniería eléctrica. Esto, además de servir al investigador como una práctica real para la implantación de un sistema de seguridad informática. Adicionalmente, se podrá utilizar como guía para las nuevas generaciones de ingenieros y técnicos que emerjan del área de las comunicaciones y redes de datos.

Así mismo, luego de la implementación de este sistema, la Institución actualizará el funcionamiento en las aplicaciones de seguridad informática, desde el punto de vista práctico, las interfaces de administración para la seguridad serán más amigables y ayudarán a generar reportes tanto para el nivel operativo como de la gerencia, contribuyendo en el proceso de toma de decisiones de la Dirección de Tecnología.

ALCANCE DE LA INVESTIGACION

Para cumplir parte de los aspectos necesarios de la seguridad informática, requerido por el plan de proyecto de la Dirección de Tecnología de la Información del Instituto de Artes Escénicas y Musicales (IAEM), se pretende implementar una red de varios sistemas y aplicaciones (servidor web, servidor de base de datos, entre otros), que se utilizarán como señuelo para los atacantes anónimos de la red como por ejemplo los blackhats (especie de hacker malicioso), dicha red tendrá características similares al caso de estudio, es decir a la red tecnológica utilizada por IAEM, no haciéndola ni más segura ni menos segura que la original, es decir, se tomará el entorno de red y se colocará dentro de la red de trampa (honeynet), para determinar parte de las vulnerabilidades existentes y como mejorarlas a la hora de que un ataque a la red se lleve a cabo.

LIMITACIONES

Los obstáculos o limitantes que eventualmente pudieran presentarse en el transcurso del proyecto, son básicamente los siguientes:

Delimitación Temática: El sistema en estudio posee una escasa documentación en relación a manuales de usuario o de implementación, sin embargo, existen varios proyectos en ciertos países como EEUU, México y Brasil que tratan el tema en cuestión y sirve de referencia a está temática. Por otra parte, existe poca documentación en relación a como están implementadas las redes dentro de la Institución objeto de estudio por lo que se debe realizar un levantamiento previo de información en cuanto a la situación actual de la red.

Resistencia al cambio: Los procesos actuales son pocos funcionales, adicionalmente no hay seguimiento a las fallas generadas ni bitácoras de registros que

ayuden a crear históricos de la seguridad informática. Con la implementación del sistema, ésta cultura administrativa cambiará radicalmente por lo que puede existir cierta resistencia al cambio por los nuevos sistemas de la red y sus formas de gestionarse ante cualquier alarma de ataque informático.

Experiencia del personal de proyecto: La familiarización del investigador con los procesos actuales de la Institución pudiera generar ciertas ventajas en el inicio del proyecto, sin embargo, las responsabilidades laborales y el día a día donde se generan actividades previstas y no previstas pueden mermar el tiempo de planificación y realización del tema de estudio.

Recursos Económicos: Este tipo de recursos se encuentra limitado a los alcances económicos del investigador, la estructura de hardware y software del sistema actual y los recursos del área de tecnología del IAEM que puedan a bien disponer para la consecución de los objetivos del proyecto.

El tiempo: Por ser el tiempo un factor importante para la realización de este proyecto, reduce el margen solamente a la presentación de una propuesta. En caso de ser factible su implementación quedará a disposición de la Institución y el Investigador un posible acuerdo para su puesta en marcha.

Limitaciones Técnicas: El organismo gubernamental en estudio debe cumplir con ciertas disposiciones y normas para la adquisición y/o mantenimiento hardware y software, lo que pudiera afectar en el tiempo y en recursos operativos disponibles para el desarrollo de la propuesta. Adicionalmente, la utilización de programas basados en software libre, implica, estar al corriente de las nuevas versiones de software que liberen a la web los desarrolladores de distintos proyectos, como los de sistemas operativos, de seguridad, virtualizadores, núcleos o kernels del sistema operativo, entre otros, que pueden afectar la operatividad de determinada herramienta.

CAPITULO II

MARCO TEORICO

El marco teórico, también llamado marco referencial, tiene como finalidad dar a la investigación un sistema coordinado y coherente de conceptos y proposiciones que permitan abordar el problema, es decir, se trata de integrar el problema dentro de un ámbito donde tenga sentido, incorporando los conocimientos previos referentes al mismo y ordenándolos de modo tal que resulten útiles en obtención de los objetivos propuestos.

En el marco de la revisión conceptual de los estudios previos e investigaciones realizadas en torno al tema de estudio, varias de las tesis que sirvieron de soporte para esta investigación, coinciden en ciertas características que deben ser tratadas por los sistemas de seguridad de la información, estas incluyen la plataforma de sistema operativo a utilizar, la naturaleza de software (de carácter privativo o libre), tipos de tareas y decisiones a tomar por parte de los implementadores, las actitudes de los usuario que emplearan y monitorearan el sistema y en general los puntos de vista tecnológicos que deben mejorarse y actualizarse para la consecución de los objetivos.

ANTECEDENTES

El autor durante el proceso de esta investigación, ha conseguido determinadas investigaciones, las cuales poseen algunas similitudes que permiten darle un enfoque general al trabajo especial de grado. A continuación se mencionan algunas de ellas:

Orozco, J. (2007). Presentó una investigación titulada “Servidores trampa (honeynet) para detección de intrusos mediante el sistema operativo solaris 10”. Ante

la Universidad Metropolitana. El objetivo general de esta tesis fue realizar un estudio técnico, económico y financiero de Servidores Trampa "honeypots" para detección de intrusos mediante el Sistema Operativo Solaris 10, para así proponer un esquema general de implantación y utilización de una Red Trampa eficiente.

Los aportes según las conclusiones una vez finalizado el análisis técnico, económico y financiero del esquema de implantación de una red trampa sobre Solaris 10, se puede decir que el proyecto es factible y rentable, visto desde cualquier punto. Desde la operatividad de la red, su implementación no repercute de manera sustancial en ningunos de los elementos de red con los que se relaciona. Desde el punto de vista económico y financiero, el proyecto ofrece una tasa interna de retorno elevada y un tiempo de pago durante el primer año, esto debido a la baja inversión, comparada con la reducción de pérdidas que el esquema de seguridad genera. Algo importante que se pone de manifiesto, es la relación que existe entre esta conclusión y el desarrollo de este proyecto de investigación que se lleva a cabo únicamente con recursos económicos del investigador y que en caso de una aceptación por parte de la Institución caso de estudio, puedan relacionar los costos mínimos de inversión del proyecto con su planificación anual y ejecución presupuestaria tal cual se lo indica la ley de gastos de la administración pública.

Martins y Tome (2005), en otra investigación, presentaron ante la Universidad Metropolitana la tesis de grado "Análisis de actividades no autorizadas en redes de área local (LAN) mediante la utilización de señuelos (honeypots) montados sobre máquinas virtuales, para el diseño e implementación de sistemas de protección." Su principal objetivo es realizar un estudio de los ataques a los que son sometidas las redes informáticas y establecer normativas de seguridad capaces de protegerlas, sin comprometer la integridad u operatividad de las mismas, con una implementación de honeypots a través de la tecnología de máquinas virtuales. De esta manera, esta investigación persigue servir de apoyo en el fortalecimiento de las políticas de seguridad que sean aplicables a los activos de la red de la Universidad Metropolitana;

con el fin primordial de incrementar la confiabilidad de la conectividad y proveerle a los equipos una plataforma de conexión estable, ofreciendo herramientas para que este fortalecimiento sea continuo e ininterrumpido en el tiempo.

Una de las conclusiones más importantes de esta investigación es que se puede mejorar la seguridad de la red de la Universidad Metropolitana, mediante la implementación de un honeypot que permita estudiar, por un período de tiempo lo suficientemente largo, el comportamiento de la actividad externa de la red y de esta manera obtener resultados estadísticos confiables, que permitan identificar aquellas horas en la que se producen la menor cantidad de actividad. Con esto, se podría constituir un conjunto de reglas aplicables a los activos y servicios de red. Estas reglas permitirían la restricción del tráfico externo para dichos activos y servicios en períodos de tiempo donde no sean necesarios. Lamentablemente el período de tiempo analizado por el sistema implementado no fue lo suficientemente largo como para arrojar resultados concretos al respecto.

Esta investigación guarda relación con este estudio justamente en la aplicación de los honeypots, que pueden ser utilizados para la investigación de sitios que han sido vulnerados por atacantes de las redes de datos. Aquí se evidencia, desde el punto de vista del sector productivo de la sociedad, ya sea un campus universitario, la empresa pública o privada, o cualquier ente social dedicado a la tecnología informática, puede conformar equipos o grupos de trabajo, que pueden descubrir nuevas brechas de seguridad y desarrollen sistemas de protección más eficientes; logrando de esta manera dar un aporte a la comunidad mundial de seguridad informática.

MARCO CONCEPTUAL

A continuación, se expone un conjunto de conceptos relacionados con la investigación, los cuales ameritan destacarse a fin de lograr una mejor comprensión.

Software Libre

La definición de open source nació a partir de Bruce Perens, uno de los pioneros creadores de Debian Linux y padre de la definición de "Sistemas open source" o de "Código Abierto".

El software de open source es un estándar muy utilizado hoy en día a nivel mundial. Tiene la ventaja de ser un sistema abierto, que permite que muchos usuarios trabajen sobre un mismo proyecto simultáneamente, pudiendo mejorarlo constantemente y de manera más rápida que si estuviese restringido a unos pocos pensadores.

Esta manera de pensar fue lo que dio inicio a Linux como sistema operativo, ya que éste no fue creado por una sola persona ni una sola compañía; ha ido evolucionando y desarrollándose de manera paralela hasta lograr competir hoy en día con los gigantes de la programación cerrada, desafiándolos en lo que a ventas y número de usuarios se refiere.

Para que un sistema pueda ser calificado como "de Código Abierto", debe cumplir ciertas características o "normativas". Las que se citan a continuación han sido extraídas de Wikipedia, una enciclopedia on-line de índole gratuito:

> "Bajo la Definición open source, las licencias deben cumplir diez condiciones para ser consideradas licencias de software abierto:
>
> 1.-Libre redistribución: el software debe poder ser regalado o vendido libremente.
> 2.-Código fuente: el código fuente debe estar incluido u obtenerse libremente.
> 3.-Trabajos derivados: la redistribución de modificaciones debe estar permitida.
> 4.-Integridad del código fuente del autor: las licencias pueden requerir que las modificaciones sean redistribuidas sólo como

parches.
5.-Sin discriminación de personas o grupos: nadie puede dejarse fuera.
6.-Sin discriminación de áreas de iniciativa: los usuarios comerciales no pueden ser excluidos.
7.-Distribución de la licencia: deben aplicarse los mismos derechos a todo el que reciba el programa.
8.-La licencia no debe ser específica de un producto: el programa no puede licenciarse solo como parte de una distribución mayor.
9.-La licencia no debe restringir otro software: la licencia no puede obligar a que algún otro software que sea distribuido con el software abierto deba también ser de código abierto.
10.-La licencia debe ser tecnológicamente neutral: no debe requerirse la aceptación de la licencia por medio de un acceso por click de ratón o de otra forma específica del medio de soporte del software."

Linux

Este es un sistema operativo gratuito y de libre distribución inspirado en el sistema Unix, escrito por un estudiante finlandés llamado Linus Torvalds en 1991, a lo que luego se le sumaría la ayuda de miles de programadores en Internet. En ese momento, se ejecutaba sólo en sistemas i386 y era esencialmente un clon creado independientemente del núcleo de UNIX, con la intención de mejorar la entonces nueva arquitectura i386. Unix es un sistema operativo desarrollado en 1970, una de sus mayores ventajas es su portabilidad a diferentes tipos de ordenadores, desde computadoras de escritorio (Pcs y MAC) hasta servidores multipropósito. Unix no está pensado para ser fácil de emplear sino para ser sumamente flexible. Igualmente pasa con Linux, no es en general tan sencillo de emplear como otros sistemas operativos, aunque se están realizando grandes esfuerzos para facilitar su uso. Pese a todo, la enorme flexibilidad de Linux y su gran estabilidad (y el bajo costo), han hecho de este sistema operativo una opción para tener en cuenta por aquellos usuarios que se dediquen a trabajar a través de las redes, naveguen por internet o se dediquen a la programación. El kernel de Linux está protegido legalmente bajo la licencia pública general de GNU, permitiendo a cualquiera la libertad de modificar y redistribuir la

fuente bajo los términos de la licencia. Dado que Linux es un sistema operativo derivado de Unix, toda su estructura y modelo se encuentra orientado a la ejecución de órdenes que prestan diferentes tipos de servicio, en tal sentido, todos los procesos, servicios y aplicaciones son independientes entre sí, lo cual implica que difícilmente se presenten las fallas que originan que el sistema se interrumpa.

Distribución Ubuntu

Ubuntu es un completo sistema operativo libre creado alrededor del núcleo Linux. La comunidad de Ubuntu gira alrededor de las ideas expresadas en la Filosofía Ubuntu, las cuales expresan: Que el software debe estar disponible de forma gratuita, que las herramientas de software deben poder ser utilizadas por la gente en su idioma local, y que la gente debe tener la libertad de personalizar y alterar su software de la manera que necesiten.

Ubuntu es una ideología ética propia de Sudáfrica, que se centra en la lealtad a las personas y en las relaciones entre ellas. La palabra procede del idioma zulú y xhosa. Ubuntu se percibe como un concepto tradicional africano, siendo considerado uno de los principios fundadores de la nueva república de Sudáfrica, y está conectado a la idea de un Renacimiento Africano. Como una plataforma basada en software libre, el sistema operativo Ubuntu lleva el espíritu de Ubuntu al mundo del software.

El esquema de numeración de las versiones de Ubuntu está basado en la fecha de lanzamiento de la distribución. El número de versión proviene del año y el mes de lanzamiento, en lugar de reflejar la versión del software.

La primera distribución (Warty Warthog) fue en Octubre de 2004 así que la versión fue la 4.10. La versión antes de la más reciente es: Maverick Meerkat se distribuyó en Octubre de 2010, por lo que su número de versión es 10.10, y es justamente la que servirá como base para la investigación. La figura número 01

representa la interfaz gráfica de Ubuntu.

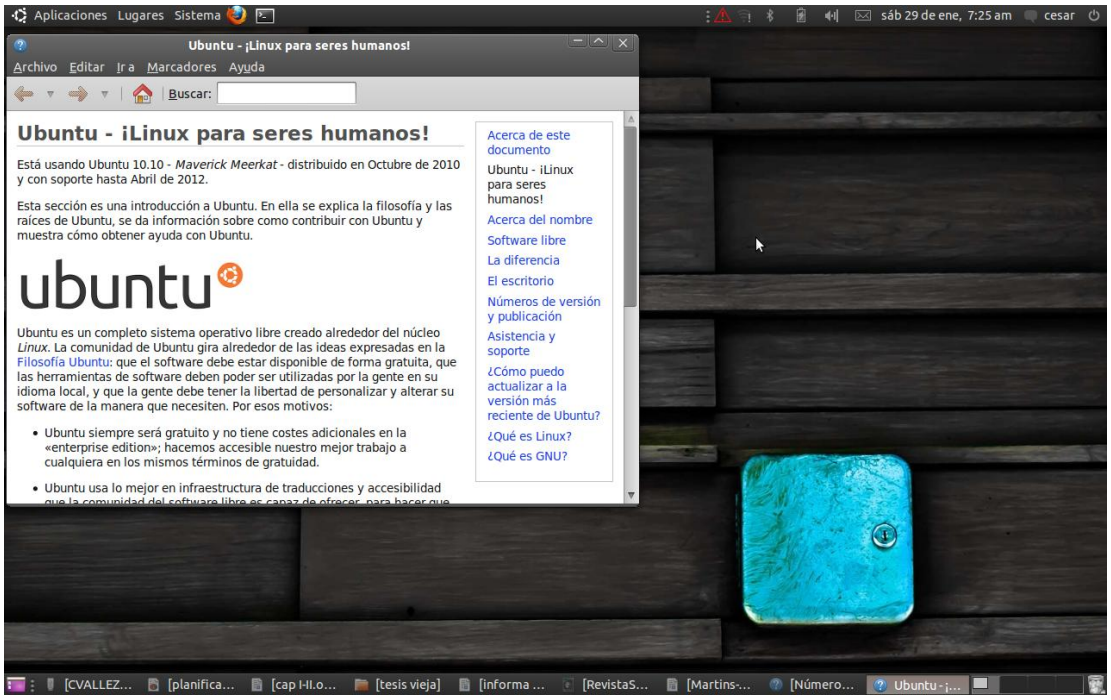


Figura 1. Interfaz gráfica de Linux (Distribución 10.10 Ubuntu)

Fuente: César Vallez (2010)

Seguridad de la Información

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio

informático, pudiendo encontrar información en diferentes medios o formas.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial.

Esta ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad.

Confidencialidad

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito sea transmitida desde el comprador al comerciante y el comerciante se conecte a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital, es uno de los pilares fundamentales de la seguridad de la información.

Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad de los sistemas es el objetivo a seguir, es decir, el sistema debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataques, como por ejemplo la denegación de servicio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para

cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, bases de datos, servidores web, entre otros, mediante el uso de clúster o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

Corta fuegos (Firewall)

Un cortafuego o firewall, es un elemento de software o hardware utilizado en una red para prevenir algunos tipos de comunicaciones prohibidas según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.

La idea principal de un firewall es crear un punto de control de la entrada y salida de tráfico de una red. Un firewall correctamente configurado es un sistema adecuado para tener una protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Su modo de funcionar es definido por la recomendación RFC 2979, la cual define las características de comportamiento y requerimientos de interoperabilidad.

Ventajas de un firewall

(a) Protege de intrusiones: El acceso a los servidores en la red sólo se hace desde máquinas autorizadas.

(b) Protección de información privada: Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

Principales Amenazas de la Seguridad Lógica

El hacker

Es una persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de "información segura".

Su formación y las habilidades que poseen les dan una experticia mayor que les permite acceder a sistemas de información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

El cracker

Se denomina así a aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un Cracker es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.

El lammer

A este grupo pertenecen aquellas personas deseosas de alcanzar el nivel de un hacker pero su poca formación y sus conocimientos les impiden realizar este sueño. Su trabajo se reduce a ejecutar programas creados por otros, a bajar, en forma indiscriminada, cualquier tipo de programa publicado en la red.

El copyhacker

Son una nueva generación de falsificadores dedicados al crackeo de Hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos a los bucaneros.

Los Copyhackers se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.

Bucaneros

Son los comerciantes de la red más no existen en ella; aunque no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios.

Phreaker

Se caracterizan por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los celulares, han tenido que ingresar también al mundo de la informática y del procesamiento de datos.

Newbie

Es el típico "novatos" de red, sin proponérselo tropieza con una página de Hacking y descubre que en ella existen áreas de descarga de buenos programas de Hackeo, baja todo lo que puede y empieza a trabajar con ellos.

Script kiddie

Denominados también “Skid kiddie”, son simples usuarios de Internet, sin conocimientos sobre Hack o Crack aunque aficionados a estos temas no los comprenden realmente, simplemente son internautas que se limitan a recopilar información de la red y a buscar programas que luego ejecutan sin los más mínimos conocimientos, infectando en algunos casos de virus a sus propios equipos. También podrían denominarse los “Pulsa Botones o Clickquiadores" de la red.

Gusanos

En informática un gusano es un virus o programa destructivo auto replicante que no altera los archivos pero reside en la memoria y se duplica a sí mismo. Los gusanos utilizan las partes automáticas de un Sistema Operativo que generalmente son invisibles al usuario. Es algo usual detectar la presencia de gusanos en un sistema cuando debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden seguir ejecutándose. Los gusanos informáticos son muy parecidos a los virus, pero los gusanos no dependen de archivos portadores para poder infectar a otros sistemas. Estos pueden modificar el sistema operativo y desconfigurarlo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades o utilizan algún tipo de ingeniería social para engañar a los usuarios de internet y poderse ejecutar.

Hijacking

Hijacking hace referencia a toda técnica ilegal que lleve consigo el apoderarse de algo, generalmente información personal, que no pertenece a quien hace uso de dichas técnicas, es por tanto un concepto muy abierto que puede aplicarse a varios

ámbitos; de esta manera se puede decir el apoderarse de módems, sesiones de terminal, conexiones de red, servicios, entre otros.

Algunos ejemplos de Hijacking

(a) Page hijacking: Secuestro de página
(b) Domain hijacking: Secuestro de dominio
(c) IP hijacking: Secuestro de una conexión TCP/IP
(d) Session hijacking: Secuestro de sesión
(e) Browser hijacking: Secuestro del navegador.
(f) Módem hijacking: Secuestro del Módem.
(g) Thread hijacking: Secuestro de un tema dentro de un foro de discusión de internet.

Hoax

Los hoax vienen del término engaño o broma, es un mensaje de correo electrónico con contenidos engañosos y normalmente distribuidos en cadena.

Su común denominador, es pedirle los distribuya "a la mayor cantidad posible de conocidos" para poderse reenviar a mayor cantidad de personas.

Esta clase de alarmas, es basadas en hechos erróneos, pero lo que es peor activan un tipo de contaminación muy diferente, propagar cientos y hasta miles de mensajes de advertencia sobre los mismos. Y aún en el caso de denuncias basadas en hecho reales, esta forma de hacerlo desvirtúa totalmente su verdadero objetivo.

Existe una variante de los hoax, llamados hoaxes, estos son falsos virus, es decir, correos electrónicos en los cuales se informa de un virus maligno, que en realidad no es cierto. Es muy importante no hacer caso de los mensajes en los cuales se dice que se borre un archivo del ordenador, puede ser gravemente dañino.

Keylogger

El keylogger es un diagnóstico utilizado en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero o enviarlas a través de internet.

El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software. Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado y al teclado mismo. Escribir aplicaciones para realizar keylogging es trivial, como cualquier programa computacional, puede ser distribuido a través de algunos troyanos o como parte de un virus informático o gusano informático.

Se dice que se puede utilizar un teclado virtual para evitar esto, ya que sólo requiere clics del ratón. Sin embargo, las aplicaciones más nuevas también registran pantallazos que anulan la seguridad de esta medida. Además, esto sería falso ya que los eventos de mensajes del teclado deben ser enviados al programa externo para que se escriba el texto, por lo que cualquier keylogger podría registrar el texto escrito mediante un teclado virtual.

Malware

La palabra malware es la abreviatura de la palabra malicious software. Este programa es sumamente peligroso para la PC, esta creado para insertar gusanos, spyware, virus, troyanos o incluso los bots, intentando conseguir algún objetivo como por ejemplo recoger información sobre el usuario de internet o sacar información de la propia PC de un usuario.

Dos tipos de malware comunes son los gusanos y los virus informáticos, este

tipo de programas tienen en común la capacidad para auto duplicarse por sí solos y de un virus o gusano terminar en 1 millón de maquinas, la diferencia que hay entre un gusano y un virus informático radica en que el gusano trabaja de forma más independiente a otros archivos, mientras que el virus depende más de un portador para poderse duplicar.

Además de los virus y gusanos dentro de este grupo podemos encontrar otros términos como: Trojan, Parasito, Adware, Spyware, Hijackers, Keyloggers, entre otros.

Caballo de Troya

Un troyano o caballo de Troya es una pieza de software dañino disfrazado de un software muy limpio. Los troyanos no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede infectar los equipos por medio del engaño.

Spyware

El spyware es todo aquel programa que se dedica recolectando información a enviar información de los usuarios. Normalmente trabajan y contaminan sistemas como lo hacen los troyanos.

Puerta trasera (backdoor)

Este es un programa que permite el acceso al sistema de la computadora esquivando los procedimientos normales de autenticación. De acuerdo a como trabajan e infectan a otros equipos, existen dos tipos de Backdoor. El primer grupo se asemeja a los troyanos, es decir, son manualmente insertados dentro de algún otro software, ejecutados por el software contaminado e infectando al sistema para poder ser

instalado permanentemente. El segundo grupo funciona de manera parecida a un gusano informático, el cuál es ejecutado como un procedimiento de inicialización del sistema y normalmente infecta por medio de gusanos que lo llevan como carga.

Exploit

Es aquel programa que ataca una vulnerabilidad particular de un Sistema Operativo. Los exploits no son necesariamente maliciosos, son normalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas malware como los gusanos informáticos.

Rootkit

Son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante.

Pharming

Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System), o en los equipos de los propios usuarios, que permite a un atacante redireccionar un nombre de dominio a otra máquina distinta. De esta forma un usuario que introduzca un determinado nombre de dominio, que haya sido redireccionado, en su explorador de internet, accederá a la página web que el atacante haya especificado para ese nombre de dominio.

El origen de la palabra pharming deriva del término phishing, utilizado para nombrar la técnica de ingeniería social, que mediante la suplantación de páginas web o

de correos electrónicos, intenta obtener detalladamente toda la información confidencial de los clientes, como nombre y apellido, contraseña, numero de tarjetas, entre otros.

Método de funcionamiento del pharming: Todos los ordenadores conectados a internet tienen una dirección IP única, que consiste en 4 números que van de 0 a 255 separados por un punto (ej: 127.0.0.1). Estas direcciones IP son comparables a las direcciones postales de las casas, o al número de los teléfonos.

Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados. O bien atacando a ordenadores, mediante la modificación del fichero presente en cualquier equipo que funcione bajo Microsoft Windows.

La técnica de pharming se utiliza normalmente para realizar ataques phishing, redireccionando el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

Anti-Pharming es el término usado para referirse a las técnicas que se utilizan para combatir el pharming. Algunos de los métodos tradicionales para combatir el pharming son: Utilización de software especializado, protección DNS y addons para los exploradores web, como por ejemplo toolbars. La protección DNS permite evitar que los propios servidores DNS sean hackeados para realizar ataques pharming. Los filtros Anti-Spam normalmente no protegen a los usuarios contra esta técnica.

Phishing

Este es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información

confidencial de forma fraudulenta, como puede ser información detallada sobre tarjetas de crédito, una contraseña u otra información bancaria.

El término phishing viene de la palabra en inglés fishing que significa *pesca* haciendo alusión al acto de pescar usuarios mediante carnadas o señuelos fabricados por los phishing cada vez más sofisticados y de este modo obtener información financiera y contraseñas. Quien lo práctica es conocido con el nombre de phisher. También se dice que el término *phishing* es la contracción de password harvesting fishing que significa: cosecha y pesca de contraseñas, aunque esto probablemente es un acrónimo retroactivo.

El estafador, mejor conocido como phisher se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea. Dado el creciente número de denuncias de incidentes relacionados con el mundo de los phishing se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica, campañas para prevenir a los usuarios y con la aplicación de medidas técnicas a los programas.

Los daños causados por el phishing oscilan entre la pérdida de contraseñas de los correos electrónicos a pérdidas económicas sustanciales. Este estilo de robo de identidad se está haciendo más popular por la facilidad con que personas confiadas normalmente revelan información personal a los phishers, incluyendo números de tarjetas de crédito y números de la seguridad social. Una vez esta información es adquirida, los phishers pueden usar datos personales para crear cuentas falsas en el nombre de la víctima, gastar el crédito de la víctima o incluso impedir a las víctimas acceder a sus propias cuentas.

Smurf

Es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar flood un objetivo (sistema atacado). En este tipo de ataque, el perpetrador envía muchas cantidades de tráfico ICMP (ping) a la dirección de broadcast, todos ellos teniendo la dirección de origen cambiada a la dirección de la víctima. Si el dispositivo de ruteo manda el tráfico a esas direcciones lo hace en capa 2 donde está la función de broadcast, y la mayoría de los host tomarán los mensajes ICMP de echo request y lo responderán, multiplicando el tráfico por cada host de la subred. Todas esas respuestas vuelven a la IP de origen que es la IP de la víctima atacada.

Spoofing

En términos del mundo de la informática hace referencia al uso de técnicas de suplantación de identidad generalmente con usos de malware o de investigación. Existen diferentes tipos de spoofing dependiendo de la tecnología a la que se refiera, como el IP spoofing, ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede generalizar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

Tipos de spoofing

Ip spoofing: Es la suplantación de IP, es decir, básicamente consiste en sustituir la IP de origen de un paquete TCP/IP por otra IP a la cual se desea suplantar.

Arp spoofing: Es la suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP falseadas con el objetivo de falsear la tabla ARP de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.

Dns spoofing: Es la suplantación de identidad por nombre de dominio. Es el falseamiento de una relación Nombre de dominio-IP ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa.

Web spoofing: Es la suplantación de una página web real. Enruta la conexión de una víctima a través de una página falsa hacia otras páginas web con el objetivo de obtener información de dicha víctima como por ejemplo, páginas web visitas, contraseñas, información subida a formularios.

Mail spoofing: Es la suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de e-mails hoax como suplemento perfecto para el uso de phising, es tan sencilla como el uso de un servidor SMTP configurado para tal fin.

Spyware

Los programas espía o spyware son aplicaciones que se encargan en recompilar información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas para poder lucrar con estas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software o para las tarjetas de crédito. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

Pueden tener acceso por ejemplo a: Dirección IP y DNS, el correo electrónico y el password, teléfono, país, páginas que se visitan, que tiempos se está en ellas y con qué frecuencia se regresa, que software está instalado en el equipo y cual se descarga,

que compras se hacen por internet, tarjeta de crédito y cuentas de banco.

Los spyware pueden ser instalados en un ordenador mediante un virus o troyano que se distribuye por correo electrónico, como el programa Magic Lantern desarrollado por el FBI, o bien puede estar oculto en la instalación de un programa aparentemente inocuo. Los programas de recolección de datos instalados con el conocimiento del usuario no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen.

Los cookies son un conocido mecanismo que almacena información sobre un usuario de internet en su propio ordenador y se suelen emplear para asignar a los visitantes de un sitio de internet un número de identificación individual para su reconocimiento subsiguiente. Sin embargo, dado que un sitio Web puede emplear un identificador cookie para construir un perfil del usuario y éste no conoce la información que se añade a este perfil, se puede considerar a los cookies una forma de spyware. Estos datos pueden ser empleados para seleccionar los anuncios publicitarios que se mostrarán al usuario, o pueden ser transmitidos a otros sitios u organizaciones.

Una vez conocidos algunos de los términos más usados para provocar problemas en la seguridad de la red de datos, se procede a continuación a ser mención de algunos de los elementos o componentes informáticos, como por ejemplo, los honeypot y los honeynet, que representan hoy por hoy una herramienta de análisis informático en lo que se refiere a la seguridad de la información. El término honeynet se origina luego de una serie de programas desarrollados en el campo práctico de la redes, como lo son los honeypot. Es por esto que para poder entender las honeynet debemos conocer primero que es un honeypot, su forma de implementación, sus características, entre otras cosas, lo cual nos facilitará el camino para poder interactuar con las herramientas del honeynet.

Definición de Honeypot

El término honeypot significa, literalmente: tarro de miel. Desde el punto de vista de la seguridad informática, se denomina honeypot al software o conjunto de computadores cuya intención es atraer a atacantes de la red, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los honeypot pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

En otras palabras un honeypot, puede entenderse como una máquina que "desea" ser atacada. Para entender esto, es necesario especificar un poco más su función dentro de una red. Un modelo básico de construcción de una intranet de una organización pequeña puede contar con un enrutador, un cortafuego, un servidor principal, diferentes estaciones de trabajo y otros recursos compartidos, así como se ilustra en la figura número 2.

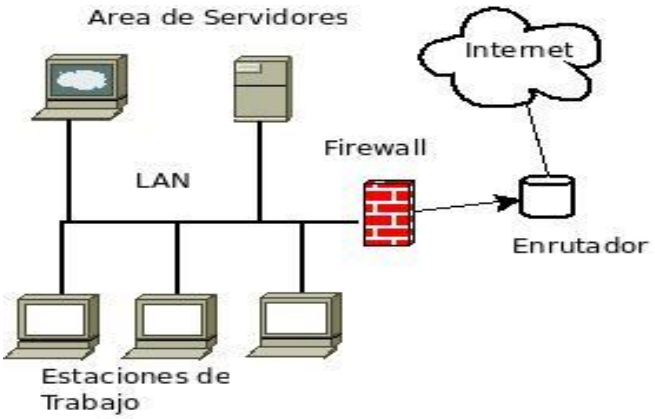


Figura 2.- Red de Área Local (LAN) de una Organización

Fuente: César Vallez (2010)

Dentro de esta red es posible ubicar un honeypot, también conocido como señuelo, una máquina dispuesta y configurada de tal manera que un atacante, bien sea interno o externo, pueda acceder de manera relativamente sencilla para realizar actividades ilícitas.

Los siguientes diagramas representan dos disposiciones diferentes de honeypots en una red de acuerdo a las necesidades de la organización:

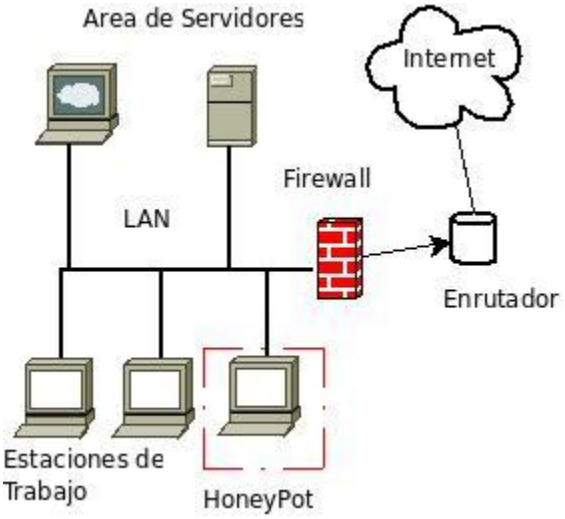


Figura 3.- Honeypot como cliente de la LAN

Fuente: César Vallez (2010)

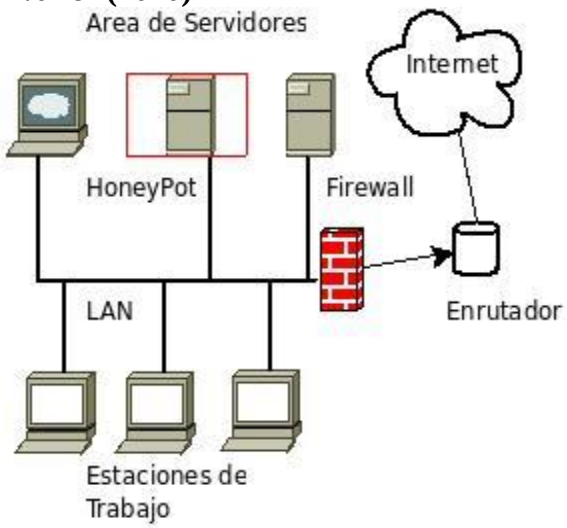


Figura 4.- Honeypot como servidor de la LAN

Fuente: César Vallez (2010)

El honeypot puede ser visto como un cliente más dentro de la red para cualquier agente externo que desconozca la verdadera estructura de la misma o puede verse como un servidor más, haciéndolo mucho más interesante para un atacante, debido a que intentará obtener información valiosa del mismo al considerarlo un servidor productivo más de la organización donde se encuentre implementado.

Es importante considerar que para un atacante de las redes, con conocimientos técnicos en seguridad y vulnerabilidades, resulta sospechoso lograr el acceso a un equipo de manera sencilla, de modo que un señuelo debe tener un sistema de seguridad que sea relativamente fácil de comprometer o violar, para no crear sospechas en la mente del atacante y que éste pueda realizar sus actividades libremente.

De esta manera, un honeypot puede definirse como un sistema de producción ficticio y controlado al que los atacantes pueden acceder de manera relativamente sencilla. Para efectos reales, y considerando el valor que puede tener una implementación de un señuelo, se puede decir que un honeypot es un recurso de seguridad cuyo valor reside en la cantidad y calidad de los ataques que reciba y de la forma en que éste sea comprometido.

Clasificación de los honeypots

Según el lugar de implementación.

Una vez definido lo que es un honeypot, resulta conveniente establecer la utilidad de su implementación. Existen dos tipos de señuelos que se han estado implementando en los ambientes de redes:

(a) Honeypots para la investigación. Son implementados por aquellas personas u organizaciones dedicadas a la investigación de la seguridad y su utilización es

básicamente para recolectar información de las actividades de los atacantes, es decir, no son implementados para proteger redes, sino que constituyen recursos educativos de naturaleza demostrativa y de investigación cuyo objetivo se centra en estudiar patrones de ataque y amenazas de todo tipo. Por lo tanto, los honeypots para la investigación se centran en recolectar información.

(b) Honeypots para la producción. Son aquellos que se utilizan para proteger a las organizaciones en ambientes reales de operación. Se implementan de manera colateral a las redes de datos o infraestructuras de tecnología y están sujetas a ataques constantes las 24 horas del día, 7 días a la semana. Se le concede cada vez más importancia debido a las herramientas de detección que pueden brindar y por la forma como pueden complementar la protección de la red y en los hosts. En contraposición a los honeypots para la investigación, los honeypots para la producción son entonces puestos en práctica en organizaciones para la protección de sus redes, siendo entonces considerados como un gran complemento a los sistemas de protección existentes.

El presente estudio implementará el uso de un honeypot para la producción, dado que estará enfocado a ser parte de un proyecto de seguridad informática de la red de cualquier organización. En nuestro caso de estudio específicamente, la implementación busca ser utilizada en una empresa pública del Estado para mitigar riesgos de ataques de la red y en caso de que suceda realizar un seguimiento y analizar los señuelos instalados.

Según el tipo de implementación.

Según la interacción que se desee por parte de los atacantes, los señuelos pueden ser clasificados en:

(a) Honeypot de baja interacción

Un honeypot de baja interacción es aquel donde los atacantes son limitados en sus acciones, dada la implementación de los servicios que utiliza el señuelo. Puede decirse que un honeypot de baja interacción estaría constituido por un equipo que emule ciertos servicios de red y una vez que los atacantes logren conectarse a estos servicios, el señuelo no les dará mayor respuesta, ya que no representa un sistema operativo o un servicio real. A modo de ejemplo, puede mencionarse el caso de un servicio de intercambio de archivos FTP, al que el atacante puede conectarse. En este caso, el sistema le solicitará información de inicio de sesión, lo que serviría para recolectar los datos usados por el intruso, quien utilizando un ataque de fuerza bruta, intentará ganar acceso al sistema. Su interacción con el servidor resultará limitada ya que no sería posible lograr una conexión al servicio considerando que éste sólo es una emulación (no un servicio real). De igual manera pudieran implementarse emulaciones de servicios como telnet, ssh y servicios de acceso remoto en general, entre otros.

El valor de los señuelos de baja interacción se centra en la detección de accesos ilegales, escaneos de servicios de red o intentos de conexión no autorizados. El tipo de interacción con estos señuelos representa un riesgo minimizado para cualquier red, ya que a través de ellos los atacantes no podrían ganar acceso a otros sistemas y comprometer así la seguridad del resto de los equipos.

Este tipo de señuelos son fáciles de implementar y mantener, sin embargo, dada su simplicidad, ofrecen resultados limitados y escasos; esto se debe a que, principalmente, se pueden registrar datos de naturaleza transaccional (como fecha de conexión, IP de origen del ataque, tiempo del ataque, IP y puerto de destino del ataque), que en escasas ocasiones resultan útiles para los administradores, quienes buscan reforzar sus sistemas de seguridad. Adicionalmente, estos productos están diseñados para detectar una actividad ya conocida y no sirven para explorar métodos nuevos, circunstancias únicas, o información que pueda servir para determinar los

propósitos específicos de un ataque recibido. Existen muchos productos en el mercado que pueden ser implementados como señuelos de baja interacción como BackOfficer Friendly, Specter y otros. Algunos de ellos pueden comprarse en Internet y otros son software libre (open source).

(b) Honeypot de alta interacción

Anteriormente fue definido lo que es un señuelo de baja interacción, así como sus alcances y limitaciones. Puede decirse que un señuelo de alta interacción es el complemento de uno de baja interacción. Este tipo de honeypot requiere un consumo grande de tiempo para su implementación y representa un alto riesgo para los activos de la red donde se implemente. A su vez, trae una amplia gama de información que puede ser recolectada y utilizada para los propósitos u objetivos que se persiguen en la organización. El tipo de información que se puede recaudar va desde lo más sencillo como la hora, fecha y origen del ataque hasta el contenido de la data transmitida para efectuar el ataque.

Específicamente, un honeypot de alta interacción es un sistema real, con servicios de red e información real, que ofrece a los atacantes una gran variedad de beneficios una vez que logran comprometerlo. Al decir que el señuelo contiene información real, se hace referencia a que es información que los atacantes pueden obtener al interactuar con los servicios de red, pero que no es de verdadera importancia para la organización. Las implementaciones más comunes de estos señuelos son los home-made honeypots (honeypots domésticos) y los honeyd.

Adicionalmente a estas implementaciones se encuentran las honeynets, que consisten en la disposición de varios honeypots en una red. Estas implementaciones tienen varias ventajas, características particulares y problemas que serán descritos más adelante en mayor detalle.

En vista de que el caso en estudio cuenta con los recursos de hardware necesarios para el desarrollo de una honeynet, se realizará la implementación en un ambiente simulado y muy parecido a los sistemas de red que hoy mantienen en la infraestructura de red de esa Institución. Esto significa una gran ventaja desde el punto de vista técnico debido a que dicho simulacro puede ser llevado a la realidad en cualquier instante y brindar beneficios en un tiempo cercano.

Elementos de interacción de un honeypot

Información: Esto está referido a lo que el atacante puede obtener y si logra vulnerar el sistema. Como bien se ha indicado se está en presencia de un señuelo; al igual que para la pesca, si se lanza un anzuelo al mar sin carnada difícilmente se logrará capturar algo. Por lo tanto, hay que darle algo al atacante que lo haga pensar que realmente ha tenido acceso a un equipo real, porque de lo contrario el señuelo no será efectivo en su tarea.

Existen varios elementos que pueden ser utilizados como componentes para crear un señuelo en los honeypot, entre los más comunes tenemos:

(a) **Servicios de red activos:** Si no hay presente un servicio de red para atacar, sencillamente carece de sentido atacar esa máquina.

(b) **Sistema de protección:** Puede ser un cortafuego u otro sistema de protección implementado en el equipo.

(c) **Sistemas de detección de intrusos (IDS):** Necesarios para detectar y capturar las actividades de los atacantes.

Es importante considerar que para un atacante experimentado, con conocimientos profundos en redes, seguridad y vulnerabilidades, resulta sospechoso

lograr el acceso a un equipo de manera sencilla, de modo que un señuelo debe tener en sí un sistema de seguridad que sea relativamente fácil de comprometer, para no crear sospechas en la mente del atacante y que éste pueda realizar sus actividades libremente.

De esta manera, un honeypot puede funcionar como un sistema de producción ficticio y controlado al que los atacantes pueden acceder de manera relativamente sencilla. Para efectos reales y considerando el valor que puede tener una implementación de un señuelo, se puede decir que un honeypot es un recurso de seguridad cuyo valor reside en la cantidad y calidad de los ataques que reciba y de la forma en que éste sea comprometido.

Sistema de Detección de Intrusos (IDS).

Un sistema de detección de intrusos (IDS por sus siglas en inglés) consiste en una serie de reglas programadas de manera tal que, como su nombre lo indica, detecten o prevengan actividades nocivas y hostiles en la red que están destinados a observar.

Este tipo de sistemas se encarga básicamente de identificar los ataques de acuerdo a ciertos patrones y alertar al administrador de la red acerca de dichas intrusiones. A pesar de detectarlas, debido a que su labor es únicamente la de reconocimiento de actividad hostil, sólo avisan sobre el evento producido sin ejecutar ningún tipo de acción en contra.

Los IDS, en su mayoría, poseen la característica de reconocer si los ataques producidos son de índole interno o externo a la red. Adicionalmente, almacenan la información histórica de las intrusiones con el fin de ejecutar posteriormente una auditoria, para así conocer las fuentes del ataque y tomar las acciones pertinentes contra ellas.

Los IDS se clasifican en dos grandes grupos: destinados a host y destinados a red. Los destinados a host son aquellos que monitorean la máquina donde se encuentran residentes, informando la actividad que recibe sólo dicha máquina. Por su parte, los sistemas destinados a redes, son aquellos que vigilan tanto la máquina en la que residen como todas aquellas que se encuentran conectadas a la misma red.

Otra característica para clasificar de los IDS es el tipo de detección que realizan: detección de anormalidades y detección de usos incorrectos. La detección de anormalidades consiste en detectar tráfico considerado como "sospechoso" de ser un ataque. Por otro lado, la detección de usos incorrectos consiste en delatar el tráfico que se genera en una red de manera incorrecta o que se redirecciona hacia sitios prohibidos por el administrador de la red o cualquier otro agente encargado de reglamentar la política de la red de una organización. Para los efectos del trabajo de grado, se analizarán exclusivamente los sistemas de detección de anormalidades.

Sistema de Prevención de Intrusos (IPS).

Un sistema de prevención de intrusos consiste en una combinación de un IDS con un sistema de seguridad. Esto permite al administrador detectar los ataques recibidos mientras ofrece la posibilidad de reaccionar ante ellos por un bloqueo de la comunicación al puerto referido, sea un ataque conocido o desconocido.

Las implementaciones de IPS, comúnmente denominadas NIPS (Network Intrusion Prevention Systems), consisten en dos interfaces de red, una interna y otra externa, donde la primera no es reconocida por la red externa, sino que es utilizada para distribuir los paquetes a los demás equipos de la red interna. De esta forma se tiene lo siguiente: una interfaz que interactúa con el tráfico de la red externa (podría ser Internet), detectando los diferentes ataques o intrusiones que se realizan en su

contra, para decidir si son o no rechazados; y una segunda interfaz que recibe los paquetes filtrados por la primera para ser distribuido en la red. En pocas palabras, una funciona como IDS y otra como sistema de distribución.

Puede decirse entonces que los IDS son el elemento principal de un IPS, que a su vez posee un componente de protección, como cortafuegos, permitiendo detectar y filtrar paquetes malignos que quieran abrirse camino en la red que éste vigilando.

El uso creciente de los sistemas informáticos ha incrementado el problema de los accesos no autorizados y la manipulación de datos. En esta línea de ideas surgen los sistemas de detección de intrusos, como uno de los campos más investigados en los últimos años.

Uno de los sistemas de detección de intrusos más utilizados en el entorno de software libre es el SNORT el cual es considerado un proyecto GPL. Este paquete es un SNIFFER y un IDS, diseñado de manera muy flexible y que posee características open source y freeware, lo cual lo hace una herramienta muy valiosa en el ámbito de la protección y vigilancia de las redes informáticas.

Fue desarrollado por Marty Roesch en conjunto con toda la comunidad mundial de desarrollos open source que se ha ido uniendo a su proyecto. En la actualidad, existen distintas herramientas y adiciones a este paquete, haciéndolo cada vez más versátil, cómodo y fácil de utilizar.

SNORT posee una capacidad de almacenar sus “logs” o registros de intrusiones en bases de datos, sea cual sea el tipo de servidor de las mismas, a fin de mantenerlos seguros y poder analizarlos posteriormente con la ayuda de otras herramientas. Para este proyecto, se utilizó el software WireShark sobre Linux equivalente a Snort.

CAPITULO III

Marco Metodológico

Diseño de la Investigación

El presente trabajo consiste en un proyecto factible, con rasgos reflexivos y analíticos donde se describen e identifican los elementos que intervienen en el planteamiento de la investigación, así como, la exposición de los diversos tópicos que conforman la misma. Igualmente se basa en una investigación con **diseño modalidad de campo**, debido a que permite realizar un análisis sistemático y objetivo del problema; los datos o información de interés se obtuvieron en forma directa por parte del investigador por lo cual, se puede afirmar que los mismos son originales y primarios, también tienen un **carácter descriptivo** ya que proporcionan la información necesaria de una muestra, para analizar la propuesta que permita implementar un sistema de red de trampa (HoneyNet-Señuelo) para la seguridad de la red de datos, basada en Software Libre y que cumpla con los estándares exigidos para la seguridad informática de las empresas públicas y privadas, partiendo inicialmente del Instituto de las Artes Escénicas y Musicales (IAEM).

Tipo de Investigación

De acuerdo al Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Experimental Libertador (2006), se define proyecto factible como "... la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o

necesidades de organizaciones o grupos sociales... " (p.07). Adicionalmente la investigación de campo como "... el análisis sistemáticos de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos o predecir su ocurrencia, haciendo uso de métodos característicos ... de investigación conocidos ..."(p.05).

En tal sentido, esta investigación se realiza en la modalidad de proyecto factible, en donde se elabora una propuesta sustentada en una guía viable para satisfacer las necesidades de la Institución y sus lineamientos enfocados al servicio público. Igualmente, se ha concebido dentro de la particularidad de la investigación de campo.

De acuerdo a Méndez Morales (1996), indica en relación al diseño de la investigación que "... Los estudios descriptivos son la base y punto inicial de los otros tipos y están dirigidos a determinar (como es y cómo esta) la situación de las variables, presencia o ausencia de algo" (p.40). En el caso del presente trabajo especial de grado, es de carácter descriptivo ya que se realizará un análisis sistemáticos de los problemas con el propósito de describir sus causas y efectos, entender su naturaleza y factores constituyentes y es de carácter explicativo, ya que cuando se analicen los datos obtenidos se determinarán las fallas de los problemas existentes evidenciando las posibles soluciones a los mismos.

Se puede agregar, que se realizó el estudio descriptivo seleccionando una serie de elementos que se midieron de manera independiente; su diseño fue tipo encuesta, en el cual se aplicó un instrumento de registro de medición (cuestionario), donde el personal adscrito a la oficina de tecnología del Instituto de las Artes Escénicas y Musicales (IAEM), respondieron directamente sus experiencias con respecto al motivo de esta investigación, facilitando el logro de los objetivos propuestos en este trabajo.

Método

El método a utilizar para la realización de la investigación es el cuantitativo, ya que sus resultados pueden ser medibles en términos numéricos en cuanto a cantidad de información de conexiones a la red recibidas y monitoreadas por un archivo de auditoría a través de períodos distintos de valoración. Adicionalmente, para el análisis del diseño actual se aplicará la investigación cualitativa, que se obtendrá a través de la observación "INSITU", esta información cualitativa servirá para realizar la propuesta de como presentar la información.

Población

Tamayo y Tamayo (1996), en su libro El Proceso de la Investigación Científica, define la población como "La totalidad de individuos o elementos en los cuales presentarse determinada característica susceptible de ser estudiada" (p.19). En este caso la población que ha definido el investigador estará conformada por 15 usuarios con nivel administrativo y soporte técnico sobre los servidores de la red y equipos de informática de la Institución y adscrito a la Oficina de Tecnología de la Información Instituto de las Artes Escénicas y Musicales (IAEM).

Muestra

Según el análisis de Méndez Morales (1996), en su libro Metodología de la Investigación, nos dice que la muestra es "Parte o subconjunto de la población" (p.47). En este caso el investigador representará la muestra por la misma cantidad de población, es decir, 15 personas, ya que esto representa una muestra finita y medible.

Técnicas e Instrumentos para la Recolección de Datos

Dentro de las técnicas para la recolección de datos encontramos que Sabino (1994) define la entrevista como "... desde el punto de vista del método científico es una forma específica de interacción social que tiene por objeto recolectar datos para la indagación. El investigador formula preguntas a las personas capaces de aportarle datos de interés." (p.162). Igualmente tenemos que Pérez (2002), clasifica la observación científica según los medios en "... no estructurada: Aquella en la cual el investigador reconoce, estudia y analiza los hechos de manera libre no utiliza ningún tipo de técnicas; y estructurada: Aquella que permite observar los fenómenos en forma sistemática... " y según la participación del Investigador la clasifica en "... participante: El investigador se involucra directamente con el grupo o comunidad, y no participante: El investigador está en contacto con la comunidad sin participar. Se comporta como un espectador."

Para la recolección de la información se utilizará las técnicas de entrevistas y observación no estructurada. Y de acuerdo a la participación del investigador se categoriza en no participante. La información necesaria para esta investigación fue recolectada mediante la aplicación de un instrumento de medición (cuestionario), el cual se estructuró con preguntas que corresponden a las causas de esta investigación. Las respuestas sirvieron de apoyo para verificar los objetivos planteados en este estudio.

Al mismo tiempo se realizaran recolección y revisión de la información de todas las actividades que se ejecutan en la organización con el objetivo de establecer los procesos que deben cumplir la investigación, todo esto se realizará a través de la observación "insitu".

Validez y Confiabilidad

Validez

El cuestionario antes de ser aplicado a la muestra en estudio, pasa por el proceso de validación del instrumento; la forma en que el autor plantea la validez será una evaluación previa que realizará los especialistas en el área de trabajo, es decir, el Director de la Oficina de Tecnología y el Coordinador de Redes, donde revisarán y aprobarán el instrumento a utilizarse para ser entonces aplicada en la población seleccionada.

Confiabilidad

Existen diversos procedimientos para calcular la confiabilidad de un instrumento de medición. Al respecto se refiere Hernández y Cols (1998) que el proceso test-retest: "Este procedimiento un mismo instrumento de medición es aplicado dos o más veces a un mismo grupo de personas, después de cierto periodo. Si la correlación de resultados de las diferentes aplicaciones es altamente positiva, el instrumento se considera confiable". En este caso se utilizará la medida de estabilidad, confiabilidad por test-retest.

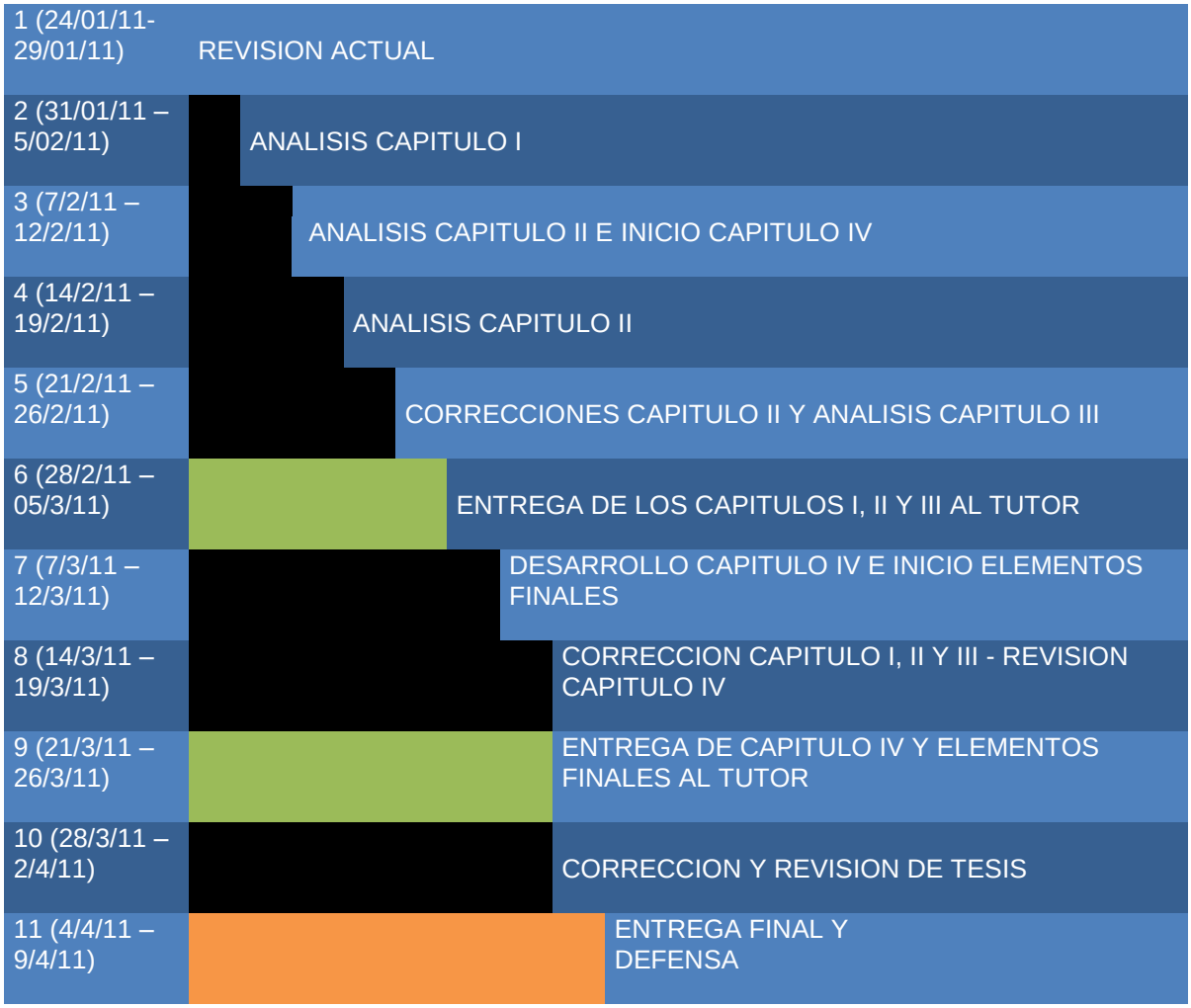
Técnicas de Análisis

Se cuantificarán los datos de acuerdo al orden de los indicadores, se establecerán las frecuencias absolutas de las respuestas conjuntamente con las observaciones en INSITU. Se elaborarán cuadros estadísticos de doble entrada presentándose los datos en forma sistemática, se tomaran en cuenta el cruce de variables utilizando el porcentaje como un estadístico simple sobre la frecuencia.

Adicionalmente se elaboraran representaciones gráficas a través de histogramas. Por último, se realizarán los análisis cualitativos de los datos arrojados en la investigación.

Plan de Trabajo de la Investigación

Tabla 01. Planificación de Entregas del Trabajo Especial de Grado



Fuente: César Vallez (2011)

Recursos y Equipos Tecnológicos

Los recursos materiales utilizados para la realización de este proyecto factible, corren por cuenta del investigador, entre los principales se destacan:

(a) Uso de 2 laptops y un computador personal, para la trascripción de los borradores y los capítulos del Trabajo de Investigación, implementación de las prácticas para poner en marcha la propuesta y ejecución de la versión definitiva del proyecto.

(b) Uso de Internet (tiempo de navegación indefinido), para la consulta de referencias electrónicas.

(c) Material digital, fotocopiado y libros especializados en la gestión de Redes para las referencias bibliográficas consultadas.

(d) Encuadernado final (preliminar y sus copias) y quema de cds conteniendo las estructura general de la tesis para su consignación ante la Escuela de Ingeniería Eléctrica.

El tiempo para la ejecución del proyecto será de un mínimo de 10 horas semanales, en días laborables, sin incluir el tiempo libre de fines de semana y días feriados que se dedicarán para la investigación y realización del trabajo.

CAPITULO IV

LA PROPUESTA

Estimación Basada en el Proceso

Selección de Tareas (Actividades)

Realizar la revisión bibliográfica estableciendo los aspectos más importantes de los sistemas de seguridad de las redes.

Identificar la organización objeto de estudio en cuanto a la configuración de las redes instaladas, que influirán sobre las bases de desarrollo de la propuesta.

Realizar un plan de actividades que permita la administración eficiente para el cambio de la aplicación actual de los servicios de la red. (Caso de Estudio)

Comunicación con los usuarios.
Predicción.
Estudio de Factibilidad Económica.
Diseño del plan general

Determinar la infraestructura y el ambiente de software actual del sistema de seguridad de la red. (Caso de Estudio)

Análisis del sistema actual
Funcionamiento

Necesidades

Limitaciones

Recursos Tecnológicos y humanos

Definir una arquitectura tecnológica que permita el control de los nuevos sistemas de seguridad de la red de datos a implementar.

Arquitectura de hardware y software

Modelado general del Sistema

Diseño de infraestructura de la red

Componentes del Sistema de Seguridad

Archivos principales del programa

Realizar un documento con las especificaciones realizadas durante todo el proceso de análisis, diseño e implementación del sistema propuesto.

Elaborar el documento con las especificaciones de diseño del sistema de seguridad de la red propuesto.

Administración del Cambio

Comunicación con los usuarios

Análisis de datos recabados de la entrevista a los usuarios

Tabla 2. Funcionamiento actual del Sistema de Seguridad.

¿Cómo considera Ud. que funciona el sistema actual de seguridad de la red del Instituto Autónomo de la Artes Escénicas y Musicales (IAEM)?				
MUY BIEN	BIEN	DEFICIENTE	MUY DEFICIENTE	TOTAL
2	3	8	2	15
La mayoría de los usuarios consultados están de acuerdo con que el sistema actual presenta deficiencias en cuanto al funcionamiento, es decir, existen problemas a la hora de realizar configuraciones y buscar administrar determinados servicios de la red que impliquen la seguridad.				

Fuente: César Vallez (2011)

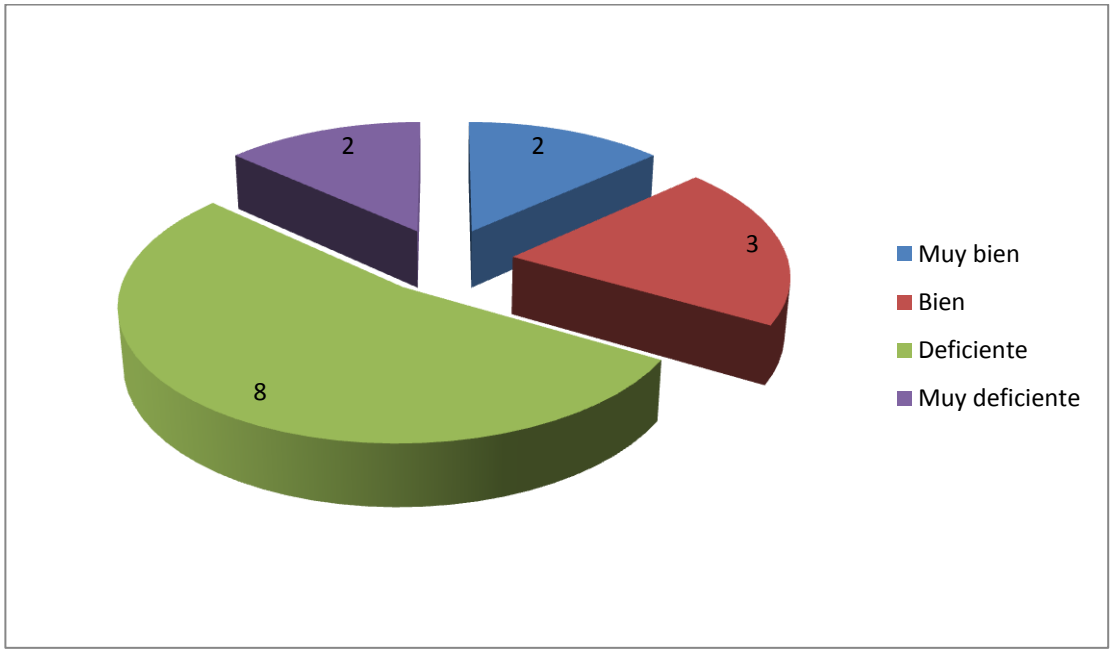


Figura 5. Gráfico de Funcionamiento actual del Sistema de Seguridad.

Fuente: César Vallez (2011)

Tabla 3. Conocimiento en cuanto a los ataques informáticos.

¿Sabe Ud. que es un ataque informático a la red?			
Si	No	No estoy seguro	Nunca lo había escuchado
9	1	3	2

Existe cierta desinformación de conceptos y definiciones necesarias para asegurar la información de la Institución, sobre todo en los aspectos de la seguridad informática. No obstante el personal más antiguo si tiene conocimiento lo que representa un ataque informático.

Fuente: César Vallez (2011)

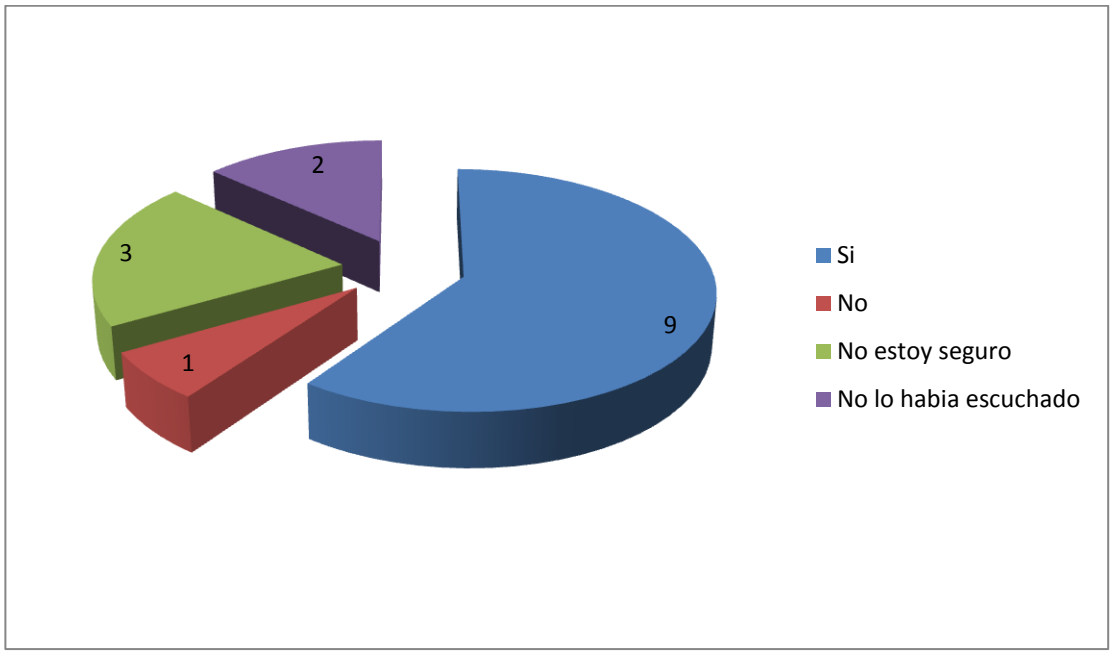


Figura 6. Gráfico de Conocimiento en cuanto a los ataques informáticos

Fuente: César Vallez (2011)

Tabla 4. Documentación de la seguridad informática.

¿Conoce Ud. de la existencia de algún documento donde estén definidos los procedimientos de seguridad de la red, en caso de un ataque informático?		
Si	No	No contestó
2	11	2
La mayoría de la documentación se encuentra en los archivos físicos resguardados de la Oficina de Tecnología, sin embargo personal clave de la Oficina no maneja información documental en cuanto a los aspectos de seguridad de la red, hubo un personal que se abstuvo de contestar por motivos de confidencialidad.		

Fuente: César Vallez (2011)

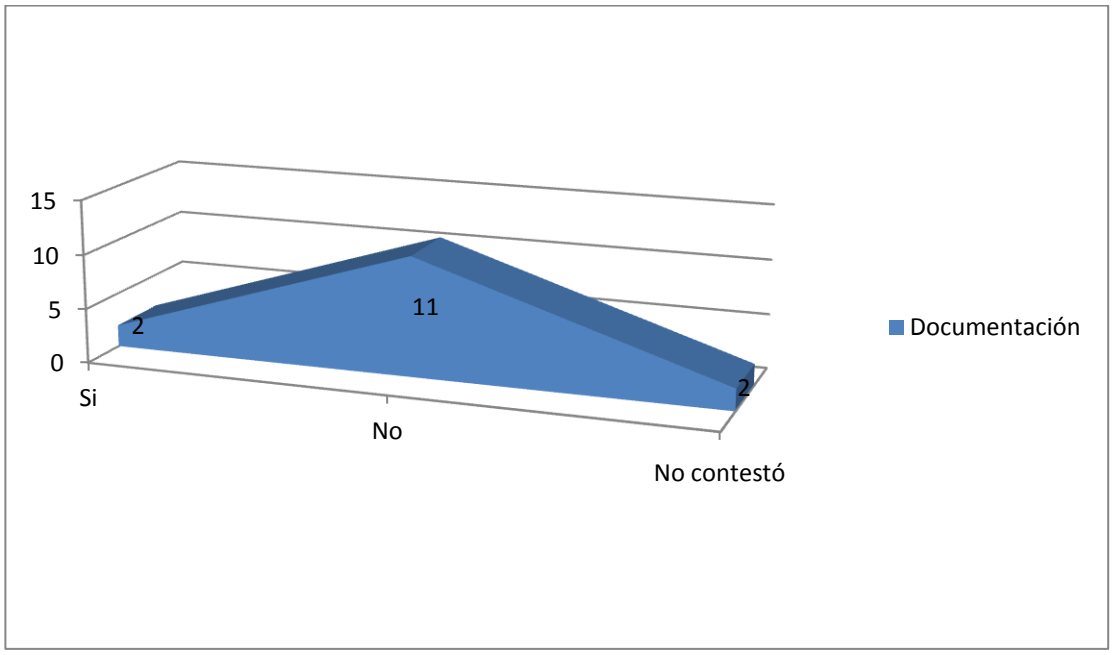


Figura 7. Gráfico de Documentación de la seguridad informática.

Fuente: César Vallez (2011)

Tabla 5. Mantenimiento del hardware de la Red de Datos IAEM.

¿Existe mantenimiento en los equipos de Hardware en la Red de datos del IAEM?		
Si	No	No contestó
8	4	3
No existe inspección ni mantenimiento de estos recursos, por personal certificado dentro de la Institución. Sin embargo, existe las garantías de servicios de Hardware (Servidores y activos de la red) de los proveedores, que al vencerse se pueden renovar pagando el soporte correspondiente.		

Fuente: César Vallez (2011)

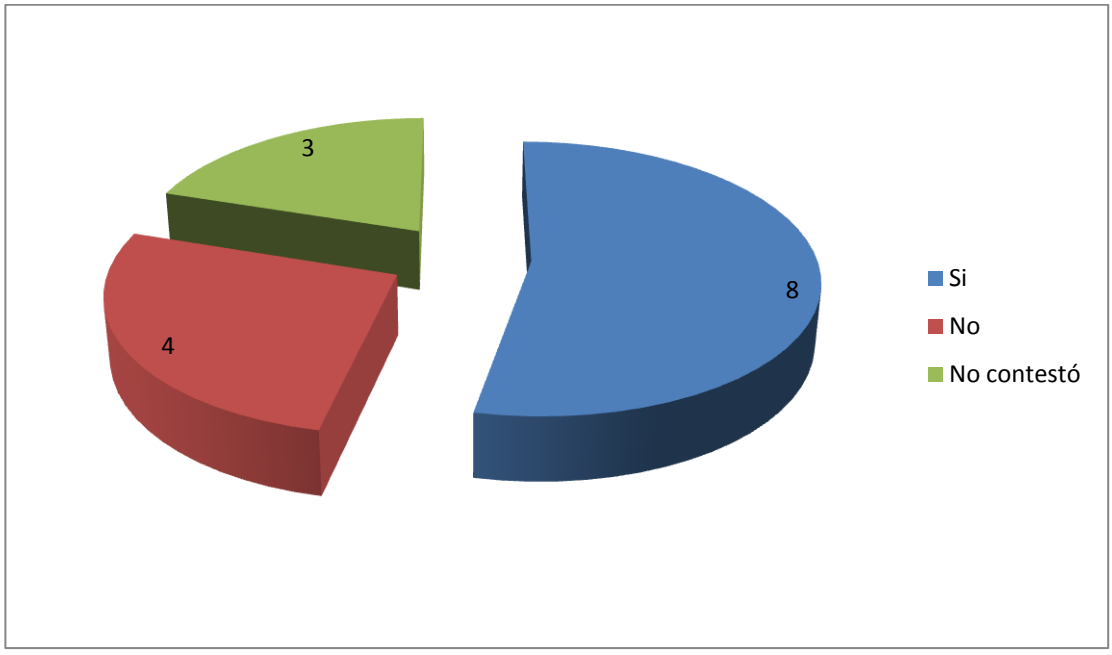


Figura 8. Gráfico de Mantenimiento del hardware de la Red de Datos IAEM.

Fuente: César Vallez (2011)

Tabla 6. Mantenimiento del Software de los Servidores de la Red de Datos IAEM.

¿Existe mantenimiento en el Software de los Servidores de la Red de datos del IAEM?		
Si	No	No contestó
13	0	2
La mayoría de los entrevistados coincidieron en que si existe una actualización periódica de los sistemas, aunque esto no implica la mejora de los mismos en cuanto a la gestión de la seguridad informática de la red. Hubo 2 personas que no contestaron alegando procedimientos de confidencialidad.		

Fuente: César Vallez (2011)

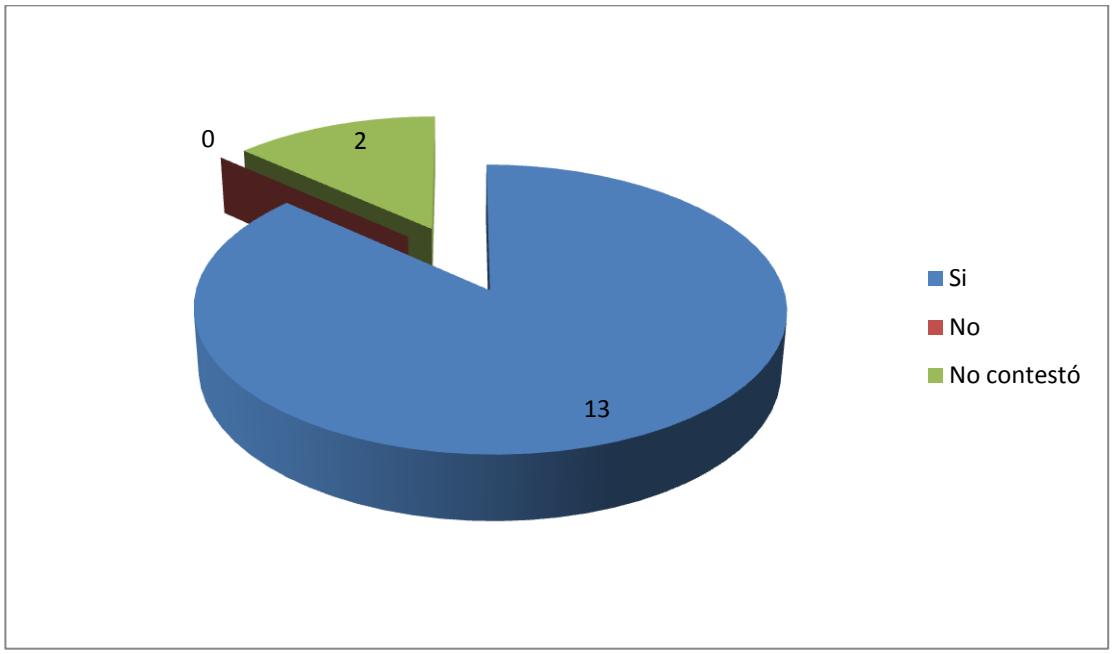


Figura 9. Gráfico de Mantenimiento del Software de los Servidores de la Red de Datos IAEM.

Fuente: César Vallez (2011)

Tabla 7. Servicios utilizados de la Red de Datos IAEM.

Qué servicios tecnológicos utiliza de los enumerados en la siguiente lista:				
Servicio	Siempre	Frecuentemente	Algunas veces	Nunca
Correo Electrónico	15			
Internet	15			
Intranet	2	11	2	
Plataforma de Red	2	13		
Mensajería (chat)	3	8	4	
Los servicios que ofrecen la red evidentemente para el personal del área de tecnología son esenciales para el día a día en su trabajo, en relación al personal de usuarios de la red también son esenciales ya que se ejecutan los niveles operativos y sustantivos de la organización utilizando la red como soporte o herramienta de apoyo para el logro de sus objetivos.				

Fuente: César Vallez (2011)

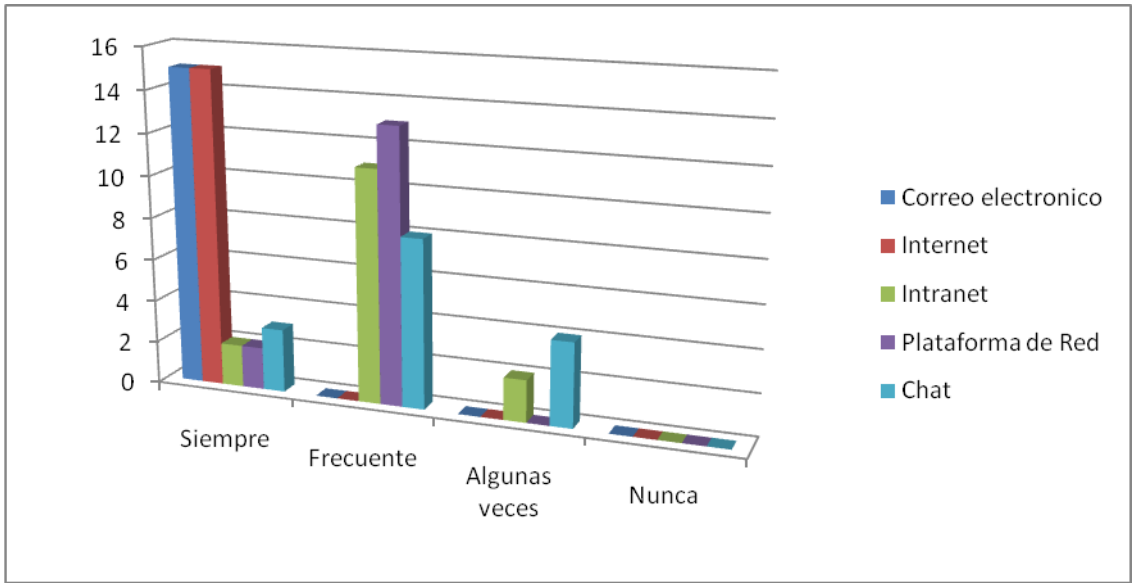


Figura 10. Gráfico de Servicios utilizados de la Red de Datos IAEM.

Fuente: César Vallez (2011)

Tabla 8. Compromiso de los Usuarios con la Seguridad Informática de la Red de Datos del IAEM.

¿Ud. piensa que los empleados están identificados con la seguridad de la información de la Institución?		
Comprometidos	No Comprometidos	Desconocen el tema
3	8	4

Los consultados manifestaron que no existe un compromiso por parte de los usuarios para mantener la seguridad informática de la Institución. Inclusive existen personas que además desconocen del tema lo cual no ayuda en la gestión de la seguridad. El número de usuarios comprometidos es mínimo y se debe incrementar con urgencia.

Fuente: César Vallez (2011)

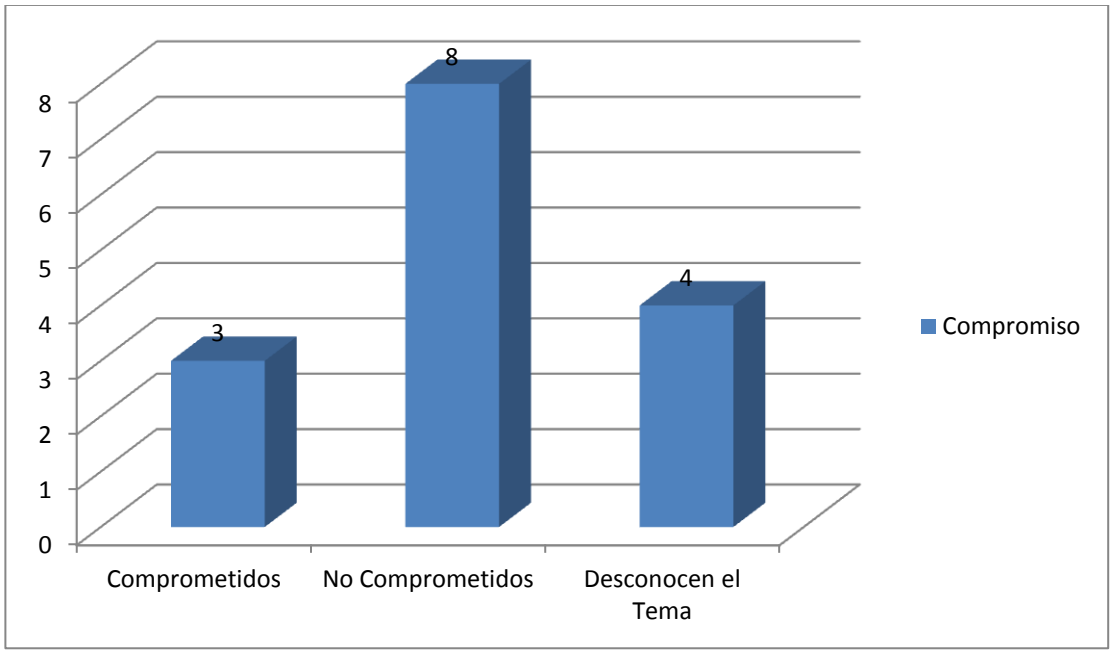


Figura 11. Gráfico de Compromiso de los Usuarios con la Seguridad Informática de la Red de Datos del IAEM.

Fuente: César Vallez (2011)

Tabla 9. Conocimiento de ataques a la Red de Datos del IAEM

¿Sabe Ud. si alguna vez la red ha sido atacada por hackers o cualquier otro tipo de amenaza informática?		
Si	No	No sabe o no contesta
10	1	4
La mayoría sabe que algunas vez la red ha sido atacada, sobre todo los servicios de página web y correo electrónico, otros no están seguro o simplemente no saben.		

Fuente: César Vallez (2011)

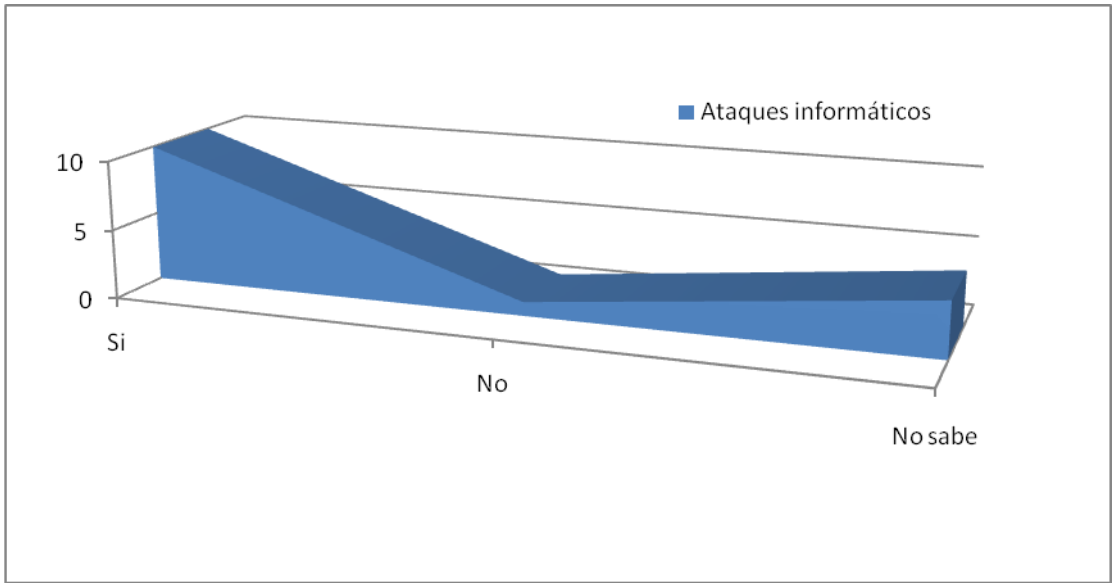


Figura 12. Gráfico de Conocimiento de ataques a la Red de Datos del IAEM

Fuente: César Vallez (2011)

Tabla 10. Documentación de ataques a la Red de Datos del IAEM

¿Sabe Ud. si hay documentación de los ataques realizados a la red de datos del IAEM?		
Si	No	No sabe o no contesta
2	10	3
La mayoría piensa que no hay documentación que permita saber a ciencia cierta que o como se realizaron las intrusiones no autorizadas a la red de datos del IAEM. Las personas que respondieron de forma afirmativa se refieren a informes realizados por la gerencia para notificación a las instancias superiores de lo sucedido. Sin embargo, la recopilación de registros con las acciones realizadas por los intrusos es inexistente.		

Fuente: César Vallez (2011)

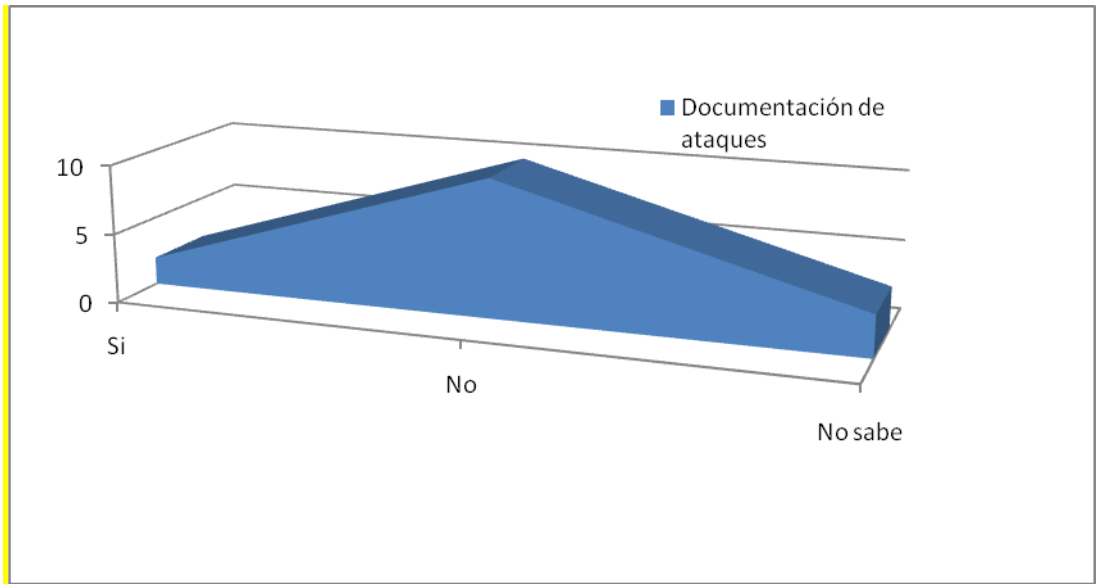


Figura 13. Gráficos de Documentación de ataques a la Red de Datos del IAEM

Fuente: César Vallez (2011)

Predicción

Miembros del equipo o personal disponible para el proyecto

El ingrediente más importante para la gestión de la propuesta es sin duda alguna el personal con que cuenta dicho proyecto para su creación, ya que su éxito estará directamente asociado con la habilidad que estos profesionales puedan ofrecer para el alcance de las metas propuestas.

Debemos destacar que este conjunto de personas colaborarán desde su punto de vista, con el investigador para la obtención de resultados óptimos y precisos, que ayuden a resolver una problemática existente actualmente en la organización.

Los participantes en el proceso del proyecto se han definido de acuerdo a la siguiente estructura:

Líder de Proyecto y Especialista de Redes: Tiene la responsabilidad de planear, coordinar e informar la ejecución de las tareas asignadas al equipo de proyecto. Además, aplicará los conocimientos adquiridos durante la fase de preparación universitaria y experiencias diversas que pueden necesitarse impredeciblemente con la finalidad de desarrollar las soluciones a los problemas específicos de seguridad informática.

Técnico de soporte a redes: Responsable de la separación objetiva entre los hechos y las suposiciones. Debe interpretar los hechos lógicamente y evaluar las relaciones y operaciones de la organización con el objeto de conseguir aislar las verdaderas necesidades del sistema de Redes de la organización.

Esfuerzo del Proyecto

El esfuerzo del proyecto para la consecución de los objetivos, se centralizará esencialmente en el investigador, el cual a través del trabajo especial de grado, se encargará fundamentalmente de analizar los requisitos, realizar el diseño y ensamblar los componentes de redes, cada uno con sus respectivos informes asociados.

Se debe recordar, que el esfuerzo se distribuye para conseguir el mejor empleo de los recursos y poder lograr las fechas topes para la entrega del proyecto. Cabe destacar para los lectores del presente trabajo de investigación, interesados en el proceso de la gestión de proyectos, que cuando las fechas límites de entrega es cada vez más ajustada, se alcanza un punto en el que el trabajo no se puede completar según la planificación, sin tener en cuenta el número de personas que lo estén realizando, debemos afrontar la realidad y definir una nueva fecha de entrega.

En la tabla 11 muestra la estimación basada en el proceso, se presentan las relaciones entre las etapas del alcance del proyecto y además se analizan las actividades claves con una ponderación, ofreciendo resultados del esfuerzo asignado a cada tarea.

Tabla 11. Estimación de Esfuerzo Basada en el Proceso

Relación Esfuerzo	Comunicación con usuario	Planificación estratégica	Análisis	Diseño	Pruebas	Total
Análisis del Diseño	-	-	10	10	2	22
Arquitectura de Red	-	-	5	10	2	17
Facilidad de uso	-	-	8	10	5	23
Cuestionario	10	-	-	-	5	15
Planificación	-	10	-	-	-	10
Riesgo asociado	-	-	5	5	3	13
Esfuerzo (%)	10	10	28	35	17	100

Fuente: César Vallez (2011)

Costes del Proyecto

Los presupuestos y costes del proyecto son una de las entradas para establecer los beneficios que debe traer consigo el desarrollo del proyecto, además de ser la traducción a datos financieros de la utilización planeada de los recursos. En este sentido, en nuestro caso de estudio la Institución cuenta con asignaciones anuales para el gasto público controladas por la Oficina de Planificación y Presupuesto quien direcciona el presupuesto financiero asignado a los distintos rubros de operatividad, en este caso existe una partida para el área de tecnología, la cual no fue suministrada al investigador por razones de confidencialidad de la Institución. No obstante, desde el punto de vista técnico financiero, las partidas pueden ser reajustadas en función de poder ejecutar el proyecto en caso de ser aprobado, por lo que recomendaron al investigador, realizar el plan de costes y entregarlo a la oficina correspondiente para su respectiva evaluación.

A continuación se muestra la tabla 12, con el presupuesto estimado que incluye los gastos del personal necesario para la realización del proyecto, la infraestructura tecnológica estimada para el alcance propuesto, así como el mantenimiento de los sistemas reutilizables para el ahorro eficiente del presupuesto, se toma en consideración un costo de materiales de oficina para el arranque del sistema y un costo de holgura para cualquier imprevisto. Cabe destacar, que los costos han sido calculados en bolívares, moneda oficial de la República Bolivariana de Venezuela, a fin de facilitar los cálculos gerenciales para la toma de decisiones. Así mismo, se debe tomar en cuenta que los beneficios se determinarán a largo plazo, luego que se realice el desarrollo total del proyecto.

Tabla 12. Costes del Proyecto

Personal	Cantidad	Tiempo (mes)	Coste Bs.(mes)	Coste total	Porcentaje presupuestario (%)
Líder de Proyecto	1	3	Bs 5.500,00	Bs 16.500,00	43,43
Técnico de Soporte	3	3	Bs 0,00	Bs 0,00	0
Sub-Total (01)			Bs 5.500,00	Bs 16.500,00	43,43
Implantación					
Análisis actual de la red	1	-	-	Bs 2.000,00	5,26
Análisis de seguridad de la red	1	-	-	Bs 1.500,00	3,95
Diseño de la red	1	-	-	Bs 4.500,00	11,85
Diseño de componentes de seguridad	1	-	-	Bs 5.000,00	13,15
Implementación	1	-	-	Bs 7.000,00	18,42
Adquisición de equipos	-	-	-	Bs 0,00	0
Materiales de Trabajo	Resma de papel, cds, marcadores, boligraficos, otros.	-	-	Bs 500,00	1,31
Imprevistos, varios.	-	-	-	Bs 1.000,00	2,63
Sub-Total (02)				Bs 21.500,00	56,57
Total General				Bs 38.000,00	100

Nota: EL personal de soporte técnico es contratado por la organización. No se requiere la adquisición de nuevo hardware. La implantación del software seleccionado en el diseño cumple con los estándares de software libre y no requiere de la adquisición de licencias propietarias. El gasto generado por la implantación corresponde únicamente al conocimiento de instalación y configuración de los sistemas del Líder de proyecto.

Fuente: César Vallez (2011)

Planificación Temporal del Proyecto

Para la planificación temporal del proyecto, se usaran técnicas dirigidas al desarrollo de las actividades, tales como: Estimaciones de esfuerzo, selección del modelo de diseño de la red de acuerdo a los objetivos propuestos y la descomposición de tareas o actividades indicando las especificaciones de cada uno de los pasos a seguir para la obtención a tiempo de los resultados.

La interdependencia entre las tareas se definirá de acuerdo a una estructura de descomposición de actividades donde el conjunto de todas ellas permitirán evaluar el proyecto como tal. Se evaluarán variables de esfuerzo, duración y fechas de inicio y culminación de tareas, que se ajustarán en la medida posible.

Con esta planificación se asume el control para administrar los recursos del proyecto y poder enfrentar posibles limitaciones y problemas que puedan acontecer en el transcurso de la ejecución del proyecto.

El investigador se apoyará en el seguimiento de esta planificación temporal, además estará realizando reuniones periódicas con el personal del equipo de proyecto, donde se informará los avances y posibles problemas confrontados, determinando así los resultados de las revisiones realizadas a lo largo del proceso de la propuesta.

La tabla 13 presenta la planificación temporal del proyecto, con las especificaciones ya descritas.

Tabla 13. Planificación Temporal del Proyecto

Tareas	Inicio	Terminación	Duración (días hábiles)	Esfuerzo (%)
Definición del Problema	17/01/2011	18/01/2011	2	3,3
Comunicación con los usuarios	19/01/2011	21/01/2011	3	5
Planificación General	24/01/2011	26/01/2011	3	5
Estudio de factibilidad económica y técnica	27/01/2011	28/01/2011	2	3,3
Análisis del sistema actual	31/01/2011	04/02/2011	5	8,3
Informe de resultado	07/02/2011	07/02/2011	1	1,8
Determinar Arquitectura de Hardware y Software de la red	08/02/2011	09/02/2011	2	3,3
Modelado General del Sistema	10/02/2011	14/02/2011	3	5
Diseño del Sistema	15/02/2011	24/02/2011	8	13,3
Componentes del Sistema	25/02/2011	11/03/2011	8	13,3
Documentación del Sistema	14/03/2011	16/03/2011	3	5
Implementación de componentes	17/03/2011	28/03/2011	8	13,3
Informe de resultado de componentes	29/03/2011	30/03/2011	2	3,3
Compaginación de informes obtenidos durante el proceso	31/03/2011	31/03/2011	1	1,8
Elaboración de documento con las especificaciones de análisis , diseño e implementación del sistema	01/04/2011	05/04/2011	3	5
Semana Holgura	06/04/2011	13/04/2011	6	10
Total			**60**	**100**

Fuente: César Vallez (2011)

Identificación del Sistema Actual

Actualidad

Hoy por hoy, el sistema de redes existente en el IAEM, ha manejado la información que ingresa de los usuarios, durante las 24 horas del día los 365 días del año, en cuanto a determinados servicios tales como correo electrónico y mensajería instantánea institucional, colocando la seguridad de la red en un segundo plano. El sistema actual está diseñado en un ambiente de red LAN[1] el cual involucra a un aproximado de 250 usuarios, el sistema operativo usado en las computadoras de estos usuarios están compartidos entre Windows xp y Linux en su versión Ubuntu, la distribución actual de la red puede observase en la siguiente figura:

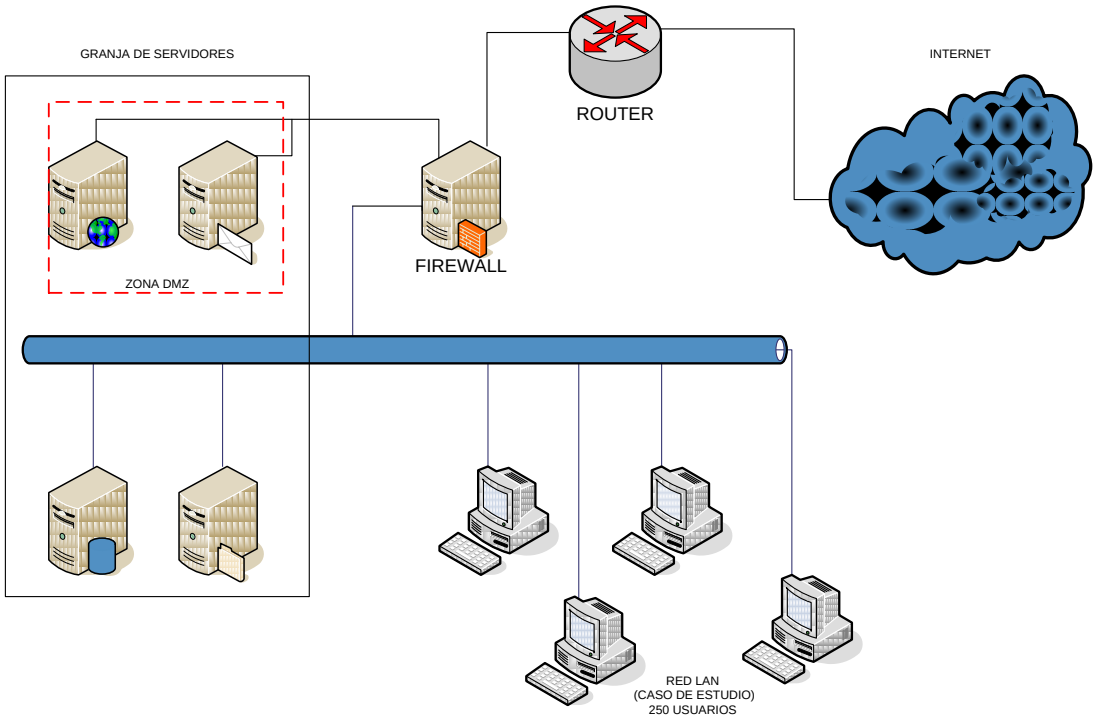


Figura 14.- Red LAN del IAEM (Actualidad)

Fuente: César Vallez (2011)

1 Una **red de área local**, **red local** o **LAN** (del inglés *local area network*) es la interconexión de varias computadoras y periféricos.

Esta red actualmente se encuentra conformada por un servicio de internet dedicado provisto por la empresa CANTV, el cual se une a un router conectado a un firewall, aquí la red se divide en tres áreas, una zona DMZ[2], una granja de servidores y la red interna de la Institución

Necesidades del Sistema

Una de las mayores necesidades en la actualidad, es la generación de reportes directamente del sistema de seguridad de la red, para un control efectivo y consecuente de los eventos diarios que acontecen desde afuera hacia adentro de la red. Se requiere un estudio para la implementación de políticas, procedimientos y normas de seguridad de la información, que aseguren el flujo diario de los datos hacia los niveles superiores de la institución, creando así una comunicación efectiva y eficiente entre los procesos operativos, gerenciales y estratégicos que se den a lugar.

Limitaciones

Las limitaciones que el sistema posee son en rasgos generales las siguientes:

a. El sistema de red tiene deficiencias en cuanto a la administración y gestión operativa, es decir, no se controla ni vigila el correcto funcionamiento de los equipos instalados.

b. Los sistemas de reportes de la seguridad de la red son escasos y no son monitorizados constantemente.

c. Los manuales del sistema y de usuario no están adecuados a las necesidades actuales, ya sea por su inexistencia o desactualización.

2 En seguridad informática, una **zona desmilitarizada** (DMZ, demilitarized zone) o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa

d. El mantenimiento correctivo en la red lo efectúa el área de soporte técnico a redes, esto sin tener la experticia suficiente para realizar tales actividades.

e. No se cumple con las normas y estándares estipuladas para el cableado estructurado de la redes LAN, lo cual puede representar una desventaja para los nuevos sistemas.

Recursos Tecnológicos y Humanos

Los recursos tecnológicos están compuestos por el hardware y software que se encuentran instalados en la red de datos de la Institución. El hardware proporciona una plataforma con las herramientas (software) requeridas para producir los registro o eventos que son el resultado diario de los servicios ofrecidos por la red. Sin embargo, visto las limitantes expuestas anteriormente, podemos deducir que no existe una adecuado escenario tecnológico que ayude a cumplir las normas exigidas por la Gerencia de la Institución. Los recursos de hardware podemos dividirla en dos áreas, la parte medular de la red y los equipos utilizados para los usuarios finales.

Las redes de la Organización está basada en una topología de red tipo estrella, la cual conecta todos sus nodos con un nodo central en la sala de servidores quien se encarga de regenerar y enviar las señales en la red. El sistema de redes tiene una infraestructura de red de área local (LAN), basada en el tipo de protocolo CSMA/CD (Ethernet) con lo cual controla la operación y tráfico de la red. Esta bajo la clasificación de 10,100,1000 Base Tx, lo cual implica 1000 Mbps en velocidad de transmisión, un máximo de 100 metros longitud para la conexión de equipos garantizando un correcto funcionamiento en la transmisión de los datos (por fabricante o empresa ensambladora de cableado), con el uso de cable par trenzado sin apantallamiento (UTP) categoría 6.

En lo referido al cableado estructurado, podemos destacar que existe una distribución horizontal con la canalización de cables hasta los puntos de datos para

cada usuario. El cable se distribuye con una disposición perimetral por falso techo, hasta las cajas terminales (wall box o face plate) situadas en la pared, que incorporan conectores estándar RJ-45. Cada host o usuarios posee su cable conector (Patch cord) entre la tarjeta NIC (Network Interfaz Conection) y la caja terminal. La red posee un Patch Panel utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones y un Rack organizador de dispositivos, por lo que se puede garantiza las velocidades especificadas por los fabricantes, sin embargo existen distribuidos en el rack cableados de distintas categorías lo cual incumple las normativas de seguridad de la ISO, IEEE, EIA / TIA, entre otras.

En cuanto a los software utilizados, por ser un ente gubernamental y cumpliendo un decreto presidencial, la mayoría de los sistemas están bajo los esquemas de software libre, esto implica que sus servidores y estaciones de trabajo tienen instalados el sistema operativo Linux, aunque existe un pequeño número de máquinas que se mantienen con el sistema operativo Windows, alegando problemas de compatibilidad con los sistemas para usuario finales.

En los actuales momentos el personal de usuarios de la Oficina de Tecnología se encuentra conformado por un Director, dos Coordinadores, cuatro Desarrolladores, dos Analistas de proyectos, cinco Técnicos de soporte a redes y usuarios y una Secretaria, quienes tienen la responsabilidad de que fluya la información a la Gerencia desde el punto de vista operativo.

Ingeniería del Producto

Propuesta para la Arquitectura de Hardware - Software del Sistema de Seguridad de la Red de Datos

La Arquitectura de Hardware y Software comprende una cantidad de decisiones significantes acerca de la organización de un Sistema; la selección de los elementos físicos estructurales y las interfaces lógicas por las cuales un sistema de red está compuesto, junto con su comportamiento que se determina por el trabajo de estos elementos. Es decir, en la realización del proceso de desarrollo que se viene ejecutando en la investigación, se han tomado en cuenta las necesidades del usuario traduciendo un requerimiento de software y de hardware, estos requerimientos son transformados en un diseño que será implementado en una plataforma para la red de datos; luego esta plataforma es probada, documentada y certificada por el personal calificado para su uso operativo correspondiente.

La plataforma tecnológica sobre la que se sustenta la propuesta está formada por los mismos servidores desde el punto de vista del hardware de la Institución, realizando una configuración de emulación de los sistemas operativos lo que representará una alta disponibilidad, en la red LAN que vienen utilizando la organización, igualmente se mantendrá la conexiones con el proveedor de servicios CANTV a través del router instalado.

En cuanto a la instalación de la infraestructura lógica se mantendrán los servicios que existen actualmente y se recomendará la incorporación de otros que ayuden en el monitoreo de la seguridad de la red como por ejemplo: Instalación de herramientas de Administración de Redes, herramientas proxy (Squid) y control de contenidos (DansGuardian), así como también herramientas de lectura de archivos de registros de auditoría (file logs), analizadores de tráfico de la red o snifer (WireShark) entre otros sistemas como los honeynets que pueden avisar y prevenir el intento de

ataques a la red en producción de la Institución.

En la actualidad la economía mundial ha tenido caídas financieras considerables, lo que ha afectado a nuestro país, es decir, ha mermado la disponibilidad financiera de la mayoría de las Instituciones públicas, en este sentido, se ha estimado costes que vayan en concordancia con el servicio que prestará la infraestructura tecnológica y el rendimiento económico de la Institución, por lo que se consideran en primer lugar la reutilización de equipos y servicios actuales e igualmente hacer recomendaciones finales para mejorar dichos servicios. En este mismo orden de ideas, por ejemplo podemos mencionar: Una posible repotenciación de equipos servidores y una reestructuración del cableado estructurado red de área local con lo cual se controla la operación y tráfico de la red, incorporando además elementos que mejoren el tráfico en la red para el cableado horizontal y vertical en los cuartos de telecomunicaciones, procurando de esta forma garantizar las velocidades especificadas por los fabricantes.

Para buscar la solución al problema planteado, el investigador decidió incorporar una estrategia de desarrollo seleccionada según la naturaleza del proyecto y de la aplicación, los métodos y herramientas con las que se cuentan y los controles y entregas que se requieren. En primera instancia se presenta un modelo de flujo de procesos del sistema (figura 15), que se pretende implantar para la seguridad de la red, para luego realizar el diseño de la infraestructura de la red con sus parámetros de seguridad y culminar con los sistemas a configurar en la red de datos, con los cuales se apoyará el desarrollo de los informes de monitoreo y seguimiento para la seguridad de la red que serán entregados a la Gerencia de la Oficina de Tecnología de la Institución. Para los fines de esta investigación, se realizará una instalación y configuración previa de los servicios con el objetivo de demostrar ante la Gerencia el modo de operación de los servicios de la Propuesta y como se realiza su puesta en marcha y posterior evaluación de los archivos de auditoría con sus resultados.

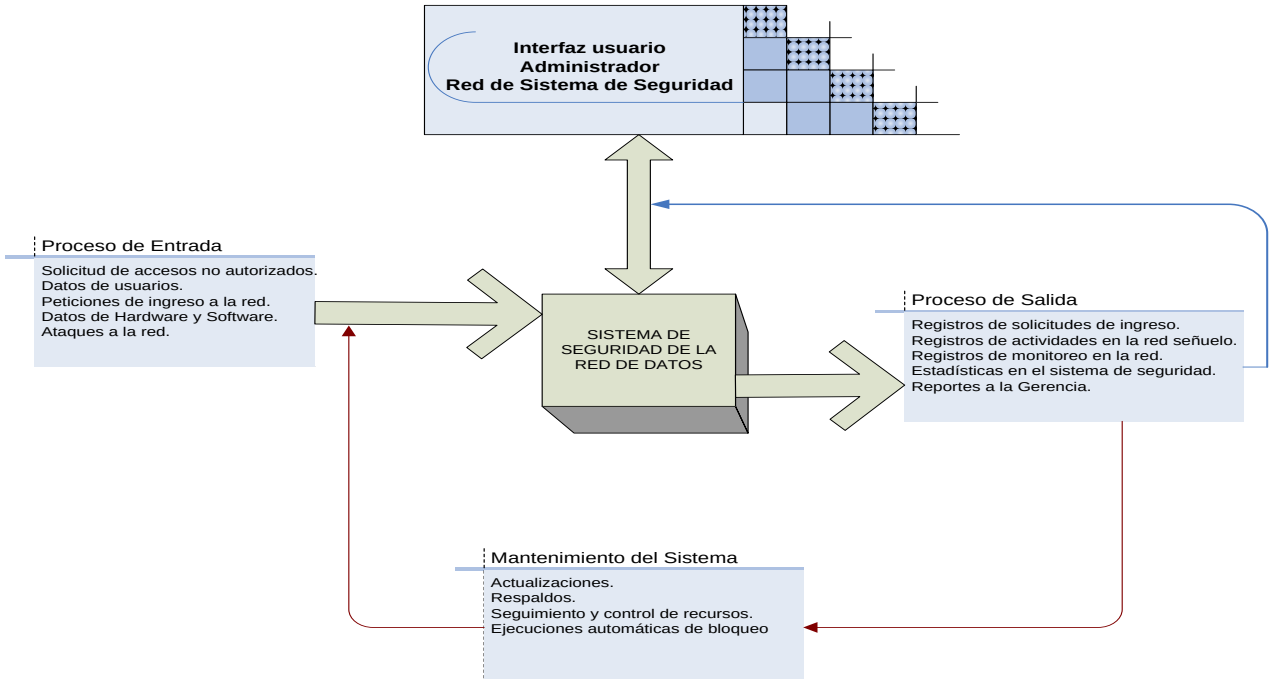


Figura 15.- Modelado del Sistema de Seguridad de la Red
Fuente: César Vallez (2011)

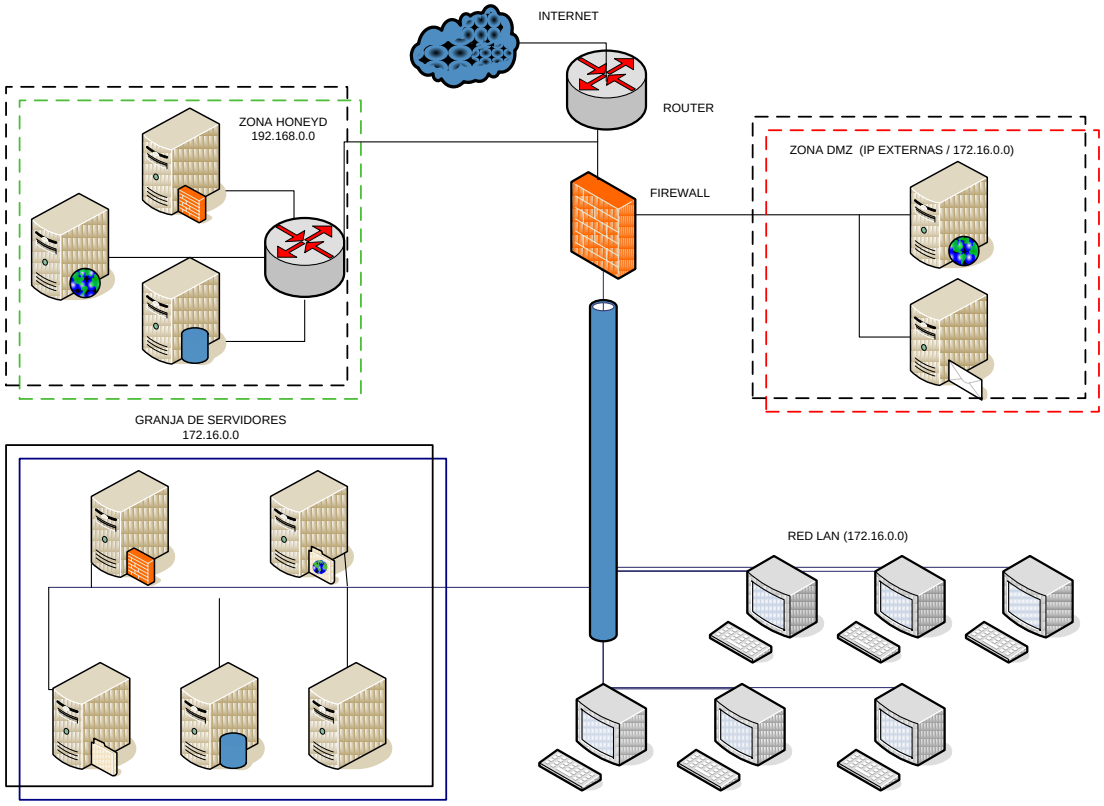


Figura 16.- Propuesta del Diseño de Infraestructura de la Red de Datos.
Fuente: César Vallez (2011)

Componentes del Sistema de Seguridad de la Red

Honeyd (Sistemas de red de Trampa)

Instalación

Honeyd, es una herramienta que nos permite implantar un honeypot de baja interacción en sistemas Unix, Linux o Windows. Además es un sistema de software libre que nos permite simular servicios e implementaciones de pilas TCP/IP de diversos sistemas operativos en uno sólo. Para lograr esto, Honeyd utiliza como base

de datos los patrones utilizados por herramientas como Nmap, p0f y Xprobe. El intruso no tiene un sistema operativo con el cual interactuar, sólo servicios emulados. Al ser una herramienta de software libre puede ser personalizada de acuerdo a las necesidades que se soliciten, por ejemplo diseñar un servicio a emular por honeyd como un servidor web. En relación a la instalación de estos sistemas en Linux, se hace realmente sencilla tanto por la orden de comando como por el gestor de instalación Synaptic, a continuación se va a realizar la instalación desde ambos puntos de vista a fin de asegurar la enseñanza a los lectores de esta investigación, así como de justificación académica para otros investigadores en su crecimiento profesional.

Modo línea de comandos:

Se debe ejecutar la orden de instalación con todas sus dependencias, se tiene la ventaja que el honeyd se encuentra en los repositorios[3] de Ubuntu por lo que el mismo realiza la descarga e instalación del paquete directamente y luego se instala, a continuación se observa (figura 17) en modo consola la orden de comando:

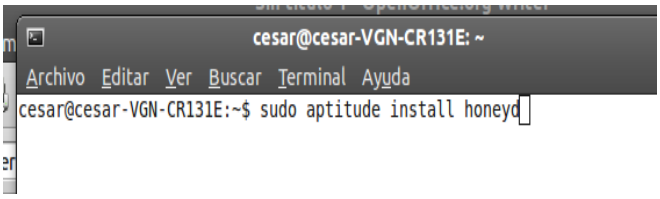


Figura 17.- Instalación modo consola de honeyd.
Fuente: César Vallez (2011)

Modo gráfico:

Aquí el investigador se ayudará con la herramienta de gestor de paquetes, por

3 Un repositorio, depósito o archivo es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

lo que debemos seleccionar en el menú Sistema → Administración → Synaptic, como vemos en la Figura 18, buscaremos el programa honeyd en la lista de software disponible y marcaremos tal como se ve, pulsamos aplicar y esperamos que se termine la instalación. Igualmente, solicita instalar diferentes librerías para la ejecución del programa, solamente se debe aceptar y completar la instalación.

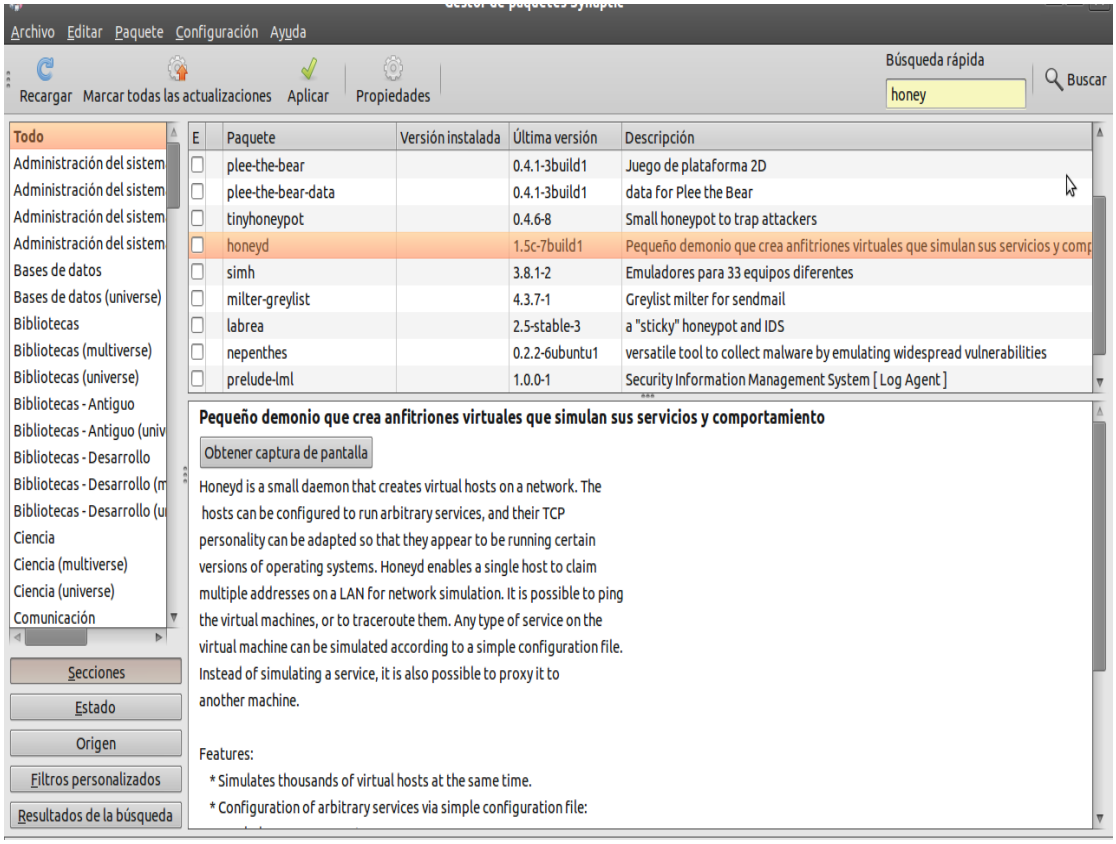


Figura 18.- Instalación honeyd a través de Synaptic
Fuente: César Vallez (2011)

Una vez realizada la instalación se procede con la configuración de los servicios dentro del archivo honeyd.conf, es justamente en este archivo donde se definirá cuales servicios serán instalados, como por ejemplo el router de entrada el servidor de seguridad, servidor web y un servidor Linux dedicado a las bases de datos

de un servicio de correo electrónico, se establecerán los parámetros de configuración de la red, es decir, las direcciones IP y su enmascaramiento, en el caso de estudio se tomo la red 192.168.0.0 con máscara 16, que luego serán usadas para ejecutar el servicio de señuelo del honeyd. El archivo de configuración fue dejado como se presenta a continuación:

```
Archivo de Configuración honeyd.conf

### Servidor de seguridad

create template
set template personality "Check Point FireWall-1 4.0 SP-5 (IPSO build)"
add template tcp port 80 "sh scripts/web.sh"
add template tcp port 23 block
add template tcp port 22 "sh scripts/test.sh"
set template default tcp action reset
set template uid 32767
bind 192.168.1.200 template

### Servidor Web IIS

create windows
set windows personality "Microsoft Windows XP Professional SP1"
set windows default tcp action open
set windows default udp action open
set windows default icmp action open
add windows tcp port 80 "perl scripts/iis-0.95/iisemul8.pl"
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
set windows uptime 3284460
bind 192.168.1.201 windows

### Servidor de archivos pop3 Linux 2.4.x

create linux
set linux personality "Linux 2.4.16 - 2.4.18"
set linux default tcp action reset
set linux default udp action reset
add linux tcp port 110 "sh scripts/pop/emulate-pop3.sh"
#set linux subsystem "/usr/sbin/httpd"
add linux tcp port 21 "sh scripts/ftp.sh"
set linux uptime 3284460
bind 192.168.1.202 linux

### Enrutador - Cisco router
create router
set router personality "Cisco IOS 11.3 - 12.0(11)"
set router default tcp action reset
set router default udp action reset
add router tcp port 23 "/usr/bin/perl scripts/router-telnet.pl"
set router uid 32767 gid 32767
set router uptime 1327650
bind 192.168.1.203 router
```

Figura 19.- Imagen de Archivo honey.conf

Fuente: César Vallez (2011)

Existe otro archivo a revisar, se llama honeyd en la ruta /etc/init.d/ del sistema de archivo de Ubuntu, aquí se encuentran los script programado para ejecutar la orden de iniciar, detener o reiniciar los servicios y simular la red honeyd.

Una vez que el archivo ha sido configurado se debe realizar las acciones para colocarlo en funcionamiento. La primera acción a ejecutar es la orden de comando para poner en funcionamiento la red configurada a la ruta del honeynet e indicar en qué interfaz trabajara, para el caso de estudio se ha instalado la red 192.168.0.0/16 en la interfaz lo[4], tal como se puede apreciar en la figura 20. Cabe destacar que estas acciones deben realizarse con privilegios de administrador del sistema.

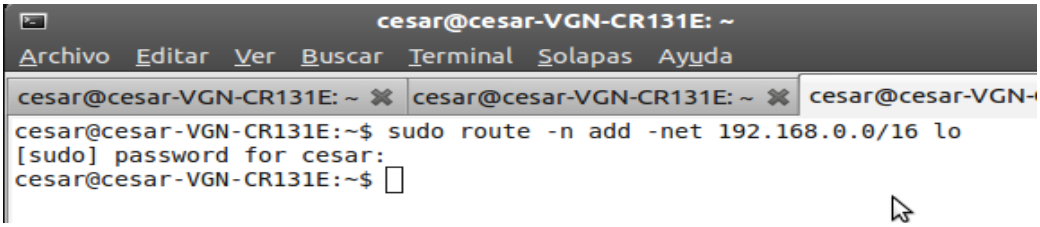


Figura 20.- Interfaz orden de comando asignación de ruta al sistema.
Autor: César Vallez (2011)

Finalmente para ejecutar el archivo de configuración del honeynet se aplica la orden honeyd, siempre tomado en cuenta tener los privilegios de administrador, adicionalmente se usa el parámetro -d porque para fines de esta investigación no se desea que se ejecuta como demonio de fondo sino que muestre los mensajes en la consola. Los parámetros -p y -f quieren decir que use esos archivos para las huellas de nmap.prints y la configuración de honeyd.conf, el parámetro -i es la interfaz de red a utilizar lo, configurada como 192.168.0.0/16. A manera de ilustración podemos observar la siguiente figura.

4 Interfaz lo, esta hace referencia al localhost del equipo donde se instale los servicios de la red.

Figura 21.- Interfaz orden de comando asignación de ruta al sistema.
Autor: César Vallez (2011)

Una vez que se tiene el servicio honeyd ejecutándose solamente queda que los administradores de la red y los servicios de seguridad informática de la empresa o institución estén alertas ante los avisos emitidos por el sistema que se van reflejando en la consola terminal del servidor honeynet que ejecuta el servicio honeyd.

Otros archivos importante y que se debe conocer para su revisión a posterior, es el log de registros de auditoría del sistema honeyd, aquí se manejan dos (02) tipos de archivos el primero es un archivo tipo demonio (daemon) el cual genera un archivo de registros estableciendo el momento de entrada en ejecución y parada del sistema honeyd, estableciendo los parámetros como por ejemplo fecha, hora, usuario que ha ejecutado las ordenes del servicio honeyd. El otro archivo es el honeyd el cual establece los registros de acciones efectuadas contra el sistema en ejecución, es decir, los intentos de ordenes (ataques) realizados desde diferentes direcciones ip hacia nuestra red configurada del honeynet.

En tal sentido, los logs de registro se convierten en los reportes más importantes, donde el administrador buscará la información que representa el ataque perpetuado en el honeynet. Para esto deberá dirigirse a los archivos contenidos en /var/log/honeypot/ donde habrá dos tipos de archivos el .log y .gz el primero representa el archivo de registro actual que contendrá las entradas de otras redes al

honeynet y el segundo contendrá los registros históricos de dichas entradas estas tendrán un orden numérico ascendente (ver figura 22).

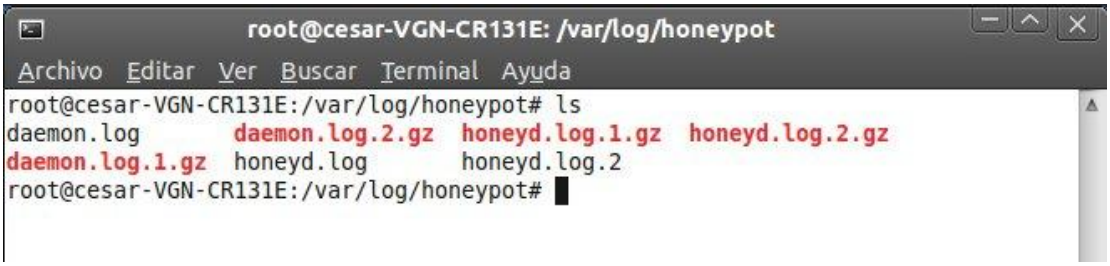


Figura 22.- Ubicación archivo de log de registros del sistema.
Fuente: César Vallez (2011)

Para obtener los registros históricos el administrador de la red deberá descomprimir tanto el archivo deamon.log.1.gz como el honey.log.1.gz, esto a través de un sencillo procedimiento de descompresión de archivo gzip, la orden a ejecutar sería gzip –d nombre del archivo, donde gzip es el programa con que se realizó la compresión .gz, -d para decirle al programa que se va descomprimir un archivo y nombre del archivo con la extensión .gz que se descomprimirá (ver figura 23). Se debe tener presente que este proceso se debe realizar una vez que se ha detenido el proceso de emulación de honeyd ya que con él se detiene el demonio que está escribiendo en el log de registro almacenado.

```
root@cesar-VGN-CR131E:/var/log/honeypot# gzip -d honeyd.log.1.gz
root@cesar-VGN-CR131E:/var/log/honeypot# ls -l
total 32
-rw-r--r-- 1 root   root       0 2011-05-07 14:28 daemon.log
-rw-r--r-- 1 root   root     450 2011-05-01 08:38 daemon.log.1.gz
-rw-r--r-- 1 root   root     517 2011-04-21 00:36 daemon.log.2.gz
-rw-r--r-- 1 root   root       0 2011-07-10 00:39 honeyd.log
-rw-r--r-- 1 root   root   15056 2011-07-09 08:09 honeyd.log.1
-rw-r--r-- 1 honeyd honeyd   204 2011-04-21 02:00 honeyd.log.2
-rw-r--r-- 1 honeyd honeyd  1758 2011-04-23 00:00 honeyd.log.2.gz
root@cesar-VGN-CR131E:/var/log/honeypot#
```

Figura 23.- Orden de descompresión archivo de log de registros del sistema.
Fuente: César Vallez (2011)

Finalmente, el administrador tendrá en su poder dos archivos de log de registro que le permitirán incluir en su reporte final de intrusión a la red de datos para entregar a la gerencia de tecnología, quien será el responsable de tomar las decisiones finales para mejorar la seguridad de datos de la Institución. Un ejemplo de estos archivos lo podemos observar en la figura 24 de esta investigación, además podemos observar el reporte completo en el anexo 1.

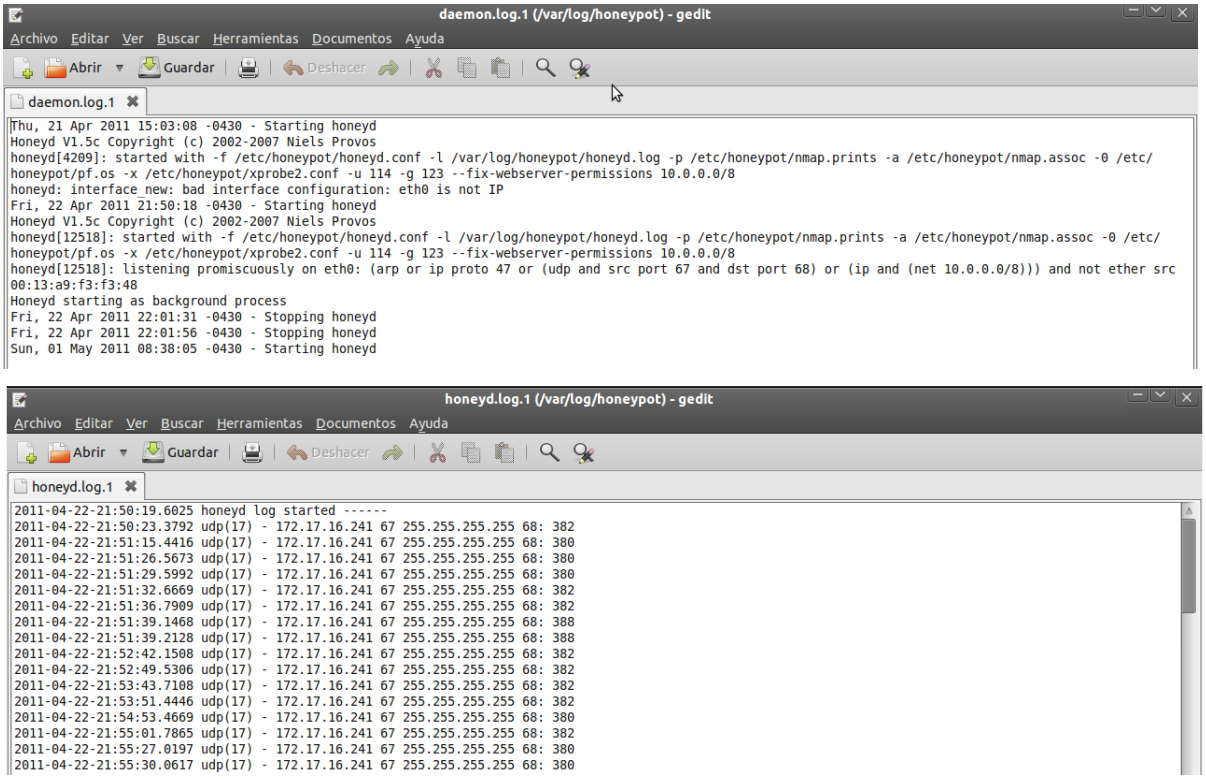


Figura 24.- Reporte daemon.log.1 y honeyd.log.1 (archivos de logs de registros del sistema).

Fuente: César Vallez (2011)

El siguiente gráfico representa la propuesta donde se describe con un esquema de flujo de datos el acceso al archivo de configuración del sistema honeynet desde el punto de vista del administrador del sistema y como sería el acceso del atacante o intruso en la red de datos.

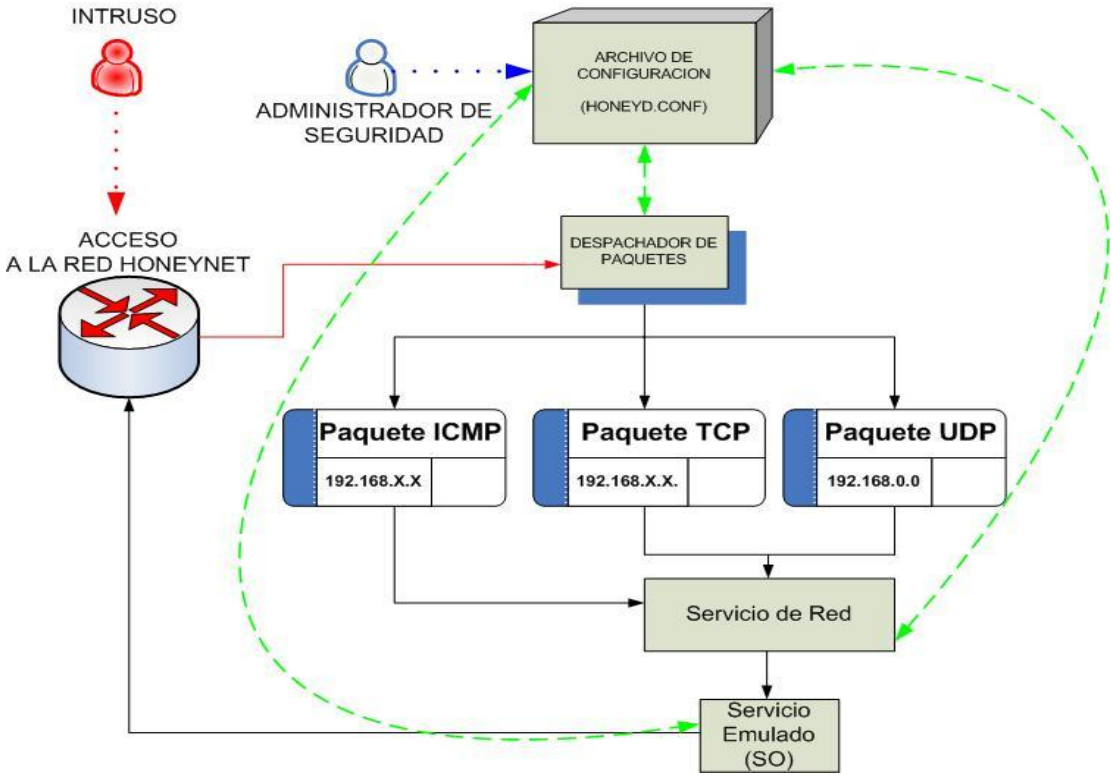


Figura 25.- Flujo de datos del archivo de configuración del sistema.
Fuente: César Vallez (2011)

Para fines de esta investigación, se realizarán unas pruebas de escanéo de puertos y analizador de la red con herramientas de tráfico de protocolos y filtrado de paquete de datos, tal como se comento al inicio. A continuación se describirán unas herramientas que se utilizarán para tales fines.

Para verificar la utilidad del honeynet se instaló la distribución de Linux llamada BackTrack en su versión estable 5.0 (figura 26), la cual se dedica exclusivamente al estudio de las vulnerabilidades en la redes de datos. Se tiene la

opción de ejecutarlo en CD vivo (livecd[5]), no obstante para el desarrollo de esta investigación se decidió instalarlo en una partición del disco duro de uno los laptops utilizados como recursos tecnológicos. Su instalación es bastante sencilla, primero se debe configurar el equipo a fin de que tome como unidad de arranque del sistema la unidad de Dvd/CD, seguidamente se iniciará el sistema de archivos de Linux montando los dispositivos de hardware del equipo y enviando la consola de usuario para colocar el login y el password, en cuyo caso se utiliza el login: root con el password: toor, dando entonces acceso al sistema, simplemente nos queda invocar el comando para iniciar la interfaz grafica startx (figura 27).

Figura 26.- Distribución Linux BackTrack versión 5.
Fuente: César Vallez (2011)

[5] Distribución de Linux que puede ejecutarse sin instalación previa en disco duro del PC.

Figura 27.- Orden de ejecución modo gráfico BackTrack versión 5.

Fuente: César Vallez (2011)

Luego que se ha ejecutado el modo gráfico de BackTrack5 podemos iniciar el icono de instalación del sistema (figura 28), el cual solicita información concerniente al idioma en que se instalará la distribución, decidiendo en este caso por el idioma español, luego ubicación geográfica con zona horaria para este caso sería Caracas, -04:30 y finalmente la partición de disco duro donde se instala el sistema, suministrando esta información se inicia el proceso de instalación de la distribución Linux el cual tarda aproximadamente unos 10 minutos en finalizar. Este tiempo depende de las características de velocidad del procesador del equipo. Seguidamente extraemos el Dvd booteable de la unidad óptica y reiniciamos el sistema el cual arrancará ubicándonos en la consola o terminal de comandos. En este momento se puede invocar nuevamente la orden de startx para ejecutar la interfaz gráfica y proceder con la simulación de análisis de vulnerabilidades en la red.

Figura 28.- Icono de instalación modo gráfico BackTrack versión 5.

Fuente: César Vallez (2011)

Los sistemas que se mencionan a continuación se encuentran instalados en la distribución de Backtrack5, por lo tanto previamente se hará mención para ubicarlo dentro del sistema y posteriormente se explicará cómo utilizarlos a fin de que sirvan como modelo de pruebas para confirmar el funcionamiento correcto del sistema honeynet.

Zenmap (Escáner de redes)

Zenmap es una herramienta de escaneo de redes muy respetada en el ambiente de software libre, muy similar a nmap, pero con la diferencia de tener una interfaz gráfica muy agradable. Para ejecutar la herramienta sólo debemos ubicar la ruta Bactrack/Information Gathering/Network Analysis/Network Scanners/zenmap. La figura 29 nos ilustra este proceso.

Figura 29.- Ejecución de Zenmap a través de BackTrack5
Fuente: César Vallez (2011)

El programa zenmap, también se puede ejecutar desde la consola, se debe invocar con privilegios de administrador del sistema solamente se debe teclear en la consola de comando la orden sudo zenmap, como se ilustra en la figura 30.

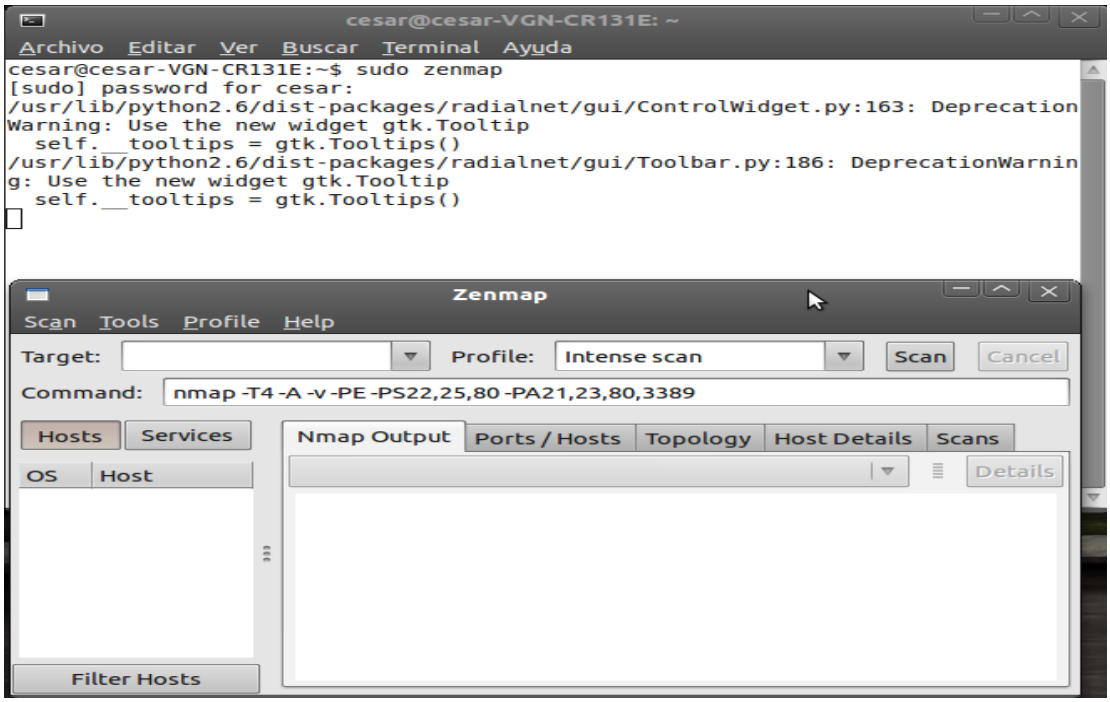


Figura 30.- Orden de ejecución a través de consola de Zenmap

Fuente: César Vallez (2011)

A medida que se vayan seleccionando las opciones de Zenmap, en la caja de comando se muestra cómo se ejecutaría el programa nmap desde la línea de comandos. Zenmap tiene una serie de perfiles predeterminados a la hora de escanear, permitiendo así realizar un escaneó rápido. Además, permite que crear perfiles de escaneó propio.

Los perfiles predeterminados son:

(a) Intense Scan: nmap -T Aggressive -A -v ip.ip.ip.ip.

(b) Operating System Detection: nmap -O -v ip.ip.ip.ip.

(c) Quick Full version Detection Scan: nmap -T Aggressive -sV -n -O ip.ip.ip.ip.

(d) Quick Operating System detection: nmap -T Aggressive -O -v ip.ip.ip.ip.

(e) Quick Scan: nmap -T Aggressive -v -n ip.ip.ip.ip.

(f) Quick Services version detection: nmap -T Aggressive -sV -v ip.ip.ip.ip.

(g) Quick and verbose scan: nmap -d -T Aggressive –packet_trace -v -n ip.ip.ip.ip.

(h) Regular Scan: nmap -v ip.ip.ip.ip.

Otra de las ventajas que nos ofrece Zenmap es que nos proporciona una serie de pestañas las cuales agrupan y nos muestra información de los escaneos ejecutados en diferentes formatos:

Port/Hosts: Muestra un listado de los puertos y nodos detectados indicando puerto, protocolo, servicio con sus respectivas versiones y el estado.

Nmap output: La salida en línea de comandos, mostrando una sintaxis en colores.

Hosts Details: Se muestra la información del análisis en forma de árbol. Datos relativos del estado de la máquina, dirección IP, Sistema Operativo, puertos y datos TCP.

Scan Details: Se muestra información del análisis seleccionado. Comando seleccionado, versión de nmap y fechas de inicio y fin.

También se puede comparar resultados de escaneos nuevos con escaneos realizados anteriormente ya que puede guardar una ráfaga de escaneo realizada. Adicionalmente, muestra un gráfico con las redes escaneadas en localhost que sirve como referencia para saber cuáles son las direcciones ip rastreadas.

WireShark (Analizador de Tráfico)

Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos y como una herramienta didáctica para la enseñanza de las redes de comunicaciones.

Algunas de las características de WireShark son las siguientes:

Disponible para UNIX, LINUX, Windows y Mac OS. Captura los paquetes directamente desde una interfaz de red. Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado. Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas. Filtra los paquetes que cumplan con un criterio definido previamente. Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente. Permite obtener estadísticas. Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Su modo de instalación también es muy sencillo, utilizando la interfaz gráfica de BackTrack5, ubicamos la siguiente ruta BackTrack/Information Gathering/Network Analysis/Network Traffic Analysis/wireshark, como se muestra en la figura 31. Mientras que la figura 32 muestra el programa WireShark en ejecución. Para su ejecución solo debemos indicarle la interfaz de conexión a la red, en este caso corresponde a eth0 y filtrar el rango de ip para el análisis en nuestro caso sería 192.168.1.0/16, seguidamente el inicia la exploración y empieza a mostrar las conexiones contra ese rango de ip en especifico.

Figura 31.- Ubicación de WireShark en BackTrack5

Fuente: César Vallez (2011)

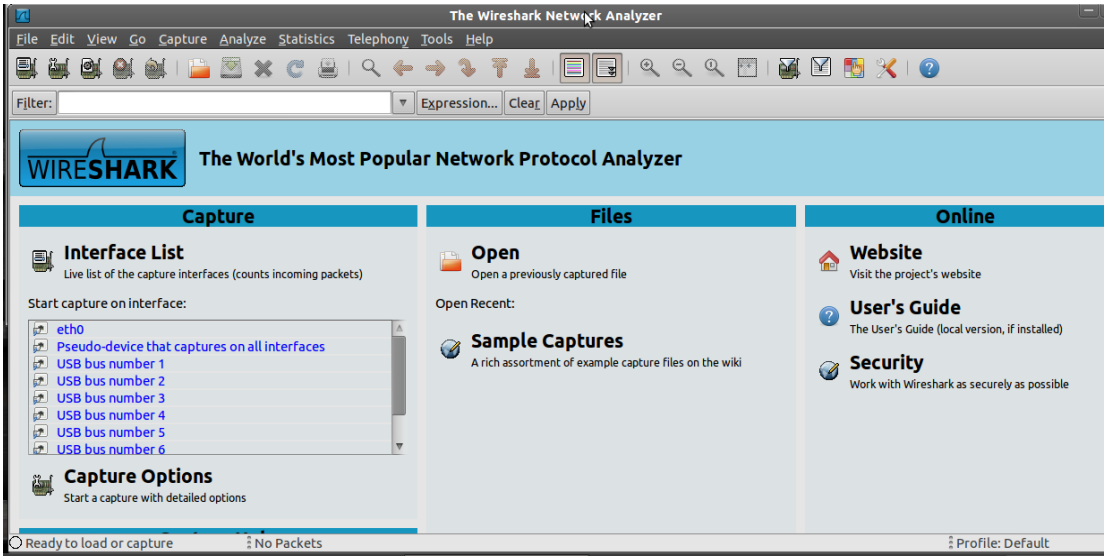


Figura 32.- Programa Wireshark en ejecución

Fuente: César Vallez (2011)

A continuación se observa la figura 33 con un ejemplo del tráfico de red analizado por WireShark.

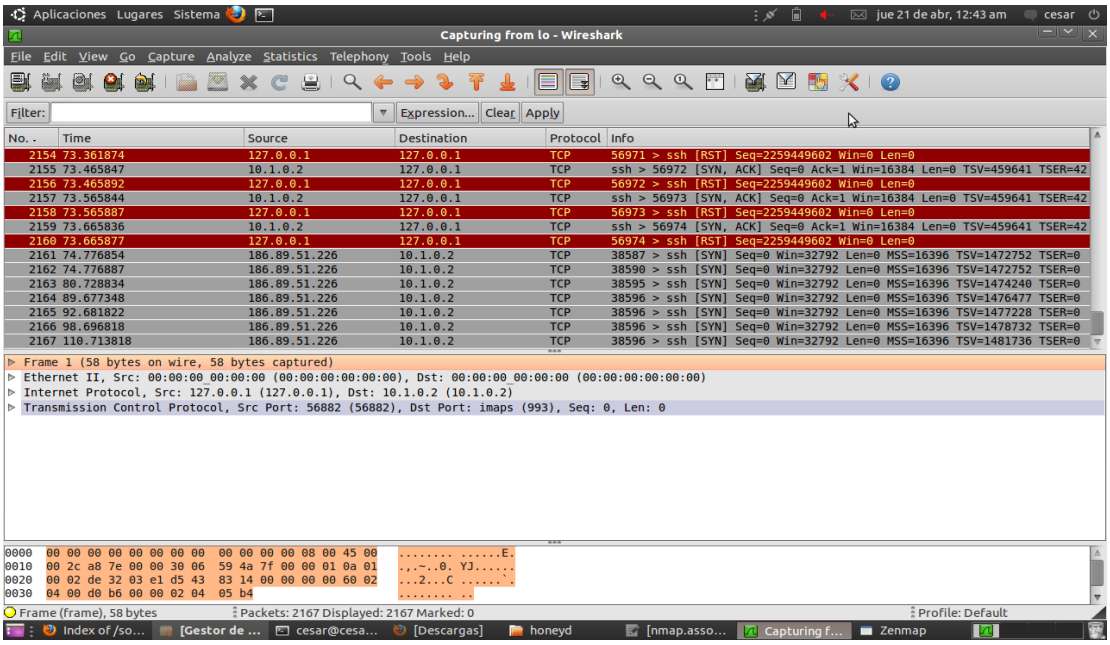


Figura 33.- WireShark en ejecución de tráfico en la red.
Fuente: César Vallez (2011)

Con estas herramientas se puede determinar el funcionamiento del honeynet analizar su interfaz de red y escanear los puertos de los servidores emulados listos para engañar a los interesados en conseguir vulnerabilidades en las redes de las organizaciones, tal como lo es el caso de estudio.

Finalmente, para establecer los procedimientos de monitoreó de la red con estas herramientas, se realizó un diagrama de flujos de datos (figura 34) que será el procedimiento a seguir por parte de los administradores de la red para la solución del sistema donde se generará la documentación técnica correspondiente que acompañará los informes respectivos de dichos administradores a la Gerencia de la Oficina de Tecnología.

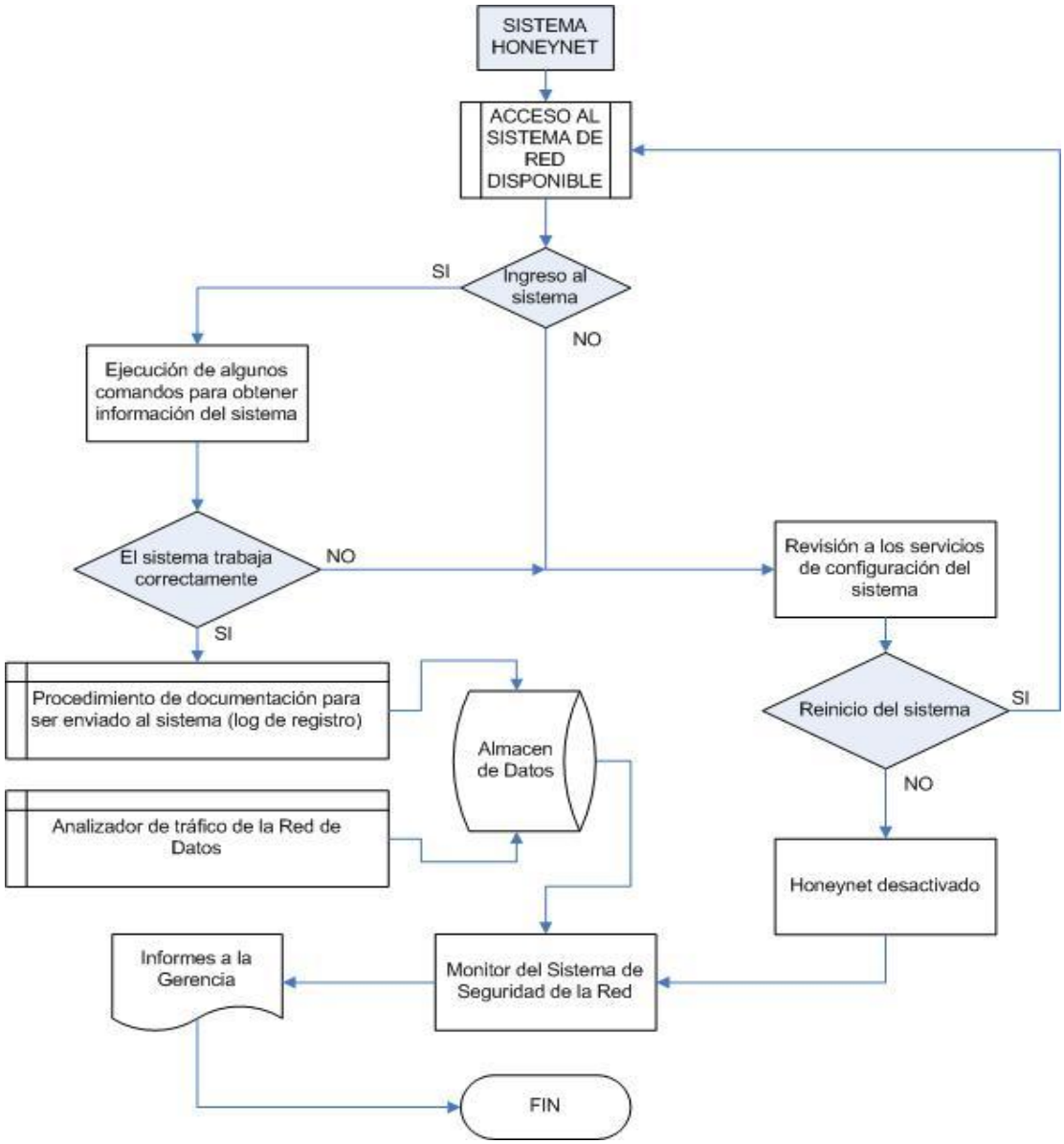


Figura 34.- Diagrama de Flujo de Datos Solución Monitoreo de la Red.

Autor: César Vallez (2011)

CONCLUSIONES

La intención del presente trabajo de grado, estuvo dirigida al logro de un objetivo general, ser considerada como un modelo de propuesta factible que permitirá implementar una red de trampa (honeynet) en las redes de datos de cualquier organización ya sea de carácter pública o privada, tomando como base del sistema propuesto, los estándares abiertos y las licencias de software libre. Adicionalmente y como complemento para la investigación se realizó un análisis caso de estudio enfocado a una Institución pública llamada Instituto de Artes Escénicas y Musicales adscrita al Ministerio del Poder Popular para la Cultura, donde se están ejecutando innumerables actividades concernientes al ámbito cultural en Venezuela y una de sus herramientas más utilizadas como apoyo a las funciones que ejecutan son precisamente la redes de datos.

El logro de este objetivo, se obtuvo a través del cumplimiento estricto de unas fases complementarias, la primera está referida al diseño una red de trampa (Honeynet) que permite realizar informes pertinentes y constantes para la Gerencia de Tecnología de la Información de Instituto de Artes Escénicas y Musicales (IAEM). En relación a este aspecto se pudo estudiar las distintas características del funcionamiento de los honeypot y honeynet a fin de determinar la estructura ideal de acuerdo a las propiedades de los sistemas que se ejecutan en la organizaciones públicas y privadas en nuestro país, tomando en consideración variables como infraestructura de la red, hardware del sistema, costes, recurso humano para la implementación y mantenimiento del sistema, entre otros que influyen directamente en la consolidación de un diseño estable para la ejecución de una red de trampa, esto se consolidó en la base para el desarrollo de la propuesta a presentar. También se realizó un análisis con los usuarios de la red caso de estudio cuyas respuestas ofrecen una percepción interna de los procesos que involucran a la red y las consideraciones de seguridad además de ofrecer la actualidad de la red necesaria para determinar los

flujos de entrada al sistema y como estos pueden ser analizados para poder obtener un resultado.

La segunda fase estaba dirigida a implementar una red de trampa (Honeynet) en un sistema de red externo al caso de estudio, siendo esta una de las más importantes metas para la obtención de objetivo general, ya que es en esta fase donde se realizaron las pruebas del sistema y se determinó que metodología se debe emplear para el desarrollo del proyecto factible. Una vez investigado la parte teórica y determinado el diseño del honeynet a utilizar, se concluyó en la práctica que un sistema factible de red de trampa a construir para la propuesta es el denominado honeynet de baja interacción, en su versión honeyd para software libre, el cual trabaja realizando emulación de servicios y sistemas operativos, lo cual representa una gran ventaja sobre todo porque el sistema será ejecutado en un ambiente de red en producción y la actividad del atacante o intruso estará limitada al nivel de emulación del honeynet que se programe. Otra ventaja que presenta este tipo de implementación es su simplicidad en cuanto al requerimiento de recursos de hardware, que sin duda alguna es fundamental y representativo en cualquier ambiente de redes de cualquier Institución pública o Empresa privada. Lo que sí es cierto, es que se debe realizar la configuración de los archivos de manera cuidadosa a fin de realizar los cambios necesarios para emular los servicios de tal manera que sean lo más parecido a la realidad de las redes de cualquier organización hoy en día. En este sentido el investigador decidió emular los servicios de un servidor web, un servidor de seguridad y un servidor de correo electrónico, habilitando los puertos necesarios para las actividades inherentes a ellos.

Como apoyo al sistema honeynet para la implementación del sistema se tomo en cuenta un sistema rastreador de puerto y un analizador de la red, embebidos en una de las últimas distribuciones especificas para el área de la seguridad de datos denominada BackTrack en su versión 5, a través de la cual se mostró parte del tráfico de red analizando los paquetes que intervienen en el honeynet, información

fundamental a los administradores de la red. En este caso existen varios tipos de sistemas que ayudan a realizar estos procesos, sin embargo el investigador se orientó por Zenmap y WireShark respectivamente.

La tercera fase estaba enfocada a la parte de documentar el diseño obtenido de la red de trampa (Honeynet) en ese ambiente externo con la finalidad de ser presentado en el IAEM para su ejecución. Con la etapa de implementación se pudo demostrar fehacientemente que el sistema se encuentra estable en el ambiente de prueba, por lo que el producto final puede ser llevado al ambiente de producción en el momento que sea solicitado por la Institución caso de estudio, también se pueden mostrar los resultados obtenidos en las pruebas de desarrollo que se activarán inmediatamente en los registros de auditoría del sistema una vez implementado y puesto en marcha en la red de datos de la Institución. Estos registros se convierten en reportes impresos que pueden acompañar los informes pertinentes de los administradores de la red, lo cual puede ser un apoyo sustancial y físico de que sucede en la red de datos del caso de estudio o en su defecto de cualquier organización que lo requiera. Además, esta investigación quedará en la Institución caso de estudio para describir los aspectos para poder instalar y configurar los archivos necesarios pensando en futuras actualizaciones.

Como otro aspecto conclusivo de la investigación, el honeynet puede ser utilizado como un sistema de propósito productivo, es decir, por medio de este sistema se ofrece la protección a la Organización mediante la prevención y detección de un ataque informático. Tomando en cuenta que la única actividad que registran los honeynet son las relacionadas con el atacante, además de que estos registros se generan rápidamente en el sistema, se puede decir entonces que todas los reportes deben ser monitoreados de forma permanente por los administradores de la red con el fin de mejorar los aspectos de prevención y detección de una futura intrusión no autorizada.

Un aspecto relevante de este estudio, ha sido el poder constatar que la tecnología en los últimos años ha ido en constante transformación, es decir, se evidencia en la propuesta como se pueden fusionar varias arquitecturas tecnológicas, para obtener rendimiento fiables y de alta calidad, apartando los precios del mercado con la utilización de tecnologías basadas en el software libre. Estas implementaciones nos brindan una importante variedad de opciones tanto de procesamiento y gestión de las redes, como los procesos de configuración y adecuación de los sistemas, puntos muy solicitados por los niveles de alta gerencia a la hora de tomar decisiones para la contratación de los servicios.

Finalmente, los riesgos son inherentemente potenciales en el uso de todas las tecnologías de seguridad, los honeynet también corren riesgos, específicamente el de ser secuestrados y controlados por el intruso y ser utilizados como plataforma de lanzamiento de otros ataques, esto implica que se debe asegurar el sistema con sistemas actualizados y configuraciones correctas en los archivos que gestionan las actividades del sistema honeynet.

RECOMENDACIONES

En función de planificar los procesos para la aplicación del diseño y puesta en marcha del sistema de red de trampas, se recomienda lo siguiente:

Instaurar a la brevedad posible el hardware y software requerido para los procesos de implementación de la red de trampas (honeynet), con los cuales se generarán los informes y registros diarios de apoyo a los administradores de la red.

Para que el sistema pueda garantizar una buena transmisión de datos y mínima pérdida de paquetes se debe mejorar el sistema físico de cableado estructurado, asegurando así las velocidades de transmisión, confiabilidad y robustez de los datos procesados y las especificaciones realizadas por los fabricantes.

Establecer en la medida de lo posible un equipo de hardware específico para el sistema propuesto, diferenciándolo así de los otros sistemas instalados en la sala de servidores del IAEM, a fin de que los usuarios administradores se aboquen a la gestión diaria de los procesos que generen.

Realizar mantenimientos periódicos al sistema en actual uso, tanto de hardware como de software, esto implica las actualizaciones con nuevos parches de seguridad que salgan a la luz pública, ya que estos sistemas funcionan las veinticuatro (24) horas del día los trescientos sesenta y cinco (365) días del año.

Determinar unas políticas de seguridad que permitan asegurar la confidencialidad de los datos y la recuperación inmediata en caso de ataques en la red del IAEM. Entre ellas, ofrecer a los usuarios finales de la Institución un sistema de charlas, talleres o seminarios que traten el tema de la seguridad informática, para que

estén preparados y sepan cómo actuar en caso de alguna actividad que vulnere la gestión de la red.

La propuesta en vista de ser un sistema aplicable a la seguridad de datos, es recomendable realizar la implementación tomando en cuenta aspectos relacionados con los respaldos periódicos de la información de los servidores ya que son estos los que manejan la información vital de la Institución y son parte de los activos más importantes que ella tiene.

Los procesos que tienen que ver con la documentación del sistema propuesto tendrán que ser acompañadas por informes técnicos explicativos por parte de los administradores de la red para ser entregados a los gerentes de tecnología para la toma de decisión. Por esto es necesario actualizar los conocimientos y destrezas de los administradores de la red o en su defecto contratar personal con esta capacidad.

Finalmente, debido al riesgo inherente que corren los sistemas con la propuesta una vez implementada, se recomienda aumentar los niveles de seguridad en la red, en cuanto a la protección del servidor de seguridad (firewall), donde se deben habilitar únicamente los servicios estrictamente necesarios en la red, dejando inhabilitados los demás puertos que no se usen, gestionando de forma más segura las actividades que se relacionen con el sistema honeynet.

REFERENCIAS BIBLIOGRAFICAS

ARIAS, F. (1999). *El Proceso de Investigación.* Caracas. Venezuela.

CABALLERO, A. (2009, Octubre). CAINE: Entorno de Investigación Asistido por Computadora. *Linux+ 58*. 58-65.

CLARET, V. (2010). *Tutores y Tesistas Exitosos.* Caracas. Venezuela.

DRUDIS, X. (2005, Mayo). Dossier: Networking. *TodoLinux 52*. 12-18.

Honeynet.br. Projeto de Honeypots divulga estatisticas de potenciais ataques. [Página Web en línea]. Disponible: http://www.honeynet.org.br/press/2005/2005-03-10a.html [Consulta: 2010, Enero 10].

JARA, J. (2008, Octubre). Penetration Test y Seguridad con Herramientas Libres. *Linux+ 47*. 28-36.

LOPEZ, J. (2009, Marzo). Zona Debian: Cortafuegos iptables y su interfaz Firestarter. *TodoLinux 98*. 21-24.

MARTINS, H. y TOME, J. (2005). *Análisis de actividades no autorizadas en redes de área local (LAN) mediante la utilización de señuelos (honeypots) montados sobre máquinas virtuales, para el diseño e implementación de sistemas de protección*. Tesis de Grado, Universidad Metropolitana, Caracas.

MENDEZ, Moralez (1998). *Metodología de la investigación.* 40.

Open Source. Definición. [Página Web en línea]. Disponible: http://es.wikipedia.org/wiki/Definici%C3%B3n_de_Open_Source [Consulta: 2010, Octubre 25].

OROZCO, J. (2007). *Servidores trampa (honeynet) para detección de intrusos mediante el sistema operativo Solaris 10.* Tesis de Grado, Universidad Metropolitana, Caracas.

PEREIRA, J. (2008, Enero). Damn Vulnerable Linux: El laboratorio de seguridad informática. *TodoLinux 84*. 31-36.

PRESSMAN, Roger.(2002). *Ingeniería del Software (Un enfoque práctico)*. (5a. ed.). España: McGraw-Hill.

Proyecto Honeynet. The Honeynet Project. [Página Web en línea]. Disponible: http://www.honeynet.org/ [Consulta: 2009, Diciembre 02].

Proyecto Honeynet Unam Chapter. Proyecto Honeynet Unam. [Página Web en línea]. Disponible: http://www.honeynet.unam.mx/content/proyecto-honeynet-unam [Consulta: 2010, Enero 10].

Proyecto Honeynet Vencert. Bienvenidos al Proyecto de Honeynet Venezuela. [Página Web en línea]. Disponible: http://honeynet.vencert.gob.ve/index.php?option=com_content&view=article&id=717:bienvenidos-al-proyecto-honeynet-venezuela&catid=35:eventos-del-vencert [Consulta: 2010, Diciembre 25].

SCHIFFMAN, M. (2002). *HACKERS. 20 Desafíos Prácticos*. (1ª. Ed.). España: McGraw-Hill.

TAMAYO y Tamayo (1999). *El proceso de la investigación científica*. 19.

Universidad Central de Venezuela. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica (2008). Instructivo y Normalización para la elaboración de Trabajos Especiales de Grado. Caracas: Vázquez, B. y Molina, J.

Universidad Pedagógica Experimental Libertador. Vicerrectorado de Investigación y Postgrado (2006). *Manual de Trabajos de Grado de Especialización y Maestrías y Tesis Doctorales.* Caracas. Venezuela.

[Anexo 01]


Aplicaciones Lugares Sistema
mié 23 de feb, 2:28 pm
ministerio de la cultura - Buscar con Google - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.google.co.ve/#hl=es&source=hp&biw=1280&bih=802&q=ministerio+de+la+cultura&aq=f&aq
Inicio SIGESP, C.A. SIGESP2011 forja sigesp
Reportes Aldea Universitaria
localhost / localhost / encl ...
http://agn.gob.ve/
Ministerio del Poder Popul...
ministerio de la cultura - B...
La Web Imágenes Vídeos Noticias Libros Traductor Gmail Más
Historial web | Configuración de búsqueda | Acceder
Google
ministerio de la cultura
Buscar
Aproximadamente 35.600.000 resultados (0,15 segundos)
Búsqueda avanzada
Todo
Imágenes
Vídeos
Noticias
Tiempo real
Más
Caracas
Cambiar ubicación
Cualquier fecha
Más reciente
Últimas 24 horas
Últimos 2 días
Última semana
Último mes
Último año
Intervalo personalizado...
Todos los resultados
Orden cronológico
Más herramientas
Ministerio del Poder Popular para la Cultura
HACKED BY kaMtiEz. INDONESIANCODER TEAM - MAGELANGCYBER TEAM @2011.
www.ministeriodelacultura.gob.ve/ - En caché - Similares
Gran Explosión Cultural Bicentenaria
Plataformas Culturales
Atención al Ciudadano
Proyectos
Gabinetes Estadales
Ministerio
Oficinas de enlace
Especiales Informativos
Más resultados de ministeriodelacultura.gob.ve »
Ministerio del Poder Popular para la Cultura - Plataformas Culturales
Plataformas Culturales. Tras la creación del Ministerio del Poder Popular ...
www.ministeriodelacultura.gob.ve/index.php?... - En caché - Similares
Ministerio del Poder Popular para la Cultura - Gran Explosión ...
14 Ago 2010 ... Ministerio del Poder Popular para la Cultura, Es el órgano ...
www.ministeriodelacultura.gob.ve/index.php?... - En caché
Ministerio del Poder Popular para la Cultura - Atención al Ciudadano
Ministerio del Poder Popular para la Cultura, Es el órgano rector, en ...
www.ministeriodelacultura.gob.ve/index.php?... - En caché - Similares
Mostrar más resultados de ministeriodelacultura.gob.ve
Noticias sobre ministerio de la cultura
Ministerio de Cultura define cobros a parques y museos
hace 5 horas
El Ministerio de Cultura y Deporte reformó el acuerdo que establecía el cobro opr ingreso a parques nacionales y museos, que oscilan de Q5 a Q25 para ...
Prensa Libre
Las competencias taurinas serán transferidas a Cultura

[Anexo 02]

```
root@cesar-VGN-CR131E: /var/log/honeypot
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@cesar-VGN-CR131E:/var/log/honeypot# cat honeyd.log
2011-04-22-21:50:19.6025 honeyd log started ------
2011-04-22-21:50:23.3792 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-21:51:15.4416 udp(17) - 172.17.16.241 67 255.255.255.255 68: 380
2011-04-22-21:51:26.5673 udp(17) - 172.17.16.241 67 255.255.255.255 68: 380
2011-04-22-21:51:29.5992 udp(17) - 172.17.16.241 67 255.255.255.255 68: 380
2011-04-22-21:51:32.6669 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-21:51:36.7909 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-21:51:39.1468 udp(17) - 172.17.16.241 67 255.255.255.255 68: 388
2011-04-22-21:51:39.2128 udp(17) - 172.17.16.241 67 255.255.255.255 68: 388
2011-04-22-21:52:42.1508 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-21:52:49.5306 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-21:53:43.7108 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-21:53:51.4446 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-21:54:53.4669 udp(17) - 172.17.16.241 67 255.255.255.255 68: 380
2011-04-22-21:55:01.7865 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
```

```
root@cesar-VGN-CR131E: /var/log/honeypot
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
2011-04-22-22:07:57.0343 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:08:48.3307 icmp(1) - 10.255.151.254 200.84.37.185: 8(0): 28
2011-04-22-22:08:59.8464 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:10:09.0582 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:11:19.4641 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:12:28.8260 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:13:38.0977 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:14:47.3876 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:14:55.5254 udp(17) - 172.17.16.241 67 255.255.255.255 68: 380
2011-04-22-22:15:57.7034 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:16:16.7908 udp(17) - 172.17.16.241 67 255.255.255.255 68: 386
2011-04-22-22:16:30.9503 udp(17) - 172.17.16.241 67 255.255.255.255 68: 388
2011-04-22-22:16:32.3403 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:16:34.0785 udp(17) - 172.17.16.241 67 255.255.255.255 68: 380
2011-04-22-22:16:47.8018 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:16:54.3116 udp(17) - 172.17.16.241 67 255.255.255.255 68: 380
2011-04-22-22:17:11.5172 udp(17) - 172.17.16.241 67 255.255.255.255 68: 388
2011-04-22-22:17:15.9630 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:18:33.4805 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:19:41.3245 udp(17) - 172.17.16.241 67 255.255.255.255 68: 384
2011-04-22-22:19:41.3644 udp(17) - 172.17.16.241 67 255.255.255.255 68: 384
2011-04-22-22:19:42.8124 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:19:42.9564 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:20:13.4815 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:20:17.5193 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:20:52.0684 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:22:01.3581 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:22:18.6556 tcp(6) S 10.138.3.50 49258 190.79.168.48 52858 [Windows
 2000 RFC1323]
2011-04-22-22:22:51.7125 udp(17) - 172.17.16.241 67 255.255.255.255 68: 388
2011-04-22-22:22:51.7645 udp(17) - 172.17.16.241 67 255.255.255.255 68: 388
2011-04-22-22:22:56.2164 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:23:10.6220 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:23:15.5138 udp(17) - 172.17.16.241 67 255.255.255.255 68: 442
2011-04-22-22:23:18.6563 tcp(6) E 10.138.3.50 49258 190.79.168.48 52858: 0 0
2011-04-22-22:24:15.4519 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
2011-04-22-22:24:21.0538 udp(17) - 172.17.16.241 67 255.255.255.255 68: 382
```

```
root@cesar-VGN-CR131E:/var/log/honeypot# cat honeyd.log.2
2011-04-19-20:33:26.9845 honeyd log started ------
2011-04-19-22:32:28.7570 honeyd log stopped ------
2011-04-20-23:02:14.1250 honeyd log started ------
2011-04-21-02:00:09.7633 honeyd log stopped ------
root@cesar-VGN-CR131E:/var/log/honeypot#
```