UNIVERSIDAD FRANCISCO GAVIDIA
FACULTAD DE INGENIERIA Y ARQUITECTURA

TRABAJO DE GRADUACION.

TESIS:
DISEÑO Y DESARROLLO DE HONEYNETS VIRTUALES UTILIZANDO VMWARE, PARA LA DETECCION DE INTRUSOS INFORMATICOS

PRESENTADO POR:

VENTURA PENADO, YESENIA LISSETH
RODRIGUEZ CAMPOS, NELSON ALFREDO

PREVIA OPCIÓN AL TITULO DE:
INGENIERO EN TELECOMUNICACIONES

SAN SALVADOR, MARZO 2008

UNIVERSIDAD FRANCISCO GAVIDIA

RECTOR
ING. MARIO ANTONIO RUIZ RAMÍREZ

SECRETARIA GENERAL
Licda. TERESA DE JESÚS GONZALEZ DE MENDOZA

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO
ING. ROBERTO ARISTIDES CASTELLON MURCIA

UNIVERSIDAD FRANCISCO GAVIDIA

ORGANIZACIÓN DE TRABAJO DE GRADUACIÓN

DECANO

ING. ROBERTO ARISTIDES CASTELLON MURCIA

ASESOR

ING. WILFREDO SANTAMARIA

JURADO EVALUADOR

ING. JOSE RAUL PINEDA

ING. LUIS GUSTAVO CISNEROS

ING. FEDERICO LEOPOLDO SILIEZAR

UNIVERSIDAD FRANCISCO GAVIDIA

TRABAJO DE GRADUACION APROBADO POR

F._____

ING. JOSE RAUL PINEDA

PRESIDENTE

F._____

ING. LUIS GUSTAVO CISNEROS

VOCAL

F._____

ING. FEDERICO LEOPOLDO SILIEZAR

VOCAL

SAN SALVADOR, MARZO 2008.

No. 32848

Universidad Francisco Gavidia

Exp. 03/01-2007/03-IT

ACTA DE LA DEFENSA DE TRABAJO DE GRADUACION

Acta No.560 Mes de Marzo de 2008

En el Salón de Usos Múltiples del Edificio A de la Universidad Francisco Gavidia, a las doce horas y treinta minutos del día veinticinco de marzo de dos mil ocho; siendo estos el día y la hora señalada para el análisis y la defensa del trabajo de graduación: ***"DISEÑO Y DESARROLLO DE HONEYNETS VIRTUALES UTILIZANDO VMWARE, PARA DETECCIÓN DE INTRUSOS INFORMATICOS"*** *Presentado por los estudiantes: Nelson Alfredo Rodríguez Campos y Yesenia Lisseth Ventura Penado. De la Carrera de:* ***INGENIERIA EN TELECOMUNICACIONES.***

Y estando presentes los interesados y el Tribunal Calificador, se procedió a dar cumplimiento a lo estipulado, habiendo llegado el Tribunal, después del interrogatorio y las deliberaciones correspondientes, a pronunciarse por este fallo:

Aprobado
Nelson Alfredo Rodríguez Campos

Aprobado
Yesenia Lisseth Ventura Penado

Y no habiendo más que hacer constar, se da por terminada la presente.

Presidente/a
Ing. Jose Raul Pineda Lemus

Vocal
Ing. Luís Gustavo Cisneros Paniagua

Vocal
Ing. Leopoldo Federico Siliezar Ledezma

Alumno:
Nelson Alfredo Rodríguez Campos

Alumna:
Yesenia Lisseth Ventura Penado

Tecnología, Humanismo y Calidad"

AGRADECIMIENTOS

“Todo lo puedo en Cristo que me fortalece” Filipenses 4:13

A mi Señor Jesucristo por brindarnos la sabiduría y ser nuestro guía en todo momento y fortalecernos cuando nos sentíamos débiles.

A mis padres María de Ventura y Juan Ventura por apoyarme en mi vida profesional y personal, colocando sus experiencias y enseñanzas desde temprana edad.

A mis hermanas Roxana Ventura y Griselda Ventura por darme ánimos de seguir adelante aun cuando hubo dificultades y obstáculos en nuestras vidas.

A mis amigos Guadalupe Carballo, Enrique Fernández, Ernesto Gómez y Delmy Reyes por sus sinceros deseos en que pudiera finalizar mis estudios universitarios.

A mi compañero Nelson Rodríguez por estar a mi lado compartiendo las buenas y malas experiencias, así como los momentos difíciles durante la elaboración del presente trabajo de graduación, apoyándome y brindándome ánimos para vencer los obstáculos que se nos presentaron durante el proceso.

Al nuestro asesor Wilfredo Santamaría por guiarnos y corregirnos durante la elaboración del trabajo de graduación.

A todos aquellos amigos y hermanos que me llevan en sus oraciones y que de alguna forma me brindan sus mejores deseos a que mis metas se cumplan para beneficio personal y profesional.

YESENIA LISSETH VENTURA PENADO

AGRADECIMIENTOS

A Dios altísimo todopoderoso, por haber derramado siempre bendiciones en nosotros, por orientarnos y permitirnos padre la conclusión de este paso en nuestras vidas. Este logro como muchos otros que tu pones en mi camino padre es para ti.

A mi papa en algún lugar cerca de Dios padre. Gracias por que siempre estás conmigo, por haberme enseñado los valores de esta vida y apoyarme hasta cuando pudiste.

A mi madre Francis y abuelita Clarita, mis dos madres, por todo el apoyo, el soporte y el cariño incondicional que me han brindado. Gracias por fórjame como soy.

A mi esposa Luz Alicia, por estar a mi lado en los momentos difíciles de esta parte de mi vida, por animarme y apoyarme a seguir siempre adelante, por todo detalle de amor y cariño.

A mis hermanos Jacque y Fran, a quien me han apoyado en cada momento de mi vida y de quienes siempre he recibido todo el cariño, gracias por escucharme siempre y por los consejos que me obsequian, gracias por estar ahí siempre en los momentos de duras o lindas decisiones.

A Yesenia Ventura, por haberme apoyado en todo momento difícil en mi carrera académica, por todos esos momentos difíciles en nuestras vidas que fueron superados. Yese, todas las bendiciones del mundo para ti y tu familia que me recibió, tengo plena fe en que todas tus metas serán alcanzadas.

NELSON RODRIGUEZ

TABLA DE CONTENIDO

PÁGINA

RESUMEN

El presente trabajo de graduación trata de los sistemas de seguridad y las herramientas adicionales para resguardar la información, siendo esta una herramienta complementaria a las tradicionales en el mercado. Se detalla un diseño de esquemas propuestos acorde a la estructura de la Universidad Francisco Gavidia, que a su vez puede ser utilizado para organizaciones interesadas en la protección de sus activos informáticos. El documento conlleva una estructura de cuatro capítulos, a continuación se hace una breve descripción de cada uno de ellos.

Capitulo 1.
Capitulo que hace mención a los aspectos generales de la seguridad de la información, se plasma el marco teórico sobre diseño, el tipo de intrusos, honeynets, herramientas de virtualización vmware y aspectos legales.

Capitulo 2.
Este capítulo comprende la investigación de campo, el objetivo de la investigación, la metodología utilizada y los resultados obtenidos en base a ella.

Capitulo 3.
Capítulo en el cual se desarrollo el diagnostico de la situación actual de la red de la Universidad Francisco Gavidia en lo que respecta la parte de seguridad así mismo se realiza el análisis de la factibilidad económica y técnica y al finalizar se presenta una propuesta de diseño de la honeynet virtual así como una propuesta de diseño amoldada a la Universidad Francisco Gavidia.

INTRODUCCIÓN

En el transcurrir del tiempo la transferencia y el manejo de información de forma virtual se han convertido en una prioridad en la vida cotidiana pero de igual manera las amenazas y la el fraude delictivo han evolucionado al mismo ritmo. Actualmente la protección de sistemas y de la información se vuelve vital para todas las instituciones independientemente el rubro o negocio que esta contenga.

Es por tal motivo que el presente trabajo de graduación tiene como finalidad ofrecer una propuesta de diseño de una herramienta de seguridad complementaria a las necesidades actuales de la Universidad Francisco Gavidia (UFG).

La propuesta del diseño se integrará con el conjunto de soluciones que la Dirección de Tecnología y Comunicaciones de la UFG (DTC) tiene como objetivo implementar en su desarrollo, según su planificación de mantener seguros los sistemas y la red de telecomunicaciones y datos. Se indican los objetivos que constituyen la parte vital del porque desarrollar un diseño de una herramienta de este tipo, fortaleciendo así las infraestructuras virtuales de la institución.

ASPECTOS GENERALES DEL PROYECTO

Objetivos.

Objetivo general.

Presentar el diseño una herramienta de seguridad informática general para la Universidad Francisco Gavidia, cuyo fin será proporcionar una solución para el fortalecimiento de la seguridad, por medio de un sistema que permita capturar, controlar y proteger los servidores de los ataques de intrusos informáticos en la infraestructura de red de la Universidad Francisco Gavidia.

Objetivos específicos.

- Presentar el desarrollo de Honeynets virtuales con múltiples sistemas operativos en una misma computadora basada en los requerimientos de la infraestructura de la red de la Universidad Francisco Gavidia.

- Presentar un diseño para la configuración del Control de Datos en el Honeynet VMware utilizando IPTables, la captura de datos utilizando herramientas como snort y realizar pruebas que garanticen el funcionamiento del sistema.

- Elaborar un prototipo de solución para la infraestructura de la red de la Universidad Francisco Gavidia.

Alcances y limitaciones del proyecto.

Alcances

El presente trabajo de graduación tiene como enfoque el desarrollar un diseño genérico para que pueda ser tomado como base general para cualquier institución u organización para la implementación de herramientas adicionales de seguridad.

Desarrollar un diseño para la implementación de las herramientas adicionales de seguridad honeynets para la Universidad Francisco Gavidia, específicamente para la infraestructura que administra y maneja la dirección de tecnología y comunicaciones, con la finalidad de reforzar las aéreas débiles en la red las cuales pueden repercutir a los procesos y actividades de la Universidad Francisco Gavidia.

La fase de implementación del proyecto en la infraestructura total de la UFG no está contemplada debido a que solo se caracterizará el prototipo del diseño en una porción controlada de red en la infraestructura de la UFG.

Se presentará un prototipo el cual está orientado a ser aplicable al área administrativa de la dirección de tecnología y comunicaciones, para comprobar que es una propuesta de solución complementaria de seguridad para los sistemas informáticos viable.

Delimitación geográfica.

La investigación de factibilidad y de diseño del presente trabajo de graduación se hace en base a la infraestructura del la Universidad Francisco Gavidia.

Se presenta una propuesta de diseño general y genérica que puede ser utilizada para el desarrollo de cualquier organización o institución con los cambios que de cada una de ellas requiera según su situación. Así mismo de presenta la propuesta para que sea desarrollada en la UFG en base al estudio de factibilidad y la investigación realizada en ella.

Delimitación específica.

El presente trabajo de graduación tiene como delimitación especifica la infraestructura que maneja la dirección de tecnología y comunicaciones. El prototipo y pruebas serán realizados en una de las dependencias de este departamento en el edificio de bibliotecas y laboratorios especializados.

Delimitación temporal.

La delimitación temporal para la realización del prototipo será de un período de 60 días calendario, los cuales incluyen el tiempo de las pruebas.

Limitaciones.

Al considerar implementar el sistema de seguridad en su totalidad se requerirá que se disponga de una computadora para este propósito, con lo básico en hardware y software las cuales se describen en el presente trabajo de graduación.

Para el crecimiento del sistema VMware será necesario el crecimiento en hardware y software conocido como sistemas operativos y las licencias de dichos sistemas, tales como en el caso de Microsoft Windows.

El trabajo de graduación está orientado para que sea desarrollado bajo el sistema operativo Linux como base y no en la plataforma de Windows, debido a que este último requiere de licenciamiento.

El prototipo que se plantea, será realizado bajo un ambiente controlado y separado ya que como una limitación es el realizar pruebas bajo el entorno de producción de la Universidad Francisco Gavidia.

Justificación.

La finalidad principal es desarrollar y presentar el diseño y prototipo de una herramienta complementaria de seguridad informática para las infraestructuras de redes de datos. Esta permitirá resguardar la integridad de la infraestructura universitaria la cual no cuenta con un recurso de esta índole.

Esta herramienta se denomina honeynets, la cual se define como una red honeypots (en inglés tarros de miel, el cual puede entenderse como algo tentador que resulta ser una trampa), siendo ésta un aplicativo que se desarrolla en computadora(s) cuya intención es atraer aquellos usuarios o sistemas malintencionados, simulando ser sistemas vulnerables o débiles a los ataques.

Pero en verdad es una herramienta de seguridad informática, utilizada para recoger información sobre los atacantes y sus técnicas. Los honeypots 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 suceso.

El presentar el desarrollo de diseño honeynets, beneficiará directamente a la Universidad Francisco Gavida y en caso puntual a la Dirección de Tecnología y Comunicaciones que es la entidad designada para garantizar y velar por un óptimo funcionamiento de las estructuras de cómputo, telecomunicaciones y

servicios en línea, estructuras las cuales deben protegerse valiéndose de todas las estrategias y herramientas como las que aquí se presentan.

Las herramientas de seguridad informática en el campo de las telecomunicaciones toman un papel protagónico en todas las infraestructuras con igual o mayor importancia de lo que representa la seguridad física misma, ya que se debe proteger servicios importantes como lo son aquellos de transferencia de dinero, almacenamiento y manejo de información.