CONCLUSIONES

A través de cada uno de los capítulos del presente documento se han enumerado una serie herramientas de seguridad que forman parte del sistema de defensa de una red y que, controlan su acceso, protegen los servicios y los recursos compartidos de la misma y permiten tener un entorno más confiable y seguro.

En la actualidad existen muchos programas que protegen los activos de las organizaciones; antivirus, escáneres de vulnerabilidades, *firewalls* y sistemas de detección de intrusos son algunos de los programas que permiten tener un mejor control sobre la disponibilidad y uso de los recursos de un sistema, todos estos programas de protección responden a una creciente necesidad de saber que está pasando en el sistema y del estado de la información que se resguarda. La simple instalación de dichos programas no garantiza un control adecuado de los recursos de una red; para garantizar un nivel de seguridad aceptable, los encargados de la seguridad deben tener amplios conocimientos sobre redes, sobre los puntos vulnerables de las redes, y de las herramientas que puede utilizar y las ventajas que puede obtener de las mismas.

En el presente trabajo, se hizo la descripción de las herramientas más usadas debido a su eficacia en la protección de ciertas áreas de la red, desde el sistema operativo hasta una arquitectura de múltiples computadoras en red.

Para el reforzamiento de la seguridad del sistema operativo se utilizó *OpenSSH* y Bastille Linux con muy buenos resultados, *OpenSSH* permitió crear conexiones cifradas tanto al equipo en que se implementó el *firewall*, como al equipo en que se implementó el detector de intrusos. El servidor SSH se configuró de tal manera que no se permite el logueo directamente como root, con lo cual se protege dicha cuenta, además se limitaron los intentos fallidos al momento de ingresar la contraseña y el número de terminales que se pueden obtener por sesión. Con esto se logró un mejor control del acceso a los equipos en que se van a desempeñar las labores de monitoreo y administración de la red.

Con Bastille Linux se hizo todo el proceso de reforzamiento del sistema operativo o *hardening*, se deshabilitaron comandos como mount, ping y at, que por defecto están habilitados en los sistemas tipo Linux y que representan vulnerabilidades para la seguridad del sistema, también fueron deshabilitados servicios como telnet y ftp por tratarse de servicios inseguros, se deshabilitaron los servicios de impresión, se limitó el número de procesos a ejecutar por usuario y se estableció una máscara de usuario adecuada, entre otras acciones que Bastille permitió configurar mediante una interfaz muy intuitiva y fácil de usar. Se obtuvieron muchas ventajas con el uso de este software, pero la más importante fue el reforzar el sistema sin la necesidad de ejecutar comandos o editar archivos como generalmente se realiza en los sistemas Linux.

En el área de protección de contraseñas y ataques de fuerza bruta la librería Cracklib y Johh the Ripper son las dos herramientas que se utilizaron para defender el sistema. Cracklib es una librería que forma parte de la instalación por defecto en los sistemas Linux actuales y únicamente se realizó la configuración de la misma para tener una forma de asegurar que las contraseñas de los usuarios de la red fuesen fuertes. Por otro lado John the Ripper, un programa muy eficiente para descifrar contraseñas, permitió detectar contraseñas débiles, lo que brindó una mayor confiabilidad en el sistema, ya que se cubrió el mismo objetivo, la protección de contraseñas, desde dos puntos de vista diferentes, uno como defensor y el otro como atacante.

Para detectar y corregir los errores en configuración del sistema operativo y las vulnerabilidades de las aplicaciones implementadas en el equipo que se utilizó como detector de intrusos, se utilizó Nessus, un escáner de vulnerabilidades muy efectivo que aprovecha todos los fallos en la configuración del sistema, los huecos de seguridad y las ventajas que proporcionan las instalaciones por defecto. Con el uso de Nessus en el equipo se detectaron más de 190 vulnerabilidades, 55 de alto riesgo, que se relacionaron con la falta de actualización del sistema operativo, las vulnerabilidades de riesgo medio y bajo se relacionaron con la actualización de librerías y huecos de seguridad en la configuración del servidor web, esto permitió conocer los puntos débiles del equipo y las aplicaciones y hacer las correcciones necesarias para proteger el sistema.

En la configuración de la red se consideró una zona desmilitarizada con un servidor web; para detectar las vulnerabilidades web en esta zona, se utilizó Nikto, herramienta basada en *Perl* que ayudó a detectar ciertos problemas que tuvo el servidor web al estar expuesto en Internet, como la vulnerabilidad Cross Site Scripting y el problema de tener la indexación de directorios activa. Los resultados obtenidos fueron bastante buenos ya que esta herramienta permitió detectar vulnerabilidades específicas que no fueron detectadas por Nessus.

Una parte muy importante en el sistema de defensa es Wireshark, herramienta con la que se pudo observar el tráfico en la red, origen y destino de dicho tráfico, protocolos utilizados, las conexiones hechas, y se pudo dar el seguimiento a las conexiones establecidas. Toda esta información permite saber que uso le dan los usuarios a los recursos disponibles en la misma, además de determinar actividades que ocupan un ancho de banda muy grande en la red y en general, tener conocimiento de lo que ocurre en la red para implementar un mejor control.

El *firewall* y el Sistema de Detección de Intrusos constituyen dos elementos importantes en el sistema de defensa de la red. Para la creación del *cortafuegos* se utilizó Turtle *Firewall*, programa que facilitó la tarea de crear las reglas de filtrado en el orden correcto, con una interfaz web amigable. Como política se estableció el denegar todo por defecto y se crearon ciertas reglas para permitir el tráfico necesario, como *Secure Shell*, http y https. Con la correcta implementación del *firewall* se logró un mejor control sobre las conexiones entrantes y salientes del entorno de red y se obtuvieron los conocimientos necesarios para crear una configuración adecuada y acorde con los requerimientos de la red.

El Sistema de Detección de Intrusos se implementó con Snort en modo de detección de intrusos, además se utilizó BASE, con lo cuál se logró tener los datos de detección en una base de datos en forma ordenada y organizada y con una interfaz web fácil de usar. Con Snort se logró un control más eficiente sobre las actividades de los usuarios dentro de la red y se pudo aseguró la detección de actividades peligrosas comparándolas con las firmas de ataques conocidos. También se realizaron pruebas sobre la creación de reglas que, aunque no se incluyen como ataques en la base de firmas, se pueden implementar para alertar sobre ciertas actividades en la red, como evitar que se visiten algunos sitios web; es decir, el detector de intrusos también sirve para alertar sobre actividades que no son consideradas como ataques.

Es claro que la correcta implementación de un *firewall* y un Sistema de Detección de Intrusos toma cierto tiempo y práctica y generalmente se pone a prueba su eficacia en ataques reales, cuando la red está expuesta a amenazas constantes, pero durante este trabajo, con base en las pruebas realizadas, se logró verificar el correcto funcionamiento de ambas herramientas y se creó una configuración apropiada para el tipo de servicios que brinda la red.

Finalmente, en el capítulo 6 se implementa una práctica sobre el reforzamiento de seguridad o *hardening* en el sistema operativo con el uso de la herramienta Bastille Linux, está práctica tiene como objetivo que el estudiante comprenda la importancia de la herramienta para el reforzamiento de la seguridad del sistema y para ello se realiza la instalación y configuración de dicha herramienta y se realizan algunas pruebas para verificar su correcto funcionamiento.

Mediante el correcto uso de las herramientas mencionadas se logró conocer los puntos vulnerables de la red y se implementaron las correcciones pertinentes para tener un control y administración segura de los recursos y servicios de la red, así como obtener el conocimiento necesario para la configuración y prueba de las herramientas y lograr su mejor desempeño.

En general, se creó un sistema de defensa completo con base en herramientas de *software libre* que permiten proteger de una manera muy efectiva los activos de una red y que contribuyen a un mejor desempeño de la misma. Estas herramientas constituyen por lo tanto un paquete importante de trabajo para un conocedor de la red y deben ser vistas como herramientas adaptables, que sin duda seguirán desarrollándose tanto como se modifiquen las necesidades de seguridad en cada área de las redes. Asimismo, se puede afirmar que quien decida implementar el sistema de defensa para una red propuesto aquí con herramientas de software libre puede tener la certeza de que como administrador de seguridad con conocimientos suficientes puede lograr una protección aceptable.

En lo personal, el presente trabajo me permitió adquirir conocimientos sobre seguridad de las redes en forma general, y en particular, sobre el tipo de sistemas de seguridad que se pueden implementar en cualquier red, las necesidades de seguridad y la forma de satisfacerlas con herramientas de *software libre*, la instalación y configuración de dichas herramientas para obtener su mejor desempeño y el manejo de la información obtenida para asegurar áreas vulnerables.

La administración de seguridad es un campo de constante actualización que requiere una correcta supervisión e investigación de los nuevos mecanismos de ataque y de defensa de un sistema y de las nuevas tecnologías y sus vulnerabilidades, por lo que se convierte en un campo de estudio muy complejo y muchas veces complicado, pero también lo convierte en un campo muy interesante para aquellas personas que ven la seguridad de los sistemas como un desafío y la solución de problemas como una forma de vida.