CONCLUSIONES

El trabajo de tesis presentado corresponde al diseño e implantación de un motor de detección de tráfico malicioso para el Telescopio de Seguridad de la UNAM como una fuente de información, proporcionando un mecanismo complementario para la atención a incidentes de seguridad informática dentro y fuera de RedUNAM.

El diseño de un mecanismo de detección en redes de gran tamaño y complejidad como RedUNAM implica un análisis exhaustivo del proceso de manejo y almacenamiento de la información debido a la gran cantidad de datos involucrados.

La elección de diferentes tecnologías y técnicas utilizadas depende de la información que se desea obtener, del enfoque de uso de dicha información y del o los sistemas con los cuales deberá interactuar. En este caso, debido a la necesidad de interacción de un mecanismo de detección con el proceso de atención a incidentes de seguridad informática dentro de RedUNAM, y al enfoque de investigación en técnicas de detección de tráfico malicioso, las tecnologías y técnicas utilizadas (honeypots, IDS, análisis estructurado de tráfico de red) resultaron convenientes y proporcionan una base para un sistema de monitoreo complejo que permita identificar de manera acertada gran variedad de amenazas dentro la red de la Universidad.

El diseño de la Darknet como un motor de detección y del sistema de procesamiento de la información para su implantación en el Telescopio de Seguridad de la UNAM, ofrecen una gran versatilidad para la generación de nuevos mecanismos que apoyen en las tareas de detección, procesamiento y almacenamiento de la información. Una de las razones es el diseño modular que permite cierta independencia entre las tecnologías utilizadas y ofrece la capacidad de tener facilidad de interacción con posibles nuevas herramientas y técnicas de captura, detección y procesamiento de información.

Uno de los principales problemas encontrados durante el desarrollo de este proyecto fue la adaptación de un proceso adecuado para que la Darknet tuviera el mejor rendimiento posible. El rendimiento de la misma con los primeros diseños del sistema era totalmente inadecuado debido a la gran cantidad de tiempo que tomaba en capturar y procesar la información. Después de un análisis y de estudiar distintas

alternativas en diferentes módulos de la Darknet, se logró que la información se manejara de manera eficiente y se pudiera aprovechar en el TSU a partir de un procesamiento en "tiempo real".

Este tipo de sistemas de detección son escasos debido a sus características. Por un lado, se necesita de una inversión de direcciones IP la cual es proporcional a la efectividad del sistema, y por otro lado, tienen un cargado enfoque para el área de investigación por lo que comúnmente es implementado por organismos académicos, de investigación o cuya misión es la generación de tecnologías de seguridad tal como las firmas antivirus.

El tamaño y capacidad de la Darknet UNAM es considerable en términos académicos, incluso es más grande que algunos de los proyectos similares en otras Universidades internacionales. Algunos otros son mucho más grandes ya que conjuntan varias organizaciones como universidades, ISP's, compañías, e incluso departamentos de defensa. Dentro de un ambiente académico a nivel nacional e incluso en Latinoamérica, no se tiene conocimiento de un proyecto similar con las características de la Darknet UNAM, lo cual la convierte en una referencia importante en ese contexto.

Con la información obtenida ahora por el TSU, el UNAM-CERT puede ser también una referencia para la detección de incidentes de seguridad informática dentro y fuera de RedUNAM mediante la notificación de incidentes a las fuentes de eventos detectados. También, gracias a las características de la información obtenida se pueden lograr intercambios de información más detallados con otras organizaciones de seguridad internacionales.

Si bien las tecnologías honeypots no son nuevas, su correcta implementación y sobre todo el buen aprovechamiento de la información generada, representan un campo explotable en el área de la seguridad en cómputo ya que permiten obtener información alternativa o complementaria a la que generan otros tipos de sistemas de detección como los IDS, firewalls, etc.

El sistema completo de la Darknet dentro del TSU aún presenta algunas tareas y retos qué resolver. Se debe hacer énfasis en mejorar los aspectos de rendimiento y la adaptación de nuevas tecnologías de detección ya que mientras mayor y mejor es la información proporcionada, la demanda en recursos físicos de procesamiento y almacenamiento aumenta.

Esta primera versión de la Darknet UNAM cumple con los objetivos propuestos, y es importante mencionar que para optimizar su utilidad, es necesario contar con un proceso de actualización y mejora constante. Las siguientes versiones de la misma y las nuevas características implementadas llevarán poco a poco a una consolidación del Telescopio de Seguridad de la UNAM como efectivo sistema de detección de amenazas de seguridad en cómputo.