INTRODUCCIÓN

A. PLANTEAMIENTO DEL PROBLEMA

El desarrollo y el incremento de las redes de datos alrededor del mundo han impulsado la creación de mecanismos para compartir, transferir o distribuir información por medios digitales. La facilidad, eficiencia y conveniencia de utilizar medios electrónicos implica, hasta cierto punto, exponer dicha información a determinadas amenazas que existen dentro de este mundo digital.

Estas amenazas potenciales como virus, gusanos, ataques dirigidos, negación de servicio (DoS), escaneos, botnets, spam, etc. si bien en concepto no son nuevas, durante los últimos años han ido evolucionando y adaptándose a los nuevos mecanismos de comunicación digital y en general al desarrollo de Internet. Algunas de sus principales características son la automatización de su distribución y la forma en que se aprovechan de las vulnerabilidades de sus objetivos. Esto significa que independientemente del daño o impacto que ocasionan, su existencia implica mayores consideraciones al momento de utilizar alguno de estos medios de comunicación digital. Tomando esto en cuenta, es entendible suponer la necesidad de poder identificar el origen de dichas amenazas con la finalidad de aplicar algún mecanismo de mitigación.

En la actualidad existen diversos mecanismos y soluciones para poder identificar anomalías en una red de datos y hasta cierto punto corregirlas. Herramientas como los sistemas de detección de intrusos (Intrusion detection system o IDS por sus siglas en inglés), sistemas de prevención de intrusos (Intrusion prevention system o IPS), firewalls, analizadores de protocolos o "sniffers", antivirus, correlacionadores de eventos (SIEM), etc. permiten monitorear y analizar la actividad del tráfico en la red, por otro lado, herramientas alternativas como las tecnologías honeypot permiten hacer un análisis y detección de tráfico de red malicioso por medio de una simulación o interacción real bajo un ambiente controlado con diversas entidades maliciosas.

Generalmente, cualquiera de estos mecanismos funciona de manera local o perimetral, es decir, pueden trabajar instalados directamente en el equipo o pueden estar monitoreando la actividad de la red por medio de un dispositivo en el perímetro de la misma. En concepto tienen muchas similitudes y la principal diferencia es solamente el alcance: actividad local o actividad en la red.

Existe otro tipo de detección de tráfico de red malicioso: las "Darknets" o "telescopios de red". En realidad es un concepto ambiguo porque no existe una definición formal que establezca sus características, sin embargo, su esquema consiste en una detección por medio de análisis de tráfico mediante diversas herramientas como IDS, honeypot, flujos, etc. desplegadas en infraestructuras de red con direcciones IP "no asignadas" o en los propios "core" de las redes. Dicha técnica no es nueva, sin embargo, a nivel mundial son escasas las implementaciones que permiten la detección de tráfico malicioso y clasificación de incidentes de seguridad en cómputo o monitoreo de actividad de Internet. Algunas de ellas, de las cuales se hablará más adelante, son CAIDA, The Darknet Project, Internet Motion Sensor, IBN, entre otros. En México no se tiene conocimiento de un proyecto similar, por lo que la implementación de la Darknet en el Telescopio de Seguridad de la UNAM representa la creación de una referencia importante en este tipo de esquemas.

La principal motivación para el desarrollo de este proyecto proviene de la necesidad de proporcionar mayor información sobre cada incidente reportado dentro de RedUNAM por parte de la Subdirección de Seguridad de la Información/UNAM-CERT. Esto representa la creación de una fuente de información y detección de incidentes de seguridad dentro y fuera de la red de la Universidad.

Implementado en entornos más pequeños y sencillos, funciona como un complemento a los sistemas de detección de intrusos, permitiendo generar estadísticas y referencias importantes de la actividad de tráfico de red malicioso.

B. Objetivo

El objetivo de este trabajo es presentar la propuesta de una Darknet como un motor de detección de tráfico de red malicioso para ser implementado en el Telescopio de Seguridad de la UNAM, explicando su diseño y características de funcionamiento, las ventajas que tiene respecto a otros tipos de herramientas, la comparación entre la UNAM-Darknet con otros modelos similares y finalmente, el análisis de la implementación puesta en producción.

C. Estructura de la tesis

El trabajo consta de seis capítulos fundamentales. El primer capítulo abarca el marco teórico de referencia que trata los conceptos relacionados con los sistemas de detección de tráfico malicioso, sistemas de monitoreo y sistemas de análisis de tráfico de red en general. Es necesario conocer y entender dichos tópicos debido a que el funcionamiento general del proyecto propuesto está basado en varios de ellos y con algunos otros tiene similitudes en cuanto a los objetivos que persiguen. El segundo capítulo presenta los fundamentos del diseño de una Darknet, sus características, funcionamiento, tipos, esquemas de implementación y un análisis al modelo de detección. En el tercer capítulo se presenta el diseño de un mecanismo de detección de tráfico malicioso para RedUNAM. Abarca el análisis del problema y de todas las consideraciones necesarias para la implementación en la red académica más grande de México. En el cuarto capítulo se profundiza en la estructura general de la herramienta desarrollada, explicando a detalle su esquema de funcionamiento ya implementado en RedUNAM y algunas otras características disponibles en el motor de detección. El quinto capítulo aborda el análisis de la implantación de la Darknet tomando en cuenta el aprovechamiento de la información recopilada, analizada, procesada y almacenada en el Telescopio de Seguridad de la UNAM.

Finalmente, en el sexto capítulo se presentan las conclusiones de la tesis las cuales abordan las deducciones finales de los resultados, ventajas y desventajas identificadas, limitaciones, capacidades posibles y las perspectivas sobre desarrollos futuros de la herramienta.