CAPÍTULO 3

DISEÑO DE UN MECANISMO DE DETECCIÓN DE TRÁFICO MALICIOSO PARA REDUNAM

En este 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 de una Darknet en la red académica más grande de México.

3.1 ANÁLISIS DEL PROBLEMA

RedUNAM es una red de datos de gran escala en términos de ambientes académicos. Su infraestructura se compone de miles de dispositivos entre equipos, servidores, switches, routers, etc. Debido a la grandeza de la Universidad tanto en cuestión geográfica como su población de más de 300,000 alumnos[14], se trata de un entorno complejo y una fuente extraordinaria de generación, distribución, transferencia y almacenamiento de información.

En realidad, el monitoreo del tráfico malicioso en RedUNAM es una cuestión demasiado compleja debido a las políticas de administración descentralizada. Esto quiere decir que cada dependencia tiene la responsabilidad de administrar su propia red, por lo que todos los eventos relacionados con tráfico malicioso no están monitoreados por un sistema centralizado, sin embargo, se cuenta con la capacidad técnica de implementar un sistema de detección generalizado a través del Telescopio de Seguridad de la UNAM.

Para el caso de RedUNAM, existe la Subdirección de Seguridad de la Información / UNAM-CERT dependiente de la Dirección General de Cómputo y Tecnologías de la Información y Comunicación (DGTIC). El UNAM-CERT se encarga de la atención a los incidentes de seguridad informática detectados y reportados por diversos mecanismos, sin embargo, la capacidad de detección por medio de métodos alternativos como una Darknet, y el aprovechamiento de ser un entorno académico, representan grandes ventajas para poder mejorar la información que se obtiene sobre

[14] Cifras del año 2010 del Portal de Estadística universitaria http://www.estadistica.unam.mx/numeralia/

tráfico malicioso para fines de detección y respuesta a incidentes y con enfoque también para el campo de la investigación.

3.2 DARKNET COMO MECANISMO DE DETECCIÓN DE TRÁFICO MALICIOSO PARA REDUNAM

La implantación de una Darknet dentro de la infraestructura de RedUNAM es totalmente factible y provechosa. El potencial de dos segmentos clase B[15] públicos permite obtener gran cantidad de información sobre tráfico malicioso dentro y fuera de la Universidad. Si bien no todas las direcciones están destinadas para la Darknet, se tiene un potencial de miles de direcciones IP disponibles para ser utilizadas. El mecanismo de detección de la Darknet está diseñado para procesar la información y generar una fuente de datos para el Telescopio de Seguridad de la UNAM. Como se mencionó en un apartado anterior, es un mecanismo que conjunta varias fuentes de información sobre tráfico de red malicioso entre las que se encuentran honeypots, sensores de spam, IDS, etc. La figura 18 muestra su estructura general.

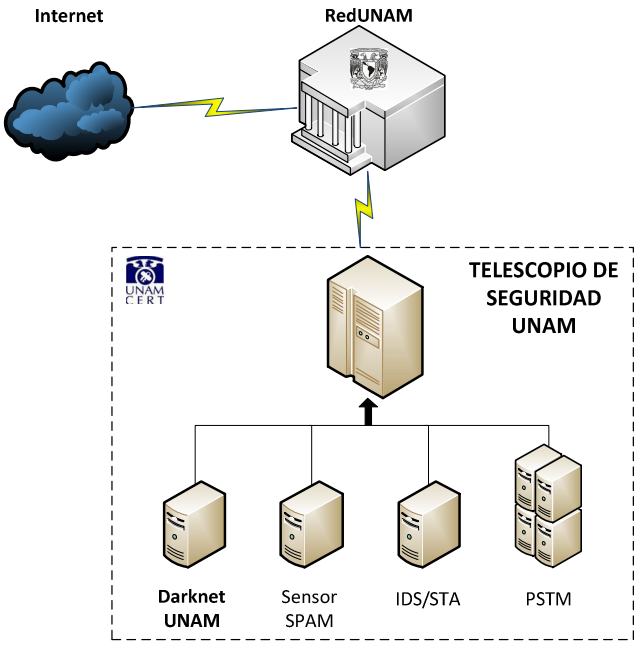

Figura 18. Esquema general del telescopio de seguridad de la UNAM

[15] Un espacio de 131,050 direcciones IPV4

La implantación de la Darknet en el TSU, lo convierte en su principal motor de generación de información debido al gran tamaño de la misma y la cantidad de información que genera.

3.3 Análisis de la infraestructura

RedUNAM consta de dos segmentos clase B, esto quiere decir que se tiene un espacio de direcciones IP públicas de aproximadamente 130,000 hosts. El número total de host en realidad es mayor si considera la gran cantidad de redes privadas con múltiples equipos dentro de ella. La tasa de transferencia de tráfico en los core[16] de RedUNAM, tiene una capacidad de 10Gbps, teniendo enlaces a 1Gbps y 100Mbps según la dependencia, instituto o facultad.

Tomando en cuenta que la Darknet utilizará miles de direcciones IP las cuales recibirán, procesarán y almacenarán el tráfico dirigido hacia ellas, se cuenta con un esquema de conectividad de gigabit ethernet[17]. Es importante señalar que dicho esquema está diseñado para funcionar de manera centralizada, es decir, se cuenta con un sistema principal que realiza las tareas de funcionamiento de la Darknet.

Una vez que la Darknet se enlace con el TSU, se logrará una correlación de eventos y un modelo de detección general sobre el tráfico entrante y saliente. Es muy importante tener presente que por el modelo de administración de la red de la Universidad, no se tiene como objetivo detectar todo evento malicioso o anómalo dentro de RedUNAM, de hecho no es posible detectar alguna amenaza específica si no se relaciona en algún momento con el tráfico de las direcciones IP de la Darknet.

3.4 Diseño de una Darknet para RedUNAM

Para poder definir las características de la Darknet-UNAM, de manera inicial se tomaron en cuenta los siguientes aspectos:

[16] Equipos principales de conectividad de RedUNAM que enrutan el tráfico entre RedUNAM y el exterior
[17] Conectividad con una tasa de transferencia aproximada de 1000 mbps, también conocida como GigaE

- Modelo de la infraestructura de RedUNAM.
- Cantidad de tráfico de red a recibir y procesar.
- Cantidad de información generada para almacenar.
- Recursos físicos de procesamiento y almacenamiento.
- Conectividad entre los servidores de la Darknet y los equipos en el UNAM-CERT.
- Tipos de tecnología a utilizar: honeypots, análisis de flujos, IDS, etc.
- Nivel de interacción y complejidad de la aplicación.
- Tecnologías utilizadas en proyectos similares.

De alguna manera cada punto influyó para definir las características técnicas, lógicas y físicas finales del diseño del motor de detección de tráfico malicioso, tomando siempre como punto fundamental el objetivo de la implementación, que es incorporar esta fuente de detección al Telescopio de Seguridad de la UNAM para mejorar la capacidad de obtención de información de incidentes de seguridad dentro y fuera de RedUNAM.

3.4.1 ALCANCE DE LA DARKNET

El alcance de la Darknet-UNAM tiene los siguientes puntos fundamentales:

- Detección de eventos de tráfico malicioso hacia y desde RedUNAM, involucrados en el espacio de monitoreo de la misma.
- Publicación de los detalles de la información a través del telescopio de seguridad de la UNAM.
- Interacción con el proceso de respuesta a incidentes dentro de RedUNAM por parte del UNAM-CERT.
- Generación de información para fines estadísticos sobre los eventos detectados.

Todo el procesamiento y almacenamiento de información se lleva a cabo en servidores dedicados y es una de las funciones fundamentales del sistema.

La importancia de la implantación de la Darknet como motor de detección de tráfico malicioso, representa la principal fuente de información para el telescopio de seguridad de la UNAM. Por este motivo, el impacto del proyecto es alto en relación a la cantidad de eventos detectados, procesados, almacenados y reportados.

3.4.2 REDIRECCIÓN DEL TRÁFICO "NO ASIGNADO"

Para el funcionamiento de la Darknet se cuenta con un esquema centralizado de recopilación de tráfico de red. Existe un servidor Darknet principal al cual es redirigido todo el tráfico que de manera global en RedUNAM no está asignado. Esto es posible gracias al apoyo por parte del departamento de operación de la red[18] de la DGTIC-UNAM, quienes han configurado todos los dispositivos de enrutamiento correspondientes para poder enviar dicho tráfico.

Debido a la cantidad de tráfico recibido, el enlace entre los dispositivos de enrutamiento y el servidor Darknet es a 1 Gbps en fibra óptica. Esto permite tener una conectividad adecuada para la cantidad de información recibida y transferida, sin embargo, como se verá más adelante, muchos de las principales consideraciones de rendimiento tienen que ver con la capacidad de procesamiento de conexiones de los equipos y con la tasa de transferencia entre el servidor Darknet y los dispositivos de almacenamiento.

La redirección configurada de todos los segmentos no asignados en los routers principales permite que el servidor Darknet reciba todas las conexiones hacia dichos segmentos en lugar de ser desechadas. Esto da la posibilidad de crear la interacción correspondiente con cada una de las conexiones para posteriormente procesar la información y almacenarla en una base de datos. La complejidad de dicha interacción es directamente proporcional con la carga que se demandará al sistema por cada conexión recibida.

[18] Departamento encargado de la configuración, instalación y mantenimiento de los enlaces y dispositivos de conectividad en RedUNAM, perteneciente a la Dirección General de Cómputo y Tecnologías de la Información y Comunicación (DGTIC).

De hecho, como parte de la redirección general, también se reciben todas las conexiones provenientes de segmentos privados que son desechados por los routers cuando se intenta rutear a cualquier segmento bogon. Esto permite detectar ciertos tipos de ataques, sin embargo dichos paquetes no son analizados por la darknet, sino por otros módulos del TSU con tecnologías IDS y de análisis de tráfico estructurado.

La figura 19 muestra la infraestructura general de la Darknet UNAM.

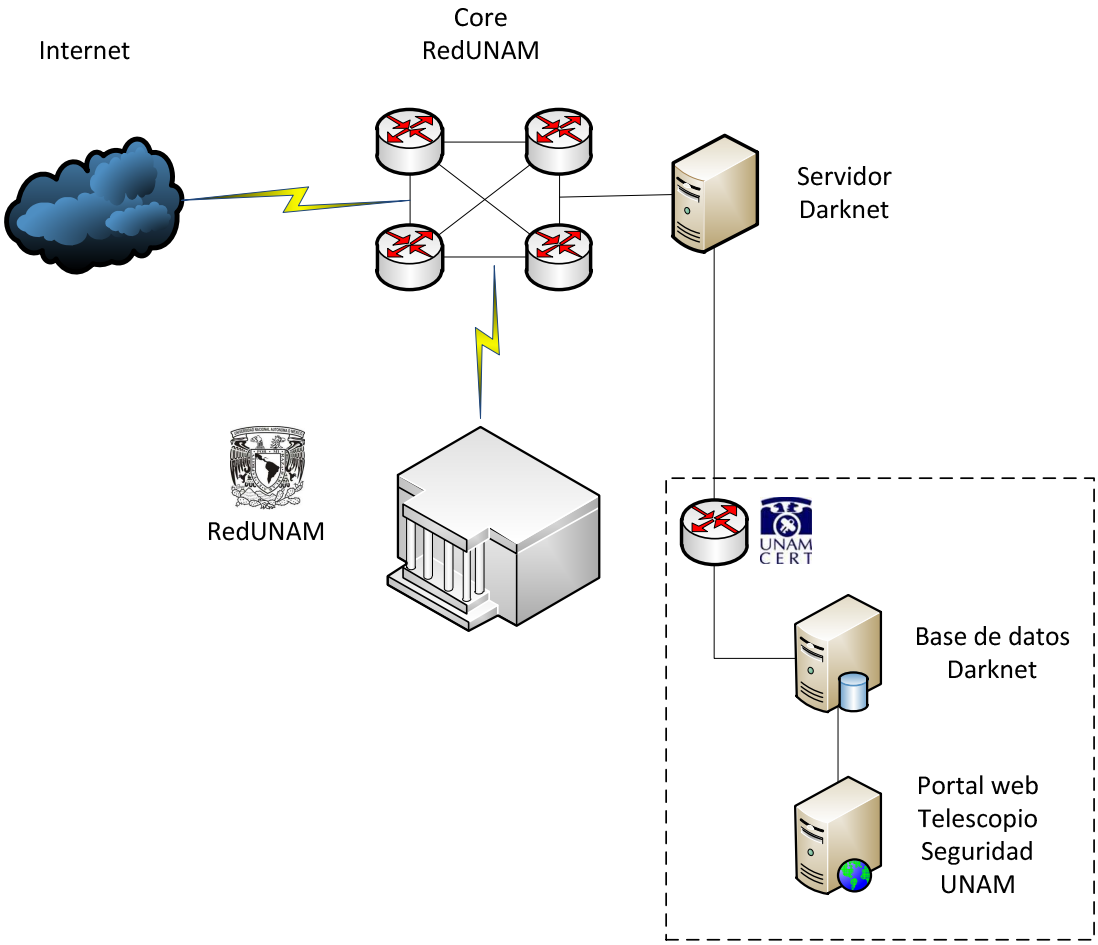

Figura 19. Esquema general de la Darknet UNAM

3.4.3 CONFIGURACIÓN DE LOS SERVIDORES

Los servidores de la Darknet tienen el rol principal de recibir el tráfico de red hacia las direcciones no utilizadas y crear una interacción. En ésta se incluyen aspectos como la

emulación de servicios, utilización de tecnologías de análisis de tráfico y detección de patrones. Para poder realizar dichas tareas, el servidor principal funciona con al menos dos interfaces de red: una para recepción de tráfico y otra para administración remota. Como ya se mencionó, una de ellas corresponde a una interfaz de fibra óptica 10/100/1000 que tiene una conexión con el router que envía el tráfico. La otra es una interfaz Ethernet UTP 10/100/1000, sin embargo como solo se utiliza para administración de sistema, la funcionalidad a 100Mbps es suficiente.

Los equipos cuentan con un sistema operativo GNU/Linux Debian mínimo y personalizado con ciertas características específicas de algunas herramientas de seguridad y propiamente del sistema desarrollado.

Es importante mencionar que en esta primera etapa del proyecto se tiene un esquema de un servidor Darknet principal. Esto se debe a motivos de pruebas, recursos y diseño general, sin embargo, para las siguientes fases de la Darknet se tienen proyectadas algunas características de cómputo distribuido para mejorar el rendimiento y poder procesar mayor cantidad de información y de manera más profunda. La tabla 10 muestra el esquema actual de los roles y características de los servidores actuales del proyecto:

Tabla 10. Esquema de roles de los servidores del proyecto

SERVIDOR PRINCIPAL	
Sistema operativo	GNU/Linux
Rol principal	Recepción y análisis del tráfico de red
Tecnologías implementadas	Honeypot, IDS, análisis de flujos
Carga aproximada del servidor	95% Recepción, análisis y procesamiento 5% Reservada para administración
Tipo	Servidor de rack multicore

SERVIDOR DE ALMACENAMIENTO	
Sistema operativo	GNU/Linux
Rol principal	Almacenamiento de información procesada
Tecnologías implementadas	Motor de base de datos, automatización de procesos de manejo de información
Carga aproximada del servidor	50% Procesos de almacenamiento 45% Consultas bajo demanda 5% Reservada para administración
Tipo	Servidor de rack multicore

SERVIDOR DE PUBLICACIÓN	
Sistema operativo	GNU/Linux
Rol principal	Sistema Web de administración y acceso a la información del TSU.
Tecnologías implementadas	Servidor Web y aplicaciones interactivas de visualización de la información
Carga aproximada del servidor	30% Procesos web 70% Disponible
Tipo	Servidor de rack multicore

3.4.4 PROCESAMIENTO DE LA INFORMACIÓN

El procesamiento de la información es una parte fundamental del proyecto. Esto implicó el análisis exhaustivo de procedimientos y algoritmos que mejor se adaptaran a al esquema del mismo.

Los aspectos fundamentales a tomar en cuenta fueron:

- Cantidad de información a analizar:
    - Cantidad aproximada de direcciones IP en el espacio de monitoreo
    - Cálculo aproximado de la cantidad de tráfico de red recibido
- Tecnologías utilizadas para detección:
    - Honeypots: tipos de herramientas y su carga de procesamiento
    - IDS: Cantidad de generación de datos de alertas
    - Flujos: Análisis estadístico y estructurado de tráfico de red
- Estructura de la información almacenada
    - Formato de la información
    - Nivel de detalle de información de incidentes detectados
    - Cantidad de evidencia almacenada
- Tipos de procesamiento
    - Tiempo real
    - Automatización programada

Debido al tamaño de la Darknet, en realidad el principal problema radica en diseñar y adaptar el mejor algoritmo para procesamiento de la información en cuestión de rendimiento y estabilidad de los sistemas. Esto quiere decir que se puede analizar una mayor cantidad de información disminuyendo la profundidad de las técnicas de análisis, sin embargo, en esta fase del proyecto se buscó encontrar un punto medio para poder realizar un análisis útil a la mayor cantidad de información posible. A grandes rasgos, en esta primera versión de la Darknet el sistema de procesamiento se adaptó a un modelo de análisis en tiempo real con procesos independientes, lo cual permitió reducir de manera drástica el tiempo que los equipos tardaban en obtener la información desde que se recibe una conexión hasta que se almacena en la base de datos.

La figura 20 muestra el esquema de procesamiento de la información por bloques principales.

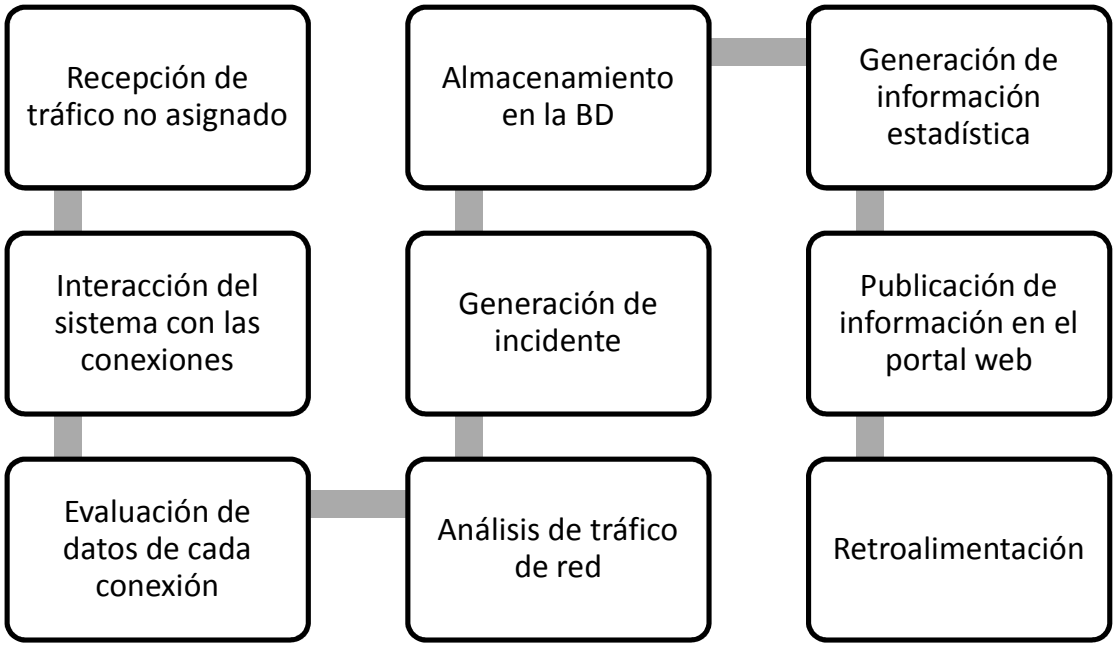

Figura 20. Procesamiento de información de la Darknet

En el siguiente capítulo se detalla este procedimiento abordando características específicas sobre el algoritmo y herramientas utilizadas.

3.4.5 OBTENCIÓN DE RESULTADOS

Para la obtención de resultados se tomó en cuenta que el sistema desarrollado cumpliera con los siguientes objetivos:

- Obtener información detallada de los incidentes generados.
  - Marcas de tiempo, protocolo, origen, destino, tipo de evento, etc.
- Capturar evidencia de tráfico malicioso.
  - Malware, binarios, flujos, etc.
- Comparar el tipo y formato de información obtenida con otros proyectos similares en el mundo.
- Reducir al máximo posible la cantidad de falsos positivos.

La correcta obtención de resultados implica que el telescopio de seguridad proporcione una fuente confiable de información sobre el tráfico malicioso detectado. Su aprovechamiento se dará cuando a partir de la interfaz final de acceso a la información (web) se obtenga de una manera estructurada todas las características antes mencionadas tanto de forma automática (sistema de atención a incidentes) y bajo demanda (consulta de información específica con fines informativos y/o estadísticos).

De esta manera, el diseño supone la capacidad de obtener información estadística y de referencia sobre datos procesados como:

- Ataques detectados
- Direcciones IP fuente de tráfico malicioso
- Tendencias de actividad anómala dentro y fuera de RedUNAM
- Interpretación de tráfico de red malicioso
- Muestras de malware
- Evidencia de tráfico malicioso (escaneos, gusanos, ataques, etc.)

Toda esta información será proporcionada con datos detallados, es decir, se podrá acceder a los eventos relacionados a un incidente proporcionando la información completa de tiempo y conectividad como protocolo, direcciones y puertos origen/destino, evidencia de posible actividad maliciosa e incluso a una muestra del malware relacionado con el evento según el tipo de actividad maliciosa. Para el caso de muestras de malware, el TSU implementará un proceso automatizado para combinarlo con una sandnet[19] (desarrollada en el proyecto UNAM-Malware[20]) y poder analizarlas.

En el quinto capítulo de esta tesis se aborda un análisis de resultados obtenidos en algunas pruebas del sistema en producción.

[19] Mecanismo de análisis automatizado de muestras de malware.
[20] Proyecto perteneciente a la SSI/UNAM-CERT http://www.malware.unam.mx encargado del análisis de malware.

3.4.6 UTILIDAD DE LA INFORMACIÓN

La información obtenida con la Darknet puede ser aprovechada en diferentes áreas:

1) Sistema de atención a incidentes (SAI) en el UNAM-CERT
    - Se obtiene un mayor detalle de información por incidente
    - Se proporciona un complemento a las fuentes de información actuales

2) Referencia en el Telescopio de Seguridad de la UNAM
    - Se le da al TSU características adicionales y le da soporte para hacer una comparativa con los pocos proyectos similares de su tipo.

3) Vinculación con organismos nacionales e internacionales para intercambio de datos sobre tráfico malicioso.
    - Fortalecer la relación con organismos enfocados a la seguridad en cómputo para compartir información, alertar y generar estadísticas.