CAPÍTULO 5

ANÁLISIS DE RESULTADOS

La etapa de pruebas de la Darknet se realizó con aproximadamente el 30% de la capacidad de la misma, esto quiere decir aproximadamente 15,000 direcciones IP.

Las características del motor de detección se fueron implementando y activando paulatinamente, midiendo la carga de procesamiento, estabilidad, tiempos y efectividad de detección. El siguiente esquema muestra las etapas de la fase de prueba:

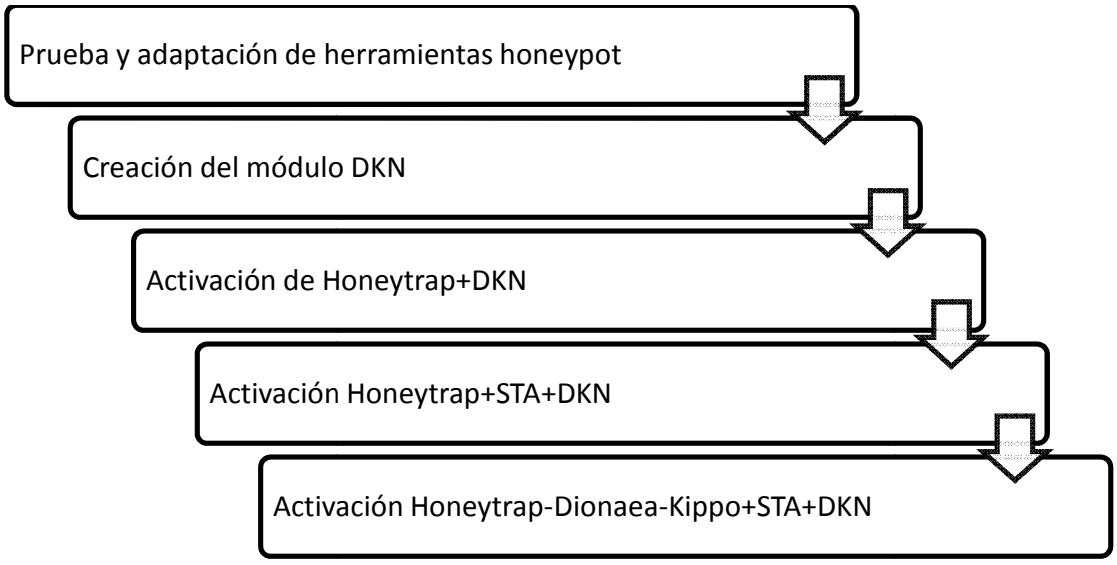


Figura 32. Etapas de la fase de prueba de la Darknet

El análisis de los resultados se basa en la medición de tres aspectos:

- Carga del sistema
- Efectividad de detección y clasificación
- Utilidad de la información

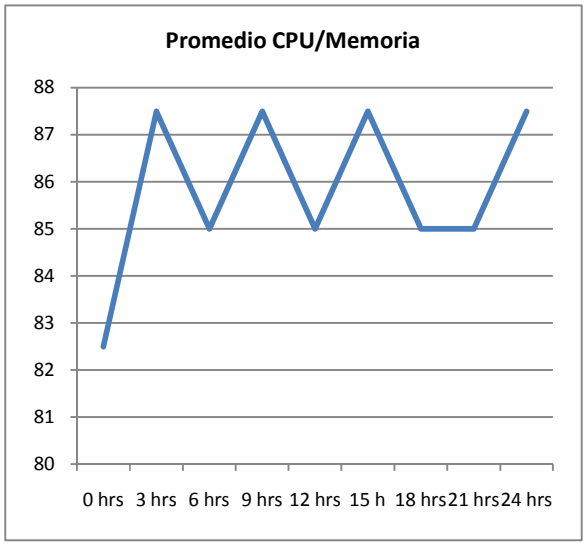
5.1 CARGA DEL SISTEMA

Una vez que se activaron todas las características, y tomando aproximadamente el 30% de las direcciones IP disponibles para la Darknet, el sistema llega a un máximo de 90% de utilización. Este parámetro es calculado a partir del monitoreo de los recursos del equipo: memoria y procesador.

La tabla 12 muestra la carga del sistema en un día promedio:

Tabla 12. Carga del sistema de la Darknet

Tiempo	Memoria	Procesador	Promedio CPU/Mem
0 hrs	75%	90%	82.5
3 hrs	80%	95%	87.5
6 hrs	80%	90%	85
9 hrs	85%	90%	87.5
12 hrs	80%	90%	85
15 h	85%	90%	87.5
18 hrs	85%	85%	85
21 hrs	80%	90%	85
24 hrs	85%	90%	87.5



Es importante reservar una determinada capacidad de carga del sistema debido a que ciertas tareas de administración lo requieren y se debe evitar que el sistema colapse. Esto en realidad es esencial ya que se observó que el sistema dejaba de responder después de estar varias horas activo al superar constantemente el 95% de la carga del sistema. En parte esto se debe a la inestabilidad de las herramientas honeypot en ciertas situaciones de conexiones masivas.

5.2 EFECTIVIDAD DE DETECCIÓN Y CLASIFICACIÓN

La característica del módulo DKN para poder detectar y clasificar eventos según reglas y patrones preestablecidos ha resultado muy efectiva. De millones de conexiones que se tienen diariamente, se logra una clasificación que reduce el número de eventos agrupando, según los criterios, en incidentes.

El saber que un barrido de puertos de 65535 conexiones únicas corresponde a un incidente, o que un equipo realiza conexiones en el puerto 22 en segmentos de red

completos buscando atacar el servicio de SSH, son ejemplos prácticos de la organización que se logra.

Se han hecho distintas mediciones de las cuales se puede extrapolar el potencial completo de la Darknet una vez que se active la detección para todo el espacio de monitoreo posible de aproximadamente entre 45,000 y 50,000 direcciones IP.

A continuación la tabla 13 muestra distintas pruebas evaluando la cantidad de incidentes detectados en un día, y tomando como base la constante de las distintas muestras, se hace una extrapolación del número aproximado con la capacidad completa.

Tabla 13. Estadísticas de detección de incidentes y captura de malware de la Darknet UNAM

Cantidad de direcciones IP activadas	Número aproximado de incidentes detectados	Cantidad aproximada de payloads binarios analizados	Cantidad de muestras únicas de malware capturado
100	2,000	3,000	40
255	4,500	8,000	80
2,550	55,000	80,000	1,100
15,000	320,000	450,000	6,500
30,000	*630,000*	*900,000*	*12,000*
50,000	*1,050,000*	*1,500,000*	*20,000*

Como se puede apreciar, la cantidad de payloads analizados es mayor a la cantidad de malware identificado. Esto se debe a dos razones fundamentales. En primer lugar, la captura de malware la realizan dos herramientas honeypots diferentes. Una de ellas, Dionaea, tiene una capacidad mayor para la captura de malware sin embargo no captura payloads de cualquier conexión por lo que el módulo DKN no los analiza, simplemente registra que la herramienta capturó un posible malware. Mientras tanto, Honeytrap captura todos los payloads de las conexiones, aún cuando no necesariamente se trate de malware y de hecho es mínima la captura de malware con esta herramienta que está más enfocada al análisis del payload de la conexión. La otra

razón se debe a que se trata de muestras únicas, es decir, quizá en algunos incidentes se captura el mismo malware pero solo se registra una vez.

El número de incidentes detectados es el otro factor de medición el cual puede ser un número considerable dependiendo de la capacidad que se active en la Darknet, sin embargo, como cualquier sistema de detección de tráfico malicioso, cierta cantidad de los incidentes representan falsos positivos. Actualmente no está implementado un mecanismo para hacer una evaluación y verificación completa de la cantidad de ellos, no obstante, mediante la definición de más reglas se ayuda a disminuir el número de eventos que correspondan a uno.

5.3 UTILIDAD DE LA INFORMACIÓN

Una vez que la información se tiene almacenada en la base de datos es fácilmente accesible. Ya que el diseño permite obtener un detalle muy preciso de cada incidente, el aprovechamiento que se le da a la misma se ha enfocado principalmente a la atención de incidentes y análisis de nuevas amenazas.

A partir de la implantación de la Darknet, se puede reportar un incidente proporcionando detalles que permitan a los dueños o administradores de los equipos detectados como origen del tráfico, mitigar de una manera más precisa o tener la evidencia suficiente para entender el problema. A pesar de que esto aún no está en producción con el Sistema de Atención a Incidentes del UNAM-CERT, el motor de detección ya almacena en la base de datos los eventos detectados, por lo que la extracción de información es de forma manual mediante consultas de base de datos y visualización de registros.

El otro enfoque de la información obtenida es la parte de investigación, la cual abre muchas expectativas debido al potencial del gran espacio de monitoreo y de ser un entorno académico. Desde su desarrollo se han hecho cambios al motor en cuanto a características y capacidades por lo que cada mejora implica un mejor aprovechamiento del TSU.

En el Anexo F se muestran ejemplos de información almacenada en la base de datos.

5.4 TAREAS PENDIENTES Y MEJORAS POSIBLES

El estado actual de la Darknet cumple con el objetivo fundamental de ser un motor de detección del TSU, sin embargo aún hay tareas por completar y aspectos a mejorar en desarrollos posteriores.

a) Interfaz WEB del TSU

   Para que la información pueda ser aprovechada de manera más sencilla y práctica, la interfaz del TSU es un desarrollo que se encuentra en proceso. El objetivo fundamental es extraer mediante Web toda la información obtenida por la Darknet.

b) Automatización con el SAI

   Se debe terminar la interacción con el Sistema de Atención a Incidentes para que el proceso de aprovechamiento y extracción de información sea de manera automatizada.

c) Integración con la sandnet del Proyecto Malware UNAM

   Se planea desarrollar un módulo que permita la integración de las muestras recopiladas por la Darknet con el laboratorio de análisis de malware perteneciente al UNAM-CERT.

d) Integración con modelos de datos compartidos

   Se planea integral al TSU un módulo para poder compartir la información con organizaciones externas. Algunos ejemplos son los formatos de Shadowserver y algunas herramientas desarrolladas por miembros de The Honeynet Project.

e) Detección de shellcodes

   La detección de shellcodes mediante distintas técnicas es una característica factible de implementar en el módulo DKN. Las mejoras implican cambios en el módulo de análisis de payloads.

f) Integración de más herramientas honeypots