**Implementación de una *Botnet* heterogénea para la ejecución de ataques coordinados**

Oswaldo Andrés Angarita León

Alberto Manuel García Grimaldos

**Software libre**

Juan Sebastián Gómez Rosas

**UNIVERSIDAD PONTIFICIA BOLIVARIANA**

**ESCUELA DE INGENIERÍA  
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

**BUCARAMANGA**

**2018**

**Implementación de una *Botnet* heterogénea para la ejecución de ataques coordinados**

**1. Especificación de la situación problemática**

En el campo de la seguridad informática, pareciera todo ser oscuro y con conocimientos inaccesibles para los menos enterados del tema.

Los interesados en aprender sobre seguridad informática no pueden acceder a toda la información, incluso en ocasiones se deben pagar costosos cursos para acceder a la misma; información que si bien estructurada técnicamente, en ocasiones llega a ser vacía en la práctica.

Además de la falta de libertad en la información, es importante destacar las falencias de seguridad en las infraestructuras nacientes, las cuales se van incorporando cada vez más rápidamente a la red; es importante destacar que estas vulnerabilidades pueden ser explotadas para diversos propósitos, sin embargo, los desarrolladores de estos productos no tienen mano firme para realizar mejoras en la seguridad de estos.

**2. Objetivos**

**2.1. Objetivo General**: Generar un proyecto de software libre para la interconexión de máquinas en una Botnet destinada para realizar ataques del tipo de denegación de servicios.

**2.2. Objetivos Específicos:**

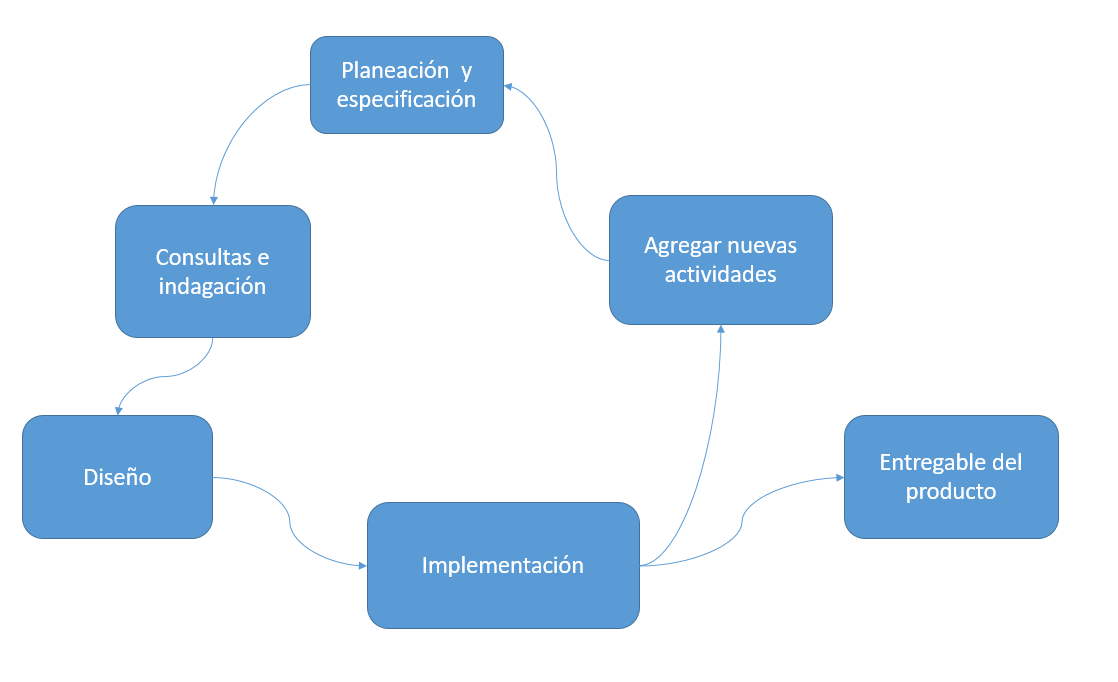
* Determinar las caracteristica de la conexión entre distintas maquinas en una LAN mediante herramientas de software libre previamente diseñadas.
* Desarrollar algoritmos desde el modelo de una Botnet con nodos maestros intercambiables y asignación dinámica de cargas.
* Acoplar las partes lógicas y físicas del proyecto.
* Socializar y liberar los resultados del proyecto.

**3. Justificación**

Se encontró la necesidad de generar información libre y accesible a todo el mundo, sobre las botnet heterogéneas y su aplicación real en un entorno controlado, para así poder complementar el aprendizaje de miles de personas, y poder generar una comunidad de aprendizaje libre y descentralizado.

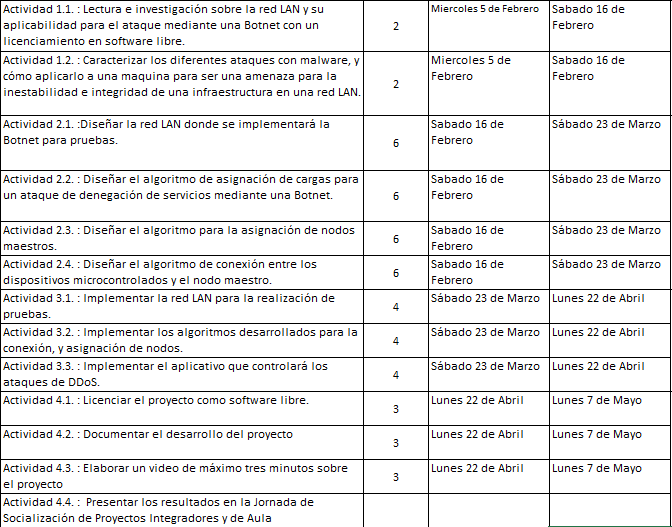
Teniendo en cuenta la creciente vinculación de dispositivos a internet, es importante pensar en que estos deben tener una infraestructura de seguridad fuerte, para poder mejorar estas estructuras de seguridad, hay que pensar como lo haría un atacante, y generar diversas herramientas para poder hacer estudios de posibles brechas de seguridad, esto soportado por las comunidades de software libe, puede hacer que a la larga se generen mejores posibilidades para asegurar diferentes infraestructuras mediante la colaboración de las personas interesadas en este tipo de proyectos.

**4. Actividades a Desarrollar**



**Tomada de [el autor]:** Se inicia con una planeación del proyecto, y se plantea una serie de preguntas del ¿por qué hacerlo? ¿Para qué? ¿En que beneficia? Entre otros. De ahí pasamos a una indagación a fondo sobre el tema y lo comparamos con otros proyectos que puedan llegar a ser similares y hacer comparativos con ellos. Luego se pasa al proceso del diseño del algoritmo y de ahí pasamos a la implementación, hacemos una realimentación y ahí se analiza si es necesario agregar nuevas actividades para complementar el proyecto, sino entregamos el producto.

**5. Cronograma de Actividades**



**6. Referencias**

[1] Gernot Vormayr, Tanja Zseby, and Joachim Fabini. (2017). Botnet Communication Patterns. En linea. Disponible: <https://publik.tuwien.ac.at/files/publik_262720.pdf>

[2] O. Kupreev, J. Strohschneider, and A. Khalimonenko, “Kaspersky DDOS intelligence report for Q3 2016,” Kaspersky lab, Tech. Rep., Oct. 2016. [En linea]. Disponible: https://securelist.com/analysis/quarterly-malware-reports/76464/ kaspersky-ddos-intelligence-report-for-q3-2016/

[3] Daniele Antonioli.(2018,febrero,1).Taking Control: Design and Implementation of Botnets for Cyber-Physical Aacks with CPSBot. En linea. Disponible: https://arxiv.org/pdf/1802.00152.pdf