**UPBotnet: un proyecto de software libre para la implementación de una *Botnet* heterogénea para la ejecución de ataques coordinados con dispositivos de IoT**

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**: Crear un proyecto de software libre para la interconexión de máquinas en una Botnet destinada a realizar ataques de denegación distribuida de servicios (DDOS).

**2.2. Objetivos Específicos:**

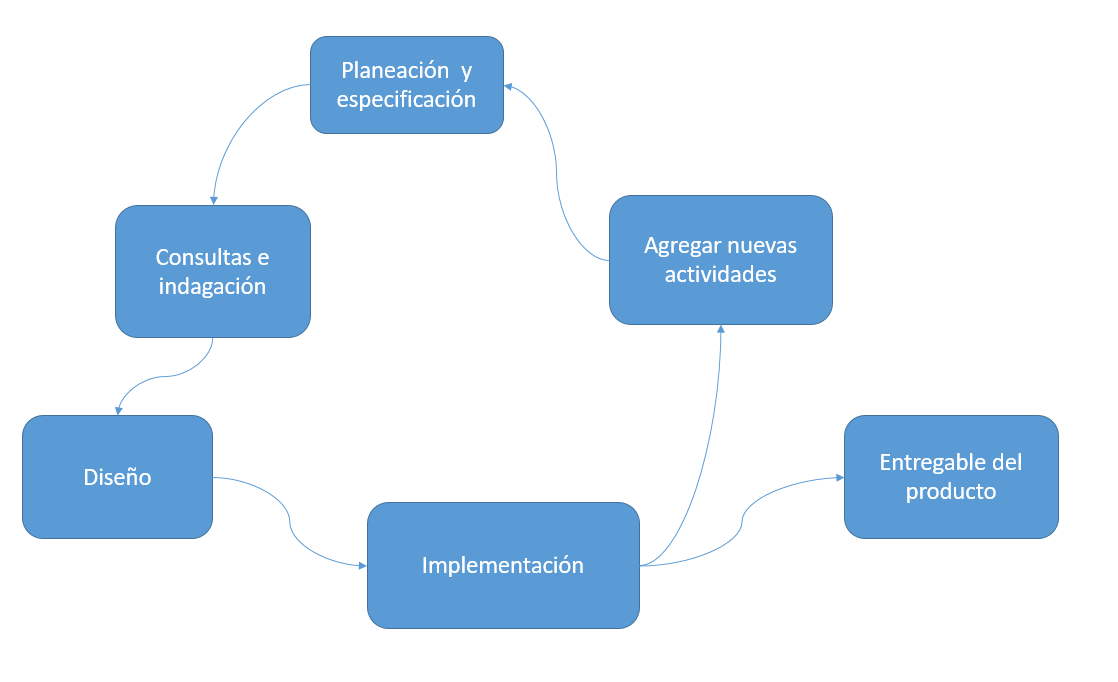
* Determinar las características de la conexión a utilizar entre distintas maquinas en una LAN.
* Diseñar algoritmos que sustenten el modelo de una Botnet con nodos maestros intercambiables y asignación dinámica de cargas.
* Integrar las partes lógicas y físicas del proyecto, aplicando el conjunto de normas de la licencia GNU/GPLv3 de software libre.

**3. Justificación**

Teniendo en cuenta la creciente vinculación de dispositivos a internet, es importante pensar que estos deben ser robustos en cuanto a su infraestructura de seguridad. Para poder mejorarlas, se deben establecer soluciones mediante los análisis de vulnerabilidades, los cuales son precisamente irrupciones en la seguridad del sistema. Esto soportado por las comunidades de software libre, puede hacer que a la larga se generen mejores opciones para asegurar diferentes infraestructuras mediante la colaboración de las personas interesadas en este tipo de proyectos.

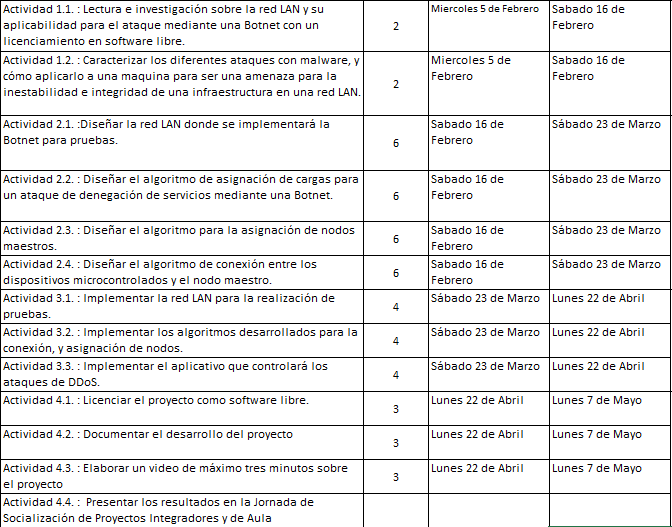
Cada vez se intenta solucionar más la necesidad de generar información libre y accesible a todo el mundo sobre el aseguramiento de brechas de seguridad. Las botnet heterogéneas y su aplicación real en un entorno controlado, pueden servir para concientizar a fabricantes y comunidades de software sobre las vulnerabilidades en dispositivos de IoT (Internet of Things), para así poder generar una comunidad de aprendizaje libre y descentralizado, y hacer de la red un lugar más seguro para navegar.

**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

Antonioli, D. (2018, febrero 1). *arxiv.* Retrieved from https://arxiv.org/pdf/1802.00152.pdf

Bell, L. (2014, marzo 6). *The Inquirer.* Retrieved from https://www.theinquirer.net/inquirer/news/2332589/bitcoin-mining-botnets-and-windows-xp-threats-are-booming-says-dell-sonicwall

Hispasec. (2018, octubre 1). *hispasec*. Retrieved from https://unaaldia.hispasec.com/2018/10/torii-es-la-nueva-botnet-iot-multiplataforma.html

Kupreev, O., Strohschneider, J., & Khalimonenko, A. (2016). *securelist.* Retrieved from https://securelist.com/analysis/quarterly-malware-reports/76464/ kaspersky-ddos-intelligence-report-for-q3-2016/

Osborne, C. (2018, septiembre 28). *zdnet*. Retrieved from https://www.zdnet.com/article/meet-torii-a-new-iot-botnet-far-more-sophisticated-than-mirai/

panda security. (2018, marzo 9). *pandasecurity*. Retrieved from https://www.pandasecurity.com/spain/mediacenter/malware/botnets/

Poor-man. (2016, octubre). *geektopia.* Retrieved from https://www.geektopia.es/es/technology/2016/10/11/noticias/un-hacker-publica-el-codigo-de-un-programa-para-hacer-ataques-ddos.html

Rouse, M. (2014, enero). *techtarget*. Retrieved from internetofthingsagenda: https://internetofthingsagenda.techtarget.com/definition/IoT-botnet-Internet-of-Things-botnet

Torres, J. (2014, octubre). *Hipertextual.* Retrieved , from https://hipertextual.com/archivo/2014/10/internet-cosas/

Vormayr, G., Zseby, T., & and Fabini, J. (2017). *Publikationsdatenbank der TU Wien.* Retrieved from publik.tuwien.ac.at: https://publik.tuwien.ac.at/files/publik\_262720.pdf