Encuentro Internacional de Educación en Ingeniería ACOFI
LA FORMACIÓN DE INGENIEROS: UN COMPROMISO PARA EL DESARROLLO Y LA SOSTENIBILIDAD
15 al 18 DE SEPTIEMBRE 2020
www.acofi.edu.co/eiei2020

METODOLOGÍA PARA LA EVALUACIÓN DE SISTEMAS INFORMÁTICOS UTILIZANDO TÉCNICAS DE ETHICAL HACKING EN PLATAFORMAS DE HARDWARE Y SOFTWARE LIBRE

Escalante Dustin, Pérez Darling, Vega Germán, Salcedo Dixon, Mardini Johan, Esmeral Ernesto

Universidad de la Costa
Barranquilla, Colombia

Resumen

Actualmente el acceso a Internet se ha convertido en un factor indispensable para el desarrollo de la humanidad. En consecuencia, organizaciones y personas acceden a diferentes servicios vía Internet, desde cualquier lugar y dispositivo. Adicionalmente, la tecnología inalámbrica (WiFi) se ha convertido en la más utilizada en los servicios de telecomunicaciones, por todas las ventajas que ofrece; respecto a movilidad, accesibilidad y disponibilidad constante a los usuarios. Sin embargo, hay varios riesgos informáticos asociados a las conexiones inalámbricas; y uno de los riesgos más importantes se origina por el desconocimiento de los niveles de seguridad en las redes inalámbricas donde se conectan ocasionalmente los usuarios; convirtiéndolos en vulnerables a atacantes que se aprovechan de la tecnología para acceder sin autorización a sus dispositivos, y modificar parámetros de configuración, robar contraseñas, información privada, entre otras acciones maliciosas. Por lo tanto, este trabajo presenta una metodología de pentesting para realizar pruebas de vulnerabilidad de dispositivos y sistemas informáticos utilizando técnicas de Ethical hacking. Esta metodología se implementó usando la herramienta llamada Metasploit Framework, que funciona sobre plataforma de hardware (Raspberry Pi) y software libre (Kali-Linux). Las pruebas ejecutadas en escenarios reales permitieron comprobar que se pueden desarrollar e implementar sistemas robustos utilizando plataformas de hardware y software abierto de bajo costo; que pueden ser utilizados en entornos productivos para evaluar la vulnerabilidad en aspectos de seguridad en dispositivos móviles y sistemas informáticos.

Palabras clave: ethical hacking; seguridad de redes; ingeniería social; software y hardware abierto

Abstract

Nowadays access to the Internet has become an indispensable factor for the development of humanity. Consequently, organizations and people access different services via the Internet, from any place and device. Additionally, wireless technology (WiFi) has become the most widely used in telecommunications services, for all the advantages it offers, regarding mobility, accessibility, and constant availability to users. However, there are several computer risks associated with wireless connections, and one of the most important risks originates from ignorance of the security levels in wireless networks where users occasionally connect, making them vulnerable to attackers who take advantage of technology to access their devices without authorization, and modify configuration parameters, steal passwords, private information, among other malicious actions. Therefore, this work presents a pen-testing methodology to perform vulnerability tests of devices and computer systems using Ethical hacking techniques. This methodology was implemented using the tool called Metasploit Framework, which works on a hardware platform (Raspberry Pi) and free software (Kali-Linux). The tests carried out in real scenarios allowed verifying that robust systems can be developed and implemented using low-cost hardware and open software platforms; It is can be used in production environments to assess vulnerability in security aspects of mobile devices and computer systems.

Keywords*: ethical hacking; network security; social engineering; open software and hardware*

1. Introducción

En la actualidad el uso de tecnologías de comunicación en los hogares, se han convertido en factores indispensables en el desarrollo de las actividades diarias. En Colombia, personas entre los 5 y más años usaron Internet desde cualquier lugar y desde cualquier dispositivo en el año 2018, (DANE, 2019).

Lo anterior, representa una gran ventaja a nivel de conectividad. Pero, más allá de los puntos a favor, hay una sociedad hiper-convergente que omite muchas veces los riesgos informáticos asociados al uso de estos dispositivos. Una de las principales desventajas que supone su uso, es la cantidad de conexiones inalámbricas (Wifi, Bluetooth, NFC, entre otras) que permite utilizar y, que en muchas ocasiones el usuario no conoce realmente el riesgo su uso de manera cotidiana. Uno de los grandes inconvenientes de las redes inalámbricas es la seguridad, como señala (Goujon, A. 2016), "al prescindir de un cable para acceder a la red, se convierte en una tecnología atractiva para los atacantes, quienes pueden utilizar el ancho de banda, modificar parámetros de configuración, robar contraseñas y credenciales, entre otras acciones maliciosas"; que se utiliza permanentemente, representando un riesgo inminente a toda la información almacenada en estos. Cuando iniciaron los ataques informáticos a ordenadores eran lo suficientemente dóciles, como para no afectar más allá del rendimiento del equipo infectado o saturar la bandeja de entrada de un correo electrónico. Si bien, en sus inicios eran muy inofensivos, virus como "STONED" infectaba el motor de arranque */.mbr* que contaba el número de reinicios desde que el equipo había sido infectado, y mostraba la frase "*your computer is now stoned*". Los famosos gusanos en la gran mayoría de ocasiones únicamente ralentizaban los procesos ejecutados en el equipo (González et

al. 2015). Existían otros de tipo "bromista" que se encargaban de molestar el trabajo realizado por el usuario, lo que conllevaba a reiniciar el equipo para solucionar el problema.

Sin embargo, tiempo después los cibercriminales vieron una manera fácil de lucrarse económicamente con actos que iban en contra de los usuarios de todos los equipos conectados a Internet. En consecuencia, aparecieron los primeros y verdaderos virus informáticos que eliminaban información sin propósito alguno. Luego, llegaron aquellos que dañaban físicamente los equipos sin posibilidad de recuperarlo. Finalmente, el malware evoluciono hasta el punto de solicitar dinero por la información que tienes en tu ordenador con tal de no eliminarla y perderla posiblemente para siempre (González et al. 2015).

Por otra parte, con la gran variedad de dispositivos que hoy hacen uso de Internet, son muchos los factores de riesgos a los que se enfrenta la sociedad, solo con un clic del usuario sobre un hipervínculo infectado con código malicioso, o que instale una aplicación que contenga un backdoor; y el atacante podrá obtener el acceso parcial o total a funciones del dispositivo de manera remota, e incluso sin dejar rastro.

Adicionalmente, las personas son inconscientes de los peligros de usar un dispositivo tecnológico sin las medidas de protección básicas, como un antivirus; incluso una simple actualización de cualquier aplicación puede darle acceso a un atacante sin que el usuario tenga conocimiento. Este trabajo de investigación tiene como foco central de acción, implementar pruebas de seguridad informática y Ethical hacking, sobre un sistema embebido. Para lograr lo anterior, se eligió la distribución Linux Kali Linux - 2019.1; debido a que contiene una arquitectura estable para ser implementada sobre la arquitectura Raspberry Pi 3 que fue seleccionada por sus prestaciones y comparativa calidad / precio. Se pretende demostrar que, de manera económica y sencilla, puede efectuarse un ataque informático que afecte en gran proporción al usuario.

Así mismo, como objetivo adicional se busca generar en las personas a tomar consciencia sobre los peligros relacionados con el uso de dispositivos que se conectan a Internet. En consecuencia, se seleccionó un vector de ataque convencional, que, por medio de diferentes scripts disponibles en Internet y técnicas de ingeniería social, logrará que un usuario ejecute de manera voluntaria un software malicioso en su ordenador, que otorgue control total a un cibercriminal.

Finalmente, utilizando el framework de *Metasploit*, se demuestra cómo es posible acceder a las funciones del ordenador infectado; así mismo, cómo manipular todo el contenido que se tiene almacenado. Por último, aplicando técnicas antiforense se proporcionará una visión de un entorno real, donde las pruebas de una intrusión quedan anuladas por el mismo atacante.

2. Trabajos Relacionados

Cuando se habla de la aplicación del Ethical hacking y pentesting, se puede encontrar en la literatura documentos donde se instruye e implementan a través de diversas herramientas tales como: Metasploit Framework, y Kali Linux. Así mismo, como complemento a las herramientas mencionadas anteriormente, trabajos recientes presentan la Raspberry Pi 3, como plataforma para

realizar implementaciones de seguridad informática. Por ejemplo: Yevdokymenko en (Yevdokymenko et al. 2017) describe el proceso de la penetración remota haciendo uso de las herramientas mencionadas (Metasploit, Rapsberry Pi, Kali Linux), partiendo de los principios del Ethical Hacking y proporcionando una ampliación teórica de los métodos, como también, las ventajas y desventaja; sin embargo, es completamente teórico y abarca el tema de forma general. En (Westerlund, O., and Asif, R. 2019) Westerlund muestra los fallos de seguridad que se encuentran en los dispositivos IoT, tales como los drones que hacen uso de la red inalámbrica Wi-Fi, explotando sus vulnerabilidades para acceder a los datos recolectados por el drone en tiempo real; siendo este trabajo relacionado con el trabajo presentado. Por el contrario, la implementación presentada en este artículo es completamente distinta; debido a que se aplican las etapas del ethical hacking e ingeniería social, explotando las vulnerabilidades del ordenador atacado, para luego obtener el control total de la ventana de comandos, cámara y modificación de archivos.

3. Metodología

Para la evaluación de lo planteado en las secciones anteriores. Inicialmente, se debe aclarar que la metodología se basa en las fases conocidas para aplicar pruebas de Ethical hacking sobre cualquier sistema informático. Por lo tanto, durante cada fase se visualizan las aplicaciones sobre el sistema embebido, y la técnica de ingeniería social que se utiliza para lograr que la víctima instale voluntariamente en su teléfono móvil la aplicación infectada con un payload malicioso.
En la primera etapa, se da un reconocimiento donde se analizan los posibles objetivos a nivel de hardware y software; debido a que, para la ejecución del código malicioso, es necesario conocer la arquitectura sobre la cual se ejecutará el payload, con el objetivo de minimizar los posibles fallos de compatibilidad que puedan afectar el ataque, ver Fig. 1.

Luego, al decidir que el ataque se realizará sobre un dispositivo con sistema operativo Windows 10; se destaca que actualmente Windows cuenta con Windows Defender, que hace parte de su plataforma de protección; y que en su última actualización añadió una función que evita que un malware pueda manipular ajustes del antivirus. Sin embargo, es posible utilizar técnicas de ofuscación de código que evadan los controles mencionados.

A continuación, se definen las herramientas que se utilizan para la creación del payload; de este tipo de herramientas se destaca una disponible en la distribución Kali Linux; que es llamada Metasploit Framework, diseñada para realizar pruebas de Pentesting, que permite agilizar los procesos de infección sobre diferentes plataformas. Adicionalmente, se utilizó un módulo dentro de Metasploit conocido como Msfvenom, que permite la creación de archivos *.exe* con la incrustación de código malicioso de manera automática; lo que permite agilizar el proceso de infección.

Posterior a la creación del payload malicioso, Metasploit permite iniciar la consola, que permite al atacante manejar todas las opciones disponibles del ordenador que ha sido infectado. Así, desde este entorno obtener control total del dispositivo, sin generar alertas visuales para el usuario.

El siguiente proceso, es definir mediante la ingeniería social, de qué forma se lograría que la víctima descargara el archivo *.exe*. Para esto, se ocultó el payload en una imagen con *ToyCon*,

que es enviada a través de un correo electrónico: Por lo tanto, una vez descargada la imagen que oculta el payload, el lado atacante estará listo Metasploit en su modo escucha esperando sobre el puerto y dirección IP seleccionada, y recibir la información del dispositivo, ver Fig. 2.

Por último, para verificar que el ataque ha sido exitoso, se efectúan técnicas anti forenses que permiten eliminar cualquier rastro de código malicioso en el ordenador. Además, mediante los módulos de Metasploit se accede a funciones que violan la privacidad del usuario, como cámara, micrófono, control de la ventana de comandos; que permite realizar cambios en archivos, entre otras opciones disponibles desde la consola.

Finalmente, de esta forma se logra demostrar la facilidad de realizar este tipo de ataques utilizando técnicas de ingeniería social combinadas con herramientas libres de Ethical hacking; donde todo el proceso se logra siguiendo el ciclo del Ethical hacking, soportado en manuales disponibles en Internet; logrando demostrar, que este tipo de ataques hoy en día son más fáciles de ejecutar, permitiendo a los cibercriminales lucrarse de diferentes formas con la privacidad y la b seguridad del usuario.

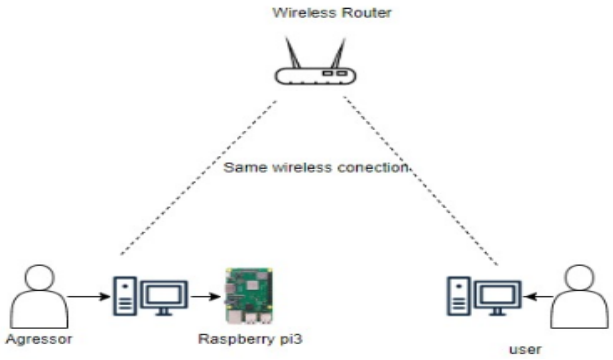

Fig. 1. Topología de ataque

4. Implementación y Evaluación

Para la evaluación e implementación, se utilizaron diferentes sistemas de hardware y software, que son analizados a continuación (ver Fig. 2):

a. Raspberry Pi 3: Este hardware clasifica dentro de los sistemas embebidos y es seleccionado por sus prestaciones que van acorde a las requeridas por la distribución de seguridad informática Kali Linux (Richardson, M., and Wallace, S. 2012).
b. Modem Inalámbrico: Con este dispositivo físico se buscó simular una red doméstica a la cual nos conectamos diariamente para navegar en Internet.
c. Smartphone: se utilizó un teléfono celular que busca hacer el papel de víctima durante el transcurso del ataque.
d. Ordenador portátil: Este dispositivo simulo ser otra víctima teniendo en cuenta el entorno real de red diseñado.

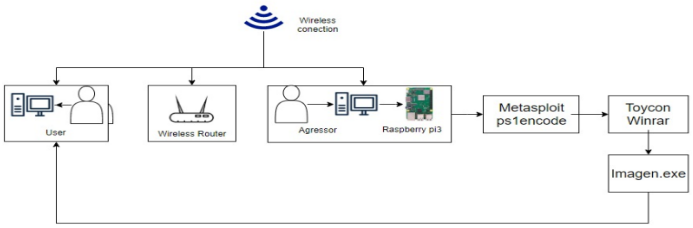

Fig. 2. Raspberry Pi que ejecuta ataques

5. Resultados

Luego de ejecutar las pruebas bajo los entornos seleccionados se obtuvieron los siguientes resultados.

En la Fig. 3, muestra que en el primer paso se realizó la creación del payload, que sirve como medio de acceso a la ordenadora; este paso hace utilizando un Script automático con nombre ***Zirikatu*** el cual sirve como puente entre Metasploit Framework.

.

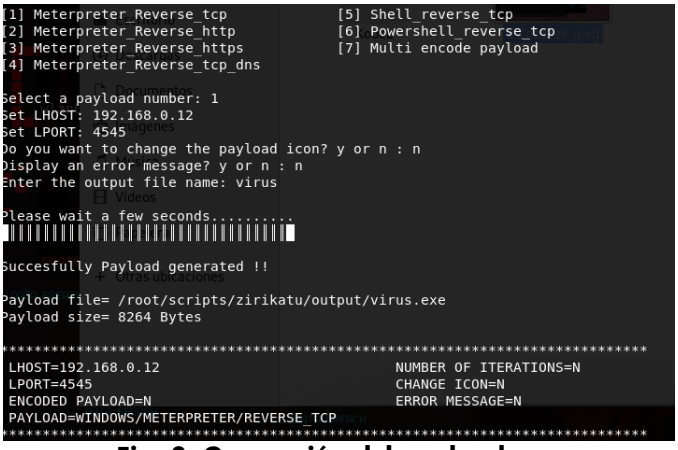

Fig. 3. Generación del payload.

Luego de generar el Payload, el framework de Metasploit se pone en modo escucha para permitir conexión con cualquier equipo o dispositivo que abra el archivo que contiene la Shellcode, ver Fig. 4.

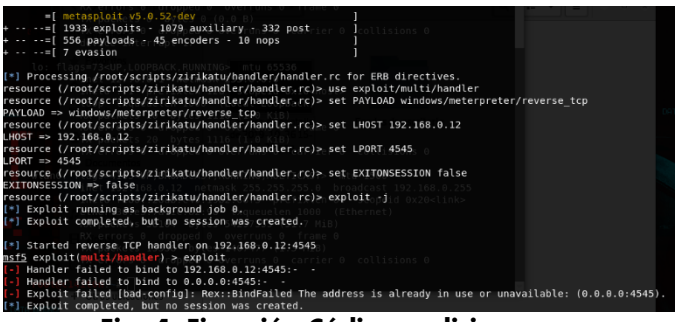

Fig. 4. Ejecución Código malicioso.

Por otro lado, una vez se ejecuta el código malicioso en el dispositivo de la víctima, se crea una sesión en *meterpreter* para que el atacante pueda interactuar con la máquina o dispositivo de la víctima, ver Fig. 5.

Fig. 5. Visualización de sesiones activas en la consola.

Así mismo, se puede ver en la Fig. 6; que se verifica en la consola de Metasploit, si existen sesiones activas para posteriormente ingresar activando la consola de meterpreter; y así, conseguir interactuar directamente con la maquina infectada mediante línea de comandos.

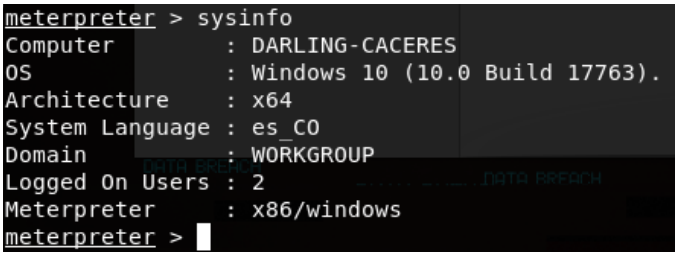

Fig. 6. Ejecución comando Sysinfo en el Meterpreter.

Luego, con el comando **Sysinfo** se logra ver la información de la máquina infectada, así como la arquitectura correspondiente, sistema operativo, dominio y nombre de usuario de la máquina.

Fig. 7. Ejecución del comando mouse en consola.

Así mismo, al ejecutar el comando **help**, se obtiene una salida con todas las opciones disponibles para trabajar con Meterpreter. Por ejemplo, una de estas opciones en el comando **mouse** el cual permite manipular el puntero en el sistema víctima, y así, manipular el portapapeles de la maquina infectada, ver en las Fig. 7 y 8.

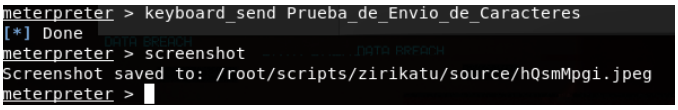

Fig. 8. Ejecución del comando Keyboard_send.

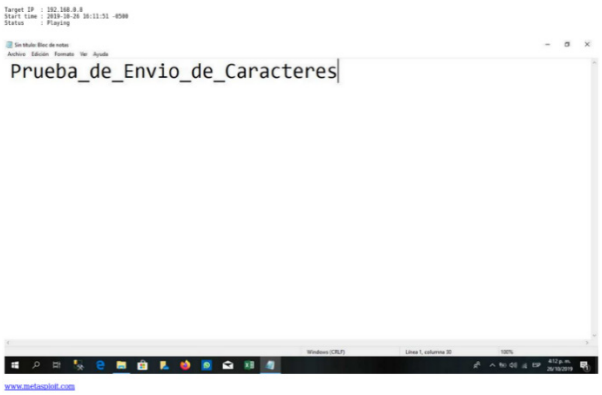

Fig. 9. Visualización del envió de pulsaciones a través del comando keyboard.

Por otro lado, con el comando **keyboard_send** se permite el envío de pulsaciones desde la maquina atacante, en la ilustración anterior vemos un claro ejemplo en la Fig. 9.

Fig. 10. Ejecución del comando Shell en la consola.

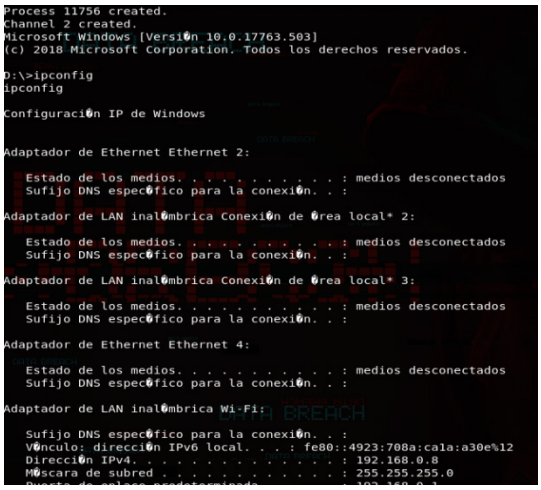

Fig. 11. Visualización permisos de usuaria a los que se obtuvo acceso.

Por último, se obtiene una *Shell* en el sistema victima para interactuar con el equipo con permisos del usuario al que hemos tenido acceso, ver Fig. 10 y 11.

6. Conclusiones

El diseño e implementación de la metodología de pentesting, permitió determinar los siguientes aspectos. Primero, que combinando técnicas de ingeniería social y de ethical hacking, se puede acceder de manera fácil a funciones de dispositivos o máquinas inalámbricas; logrando ejecutar funciones que violan la privacidad del usuario, como cámara, micrófono, control de la ventana de

comandos, realizar cambios en archivos; entre otras opciones disponibles desde la consola. Segundo, evidenció lo expuesto que están los datos cuando se accede a redes inalámbricas desconocidas que solicitan un inicio de sesión para acceder al Internet, lo que puede traer como consecuencia la llegada constante de e-mails, con malware oculto; que pueden dañar, robar, o manipular la información que se almacena en dispositivos.

Adicionalmente, las pruebas ejecutadas en escenarios reales permitieron comprobar que se pueden desarrollar e implementar sistemas robustos utilizando plataformas de hardware y software abierto de bajo costo; que pueden ser utilizados en entornos productivos para evaluar la vulnerabilidad en aspectos de seguridad en dispositivos móviles y sistemas informáticos.

Por último, es importante destacar la facilidad con la que se puede vulnerar tanto la privacidad, como la seguridad de la información a través de las nuevas tecnologías. Por lo tanto, los usuarios deben recordar y estar alertas, porque con un simple clic en el lugar equivocado, la descarga de una inofensiva imagen, o la instalación de un software con un backdoor; puede desencadenar un ataque para un usuario.

7. Referencias

- Departamento Administrativo Nacional de Estadística (DANE). (2019. Agosto). Boletín Técnico Indicadores básicos de tenencia y uso de Tecnologías. Consultado el 20 de octubre de 2019 en https://www.dane.gov.co/files/investigaciones/boletines/tic/bol_tic_hogares_departamental_2018.pdf
- González. A., Pérez, H., and Guevara, P. Gusanos informáticos. (2015, julio). Consultado el 20 de diciembre de 2020 en https://www.amc.edu.mx/revistaciencia/images/revista/66_3/PDF/Gusanos.pdf.
- Goujon, A. (2016, junio). ¿Cómo utilizan los usuarios las redes Wi-Fi?. Consultado el 20 de enero de 2020 en https://www.welivesecurity.com/la-es/2012/08/06/como-utilizan-usuarios-redes-wifi/
- Richardson, M., & Wallace, S. (2012). Getting started with raspberry PI. " O'Reilly Media, Inc."
- Westerlund, O., & Asif, R. (2019, febrero). Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things. In 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS) (pp. 1-10). IEEE.
- Yevdokymenko, M., Mohamed, E., and Onwuakpa, P. (2017, octubre). Ethical hacking and penetration testing using raspberry PI. In 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) (pp. 179-181). IEEE.

Sobre los autores

- **Escalante Dustin**: Estudiante de Ingeniero Sistemas, de la Universidad de la Costa. descalan7@cuc.edu.co.
- **Pérez Darling**: Estudiante de Ingeniero Sistemas, de la Universidad de la Costa. dperez38@cuc.edu.co.
- **Vega German**: Estudiante de Ingeniero Sistemas, de la Universidad de la Costa. gvega2@cuc.edu.co.
- **Salcedo Dixon**: Dr. en Ingeniería de Universidad Pontificia Bolivariana. Profesor titular de la Universidad de la Costa, dsalcedo2@cuc.edu.co.
- **Mardini Johan**: Master en Ingeniería de Sistemas de la Universidad Simón Bolívar. Profesor medio tiempo de la Universidad de la Costa, jmardini@acofi.edu.co.
- **Esmeral Ernesto**: Master en Gestión de las TICs de la Universidad Simón Bolívar. Profesor asistente de la Universidad de la Costa. eesmeral2@cuc.edu.co.
