Apelidos, nome /Apellidos, nombre: Botana de Castro, Elena			
Título: Sistema de prevención de intrusiones en redes Wireless basadas en tecnología Wi-Fi			**Mención cursada:** Tecnoloxías da Información

Resumo / Resumen:
En la actualidad, la seguridad se ha convertido en uno de los campos de mayor preocupación tanto en las grandes empresas como en las PYMES e incluso entre particulares. Se están creando nuevas unidades a nivel estatal en ciberseguridad con miembros de los diferentes cuerpos de seguridad del estado y el número de empresas privadas que están incorporando a personal formado para crear nuevas unidades específicas en seguridad es cada vez mayor. Los sistemas estándares de gestión WiFi (routers) únicamente se encargan de proporcionar conectividad, pero por lo general dejan de lado la seguridad. Por otro lado, los Sistemas de Detección de Intrusiones Inalámbricos (WIDS) únicamente se encargan de detectar las amenazas constantes a las que están expuestas pero este tipo de redes no ofrecen ningún tipo de solución a dichos ataques en calidad de bloqueo o respuesta.

El sistema desarrollado para este trabajo de fin de grado es capaz de proveer un Sistema de Prevención de Intrusiones en redes WiFi basado en software y hardware libre capaz de detectar y reaccionar a los ataques más comunes sobre este tipo de redes, incluso algunos de estos ataques no son detectados o mitigados por los sistemas de prevención de intrusiones comerciales disponibles en el mercado. Además, tiene la capacidad de ampliar sus funcionalidades y módulos con facilidad gracias a la independencia de los mismos. Es capaz de notificar mediante el uso de un bot de Telegram y, de manera redundante en caso de que se produzca algún tipo de error en la transmisión de la primera notificación, envía una segunda notificación del ataque mediante un SMS. De cualquier forma, estas notificaciones solamente advierten al usuario de que su red está siendo víctima de un ataque, la respuesta a estas amenazas es automática.

Como dato reseñable, este proyecto ha entrado a formar parte de un programa lanzadera de la OTRI de la UDC, habiendo sido elegido entre los 5 trabajos que van a representar a la Universidad.

Además, debido a los resultados tan positivos observados tras la finalización del proyecto, se ha llevado a cabo el registro de propiedad intelectual del proyecto:
Autores: Elena Botana de Castro, Adrián Carballal Mato, Carlos Fernández Lozano, Antonino Santos del Riego.
Título: Sistema de prevención de intrusiones en redes wireless basadas en tecnología Wi-Fi.
Número: C-286-2018
Número de asiento registral: 03/2018/1399

Posibles aplicacións / Posibles aplicaciones:
Con la entrada en vigor del Reglamento General de Protección de Datos (RGPD), la seguridad informática cobra cada vez mayor importancia principalmente en las empresas. Aunque también cabe destacar que, a nivel usuario, también está cobrando mayor relevancia debido a robos de datos o accesos no autorizados. En este contexto se encuadran los sistemas de prevención de intrusiones, pero tanto por su precio como por su difícil configuración resulta difícil que PYMES e incluso de forma particular se pueda tener acceso a uno de estos sistemas.

En este proyecto se ha tenido todo esto en cuenta, de forma que se ha desarrollado un sistema de prevención de intrusiones basado en software y hardware libre, de fácil configuración que proporciona tanto a empresas como a los ciudadanos una alternativa para protegerse de los principales ataques sobre redes WiFi. De esta forma, las principales aplicaciones de este trabajo son las siguientes:

- Detección y mitigación de ataques de **denegación de servicio.**
- Detección y mitigación de ataques **Evil Twin basados en RSSI**.
- Detección y mitigación de ataques **ARP Cache Poisoning**.

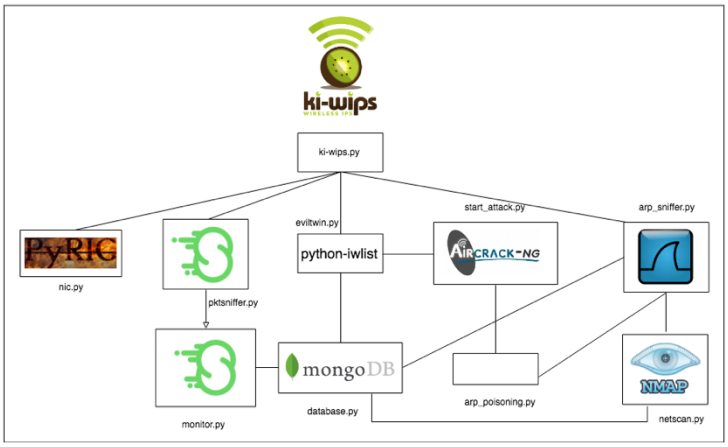
Tanto la detección y mitigación de ataques **Evil Twin basados en RSSI** y ataques **ARP Cache Poisoning**, se trata de unas funcionalidades que no son proporcionadas por los sistemas de prevención de intrusiones comerciales disponibles en el mercado.

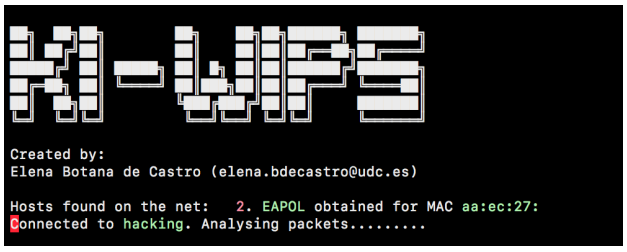
Etapas para o seu desenvolvemento futuro / Etapas para su desarrollo futuro:
El sistema ha sido desarrollado de manera modular, de forma que cualquier persona con un mínimo de conocimientos puede extender el sistema mediante la creación de módulos independientes de manera sencilla. De esta forma, además de hacer uso de software libre para su desarrollo, se favorece enormemente la extensibilidad del sistema.

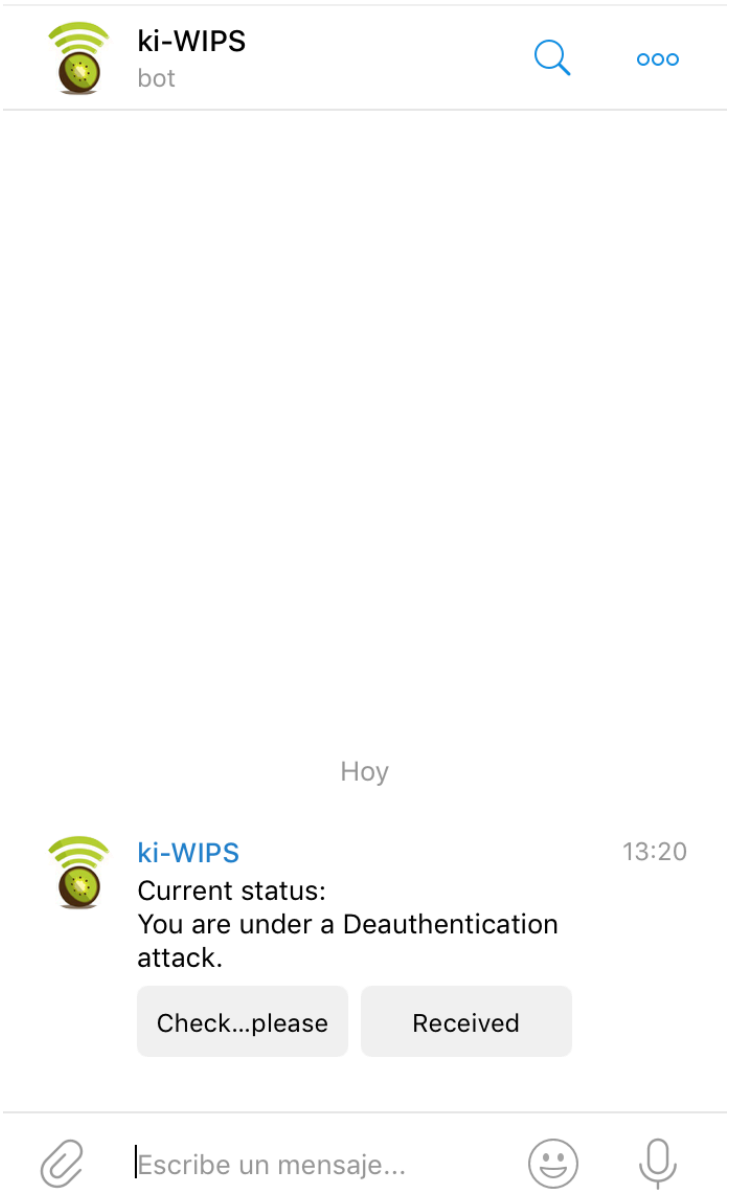
En lo referente al desarrollo futuro del sistema, cabe destacar los siguientes puntos:

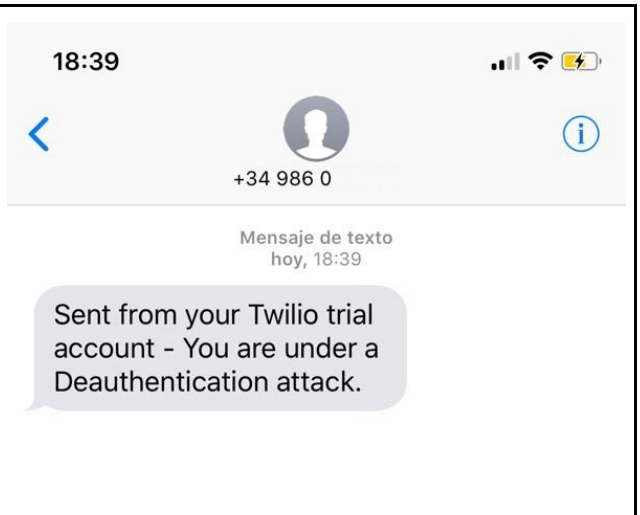
- *Machine learning* para detección de ataques.
- Ampliación de la cantidad de módulos del sistema.
- Diseño de un hardware específico para el sistema.

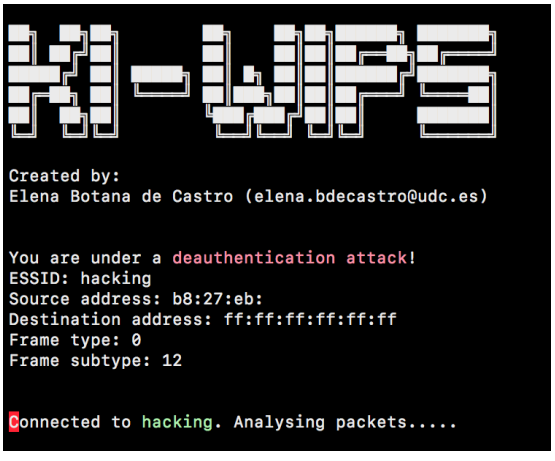
Imaxes representativas / Imágenes representativas:

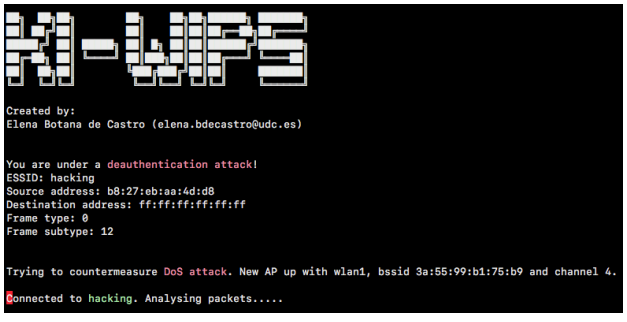


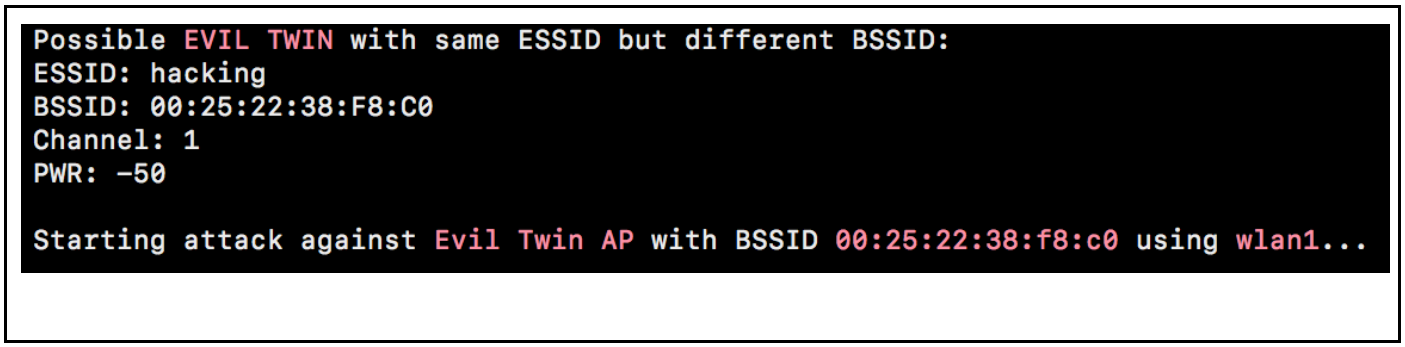



ki-WIPS
bot
Hoy
ki-WIPS
13:20
Current status:
You are under a Deauthentication attack.
Check...please
Received
Escribe un mensaje...


18:39
+34 986 0
Mensaje de texto
hoy, 18:39
Sent from your Twilio trial account - You are under a Deauthentication attack.


Created by:
Elena Botana de Castro (elena.bdecastro@udc.es)
You are under a deauthentication attack!
ESSID: hacking
Source address: b8:27:eb:
Destination address: ff:ff:ff:ff:ff:ff
Frame type: 0
Frame subtype: 12
Connected to hacking. Analysing packets.....


Created by:
Elena Botana de Castro (elena.bdecastro@udc.es)
You are under a deauthentication attack!
ESSID: hacking
Source address: b8:27:eb:aa:4d:d8
Destination address: ff:ff:ff:ff:ff:ff
Frame type: 0
Frame subtype: 12
Trying to countermeasure DoS attack. New AP up with wlan1, bssid 3a:55:99:b1:75:b9 and channel 4.
Connected to hacking. Analysing packets.....


Possible EVIL TWIN with same ESSID but different BSSID:
ESSID: hacking
BSSID: 00:25:22:38:F8:C0
Channel: 1
PWR: -50
Starting attack against Evil Twin AP with BSSID 00:25:22:38:f8:c0 using wlan1...

X