

PPDRON 2016 - Noviembre.

Informe de desarrollo del Software

Versión 1.0

PPDRON 2016 - Noviembre.

Historial de Revisiones.

Fecha	Versión	Descripción	Autor
17 - Noviembre - 2016	1.0		Diego Sierra Larry Portocarrero Andrea Velandia

PPDRON 2016 - Noviembre.

Tabla de Contenido

1. Introducción

1.1 Propósito

1.2 Alcance

1.3 Resumen

2. Marco Empresarial

3. Formulación y Planeación del Proyecto

3.1 Formulación del proyecto

3.2 Planeación del proyecto

3.2.1 Plan de trabajo

3.2.2 Estimaciones

3.2.3 Programas y mecanismos de control, administración y seguimiento del proyecto

4. Metodología

5. Desarrollo del proyecto

5.1 Características, atributos de calidad del sistema y modelos de análisis

5.2 Diseño y arquitectura del sistema

5.3 Implementación

5.4 Pruebas del sistema

5.5 Aseguramiento de calidad

6. Resultados

7. Conclusiones y recomendaciones

8. Referencias

9. Anexos

PPDRON 2016 - Noviembre.

Documento de proceso de Desarrollo de Software.

1. Introducción.

Este documento describe el Desarrollo del Software PPDRON, como respuesta al proyecto de aula de la asignatura Trabajo de Campo de la Universidad Pedagógica y Tecnológica de Colombia. El proyecto está basado en la metodología de desarrollo SCRUM, en la que a través del cumplimiento de las fases de desarrollo e implementación de software se obtiene un sistema orientado a auditoria de redes en el grupo de investigación TELEMATICS

1.1 Propósito.

El propósito de este documento es proporcionar la información necesaria para controlar y hacer seguimiento al proyecto dirigido al ingeniero Alejandro Mora, del grupo TELEMATICS, para diagnosticar el nivel de seguridad de redes inalámbricas, a través de la identificación de vulnerabilidades y posibles ataques en un futuro.

1.2 Alcance.

El documento de proceso de Desarrollo del Software describe de manera general, el plan usado para el desarrollo del sistema "PPDRON". El detalle de las iteraciones individuales se describe en los documentos anexos. En este se definen las características del producto a desarrollar, lo cual constituye la base para la planificación del proyecto. Para el desarrollo del proyecto, se tiene como base la comunicación en la captura de requisitos por medio del cliente para hacer una estimación aproximada, y posteriormente, el avance del proyecto y el seguimiento permite definir y ajustar los artefactos de cada una de las iteraciones y entregables del proyecto.

1.3 Resumen.

El documento está organizado en las siguientes secciones: el marco empresarial que describe la organización de nuestro cliente, la formulación y planeación del proyecto que detalla la oportunidad presentada y como se abordó en el transcurso del proceso de desarrollo, la metodología usada para ejecutar cada una de las fases de desarrollo, el desarrollo del proyecto.

PPDRON 2016 - Noviembre.

2. Marco Empresarial.

El sector al que llevaremos el producto es el sector privado, el conjunto de la actividad económica que no está controlada por el estado, el sector estará delimitado por las empresas dedicadas a la seguridad informática. El cliente del proyecto, el ingeniero Alejandro Mora, tiene conocimientos avanzados de seguridad informática y hace parte de un grupo de investigación especializado en redes de computadores, utilizara el software dentro de una placa para mejorar el nivel de seguridad de las redes que tiene a cargo, además adaptará el sistema a cualquier dron que tenga.

3. Formulación y Planeación del Proyecto.

3.1 Formulación del proyecto.

Desde 1999, Nokia y Symbol Technologies crearon la asociación Wireless Ethernet Compatibility Alliance (WECA) y que en 2003 fue renombrada a WI-FI Alliance (Wireless Fidelity), las comunicaciones inalámbricas pasaron a ser parte de la vida cotidiana, hasta el punto de que en la actualidad estamos completamente conectados, ya sea con nuestro móvil o cualquier otro dispositivo inalámbrico con el cual estamos en constante envío o recepción de información.

De este modo, con el avance continuo de estas tecnologías, las posibilidades de dotar la industria y empresas de mejores servicios son grandes, los sistemas informáticos, son hoy en día una realidad emergente y con muchas expectativas de cara al futuro tanto en entornos empresariales o públicos.

Entre las tecnologías existentes aplicadas a la infraestructura de las empresas, se impone la comunicación mediante redes inalámbricas wifi. Las redes de comunicación wifi basadas en el estándar 802.11, al igual que la mayoría de redes inalámbricas, no están exentas de potenciales peligros que pueden ponerlas en un serio riesgo de compromiso de seguridad, amenazando la confiabilidad de la información recolectada de un entorno urbano, aumentando el riesgo de que se una vulnerabilidad o fallo en una infraestructura pueda

PPDRON 2016 - Noviembre.

extenderse y ocasionar fallos en otra, y así sucesivamente provocando un fallo en cascada.

La principal característica de los ataques a estas redes consiste en la naturaleza del medio de comunicación. Las comunicaciones inalámbricas utilizan el espectro electromagnético, por lo que un atacante con la cobertura adecuada podría interceptar la información sin ser detectado. Adicionalmente, muchas de las aplicaciones de estas redes se desarrollan en entornos no controlados e incluso hostiles, por lo que la seguridad física de los puntos de acceso tampoco puede controlarse. De estos dos factores se derivan la mayor parte de los riesgos, los cuales afectarán a la información y a la infraestructura.

Las redes inalámbricas están predispuestas a múltiples ataques debido a que su despliegue se realiza en áreas abiertas.

Las redes inalámbricas tienen un alto grado de disturbios y vulnerabilidad, además están presentes en ambientes hostiles. El software es desarrollado para facilitar la aplicación de las pruebas de prenteración a los hackers especialistas en seguridad informática.

3.2 Planeación del proyecto.

3.2.1 Plan de trabajo.

3.2.1.1 Objetivos del proyecto.

3.2.1.1.1 Objetivo General: Diagnosticar la seguridad de una red inalámbrica, a través de la identificación de sus vulnerabilidades y los posibles ataques que pueda sufrir.

3.2.1.1.2 Objetivos Específicos:

- Identificar el ataque más apropiado según el tipo de cifrado de la red.
- Registrar el acceso a una red.

PPDRON 2016 - Noviembre.

- Definir una escala de medición que corresponda a la seguridad de las redes.
- Estimar puntos estratégicos para la facilitación de las pruebas de penetración.
- Seleccionar el vehículo adecuado para transportar la información de los resultados.

-

3.2.1.1.3 Oportunidad del Negocio: Mejoramiento en las tareas repetitivas de pruebas de penetración para el aseguramiento del perímetro de una empresa a través de aviones no tripulados o robots que permitan detectar las vulnerabilidades de las redes inalámbricas.

3.2.1.1.4 Beneficiarios: Toda persona, entidad, institución, propietaria y/o usuaria de un punto de acceso inalámbrico.

3.2.1.1.5 Roles usuario finales: Hacker especialista en seguridad informática.

3.2.1.1.6 Atributos de Calidad del Software Funcionales:

- El sistema debe localizar el punto de acceso objetivo de la prueba de penetración.
- El sistema debe determinar de manera autónoma el mejor método de acceso, según las características del punto de acceso.
- El sistema debe generar un reporte sobre el nivel de seguridad del punto de acceso evaluado.
- El sistema puede movilizarse en sitios de difícil acceso, para lograr mejor cobertura del punto de acceso.
- El sistema debe registrar la información correspondiente al nombre de la red, el tipo de la red, el cifrado de la red, el tipo de ataque usado y la contraseña.

3.2.1.1.7 Atributos de Calidad del Software No Funcionales

- **Disponibilidad:** La duración de la batería del dron debe funcionar eficientemente media hora, después de haber sido cargado.

PPDRON 2016 - Noviembre.

- **Usabilidad:** El tiempo de aprendizaje del sistema por un usuario será menor a 1 hora, tras el cual no cometerá menos de 3 errores diariamente. El sistema debe contar con manuales de usuario estructurados adecuadamente.
- **Portabilidad:** El sistema funcionara en cualquier dron que tenga una duración mayor a 30 minutos. El sistema operará de forma correcta en ambientes de difícil acceso a excepcion de los ambientes acuáticos, en caso de fuego o temperatura menos 5°C.
- **Escalabilidad:** El sistema debe ser construido sobre la base de un desarrollo evolutivo e incremental, de manera tal que nuevas funcionalidades y requerimientos relacionados puedan ser incorporados afectando el código existente de la menor manera posible; para ello deben incorporarse aspectos de reutilización de componentes. El sistema debe estar en capacidad de permitir en el futuro el desarrollo de nuevas funcionalidades, modificar o eliminar funcionalidades después de su construcción y puesta en marcha inicial.
- **Seguridad:** El acceso al reporte y manejo del sistema estará con acceso limitado a unas credenciales del administrador del sistema.

3.2.2 Estimaciones.

3.2.2.1. Estimación de recursos.

3.2.2.1.1. Operacionales: Para realizar el proyecto el recurso humano necesario se compone de cinco personas distribuidas así: Cliente, Director de proyecto, Gerente, Programador y analista.

3.2.2.1.2. Técnicos: Para el desarrollo del proyecto es necesario contar con una placa Raspberry pi, un dron terrestre elaborado por el equipo, tres equipos portátiles, antena wifi, sistema operativo debian (basado en linux), la suite de seguridad informática, aircrack, tarjeta sd, linset.

PPDRON 2016 - Noviembre.

3.2.2.1.3. Económicos: El proyecto investigativo depende de la movilidad del equipo al perímetro que requiere ser auditado, así como de adquirir la placa Raspberry pi por lo cual se requiere una inversión de \$37.310.000 pesos que comprenden la placa Raspberry pi, el carro para transportar el sistema, una tarjeta SD, una antena wifi, los salarios de los integrantes del equipo por el tiempo de desarrollo del proyecto (2 meses) y los equipos portátiles que usarán los integrantes del equipo.

3.2.2.2. Análisis de Riesgos.

Como primera medida se identificaron una serie de riesgos, divididos según su tipo: proceso, producto, persona o proyecto

Ver anexo identificación de riesgos.

Para la gestión de riesgos se escogieron los riesgos de mayor impacto, que se traducen a los riesgos con un nivel de rango mayor a 60 en una escala de 1-100.

1. Fallos en el software: Los componentes del software elegido no trabajan adecuadamente.

Plan de prevención: Plantear diversos métodos para el desarrollo de cada módulo de software.

Plan de contingencia: Cuando se presente esta situación lo recomendable es regresar a la última versión del proyecto, que funcionaba con un buen rendimiento. Además se deben buscar las posibles causas de la situación de fallo, para solucionarlas en caso de que se presenten de nuevo o evitarlas en un futuro. A partir de ahí se generará una nueva línea de desarrollo, que tendrá como finalidad entregar un software funcional.

PPDRON 2016 - Noviembre.

2. Complejidad del sistema a construir: El sistema no ha sido abstraído correctamente, por lo tanto no se han cumplido con varios hitos.

Plan de prevención: Desarrollo de un cronograma para cada rol, para establecer la cantidad de tiempo correspondiente a cada una de las actividades, y de esta manera determinar el tiempo total de desarrollo e implementación, para decidir si este se ajusta a las peticiones del cliente.

Plan de contingencia: Reajuste de los requisitos funcionales, con el fin de dejar únicamente los que se puedan abarcar.

3. Falta de experiencia en el lenguaje de desarrollo: Problemas que se puedan presentar al momento de programar en un nuevo entorno de desarrollo.

Plan de prevención: Dos sesiones de capacitación por parte del programador por semana.

Plan de contingencia: Acudir a la documentación existente del lenguaje y a material didáctico que permita.

4. Inadecuada selección de las herramientas CASE: Mala interpretación por parte del equipo de la problemática establecida.

Plan de prevención: Utilización de herramientas reconocidas, de fácil manejo y que permitan exportar archivos.

Plan de contingencia: Cambio de herramienta CASE.

5. Incumplimiento de requisitos: Dejar de cumplir los requisitos provocaría el fallo total del proyecto.

Plan de prevención: Entablar una conversación con el cliente, para redactar los requisitos primordiales y sobre todo que tengan una factibilidad de cumplimiento.

PPDRON 2016 - Noviembre.

Plan de contingencia: Utilizar la semana de colchón para cubrir los requisitos faltantes, sino es posible replantear requisitos no entregados, añadirlos a los requisitos futuros.

3.2.3 Programas y mecanismos de control, administración y seguimiento del proyecto.

3.2.3.1. RTF revisiones técnicas y formales: Las revisiones técnicas formales se llevarán a cabo los días lunes de cada semana para verificar el avance del equipo en las tareas asignadas para cada rol.

3.2.3.2. Plantillas y listas de chequeo: Las plantillas y listas de chequeo serán realizadas por el documentador y el gerente del proyecto.

3.2.3.3. Software de calendarización de proyectos: Para realizar la planeación y calendarización de proyectos el equipo utilizará Libre Project como herramienta de calendarización y symphonical para planear las actividades de cada sprint de acuerdo con la metodología escogida (Scrum).

3.2.3.4. herramientas colaborativas: Como herramientas colaborativas el equipo usará Google Drive para almacenar toda la documentación del proyecto, Google Docs para facilitar las revisiones y correcciones que se deban hacer y GitHub para contener toda la parte de desarrollo como los códigos fuente y manejar versionamiento.

4. Metodología.

Luego del estudio de las condiciones de mercado y desarrollo para el proyecto, la metodología aplicada al proceso de producción será SCRUM, basada en desarrollo de proyectos de manera iterativa enfocándose principalmente en los módulos, funcionalidades y características que agregan más valor, con respecto a los objetivos, avances y tiempos de entrega en el producto, recibiendo

PPDRON 2016 - Noviembre.

constante retroalimentación del área de negocio para adaptar la construcción del producto a las cambiantes necesidades del proyecto.

Los procesos Scrum están diseñados de tal manera que el equipo de trabajo y las personas involucradas pueden trabajar a un ritmo de trabajo cómodo,, y ayudan a que este ritmo de trabajo continúe indefinidamente.

En etapas finales del proyecto asegurará una entrega del producto muy próxima a los deseos del cliente, optimizando tiempo, recursos y esfuerzos durante el desarrollo.

La duración de cada sprint fue de 1 semana, en cada sprint se abordó la construcción de un módulo del software y transversalmente la ejecución de las siguientes actividades: requisitos, análisis, diseño y pruebas. Se realizará una retrospectiva un día después de finalizar el sprint.

5. Desarrollo del proyecto.

5.1 Características, atributos de calidad del sistema y modelos de análisis.

5.1.1 REQUISITOS ESPECÍFICOS.

A continuación se describe la funcionalidad del software, los requerimientos del cliente, la interfaz gráfica de usuario que va a tener el software.

5.1.1.1 Interfaces Externas.

La información del reporte contendrá los resultados obtenidos de las pruebas realizadas a punto de acceso preconfigurado, se presentara la información en forma de tabla, incluyendo el nombre de la red, tipo de encriptación, vulnerabilidad encontrada, tiempo, credenciales obtenidas. Adicionalmente se incluye recomendación con respecto a los resultados obtenido.

PPDRON 2016 - Noviembre.

5.1.2 REQUERIMIENTOS DE USUARIO.

- El usuario que hará uso de la aplicación serán el tester.
- La aplicación permitirá la comodidad con respecto aplicación de pruebas de penetración en redes inalámbrica.
- También generará un reporte en formato HTML con las recomendaciones para el tester.

5.1.3 REQUERIMIENTOS DEL SISTEMA.

- Procesador Intel® Core™ i3-4150 (3MB Caché, 3.50 GHz).
- Memoria RAM 1 GB.
- Memoria SD 8 GB.
- Raspbian Jessie.
- Aircrack-ng.
- Reaver.
- PixieWPS.
- Nmap.
- Ettercap.
- Tshark.
- Evilgrade.
- Metasploit

5.1.4 REQUERIMIENTOS FUNCIONALES.

- El sistema debe localizar el punto de acceso objetivo de la prueba de penetración.


PPDRON 2016 - Noviembre.

- El sistema puede determinar de manera autónoma el mejor método de acceso, según las características del punto de acceso.
- El sistema debe tener un tiempo de ejecución de 15 minutos.
- El sistema debe guardar los paquetes capturados en el directorio de ejecución de PPDRON.
- El sistema debe generar un reporte sobre el tipo de seguridad del punto de acceso evaluado.
- El sistema puede movilizarse de manera adecuada, para lograr mejor cobertura del punto de acceso.

PPDRON 2016 - Noviembre.

5.2 DISEÑO Y ARQUITECTURA DEL SISTEMA

- **Identificación de stakeholders:** En la siguiente tabla se describe en detalle el usuario que utilizará el sistema.

<u>Stakeholder</u>	Descripción	Escenario	Vistas
 PEPE	El usuario PEPE es quien interactúa con el sistema para realizar el ataque y extrae la información del informe para realizar las respectivas Correcciones.	-Escenario el Diseño.	- Escenarios. - Diagrama de Caso de uso. -Diagrama de Procesos.

Identificación de Stakeholders.

- **Vista Lógica - Diagrama de Clases:** El diagrama de clases (ver figura 1) describe la estructura del sistema y las clases con las que se va a trabajar.

Figura 1. Diagrama de Clases PPDRON.

PPDRON 2016 - Noviembre.

- **Vista de Escenarios – Diagramas de Casos de Uso.**

Este caso de uso (ver figura 2) indica la interacción del usuario con PPDRON, en este caso el usuario ubica a PPDRON en el sitio donde se quiere realizar el ataque.

En este caso de uso (ver figura 3) el usuario configura el archivo *Settings.py* antes de realizar el ataque.

Para este caso de uso (ver figura 4), luego de configurar el archivo *Settings.py* se procede a realizar el ataque a la red.

PPDRON 2016 - Noviembre.



Figura 4. Caso de Uso Realizar Ataque.

En este caso de uso (ver figura 5), se muestra con detalle lo que hace PPDRON al atacar la red.

En este caso de uso (ver figura 6), el usuario extrae el reporte generado por PPDRON.

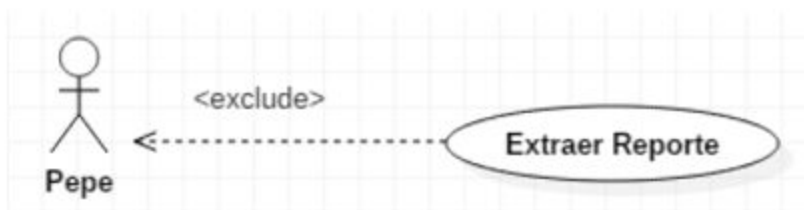


Figura 6. Caso de Uso Extraer Reporte.

PPDRON 2016 - Noviembre.

- **Vista de Procesos – Diagramas de Procesos.**

En este diagrama de proceso (ver figura 7), el usuario ubica a PPDRON en el sitio donde quiere realizar el ataque a la red.

PPDRON 2016 - Noviembre.

Para este diagrama de proceso (ver figura 8), se puede observar la interacción entre el usuario y el sistema durante la configuración del archivo *Settings.py*.

Figura 8. Diagrama de Proceso Configurar Archivo Settings.py

En este diagrama de proceso (ver figura 9), se observa la interacción entre el sistema y el usuario mientras se realiza el ataque a la red, al finalizar el usuario podrá extraer un reporte en formato HTML en el que encontrará las vulnerabilidades identificadas y las recomendaciones para subsanarlas.

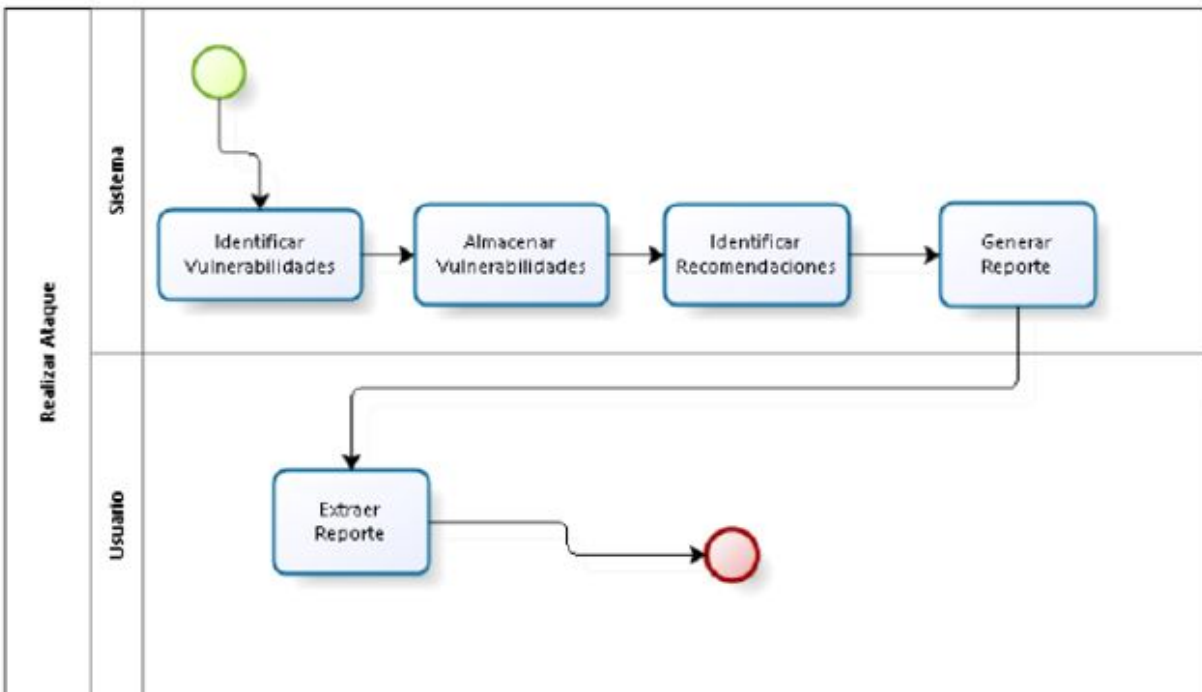


Figura 9. Diagrama de Proceso Realizar Ataque.

PPDRON 2016 - Noviembre.

- **Vista Física – Diagrama de Despliegue.**

En este diagrama (ver figura 10), se detalla la arquitectura física del sistema (hardware).

PPDRON 2016 - Noviembre.

- **Vista de Componentes – Diagrama de Despliegue.**

En el siguiente diagrama (ver figura 11), se observan los componentes del sistema y las dependencias entre estos.

5.3 Implementación.

La implementación de sistema desarrollado se hace sobre una placa raspberry pi 2 model b, instalando todas las dependencias establecidas para el funcionamiento del sistema. Adicionalmente se entrega el manual de usuario y técnico.

Posteriormente se instala la solución sobre un drone terrestre y se hacen las pruebas de funcionamiento con la alimentación por baterías.

5.4 Pruebas del sistema.

Se aplicaron pruebas al sistema terminado y completamente funcional. A continuación se muestran en detalle los casos de prueba finales a todo el

PPDRON 2016 - Noviembre.

sistema (ver tabla 1 a la 10).

PPDRON 2016 - Noviembre.

Caso de Prueba N°:	2	Responsable:	Andrea Katherine Velandia.
Fecha:	31 - 10 - 16	Historia de Usuario:	Identificar Tipo de Encriptación de la Red.
Autor Caso de Prueba:	Andrea Katherine Velandia.		
Escenario: Para la ejecución de este caso de prueba es necesario que el usuario ingrese en el sistema el nombre de la red que va a ser atacada.			
Secuencia Lógica: <ul style="list-style-type: none">● Configurar el archivo Settings.py con la siguiente información: nombre de la red teniendo en cuenta mayúscula y minúscula, interfaz, tiempo de escaneo del espectro, la MAC del AP y el tiempo destinado para realizar el escaneo.			
Resultados Esperados: <ul style="list-style-type: none">● Se espera que el sistema inicie el ataque.● Se espera que el sistema genere un mensaje indicando el inicio del ataque.● Si el sistema no puede encontrar el AP, se espera que genere un mensaje indicando que no encontró el AP.			
Resultados Obtenidos: <ul style="list-style-type: none">● El sistema encuentra el tipo de encriptación de la red y lo muestra en la pantalla.● Cuando el sistema no encuentra el tipo de encriptación de la red genera un mensaje indicando que no encontró el AP.			
Estado de la Prueba: PASÓ: X NO PASÓ:			
Observaciones:			

Tabla 2. Caso de Prueba 2 Identificar Tipo de encriptación de la red.

PPDRON 2016 - Noviembre.

Caso de Prueba N°:	5	Responsable:	Andrea Katherine Velandia.
Fecha:	31 - 10 - 16	Historia de Usuario:	Determinar ataque según vulnerabilidad del punto de acceso.
Autor Caso de Prueba:	Andrea Katherine Velandia.		
Escenario: Para la ejecución de este caso de prueba es necesario que el usuario ingrese en el sistema el nombre de la red que va a ser atacada.			
Secuencia Lógica: <ul style="list-style-type: none">● Configurar el archivo Settings.py con la siguiente información: nombre de la red teniendo en cuenta mayúscula y minúscula, interfaz, tiempo de escaneo del espectro, la MAC del AP y el tiempo destinado para realizar el escaneo.			
Resultados Esperados: <ul style="list-style-type: none">● Se espera que el sistema seleccione el AP correcto para el ataque.● Se espera que el sistema inicie el ataque teniendo en cuenta la encriptación del punto de acceso.			
Resultados Obtenidos: <ul style="list-style-type: none">● El sistema muestra líneas verdes que indican el correcto funcionamiento y líneas rojas si se encuentra un error.● Al cumplir con el tiempo estipulado el sistema escanea la red y luego selecciona el punto de acceso.			
Estado de la Prueba: PASÓ: X NO PASÓ:			
Observaciones:			

Tabla 5. Caso de Prueba 5 Determinar ataque según vulnerabilidad del punto de acceso.

PPDRON 2016 - Noviembre.

PPDRON 2016 - Noviembre.

PPDRON 2016 - Noviembre.

El sistema cumplió con los objetivos propuestos en el documento de especificación de requisitos, el tiempo de respuesta es óptimo, genera mensajes con la información necesaria para el usuario, genera un informe el formato HTML en el cual se visualiza la

PPDRON 2016 - Noviembre.

información de la red, proporciona recomendaciones según el tipo de ataque. El sistema aprobó con éxito los casos de prueba ejecutados. No fue posible la realización de pruebas de seguridad debido a que existe una baja probabilidad que la placa sea atacada por un dispositivo externo.

5.5 Aseguramiento de calidad.

La calidad de un producto es consecuencia del control en el ciclo de vida de un sistema. Para la evaluación de calidad se utilizaron checklist en cada fase de desarrollo basadas en el estándar iso 12207, para corregir errores y determinar omisiones o falta de elementos, las principales fallas y observaciones que se tuvieron fueron las siguientes:

- El modelo scrum se adapta al tipo de proyecto y al tiempo de desarrollo
- Se utilizaron las herramientas del plan de trabajo
- Lo siguientes requerimientos no son comprensibles:
 - El sistema debe generar un reporte sobre el nivel de seguridad del punto acceso evaluado.
 - El sistema debe determinar el mejor método de acceso.
- Construir un glosario acerca de las tecnologías usadas y el lenguaje usado en seguridad y redes
- Cambiar los requerimientos respecto a los ataques realizados
- Hace falta definir requisitos futuros
- Especificar el tiempo de duración máxima para un ataque
- Hace falta especificar el archivo de configuración
- Hace falta definir la generación de reportes en realizar ataque
- Hacen falta las pruebas finales
- Hace falta una power bank par la energización de la placa
- Realizar un documento de pruebas por cada sprint
- Añadir el ítem de resultados obtenidos en los casos de prueba

Con base a las observaciones el equipo de desarrollos hizo una serie de mejoras par acumpli con los items establecidos para cada fase de desarrollo.

Posteriormente, se desarrolló la evaluación de calidad de producto basada en el estándar ISO/IEC 9126, planteada y realizada por parte de un grupo externo, que hizo mediciones de cada característica.

6. Resultados.

PPDRON 2016 - Noviembre.

- Esta es una herramienta que ayuda a la aplicación de pruebas de penetración a redes inalámbricas.
- El software se desarrolló en el tiempo establecido y se entregó a tiempo.
- Se cumplieron las expectativas del cliente, respecto a la funcionalidad del software y su uso.
- Se adecuo satisfactoriamente un carro control remoto para transportar la placa que contiene el sistema
- El sistema cumple con todos los requerimientos de software establecidos previamente en el plan de trabajo.

7. Conclusiones y recomendaciones.

- La metodología de desarrollo escogida permitió abordar las actividades planeadas para el proyecto.
- La implementación de este tipo de proyectos debe regirse de acuerdo a la normatividad de cada país.
- La implementación del sistema en un dron debe regirse de acuerdo a las leyes que rigen este campo.

8. Referencias.

- IEEE. (1998). "Especificación de Requisitos según el estándar de IEEE 830"
Recuperado de: <http://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf>
- IEEE. (2000). "Documento de Arquitectura de Software IEEE 1471-2000".
Recuperado de:

PPDRON 2016 - Noviembre.

<https://jjegonzalezf.files.wordpress.com/2009/07/das-ieee1471-restaurant.pdf>

- ISO/IEC. (2002). "EVIDENCE PRODUCT CHECKLIST for ISO/IEC Standard 12207 Software Life Cycle Processes". Recuperado de: <http://www.techstreet.com/direct/SEPT/12207-2004ChecklistSample.pdf>

9. Anexos.

Identificación de riesgos

Persona

Amenaza	Descripción	Situación actual	Probabilidad	Impacto	Nivel de rango
Disponibilidad nula de algún integrante del grupo de desarrollo	Miembros del equipo no disponibles en momentos críticos.	No presentado	15	80	47.5
Cambio de requisitos	Cambio de requisitos por parte del cliente que precisan cambios en el diseño.	No presentado	5	30	17.5
Asignación inadecuada de roles	Procesos de selección de talento humano inadecuado y de cargos incorrectos.	No presentado	15	45	30
Características inapropiadas de los clientes	Error al identificar clientes que aporten al proyecto.	No presentado	10	20	15
Falta de inclusión del cliente en el proyecto.	El cliente no puede participar en revisiones y reuniones	No presentado	10	60	35
Baja motivación	Baja moral del personal, malas relaciones entre los miembros del equipo de desarrollo.	No presentado	30	70	50
Falta de comunicación	Dificultad de comunicación entre los miembros del equipo de desarrollo, o entre los desarrolladores y el cliente, lo que ocasiona retrasos y errores.	No presentado	40	30	35

PPDRON 2016 - Noviembre.

Producto

<i>Amenaza</i>	<i>Descripción</i>	<i>Situación actual</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Nivel de rango</i>
<i>Vehículo inadecuado</i>	<i>Error al estimar el tipo de vehículo que transporte la placa</i>	<i>No presentado</i>	<i>30</i>	<i>20</i>	<i>25</i>
<i>Hardware obsoleto</i>	<i>Utilización de recursos tecnológicos físicos que no tienen las características para generar un producto novedoso y competitivo</i>	<i>No presentado</i>	<i>10</i>	<i>50</i>	<i>30</i>
<i>Fallos en el software</i>	<i>Los componentes del software elegido no trabajan adecuadamente</i>	<i>No presentado</i>	<i>35</i>	<i>85</i>	<i>60</i>
<i>Incumplimiento de los tiempos propuestos</i>	<i>Los algoritmos de ataque no cumplen con los tiempos de respuesta</i>	<i>No presentado</i>	<i>40</i>	<i>60</i>	<i>50</i>
<i>Problemas climáticos</i>	<i>El clima puede afectar considerablemente la eficacia del sistema</i>	<i>No presentado</i>	<i>60</i>	<i>50</i>	<i>55</i>

Proyecto

<i>Amenaza</i>	<i>Descripción</i>	<i>Situación actual</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Nivel de rango</i>
<i>Tamaño estimado demasiado pequeño</i>	<i>El proyecto no fue concebido para los tiempos de desarrollo e implantación.</i>	<i>No presentado</i>	<i>20</i>	<i>90</i>	<i>55</i>
<i>Complejidad del sistema a construir</i>	<i>El sistema no ha sido abstraído correctamente, por lo tanto no se han cumplido con varios hitos</i>	<i>No presentado</i>	<i>70</i>	<i>50</i>	<i>60</i>
<i>Falta de recursos</i>	<i>Los recursos no están disponibles en un determinado momento</i>	<i>No presentado</i>	<i>50</i>	<i>20</i>	<i>30</i>
<i>Errores en la estimación del presupuesto</i>	<i>Falta de realización de un estudio que sustente el monto de inversión en el proyecto, además del manejo de contingencias</i>	<i>No presentado</i>	<i>30</i>	<i>30</i>	<i>30</i>
<i>Cambio de políticas de gestión</i>	<i>Cambio en los estándares y metodologías a seguir por el grupo</i>	<i>No presentado</i>	<i>40</i>	<i>20</i>	<i>30</i>
<i>Interferencia por parte de animales</i>	<i>Disturbios en el funcionamiento correcto del sistema, creadas por</i>	<i>No presentado</i>	<i>20</i>	<i>30</i>	<i>25</i>

PPDRON 2016 - Noviembre.

<i>la intrusión de animales</i>					
<i>Investigación incompleta</i>	<i>Riesgos intensos en investigación y generación de ideas para cumplir con los objetivos</i>	<i>No presentado</i>	30	60	45
<i>Proceso</i>					
<i>Amenaza</i>	<i>Descripción</i>	<i>Situación actual</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Nivel de rango</i>
<i>Falta de experiencia en el lenguaje de desarrollo</i>	<i>Problemas al programar en un nuevo entorno de desarrollo</i>	<i>No presentado</i>	50	70	60
<i>Diseño inadecuado</i>	<i>Falta de experiencia y de conocimientos al modelar la arquitectura del sistema.</i>	<i>No presentado</i>	30	50	40
<i>Definición del proceso</i>	<i>Definición del proceso de software y el seguimiento, errores en el análisis</i>	<i>No presentado</i>	30	50	40
<i>Retrasos en la especificación de requisitos</i>	<i>Demoras en construir y comprender los requisitos del sistema y detallar sus conceptos.</i>	<i>No presentado</i>	15	70	42.5
<i>Falta de monitoreo e implementación</i>	<i>Falta de seguimiento a cada una de las etapas de desarrollo e implementación.</i>	<i>No presentado</i>	40	70	55
<i>Inadecuada selección de las herramientas CASE</i>	<i>Mala interpretación por parte del equipo de la diagramación realizada.</i>	<i>No presentado</i>	80	80	80
<i>Documentación apropiada</i>	<i>Cantidad y calidad de los documentos entregados al cliente,</i>	<i>No presentado</i>	20	20	20

PPDRON 2016 - Noviembre.

	<i>documentos que no han sido redactados de forma objetiva ni revisados detenidamente</i>				
<i>Cambios en las prioridades</i>	<i>Modificación de la importancia de los hitos y por lo tanto de los tiempos de entrega</i>	<i>No presentado</i>	<i>50</i>	<i>40</i>	<i>45</i>
<i>Falta de cumplimiento de los requisitos</i>	<i>Dejar de cumplir los requisitos provocaría el fallo total del proyecto.</i>	<i>No presentado</i>	<i>30</i>	<i>90</i>	<i>60</i>
<i>Aplicación errónea de las RTF</i>	<i>No se llevan a cabo regularmente revisiones técnicas formales de las especificaciones de requisitos, diseño y código</i>	<i>No presentado</i>	<i>40</i>	<i>70</i>	<i>55</i>
<i>Falta de documentación en el código</i>	<i>Código sin documentar, que más adelante generará problemas en la fase de mantenimiento</i>	<i>No presentado</i>	<i>50</i>	<i>40</i>	<i>45</i>
<i>Mala ejecución de los tests de prueba</i>	<i>Realización inapropiada de tests de alto, mediano y bajo nivel</i>	<i>No presentado</i>	<i>30</i>	<i>70</i>	<i>50</i>
<i>Mal uso del repositorio central</i>	<i>El repositorio no es usado de acuerdo a lo establecido por el grupo de trabajo, ni se ha hecho un mantenimiento constante.</i>	<i>No presentado</i>	<i>30</i>	<i>30</i>	<i>30</i>

PPDRON 2016 - Noviembre.