Universidad del País Vasco
Euskal Herriko Unibertsitatea

Escuela Universitaria de Ingeniería Vitoria-Gasteiz
Ingeniaritzako Unibertsitate Eskola Vitoria-Gasteiz

Desarrollo de herramientas de seguridad informática para Android

Memoria del Trabajo de Fin de Grado

presentada para optar al grado de

Ingeniería Informática de Gestión y Sistemas de Información

por

Ander Granado Masid

Director: Pablo González Nalda

29 de marzo de 2017

Agradecimientos

Índice general

Índice de figuras

Resumen y Organización de la memoria

I

Alcance del Trabajo

1 Descripción, Objetivos y Motivación del proyecto

1.1. Descripción

En este trabajo se desarrolla un estudio sobre el campo de la seguridad informática, mas concretamente sobre las diferentes herramientas de seguridad informática. En base a eso, se desarrolla una aplicación para dispositivos móviles que busca, de manera sencilla para el usuario, proporcionar soluciones a tareas recurrentes dentro del campo de la seguridad informática, basandose en herramientas ya existentes. Estas herramientas, usadas por pentesters, analistas forenses o hackers de sobrero blanco permiten elaborar operaciones de todo tipo, desde escanear una red inalámbrica hasta romper el cifrado de un archivo para acceder a la información que contiene.

Gran parte de esta herramientas son gratuitas [Oficina de Seguridad del Internauta(2017)] o incluso de software libre [GitHub, Inc(2017)], lo que otorga la posibilidad de que dichas herramientas mejoren continuamente.

Sin embargo, el mayor problema de este tipo de herramientas suelen ser su público objetivo. Normalmente este tipo de herramientas están diseñadas para profesionales del sector, profesionales tanto con conocimientos de seguridad informática como de programación o administración de sistemas. La mayoría de estas herramientas se basan en librerías o frameworks completos, con cierta dificultad de uso, o scripts CLI. Debido a esto, cierta tarea como escanear una red, que para un experto en ciberseguridad o un administrador de sistemas se convierte en 5 segundos tecleando un comando, para un usuario medio se convierte en un auténtico quebradero de cabeza.

1.2. Objetivos

El objetivo de este este proyecto es doble. Por una parte se busca realizar un análisis del campo de la seguridad informática, un *estado del arte* del área que permita vislumbrar cuales son las diferentes aplicaciones de dicho área y a partir de ahí concretar las necesidades más importantes dentro de ese campo para, al final, acabar elaborando una aplicación para Android que nos proporcione ciertas utilidades.

Por otra parte, también se busca que la aplicación a elaborar sirva tanto para usuarios experimentados en la materia como para un público general. Para ello, un buen diseño de la interfaz gráfica (GUI) o diferentes principios de experiencia de usuario (UX) jugarán un papel fundamental. De esta manera lograremos una transición entre herramientas accesibles solo para unos pocos a una herramienta para todo el mundo.

1.3. Motivación

A día de hoy la informática es un industria fundamental dentro de la sociedad en general y de las vidas de las personas en particular. Los ordenadores personales son la herramienta fundamental de trabajo en una gran cantidad de áreas, ademas de una herramienta que se encuentra en prácticamente cualquier hogar. Los denominados Smartphones junto a Internet se han convertido en la principal herramienta de comunicación. La revolución causada por la industria llega hasta tal punto que una organización como la ONU ha declarado Internet *como un derecho humano por ser una herramienta que favorece el crecimiento y el progreso de la sociedad en su conjunto* [El Mundo(2011)],.

Teniendo en cuenta toda la información que transmitimos, almacenamos y procesamos, sería lógico pensar que la seguridad de dicha información es vital. El área de la seguridad informática se encarga de ofrecer los mecanismos necesarios para que nuestra información no se vea comprometida de ninguna manera y nuestros dispositivos permanezcan seguros y con la menor cantidad de vulnerabilidades posible. Cada vez este área resulta mas importante, y sobre todo ahora con la llegada del Internet of Things (IoT), ya que pasamos de tener no solo nuestros ordenadores o Smartphones conectados a Internet, sino que tenemos otros dispositivos como nuestro coche o nuestra lavadora conectados, con los riesgos que ello conlleva.

2 Viabilidad

Explicar para que sirve este punto y lo mas importante, explicar la separación en las 2 fases y el por qué de ésta.

2.1. Requisitos funcionales del trabajo

Poner los RF. Puntos cortos. Nada de párrafos. Como mucho 3 lineas por RF. No tienen que ser específicos, pero tiene que ser cosas que se cumplan si o si. Se pueden hacer a nivel general, si distinguir entre fases.

2.2. Planificación del tiempo

2.2.1. Estructura de Descomposición del Trabajo

El EDT. Se pone la separación en 2 fases, y en cada fases se puede separa por diferentes secciones. Poner por separado el EDT de la fase 1 y el de la Fase 2.

2.2.1.1. Fase 1

2.2.1.2. Fase 2

2.2.2. Agenda del proyecto

Poner el horario de trabajo, festivos y todo este tema que sirva para elaborar los cronogramas y determinar el tiempo del proyecto.

2.2.3. Tareas

Todas las tareas tanto de la Fase 1 como de la Fase 2, primero en lista y después como en cuadritos con descripción y tal.

0. Análisis del proyecto

- **0.1** Objetivos del proyecto
- **0.2** RF del proyecto

1. FASE 1

- **1.1** Formación
  - **1.1.1** Formación seguridad informatica
  - **1.1.2** Formación Pentesting
    - **1.1.2.1** Formación Teórica
    - **1.1.2.2** Formación NMap
  - **1.1.3** Formación Android
    - **1.1.3.1** Formación Diseño de GUI
    - **1.1.3.2** Fornacion Java, Gradle, ...
  - **1.1.4** Formación Git
  - **1.1.5** Formacion Latex

1.2 Elaboración del estado del arte

1.2.1 Evaluar estado de la profesión

1.2.2 Evaluar diferentes areas y aplicaciones

1.2.3 Documentar estado del arte

1.3 Preparación de la Fase 2

1.3.1 Conclusiones de la Fase 1

1.3.2 Revisión de objetivos

1.3.3 Modificación del análisis del proyecto

2. FASE 2

2.1 Preparación del entorno de trabajo

2.1.1 Instalación de herramientas

2.1.2 Configuracion de herramientas

2.2 Desarrollo de la aplicación

2.2.1 Diseño de la GUI

2.2.2 Implementacion de la apicación

2.2.2.1 Programación de herramientas básicas

2.2.2.2 Integración de Nmap

2.2.2.3 Programación de parser de elementos

2.2.2.4 Enlazado de datos con la GUI

2.2.3 Testeo

2.2.4 Corrección de bugs/errores

3. Elaboración de la memoria

3.1 Integración del estado del arte

3.2 Documentación de la aplicación desarrollada

3.3 Resumen de la memoria

3.4 Elaborar presentación

3.5 Preparación de la defensa

4. Reuniones periódicas

A continuación se explica mediante una breve definición en que consiste cada tarea, ademas de especificar su duración en horas.

Número: 0.1.

Nombre: Objetivos del proyecto.

Descripción: Definir los objetivos que tiene que cumplir el TFG.

Trabajo estimado: 5 horas.

Número: 0.2.

Nombre: RF del proyecto.

Descripción: Definir, en base a los objetivos del proyecto, los Requisitos funcionales concretos del proyecto.

Trabajo estimado: 5 horas.

Número: 1.1.1.

Nombre: Formación seguridad informática.

Descripción: Familiarizarse con el amplio entorno de la seguridad informática y comprender las diferentes áreas, objetivos y el estado de dicho campo.

Trabajo estimado: 30 horas.

Número: 1.1.2.1.

Nombre: Formación Teórica.

Descripción: Familiarizarse con los conceptos de Pentesting, las diferentes técnicas usadas y las diferentes fases del proceso de Pentesting.

Trabajo estimado: 20 horas.

Número: 1.1.2.2.

Nombre: Formación NMap.

Descripción: Familiarizarse con el entorno de NMap, como implementarlo, usarlo para obtener información y de que formas se puede obtener información estructurada y organizada para su posterior uso.

Trabajo estimado: 10 horas.

Número: 1.1.3.1.

Nombre: Formación Diseño de GUI.

Descripción: Aprender a usar herramientas de diseño de GUI, diferentes patrones de Diseño en sistemas Android, y el uso de IDEs o herramientas para desarrollar dichas GUIs.

Trabajo estimado: 10 horas.

Número: 1.1.3.2.

Nombre: Formación Java, Gradle, ...

Descripción: Aprender sobre el uso de Java para desarrollar aplicaciones Android, diferentes clases, utilidades o conceptos recurrentes en la programación para Android.

Trabajo estimado: 15 horas.

Número: 1.1.4.

Nombre: Formación Git.

Descripción: Aprender el uso de dicho sistema de control de versiones para llevar un control riguroso del desarrollo del proyecto y de la aplicación.

Trabajo estimado: 5 horas.

Número: 1.1.5.

Nombre: Formación Latex.

Descripción: Aprender diferentes conceptos de LaTeXpara elaborar tanto el estado del arte como el propio informe de la manera mas clara y elegante posible.

Trabajo estimado: 5 horas.

Número: 1.2.1.

Nombre: Evaluar estado de la profesión.

Descripción: Analizar los diferentes campos de la profesión, las necesidades mas demandadas y los diferentes perfiles de profesionales dentro del campo.

Trabajo estimado: 5 horas.

Número: 1.2.2.

Nombre: Evaluar diferentes áreas y aplicaciones.

Descripción: Evaluar las necesidades concretas a nivel técnico, las aplicaciones mas usadas y las virtudes y carencias de éstas.

Trabajo estimado: 10 horas.

Número: 1.2.3.

Nombre: Documentar estado del arte.

Descripción: Elaborar la documentación en base a toda la información recogida para obtener un elaborado estado del arte.

Trabajo estimado: 5 horas.

Número: 1.3.1.

Nombre: Conclusiones de la Fase 1.

Descripción: Elaborar una serie de conclusiones en función a todo el estudio realizado sobre el campo de la seguridad informática.

Trabajo estimado: 5 horas.

Número: 1.3.2.

Nombre: Revisión de objetivos.

Descripción: Revisión de los objetivos y los requisitos funcionales de la aplicación a desarrollar en función a todo lo investigado.

Trabajo estimado: 5 horas.

Número: 1.3.3.

Nombre: Modificación del análisis del proyecto.

Descripción: Modificar la parte de análisis del proyecto realizada anteriormente, antes de comenzar con la Fase 1.

Trabajo estimado: 5 horas.

Número: 2.1.1.

Nombre: Instalación de herramientas.

Descripción: Instalación de todo lo necesario para desarrollar la aplicación.

Trabajo estimado: 5 horas.

Número: 2.1.2.

Nombre: Configuración de herramientas.

Descripción: Configuración de todas las herramientas para que el desarrollo de la aplicación sea lo mas cómodo posible.

Trabajo estimado: 5 horas.

Número: 2.2.1.

Nombre: Diseño de la GUI.

Descripción: Diseñar una interfaz gráfica clara y sencilla de usar para interactuar con las funciones a implementar.

Trabajo estimado: 15 horas.

Número: 2.2.2.1.

Nombre: Programación de herramientas básicas.

Descripción: Programar herramientas básicas para el escaneo de redes.

Trabajo estimado: 10 horas.

Número: 2.2.2.2.

Nombre: Integración de Nmap.

Descripción: Integrar el núcleo de NMap en la aplicación para poder hacer uso de toda su funcionalidad.

Trabajo estimado: 10 horas.

Número: 2.2.2.3.

Nombre: Programación de parser de elementos.

Descripción: Elaborar un puente entre NMap y la aplicación para obtener los datos de NMap y poder usarlos en la aplicación de la manera más organizada posible.

Trabajo estimado: 20 horas.

Número: 2.2.2.4.

Nombre: Enlazado de datos con la GUI.

Descripción: Enlazar los datos con las diferentes vistas a través de diversos controladores, para poder visualizar e interactuar con ellos.

Trabajo estimado: 15 horas.

Número: 2.2.3.

Nombre: Testing.

Descripción: Una vez desarrollada la aplicación, realizar un amplio testeo para comprobar que funciona correctamente.

Trabajo estimado: 10 horas.

Número: 2.2.4.

Nombre: Corrección de bugs/errores.

Descripción: En base a los errores detectados en el testeo, implementar las correcciones a dichos fallos.

Trabajo estimado: 15 horas.

Número: 3.1.

Nombre: Integración del estado del arte.

Descripción: Integrar el estado del arte desarrollado dentro de la memoria.

Trabajo estimado: 5 horas.

Número: 3.2.

Nombre: Documentación de la aplicación desarrollada.

Descripción: Elaborar en base a todo el proceso de desarrollo una documentación clara sobre la aplicación e integrarla en la memoria.

Trabajo estimado: 15 horas.

Número: 3.3.

Nombre: Resumen de la memoria.

Descripción: Terminar la elaboración de la memoria, añadiendo las diferentes secciones necesarias y el formato correspondiente.

Trabajo estimado: 5 horas.

Número: 3.4.

Nombre: Elaborar presentación.

Descripción: Elaborar la presentación en diapositivas que se usará en la defensa ante el tribunal.

Trabajo estimado: 5 horas.

Número: 3.5.

Nombre: Preparación de la defensa.

Descripción: Preparar la defensa ante el tribunal en función a la documentación elaborada.

Trabajo estimado: 10 horas.

Número: 4.

Nombre: Reuniones periódicas.

Descripción: Reuniones periódicas con el director del TFG para llevar un control del desarrollo del proyecto.

Trabajo estimado: 15 horas.

2.2.4. Entregables

Entregables durante la Fase 1, si hay (en este caso seria solo la parte de la memoria).

2.2.4.1. Fase 1

2.2.4.2. Fase 2

2.2.5. Cronograma

Distribución de tareas de la Fase 1 en un cronograma generado con Project o una herramienta similar.

2.3. Fase 2

Parte de la aplicación.

2.3.1. Tareas

Todas las tareas de la Fase 2, primero en lista y después como en cuadritos con descripción y tal.

2.3.2. Entregables

Entregables durante la Fase 2, si hay (aplicación + la otra parte de la memoria que sirve como documentación de la aplicación y así).

2.3.3. Cronograma

Distribución de tareas de la Fase 2 en un cronograma generado con Project o una herramienta similar.

2.4. Gestión de costos

Poner los recursos que se necesitan.

2.4.1. Presupuesto

Todas las tablas y así, todo lo dado en la asignatura de Mari Carmen.

2.5. Gestión de riesgos

2.5.1. Fase 1

Poner los diferentes riesgos de la Fase 1. En esta fase son pocos o ninguno, por el carácter teórico de la fase.

2.5.1.1. Explicación y plan de contingencia

Explicar dichos riesgos. Poner por puntos. Puntos como descripción, peligrosidad, y medidas preventivas o para corregir. Nada de párrafos.

2.5.2. Fase 2

Poner los diferentes riesgos de la Fase 2. En esta fase los risegos son mucho mayores, ya que puede haber desde complicaciones a la hora de programar, limitaciones por no ser root,... Mil historias.

2.5.2.1. Explicación y plan de contingencia

Explicar dichos riesgos. Poner por puntos. Puntos como descripción, peligrosidad, y medidas preventivas o para corregir. Nada de parrafos.

II

Fase 1: Estado del Arte de la Seguridad Informática

3

Conceptos Generales

Lo primero para hablar sobre seguridad informática es explicar que es (lógico no?). Diferenciar ente seguridad informática y seguridad de la información y definir y explicar ligeramente los términos mas usados en el campo.

3.1. Seguridad Informática

3.2. Seguridad de la Información

3.2.1. Diferencias respecto a la Seguridad Informática

3.3. Servicios de la Seguridad de la Información

3.3.1. Confidencialidad, Integridad y Disponibilidad

3.3.2. Otros servicios

3.3.2.1. Autenticación

3.3.2.2. Anonimato

3.3.2.3. Protección a la réplica

4 Aplicaciones de la Seguridad Informática

Después de hablar de los conceptos básicos sobre la seguridad informática, en este capítulo se profundiza en las diferentes aplicaciones que tiene y en que áreas. En definitiva, explicar para que se usa donde se usa, también un poco cómo se usa en cada área y porque es tan importante su uso.

5 Pentesting

En esta sección se profundiza sobre el Pentesting, que al final es el área de la seguridad informaticá sobre la que va la aplicacion, el hecho de obtener información de sistemas y redes.

5.1. Objetivos

5.2. Partes

5.2.1. Recogida de información

5.2.1.1. Internal Footprinting

5.2.1.2. External Footprinting

5.2.2. Análisis de vulnerabilidades

5.2.3. Ataques de penetración

5.2.3.1. Ataques de contraseñas

5.2.3.2. Exploits

5.2.3.3. Auditoría de Aplicaciones Web

5.2.3.4. Ataques a redes

Ataques Wireless

6 Conclusiones

En este punto se extraen las conclusiones de todos los puntos anteriores, encarando el capitulo a elaborar la aplicación

III

Fase 2: Desarrollo de la aplicación

7 Introducción

Explicar tras el estado del arte en que va a consistir la aplicación.

8 Tecnologías y herramientas

Explicar las tecnologias que se van a usar para desarrollar la aplicación. He metido este punto aquí, en la FASE 2 ya que va mas ligado a ella, y ponerlo justo antes del desarrollo en sí me parece correcto.

8.1. Kali Linux

8.2. NMap

8.3. Android

8.3.1. Android SDK

8.3.2. Android Studio

8.4. Otras herramientas

8.4.1. Git

9 Desarrollo de la aplicación

Aquí ya al lío. Explicar como va a ser la GUI y como se han programado los diferentes aspectos de la app.

10 Testeo y corrección de errores

Tras programarlo todo pueden salir fallos, hay que hacer pruebas, e incluso habrá que cambiar cosas o añadir cosas nuevas. Todo eso va explicado aquí. NO CONFUNDIR con añadir nuevos requisitos funcionales o que se haya alargado el tiempo, eso va en la última parte, en la de conclusiones

IV

Análisis y conclusiones del Trabajo

V

Apéndices

Bibliografía

[El Mundo(2011)] El Mundo, June 2011. URL http://www.elmundo.es/elmundo/2011/06/09/navegante/1307619252.html.

[GitHub, Inc(2017)] GitHub, Inc, 2017. URL https://github.com/showcases/security.

[Oficina de Seguridad del Internauta(2017)] Oficina de Seguridad del Internauta, 2017. URL https://www.osi.es/es/herramientas-gratuitas.