Universidad del País Vasco
Euskal Herriko Unibertsitatea

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

Título Provisional

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

14 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.

2.3. Fase 1

Parte de teoría

2.3.1. Tareas

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

2.3.2. Entregables

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

2.3.3. Cronograma

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

2.4. Fase 2

Parte de la aplicación.

2.4.1. Tareas

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

2.4.2. Entregables

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

2.4.3. Cronograma

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

2.5. Gestión de costos

Poner los recursos que se necesitan.

2.5.1. Presupuesto

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

2.6. Gestión de riesgos

2.6.1. Fase 1

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

2.6.1.1. Explicación y plan de contingencia

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

2.6.2. 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.

2.6.2.1. 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

Conceptos, tecnologías y herramientas

3

Conceptos Generales

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 Pentesting

4.1. Objetivos

4.2. Partes

4.2.1. Recogida de información

4.2.2. Análisis de vulnerabilidades

4.2.3. Ataques de penetración

4.2.3.1. Ataques de contraseñas

4.2.3.2. Exploits

4.2.3.3. Auditoría de Aplicaciones Web

4.2.3.4. Ataques a redes

Ataques Wireless

5 Tecnologías y herramientas

5.1. Kali Linux

5.2. NMap

5.3. Android

5.3.1. Android SDK

5.3.2. Android Studio

5.4. Otras herramientas

5.4.1. Git

III

Desarrollo del Trabajo

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.