



Universidad
del País Vasco

Euskal Herriko
Unibertsitatea



Escuela Universitaria
de Ingeniería
Vitoria-Gasteiz

Ingeniariatzako
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

11 de abril de 2017

Agradecimientos

Índice general

Agradecimientos	III
Resumen	XI
I. Alcance del Trabajo	1
1. Descripción, Objetivos y Motivación del proyecto	3
1.1. Descripción	3
1.2. Objetivos	4
1.3. Motivación	4
2. Viabilidad	5
2.1. Requisitos funcionales del trabajo	5
2.2. Planificación del tiempo	6
2.2.1. EDT	6
2.2.1.1. Fase 1	8
2.2.1.2. Fase 2	9
2.2.2. Agenda del proyecto	9
2.2.3. Tareas	10
2.2.4. Entregables	20
2.2.4.1. Fase 1	20

2.2.4.2. Fase 2	20
2.2.5. Cronograma	21
2.3. Gestión de costos	24
2.3.1. Presupuesto	26
2.4. Gestión de riesgos	26
2.4.1. Fase 1	26
2.4.1.1. Explicación y plan de contingencia	27
2.4.2. Fase 2	27
2.4.2.1. Explicación y plan de contingencia	27
II. Fase 1: Estado del Arte de la Seguridad Informática	29
3. Conceptos Generales	33
3.1. Seguridad Informática	34
3.2. Seguridad de la Información	34
3.2.1. Diferencias respecto a la Seguridad Informática	34
3.3. Servicios de la Seguridad de la Información	34
3.3.1. CID	34
3.3.2. Otros servicios	34
3.3.2.1. Autenticación	34
3.3.2.2. Anonimato	34
3.3.2.3. Protección a la réplica	34
4. Aplicaciones	35
5. Pentesting	37
5.1. Objetivos	38
5.2. Partes	38
5.2.1. Recogida de información	38
5.2.1.1. Internal Footprinting	38
5.2.1.2. External Footprinting	38
5.2.2. Análisis de vulnerabilidades	38
5.2.3. Ataques de penetración	38
5.2.3.1. Ataques de contraseñas	38

5.2.3.2. Exploits	38
5.2.3.3. Auditoría de Aplicaciones Web	38
5.2.3.4. Ataques a redes	38
6. Conclusiones	39
III. Fase 2: Desarrollo de la aplicación	41
7. Introducción	43
8. Tecnologías y herramientas	45
8.1. Kali Linux	45
8.2. NMap	45
8.3. Android	45
8.3.1. Android SDK	45
8.3.2. Android Studio	45
8.4. Otras herramientas	45
8.4.1. Git	45
9. Desarrollo de la aplicación	47
10. Testeo y corrección de errores	49
IV. Análisis y conclusiones del Trabajo	51
V. Apéndices	53

Índice de figuras

2.1.	EDT completo	7
2.2.	EDT de la Fase 1	8
2.3.	EDT de la Fase 2	9
2.4.	Cronograma de la fase inicial	21
2.5.	Cronograma de la Fase 1	22
2.6.	Cronograma de la Fase 2	23
2.7.	Cronograma de la elaboración de la memoria	24

Resumen y Organización de la memoria

I

Alcance del Trabajo

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 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, además 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.

Este capítulo tiene como objetivo realizar, en base a los objetivos marcados en el capítulo anterior, elaborar un análisis de viabilidad del proyecto, analizando las diferentes tareas que contiene, calculando los correspondientes gastos y sus inherentes riesgos, que pueden afectar, atrasando o incluso impidiendo, la realización del proyecto.

2.1. Requisitos funcionales del trabajo

Los requisitos funcionales de la aplicación (RF a partir de ahora) se elaboran en base a los objetivos descritos y son los siguientes:

- Elaborar un estado del arte que analice el campo de la seguridad informática, sus aplicaciones y analice el área del pentesting
- Elaborar una aplicación que permita obtener información sobre redes y nodos de la red
- Integrar correctamente herramientas de terceros para lograr que la aplicación resulte lo mas escalable posible.
- Aplicar principios sobre experiencia de usuario (UX) y sobre el diseño de interfaces gráficas (GUI) para que la aplicación sea lo mas sencilla y cómoda de usar

2.2. Planificación del tiempo

2.2.1. Estructura de Descomposición del Trabajo

El EDT, o Estructura del Desglose del Trabajo, es un sistema jerárquico que permite organizar las diferentes tareas de un proyecto. Es una técnica ampliamente usada para gestionar todo tipo de proyectos, especialmente proyectos de software.

A la hora de planificar el tiempo, se ha tenido en cuenta un enfoque en dos fases, a las cuales denominaremos Fase 1 y Fase 2. Esto es debido al carácter del proyecto. Por una parte, para elaborar la aplicación anteriormente mencionada, resulta fundamental realizar un estudio sobre el campo de la seguridad informática, mas concretamente sobre el área del pentesting, para poder llegar a encontrar las mejores herramientas y técnicas que permitan desarrollarla. Este estudio, bien desglosado y fundamentado, llevara a la obtención de un elaborado estado del arte, que sera el principal objetivo de la Fase 1. Además, dicha fase contiene un periodo de aprendizaje y familiarización con diversos conceptos y tecnologías, que también quedaran reflejados.

En la Fase 2, en función de lo aprendido en la Fase 1, se elaborará la aplicación en base a los criterios de implementar diversas utilidades junto a un experiencia de usuario (UX) óptima, que vendrá acompañada de un buen diseño de una interfaz gráfica (GUI).

El EDT completo quedaría tal y como se muestra en la figura 2.1.

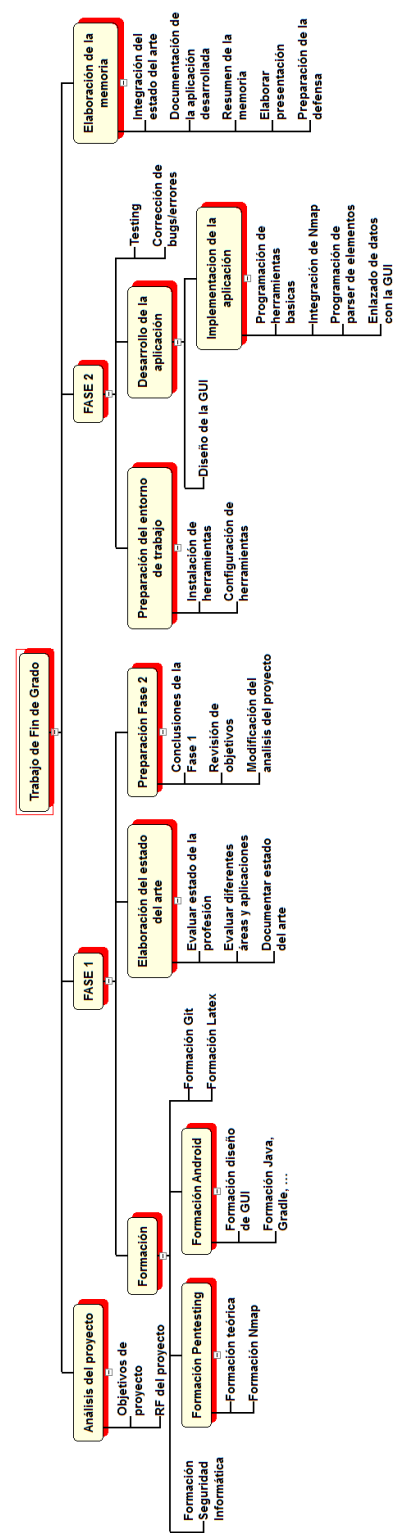


Figura 2.1.: EDT completo

2.2.1.1. Fase 1

El EDT para la Fase 1 quedaría como se muestra en la figura 2.2..

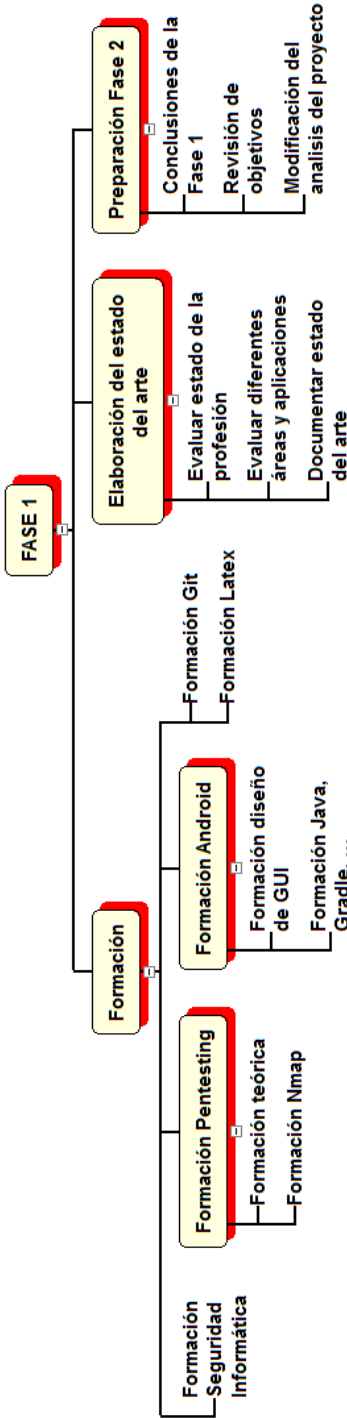


Figura 2.2.: EDT de la Fase 1

2.2.1.2. Fase 2

El EDT para la Fase 2 quedaría como se muestra en las figura 2.3.

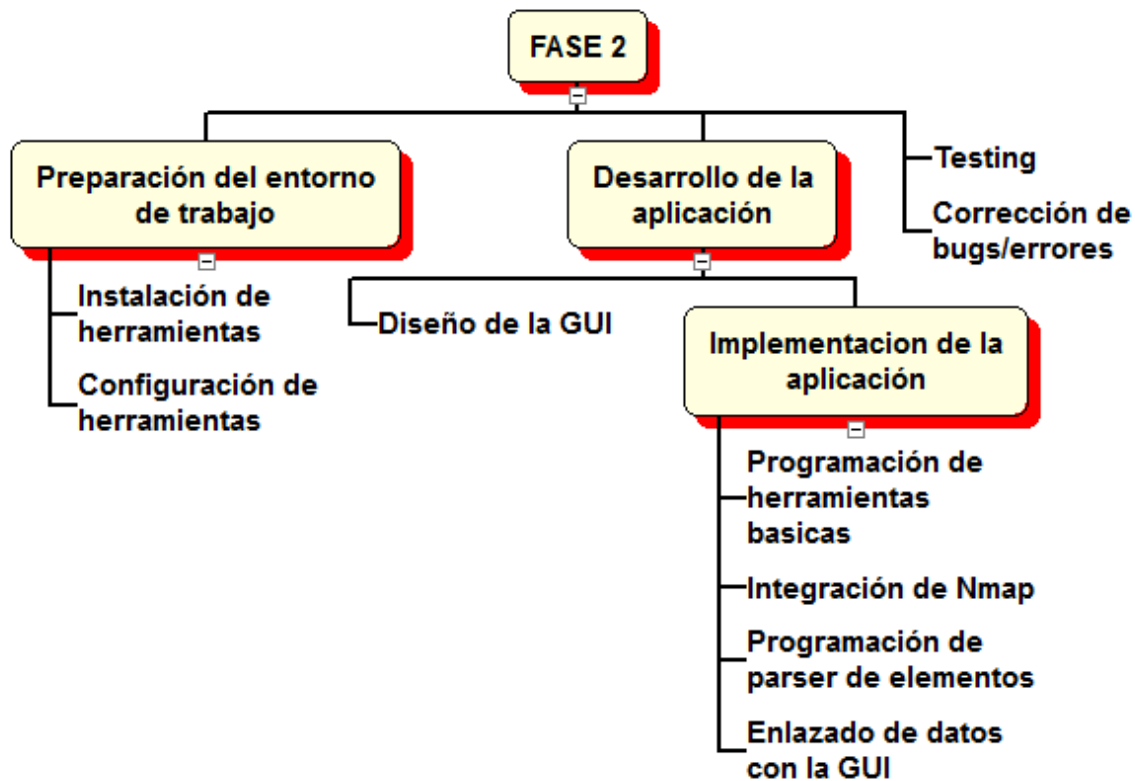


Figura 2.3.: EDT de la Fase 2

2.2.2. Agenda del proyecto

El proyecto se llevara a cabo durante varios meses, comenzando en abril. Se trabajará a media jornada (4 horas) de lunes a viernes, con las siguientes excepciones. Primero, se tendrá en cuenta el calendario de festivos oficiales para aplicar algunas jornadas festivas en cuyos días no se trabajará. Esos días quedan reflejados en la tabla 2.1. A esos festivos se les aplica unas excepciones, en las cuales, aun siendo festivo, se trabajará igualmente. Esos festivos en los que se trabaja están indicados en rojo.

Fecha	Evento
1 de Enero	Año nuevo
6 de Enero	Día de Reyes
19 de Marzo	San José
2 de Abril	Jueves Santo
3 de Abril	Viernes Santo
6 de Abril	Lunes de Pascua
28 de Abril	San Prudencio
1 de Mayo	Día del trabajo
25 de Julio	Santiago Apóstol
5 de Agosto	Virgen Blanca
15 de Agosto	Asunción de la Virgen
12 de Octubre	Fiesta Nacional de España
8 de Diciembre	Inmaculada Concepción
25 de Diciembre	Navidad

Cuadro 2.1.: Calendario de días festivos oficial (de Álava)

Por otra parte, existen una serie de días en los que se aplica una reducción de la jornada laboral de 4 a 2 horas (en los días considerados laborales), debido básicamente a exámenes. Estos periodos vienen indicados en la tabla 2.2.

Nombre del periodo	Fecha de inicio	Fecha de fin
Exámenes Convocatoria Ordinaria	16 de mayo	23 de mayo
Exámenes Convocatoria Extraordinaria	27 de junio	4 de julio

Cuadro 2.2.: Reducciones de la jornada laboral

En base a dicho calendario, la fecha estimada de finalización del proyecto es del 24 de Julio.

2.2.3. Tareas

El EDT completo de tareas, al que se añaden la fase inicial de objetivos del proyecto, y toda la fase final de elaboración de la memoria, presentación y la defensa quedaría de la siguiente

manera.

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 Configuración de herramientas

2.2 Desarrollo de la aplicación

2.2.1 Diseño de la GUI

2.2.2 Implementación de la aplicación

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, además 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 \LaTeX para 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

2.2.4.1. Fase 1

El entregable de la Fase 1 consistirá en un estado del arte redactado sobre el campo de la seguridad informática, enfocándose en el área del pentesting.

2.2.4.2. Fase 2

El entregable de la Fase 1 consistirá en una aplicación elaborada, que sirva como herramienta para el escaneo de redes informáticas. La aplicación, elaborada para Android, está correctamente empaquetada, con los posibles fallos corregidos y además dispondrá de una GUI sencilla de usar.

2.2.5. Cronograma

El cronograma completo, con las dos fases, como se muestra en las figuras 2.4, 2.5, 2.6 y 2.7 respectivamente.

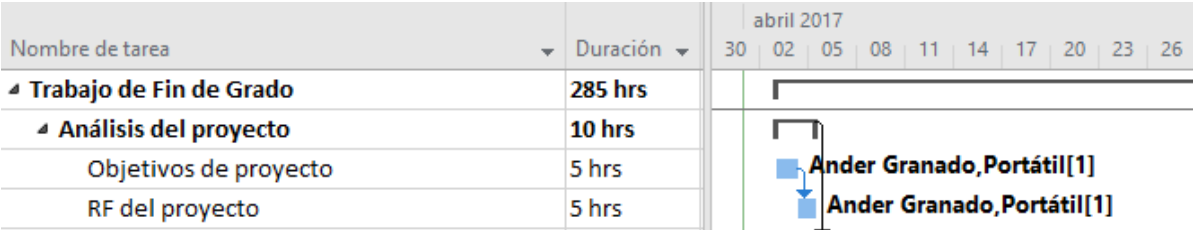


Figura 2.4.: Cronograma de la fase inicial

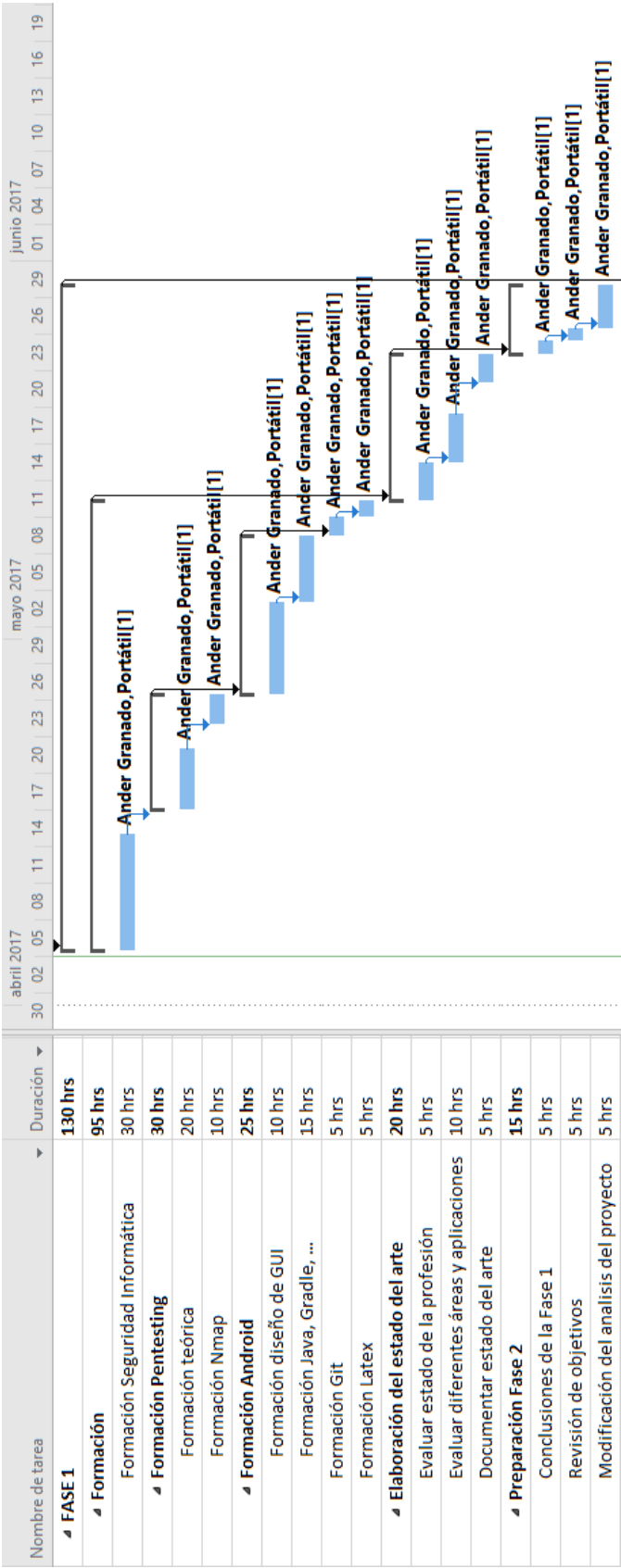


Figura 2.5.: Cronograma de la Fase 1

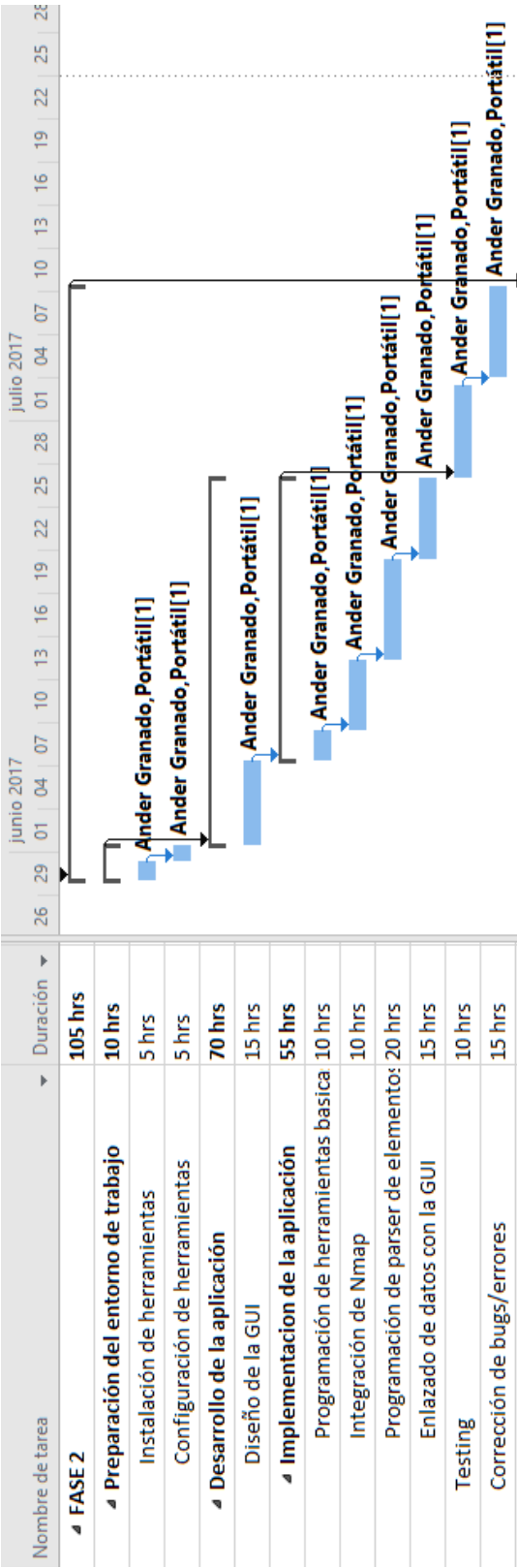


Figura 2.6.: Cronograma de la Fase 2

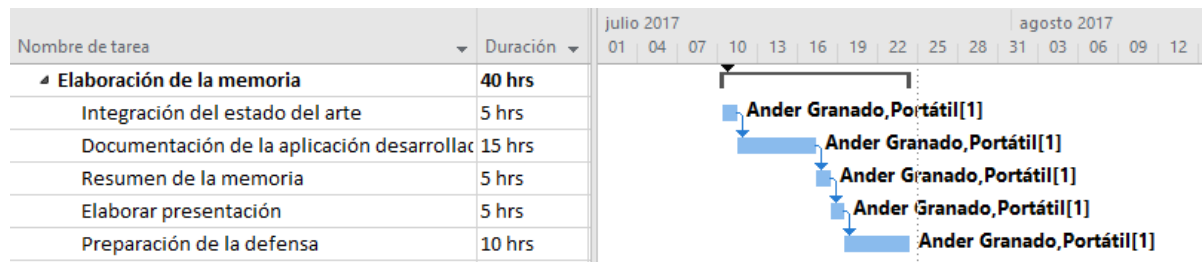


Figura 2.7.: Cronograma de la elaboración de la memoria

2.3. Gestión de costos

Poner los recursos que se necesitan.

Concepto	Coste
Ander Granado	14,00 €/h

Cuadro 2.3.: Recursos de trabajo

Concepto	Coste
Ordenador portátil	700,00 €
BQ Aquaris M5	250,00 €

Cuadro 2.4.: Recursos materiales (hardware)

Concepto	Coste	Numero de licencias
Windows 10	135,00 € [Microsoft(2017b)]	1
Project 2016	1369,00 € [Microsoft(2017a)]	1
WBS Chart Pro	187,50 € [Critical Tools(2017)]	1
Ubuntu 16.04	0,00 €	1
TeX Studio	0,00 €	1
Android Studio	0,00 €	1
NMap	0,00 €	1
Git	0,00 €	1
GitHub	0,00 €	1

Cuadro 2.5.: Recursos materiales (software)

Concepto	Trabajo (h)	Trabajo horas extra	Coste	Coste horas extra	Importe
Ander Granado	285	0	14,00 €/h	0	4.044,00 €

Cuadro 2.6.: Costo de recursos de trabajo

Concepto	Unidades	Coste	Importe
Ordenador portátil	1	1,50 €/uso	29 x 1,50 € = 43,50 €
BQ Aquaris M5	1	1,50 €/uso	7 x 1,50 € = 10,50 €
TOTAL			54,00 €

Cuadro 2.7.: Costo de recursos materiales

Concepto	Coste unitario	T. de amortización	C. U. amortización	T. de uso	Importe
Ordenador portátil	700,00 €	4800 horas			
BQ Aquaris M5	250,00 €	4800 horas			
Windows 10	135,00 €	4800 horas			
Microsoft Project 2016	1369,00 €	4800 horas			
WBS Chart Pro	187,50 €	4800 horas			
Ubuntu 16.04	0,00 €	4800 horas			
TeX Studio	0,00 €	4800 horas			
Android Studio	0,00 €	4800 horas			
NMap	0,00 €	4800 horas			
Git	0,00 €	4800 horas			
GitHub	0,00 €	4800 horas			

Cuadro 2.8.: Amortizaciones de hardware y de software

Concepto	Importe
Recursos de Trabajo (R.T.)	4.044,00 €
Recursos Materiales (R.M.)	4.044,00 €

Cuadro 2.9.: Total presupuesto

2.3.1. Presupuesto

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

2.4. Gestión de riesgos

2.4.1. Fase 1

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

2.4.1.1. Explicación y plan de contingencia

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

2.4.2. Fase 2

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

2.4.2.1. Explicación y plan de contingencia

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

II

Fase 1: Estado del Arte de la Seguridad Informática

Conceptos Generales

ESTADO DEL ARTE EN PROGRESO AQUI:

https://docs.google.com/document/d/1Zduryv6S6K_mwBTUrqA1NTov28VGW_3DHoxPQBBf608/edit?usp=sharing

Lo primero para hablar sobre seguridad informática es explicar que es (lógico no?). Diferenciar entre 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

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.

Pentesting

En esta sección se profundiza sobre el Pentesting, que al final es el área de la seguridad informática sobre la que va la aplicación, 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

Conclusiones

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

III

Fase 2: Desarrollo de la aplicación

Introducción

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

Tecnologías y herramientas

Explicar las tecnologías 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

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.

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

Apéndice

Bibliografía

- [Critical Tools(2017)] Critical Tools, 2017. URL <https://store.criticaltools.com/>.
- [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>.
- [Microsoft(2017a)] Microsoft, 2017a. URL https://www.microsoftstore.com/store/mseea/es_ES/pdp/Project-Profesional-2016/productID.324452600.
- [Microsoft(2017b)] Microsoft, 2017b. URL https://www.microsoftstore.com/store/mseea/es_ES/pdp/Windows-10-Home/productID.320437800.
- [Oficina de Seguridad del Internauta(2017)] Oficina de Seguridad del Internauta, 2017. URL <https://www.osi.es/es/herramientas-gratuitas>.