



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

INGENIERÍA EN INFORMÁTICA

Proyecto de seguridad informática



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

INGENIERO EN INFORMÁTICA

Proyecto de seguridad informática

- Departamento: Teoría de la señal, Telemática y Comunicaciones
- Director del proyecto: Gabriel Maciá Fernández
- Autor del proyecto: Moisés Gautier Gómez

Granada, 23 de abril de 2016

Fdo: Moisés Gautier Gómez

Índice general

Índice general	I
Índice de tablas	III
Índice de figuras	V
1. Introducción	1
1.1. Objetivos	1
1.2. Contexto: Historia sobre los sistemas de detección	2
1.3. Alcance	2
1.4. Visión global	2
2. Estado del arte	3
3. Especificación y análisis de requisitos	5
4. Diseño	7
5. Implementación	9
6. Evaluación	11
7. Planificación y estimación de costes	13
7.1. Software utilizado	13
7.2. Licencia	13

Índice de tablas

Índice de figuras

Capítulo 1

Introducción

“CITA” “Estar preparado para la guerra es uno de los medios más eficaces para conservar la paz” - George Washington

Hacer una breve descripción sobre el mundo de la seguridad informática, su repercusión en la sociedad y el futuro que tendrá en la revolución “digital” de todos los procesos de la vida cotidiana y empresarial con casos cómo el internet de las cosas y demás guisados.

También explicar un poco por encima del cometido a grandes rasgos por el que esa necesidad de vigilar dónde van los datos, conexiones y demás dentro de una máquina (O.S.) obliga a éste tipo de software (iptables, snort, glances) a funcionar y cómo una recopilación y procesamiento de los datos que estos generan permiten enfocar unas soluciones más prácticas y concisas sobre cómo actuar ante fuga de información (citar casos cómo wikileaks o robo de información en empresas por decir algo vamos)

1.1. Objetivos

El objetivo principal del proyecto es controlar los tipos de conexiones entrante y salientes de una máquina en sus diferentes protocolos de comunicación y mecanismos de gestión (firewall, ids, watchdogs, etc).

La aplicación deberá cumplir los siguientes requisitos:

- Ser una herramienta multiplataforma y que permita a cualquier usuario definir sus propias interfaces de gestión de incidencias (en el sentido de que pueda hacerse una clase.py en el kernel de la aplicación y esta sea capaz de hacer el resto simplemente con instanciar a dicha nueva clase.
- Dotar de funcionalidad gráfica que permita extraer información en tiempo real con gráficas o mecanismos visuales (en web) del sistema de base de datos que ha procesado los inputs de las fuentes para las que ha sido configurada.
- Dotar de una api interna que nos permita extraer información en tiempo real en un formato uniforme para la web o para que alguien pueda usar la funcionalidad del proyecto para su propio beneficio usando herramientas generadas en el backend para otro tipo de aplicaciones (fumada guapa)

1.2. Contexto: Historia sobre los sistemas de detección

Contar alguna de las historias del libro el arte de la intrusión a modo de referencia, o buscar por ahí alguna relacionada con fuga de datos o similares.

1.3. Alcance

Que resultado se obtendrá con el proyecto y cómo se divide este internamente. Aquí podría poner el gráfico del controller, bd, visualizations, manager y demás. Si se usa alguna notación también podría especificar cuál y porque.

1.4. Visión global

Cómo se divide internamente la memoria del pfc y que se va a hacer referencia en cada parte de la misma.

Capítulo 2

Estado del arte

Si por estado del arte se refiere a los precedentes del proyecto cómo herramienta, pues hay muchas que ya hacen algo similar cómo lookwise, logstash, elasticsearch, kibana, etc.

que aportan estos software al público general y porque la necesidad de mi pfc tal cuál. Podría explicar que se enmarca en un proyecto de investigación del grupo o invertarme una nube de humo muy grande.

Realizar una aproximación temporal en el tiempo para describir la evolución de las otras soluciones. Esto no lo entiendo muy bien [NOTA]

Tecnologías (descripción) python: librerías cómo pygtail, gunicorn, django (framework), d3, c3, react

Capítulo 3

Especificación y análisis de requisitos

Análisis de requisitos en el plan se necesita desarrollar una aplicación para solventar éste problema y se ha planteado con estas premisas (source, controller, manager, etc) que a su vez han necesitado de un aprendizaje, explicar porque se ha hecho una cosa de una manera (sqlite3 vs mysql), etc.

Especificacion de los requisitos

Análisis (Justificacion de la especificacion)

Capítulo 4

Diseño

<diseño>——</diseño>

- estructura de clases (diagrama)
- diseño de la vista (patrón)
- arquitectura del sistema

Capítulo 5

Implementación

<implementacion>——</implementacion>

- git
- archivos de instalación
- archivos de configuración (estructura)
- fuentes del código
- jerarquía de clases (implementación)

Capítulo 6

Evaluación

- pruebas funcionales y no funcionales
- caja blanca
- caja negra

Capítulo 7

Planificación y estimación de costes

Ya tengo hecho así por encima el diagrama de gantt de todo el proyecto. Tendría que definir las tareas en el diagrama pero lo que haré será meter aquí los apuntes que he ido metiendo en la herramienta Taiga para que se vea alguna descripción o apuntes que he ido tomando por cada tarea del diagrama.

7.1. Software utilizado

El lenguaje usado es python 2.7, luego django con todo los paquetes asociados (poner algún enlace de referencia dónde se listen los paquetes más importantes que he tenido que instalar sin nombrar todas las dependencias de estas)

He usado cómo IDE Pycharm del proyecto jetbrains

Para la memoria \LaTeX y para las gráficas tikz supongo.

7.2. Licencia

La licencia del proyecto para su posterior uso. En el actual repositorio de bitbucket no se ha especificado la licencia tal cuál, pero cuando ya este más estable el asunto también lo pondre en github para subirlo y demás. Ahí ya si que tendré que especificarla. En principio sino es para ningún proposito comercial, con la MIT sería suficiente. Sino alguna variante de la GPL o la Mozilla o similares.

