16-jul-2016

UGR

Encargado del proyecto	
Fechas de inicio y fin del proyecto	01-may-2015 - 19-jul-2016
Progreso	0%
Tarea	80
Recursos	0

El objetivo principal del proyecto es desarrollar un software que permita recopilar y visualizar la información generada por las aplicaciones de monitorización y control de seguridad que se ejecutan en una máquina.

La motivación del mismo surge fruto de la necesidad de monitorizar un red corporativa a través de un mecanismo de gestión automatizada de eventos, o lo que viene siendo un SIEM. Los pasos para la realización de este sistema se han modularizado y dividido en diferentes etapas que se acometarán cómo un todo dentro del proyecto de investigación VERITAS (http://nesg.ugr.es/veritas/) del Network Engineering & Security Group (NESG - http://nesg.ugr.es/) perteneciente al área de Ingeniería Telemática de la Universidad de Granada.

Tarea

Nombre	Fecha de inicio	Fecha de fin
Comienzo del proyecto	1/05/15	1/05/15
Planificación y estudio del estado del arte	4/05/15	7/05/15
Tecnología de los Monitores	11/05/15	15/05/15
Tecnología de los mánager	12/05/15	18/05/15
Tecnología de las BBDD	13/05/15	19/05/15
Tecnología de los assets	18/05/15	21/05/15
Tecnología de la visualización	25/05/15	28/05/15
Definición de la estructura en Git (BitBucket) y uso de la Heramienta Taiga	1/06/15	4/06/15
Reunión de planificación con el Tutor *Reunión día Martes 9 de Junio de 2015 - Duración: 1 hora* *Se trataron los siguientes puntos* *- Tipo de formato de los logs de los firewalls (iptables y essentials)* *- Centrar el esfuerzo en crear una base de datos que pueda ser flexible con distintos assets no contemplados en el caso base* *- El trabajo de los monitores será del tipo hilo padre (Manager) e hilos hijos (monitores) que harán la monitorización de lo assets del sistema.*	9/06/15	9/06/15
Reunión de planificación con el Tutor *Reunión día Jueves 11 de Junio de 2015 - Duración: 2:30 hora* *Se trataron los siguientes puntos* *- Especificación de nuevas tareas semanales y la definición de la base de datos.*	11/06/15	11/06/15
Arquitectura Manager	12/06/15	17/06/15
Arquitectura BBDD - Formato de Tablas	12/06/15	12/06/15
Arquitectura Local Visualization	12/06/15	17/06/15
Arquitectura Assets	12/06/15	17/06/15
Arquitectura Monitor	12/06/15	17/06/15
Reunión de planificación con el Tutor	19/06/15	19/06/15
Tarea 1: Análisis de Base de Datos	15/06/15	17/06/15
Tarea 2: Implementar una primera solución de BD	15/06/15	17/06/15
Tarea 2.1: Forma de operaciones con la BD	15/06/15	15/06/15
Tarea 3: Definir las tablas de la base de datos	16/06/15	29/06/15
Tarea 4: Procesos vs hilos	18/06/15	29/06/15
Tarea 5: Modelos diferentes de monitores	12/06/15	12/06/15
Reunión de planificación con Tutor	26/06/15	26/06/15
Tarea 6: Driver de fuente	29/06/15	30/06/15
Tarea 6.1 : Check Source	29/06/15	29/06/15
Tarea 6.2: Forma de comprobar si un dato de source se ha actualizado	1/07/15	6/07/15
Tarea 6.3 : Implementar una primera solución para iptables	29/06/15	15/02/16
Tarea 6.4 : Configuración de rsyslog para generación logs iptables	26/10/15	28/10/15
Métodos que hay que crear en la BD	23/06/15	29/06/15
Reunión de planificación con Tutor	1/07/15	1/07/15
Diseñar un diagrama en UML de clases para la base de datos	30/06/15	30/06/15
Reunión de planificación con Tutor	6/07/15	6/07/15
Reunión de planificación con Tutor	13/07/15	13/07/15

Tarea

Nombre	Fecha de inicio	Fecha de fin
Reunión 29 de Octubre	29/10/15	29/10/15
Reunión 30 de Octubre	30/10/15	30/10/15
Cambiar nombre de las columnas events	3/11/15	3/11/15
Fichero de configuración de log_sources	3/11/15	9/11/15
Cambiar nombres de tablas	3/11/15	3/11/15
Añadir campos a la tabla log_sources	3/11/15	10/11/15
Cambiar campos tabla IPs	3/11/15	3/11/15
Nuevas sources a procesar	3/11/15	10/11/15
Comprobar si existe una línea en blanco en el archivo de log	9/11/15	10/11/15
Resolución a la inversa para obtener el hostname de una ip	4/11/15	10/11/15
Refactorización del código fuente	3/11/15	3/11/15
Cambiar el nombre de archivos	3/11/15	3/11/15
Reunión 12 de Noviembre	12/11/15	12/11/15
Inicialización de clase Iptables	16/11/15	17/11/15
Refactorizar el código	16/11/15	17/11/15
Base de Datos - 1	16/11/15	17/11/15
Base de Datos - 2	16/11/15	17/11/15
Base de Datos - 3	16/11/15	17/11/15
Base de Datos - 4	16/11/15	18/11/15
GUI: Evaluar alternativas y ponerlas en funcionamiento	16/11/15	20/11/15
Estudio: Servicio entre BD y Front-end	16/11/15	4/12/15
Proceso de aprendizaje Django	7/12/15	8/02/16
Archivo de configuración de supervisor	16/12/15	16/12/15
Cambiar el formato de los timestamps de rsyslogd	18/12/15	18/12/15
Herencia en modelo de django	14/01/16	14/01/16
Aprendizaje de Reactjs (api para la aplicación)	22/01/16	22/04/16
Gulp (Optimización de código js y css)	25/01/16	26/01/16
Bower	26/01/16	26/01/16
Webpack / browserify	28/01/16	28/01/16
D3js - Proceso de aprendizaje	29/01/16	11/04/16
Visualización de la base de datos primera aproximación	4/11/15	22/04/16
Dotar a X.offset y X.log de permisos adm o de lectura	11/11/15	14/01/16
Reunión 11 de Febrero 2016	11/02/16	11/02/16
Reunión 13 de Mayo 2016	13/05/16	13/05/16

Tarea

Nombre	Fecha de inicio	Fecha de fin
[LATEST] Problemas imprevistos en las fechas del sistema *Me he dado un problema esta semana dado que la lista de días de esta semana es la siguiente [25,26,27,28,29,30,0]. Ése cero al final representa al día 1 del mes de mayo. Lo que sucede es que a la hora de iterar sobre la lista ese cero cómo que no cuadra.* *Lo que he tenido que hacer es generarme una lista de la primera semana del mes siguiente por si acaso vuelve a ocurrir este problema y usarla en otro bucle si detectamos un día cero en la siguiente lista, corresponden a los días del mes anterior que previamente teniamos, es decir:* *lista del mes de abril de la semana actual: [25, 26, 27, 28, 29, 30, 0]* *lista del mes de mayo de la primera semana: [0, 0, 0, 0, 0, 0, 1]* *Usando estas dos lista tengo cubierto la semana de abril que no sea cero y la semana de mayo que no sea cero y así poder insertar o poder tomar la fecha en concreto de toda la semana.*	25/04/16	12/05/16
[LATEST] Proceso de generación visual - Reactjs - C3js	25/04/16	12/05/16
[NEXT] Memoria pfc	16/05/16	15/07/16
[NEXT] Usar el paquete de configuración para iptables *Configuración y uso del paquete configparser para la lectura de archivos de configuración de iptables en este supuesto.*	27/05/16	30/05/16
[NEXT] Refactorizar el código	30/05/16	10/06/16
[NEXT] Separar la ejecución de iptables del resto.	13/06/16	24/06/16
[NEXT] [NEXT] Implementar la clase MANAGER, y monitorizar el número de hebras que se están ejecutando de los monitores (por fuente).	13/06/16	24/06/16
[NEXT] Implementar Iptables cómo heredada de una clase Controller	13/06/16	24/06/16
[NEXT] Hacer diagrama de flujo de ejecución de la aplicación Django	27/06/16	6/07/16
Reunión 7 de Julio 2016	7/07/16	7/07/16
Reunión 8 de Julio 2016	8/07/16	8/07/16
[NEXT] Bibliografía	18/07/16	18/07/16
[NEXT] Visualización	8/07/16	8/07/16

Diagrama de Gantt

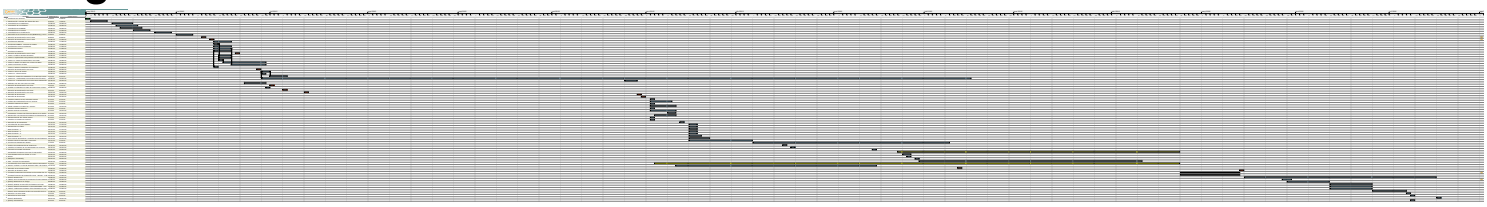

Diagrama de recursos