Auditoría de Redes

Introducción

Todos los sistema de comunicación desde el punto de vista de la auditoria, presentan en general una problemática común: la información transita por, y es accesible desde, lugares físicamente alejados de las personas responsables. Esto presupone un compromiso en la seguridad, porque no existen métodos físicos que garanticen la inviolabilidad de la información. Ni tampoco un compromiso en la disponibilidad, dado que un fallo en las comunicaciones impide dar el servicio.
Cuando se establece una comunicación a través de la red, la información desciende a través de una pila formada por las siete capas que presenta el modelo OSI (condensadas en cuatro en el modelo TCP/IP equivalente) atraviesa el medio físico y asciende a través de las siete capas en la pila de destino.
Este modelo lleva a presentar diferentes vulnerabilidades dependiendo de la capa en que nos encontremos. Para el caso de la red física pueden producirse tres tipos de incidencias:

- Alteración de bits
- Alteración de secuencia
- Ausencia de paquetes

Por causas dolosas, los tres mayores riesgos a tener en cuenta son:

- Indagación (un paquete es leído por terceros)
- Suplantación (un tercero puede introducir un paquete)
- Modificación

Para este tipo de problemas la única medida efectiva en las redes de tipo WAN y MAN es el uso de criptografía, en redes LAN suelen ser más prácticas el uso de medidas de control de acceso al edificio y al cableado. Cuando hablamos de redes locales, el mayor peligro físico es que alguien instale una escucha no autorizada.

Auditando a la Organización

Cada vez más y más las comunicaciones están tomando un papel determinante en el tratamiento de datos, convirtiéndose en una función clave en la empresa. Es por ello que las políticas de seguridad en esta área, deben estar escritas, aprobadas formalmente y actualizadas. Estos mecanismos lo que buscan es proteger de los riesgos previsibles, estos procedimientos deben estar documentados y verificados, de manera tal de detectar problemas o intrusiones. La organización a cargo de la red, debe poseer una estructura y unos procedimientos a seguir que aseguren las mejores prácticas en el soporte y provisión de servicios. El modelo ITIL (Biblioteca de Infraestructura de Tecnología de la Información) es un estándar orientado al ciclo de vida del servicio de las Tecnologías de la Información, se encuentra estructurado en cinco áreas que corresponden a:

- Estrategia de Servicio
- Diseño del Servicio
- Transmisión en el Servicio
- Operación del Servicio
- Mejora Continua del Servicio

El primer punto de una auditoria es determinar que la función de gestión de redes y comunicaciones esté claramente definida y gestionada, debiendo ser responsable, de:

- Gestión de la red, inventario de equipamiento y normativa de conectividad.
- Vigilancia de las comunicaciones, registro y resolución de problemas.
- Participación activa en la estrategia de proceso de datos, fijación de estándares de comunicaciones a usarse en el desarrollo de aplicaciones y evaluación de necesidades en comunicaciones.
- Mantener la documentación de la red al día.
- Revisión de costes y su asignación, de proveedores y servicios de transporte, y selección de equipamiento.

Como objetivos de control se debe tener en cuenta, los siguientes aspectos:

- Una política de seguridad escrita, entendida y ejecutada.
- Un área de comunicaciones responsable de seguir procedimientos operativos documentados.
- Procedimientos y registro de inventario y cambios.
- Segregación de tareas y de funciones de control de la red.
- Separación de entornos de desarrollo, pruebas y producción.
- Procedimientos para vigilar el uso de la red de comunicaciones, realizar ajustes para mejorar el rendimiento, registrar y resolver cualquier problema, y controlar costes y proveedores.
- Procedimientos de seguridad y control de intrusiones en la red.
- Participación activa del área de comunicaciones en el diseño de las nuevas aplicaciones online para asegurar que se sigue la normativa de comunicaciones, se planifica la capacidad requerida, y se acepta su puesta en marcha.

Auditando la red física

En una primera división, se establecen distintos riesgos para los datos que circulan dentro del edificio, de aquellos que viajan por el exterior. Por lo tanto debe auditarse hasta qué punto las instalaciones físicas del edificio ofrecen garantías, y se han estudiado las vulnerabilidades existentes.

Como objetivo de control, se debe reseñar las existencia de:

- Áreas seguras para los equipos de comunicaciones, previniendo así accesos inadecuados.
- Protección y tendido adecuado de cables y líneas de comunicaciones.
- Mantenimiento y gestión de equipos de red.
- Controles de utilización de los equipos de pruebas en comunicaciones.
- Atención específica a la recuperación de los sistemas de comunicación de datos, en el plan de recuperación de desastres en sistemas de información.
- Controles específicos en caso de que se utilicen salidas directas al exterior, para prevenir accesos no autorizados

Auditando la red lógica

Cada vez más se tiende a que un equipo pueda comunicarse con cualquier otro equipo, de manera que sea la red de comunicaciones el vínculo común que las une, es decir la red hace que un equipo pueda ilegítimamente acceder a cualquier otro, incluyendo el tráfico que circule hacia cualquier equipo de la red, todo esto de manera lógica sin la implementación de algún dispositivo físico. Es por esto que una buena estrategia es segmentar la red, de manera que unos problemas en un segmento no tienen porqué afectar a

toda la instalación. Una intrusión se puede contener mejor si el acceso a un punto no implica el acceso a todo. A su vez la segmentación ayuda a detectar mal uso interno, y limitar el acceso ilegítimo conseguido mediante herramientas legítimas.

Como objetivos de control, se debe revisar la existencia de:

- Política documentada de uso de servicios de red.
- Autenticación de usuarios obligatoria, para limitar y detectar cualquier intento de acceso no autorizado.
- Autenticación de equipos, para limitar y detectar cualquier intento de conectar un equipo no autorizado a la red de comunicaciones.
- Las funcionalidades para uso remoto de equipos como puertos abiertos y operación remota han de estar desactivadas.
- Segregación de redes, para incrementar puntos de control y posiblemente la defensa en profundidad.
- Controles de privilegios de usuario de conexión a la red.
- Control de flujos de información, encaminamiento y redundancia.
- Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

Herramientas que sirven para auditar una red

Se pueden auditar 2 elementos principales:

- Elementos funcionales: Configuración de los equipos, accesos, restricciones, vulnerabilidades en los equipos, políticas de tráfico, etc.
- Elementos no funcionales: Velocidades constantes (tanto de subida como de bajada), tiempo de convergencia de los routers en la red, señal intermitente, cobertura de la señal inalámbrica, etc.

Tener en cuenta a la hora de auditar:

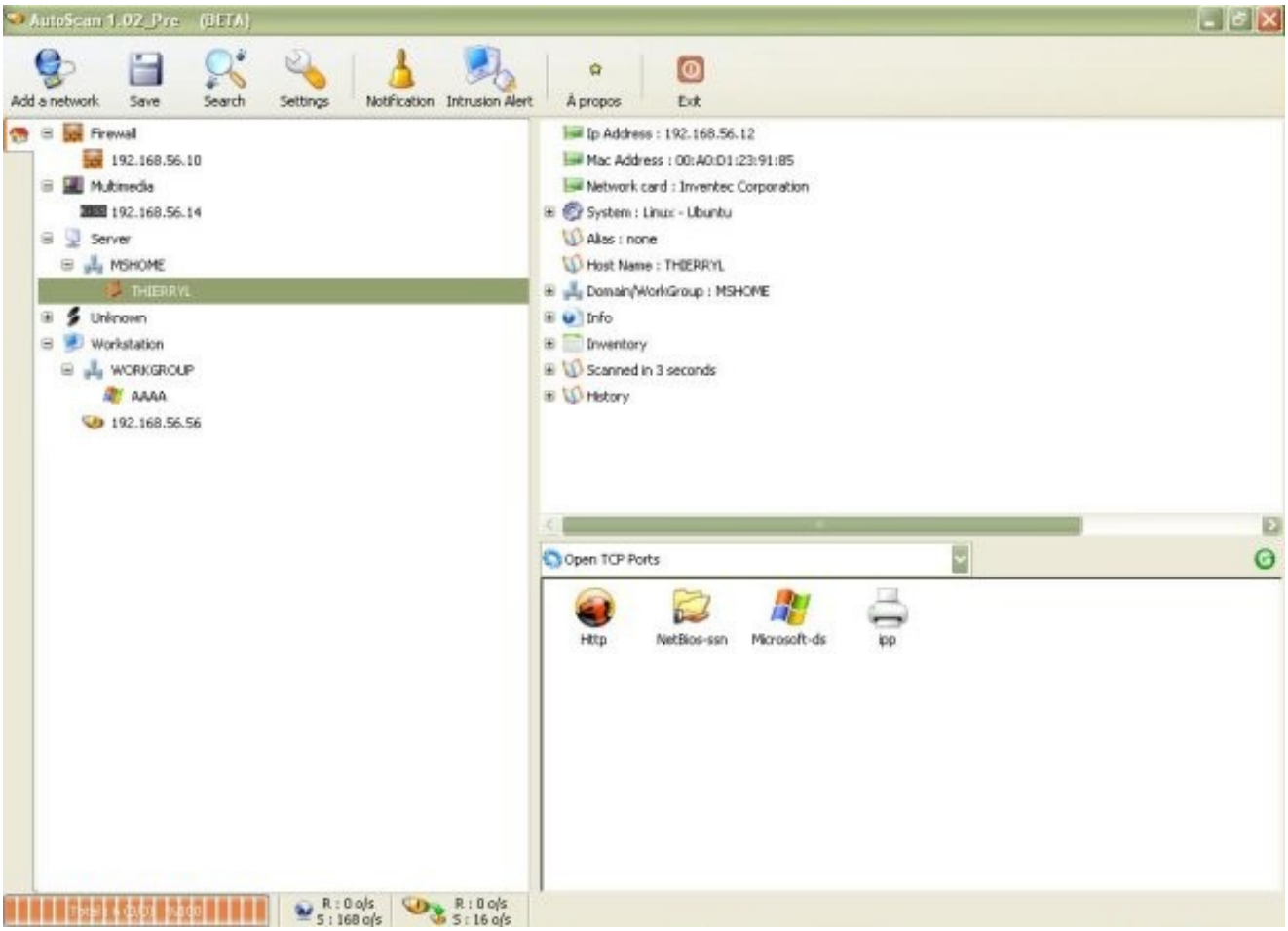
- Usuarios (equipos) no autorizados en nuestra red.
- El tráfico de nuestra red (para detectar tráfico sospechoso).
- Vulnerabilidad en nuestros usuarios.
- En caso de tener servidores en nuestra red, se deberán llevar a cabo auditorías específicas para cada servicio.

Para las redes inalámbricas:

- Seguridad en nuestros puntos de acceso (AP)
- Difusión de nuestra señal
- Tipo de seguridad en la conexión
- Tipo de cifrado (en caso de que el AP lo permita)
- Alcance longitudinal (esférico) de nuestra señal.

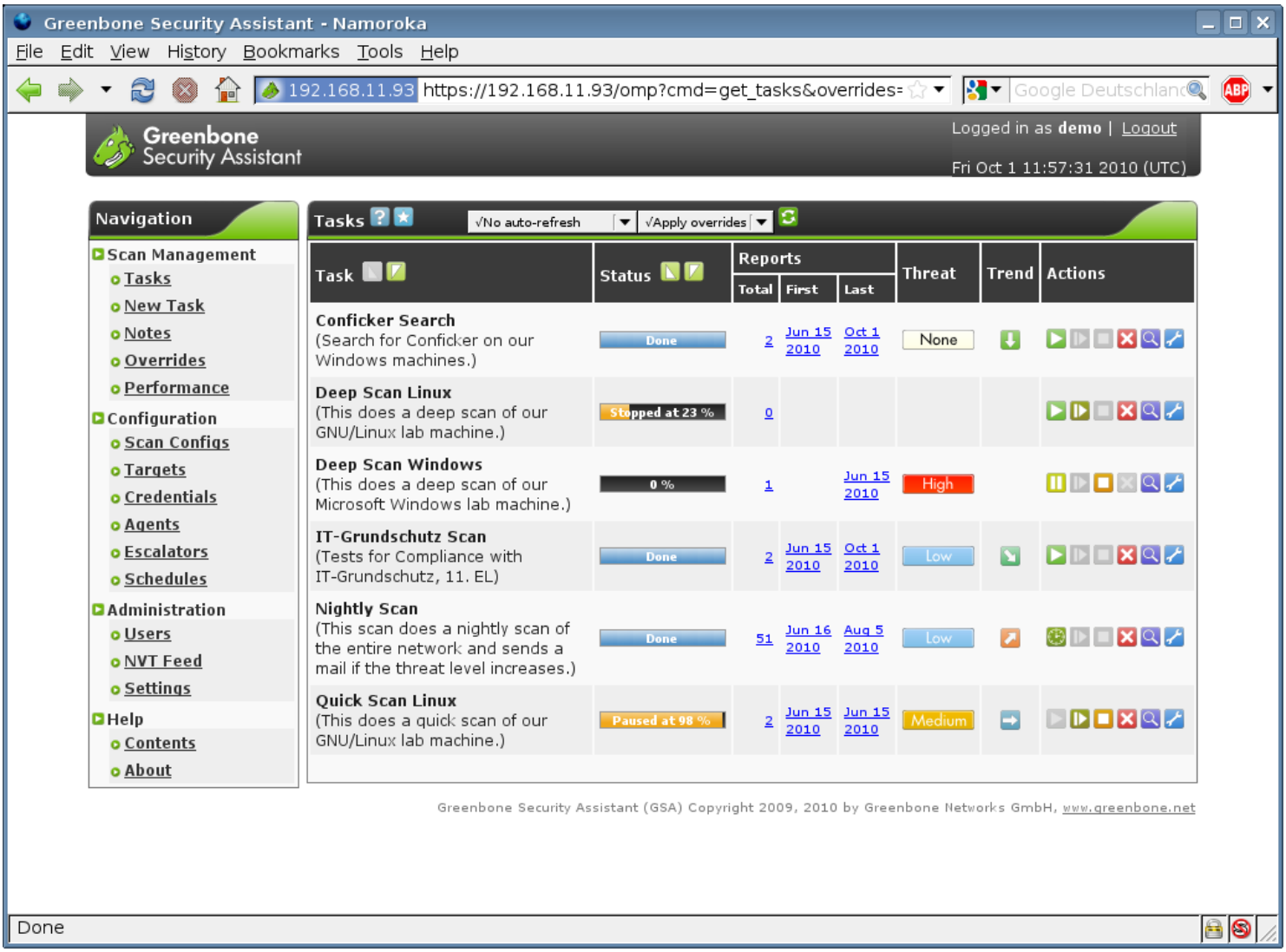
Autoscan

Para descubrimiento de red, su principal objetivo es identificar equipos conectados a la red.



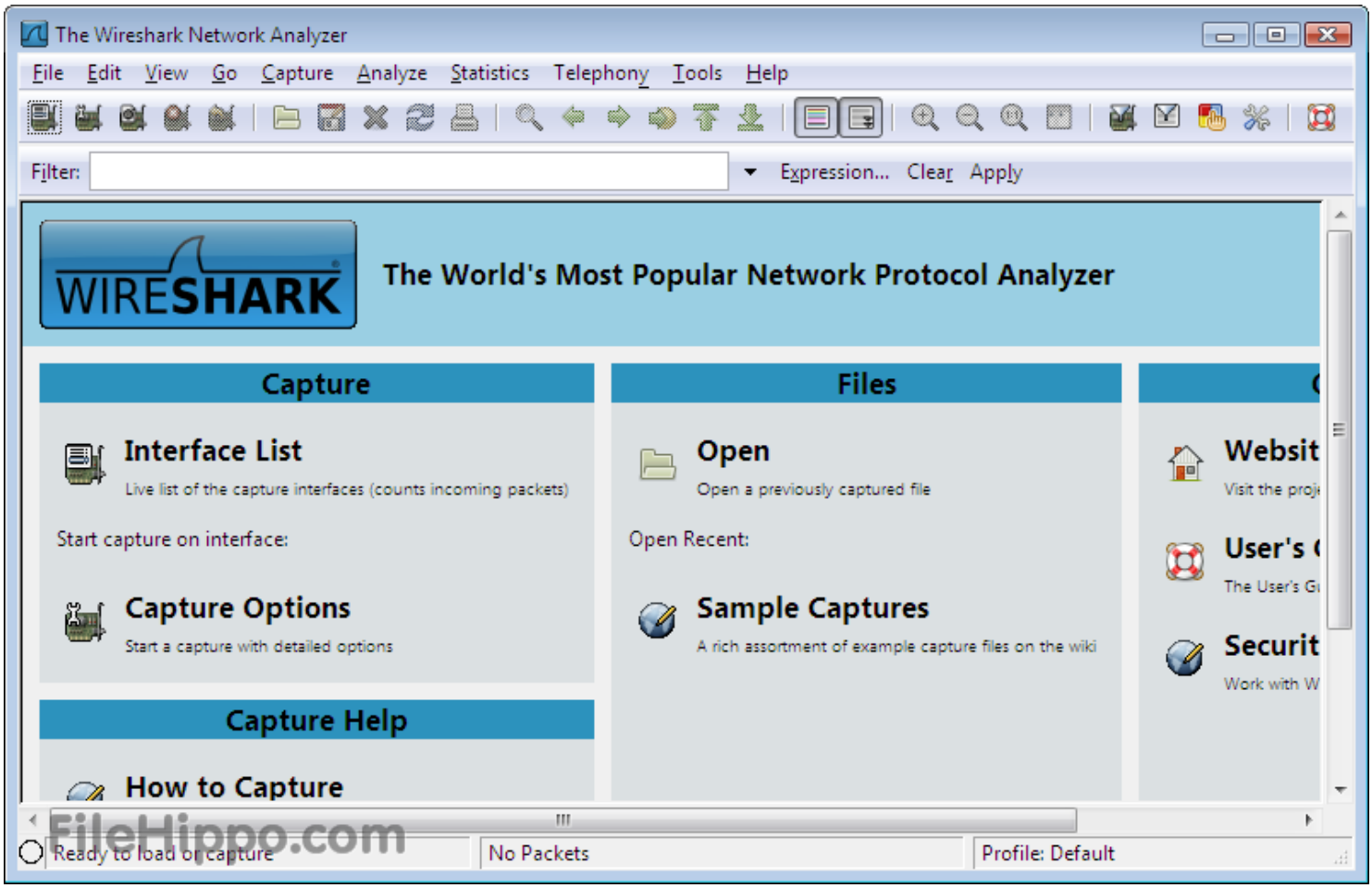
OpenVAS

Herramienta para la detección de vulnerabilidades en la red.



Wireshark

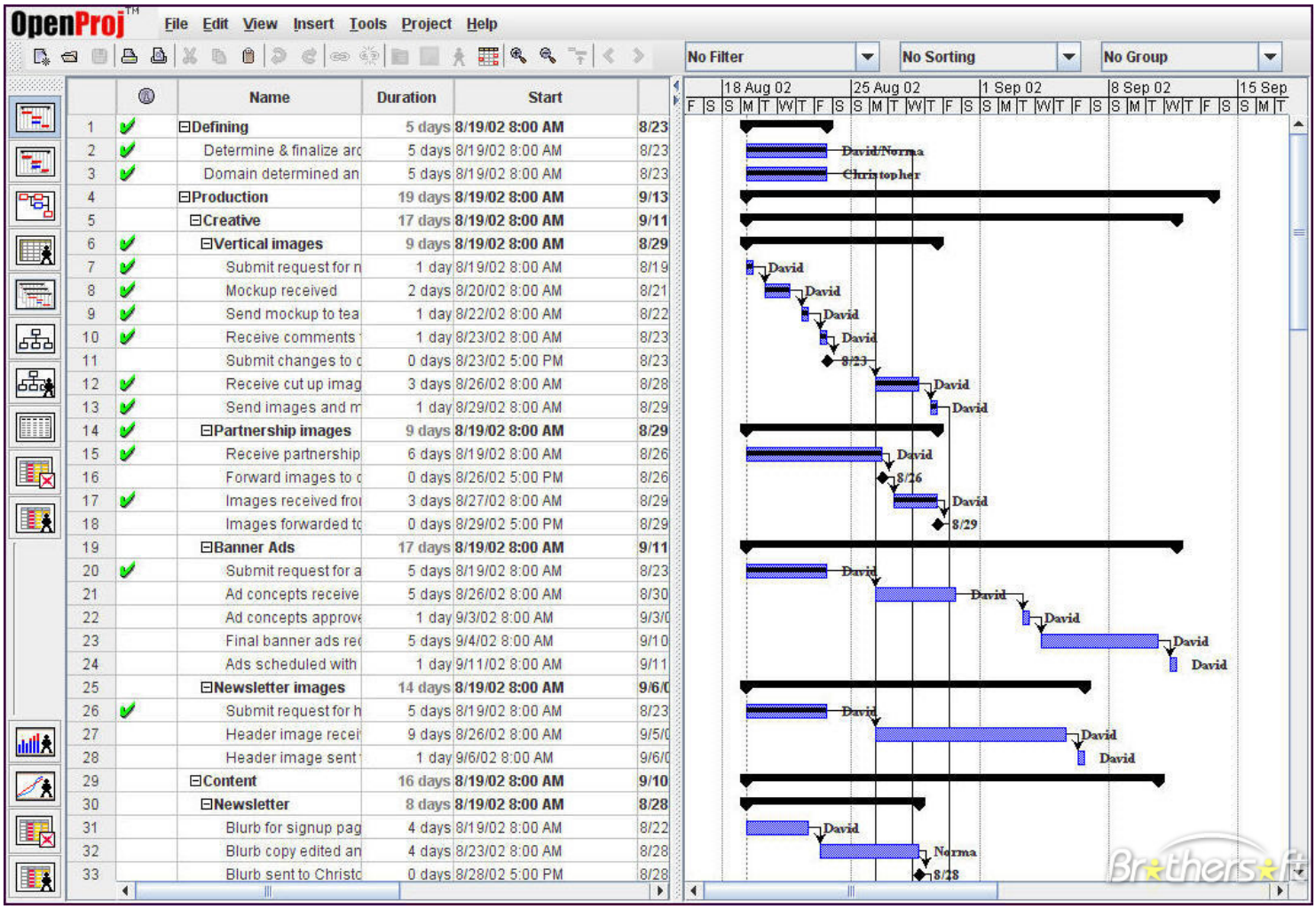
Aplicación para analizar protocolos de red Trabaja en modo promiscuo Puede analizar todo el tráfico que pasa en una red.



Herramientas para la gestión de proyectos

OpenProj

OpenProj fue la herramienta elegida para desarrollar la etapa tres. OpenProj es un software de administración de proyectos desarrollado en Java, lo que permite ejecutarlo en diferentes sistemas operativos, esto fue esencial para nosotros ya que trabajamos con sistema operativo Windows y Linux.



Alguna de las funcionalidades que ofrece la herramienta son:

- Costos de valor acumulado.
- Diagrama de Gantt.
- Gráfico PERT.
- Estructura de descomposición del recurso gráfico.
- Informes de uso de tareas.
- Diagrama de Estructura de descomposición del trabajo.

La herramienta presenta algunos problemas:

- Al asignar los recursos y cambiar la duración, el programa dejaba huecos entre las tareas. Se solucionó reiniciando la aplicación.
- Limitaciones respecto a la exportación de los datos como histogramas y curvas sin ejes, no permite exportación a pdf.
- El diagrama de red presentado puede confundir y no permite ordenar las tareas.
- Corrompe los archivos cuando se trabaja con demasiadas tareas.
- No se encontró forma de armar la distribución de costos considerando la regla 30/70 mensual.

Como ventajas frente a otras opciones como Ms Project tenemos:

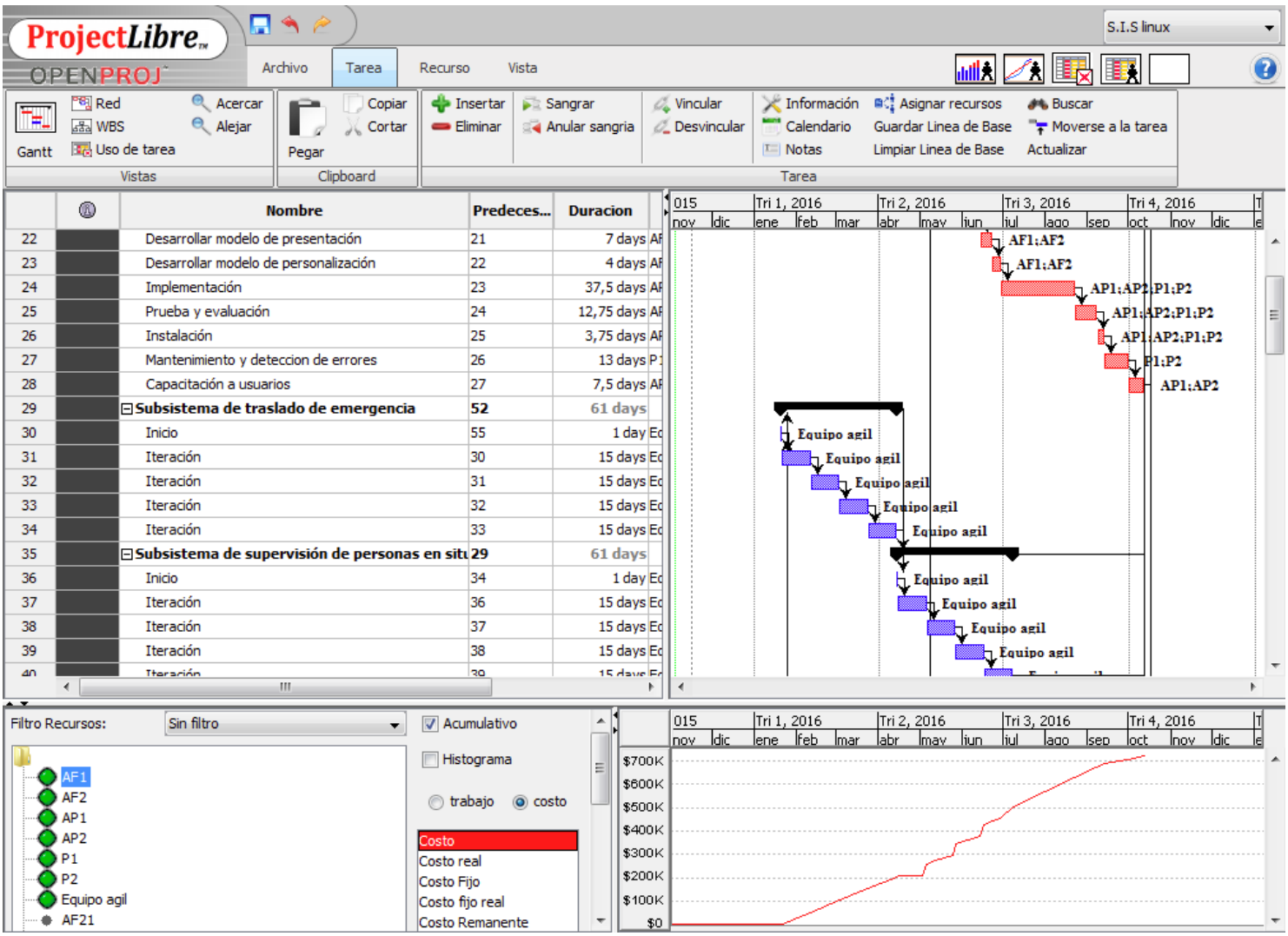
- Libre: OpenProj es un proyecto de software libre de gestión de proyectos.
- Adaptabilidad: OpenProj puede abrir archivos de Microsoft Project y puede guardar archivos en formato propio como en xml.
- Ligero: Si se compara OpenProj vs Microsoft Project, OpenProj requiere menos recursos para instalar.

- Independiente del Sistema operativo: OpenProj se ejecuta en la plataforma Java por lo que puede ejecutarse en diferentes sistemas operativos.

ProjectLibre

OpenProj fue desarrollado por Projity como alternativa a Microsoft Project. A finales del año 2008 fue adquirida por Serena Software y fueron ellos quienes se hicieron cargo del proyecto. Un tiempo después Serena Software abandonó OpenProj.

Tras lo anterior los dueños originales retomaron el proyecto y crearon ProjectLibre.



Decidimos usar ProjectLibre cuando los archivos sobre los que trabajábamos, se corrompieron. No pudimos encontrar una solución dado que OpenProj fue abandonado.

Las funcionalidades que ofrece son las mismas que OpenProj pero podemos destacar algunas que no estaban incorporadas en el programa anterior:

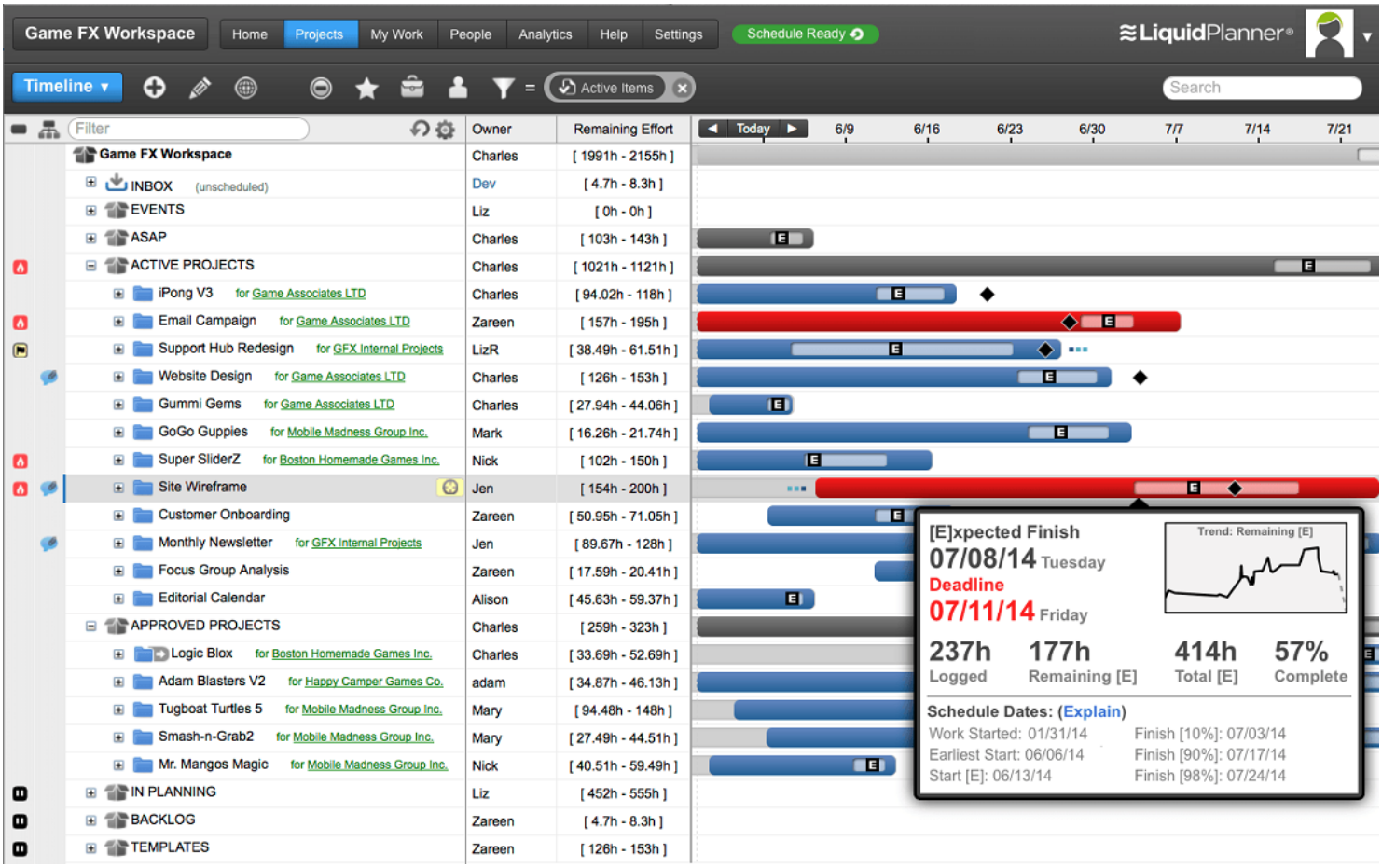
- Exportar diagramas a .pdf
- Exportar diagramas a .png
- Abrir archivos Ms Project 2003, 2007 y 2010

Al día de hoy ProjectLibre es la herramienta elegida para la administración de proyectos y ha sido descargada 1750000 veces en 210 países diferentes. Además la empresa Serena Software, la cual abandonó OpenProj, recomienda usar ProjectLibre.

LiquidPlanner

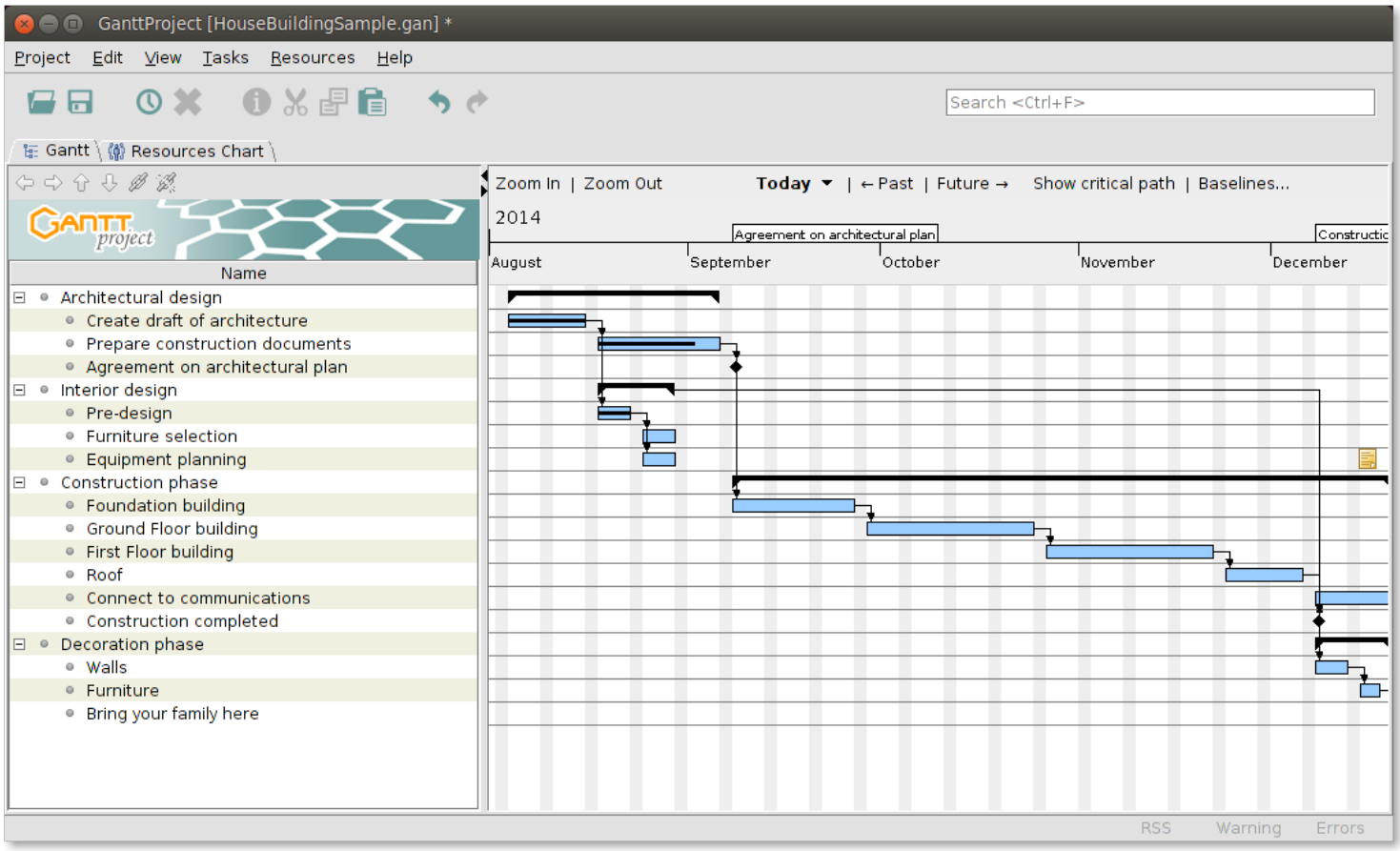
Es una herramientas de gestión de proyectos online desarrollada en el framework Ruby On Rails. Fue fundada en 2006 y su primera beta se dio a conocer en 2008.

LiquidPlanner estima la duración del proyecto basado en las prioridades y la duración de las tareas del mismo. Posee un panel que permite conocer las tareas asignadas a cada uno de los miembros del equipo y cuando estas deben terminarse. Es accesible desde cualquier navegador y dispositivo móvil, todos los participantes del proyecto tienen acceso a documentos, comentario y reportes, permitiendo un trabajo colaborativo a través de Internet.



Los precios de LiquidPlanner son de US$29 por mes el standard, US$39 el profesional y US$49 para empresas.

GanttProject



Es un programa gratuito para la administración de proyectos que funciona en Windows, Linux y Mac. Las características destacadas de este programa son:

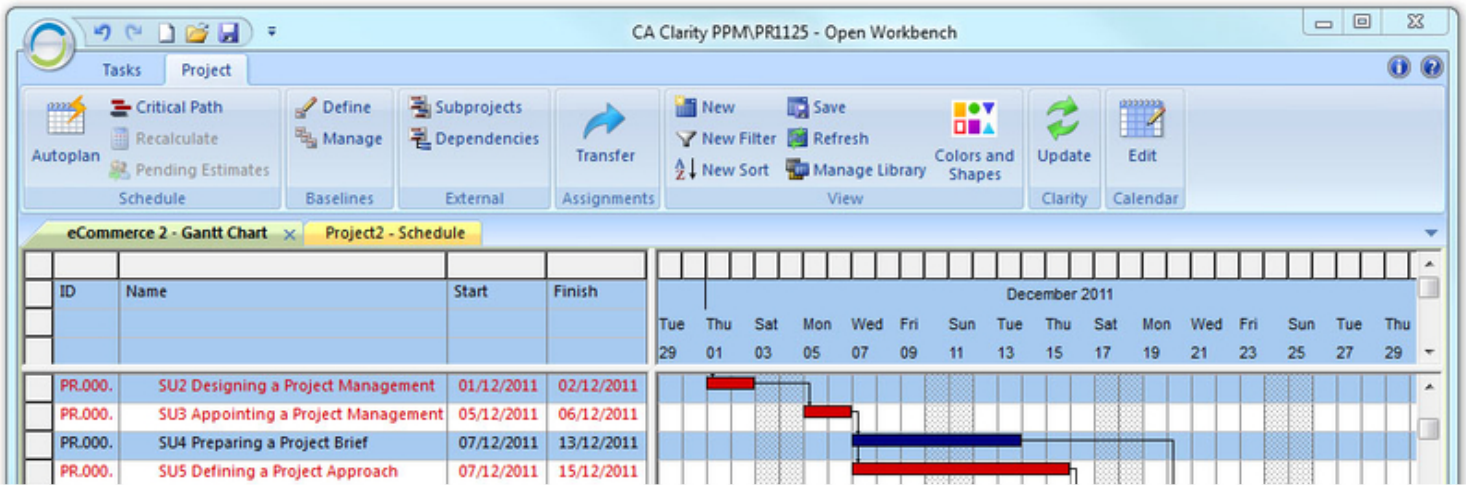
- Permite realizar gráficas de Gantt.
- Permite asignar recursos y monitorear los recursos asignados a tareas.
- Permite exportar archivos pdf, png/jpeg, csv.
- Permite exportar/importar a Microsoft Project.
- Permite trabajar en forma colaborativa en el mismo proyecto.

Open Workbench

Es una aplicación de software libre, dirigida al sistema operativo Windows, y que ofrece una robusta funcionalidad para la gestión de proyectos en la empresa, permitiendo el diseño de programas, calendarización, administración de tiempos, entre otros.

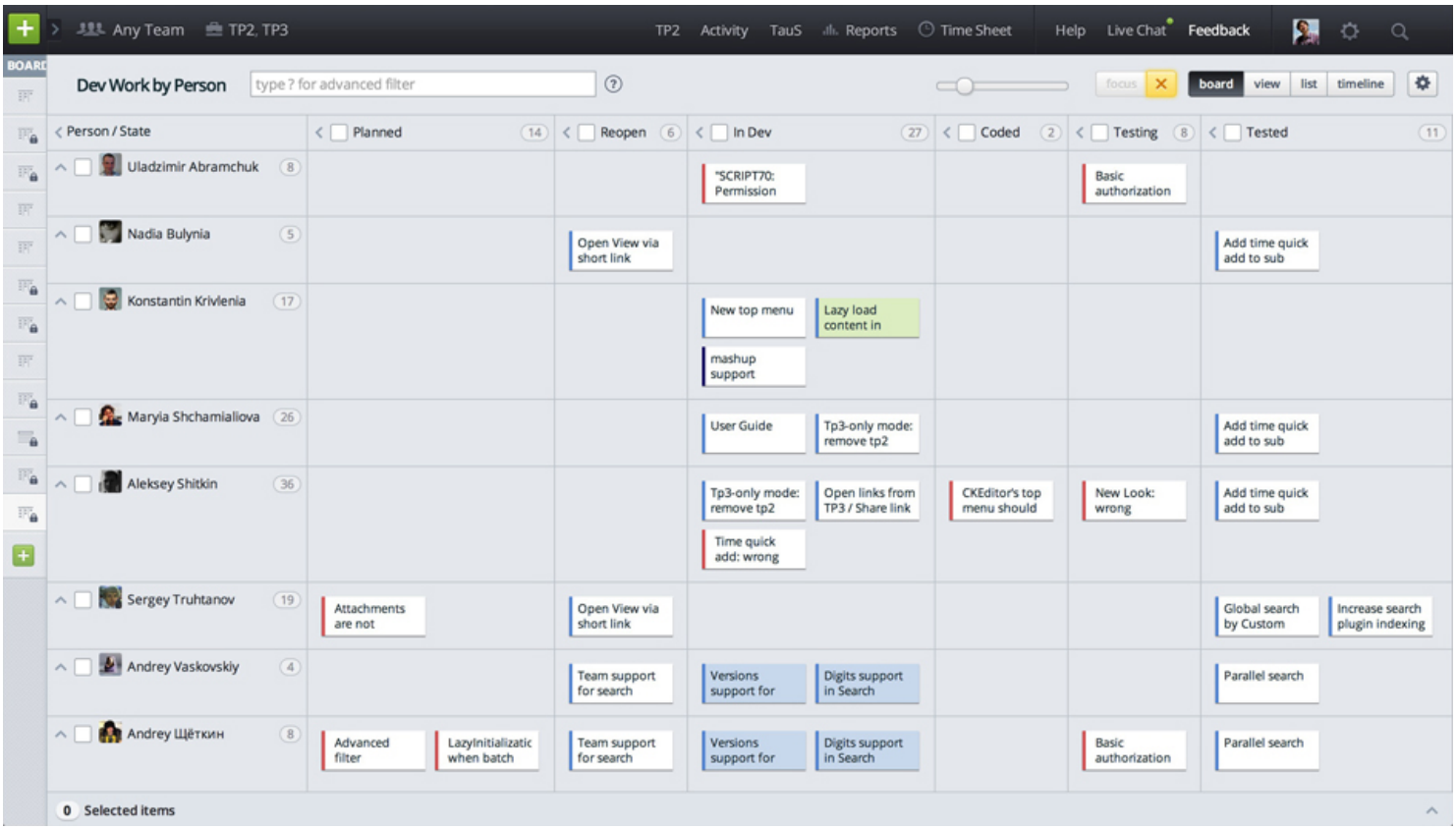
La aplicación es de libre distribución, y ha sido desarrollada para empresas que inician su camino, y que desean hacer uso apropiado de sus recursos. La aplicación es muy similar a la incluida en el paquete comercial de Microsoft Office (Microsoft Project).

Open Workbench, permite en un sinfín de tareas, tales como diseño de gráficas de Gantt, asignación de tareas, relaciones, tiempos de actividad, entre otros. Como aplicación libre, cumple todo los requisitos para ser efectiva.



TargetProcess

Targetprocess es un software de administracion de proyectos que apunta a las metodologias agiles como Scrum y Kanban. Este software es accesible mediante navegadores web y aplicaciones mobiles para dispositivos iPhone, iPad y Android. No es de uso libre, sin embargo es gratis hasta para cinco usuarios. Targetprocess soporta varios procesos de desarrollo de software, incluyendo Scrum, Kanban y Extreme Programing. Ademas se puede integrar con Git, Subversion, Perforce, TFS, JIRA, Bugzilla, NUnit, JUnit, Selenium, Visual Studio y Eclipse.



Redmine

Redmine es una herramienta para la gestión de proyectos que incluye un sistema de seguimiento de incidentes con seguimiento de errores. Otras herramientas que incluye son calendario de actividades, diagramas de Gantt para la representación visual de la línea del tiempo de los proyectos, wiki, foro, visor del repositorio de control de versiones, RSS, control de flujo de trabajo basado en roles, integración con correo electrónico, etcétera.

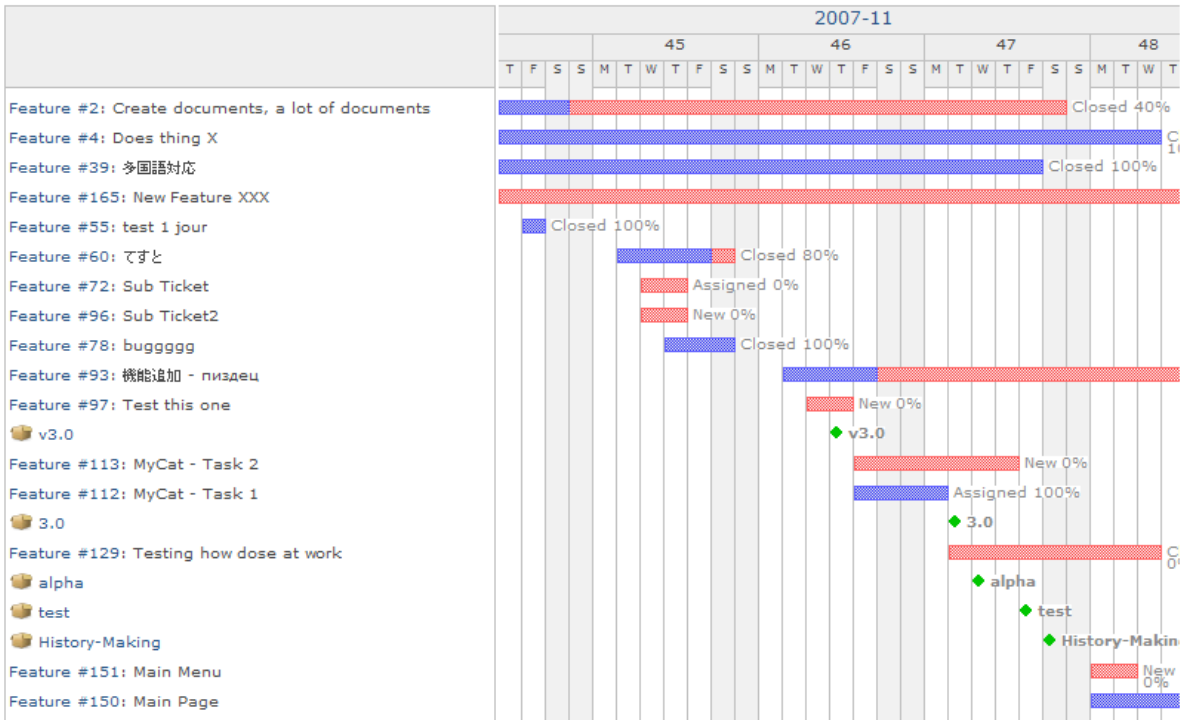
Está escrito usando el framework Ruby on Rails. Es software libre y de código abierto, disponible bajo la Licencia Pública General de GNU v2.

Caracteristicas:

- Soporta múltiples proyectos.
- Roles flexibles basados en control de acceso.
- Sistema de seguimiento de errores flexible.
- Diagramas de Gantt y calendario.
- Administración de noticias, documentos y archivos.
- Fuentes web y notificaciones por correo electrónico.
- Integración SCM (Subversion, CVS, Git, Mercurial, Bazaar y Darcs).
- Soporta diferentes bases de datos (MySQL, PostgreSQL y SQLite).
- Plugins.

Gantt

1 months from November 2007 Submit



Gantt

- [ ] Bug
- [x] Feature
- [ ] Support
- [ ] Marketing

Apply