Capítulo 9

Conclusiones y líneas de avance

9.1. Conclusiones

En esta sección de la memoria de este Proyecto de Fin de Carrera exponemos las conclusiones finales del trabajo desarrollado.

Las principales conclusiones son:

- Este proyecto ofrece al «Estado del arte» actual un sistema que integra módulos y funcionalidades de distinta naturaleza, estableciendo una relación entre los mismos.
- La permisividad y flexibilidad del sistema al adaptarse a los cambios que manualmente pueda realizar el usuario en los ficheros de configuración (mediante editores de texto u otras utilidades gráficas). Se ha tenido en especial consideración que los distintos módulos respeten el formato y contenidos originales de los ficheros de configuración, haciendo que sean adaptables a los cambios provocados en los mismos.
- La ventaja en la utilización de un sistema operativo estándar y abierto.
- La enorme potencia y versatilidad del uso de librerías de código abiertas de PHP, además de la conveniencia a la hora de la reducción de costes en el desarrollo de las interfaces.
- Al basarnos en una estructura modular y de tres capas, se hace posible con facilidad la integración de nuevos módulos en el sistema así como la sustitución de los ya existentes por otros.

Así mismo, el desarrollo de este Proyecto nos ha permitido ampliar nuestros conocimientos sobre distintas materias y campos. Algunas de las aportaciones personales con las que este Proyecto nos ha enriquecido son:

- Conocimientos de herramientas (*software*) sobre seguridad y monitorización.

- Conocimientos (profundos) del lenguaje de programación PHP.
- Utilización de PHP como lenguaje orientado a objetos.
- Profundización en la estructura interna de los sistemas GNU/Linux.
- Desarrollo de paquetes Debian.
- Personalización y creación de *kernels* para GNU/Linux.

9.2. Futuras líneas de avance

Este PFC admite gran cantidad de adiciones e innovaciones en un futuro inmediato. La arquitectura modular (tanto del sistema operativo escogido como de las interfaces desarrolladas) hacen simple la incorporación de nuevas funcionalidades al sistema desarrollado.

Algunas de las posibilidades de mejora y de continuación para este Proyecto son:

1. Extender las interfaces de configuración a más parámetros además que los seleccionados, como las rutas de almacenamiento interno de los archivos, opciones adicionales en los recolectores, etc.

2. Separar por completo el código PHP del HTML, lo que implicaría la separación total de la presentación de la interfaz de su implementación. Esto se debe a que durante el desarrollo de los módulos se ha hecho uso en algún momento de pequelas cadenas de código HTML incrustado dentro del PHP.

3. Realizar mejoras en el código de los módulos desarrollados que mejoren el comportamiento de los mismos y permitan, en medida de lo posible, la «autorecuperación» de situaciones erróneas. Algunos ejemplos de esto son: permitir que *flow-capture* no se configure en interfaces inexsistentes, hacer que *FlowScan* se detenga en en caso de iniciarse el sistema y estar el servicio configurado en el arranque, etc.

4. Ampliar los aspectos del tratamiento de la información y su procesado de cada a un usuario humano, permitiendo más opciones para su estudio (especialmente para el caso de *syslog-ng*).

5. Integrar la ejecución de operaciones remotas de control en la interfaz de usuario, de manera que se facilite pasar de realizar la monitorización estadística a la retransmisión de tráfico en el sistema remoto mediante la activación del módulo *ROUTE*.

6. Desarrollar los módulos correspondientes a las demás utilidades y tecnologías estudiadas en este Proyecto, como *syslog-ng* o *flow-export* y sus complementos *flow-fanout* o *flow-send*, para permitir al usuario su configuración y manipulación.

7. Integrar finalmente la interfaz y las utilidades seleccionadas dentro de la distribución en CD autoarrancable «Anubix», desarrollada en el PFC *Anubix: Servidor de seguridad perimetral*. Si bien el diseño y la realización completas de este Proyecto se han dirigido a la compatibilidad absoluta con dicho PFC, no se ha realizado la integración dentro de la distribución «Anubix» por la extensión y complejidad que alcanzaría este Proyecto.