Conclusiones

El objetivo de este trabajo de tesis fue implementar un detector de malware con software libre empleando el protocolo Netflow.

Para ello:

- Se realizó una investigación profunda acerca del protocolo Netflow para poder entender el funcionamiento de esta técnica enfocada en el monitoreo de red mediante la recolección de flujos directamente del switch o router que soporten dicha técnica, esta investigación fue descrita en la sección 1.3.
- Se realizó una investigación detallada acerca de alguna alternativa de uso libre que fuera capaz de sustituir, en buena medida, al software comercial Netflow que esta implementado en la institución, esta investigación fue descrita en el capítulo 2.
- Se implementó el software "Listry-AIGC" en la institución. El funcionamiento de este software fue descrito en el capítulo 3 y, en los anexos B y C.
- Se realizó una investigación acerca de las diversas técnicas utilizadas por el malware para infectar a sus víctimas en capas inferiores del modelo OSI. Obteniendo como resultado los cuatro comportamientos habitúales utilizados por el malware y que fueron descritos en la sección 4.3.
- Aprovechando la posibilidad de implementar pluglins en el software Nfsen, se creó el plugin 'escaneo', enfocado en la detección de malware de acuerdo con los comportamientos descritos en la sección 4.3. El funcionamiento de este plugin se describió en la sección 4.4.
- Se realizaron pruebas para demostrar el correcto funcionamiento del software "Listry-AIGC" enfocado en el monitoreo de red y en la detección de malware mediante el plugin escaneo. Las pruebas realizadas se describieron en la sección 5.2.1 y 5.2.2 respectivamente.

El software Nfsen implementado demostró ser la mejor alternativa de uso libre capaz de sustituir a software propietario que utiliza el protocolo Netflow. Debido a que brinda estadísticas muy detalladas de lo que está pasando en la red, y mediante filtros se puede acotar la información obtenida en estadísticas muy detalladas, además de permitir la creación de vistas específicas y alertas enfocadas en el monitoreo de red.

Además el software Nfsen ofrece grandes beneficios al poder ser enfocado, mediante plugins, a realizar alguna acción complementaria al monitoreo de red. En este caso se aprovechó esta ventaja para crear un plugin enfocado en la detección de malware. El plugin creado es capaz de detectar de forma individual o en conjunto las cuatro técnicas de detección de malware descritas en la sección 4.3. Con la principal ventaja de no requerir intervención alguna del usuario final, debido a que el plugin notifica automáticamente mediante él envió de un email la(s) anomalía(s) detectada(s) y guarda un registro de esta(s) anomalía(s) en una base de datos creada en MySQL para futuros análisis. Naciendo con estas herramientas añadidas el software "Listry-AIGC"

Para verificar el correcto funcionamiento del software "Listry-AIGC" enfocado en el monitoreo de red se realizaron las siguientes pruebas:

- El software "Listry-AIGC" se mantuvo en pruebas por 6 meses. En este periodo de tiempo, el software Nfsen recolectaba información de un router asociado a un edificio. Las estadísticas obtenidas eran en promedio 250 flujos capturados cada 5 minutos.
- Se crearon diversos profiles y alertas enfocados en el monitoreo de red y descritos en la sección 5.2.1.
- Se añadieron graficas que permiten visualizar las estadísticas obtenidas cada 3 horas. Además de acceder a la interfaz web mediante HTTPS (Hypertext Transferer Protocol Secure).

El plugin escaneo fue desarrollado como un módulo backend que se actualiza cada que el software Nfsen recibe un nuevo archivo Nfcapd y un módulo frontend que muestra los resultados obtenidos de la ejecución del módulo backend

Para verificar el correcto funcionamiento del software Nfsen enfocado en la detección de malware presente en la red central de la institución, se realizaron las siguientes pruebas:

- Se crearon cuatro escenarios distintos. Cada uno de estos escenarios simulaba el comportamiento de un malware mediante alguna de las técnicas descritas en la sección 4.3.
- Se observó la respuesta devuelta por el plugin escaneo ante cada uno de estos escenarios sometidos, descrita en la sección 5.2.2.
- Se verifico el correcto envió de los correos generados por el plugin escaneo al administrador de red.
- Se verifico el correcto almacenamiento de anomalías detectadas en las tablas creadas en MySQL

Con el desarrollo exitoso de este proyecto de tesis se logró tener una nueva herramienta de uso libre, que es capaz de sustituir en buena medida a software propietario que utiliza el protocolo Netflow. Además de desarrollar una técnica innovadora en la detección de malware que opera en capas inferiores del modelo OSI mediante el monitoreo de red.

Por todo lo descrito se cumplió con el objetivo establecido, ya que se encontró una alternativa de uso libre capaz de sustituir al software comercial Netflow implementado en la institución. Además de implementar un detector basado en la detección de malware por medio del monitoreo de red mediante patrones típicos de comportamiento en capas inferiores del modelo OSI.