Introducción

Objetivo.
Implementar un detector de malware con software libre empleando el protocolo Netflow.

Descripción del problema.
Generalmente las herramientas de seguridad como los antivirus, firewalls, *IDS (Intrusion Detection System)* e *IPS (Intrusion Prevention System)*, operan en capas superiores del modelo OSI, y muy pocas de ellas operan en capas inferiores. Esto representa un problema cuando tratamos de detectar la actividad de un malware o código malicioso (Proviene del término en inglés "**mal**icious soft**ware":** Todo aquel software que perjudica a una computadora) que sea capaz de infectar a sistemas de cómputo mediante diversos ataques a capas inferiores del modelo OSI, como puede ser: *IP flooding*, *IP spoofing*, *Ping of Death*, *Arp spoofing*, entre otros, o explotando vulnerabilidades presentes en el protocolo TCP/IP.

A pesar de que las herramientas de seguridad han mejorado enormemente sus métodos de detección de malware, muy pocas son capaces de detectar algún malware de "día cero" (nuevo malware creado y que no se tiene ningún registro acerca de él), dado que para este tipo de malware no se tiene conocimiento sobre su comportamiento y no se tiene referencia alguna de él.

Una vez que el malware ha logrado infectar a un sistema de cómputo, buscará propagarse lo más rápido posible dentro de la red, comenzando con un escaneo de puertos o un escaneo de IP's en búsqueda de más "víctimas". Dependiendo del tipo de malware, éste podría enviar información confidencial hacia IP's desconocidas, o realizar un ataque de negación de servicio en conjunto con otras sistemas de cómputo infectados con el objetivo de saturar un servidor especifico, entre otras acciones.

Por todo lo mencionado acerca del malware y la capacidad de propagación y *polimorfismo* que presenta, es necesario investigar técnicas innovadoras que sean capaces de detectar malware. Una solución viable es la detección de malware mediante el monitoreo de red.

El monitoreo de red es una actividad que comúnmente desarrollan los administradores de redes de las empresas. Debido a que permite observar el comportamiento de la red en tiempo real. Específicamente:

- Se observa la cantidad de ancho de banda consumido.
- El porcentaje de utilización de protocolos *TCP, UDP*, *ICMP* entre otros.
- Utilización de servicios como HTTP, SSH, FTP, SNMP, SMTP, entre otros.
- La actividad presente en las redes de usuarios y redes de servidores.
- Comportamiento anormal de la red.

La siguiente tabla muestra los métodos más comunes utilizados en el monitoreo de red.

Tabla I.1 Diversas técnicas utilizadas para monitorear la red.

Método	Breve Descripción
Activar la tarjeta de red en modo promiscuo	La tarjeta de red captura todo el tráfico que circula a través de ella.
SNMP	Protocolo de la capa de aplicación del modelo OSI que facilita el intercambio de información de administración entre dispositivos de red
Netflow	Captura el tráfico directamente de un router o switch que soporte esta tecnología.

Sin embargo se tiene el inconveniente de que no existe un estándar enfocado en el monitoreo de red y que sea aplicable a todas las herramientas enfocadas en esta tecnología. El tener un estándar facilitaría la comunicación entre las diversas técnicas utilizadas para monitorear redes.

Para tratar de resolver este problema CISCO ha desarrollado un protocolo llamado Netflow enfocado en el monitoreo de red.

Como principales características de Netflow son:

- ✓ Estandarizado RFC 3954 (Cisco Systems Netflow Services Export Version 9).
- ✓ Actualmente tiene 10 versiones (Netflow V1-V9 y V10 IPFIX).
- ✓ Obtiene los datos directamente del router o switch, a diferencia de otras tecnologías de monitoreo.
- ✓ Permite contabilizar el ancho de banda consumido.
- ✓ Provee una visión detallada acerca del comportamiento de la red.
- ✓ Se logra tener un alcance del 100%, debido a que se puede activar en cada router o switch presente.

Sin embargo, la principal desventaja del protocolo Netflow es que el software propietario o comercial tiene un gran costo en ambientes de producción. Una alternativa a este inconveniente es utilizar software libre u open source (software distribuido y desarrollado libremente) que soporte completamente dicho protocolo.

Solución.
El problema expuesto en la sección “descripción del problema”, se puede resolver de las siguientes formas:

1. Mejorando el proceso de hardening en la institución. (Diversas herramientas de seguridad que trabajan en conjunto para proteger los bienes o activos).
2. Por medio de la compra de un software propietario o comercial Netflow enfocado en la detección de malware. Ejemplo: Arbok Netflow.
3. Por medio de la investigación sobre una alternativa software libre que soporte el protocolo Netflow y sobre ella implementar un detector de malware.

De las cuales las propuestas 1 y 3 son más viables, debido a que se investigará sobre alguna alternativa software libre basada en el protocolo Netflow y sobre ella se implementará un detector de malware, mientras que el aplicar la propuesta 2 implica pagar por la licencia y el uso del nuevo software.

La siguiente tabla muestra las ventajas y desventajas del proyecto propuesto.

Tabla I.2 Ventajas y desventajas del proyecto de tesis

Ventajas	Desventajas
✓ Propuesta de una solución innovadora en la detección de malware. ✓ Nueva herramienta enfocada en el monitoreo de red y en la detección de malware. ✓ Utilización del protocolo Netflow ✓ Utilización de software Libre ✓ Costos mínimos en su utilización. ✓ Posibles modificaciones hacia el nuevo software. ✓ Posible detección de malware de "día cero". ✓ La nueva herramienta de seguridad desarrollada será implementada en una institución importante en nuestro país.	× Escasas alternativas de software libre que soporten el protocolo Netflow. × Escasa información acerca del comportamiento del malware. × Existe software propietario o comercial muy robusto que soporta el protocolo Netflow. × Solo podrá detectar malware que deje evidencia en la red. × Capacitación a usuarios que no conozcan sistemas operativos Linux.

La nueva herramienta trabajará en conjunto con las demás herramientas de seguridad que se tienen implementadas en la institución, fortaleciendo el esquema de seguridad implementado en la institución.

Justificación

Por todo lo mencionado el presente trabajo tiene como objetivo investigar una alternativa de software libre que soporte el protocolo Netflow e implementar un detector capaz de encontrar malware en la red.

Con el éxito del presente proyecto de tesis, propondré una nueva herramienta de seguridad que cumpla con los siguientes objetivos:

- Implementado con software libre.
- Monitoreo de red basado en el protocolo Netflow.
- Detección de malware basado en patrones de comportamiento anómalo y posible detección de ataques de "día cero".
- Enfocada hacia capas inferiores del modelo OSI.
- Compatibilidad total con otras herramientas de seguridad.

Las restricciones encontradas en este proyecto es la escasa información acerca del comportamiento del malware, además de encontrar muy pocas alternativas de software libre que soporten en protocolo Netflow.

El proyecto de tesis se pretende implementar en una institución, por lo tanto no se podrán mostrar datos referentes a la institución donde será implementado, por cuestiones de integridad y confidencialidad de la información presente en la institución.

Método

Para la resolución del proyecto propuesto de tesis se aplicó la siguiente metodología:

1. Investigación acerca del funcionamiento del protocolo Netflow.
2. Investigación acerca de alternativas software libre que trabajen sobre el protocolo Netflow y en ellas se pueda implementar un detector de malware.
3. Elección de la mejor alternativa, con base en un análisis detallado realizado y puesta en marcha.
4. Investigación acerca del comportamiento del malware.
5. Creación del detector de malware.
6. Pruebas.
7. Puesta en marcha de la nueva herramienta sobre un ambiente de producción en una institución de alta importancia en el país.
8. Creación de toda la documentación requerida.

Estructura del proyecto de tesis.

El proyecto de tesis se ha dividido en cinco capítulos y cuatro anexos de la siguiente forma:

- El capítulo uno tiene el objetivo de proporcionar toda la información teórica requerida en la realización del proyecto tesis.
- El capítulo dos tiene el objetivo de explicar todo el proceso realizado en la elección del software libre que se implementó en la institución. Además de mostrar una comparación entre el software libre elegido con el software propietario utilizado en la institución.
- El capítulo tres tiene el objetivo de explicar la implementación realizada del protocolo Netflow en la institución y el funcionamiento del software elegido en el capítulo dos.
- El capítulo cuatro tiene el objetivo de explicar las diversas técnicas utilizadas para la detección del malware. Además del desarrollo y funcionamiento del plugin creado.
- El capítulo cinco tiene el objetivo de mostrar el correcto funcionamiento del software “Listry-AIGC”, software que incluye a la alternativa elegida en el capítulo dos, además de diversas funcionalidades añadidas a él; enfocado sobre el monitoreo de red y la detección de malware mediante el plugin explicado en el capítulo cuatro. Además de mostrar las conclusiones obtenidas en la realización del proyecto de tesis.
- El anexo A tiene un glosario creado.
- El anexo B explica la instalación del software “Listry-AIGC”.
- El anexo C se ha creado como una guía de usuario del software “Listry-AIGC”.
- El anexo D muestra el código del plugin creado y explicado en el capítulo cuatro.