

**“DESARROLLO DE UN SISTEMA INMUNE ARTIFICIAL PARA LA SEGURIDAD
EN REDES”**

Juan David Betancur Vallejo

**Universidad Tecnológica De Pereira
Facultad Ingenierías: Eléctrica, Electrónica, Física y Ciencias Computación
Programa Ingeniería de Sistemas y Computación
Pereira
2007**

**"DESARROLLO DE UN SISTEMA INMUNE ARTIFICIAL PARA LA SEGURIDAD
EN REDES"**

Juan David Betancur Vallejo

Desarrollo de Software

**Director
Néstor Darío Duque Méndez, Ph.D.(c)
Universidad Nacional de Colombia
Sede Manizales**

**Universidad Tecnológica De Pereira
Facultad Ingenierías: Eléctrica, Electrónica, Física y Ciencias Computación
Programa Ingeniería de Sistemas y Computación
Pereira
2007**

Nota de Aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

DEDICATORIA

Algunas cosas

JUAN DAVID BETANCUR VALLEJO

AGRADECIMIENTOS

TABLA DE CONTENIDO

1 INICIATIVA DEL PROYECTO.....	25
1.1 Título del Proyecto.....	25
1.2 Definición del Problema.....	25
1.3 Justificación	26
1.4 Objetivos	27
1.4.1 Objetivo General	27
1.4.2 Objetivos Específicos	27
1.5 Diseño Metodológico	27
1.5.1 Definición de la Hipótesis.....	27
1.5.2 Indicador	28
1.5.3 Universo	28
1.6 Personas que Participan en el Proyecto.....	28
1.6.1 Director.....	28
1.6.2 Ejecutor	28
1.6.3 Asesores	28
2 MARCO TEÓRICO.....	29
2.1 Estado del Arte de los Sistemas Inmunes Artificiales.....	29
2.2 Principios de Inteligencia Artificial Aplicados.....	34
3 SELECCIÓN DE CRITERIOS PARA LA EVALUACIÓN DE PAQUETES	37
3.1 Números de Puertos	37
3.1.1 Puertos Bien Conocidos.....	38
3.1.2 Número de Puertos en la Cabecera TCP.	38
3.2 Direcciones IP.....	39
3.2.1 Direcciones Privadas	39
3.2.2 Direcciones Públicas.....	40
3.2.3 Direcciones en Listas Negras	40
3.2.4 Direcciones origen y destino	41
3.3 Banderas de la Cabecera TCP.....	41
3.3.1 SYN	42
3.3.2 FIN	42
3.3.3 Combinaciones incorrectas de SYN y FIN	42
3.4 Conclusiones de la Selección.....	43
4 MODELAMIENTO DE LA HERRAMIENTA.....	45
4.1 Etapa de Análisis	45
4.1.1 Diagrama de Casos de Uso	45
4.1.2 Especificación de Casos de Uso.....	46
4.1.3 Diagramas de Secuencia	51
4.1.4 Diagramas de Colaboración.....	54
4.1.5 Diagrama de Estados.....	57
4.1.6 Modelo de Clases	58
4.2 Etapa de Diseño Arquitectónico del Sistema.....	59

4.3 Diseño de Objetos	61
4.3.1 Herramientas de Desarrollo	61
4.3.2 Ingeniería Inversa de las Herramientas	64
4.3.3 Interfaces Hombre-Máquina.....	65
4.3.4 Modelo de Componentes	69
4.3.5 Modelo de Distribución.....	70
5 DIFICULTADES ENCONTRADAS	71
6 APORTES	73
7 CONCLUSIONES.....	75
8 BIBLIOGRAFÍA	77
ANEXO A. CÓDIGO FUENTE DOCUMENTADO	79
ANEXO B. MANUAL DE USUARIO	81
ANEXO C. MANUAL DE PRUEBAS	85

LISTA DE FIGURAS

Gráfica 1 Cabecera TCP	43
Gráfica 2 ¿Dónde se Encuentran las Banderas?	43
Gráfica 3 Esquema de las Banderas de una Cabecera TCP	44
Gráfica 4 Casos de Uso	45
Gráfica 5 Caso de Uso Actualizar Escenario: Actualización en Línea Exitosa	51
Gráfica 6 Caso de Uso Actualizar Escenario: Actualización Local Exitosa	51
Gráfica 7 Caso de Uso Configurar Escenario: Configuración Exitosa	52
Gráfica 8 Caso de Uso Revisar Bitácoras Escenario: Consulta Exitosa	53
Gráfica 9 Caso de Uso Analizar Escenario: Paquete Malicioso	53
Gráfica 10 Caso de Uso Actualizar, Escenario Actualización Local	54
Gráfica 11 Caso de Uso Actualizar, Escenario Actualización en Línea	54
Gráfica 12 Caso de Uso Analizar	55
Gráfica 13 Caso de Uso Bitácoras	55
Gráfica 14 Caso de Uso Configurar	56
Gráfica 15 Diagrama de Transición de Estados Caso de Uso Analizar	57
Gráfica 16 Diagrama de Clases	58
Gráfica 17 Diagrama de Subsistemas	60
Gráfica 18 Secuencia de Ventanas desde la Ventana Principal	61
Gráfica 19 Diagrama de Clases wxPython	64
Gráfica 20 Ventana Principal	65
Gráfica 21 Opciones de la Ventana Principal	66
Gráfica 22 Selección de Interfaz	67
Gráfica 23 Configuración General	67
Gráfica 24 Listado de Bitácoras	67
Gráfica 25 Detalles de una Bitácora	68
Gráfica 26 Diagrama de Componentes del Sistema	69
Gráfica 27 Ejemplo de Distribución para la Ubicación de la Herramienta	70

LISTA DE TABLAS

Tabla 1 Caso de Uso Actualizar	46
Tabla 2 Caso de Uso Configurar	47
Tabla 3 Caso de Uso Revisar Bitácoras	48
Tabla 4 Caso de Uso Analizador	49
Tabla 5 Caso de Uso Informar	49
Tabla 6 Caso de Uso Crear Bitácora	50

GLOSARIO

En el glosario que se presenta a continuación se describen términos que se consideran importantes para la comprensión de los temas que se tratarán en el documento, algunas definiciones son tomadas de Wikipedia (<http://es.wikipedia.org>).

ANTÍGENO: Es una molécula (generalmente una proteína o un polisacárido) de superficie celular, que puede inducir la formación de anticuerpos. Hay muchos tipos de moléculas diferentes que pueden actuar de antígenos, como las proteínas, los polisacáridos y, más raramente, otras moléculas como los ácidos nucleicos.

CÉLULAS B (LINFOCITOS B): Linfocitos B de los cuales depende la inmunidad mediada por anticuerpos, con actividad específica de fijación de antígenos. Las células B dan origen a las células plasmáticas que producen anticuerpos.

CÉLULAS T (LINFOCITOS T): Son los responsables de la respuesta inmune realizada por células, así como de funciones de cooperación para que se desarrollen todas las formas de respuestas inmunes, incluida la respuesta de anticuerpos por los linfocitos B

CIDR (CLASSLESS INTERDOMAIN ROUTING): Enrutamiento Inter-dominios sin clases. Se introdujo en 1993 y representa la última mejora en el modo como se interpretan las direcciones IP. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas. De esta manera permitió:

- Un uso más eficiente de las cada vez más escasas direcciones IPv4.
- Un mayor uso de la jerarquía de direcciones, disminuyendo la sobrecarga de los enrutadores principales de Internet para realizar el enrutamiento.

DNS (DOMAIN NAME SYSTEM): Sistema de Nombres de Dominio, es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

DoS (Denial of Service): Denegación de Servicios, es un ataque a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

FTP (FILE TRANSFER PROTOCOL): Protocolo de Transferencia de Archivos. Se usan programas para FTP como son CuteFTP o LeapFTP para Windows, por ejemplo, que permiten la conexión entre dos computadores, usando por lo general el puerto 21 para conectarse (aunque se pueden usar otros puertos). Por medio del Protocolo de transferencia de archivos se pueden actualizar y descargar archivos entre el cliente y el host.

HTTP (HYPERTEXT TRANSPORT PROTOCOL): es el protocolo de la Web (WWW), usado en cada transacción. Las letras significan Hyper Text Transfer Protocol, es decir, protocolo de transferencia de hipertexto. El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares. HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Al finalizar la transacción todos los datos se pierden.

IANA (Internet Assigned Numbers Authority): Es la autoridad internacional encargada de preservar la coordinación central de funciones globales de Internet para el bienestar del público.

IDS (Intusion Detection System): Un sistema para la detección de intrusos es una herramienta de software o hardware que se sitúa en un punto específico de una red para analizar el tráfico que pasa por la misma, detectando accesos no autorizados, mediante el análisis de los paquetes capturados.

ISP (INTERNET SERVICE PROVIDER): Un proveedor de servicios de internet es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros.

PATÓGENO: Del griego pathos, enfermedad y genein, engendrar. Es toda aquella entidad biológica capaz de producir enfermedad o daño en la biología de un hospedero (humano, animal, vegetal, etc.) sensiblemente predispuesto.

TCP (Transmission Control Protocol): Protocolo de Control de Transmisión. Es uno de los protocolos fundamentales en Internet. Muchos programas dentro de

una red de computadores pueden usar TCP para crear *conexiones* entre ellos a través de las cuales enviarse datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP soporta muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP y SSH.

TELNET: Es el protocolo estándar de Internet que permite la conexión a una terminal remota.

SPOOFING: En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación, su forma de operar es capturando un paquete y luego manipularlo para cambiar ciertos atributos claves y luego re-insertarlo en la red para que cumpla su misión.

SSH (SECURE SHELL): Es el nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas remotas a través de una red, de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible amenazar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos. Al igual que telnet, sólo permite conexiones tipo terminal de texto, aunque puede redirigir el tráfico de X para poder ejecutar programas gráficos si se tiene un Servidor X en ejecución.

WINS (WINDOWS INTERNET NAMING SERVICE): Es un servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otro ordenador de la red.

RESUMEN

El proyecto que se desarrolla en el presente documento tiene como idea principal construir un sistema inmune artificial para la seguridad en redes, es un aporte para la comunidad mundial ya que hoy en día no existen desarrollos que involucren este tipo de metodologías, por lo menos no enfocado a solucionar estos problemas que afectan tanto a las empresas.

Esta solución podría reducir un poco los costos de implementar la seguridad en la red de una empresa ya que los dispositivos IDS tienen algunos inconvenientes para cierta porción de las empresas como son: costos, tecnología propietaria y futuras actualizaciones. Al ser la solución propuesta adaptable se pueden ofrecer mejoras en los servicios de IDS. Una de las ideas básicas de un Sistema Inmune Artificial es simular los linfocitos que viajan por el torrente sanguíneo buscando virus, bacterias e infecciones entonces el software puede viajar por la red en busca de paquetes extraños, intentos de ataques y demás vulnerabilidades que puedan existir en una red. No estarían en un sitio fijo y funciona de igual forma para ataques tanto internos como externos.

La otra idea básica es centralizada utilizando capas, al igual que el sistema inmune natural, el cual utiliza diferentes niveles de protección, desde la piel hasta las células en la sangre, este es el enfoque que se utilizó para el análisis y desarrollo de la herramienta que se presenta a continuación.

INTRODUCCIÓN

Los sistemas inmunes artificiales son una aproximación a los sistemas inmunes naturales de los vertebrados, los cuales protegen a estos animales, incluyendo al hombre, de los virus, bacterias y demás infecciones que los rodean. Estos sistemas se pueden aplicar en diferentes principios computacionales como: detectores de cambios distribuidos, anti-virus y los conocidos detectores de intrusos o IDS.

Incluso para un solo principio se pueden utilizar diferentes aproximaciones así por ejemplo, para la detección de procesos corruptos se pueden utilizar varios diseños (distribuidos, centralizados, con agentes inteligentes).

En este caso se presenta una herramienta centralizada, por capas, con la cual se pretende detectar intrusos en una red analizando las cabeceras de los paquetes TCP e identificando ciertos patrones comunes, generando un reporte inmediato al administrador y guardando la información necesaria para tratar de rastrear el intruso.

El presente documento contiene la información necesaria para comprender, estudiar y utilizar la herramienta que se desarrolló para la seguridad en redes de datos utilizando un sistema inmune artificial.

1 INICIATIVA DEL PROYECTO

1.1 Título del Proyecto.

“Desarrollo de un Sistema Inmune Artificial para la Seguridad en Redes”

1.2 Definición del Problema

El campo de la seguridad en cómputo es muy extenso y variado, por lo cual existen infinidad de herramientas y metodologías a las que los administradores de redes pueden recurrir para evitar que la información sea accesada por personas no autorizadas.

Una manera de llevar a cabo este control es usando herramientas preventivas, como lo son firewalls, anti-spywares, entre otras; también existen herramientas forenses en caso de que las anteriores no sean suficientes y se llegue a la situación de que alguien entró al sistema y sea necesario recuperar información perdida, analizar los posibles pasos que tomó el intruso y que evidencias dejó para una posible persecución.

Pero existen en realidad pocas herramientas que sean proactivas, que detecten el intruso en el momento, le cierren el paso, suenen las alarmas y aconsejen al administrador qué actualizaciones son necesarias para evitar un ataque de este tipo en el futuro. Entre estas herramientas están IDS (en inglés, sistemas de detección de intrusos), o IPS (en inglés, sistemas de prevención de intrusos), estas herramientas pueden ser: software instalado en un equipo que tenga la empresa o hardware especializado para esta función, estos dispositivos se ubican dentro de una red en sitios específicos para analizar el tráfico de paquetes.

Como ya se mencionó, estas herramientas pueden ser implementadas en software utilizando diferentes paradigmas de acción, uno de ellos es la utilización de algoritmos inmunes artificiales para generar un sistema inmune artificial.

“Un Sistema Inmune Artificial (AIS) es un tipo de algoritmo de optimización inspirado en los principios y procesos del sistema inmune de los vertebrados. Los algoritmos por lo regular aprovechan las características de aprendizaje y memoria de los sistemas inmunes para resolver un problema. Dichos algoritmos están

fundamentados en la inteligencia artificial y estrechamente relacionados con los algoritmos genéticos.”¹

El fin de este proyecto es desarrollar una herramienta que en principio actúe como un analizador de tráfico en búsqueda de rastros o indicios de ataques en las cabeceras de los paquetes TCP, basado en los principios del sistema inmunológico de los vertebrados y fundamentado en el uso de la inteligencia artificial, en particular los sistemas expertos, generando logs o bitácoras para que se pueda hacer un seguimiento del ataque por parte del administrador de la red.

Al ser la solución “auto-actualizable” y adaptable, no está basada en reglas fijas, ofrece mejoras en los servicios de IDS, ya que la idea básica se asocia a los linfocitos que buscan virus, bacterias e infecciones y pueden aprender de su experiencia entonces el software busca paquetes extraños, intentos de ataques y demás vulnerabilidades que puedan existir en una red.

1.3 Justificación

Debido al aumento de los ataques, virus, accesos indebidos a las redes públicas y privadas, y la curiosidad de ciertas personas por la información confidencial se necesitan varios dispositivos como son: sistemas de detección de intrusos, un firewall, un sistema antivirus y otro sistema anti-spam en lo referente a seguridad, estabilidad y confiabilidad en la administración de la red de una empresa.

Surge entonces la idea de desarrollar un software con capacidades de aprender nuevos riesgos, que se adapte a cualquier topología de red, que reduzca el tiempo de respuesta y la intervención humana en la administración.

Con esta idea se pretende que el software identifique patrones asociados con virus, spam o intrusos, el sistema puede ir aprendiendo que cosas son buenas y que cosas son malas, al igual que lo hace el sistema inmune de los vertebrados. El software se fundamenta en teorías de inteligencia artificial.

Las actualizaciones en caso de ser requeridas se podrían suministrar mediante transfusiones desde otras redes dónde el software ha sufrido un poco más y por lo tanto es más fuerte a ciertos tipos de ataques, no será necesario estar casado con una empresa fabricante para el soporte de las máquinas y en un futuro no habría necesidad de una actualización física por el cambio de sistema operativo para seguir siendo efectivos.

¹ WIKIPEDIA. Artificial Immune System. Disponible en Internet: http://en.wikipedia.org/wiki/Artificial_immune_systems [febrero 2006]

Desde el punto de vista investigativo poseer una herramienta que permita ir afinando diversos factores y comparar esta noble visión con otras propuestas se presenta interesante

1.4 Objetivos

1.4.1 Objetivo General: Desarrollar de un software basado en un Sistema Inmune Artificial para la Seguridad en Redes.

1.4.2 Objetivos Específicos

- Determinar los elementos relevantes de los Sistemas Inmunes Artificiales que apoyarían un IDS.
- Realizar el análisis y el diseño de una herramienta de software basada en un Sistema Inmune Artificial aplicado a la seguridad en redes utilizando una metodología orientada a objetos.
- Describir el estado del arte de los sistemas inmunes artificiales.
- Realizar la implementación del sistema utilizando software libre.
- Validar el sistema con tráfico proveniente de sistemas reales.
- Hacer pruebas comparativas de la efectividad del sistema con otros sistemas similares de seguridad.
- Elaborar la documentación necesaria para el uso de la herramienta por cualquier administrador de una red.
- Plantear posibles desarrollos futuros, nuevos módulos y sugerencias.

1.5 Diseño Metodológico

1.5.1 Definición de la Hipótesis: El desarrollo de una herramienta de software aplicada a la seguridad en redes utilizando la teoría de sistemas inmunes artificiales brindará una nueva aproximación a la solución de la problemática referente a la vulnerabilidad de la información.

1.5.2 Indicador: Se espera que la herramienta llegue grado de efectividad satisfactorio en detectar patrones de vulnerabilidad en el sistema mediante el análisis de bitácoras y paquetes.

1.5.3 Universo: Todas las empresas, personas y hogares que necesiten o quieran tener un sistema de protección de información.

1.6 Personas que Participan en el Proyecto

1.6.1 Director

Néstor Darío Duque Méndez, Ph.D. (c)
Profesor Universidad Nacional de Colombia
Sede Manizales

1.6.2 Ejecutor

Juan David Betancur Vallejo
Estudiante Ingeniería de Sistemas y Computación
CCNA®

1.6.3 Asesores

Ingeniera María Fernanda Zúñiga
Profesora Universidad Tecnológica de Pereira.
Ingeniería de Sistemas y Computación.

Ingeniero John Alexis Guerra Gómez
Profesor Universidad Tecnológica de Pereira
Ingeniería de Sistemas y Computación.

2 MARCO TEÓRICO

2.1 Estado del Arte de los Sistemas Inmunes Artificiales

Con la evolución de la tecnología, la globalización y el Internet, cada vez más las redes de datos van cobrando una mayor importancia dentro de una organización, ya sea una empresa o incluso en el hogar. La información, a su vez, va ganando más relevancia e interés, y al ser ésta en forma digital está expuesta a múltiples amenazas (virus, troyanos, ataques de terceros, etc.).

En la actualidad se tiene una mayor cantidad de información valiosa al igual que mayor número de personas que quieren apoderarse de ella, ya sea con fines malignos o sólo por curiosidad; y con el reciente auge de las telecomunicaciones, la facilidad de los nuevos usuarios de conseguir información, la tremenda curiosidad que se despierta a diario en los jóvenes involucrados en la informática y los altos costos que implican tener personal y dispositivos especializados en seguridad informática hacen que este campo del conocimiento pueda ser explotado para estos fines.

Pero al igual que existen personas interesadas en apoderarse de la información ajena, también se encuentran personas y empresas interesadas en proteger la información ya sea propia o la de otros, estas personas o empresas enfocan sus esfuerzos en ir un paso adelante, desarrollan sistemas especializados (dispositivos y software) tales como firewalls, IDS, IPS, anti spam, entre otros.

Un campo de la ciencia informática que hasta ahora poco se ha explorado enfocado hacia la solución de estos problemas es la inteligencia artificial, y en particular los sistemas inmunes artificiales, que sugieren una aproximación nueva para enfrentar estos inconvenientes.

Para entender este enfoque antes se debe conocer cómo funciona el sistema inmune natural, y cómo se puede simular este comportamiento en un ambiente artificial, en particular, la seguridad en redes y algunas alternativas a la solución que se desea plantear en este proyecto.

Sistemas Inmunes Naturales

El cuerpo humano es víctima de ciertos virus o bacterias que pueden encontrar un ambiente estable, controlado, con grandes cantidades de proteínas, grasas, carbohidratos, protección contra otros virus o contra gérmenes y bacterias que

puedan amenazarlos, lo que acrecienta, los virus, bacterias y gérmenes viviendo en el cuerpo con el tiempo.

Pero, ¿qué evita que estos virus, bacterias y gérmenes nos hagan la vida imposible, nos llenen de enfermedades e incluso conlleven a la muerte?: Nuestro sistema inmune.

Este sistema consta de varias capas de defensa o barreras sucesivas, cada una más específica y especializada que la anterior, la primera es la piel, la cual nos protege de todas la infecciones que nos rodean, sin ella cualquier patógeno podría ingresar a nuestro sistema.

Luego tenemos una segunda barrera llamada fisiológica, la temperatura y pH hacen que, para muchos de estos organismos extraños las condiciones sean adversas y mueran enseguida.

En el caso de que estos patógenos logren vencer estas dos barreras el sistema inmune innato y el sistema inmune adaptativo entran en acción. El sistema inmune innato es el más primitivo, se desarrolló hace 550 millones de años², son células que limpian el sistema de patógenos como moléculas extracelulares y otros materiales mediante la ingestión de dichos elementos.

Por su parte el sistema inmune adaptativo es más moderno ya que sólo surgió hace 90 millones de años³, este sistema es más sofisticado e involucra diferentes tipos de células y moléculas, es llamado adaptativo porque es responsable de la inmunidad adquirida por un organismo a lo largo de su vida.

La información sobre la respuesta mejorada por el sistema inmune adaptativo se conserva aún después de que el patógeno es eliminado, mediante una especie de memoria inmunológica, y permite que este sistema desencadene ataques más rápidos, fuertes y precisos si en el futuro el sistema inmune detecta este tipo de patógenos nuevamente.

Al igual que la inmunidad innata, la inmunidad adaptativa depende de la habilidad del sistema en general para poder distinguir entre las moléculas propias o self y las que no lo son o not self, con este detalle se tratan de evitar los falsos positivos o los falsos negativos que son un problema grave para el sistema. El falso negativo puede resultar muy perjudicial para el organismo ya que las células

² EISEN DP, MINCINTON RM. MBL, UN VALOR EN ALZA DEL SISTEMA INMUNE. Traducción disponible en Internet:<http://www.ucm.es/info/fmed/medicina.edu/Infecciones/mbi.htm> [febrero 2006]. artículo original disponible en: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=14614673&dopt=Abstract [febrero 2006]

³ Ibid.

atacarían los tejidos, células y órganos internos por no poder reconocer acertadamente un ataque.

Otro rol que cumple el sistema inmune natural es la identificación y eliminación de tumores. En cada tumor aparecen células transformadas o mutaciones de las mismas que generan antígenos, estos antígenos no son reconocidos como células normales y la reacción del sistema ante este nuevo cuerpo foráneo es atacarlo, logrando así la reducción de los tumores que pueden surgir en el organismo.

La respuesta primaria del sistema inmune es la destrucción de las células foráneas, ya sean patógenos o antígenos, para esto utiliza células T asesinas, algunas veces con asistencia otras células T para el sistema inmune un tumor muestra señales de células iguales a las de una infección viral.⁴

Según Tanja Lange, Boris Perras, Horst L. Fehm y Jan Born, en su artículo "Sleep Enhances the Human Antibody Response to Hepatitis A Vaccination", el hecho de tener un buen reposo y sueño normal aumenta la funcionalidad del sistema inmune.⁵

Por el contrario llevar una vida de estrés puede ocasionar múltiples trastornos en este sistema, recientemente científicos han estado estudiando la relación mente-cuerpo para poder demostrar que en realidad se puede mostrar una inmunosupresión por cierto grado de estrés alcanzado.⁶

Sistemas Inmunes Artificiales para Seguridad en Redes⁷

Con base en los sistemas inmunes naturales se plantea la posibilidad de simular su funcionamiento utilizando algoritmos genéticos e inteligencia artificial.

Ahora bien, ¿Por qué es deseable emular el sistema inmune natural de los vertebrados y aplicarlo a la seguridad en redes de datos?

⁴ RITZ U, SELIGER B, FERRONE S (2006). "Molecular mechanisms of HLA class I antigen abnormalities following viral infection and transformation"

⁵ TANJA LANGE et al. Sleep Enhances the Human Antibody Response to Hepatitis A Vaccination. Disponible en Internet: <http://www.psychosomaticmedicine.org/cgi/content/full/65/5/831> [Marzo 2006]

⁶ FAITH Re, KHANSARI Dn, MURGO Aj,. Effects of stress on the immune system. Disponible en Internet: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=pubmed&dopt=Abstract&list_uids=2186751 [Marzo 2006]

⁷ FORREST, Stephanie. HOFMEYR, Steven. SOMAYAJI, Anil. Principles of a Computer Immune System. Disponible en Internet: <http://www.cs.unm.edu/~immsec/publications/nspw-97.pdf>. [octubre 2005]

Enumerando algunos aspectos del sistema inmune se puede notar que posee una gran robustez, estabilidad y confiabilidad.

- Multicapas: posee varias capas para la protección del sistema en varios niveles.
- Desechabilidad: los elementos que componen el sistema no deben ser esenciales ya que si fallan todo el sistema falla. Deben poder ser reemplazados por otros componentes que cumplan funciones similares, aunque no iguales, evitando con esto un único posible punto de falla.
- Autonomía: el sistema inmune no necesita de constante atención ya que toma sus propias decisiones. Este punto puede no llegar a ser aplicable a los sistemas informáticos ya que la falta de mantenimiento y atención que se le deba prestar, puede llegar a dejarnos con un sistema posiblemente incorrecto en su configuración o en su aprendizaje ya que con los constantes cambios en las tecnologías lo que hoy se considera perjudicial posiblemente en un futuro ya no lo sea.
- Adaptabilidad: el sistema aprende sobre nuevos virus, bacterias y ataques de manera independiente o por medio de las actualizaciones o transfusiones que se le apliquen, además puede recordar este nuevo conocimiento.
- No hay lugares para esconderse: el sistema debe poder analizarse a si mismo, así como los linfocitos se analizan entre ellos por ser también células.

Debido a estos y otros aspectos se puede creer que el sistema inmune de los vertebrados merece ser imitado para la seguridad en sistemas informáticos y redes de datos. La complejidad del sistema natural genera muchos retos y dificultades y este trabajo se presenta como un paso en esta nueva aproximación.

Ahora, si el sistema inmune humano permite vivir más o menos 70 años con ataques diarios de virus, bacterias y demás infecciones mortales, ¿por qué no utilizar esta idea para beneficio de los administradores de sistemas informáticos?

Los sistemas inmunes artificiales han tenido un largo recorrido, por lo menos en el aspecto teórico, ya que en el desarrollo práctico de estas teorías apenas se encuentran algunos documentos o publicaciones sobre una aplicación que utilice estos principios para su funcionamiento.

La aplicabilidad de estos ideales es muy variada entre las cuales tenemos: respuestas automatizadas, computación distribuida, epidemiología y sistemas de detección de intrusos, entre otras.

Pero como ya se mencionó, todos estos conceptos están plasmados en documentos, publicaciones y artículos, muy pocos se han llevado a un nivel algo más tangible y/o aplicado, por lo menos en lo observado en la consulta a través de la web. En relación a la propuesta de este documento se tiene que el Departamento de Ciencias de la Computación de la Universidad de Nuevo México en Albuquerque, ha presentado una herramienta IDS llamada LISYS⁸.

Esta herramienta monitorea los paquetes SYN del protocolo TCP para detectar anomalías en el tráfico de red. Funciona de la siguiente manera:

Un paquete llega a un equipo de la red, el cual tiene instalado un cliente de la herramienta que se encarga de filtrar los paquetes SYN y enviarlos a un equipo servidor en el que se realizan las evaluaciones de dicho paquete para comprobar su validez, si el paquete presenta anomalías se envía un correo electrónico al administrador del sistema, quien debe decidir si se trata de un paquete irregular pero válido o en realidad es considerado un ataque.

Según esta información, LISYS es un sistema cliente servidor que sólo analiza los paquetes de sincronización SYN de el protocolo TCP. Y hasta el momento de la redacción de este documento se menciona que esta aplicación está en una etapa muy preliminar del desarrollo. Tampoco se han encontrado otras herramientas que se basen en este principio para la solución del problema planteado, la seguridad en redes.

A nivel internacional, y como resultado de una extensa consulta a través de Internet, no se ha encontrado otra base diferente a la universidad antes mencionada como la única que ha publicado algún tipo de documentación que muestra que se ha estado trabajando en estos principios enfocados a este tema en particular⁹.

Esta universidad y en especial el departamento de ciencias de la computación ha logrado varios desarrollos enfocados a distintos aspectos de la seguridad informática y de otros como una radio adaptativa.¹⁰ Al ser de las pocas instituciones que se tiene conocimiento de estar trabajando en este principio han

⁸ FORREST, STEPHANIE. LYSYS. Disponible en Internet: <http://www.cs.unm.edu/~forrest/software/lisys/> [diciembre 2005]

⁹ COMPUTER SCIENCE DEPARTMENT. UNIVERSITY OF NEW MEXICO. Computer Immune Systems. Disponible en Internet: <http://www.cs.unm.edu/~immsec/begin.html> [octubre 2005]

¹⁰ COMPUTER SCIENCE DEPARTMENT. UNIVERSITY OF NEW MEXICO. Data Sets and Software. Disponible en Internet: <http://www.cs.unm.edu/~immsec/data-sets.htm> [octubre 2005]

logrado tener una gran aceptación internacional, prueba de ello es el patrocinio de grandes empresas como Intel, IBM y Microsoft.¹¹

A nivel local no se tiene conocimiento de ninguna otra institución que esté realizando un trabajo similar, así que al momento de realización de este proyecto y la redacción de este documento, la solución se presenta como una innovación regional y nacional.

2.2 Principios de Inteligencia Artificial Aplicados

La inteligencia artificial posee diversos principios y formas de enfrentar un problema, algoritmos genéticos, computación difusa, algoritmos heurísticos, redes neuronales, sistemas expertos, entre muchas otras.

Para este proyecto se utilizaron las bases de un sistema experto, o sea, simular la respuesta de un experto para la resolución de un problema particular, en este caso el experto es el sistema inmune natural de los vertebrados, en particular la aplicación del modelo de capas que utiliza dicho sistema para la protección del organismo de las infecciones que provienen del mundo exterior.

“Un sistema experto (SE) es una rama de la Inteligencia Artificial y es aquel que imita las actividades de un humano para resolver problemas de distinta índole (no necesariamente tiene que ser de Inteligencia Artificial). También se dice que un SE se basa en el conocimiento declarativo (hechos sobre objetos, situaciones) y el conocimiento de control (información sobre el seguimiento de una acción).”¹²

Estos sistema pueden ser de diferentes tipos, basados en reglas, basados en casos y basados en redes bayesianas, así aplicando estos principios la solución al problema planteado se puede obtener aplicando reglas heurísticas, razonamiento de casos, tratando de encontrar una solución a un problema similar del pasado o utilizando redes bayesianas y el teorema de Bayes.¹³

Este tipo de programas o sistemas aunque tienen mucha aplicabilidad y posibilidades de acción muy grandes, también tienen limitaciones fuertes, por ejemplo, al ser un especialista o experto en un problema en particular es completamente inoficioso o hasta idiota para cualquier otro problema, y al estar

¹¹ COMPUTER SCIENCE DEPARTMENT. UNIVERSITY OF NEW MEXICO. Sponsors. Disponible en Internet: <http://www.cs.unm.edu/~immsec/sponsors.htm> [octubre 2005]

¹² WIKIPEDIA. Sistema Experto. Disponible en Internet: http://es.wikipedia.org/wiki/Sistema_experto [junio 2006]

¹³ El teorema de Bayes, descubierto por Thomas Bayes, en la teoría de la probabilidad, es el resultado que da la distribución de probabilidad condicional de una variable aleatoria A dada B en términos de la distribución de probabilidad condicional de la variable B dada A y la distribución de probabilidad marginal de sólo A .

basado en reglas primarias fijas se puede perder casi por completo la creatividad y el sentido común.

Debido a estas limitaciones estos sistemas son utilizados como soporte de un experto y no como reemplazo del mismo, ya que en ocasiones sólo la experiencia y el sentido común de los humanos pueden resolver un problema, entonces estos sistemas pueden ser utilizados para el monitoreo y diagnóstico de ciertos ambientes, en nuestro caso la red de una empresa.

Desde una era muy temprana en el desarrollo de la computación se han venido mostrando desarrollos de sistemas expertos para la solución de ciertos problemas, prueba de ello es MYCIN desarrollado en la universidad de Stanford en la década de los 70's, e inclusive desde mucho antes ya se estaban haciendo la pregunta ¿pueden las máquinas pensar?. Uno de los primeros investigadores en este campo fue John McCarthy¹⁴ quien nombró este concepto como Inteligencia Artificial o AI (en inglés Artificial Intelligence) en 1956.¹⁵

“En la década de los ochenta se ponen de moda los SE, numerosas empresas de alta tecnología investigan en este área de la inteligencia artificial, desarrollando SE para su comercialización. Se llega a la conclusión de que el éxito de un SE depende casi exclusivamente de la calidad de su base de conocimiento. El inconveniente es que codificar la pericia de un experto humano puede resultar difícil, largo y laborioso.”¹⁶

Para la implementación de esta herramienta se ha tomado como base el principio de que un sistema inmune natural esta regido por capas, cada capa representa un nivel de protección y en cada nivel hay valores que permite o niegan el paso a los patógenos que pretender entrar al sistema.

De igual forma en la solución acá planteada se tienen capas de filtración de paquetes, evaluando cada paquete y haciendo un match o comparación de sus características con valores reconocidos como perjudiciales. La clasificaciones de las amenazas se plantearán más adelante en este documento.

Así como resultado tendremos una evaluación de la situación acertada, evitando al máximo encontrar falsos positivos y falsos negativos. Esto se refiera a marcar algo bueno como malo y algo malo como bueno.

¹⁴ WIKIPEDIA. John McCarthy (computer scientist). Disponible en Internet: http://en.wikipedia.org/wiki/John_McCarthy_%28computer_scientist%29 [junio 2006]

¹⁵ WIKIPEDIA. Dendral. Disponible en Internet: <http://en.wikipedia.org/wiki/Dendral> [junio 2006]

¹⁶ MONTES CASTRO, JESÚS. Sistemas Expertos (SE). Dispoible en Internet: <http://www.monografias.com/trabajos16/sistemas-expertos/sistemas-expertos.shtml> [julio 2006]

Al terminar esta evaluación la herramienta presentará un informe en un archivo log o bitácora para tener una trazabilidad de lo ocurrido, de igual manera alertará al administrador de la red si se está sufriendo algún incidente mediante un correo electrónico, previamente configurado por el administrador.

3 SELECCIÓN DE CRITERIOS PARA LA EVALUACIÓN DE PAQUETES

Para el análisis, desarrollo e implementación de la herramienta es necesario establecer ciertos criterios de evaluación de los paquetes capturados y analizados para decidir su impacto en la red o en los equipos conectados a la misma. Dichos criterios deben permitir a la herramienta un correcto funcionamiento dejando aparte la mayor cantidad de paquetes correctos que puedan ser mal interpretados. Se debe guardar un correcto balance entre los 3 criterios en que se basa la seguridad informática: Integridad, Confidencialidad y Disponibilidad¹⁷; evitar al máximo la notoriedad de la herramienta por parte de los usuarios e inclusive por parte del administrador.

Al tratarse de una herramienta de software para el análisis de la red, ésta debe ser implantada en un equipo o servidor que permita analizar el segmento de red a ser estudiado. De igual manera al ser una herramienta libre puede implantarse en varios equipos y en varios segmentos con lo que se logra una mayor cobertura, analizando, tanto paquetes externos como internos reduciendo al máximo la posibilidad de un ataque desde dentro de la organización que es, según el FBI y el Instituto de Seguridad en Computo (CSI) en su reporte anual¹⁸, una de las tres mayores amenazas de ataques que se pueden presentar.

Debido a la gran cantidad de parámetros para analizar en una red y el alcance de este proyecto se ha optado sólo por analizar las cabeceras de los paquetes TCP, en búsqueda de combinaciones incorrectas, poco usuales y/o sospechosas en las banderas, direcciones de origen o destino reportadas en las listas negras entre otros que se explicarán a lo largo de este capítulo.

3.1 Números de Puertos

Los números de puerto son usados para un registro de las diferentes comunicaciones que se tienen entre equipos al mismo tiempo:

Los números de puertos tienen los siguientes rangos¹⁹:

¹⁷ NTC-ISO/IEC 17799:2006

¹⁸ CSI/FBI. Computer Crime and Security Survey. Disponible en Internet: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf [noviembre 2006]

¹⁹ IANA. Port Numbers. Disponible en Internet: <http://www.iana.org/assignments/port-numbers> [abril 2006]

- Números inferiores a 1024, considerados como puertos bien conocidos.
- Los puertos registrados son usados por aplicaciones específicas de ciertos fabricantes y se encuentran en el rango 1024 a 49151.
- Números por encima de 49151 son puertos asignados dinámicamente.

3.1.1 Puertos Bien Conocidos

“Los puertos bien conocidos son asignados por la IANA y en la mayoría de los sistemas sólo pueden ser usados por procesos del sistema o procesos root o programas ejecutados por usuarios privilegiados.

Los puertos son usados en [RFC793]²⁰ para nombrar el final lógico de las conexiones que llevan conversaciones de largo término. Con el propósito de proveer servicios a llamadas anónimas o desconocidas, un puerto de servicio de contacto es definido.²¹

Así, por ejemplo, un puerto bien conocido es el 21 el cual es asociado a servicios de FTP, el 80 es el puerto comúnmente asociado a WEB y el 22 al acceso a SSH.

La lista completa de asociaciones a los puertos bien conocidos puede ser encontrada la página de la IANA.²²

3.1.2 Número de Puertos en la Cabecera TCP.

En cada cabecera de un paquete TCP deben existir dos números de puertos, el de origen y el de destino; el puerto de origen es un puerto que el equipo que envía el paquete escoge aleatoriamente de los puertos por encima de 49151, esto para que cada conexión pueda ser identificada por los equipos, ya que pueden existir varias comunicaciones entre los mismos equipos.²³

El puerto de destino generalmente es un puerto de los bien conocidos, ya que un equipo se conecta a otro para obtener un servicio que se está ofreciendo y como

²⁰ Postel, J., ed., "Transmission Control Protocol - DARPA Internet Program Protocol Specification", STD 7, RFC 793, USC/Information Sciences Institute, September 1981.

²¹ IANA. Port Numbers. Disponible en Internet: <http://www.iana.org/assignments/port-numbers> [abril 2006]

²² Ibid

²³ Cisco Networking Academy Program CCNA

ya se mencionó puede ocurrir que un equipo tenga varias conexiones y por lo tanto es necesario identificar cada una, esto se realiza con los puertos de origen.

Con esta información básica se puede concluir que si una cabecera TCP tiene como puerto de origen y de destino el mismo número, se puede interpretar el paquete como sospechoso o malicioso, y si estos puertos están en el rango de los puertos bien conocidos se puede afirmar casi sin dudas que es un intento de ataque.²⁴

Al encontrar esta situación la herramienta podrá, informar que se está sufriendo un ataque, generar el log o bitácora con que podemos rastrear el paquete, el origen y posible ubicación del atacante en tiempo real, si se trata de un ataque interno se puede ubicar la dirección IP de origen en los planos de diseño de direcciones. O si existen servidores DNS o WINS se puede llegar al punto exacto del equipo que está intentando el ataque.

3.2 Direcciones IP

“Actualmente existen dos tipos de direcciones IP: IP versión 4 (IPv4) e IP versión 6 (IPv6). IPv4 fue inicialmente puesta en marcha el 1 de Enero de 1983 y es aún la versión más usada. Las direcciones IPv4 son números de 32 bits frecuentemente usados como 4 octetos en notación decimal separados por puntos (por ejemplo 192.0.32.67).”²⁵

Es gracias a estas direcciones que dos equipos se pueden comunicar, ya que cada uno puede identificar al otro con una única dirección. Para garantizar esta unicidad y no corromper el flujo normal de los paquetes en Internet, las direcciones IP se clasifican en dos grandes tipos: Privadas y Públicas.

3.2.1 Direcciones Privadas

Este tipo de direcciones se creó para suplir la necesidad de direcciones IP que una empresa posee en su interior, debido al creciente número de PC's que cada empresa necesita y la poca disponibilidad de direcciones que se pueden otorgar, la IANA decidió establecer ciertos rangos de direcciones para ser utilizadas para direccionar los equipos de cómputo de una organización.

²⁴ KENT FREDERICK, Karen. Network Intrusion Detection Signatures, Part One. Disponible en Internet: <http://www.securityfocus.com/infocus/1524> [agosto 2006]

²⁵ IANA. IP Addresses Service. Disponible en Internet: <http://www.iana.org/ipaddress/ip-addresses.htm> [agosto 2006]

Estos rangos se pueden observar en las 3 diferentes clases que la IANA tiene reservados para las redes privadas internas:

10.0.0.0 -> 10.255.255.255 (prefijo 10/8) Clase A
172.16.0.0 -> 172.31.255.255 (prefijo 172.16/12) Clase B
192.168.0.0 -> 192.168.255.255 (prefijo 192.168/16) Clase C

Con estos rangos de direcciones se puede cubrir desde la red más simple a la más compleja organización con varias sucursales sin necesidad de utilizar las valiosas direcciones IP públicas que cada día son más escasas.

3.2.2 Direcciones Públicas

Las direcciones públicas son las direcciones que quedan por fuera del rango de las direcciones privadas y son las utilizadas para las máquinas conectadas a Internet, las cuales deben garantizar, como ya se mencionó, que son únicas para cada una. Estas direcciones se pueden obtener mediante un ISP.

Debido al gran auge que tuvo Internet las direcciones IP versión 4 se comenzaron a terminar y fue necesario crear nuevas formas de evitar que se agotaran definitivamente. Además de las direcciones privadas también se utilizaron nuevos esquemas como el CIDR y finalmente se creó una nueva versión para suplir la creciente demanda por direcciones públicas.

3.2.3 Direcciones en Listas Negras

Ya que las direcciones públicas son únicas es posible identificar compañías, ISP's e incluso países que pueden ser considerados como una amenaza, esto se logra ya que cada dirección IP corresponde a una única entidad y se lleva un registro de ello. Así por ejemplo la dirección 200.21.98.4 pertenece a COLOMBIA TELECOMUNICACIONES S.A. ESP y se puede conseguir incluso el número de teléfono de la persona encargada de esta dirección o en la mayoría de los casos de un rango de direcciones.

Con esto se puede identificar, como ya se mencionó, direcciones IP que pueden ser directamente bloqueadas o monitoreadas de cerca. Existen sitios en Internet donde se pueden encontrar listas actualizadas, las cuales se pueden descargar y utilizar a favor de la empresa, haciendo las correcciones y/o ampliaciones que considere necesarias.

Entonces si es posible tener acceso a estas listas se pueden generar algoritmos que comparen las direcciones de origen y/o destino contra estas listas y poder

reconocer si se está sufriendo un ataque o hay alguna persona de la organización interesada en estos sitios, ubicarla y evitar un incidente mayor.

Además según el funcionamiento de la herramienta y el ambiente en el cual se ubique, esta lista puede ir aumentando con direcciones aprendidas de incidentes ocurridos, utilizando una pequeña estadística para no bloquear completamente un dominio al primer indicio de ataque, ya que, puede ocurrir que sea un incidente aislado y no por eso se debe bloquear toda una institución, por ejemplo una universidad que presta varios servicios entre ellos internet para los estudiantes.

3.2.4 Direcciones origen y destino

En todo paquete TCP existen dos campos designados a las direcciones IP. Estos son: dirección origen y dirección destino, se utilizan para poder enrutar el paquete hacia su destino o para devolver un mensaje de error en caso de que destino sea inaccesible. Estos dos campos pueden ser manipulados para provocar un fallo en ciertos sistemas, dependiendo de sus características. El ataque más común utilizando estos campos es el “land” o “landing”, el cual consiste en poner la dirección de destino igual a la dirección de origen, con lo que se logra que el sistema no sepa qué hacer con el paquete y finalmente se paralice completamente. Es un ataque del tipo DoS.

Ese tipo de ataques es muy común, por su facilidad de generación, ya que existen múltiples herramientas de spoofing que puede ayudar a cualquier persona a generar estos paquetes.

3.3 Banderas de la Cabecera TCP

Las banderas de la cabecera TCP son 6 bits que se activan para hacer referencia al contenido del paquete. Estos bits son nombrados así²⁶:

SYN: bandera de sincronización, utilizada conjuntamente con otras banderas para establecer una conexión.

FIN: bandera de finalización, utilizada para terminar una conexión.

URG: bandera de urgente, se utiliza para establecer cierta prioridad al paquete.

ACK: bandera de reconocimiento, se utiliza para informar al equipo que envía el paquete que éste ha sido recibido con éxito.

²⁶ IANA. TCP Header Flags. Disponible en Internet: <http://www.iana.org/assignments/tcp-header-flags> [julio 2006]

RST: bandera de reset, se utiliza para reinicializar la conexión.

PSH: bandera de push, se utiliza para que el paquete sea enviado tal cual se generó, sin la posibilidad de ir mezclado con otros datos de paquetes generados subsecuentemente.

3.3.1 SYN

Esta bandera es muy utilizada ya que es necesaria para establecer una conexión con el saludo de tres vías o three-way handshake, este saludo se elabora de la siguiente forma: se envía un paquete con la bandera SYN activa al equipo remoto con el cual se desea hacer la conexión, se recibe un paquete con las banderas SYN y ACK activas, las cuales indican que el equipo remoto recibió el paquete y que puede establecer la conexión y regresa un paquete con la bandera ACK activa, la cual indica que ha recibido el último paquete y que puede comenzar la transmisión de datos.

3.3.2 FIN

La bandera FIN es utilizada para terminar una conexión; esta finalización puede ocurrir de varias formas, una al igual que el inicio con un saludo de tres vías pero en vez de la bandera SYN se activa la bandera FIN. Otra forma es terminar la conexión por partes, primero un lado de la conexión termina y se dice que la conexión quedó medio-abierta, luego la otra parte puede seguir enviando información y luego terminar la conexión.

La última forma de terminar una conexión es de forma simultánea, ambas partes envían un paquete FIN y luego ambas partes envían un paquete de ACK o reconocimiento.

3.3.3 Combinaciones incorrectas de SYN y FIN

Probablemente la combinación ilegal más conocida es la de tener ambas banderas activas, como ya sabemos una significa el comienzo o sincronización de una conexión y la otra la finalización, por lo tanto una combinación de estas dos banderas es ilógica y es un signo fiel de estar sufriendo un ataque.²⁷

²⁷ KENT FREDERICK, Karen. Abnormal IP Packets. Disponible en Internet: <http://www.securityfocus.com/infocus/1200> [septiembre 2006]

Este tipo de combinación no se puede conseguir por un error del sistema o por corrupción normal de los paquetes, sino por una manipulación deliberada de los mismos, ya sea de forma manual, o con algún software de spoofing que se pueden descargar desde varios sitios en Internet.

3.4 Conclusiones de la Selección

Para terminar este capítulo, se llegan a unas conclusiones de qué es posible utilizar para detectar paquetes con anomalías que pueden indicar que se está sufriendo o se va a sufrir un ataque. En los siguientes gráficos se tratará de clarificar la estructura de un paquete TCP normal, dónde se buscaron las anomalías.

Gráfica 1 Cabecera TCP

Bit 0		Bit 15		Bit 16		Bit 31	
Puerto origen (16)				Puerto destino (16)			
Número de secuencia (32)							
Número de acuse de recibo (32)							
Longitud del encabezado (4)		Reservado (6)	Bits de código (6)		Ventana (16)		
Checksum (16)				Urgente (16)			
Opciones (0 ó 32 si las hay)							
Datos (varía)							

Fuente: Cisco Networking Academy Program CCNA

Gráfica 2 ¿Dónde se Encuentran las Banderas?

Bit 0		Bit 15 Bit 16		Bit 31
Puerto origen (16)		Puerto destino (16)		
Número de secuencia (32)				
Número de acuse de recibo (32)				
Longitud del encabezado (4)	Reservado (6)	Bits de código (6)	Ventana (16)	
Checksum (16)		Urgente (16)		
Opciones (0 ó 32 si las hay)				
Datos (varía)				

Fuente: Cisco Networking Academy Program CCNA

Gráfica 3 Esquema de las Banderas de una Cabecera TCP

U R G	A C K	P S H	R S T	S Y N	F I N
-------------	-------------	-------------	-------------	-------------	-------------

En caso de que en esta cabecera se encuentren activos los campos de SYN y FIN activos se considera, como ya se mencionó anteriormente, que el paquete es incorrecto e indicio de que se está sufriendo un ataque.

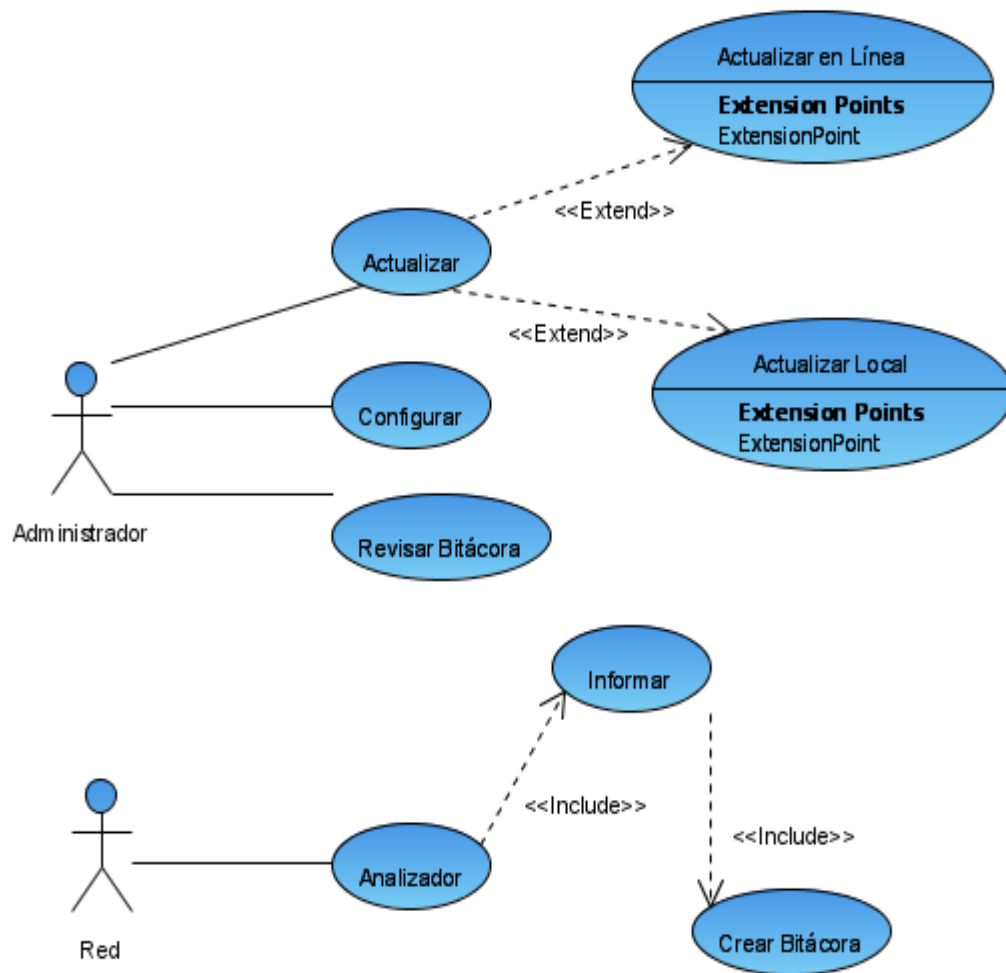
Cualquier otra combinación de estas banderas puede ser considerada correcta, aunque existen ciertos tipos de ataques que manipulan estas banderas para generar un ataque de denegación de servicios generando un paquete de sincronización correcto y luego uno de reinicio también correcto. Para reconocer este tipo de ataques la herramienta deberá tener cierto tipo de memoria, lo cual se encuentra por fuera del alcance de este proyecto, pero se planteará como un módulo para ser desarrollado posteriormente.

4 MODELAMIENTO DE LA HERRAMIENTA

4.1 Etapa de Análisis

4.1.1 Diagrama de Casos de Uso

Gráfica 4 Casos de Uso



4.1.2 Especificación de Casos de Uso

Tabla 1 Caso de Uso Actualizar

Actualizar		
Actores	Administrador	
Propósito	Realizar las actualizaciones al sistema	
Resumen	El administrador solicita al sistema que se actualice y le especifica la ubicación de las actualizaciones disponibles	
Tipo	Esencial y primario	
Curso Normal de los Eventos	<div>Acción del Actor</div> <div>Respuesta del Sistema</div>	
	1	El administrador desea actualizar el sistema
	2	El sistema presenta dos opciones
	3	El administrador selecciona entre: <ul style="list-style-type: none"> Actualización en línea (Ver Sección) Actualización local (Ver Sección)
Sección actualizar en línea	1	El administrador quiere actualizar el sistema
	2	El sistema proporciona todas las opciones para el ingreso de la información correspondiente
	3	El administrador ingresa los ítems solicitados
	4	Se advierte sobre la disponibilidad de la conexión
	5	Se acepta la advertencia
	6	Se procede a la actualización del sistema

Sección actualización local	1	El administrador quiere actualizar el sistema	
	2		El sistema le proporciona todas las opciones para el ingreso de la información correspondiente a la actualización local
	3	El administrador ingresa y selecciona los ítems solicitados	
	4		Se advierte sobre la disponibilidad del dispositivo seleccionado
	5	Se acepta la advertencia	
	6		Se procede a la actualización del sistema
Curso alternativo actualización en Línea	Línea 3: El administrador no ingresa los ítems solicitados, se le sigue solicitando que los ingrese o que cancele la operación		
Curso alternativo actualización local	Línea 3: El administrador no ingresa los ítems solicitados, se le sigue solicitando que los ingrese o que cancele la operación		

Tabla 2 Caso de Uso Configurar

Configurar		
Actores	Administrador	
Propósito	Permitir la configuración del sistema	
Resumen	El administrador realiza la configuración inicial o una modificación posterior del sistema	
Tipo	Esencial y primario	
Curso normal de los eventos	Acción del Actor	
	1	El administrador requiere configurar el sistema
	2	
		Respuesta del Sistema
		El sistema proporciona todas las opciones necesarias para su configuración

	3	El administrador ingresa la información	
	4		El sistema valida que la información esté completa y advierte sobre el registro de esta información
	5	El administrador acepta la advertencia	
	6		El sistema registra la nueva configuración y la activa
Curso alterno	Línea 3: El administrador no ingresa los ítems solicitados, se le sigue solicitando que los ingrese o que cancele la operación		

Tabla 3 Caso de Uso Revisar Bitácoras

Revisar Bitácoras			
Actores	Administrador		
Propósito	Revisar las bitácoras generadas por el sistema		
Resumen	El administrador le indica al sistema que quiere revisar las bitácoras, el sistema muestra las bitácoras disponibles para ser revisadas		
Tipo	Esencial y primario		
Curso normal de los eventos	Acción del Actor		Respuesta del Sistema
	1	El administrador requiere analizar las bitácoras	
	2		El sistema le presenta un listado de todas las bitácoras disponibles
	3	El administrador selecciona una bitácora de la lista presentada	
	4		El sistema formatea la información y la presenta en de una manera más legible
Curso alterno	Línea 3: El administrador no selecciona una bitácora de la lista, se le informa que no lo ha hecho y se sigue en espera de que seleccione una o cancele la operación		

Tabla 4 Caso de Uso Analizador

Analizado		
Actores	Red	
Propósito	Escuchar y analizar los paquetes que pasan por la red, para realizar acciones dependiendo del resultado del análisis	
Resumen	Los paquetes que pasan por la red capturados para analizarse, en caso de ser paquetes maliciosos se hace un llamado al caso de uso informar.	
Tipo	Esencial y primario	
Curso normal de los eventos	Acciones del Actor	
	1	Un paquete pasa por la red interna
	2	El sistema lo captura, lo analiza y decide no hacer nada
Curso alterno	Línea 2: El sistema considera que el paquete es maligno o malicioso, se ejecuta un llamado al caso de uso informar proporcionándole los datos necesarios para el informe.	

Tabla 5 Caso de Uso Informar

Informar			
Caso de uso	Informar		
Actores	Ninguno		
Propósito	Informar al administrador de los nuevos cambios que se han realizado y los errores que se han corregido		
Resumen	El sistema encuentra un tráfico peligroso, llama a este caso de uso con los datos necesarios para el informe, el cuál se realiza mediante correo electrónico y luego se genera una entrada en la bitácora correspondiente usando caso de uso crear bitácora.		
Tipo	Esencial y primario		
Curso normal de los eventos	Acción del Actor		Respuesta del Sistema
	1		Se genera un informe para ser enviado por correo electrónico
	2		Se envía el correo al administrador del sistema.
	3		Se llama al caso de uso generar bitácora

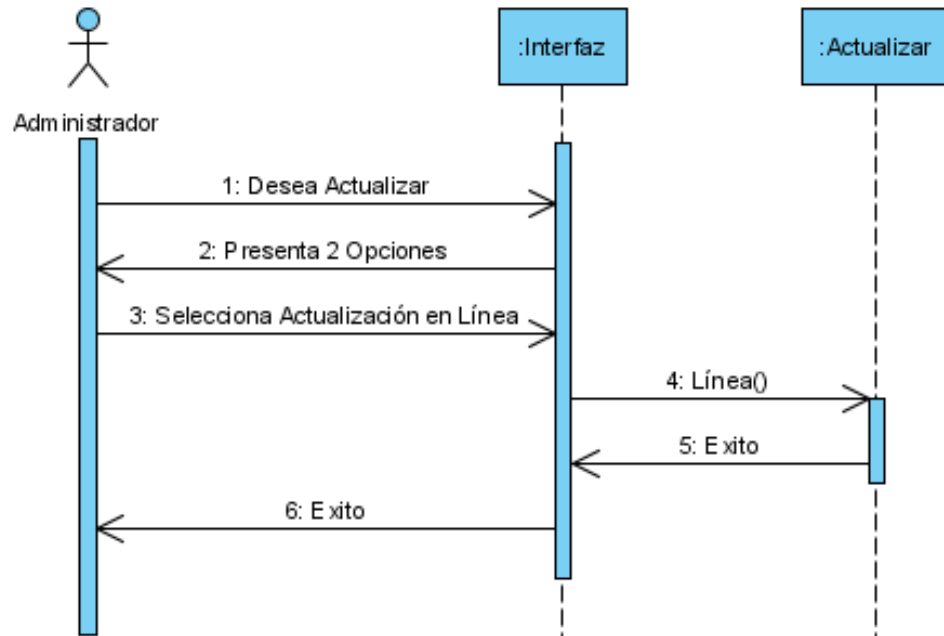
Curso alterno	Línea 2: No se puede enviar el correo, se reintenta la operación por 5 ocasiones más, si continúa el error se descarta la operación y se crea una bitácora
----------------------	---

Tabla 6 Caso de Uso Crear Bitácora

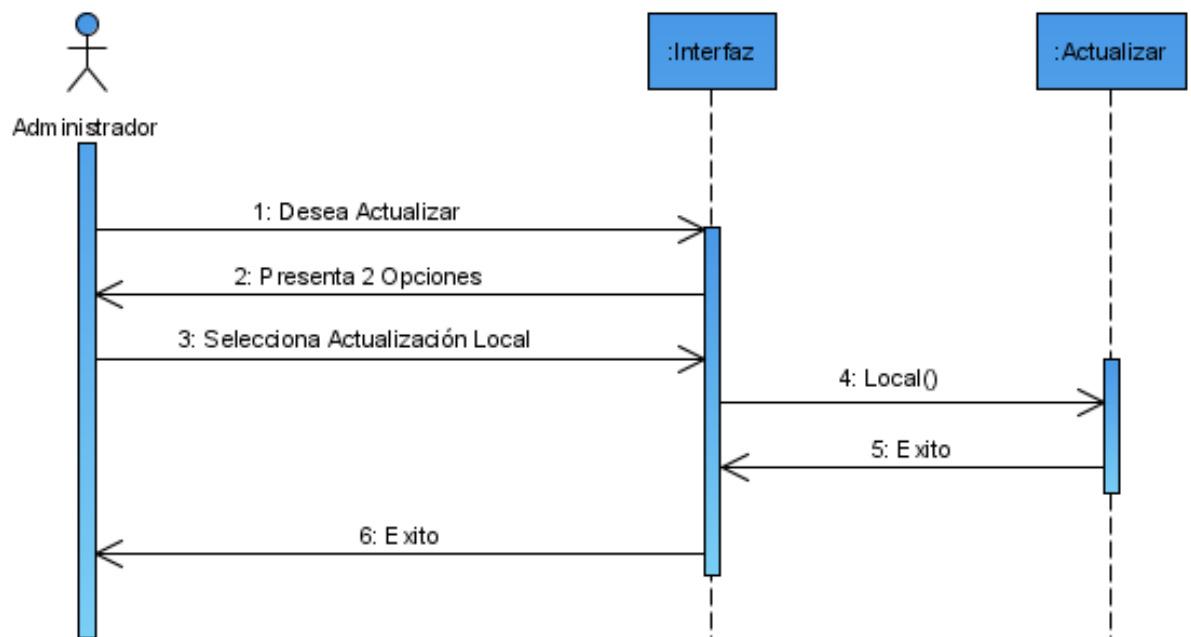
Crear Bitácora			
Caso de uso	Crear Bitácora		
Actores	Ninguno		
Propósito	Crear una bitácora que registra los eventos del sistema		
Resumen	El sistema después de cada evento relacionado con el análisis de paquetes genera una entrada en una bitácora para tener una trazabilidad del proceso. Las bitácoras se generan diariamente.		
Tipo	Esencial y primario		
Curso normal de los eventos	Acción del Actor		Respuesta del Sistema
	1		Se genera un evento en el sistema
	2		El sistema crea una entrada en la bitácora del día

4.1.3 Diagramas de Secuencia

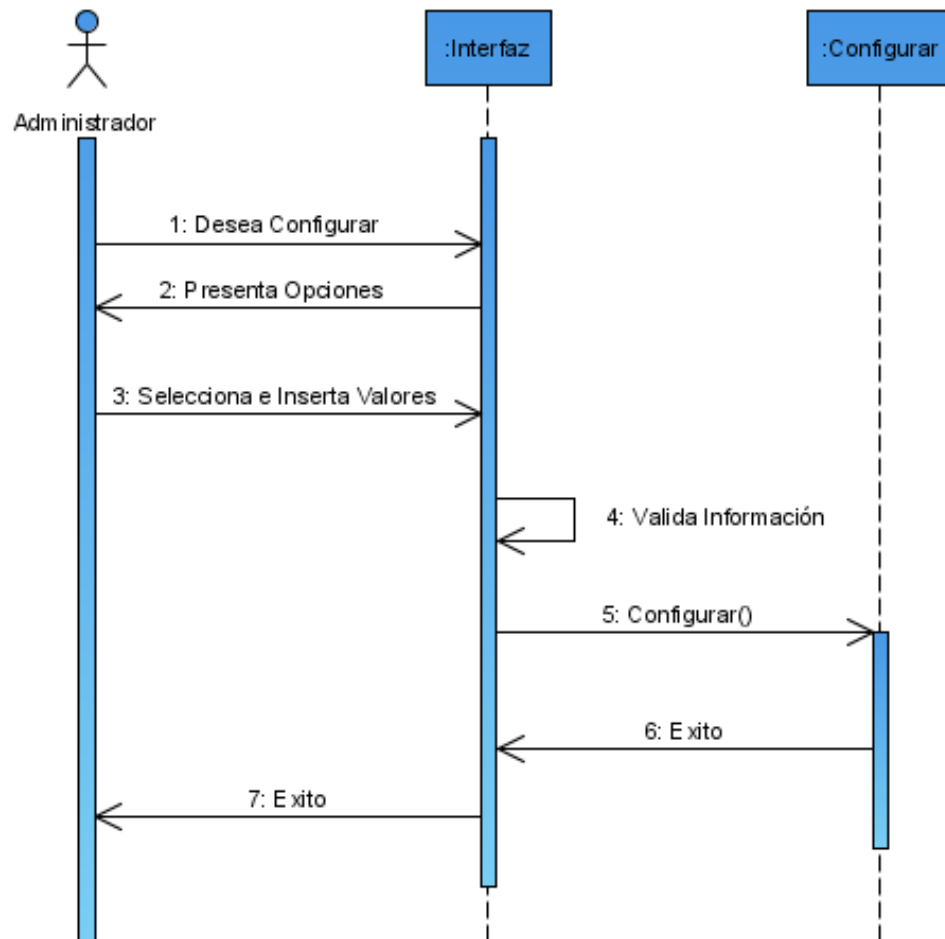
Gráfica 5 Caso de Uso Actualizar Escenario: Actualización en Línea Exitosa



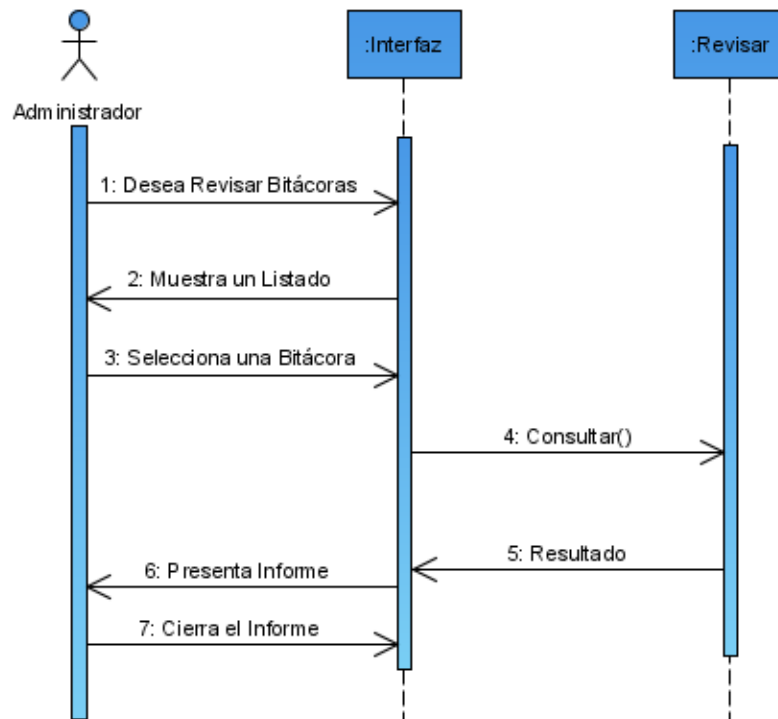
Gráfica 6 Caso de Uso Actualizar Escenario: Actualización Local Exitosa



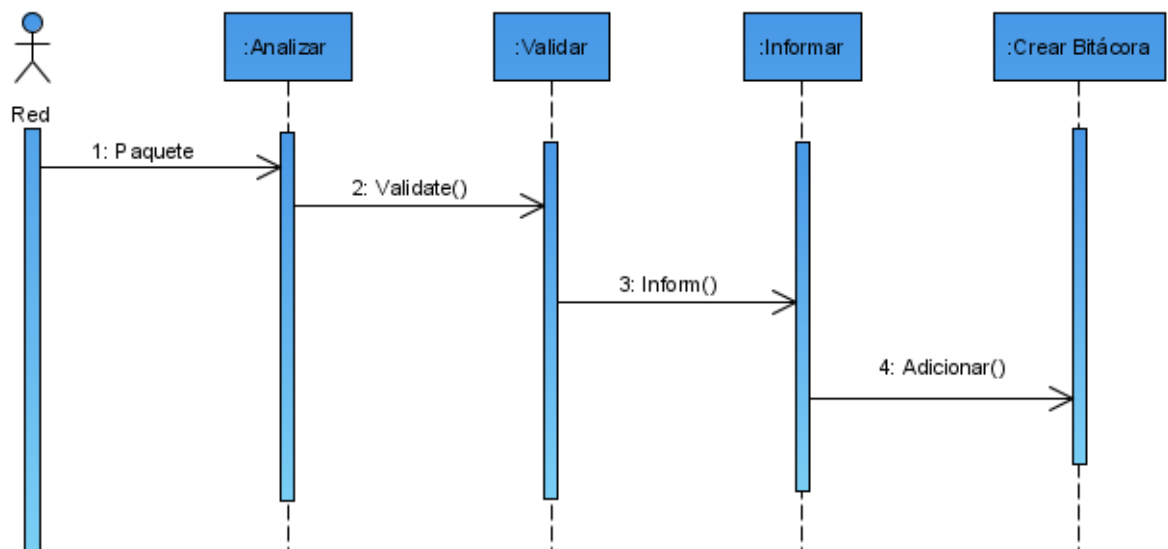
Gráfica 7 Caso de Uso Configurar Escenario: Configuración Exitosa



Gráfica 8 Caso de Uso Revisar Bitácoras Escenario: Consulta Exitosa

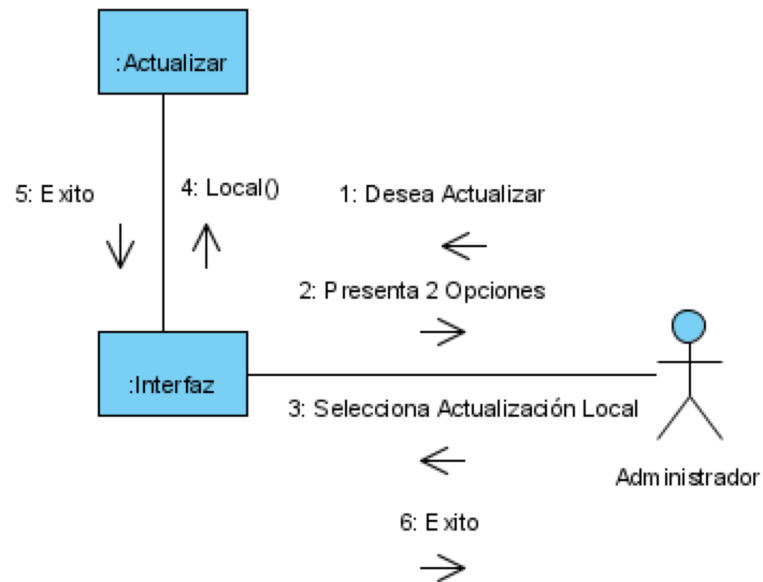


Gráfica 9 Caso de Uso Analizar Escenario: Paquete Malicioso

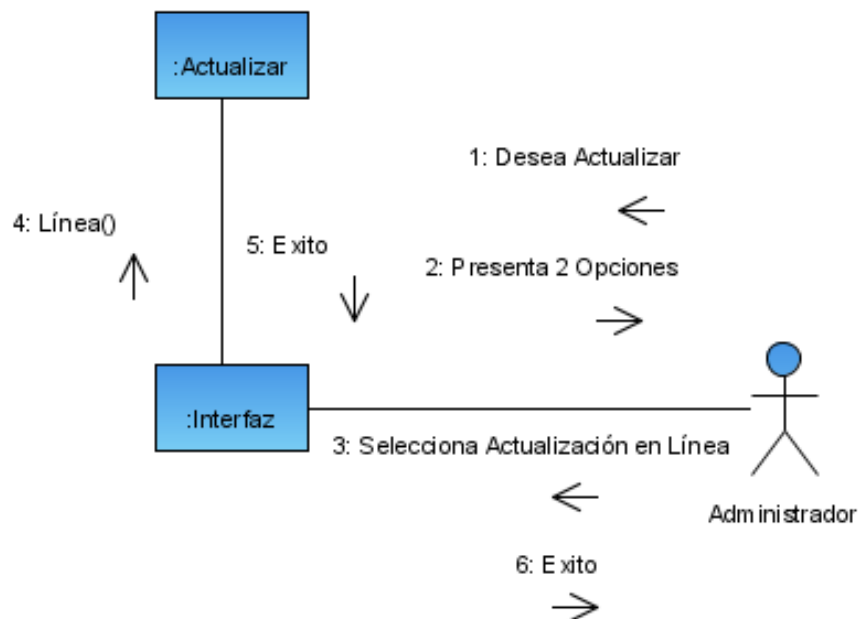


4.1.4 Diagramas de Colaboración

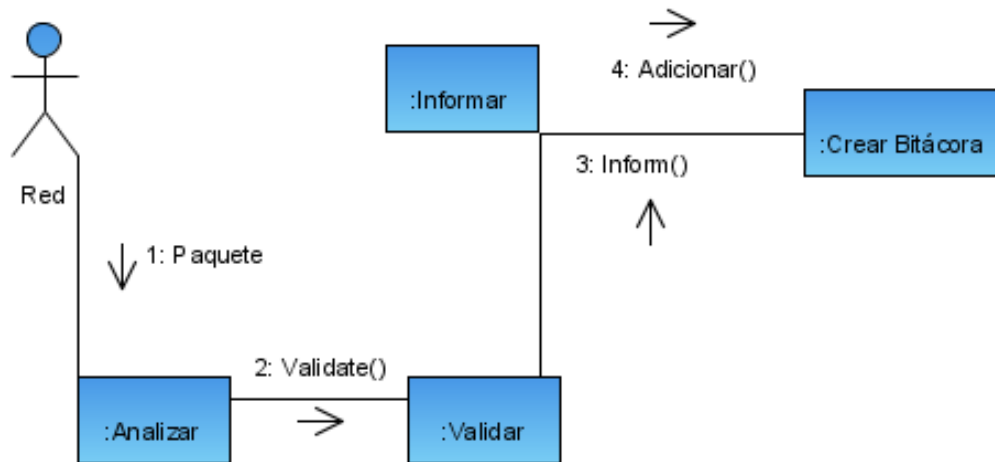
Gráfica 10 Caso de Uso Actualizar, Escenario Actualización Local



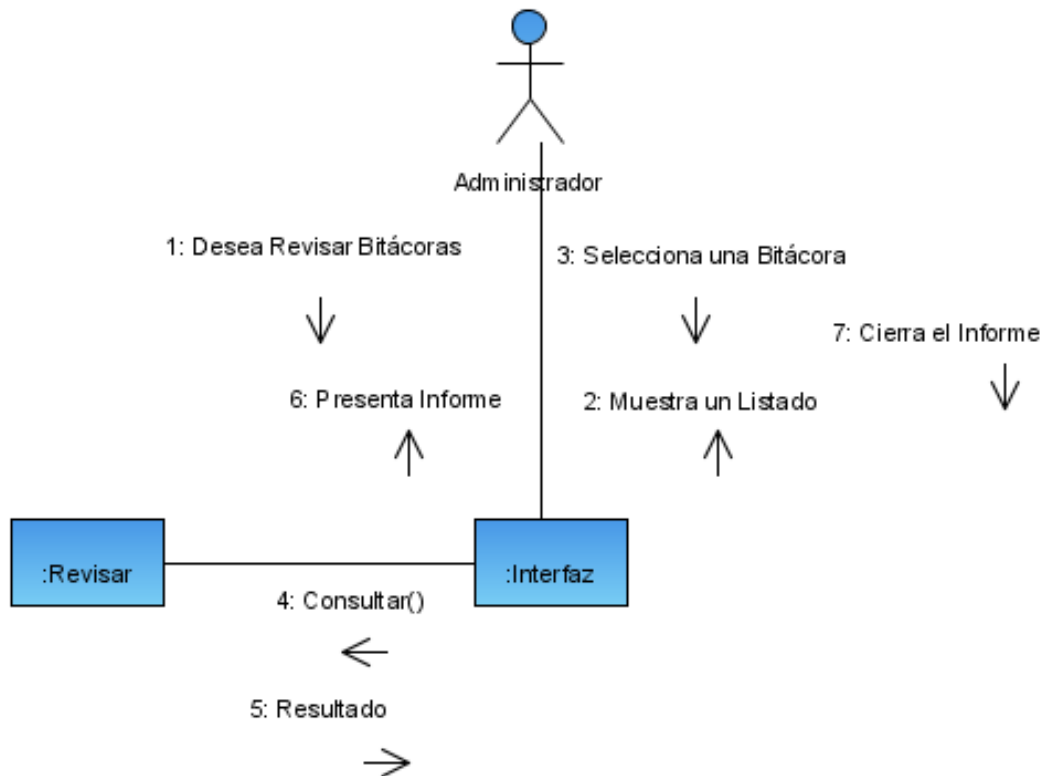
Gráfica 11 Caso de Uso Actualizar, Escenario Actualización en Línea



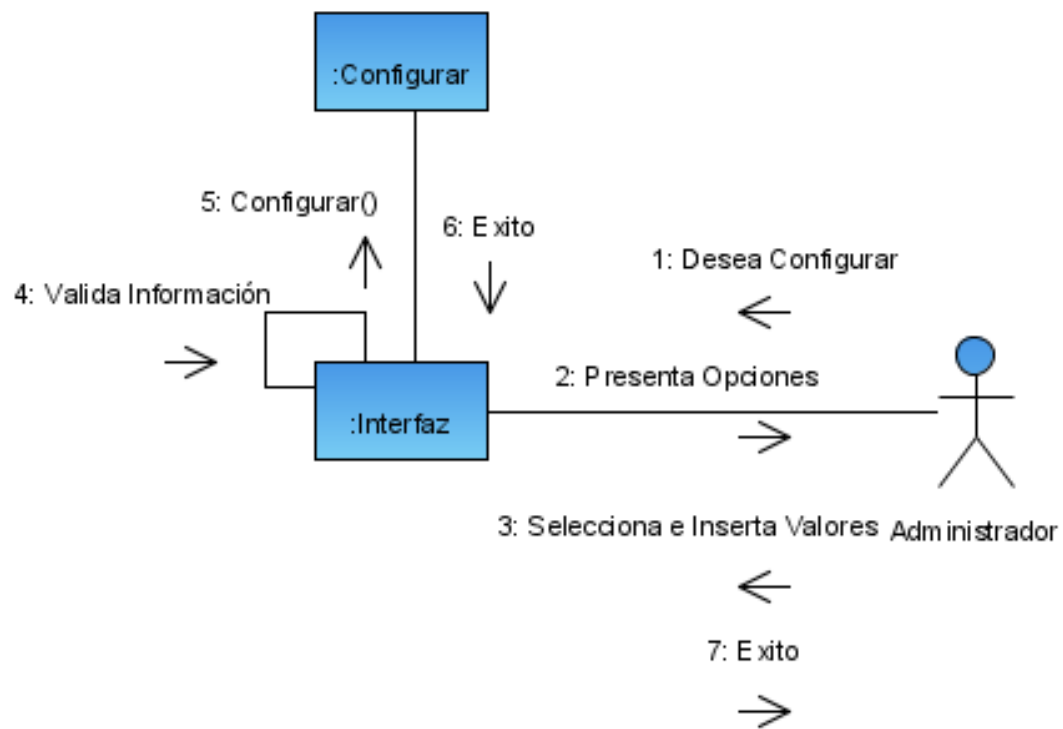
Gráfica 12 Caso de Uso Analizar



Gráfica 13 Caso de Uso Bitácoras



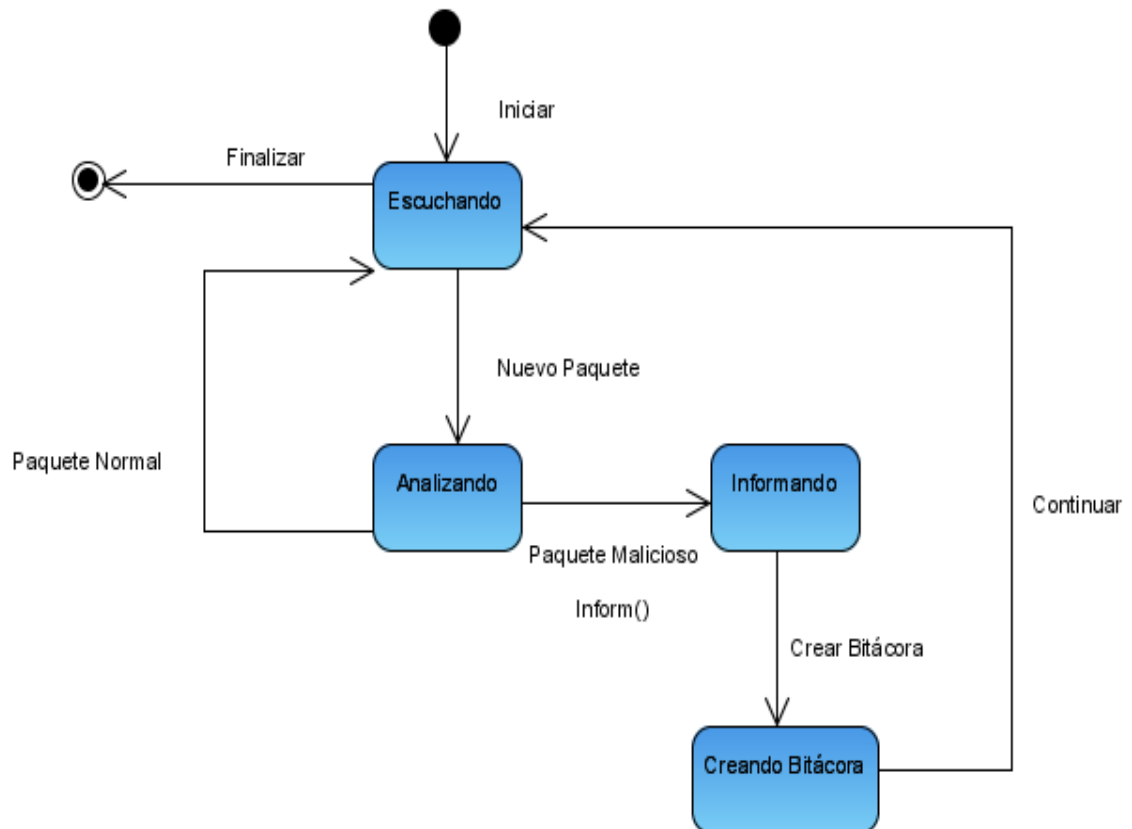
Gráfica 14 Caso de Uso Configurar



4.1.5 Diagrama de Estados

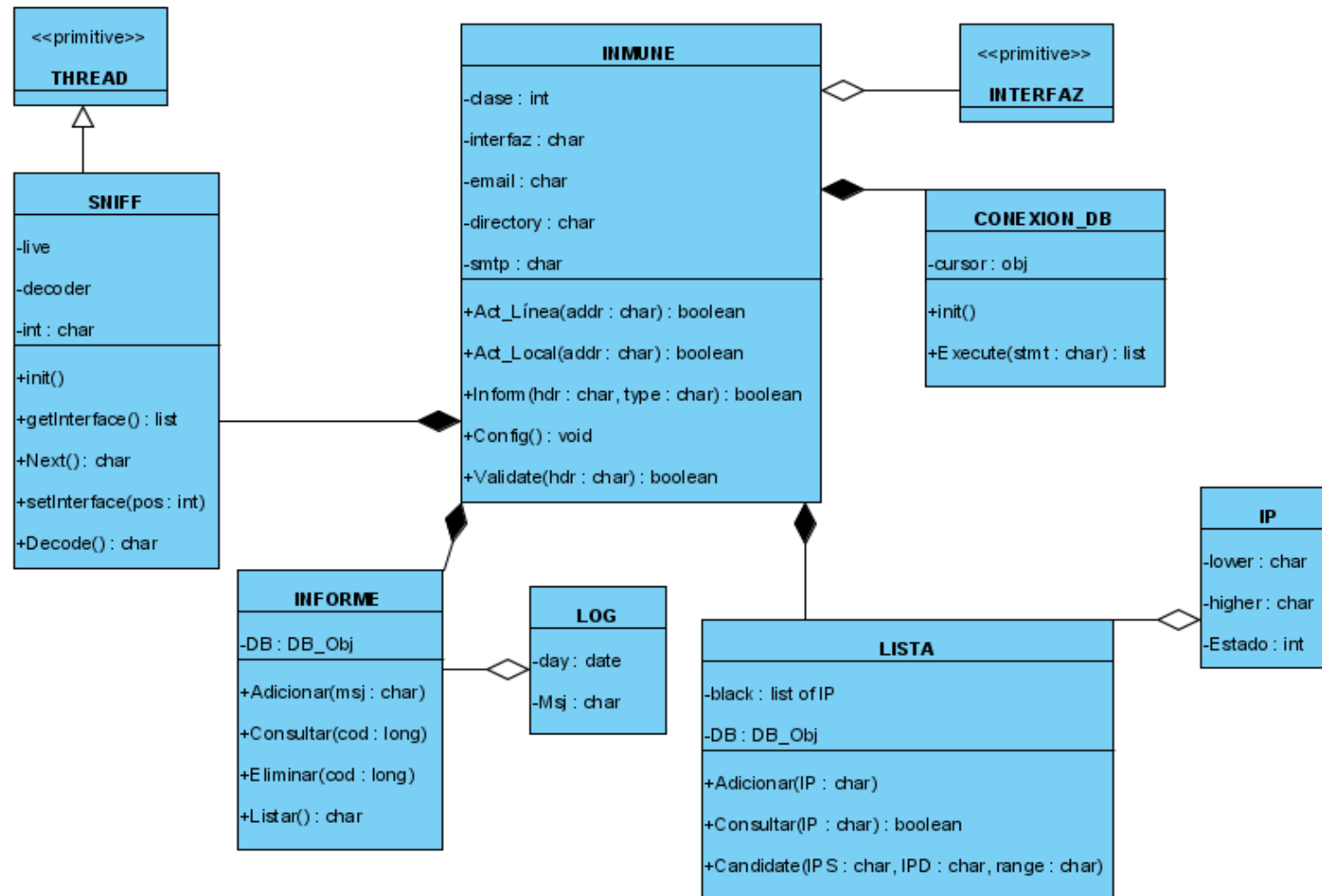
Sólo se modela el diagrama del caso de uso analizar por considerarse como el más relevante en la funcionalidad de la herramienta.

Gráfica 15 Diagrama de Transición de Estados Caso de Uso Analizar



4.1.6 Modelo de Clases

Gráfica 16 Diagrama de Clases



4.2 Etapa de Diseño Arquitectónico del Sistema

Se utilizó una arquitectura tipo monousuario para el desarrollo de esta herramienta.

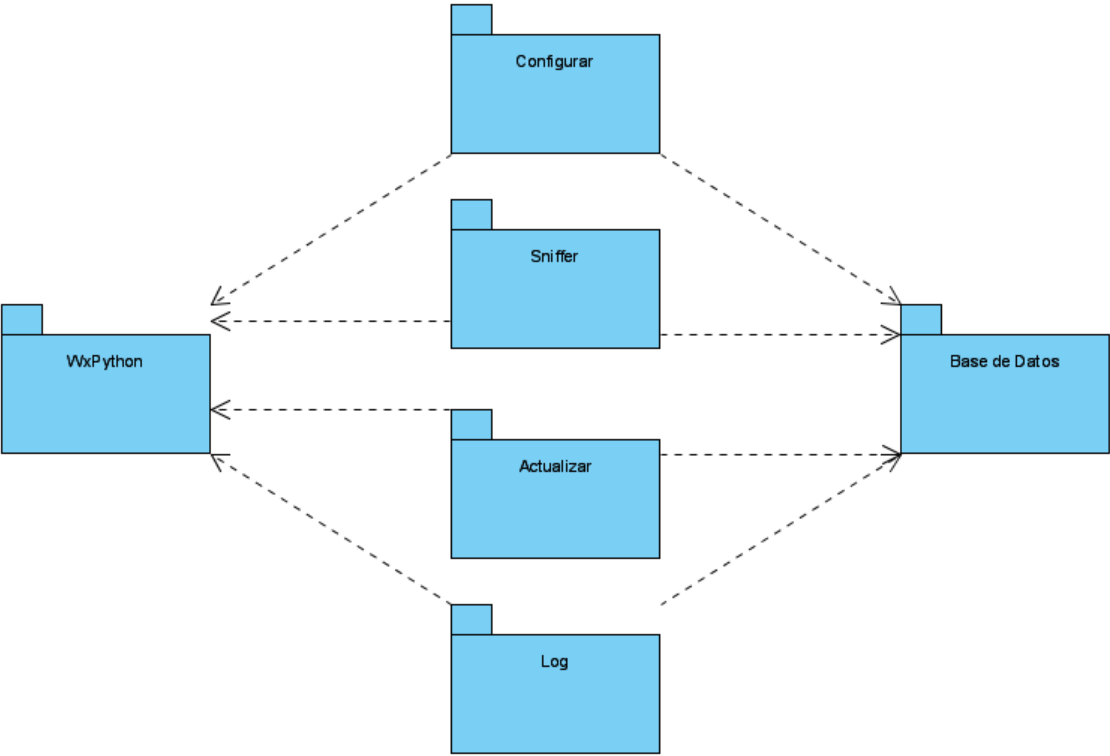
- **Hardware:** uno o más computadores, de acuerdo a la empresa que adquiera el software.
- **Redes y comunicaciones:** Este software se diseña para ser utilizado en una red de datos, por lo tanto el equipo o los equipos en que se instale deben estar conectados a la red, además, para el envío de los informes al administrador se debe disponer de acceso a Internet o un servidor de correo interno.
- **Sistema Operativo:** El software es multiplataforma, ha sido probado en distribuciones Windows, pero debido a la naturaleza de las herramienta de desarrollo funciona en cualquier plataforma que se desee instalar (GNU/Linux, Solaris, MacOS, etc.).
- **Herramienta para la interfaz hombre máquina:** se quiere desarrollar el software con interfaz amigable al usuario; se implementará el software utilizando el paquete de funciones gráficas de Python, cuyo nombre es wxPython.

Subsistemas

Subsistemas de Visualización

- **Librería de interfaces gráficas de usuario** es la librería que contiene los elementos gráficos tales como ventanas, botones, cajas de texto, cajas de chequeo, etc.
- **Aplicaciones** Es una interfaz de usuario que permite comunicarse con el sistema. Cada aplicación es un subsistema.

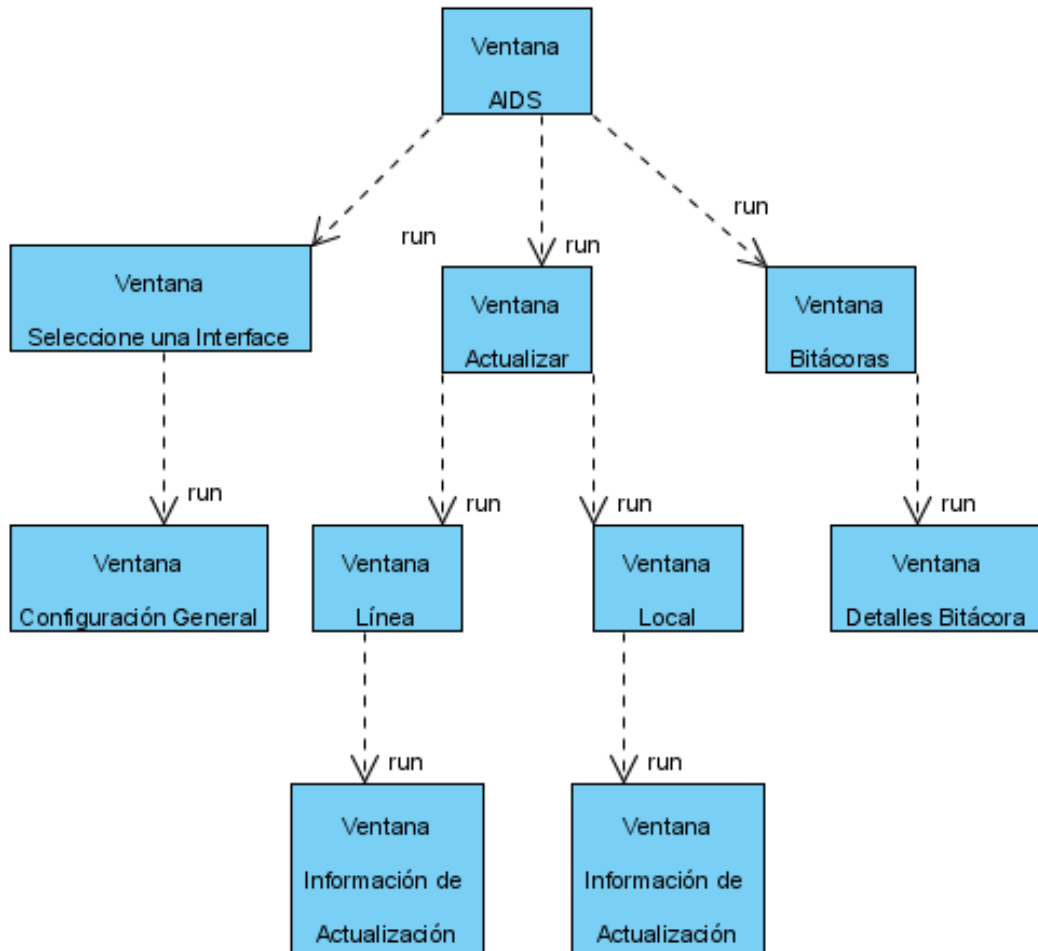
Gráfica 17 Diagrama de Subsistemas



Descripción de subsistemas de aplicación

- Diagrama de secuencia de ventanas

Gráfica 18 Secuencia de Ventanas desde la Ventana Principal



4.3 Diseño de Objetos

4.3.1 Herramientas de Desarrollo

Al igual que la herramienta resultante de este proyecto, el software a utilizar es software libre.

- **SVN**

Es un software de sistema de control de versiones diseñado específicamente para reemplazar al popular **CVS**, el cual posee varias deficiencias. Es software libre bajo una licencia de tipo Apache/BSD. Implementa un sistema de control de versiones que mantiene el registro de todo el trabajo y los cambios en la implementación de un proyecto (de programas) y permite que distintos desarrolladores (potencialmente situados a gran distancia) colaboren entre sí en la elaboración de proyectos en común. Se utilizará en este proyecto para llevar control de todos los cambios realizados en el producto durante toda su etapa de desarrollo y mantenimiento.

- **Python**

Python es un lenguaje de programación orientado a objetos y dinámico que puede ser usado para muchas clases de desarrollo de software. Ofrece un gran soporte para integración con otros lenguajes y herramientas, y viene con librerías estándar muy completas. Muchos programadores de Python reportan un sustancial aumento en la productividad y sienten que el lenguaje los anima a realizar desarrollos de alta calidad con un código más sencillo para realizarle mantenimiento. Python se puede ejecutar en Windows, Linux/Unix, Mac OS X, Amiga, Palm Handhelds y teléfonos móviles Nokia. También es portable en máquinas virtuales de Java y .NET.

Python es distribuido bajo una licencia de código libre aprobada por la OSI y es libre para usos comerciales en cualquier producto.

La herramienta será desarrollada en Python para aprovechar su alto grado de dinamismo, versatilidad, facilidad de mantenimiento y corto tiempo de desarrollo.

- **WxPython**

Es un **GUI toolkit** (conjunto de herramientas que permiten desarrollar Interfaces Gráficas de Usuario) para programación en lenguaje Python. Esta herramienta permite a los programadores de Python desarrollar programas robustos, con alta funcionalidad en interfaces gráficas de usuario de una manera simple. Está implementado como un módulo de extensión (código nativo) en Python, que envuelve la popular librería GUI **wxWidgets** (escrita en C++).

wxPython es de código abierto, lo cual permite realizar desarrollos sin restricciones y proporciona el código fuente para que los desarrolladores le hagan cambios y adaptaciones que crean necesarios para sus aplicaciones, o para resolver inconvenientes por ciertas posibles limitaciones. Es multiplataforma, lo cual permite ejecutar los programas en muchas plataformas sin realizar modificaciones.

Es soportado en plataformas Windows de 32 bits, en la mayoría de Unix y sistemas basados en Unix (como Linux), y Macintosh OS X.

En wxPython se desarrollará la interface gráfica para la administración del software.

- **SPE (Stani's Python Editor)**

Es un IDE (Entorno Integrado de Desarrollo) para Python con auto indentación, auto completado, tips de ayuda, coloreado de sintaxis, visor UML, explorador de clases, indexado de código fuente, buscador de archivos Python, ayuda. Este IDE corre en Windows, Linux y Mac OS X.

En este editor se desarrollará el producto junto con su interface gráfica ya que es un editor muy potente, liviano y gratuito.

- **Pcap**

Es un modulo de extensión de Python el cual interactúa con la librería de captura de paquetes libpcap. Pcap permite que desarrollos en Python puedan capturar paquetes en una red. Pcap es muy efectivo cuando se usa en conjunto con la librería para el manejo de paquetes Impacket, la cual es una colección de clases hechas en Python para construir y desmembrar paquetes de red.²⁸

- **Impacket**

Es una colección de clases hechas en Python enfocadas en proveer acceso a los paquetes de red. Impacket permite a los desarrolladores en Python capturar y decodificar paquetes de red, de una manera simple y consistente.

²⁸ CORE SECURITY TECHNOLOGIES. What is Pcap?. Disponible en Internet: <http://oss.coresecurity.com/projects/pcapy.html> [septiembre 2006]

Incluye soporte para protocolos de bajo nivel como IP, UDP, y TCP; al igual que para los protocolos de alto nivel como NMB y SMB.²⁹

- **Nemesis**

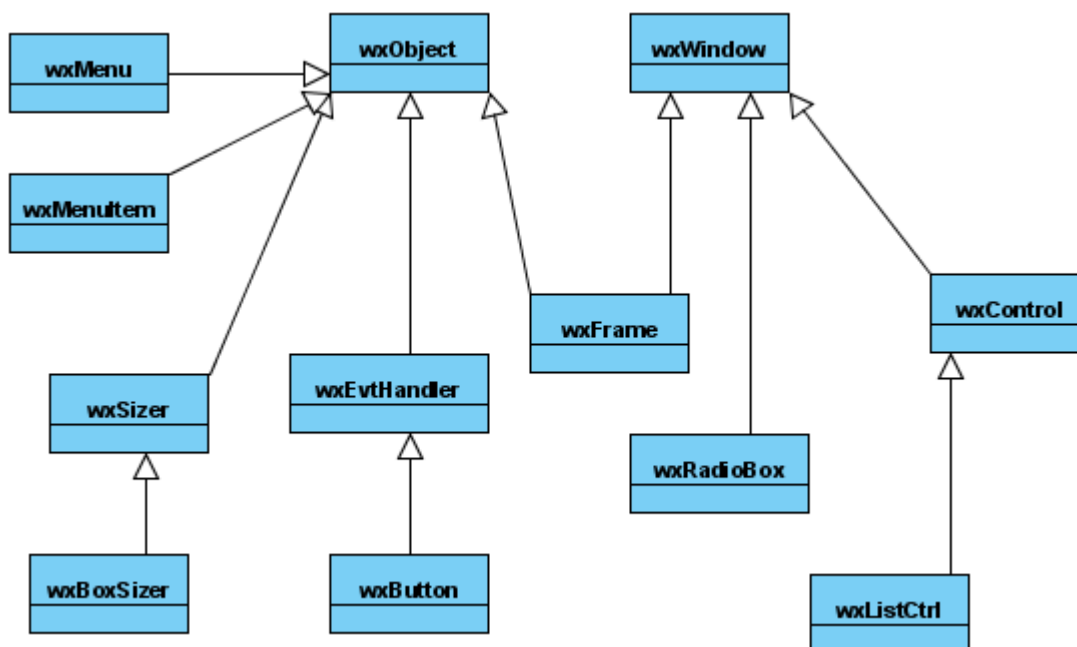
Es una herramienta que trabaja bajo línea de comandos y permite la creación e introducción de paquetes en la red, funciona en sistemas Windows y similares a Unix como GNU/Linux. Es una excelente herramienta para probar sistemas IDS, firewalls, entre otros. Al ser una herramienta de línea de comando es perfecta para trabajos por lotes.

Nemesis puede crear e inyectar paquetes de los siguientes protocolos: ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP y UDP. Casi cualquier paquete personalizado puede ser creado.³⁰

Por medio de esta herramienta de software se pretende probar el sistema inmune artificial generando un listado de paquetes corruptos para inyectarlos en la red y analizando la respuesta del sistema, con la respuesta esperada.

4.3.2 Ingeniería Inversa de las Herramientas

Gráfica 19 Diagrama de Clases wxPython

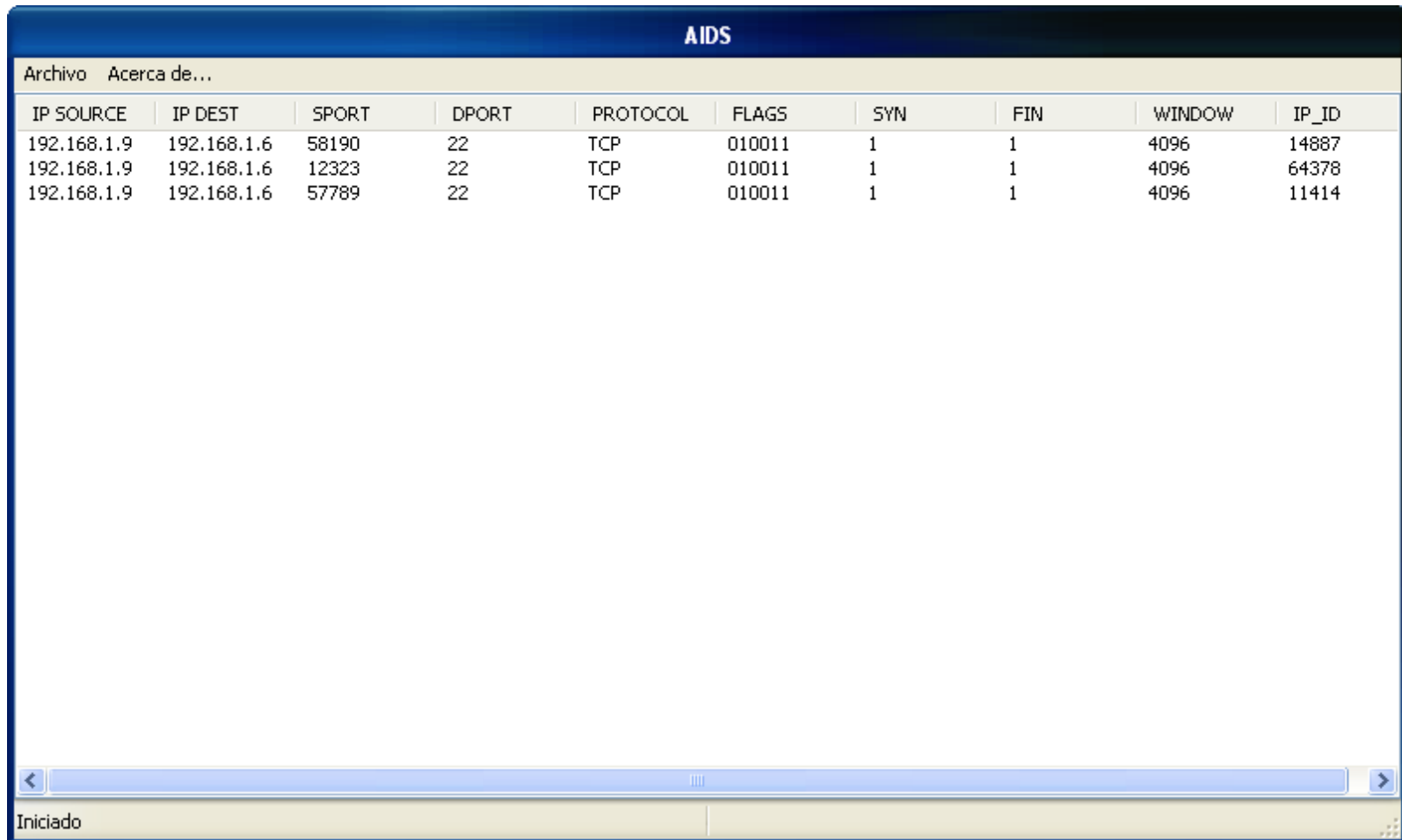


²⁹ CORE SECURITY TECHNOLOGIES. What is Impacket?. Disponible en Internet: <http://oss.coresecurity.com/projects/impacket.html> [septiembre 2006]

³⁰ NATAN, Jeff. Nemesis. Disponible en Internet: <http://nemesis.sourceforge.net/> [enero 2007]

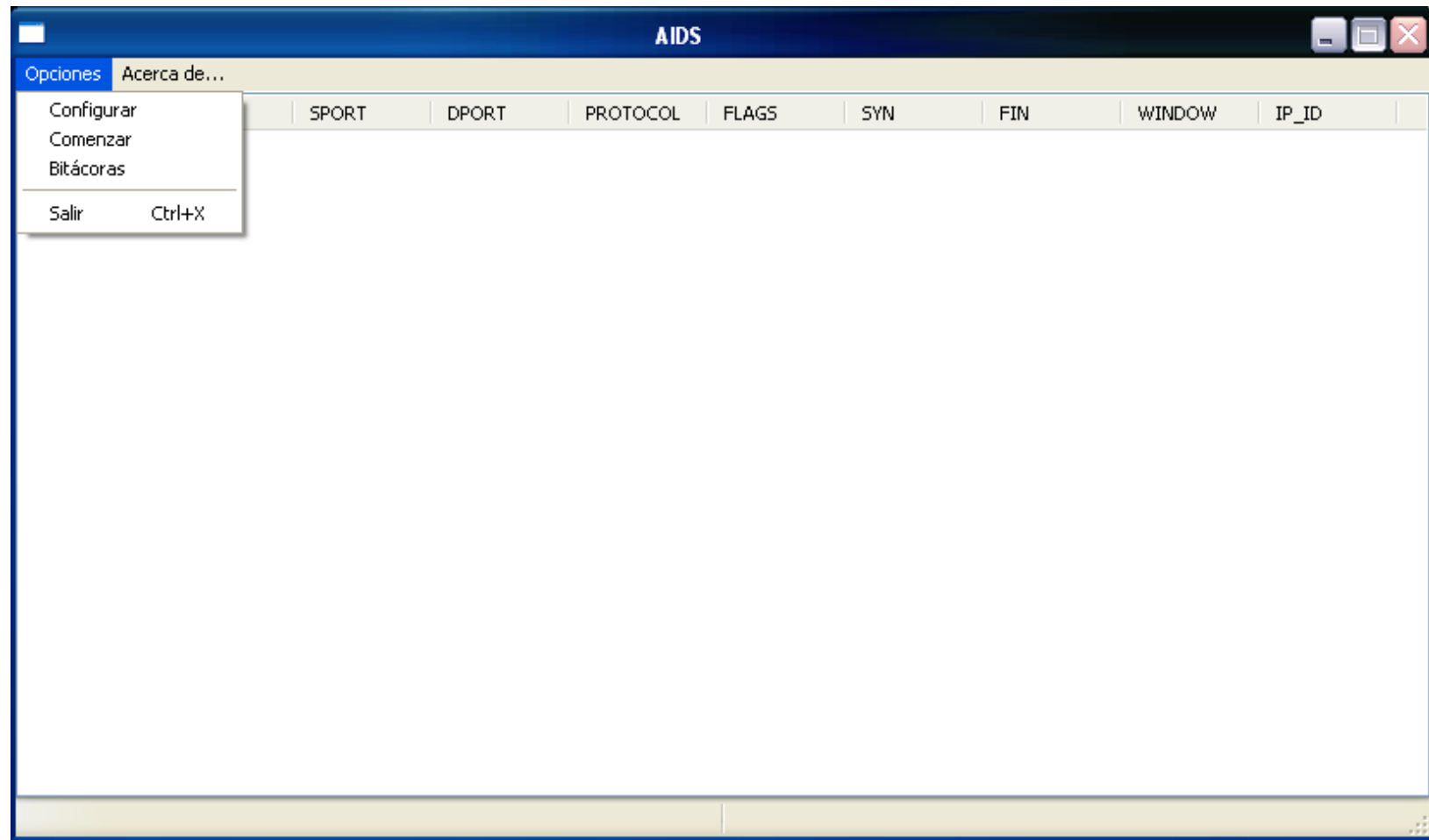
4.3.3 Interfaces Hombre-Máquina

Gráfica 20 Ventana Principal

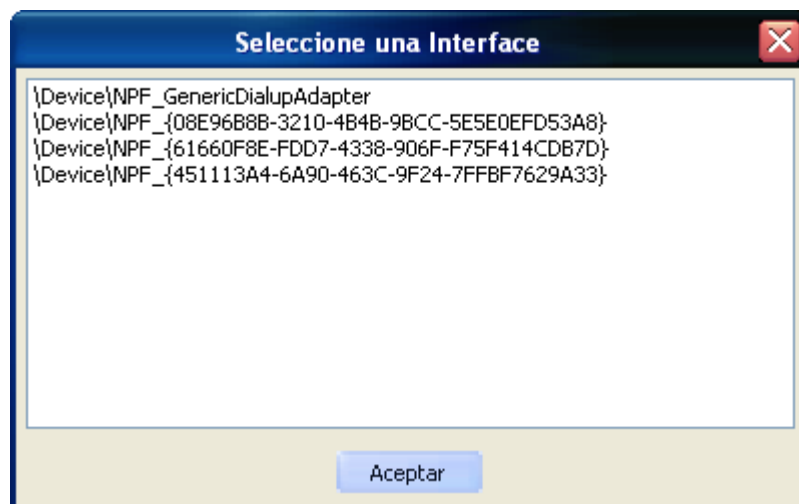


IP SOURCE	IP DEST	SPORT	DPORT	PROTOCOL	FLAGS	SYN	FIN	WINDOW	IP_ID
192.168.1.9	192.168.1.6	58190	22	TCP	010011	1	1	4096	14887
192.168.1.9	192.168.1.6	12323	22	TCP	010011	1	1	4096	64378
192.168.1.9	192.168.1.6	57789	22	TCP	010011	1	1	4096	11414

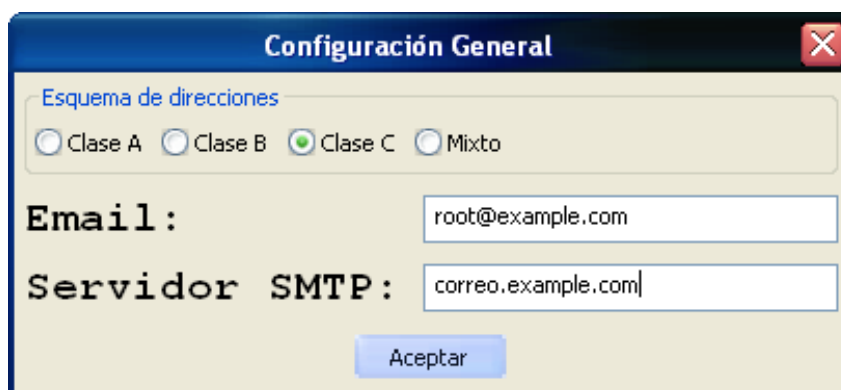
Gráfica 21 Opciones de la Ventana Principal



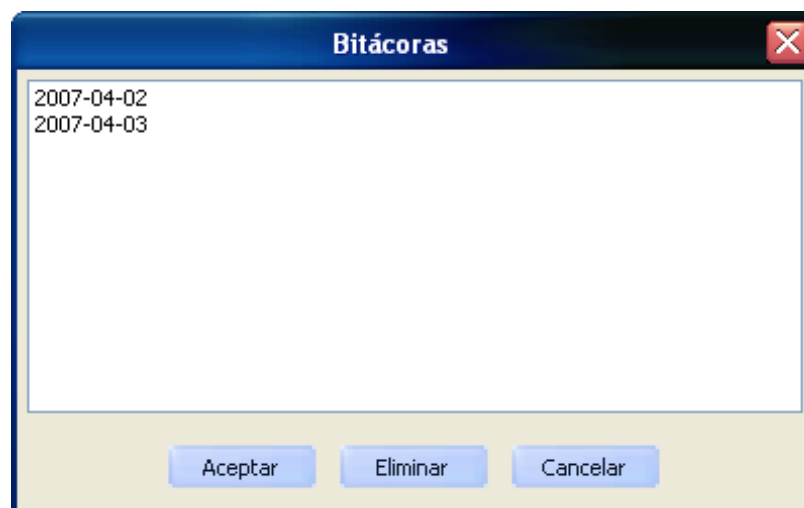
Gráfica 22 Selección de Interfaz



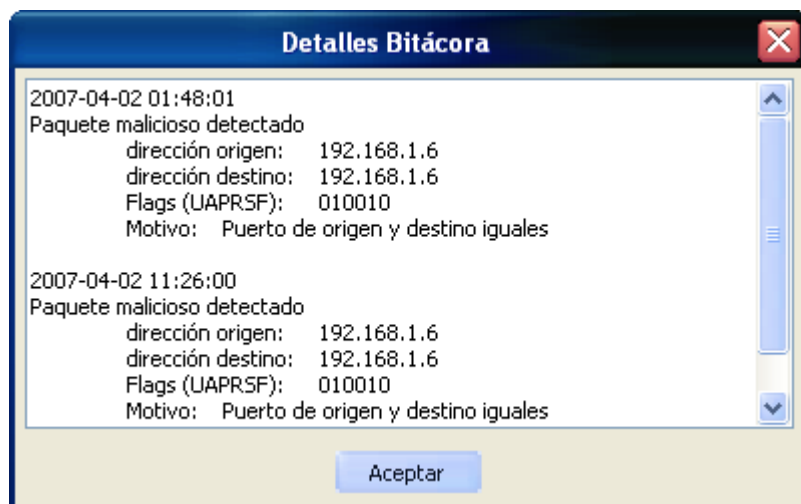
Gráfica 23 Configuración General



Gráfica 24 Listado de Bitácoras

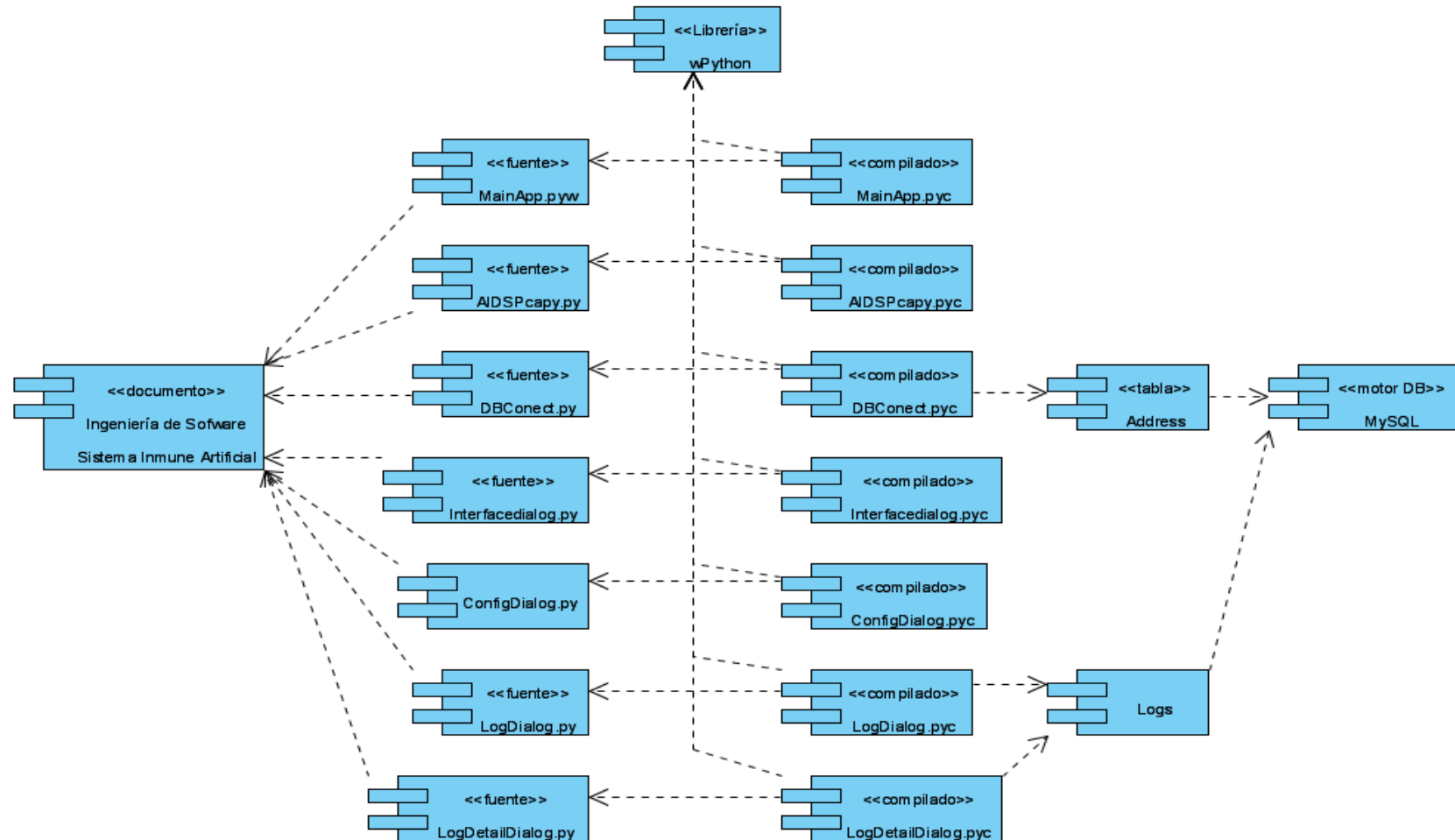


Gráfica 25 Detalles de una Bitácora



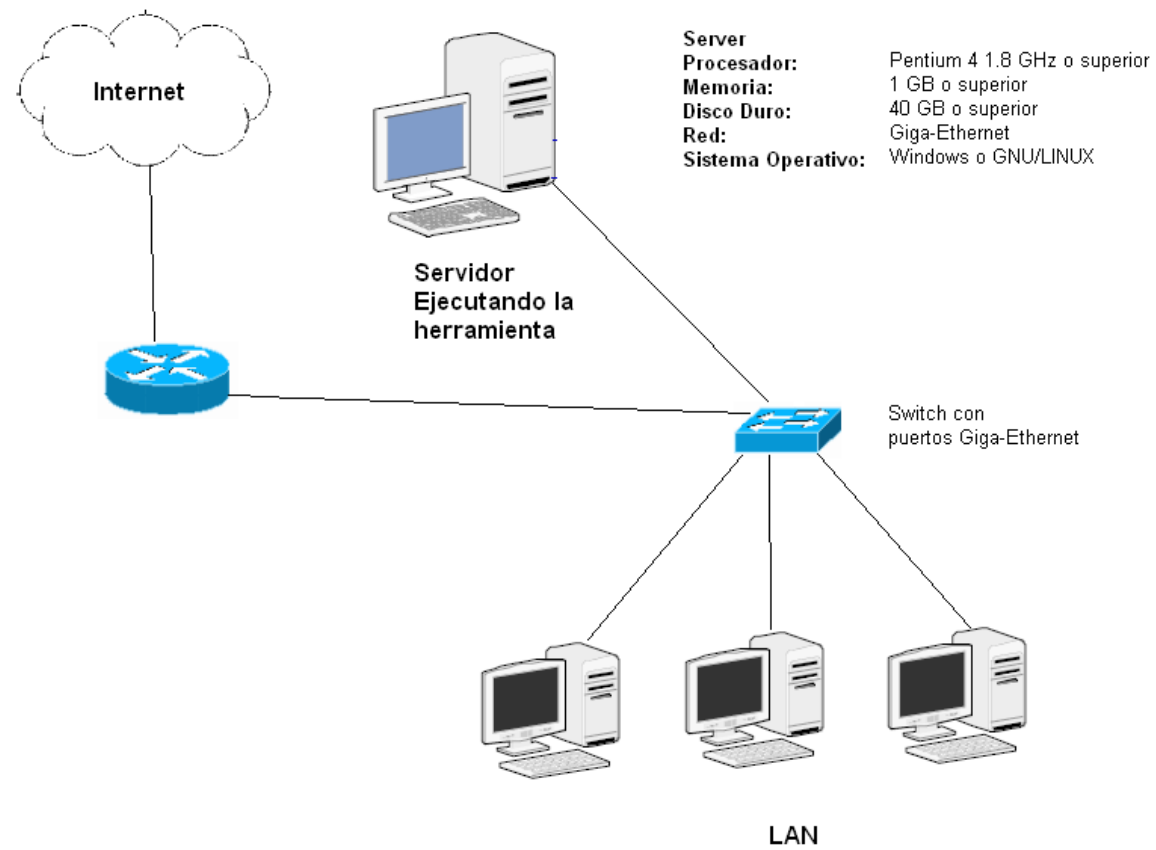
4.3.4 Modelo de Componentes

Gráfica 26 Diagrama de Componentes del Sistema



4.3.5 Modelo de Distribución

Gráfica 27 Ejemplo de Distribución para la Ubicación de la Herramienta



5 DIFICULTADES ENCONTRADAS

Durante la realización de este proyecto se encontraron las siguientes dificultades:

La herramienta encontrada para realizar las pruebas requiere versiones antiguas de las librerías que se utilizaron en el desarrollo e implementación de la herramienta, y ambas son incompatibles por lo tanto se necesitó de una máquina externa para realizar las pruebas con sus respectivas versiones. Esto a la larga no es un problema porque se pudo comprobar que la herramienta realmente funcionaba en un ambiente real.

La poca documentación y desarrollos existentes en cuanto a los sistemas inmunes artificiales enfocados a la seguridad de redes se refiere. Se encontró suficiente documentación de la base teórica de dichos sistemas enfocada a resolución de problemas en general, el funcionamiento del sistema inmune natural y que aspectos eran deseables de éste último sistema.

La documentación de las librerías utilizadas en el desarrollo se encuentran muy incompletas y sólo muestran ejemplos generales para el uso de las mismas, en caso de requerirse un poco más de detalle para el uso de estas librerías en programador debe estudiar el código fuente, pero gracias a que este código está disponible para los usuarios se pudo lograr un estudio más profundo de ellas.

6 APORTES

Se realizó el análisis y diseño de una herramienta de software basada en sistemas inmunes artificiales para la seguridad en redes.

Se implementó dicha herramienta utilizando software libre, y este resultado también pertenecerá a esta comunidad, ya que es deseo del realizador que se siga desarrollando esta cultura, además de la herramienta, recibiendo aportes de personas con otras habilidades en el campo del desarrollo e implementación de software.

Se documentó por completo la herramienta, generándose los manuales de usuario final, técnico y de pruebas, dichos documentos se anexan a este proyecto, y se empaquetaran con el código fuente de la herramienta para ser distribuido a través de Internet.

Se demostró que es posible llegar a una solución de seguridad informática utilizando el paradigma de acción de sistemas inmunes artificiales.

Se plantearon desarrollos futuros para complementar esta herramienta, estos desarrollos pueden ser considerados como proyectos de grado para generaciones venideras.

Se impulsó el desarrollo local y regional en nuevos paradigmas de resolución de problemas referentes a la seguridad en redes.

Se redactó un artículo que expone de una manera breve y clara las ideas principales de la herramienta, así como los fundamentos del desarrollo de dicha solución. Este artículo se postula como artículo científico en varios lugares, uno de ellos la revista Scientia et Technica perteneciente a la Universidad Tecnológica de Pereira, buscando un mayor reconocimiento a nivel nacional y global.

7 CONCLUSIONES

Se determinaron los elementos relevantes de los sistemas inmunes artificiales que apoyaron el desarrollo de la herramienta.

Se documentó el proceso de análisis y diseño de una herramienta basada en sistemas inmunes artificiales para la seguridad en redes, utilizando una metodología orientada a objetos.

Se describió el estado del arte de los sistemas inmunes artificiales para la resolución de ciertos problemas.

Se realizó la implementación de la herramienta en sus etapas básicas utilizando software libre y orientado a objetos. Mostrando gran funcionalidad.

Se validó el sistema mediante pruebas de funcionamiento de caja negra y en un ambiente real controlado.

Se realizaron pruebas comparativas de la efectividad de la herramienta usando **datos presentados por DARPA en**

Se elaboró la documentación de usuario final, para que cualquier administrador de una red pueda llegar a implantar la herramienta de forma exitosa.

Se elaboró el manual técnico de la herramienta así como el manual de pruebas de caja negra.

Se plantean los siguientes desarrollos futuros:

- Implementación del módulo de actualización ya sea en línea o local, consulta a bases de datos de listas negras de direcciones IP a través de Internet, y realizar aportes a dichas listas dependiendo del resultado de la herramienta.
- Sincronización de la herramienta en una empresa con otra a través de la red y/o a través de medios removibles.
- Análisis de otros protocolos para construir una herramienta más robusta y eficaz.

- Análisis de la carga (payload) de cada paquete para adicionar a la herramienta funcionalidad como anti-virus y anti-spam.
- Implementación de un módulo de interface con un firewall, el cual permitirá a la herramienta interactuar con el firewall que posee la empresa y/o uno adicional que se puede generar con el uso de IPTABLES en un ambiente GNU/LINUX. Así, en caso de que se detecte una anomalía impedir el tráfico detectado mediante una nueva regla en el firewall.
- Aplicar nuevos modelos aprendidos de un sistema inmune, por ejemplo la distribución, tener la herramienta no centralizada sino distribuida en la red.
- Aplicar el modelo de agentes que viajan por la red en busca de paquetes, así como lo hacen los linfocitos en el sistema inmune natural.
- Elaborar la documentación detallada de las librerías utilizadas, como son Pcap y Impacket, las cuales cuentan con muy poco detalle en su publicación oficial.
- Implementar un sistema de encriptamiento para la información almacenada en los archivos de configuración, con lo cual se puede además complementar el envío de correos electrónicos con autenticación por parte del servidor.

8 BIBLIOGRAFÍA

- CALDER, Alan. Nueve Claves Para El Éxito, Una visión general de la implementación de la norma NTC-ISO/IEC 27001. ICONTEC, 2006, 128 p. ISBN 958-9383-62-9.
- CISCO NETWORKING ACADEMY PROGRAM (En línea), CCNA Curriculum Version 3.1, <http://cisco.netacad.net>.
- CORE SECURITY TECHNOLOGIES; herramientas Pcap y Impacket: <http://oss.coresecurity.com>.
- CUFF, Andy; Intrusion Detection Terminology, September 03 2003, <http://www.securityfocus.com/infocus/1728>.
- EISEN DP, MINCINTON RM (traducción en línea); <http://www.ucm.es/info/fmed/medicina.edu/Infecciones/mbl.htm>. artículo original en: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&list_uids=14614673&dopt=Abstract.
- HOW STUFF WORKS (En línea); Health Stuff, How Your Immune Systems Works (<http://health.howstuffworks.com/immune-system.htm>).
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tesis y otros trabajos de grado 2004-2005. Santafé de Bogotá: ICONTEC.
- KENT FREDERICK, Karen (En Línea); Network Intrusion Detection Signatures, Part One, December 19, 2001, <http://www.securityfocus.com/infocus/1524>, Part Two, January 22, 2002, <http://www.securityfocus.com/infocus/1534>, Part Three, February 19, 2002, <http://www.securityfocus.com/infocus/1544>.
- KENT FREDERICK, Karen (En Línea); Abnormal IP Packets, November 13 2000, <http://www.securityfocus.com/infocus/1200>.
- FORREST, Stephanie. HOFMEYER, Steven. SOMAYAJI, Anil. Principles of a Computer Immune System. 1997 New Security Paradigms Workshop, pp. 75-82, ACM (1998).

- POSTEL, J., "Transmission Control Protocol - DARPA Internet Program Protocol Specification", STD 7, RFC 793, USC/Information Sciences Institute, September 1981
- PYTHON (En línea); <http://www.python.org/doc/>.
- SCHOOLSCIENCE (En línea); Human Inmune System <http://www.schoolscience.co.uk/content/4/biology/abpi/immune/index.html>.
- VARIOS AUTORES, (En Línea); Computer Science Department, Unversity of New Mexico, <http://www.cs.unm.edu/~immsec/papers.htm>.
- WIKIPEDIA (En línea); <http://es.wikipedia.org>, <http://wikipedia.org>.
- WXPYTHON (En línea); [http:// http://www.wxpython.org/online/docs.php](http://http://www.wxpython.org/online/docs.php).

ANEXO A. CÓDIGO FUENTE DOCUMENTADO

MainApp.pyw:

InterfaceDialog.py:

AIDSPcapy.py:

ConfigDialog.py:

LogDialog.py:

LogDetailDialog.py:

DBConect.py:

ANEXO B. MANUAL DE USUARIO

Requisitos Software:

- Python 2.3 o superior
- Winpcap 3.1 o superior (Windows), Libpcap 0.8.3 o superior (GNU/Linux)
- Librería Pcap
- Librería Impacket
- Librería wxPython 2.8.3 o superior
- Base de Datos MySQL
- Librería MySQLdb
- Servidor de correo (smtp), indispensable para el envío de informes mediante este sistema

Requisitos Hardware:

- Tarjeta de red que soporte modo promiscuo
- 256 MB RAM

Ejecución de la herramienta:

Luego de cumplir con los requisitos antes mencionados se debe configurar la base de datos para el almacenamiento de la información relevante. Se siguen los siguientes pasos.

Crear una base de datos llamada 'AIDS', respetando las letras mayúsculas así: `create database AIDS` o utilizando una herramienta gráfica diseñada para este fin, luego un usuario llamado 'admais' deberá tener todos los permisos en dicha base de datos, esto se logra con el comando: `grant all privileges on AIDS.* to 'admais'@'%' identified by 'admARIS'.`

Una vez concluidas estas operaciones se procede a la ejecución de la herramienta utilizando el archivo ejecutable MainApp.pyw. En caso de que el administrador desee utilizar nombres y contraseñas diferentes a los propuestos en este documento, se deben modificar dichos campos el archivo DBConect.py, para que la herramienta pueda reconocer los valores cambiados.

De igual forma se debe modificar el archivo antes mencionado en caso de que la base de datos sea ejecutada en un equipo diferente al equipo dónde se esta configurando la herramienta, cambiando el campo de host con la dirección IP o, en caso de que se disponga de un equipo DNS, con el nombre del equipo servidor de bases de datos.

La primera vez que se ejecute el sistema inmune artificial aparece una ventana, la cual es usada para seleccionar de la lista mostrada la interface de red que se desea utilizar para la captura de los paquetes.

Una vez realizada esta selección se prosigue con el proceso de configuración seleccionando, de la ventana siguiente, la clase de esquemas de direcciones que posee la empresa, ej: clase A rango 10.0.0.0 a 10.255.255.255, clase C 192.168.0.0, o mixta si la empresa posee un tipo de direccionamiento mixto ej: direcciones clase B para servidores y clase A para los demás usuario.

Luego se escribe el correo electrónico del administrador al cual llegaran los informes de los paquetes marcados como maliciosos por la herramienta y además el nombre del equipo servidor de correo (por defecto se utilizará el equipo local).

Por último, es necesario configurar el servidor de correo de la empresa para que permita al equipo dónde se encuentre instalado el sistema inmune artificial enviar correos; para esta versión de la herramienta se necesita que dicho servidor no use autenticación. La configuración de un servidor de correos escapa del fin de este manual, pero se recomienda al lector la siguiente página para instalar y configurar dicho servicio. <http://www.postfix.org/>

Una vez terminado este proceso la herramienta ha quedado configurada y se puede comenzar a utilizar.

Usando la herramienta:

En el menú Opciones se encuentra un acceso llamado Comenzar, el cual da inicio al funcionamiento de la herramienta. Se puede observar el estado de la de la misma en la barra de estado. De igual forma para detener el escaneo de paquetes, en el menú Opciones se selecciona Detener.

Cuando un paquete es detectado por el sistema en la ventana principal aparecerán las características más relevantes de dicho paquete como son: la dirección IP de origen y destino, los puertos de origen y destino, el tipo de protocolo, para esta versión de la herramienta sólo se tendrá en cuenta el protocolo TCP, la combinación de las banderas, el estado de las banderas de

sincronización y finalización, el tamaño de la ventana y el identificador del paquete.

Modificando la herramienta:

Para modificar alguna parte de la configuración, ej: el esquema de direcciones cambió, el administrador quiere cambiar de correo electrónico de informes, cambiar el directorio de los archivos log o la interface de red activa. El administrador podrá acceder a esta información mediante el menú Opciones en el cual se encuentra el acceso a ella con el nombre de Configurar.

Revisando las bitácoras:

Para revisar las bitácoras generadas por la herramienta el administrador debe utilizar el menú Opciones -> Bitácoras, desde el cual aparecerá una ventana con un listado de las bitácoras generadas diariamente, allí podrá seleccionar una para ver más detalladamente el comportamiento de la red en ese día.

Eliminando una bitácora:

Para eliminar una bitácora el administrador debe estar situado en el listado general de logs, dese allí él podrá marcar una bitácora y presionar el botón de eliminar, para eliminar esta bitácora del sistema.

NOTA: Una vez eliminada una bitácora, no es posible su recuperación.

ANEXO C. MANUAL DE PRUEBAS

En las tablas siguientes se pretende mostrar el comportamiento de la herramienta a ciertos estímulos por parte de los actores que interactúan con ella, como lo son el administrador del sistema o usuario y la red.

Para la realización de las pruebas se utilizó la herramienta nemesys, con la cual fue posible la construcción de los paquetes personalizados necesarios.

- Resultado de las pruebas realizadas al sistema inmune artificial:

Caso de Prueba	Elemento	Entrada	Salida Esperada	Salida Obtenida
Paquete normal escaneado	Un paquete capturado es normal	Paquete normal	Ninguna	Ninguna
Paquete malicioso escaneado, tipo 1	Ingreso de paquete con banderas FIN y SYN activas	Paquete FIN y SYN	Descomposición del paquete, correo electrónico, entrada en la base de datos	Descomposición del paquete, correo electrónico, entrada en la base de datos
Paquete malicioso escaneado, tipo 2	Ingreso de paquete con puertos de origen y destino iguales	Paquete con puertos de origen y destino iguales	Descomposición del paquete, correo electrónico, entrada en la base de datos	Descomposición del paquete, correo electrónico, entrada en la base de datos
Paquete malicioso escaneado, tipo 3	Ingreso de paquete con direcciones de origen y destino iguales	Paquete con direcciones de origen y destino iguales	Descomposición del paquete, correo electrónico, entrada en la base de datos	Descomposición del paquete, correo electrónico, entrada en la base de datos
Paquete malicioso escaneados, tipo 4.1 (estado fuera de rango)	Ingreso de paquete con dirección origen o destino en lista negra	Paquete con dirección origen o destino en lista negra	Descomposición del paquete, correo electrónico, entrada en la base de datos	Descomposición del paquete, correo electrónico, entrada en la base de datos

Paquete malicioso escaneado, tipo 4.2 (estado dentro de rango)	Ingreso de paquete con dirección origen o destino en lista negra	Ingreso de paquete con dirección origen o destino en lista negra	Aumento en el contador de estado	Aumento en el contador de estado
--	--	--	----------------------------------	----------------------------------

- Resultado de las pruebas realizadas a la interfaz de usuario:

Caso de Prueba	Elemento	Entrada	Salida Esperada	Salida Obtenida
Selección de interface de red (válida)	Selección de la lista, clic en botón Aceptar	Selección, Clic	Entrada a la ventana "Configuración General"	Entrada a la ventana "Configuración General"
Selección de interface de red (no selección)	No se selecciona de la lista, clic en botón Aceptar	Clic	Mensaje "Debe seleccionar una interface"	Mensaje "Debe seleccionar una interface"
Ingreso de información ventana "Configuración General" (correcto)	Ingreso de información, clic en botón Aceptar	Ingreso información, clic	Entrada a la ventana principal "AIDS"	Entrada a la ventana principal "AIDS"
Ingreso de información ventana "Configuración General" (incompleto)	No se ingresa la información completa, clic en botón Aceptar	Clic	Mensaje "Información incompleta"	Mensaje "Información incompleta"
Selección "Opciones -> Configurar"	Se selecciona Configurar del menú Opciones	Clic	Entrada ventana "Selección de Interface de red"	Entrada ventana "Selección de Interface de red"

Selección "Opciones -> Bitácoras"	Se selecciona Bitácoras del menú Opciones	Clic	Entrada ventana "Bitácoras"	Entrada ventana "Bitácoras"
Selección de una bitácora (válida)	Se selecciona una bitácora del listado, clic botón Aceptar	Selección, Clic	Entrada ventana "Detalles Bitácora"	Entrada ventana "Detalles Bitácora"
Selección de una bitácora (inválida)	Se seleccionan varias bitácoras o ninguna, clic botón Aceptar	Selección, Clic Clic	Mensaje "Entrada no válida"	Mensaje "Entrada no válida"
Eliminación de una bitácora (válida)	Se selecciona una bitácora, clic botón Eliminar	Selección, Clic	Mensaje "Se eliminarán definitivamente esta bitácora"	Mensaje "Se eliminarán definitivamente esta bitácora"
Eliminación de una bitácora (inválida)	No se selecciona bitácora, clic botón Eliminar	Clic	Mensaje "Se debe seleccionar una bitácora para eliminar"	Mensaje "Se debe seleccionar una bitácora para eliminar"
Aceptación advertencia en eliminar bitácora	Se acepta la advertencia mostrada, clic Aceptar	Clic	Se eliminan las entradas de la base de datos	Se eliminaron las entradas en la base de datos
Cancelación eliminación bitácora	Se cancela el proceso, clic Cancelar	Clic	Entrada ventana "Bitácoras" No se eliminan registros	Entrada ventana "Bitácoras" No se eliminaron registros
Salida del sistema	Selección salir	Clic	Salida del sistema	Salida del sistema