Modelo de un IDS para proteger sistemas del tráfico ICMP: Caso del Ataque "Loki"

Miguel P. TORREALBA
Mireya M. MORALES
Departamento de Formación General y Ciencias Básicas, Universidad Simón Bolívar (USB)
Baruta, Estado Miranda, Apdo Postal 89000 / Zona 1080-A, Venezuela

y

Eddy CARRASCO
Departamento de la Escuela de Computación, Universidad Central de Venezuela (UCV)
Caracas, Distrito Capital, Apdo Postal 47747 / Zona 1051, Venezuela

RESUMEN

Ejercer una administración correcta y efectiva de la seguridad telemática en las redes corporativas de datos resulta difícil de aplicar; eso se debe, fundamentalmente, a la complejidad y diversidad de elementos que deben ser considerados. Los administradores y operadores de sistemas y redes informáticas son responsables de esto y persiguen fundamentalmente asegurar el procesamiento y tránsito de la información digitalizada; para ello deben aplicar métodos y estrategias estructuradas que reduzcan el riesgo de pérdidas a un nivel aceptable para la corporación, e instrumenten las directivas de la política de seguridad institucional. Esta labor exige que se haga uso de instrumentos y herramientas que automaticen acciones y procedimientos comunes del trabajo referido. Este trabajo expone el desarrollo de un modelo de un IDS orientado a objetos de una futura herramienta de apoyo a la gestión de la seguridad, cuyo propósito es el de detectar ataques de canal encubierto en el tráfico del Protocol ICMP del TCP/IP. Para lograr eso se aplicó una metodología de desarrollo propia, racional, estructurada, ordenada y completa; la misma incluyó la elaboración de un prototipo de software que identificó los aspectos funcionales para el caso del ataque del "Proyecto Loki" y permitió reconocer la eficacia del instrumento.

Palabras Claves: Gestión de la Seguridad Informática, Hackers, IDS, Canales Encubiertos, ICMP.

1. INTRODUCCIÓN

"*Cuanto más rápidamente cambie el medio, más breves son las formas de organización.*"

Alvin Toffler
El "Shock" del Futuro

En el mundo corporativo de nuestros días, se da por cierto que un correcto apoyo tecnológico para el procesamiento de la información puede convertirse en una ventaja competitiva que haga la diferencia para predominar o aventajar significativamente al rival. A su vez ese apoyo tecnológico se fundamenta en el empleo de sistemas computacionales, a menudo dispersos geográficamente, que operan y colaboran para alcanzar un propósito común. Ello es producto de un hecho predominante, la información a procesar no está centralizada o bien, sus resultados deben entregarse en un lugar diferente de donde se originó. Adicionalmente, el advenimiento de la Internet ha generado muchas transformaciones en los modos tradicionales de trabajar; uno de ellos es la tendencia de las organizaciones a disponer de acceso cómodo y seguro a la misma, con el propósito de disponer de una rica fuente de datos, altamente actualizada y de un mecanismo mundial rentable para sus comunicaciones.

Lo anterior descrito es fácil de desear, lo difícil de obtener es una gestión efectiva de la infraestructura señalada que garantice una alta disponibilidad y utilización de la misma. Esa aspiración constituye en sí el propósito de la administración de sistemas y redes de computadoras [1]. La gestión correcta de la infraestructura que permite el procesamiento de la tecnología de la información se revela entonces como una labor de alta complejidad, ya que debe considerar el funcionamiento en conjunto y a menudo concurrente, de sistemas heterogéneos que incluyen cientos o miles de partes. La esencia del problema radica entonces en organizar dinámica y adecuadamente la totalidad de operaciones de cada recurso, así como también en supervisar y optimizar esa misma disposición.

Por otra parte, una de las áreas principales que incluye la administración de esa plataforma tecnológica se asocia con la seguridad de la misma. Protegerla significa entonces, garantizar niveles aceptables de su disponibilidad y de procesamiento correcto. Reducir los riesgos potenciales a grados que se puedan tolerar y evitar, que si los mismos se transforman en ataques reales a la seguridad de la organización, no se perjudique drásticamente la misión establecida en la institución. Todo esto también es un trabajo de enorme dificultad, ya que involucra tratar con tecnología moderna de la información y con algo más complicado, el factor humano que dirige y manipula todo el sistema.

La ideal parece ser entonces abordar el trabajo bajo la idea de una constante adaptación al contexto que se protege y que se ve sometido a amenazas muy dinámicas; emplear aproximaciones sistemáticas y estructuradas que regulen un impacto desfavorable de los peligros sobre la plataforma. Dicha labor demandará la conjunción de procedimientos e instrumentos clásicos con otros propios, que favorezcan el tratamiento particular de la realidad local y única. La ingeniería de la seguridad trata acerca de cómo hacer realidad eso.

Este trabajo ilustra una estrategia de desarrollo de una herramienta para el apoyo de la gestión de la seguridad informática y ha sido organizado en dos grandes bloques: el primero -secciones 2 y 3- tratan aspectos propios de cómo instrumentar la gestión de la seguridad y el segundo -secciones 4, 5, 6 y 7- discuten el método de desarrollo del modelo de una posible herramienta de protección que se deriva del mismo.

2. EL ÉXITO Y LOS ESPEJISMOS EN LA GESTION DE LA SEGURIDAD INFORMATICA

"Conoced al enemigo y conoceos vos mismos; en cien batallas nunca correréis ningún peligro."

Sun Tzu
EL Arte de la Guerra

Aunque la gestión de la seguridad informática empieza en el discernimiento de planes y estrategias armoniosas con el buen funcionamiento de la corporación, se hace palpable en los mecanismos y herramientas que regulan el accionar de la red corporativa de datos y que protegen la información que sobre ella se procesa. Es identificable además en el correcto cumplimiento de la política organizacional de uso aceptable que controla el manejo de los bienes o recursos por parte de todos los empleados o afines de la institución.

De forma que los administradores de sistemas y redes telemáticas no deben considerar que el éxito de su trabajo radica en la presencia o el buen accionar de un instrumento en particular, por ejemplo en el empleo de un "firewall". Por el contrario, ese medio de protección debe encajar como un elemento constituyente del plan corporativo de la seguridad. El éxito entonces se debe centrar en los principios universales de la seguridad y en lo adecuado del plan dinámico que habrá que implementar; en poseer procedimientos correctos que indiquen el modo de actuar de todos los trabajadores frente a cualquier incidente posible. En la buena selección del paradigma filosófico de la seguridad que sostendrá dicho plan y en la explotación máxima de las habilidades humanas como eje central de la defensa y protección. Una buena gestión de la seguridad informática debe regular sin entorpecer el empleo de los sistemas telemáticos y para ello ha de permitir el constante cambio tecnológico de la organización en modo coordinado.

Así pues, un plan estratégico deberá constituirse desde tres posibles escenarios de incidentes: el preventivo, el reactivo y el forense. Adicionalmente, para cada uno de estas secciones se deberán integrar aspectos técnicos de ataques y respuestas con acciones legales y normas propias de la organización. De este planteamiento se deduce entonces la necesidad organizacional de aplicar un proceso de adiestramiento que capacite a sus empleados. Se transfiere así la responsabilidad exclusiva de los administradores y operadores por desempeñar efectivamente una buena gestión de la seguridad informática, a las manos de toda la comunidad corporativa, especificando claramente las responsabilidades y potestades necesarias de acuerdo al rol que desempeña cada trabajador. La protección se globaliza y se disminuye posibilidades para ataques de ingeniería social.

Ese modo de proceder significa entonces tomar en consideración lo relevante del factor humano y permite más tarde concentrar el trabajo de los especialistas de la seguridad corporativa en aspectos mucho más técnicos. Uno de esos aspectos se refiere a la identificación correcta de los riesgos, al estudio detallado de los ataques y atacantes posibles y a la manera como se debe preparar contramedidas frente a todas las posibles amenazas de la seguridad informática de la institución.

Dentro del ámbito más técnico el aspecto inmediato a considerar se refiere a las amenazas y sus posibles medidas de protección. Las primeras pueden provenir desde adentro o afuera de la organización. El factor humano es clave para todos los casos [2] y por eso es que resulta imprescindible el plan holístico y los análisis cuantitativos de riesgos factibles. En función de la prioridad de resultados y en consonancia con la política de seguridad institucional, se deberán aplicar las medidas protectivas. Esas medidas se instrumentarán como procedimientos y muy posiblemente requieran medios y mecanismos técnicos que apoyen su ejecución. De modo que habrá que asociar herramientas del tipo preventivas, otras para la reacción frente a un ataque en curso y las últimas, para el análisis forense de lo ya acontecido.

Una dificultad tradicional a todo este proceder radica en que las corporaciones acostumbran a dejar solo en manos de los fabricantes y diseñadores la elaboración de los instrumentos para su protección. Se ignora así la importancia de la diversidad corporativa, por el contrario, se afianza la creencia en una cultura única y común de la organización. Es decir, se subestima principalmente lo crítico del elemento humano y se apunta a creer en el espejismo de que el problema es únicamente de naturaleza técnica y que en consecuencia, se soluciona con otra tecnología. El esquema de consentir en que las protecciones provendrán del desarrollo de software especializado o de mejores algoritmos criptográficos se sostiene además porque aparenta reducir costes y proclama que el cliente se debe dedicar solamente a su negocio. Se le hace creer que su seguridad puede ser sostenida sin su esfuerzo directo. Adicionalmente, la organización adapta su funcionamiento al mecanismo o a la herramienta universal que el fabricante diseñó. Se olvida que ese diseño es hecho en una forma genérica y que no puede aprovechar todas las características potenciales del cliente; se deja de lado también el hecho de que depende del tiempo de respuesta del fabricante.

En todo este panorama el cliente no considera la exigencia por una mejor calidad del software que se le entrega, cosa que conviene a los intereses de algunos fabricantes de software comercial y se responsabiliza a estar pendiente de la última actualización o protección provista. El fabricante por su parte puede propiciar la dependencia, ya que es quien conoce todos los detalles intrínsecos del sistema que puede convertirse en potencial víctima. Además posee los recursos para enmendar la vulnerabilidad. En nuestros días emite boletines con alertas y recomendaciones en materia de seguridad. Se propicia así una aproximación a la idea de que la seguridad se puede obtener a pesar de la ignorancia en el tema, es decir, seguridad a través de la oscuridad.

Un aspecto final de este modo de obrar ahora tradicional, se refiere a que por naturaleza es reactivo. Lo común es que el fabricante identifique el problema después de que alguna víctima lo reporta. Una carrera por reducir el lapso de tiempo que requiere elaborar el correctivo sucede entonces. A ese tiempo hay que agregarle el del usuario que lo aplica; en aquellos casos en que el ataque se extiende rápidamente habrá un costo sustancial, en tiempo y dinero, para reparar y recuperar la normalidad operativa. Un ejemplo conocido de lo anterior sucede con el tratamiento de los virus y gusanos de computadoras.

3. HACIA UNA GESTIÓN INTEGRAL DE LA SEGURIDAD INFORMÁTICA

"El caos sugiere que, en vez de resistirnos a las incertidumbres de la vida, lo que deberíamos hacer es aceptarlas. Y aquí es donde entra el segundo tema, la creatividad."

John Briggs y F. David Peat
Las Siete Leyes del Caos

La aproximación de trabajo planteada anteriormente requiere reforzarse; eso significa que la organización deberá desarrollar adicionalmente sus propias medidas y herramientas para propender a una gestión de la seguridad proactiva. Esta postura obliga a considerar inicialmente el punto referente al personal que deberá encargarse de ello; se requiere un cuerpo de trabajadores que posean las destrezas, habilidades, conocimientos y competencias suficientes para satisfacer las demandas necesarias.

Un paradigma tradicional de la seguridad llegó a aceptar que dentro del personal de las empresas existieran algunos dedicados a responsabilizarse por el problema de la seguridad de la organización. Las protecciones que centraban dicha labor en la seguridad física de recursos, en el almacenamiento y trasferencia de documentos en papel y en el cuidado de los seres humanos. Ese paradigma debe ser modificado; requiere considerar también la información digital y su paso por sistemas telemáticos que no necesariamente se pueden supervisar con la aplicación directa de nuestros sentidos naturales.

La corporación de la era de la información debe contratar aquellos recursos humanos que posean la capacidad de extender la vigilancia; ello posiblemente obligue a considerar perfiles especializados para cubrir el amplio espectro de tareas que ahora se presentan. Algunos deberán ser capaces de desarrollar soluciones ad hoc y otros deberán poder complementar o ampliar los instrumentos para su trabajo. Es decir, no depender exclusivamente de las soluciones de los fabricantes y por el contrario ser capaces de generar tecnología local que resuelva la problemática propia de la institución.

Ese espíritu de gestión de los sistemas no es novedoso, ya que algunos desarrollos muy extendidos, como el caso de los sistemas Unix, brindaban una baúl de herramientas y ciertas facilidades para que el mismo fuera ampliado o adaptado según los requerimientos del usuario [3]. La idea es colocar sistemas adicionales que los atacantes no esperen encontrar con capacidad para vigilar y detectar posibles intrusiones. Mecanismos que no respondan a la vulnerabilidad declarada en otros productos comerciales. Errores podrán tener, pero obligarán a un atacante a que las descubra, cosa que generará un consumo de tiempo adicional que puede resultar valioso para quien defiende. El vándalo verá reducida su capacidad para aprovecharse de una debilidad previamente divulgada y deberá confeccionar sus propios "exploit" para obtener éxito.

En otros casos el personal especializado de la seguridad deberá adaptar soluciones que se provean con su código fuente original a sus propias necesidades. Esta aproximación facilita la automatización de toma de decisiones que bajo situaciones de ataques a veces desbordan la capacidad de respuesta del personal. Se provee además de un medio para instrumentar las especificaciones de la política corporativa de la seguridad informática. Bajo todas esas consideraciones se comprende que las respuestas se trasladan así al plano de la creatividad y habilidad de quienes defienden el perímetro de la infraestructura tecnológica de la organización. Se aplica así el paradigma de conseguir seguridad a través de la diversidad.

Así pues, una comunidad adiestrada y un personal especializado con capacidad para evaluar la inseguridad de la empresa y proponer soluciones que exploten la diversidad de sus sistemas, pueden brindar mayor capacidad de respuesta frente a los incidentes.

El personal encargado deberá probarse además bajo simulacros de "incidentes en progreso" para verificar su efectividad, al igual que la colaboración del resto de los empleados de la corporación. Así la política deberá abordar situaciones que permitan verdaderamente confirmar la preparación que se posee a efectos de mejorar y refinar constantemente los procedimientos establecidos y la utilidad de las herramientas empleadas. La idea perseguida es entonces no depender únicamente de alertas que emiten fabricantes y organizaciones de respuesta a situaciones de emergencia en seguridad telemática.

En el resto de este trabajo se describirá un proceder para desarrollar un instrumento propio de protección informática. Este último se enmarca bajo la perspectiva descrita en esta sección. Se pretende demostrar así, con un ejemplo real, una posible guía que bien podría ser de utilidad para el personal encargado de mantener la seguridad de una empresa.

4. EL METODO DE TRABAJO PARA DESARROLLAR HERRAMIENTAS PROPIAS DE LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

"Ahora bien, vale mucho más no pensar nunca en investigar la verdad de cosa alguna que hacerlo sin método; es realmente cierto, en efecto, que los estudios de esta clase llevados sin orden y las meditaciones confusas, oscurecen la luz natural y ciegan los espíritus."

Descartes
EL Discurso del Método

El desarrollo de instrumentos propios o la modificación de otros que ya existen se puede fundamentar en un tratamiento sistémico de desarrollo de software. Esta labor se ejecutó con el empleo de un método de trabajo que consistió en un plan prefijado de acciones y un conjunto de directrices para alcanzar la meta propuesta. Se obtuvo de esa forma un plan que con el paso del tiempo y a través de su implementación, dio paso a refinamientos y ajustes que resultaron efectivos. El método resultó ser entonces un desarrollo de *tipo individual* que se confirma a través del resultado exitoso que se obtuvo con la existencia y funcionamiento del producto perseguido [4].

El método puede ser descrito como: racional, estructurado, ordenado y completo. Su presentación puede hacerse como una sucesión de etapas temporales que integran acciones realizadas como se ilustra en la Figura 1.

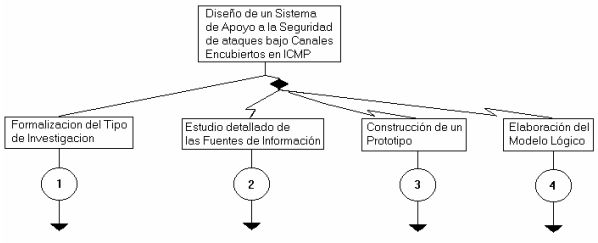

Figura 1: etapas que conforman el método

La Figura 2 muestra a su vez las partes que constituyeron la formulación de la investigación que se estaba ejecutando. Como esta fase se vinculaba propiamente a un trabajo de grado para un curso de estudiantes gradudados en computación, no resulta necesaria de ejecutar para el personal de la organización.

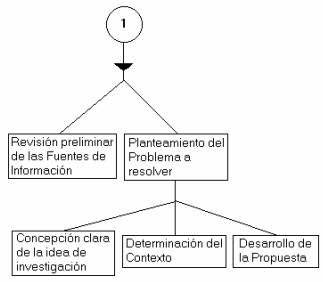

Figura 2: etapa primera del método

La Figura 3 ilustra la etapa que permitió determinar las fuentes apropiadas de información para investigar sobre la amenaza que se deseaba controlar. En este caso se debió reconocer el ataque, su autor, aplicación y conformación técnica. Luego, se procedió a consultar sobre protecciones previas. En este paso se identificó el espacio para el nuevo desarrollo de una protección de software y se estableció su utilidad.

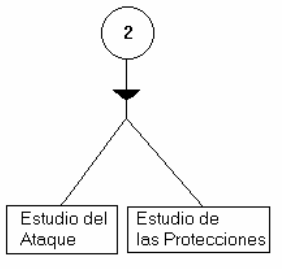

Figura 3: etapa segunda del método

La Figura 4 expresa los pasos principales para construir un prototipo de la herramienta.

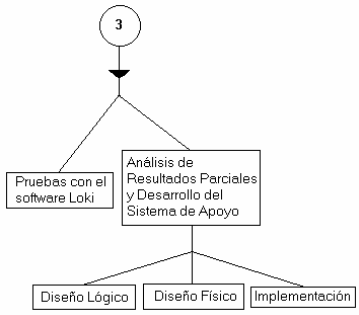

Figura 4: etapa tercera del método

La Figura 5 describe los pasos que conformaron la etapa final. Aquí se analizaron los resultados obtenidos al experimentar con el prototipo para incluir la información recabada como parte del modelo final de la herramienta. De esta forma el modelo ilustra una herramienta factible de realizar.

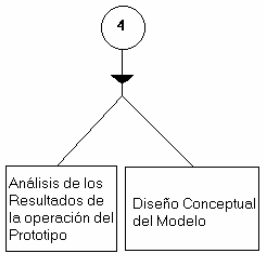

Figura 5: etapa cuatro del método

Hasta ahora nos hemos concentrado en el método empleado. En la siguiente sección explicaremos cual fue el riesgo que se estaba tratando.

5. EL TRÁFICO DE INFORMACIÓN ENCUBIERTA DENTRO DE LAS REDES TCP/IP

"Nada hay oculto que no deba ser manifestado, ni nada secreto que no deba ser conocido y sacado a la luz."

Lucas 8:17

El problema de los canales encubiertos en la seguridad de la información ha sido largamente discutido y resulta común entender que en el mismo ataque se contraviene alguna directiva de seguridad sobre el acceso a cierta información clasificada. La idea principal es emplear un mecanismo válido del tratamiento de la información para acceder, ilegalmente y en forma secreta, a otra que está restringida. Tradicionalmente esta amenaza se categoriza en dos posibles modos: como canales de comunicación encubiertos del tipo almacenamiento o del tipo tiempo. Varios de los protocolos del TCP/IP son medios para este tipo de ataque y en 1996, un "hacker" conocido como "Demon9", reveló en la revista "Prack" un mecanismo conocido como "Proyecto Loki" que sirve para instrumentar un canal encubierto de información inmerso en la transferencia de mensajes ICMP. Loki emplea los mensajes ICMP de tipo

ECHO o ECHO REPLY como medios de transporte para transferir información con intención subversiva [5].

En la Figura 6 se presenta un diseño conceptual del prototipo que incluye cuatro elementos fundamentales de operatividad: un módulo de captura de la totalidad de los datagramas que viajan en el segmento físico de la red, un módulo que filtra los mensajes ICMP, otro que busca en dicho tráfico solamente aquellos que son del tipo ECHO o ECHO REPLY y uno más, que examina la estructura potencialmente vacía que puede contener la información subrepticia del ataque.

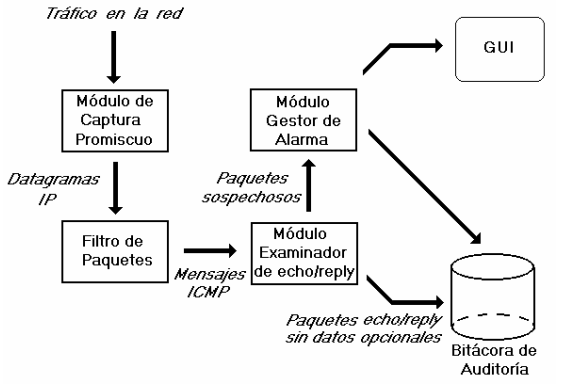

Figura 6: Diseño lógico del prototipo

6. LA EXPERIMENTACION CON SISTEMAS REALES COMO VERDADERA FUENTE DE INFORMACIÓN EN LA SEGURIDAD INFORMÁTICA

"Cuando usted está tratando con redes de computadoras y software, debe actuar más como un físico que como un matemático. Usted tiene que tratar con el mundo real y no puede ocultar los hechos, problemas, fenómenos, bugs y cualquier otra cosa que se presentan. Así que ser honesto acerca de lo que se está haciendo y no esconder lo que acontece es un bonito lema por el cual vivir."

Vinton G. Cerf
Entrevista para "Amos de la Tecnología" de "Scientific American"

La Figura 7 representa la secuencia de operaciones que se espera sucedería durante una captura y emisión de la alarma. Su construcción se derivó de la experimentación con el código de un sistema Cliente - Servidor de tipo puerta trasera que opera sobre ICMP. Ese software se obtuvo a partir del boletín electrónico "Confidence Remains High #9" que se distribuye libremente en la Internet desde 1998 y se atribuye a un programador con seudónimo "Bit". La idea de trasfondo parece ser demostrar otra versión del ataque Loki.

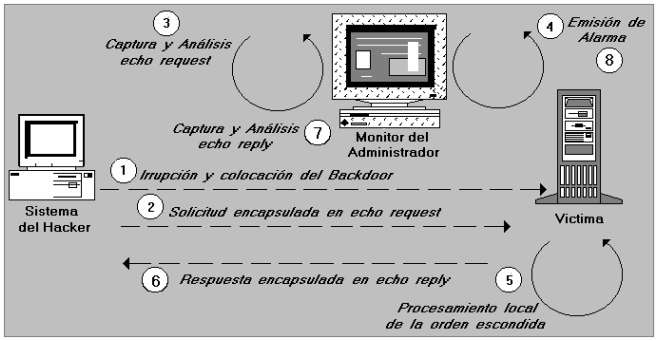

Figura 7: acciones para detectar el ataque "Loki"

El ataque que describe el grupo "CodeZero" en su boletín CRH#9 funciona después de que un "hacker" logra irrumpir en un sistema Unix/Linux y coloca un programa del tipo puerta trasera. Ese conjunto de instrucciones constituyen en sí el servidor que atenderá las peticiones remotas del atacante -código del cliente-, ejecutará sus órdenes y enviará las respuestas en forma similar a mensajes ocultos en un canal encubierto.

Muchas formas posibles pueden ser utilizadas para irrumpir exitosamente en el sistema víctima y "sembrar" el cliente. Muestra de ello se constata al revisar los continuos mensajes de vulnerabilidades que emiten constantemente grupos reconocidos como el CERT. Disfrazar u ocultar la actividad del servidor requiere alguna experiencia; un proceder simple sería apoyarse en el funcionamiento del demonio "Cron" para iniciar el servidor bajo una designación que parezca común o normal del sistema. Otra alternativa más sofisticada sería codificar el servidor como parte constituyente kernel del sistema para así esconder rastros de las operaciones. En Linux la concepción de módulos anexos al kernel también puede ser empleada.

De modo que el atacante bajo el esquema de acción tipo "Loki" se convierte en un intruso del sistema de la víctima, ya que se sobrepone al hecho no tener un acceso directo y real al mismo. Puede entonces ejecutar asíncronamente cualquier orden en el sistema ya que el servidor se ejecuta en modo supervisor.

El prototipo elaborado opera en modo similar al cliente ICMP distribuido por "Bit" que recibe respuestas en un área de los mensajes ICMP que, según el RFC 792, se supone no contendría información y estaría rellena con "ceros" [6]. Se elaboró para que verificara, en tiempo real, un patrón de datos diferente al relleno de ceros que indica dicho RFC y emitiera una alarma de posible ataque en progreso. Se evita así una acción drástica de respuesta que pudiese bloquear un tráfico benigno ICMP, y se deja en manos de los oficiales de seguridad las subsecuentes decisiones.

Una de las cosas que la experimentación permitió constatar es que la mayoría de las instrumentaciones de activación de mensajes ICMP del tipo "echo/echo reply", como es por ejemplo la orden "ping" del TCP/IP, incumplen con la recomendación del RFC. Por esta razón se advirtió la necesidad de que el modelo final incluya el procesamiento de patrones sofisticados como elemento crítico de la herramienta de protección.

El prototipo fue desarrollado en un sistema Linux de la distribución Red Hat 7.0 .Los lenguajes de programación empleados fueron C -para la codificación del programa tipo "sniffer", el módulo de filtro y el examinador de patrones-; algunas rutinas se codificaron en Bash Shell para ensamblar el sistema y varios programas con TCL/TK para el desarrollo de una interfaz gráfica de usuario simple y amigable [4].

La Figura 8 muestra el mensaje de alerta que emite el prototipo para Detección de Ataques de Tráfico Encubierto (DATE). La gráfica ilustra la operatividad del sistema en una plataforma Ms-Windows 98® ya que se ejecutaron satisfactoriamente adicionalmente pruebas de portabilidad de la herramienta.

Figura 8: alerta que emite el prototipo al detectar un ataque "Loki"

7. MODELO FINAL DE UNA HERRAMIENTA PARA APOYAR LA GESTION PROACTIVA DE LA SEGURIDAD INFORMÁTICA

"Aceptamos el sistema de controles de seguridad en ciertas áreas de nuestra vida, a fin de que el resto de ella pueda verse libre, pero no el que los controles tengan que ser extendidos indiscriminadamente y demasiado celosamente a esferas en las que no hay necesidad evidente de ello."

Edward A. Shills
El Telón de Papel en América (1952)

A partir de la información y experiencia recabada con el uso del prototipo se procedió a formular un modelo final de una herramienta. A esta altura estaba claro que la formulación de la misma podía clasificarse como la elaboración de un Sistema de Detección de Intrusos de la categoría "red" [7][8]. Se deseaba entonces diseñar un modelo de una herramienta adaptativa ante nuevas amenazas del tipo canal encubierto; por ello se buscó una orientación orientada al objeto como eje central de esta tarea. La idea de reutilizar software ya generado también reforzó esta estrategia.

Para el modelo final los objetos se identificaron a partir de la observación de las entidades reales que estaban presente en el funcionamiento del prototipo [4]. El análisis asociado reveló pues que la Trama ICMP y el mecanismo detector ICMP eran los objetos del modelo. Posteriormente, por simple agrupación de instancias se puedo establecer que las clases directas serían Tramas de Protocolos del TCP/IP y mecanismo detector del ataque de canal encubierto para cualquier Protocolo de TCP/IP. De ese modo el modelo expande su rango de acción a otros protocolos vulnerables del TCP/IP PSS. La Figura 9 muestra los atributos y comportamientos identificados según la notación Coad-Yourdon.

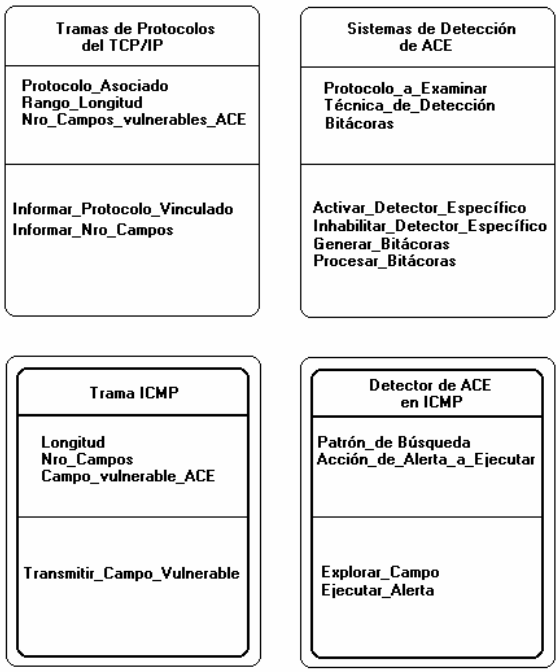

Figura 9: atributos y comportamientos contemplados

Para este paso lo que resulta más importante de resaltar es la propuesta de un atributo denominado "Patrón_de_búsqueda" que constituye en sí el instrumento tecnológico central del detector. Los falsos positivos o negativos que genera el empleo de la herramienta dependerán de este elemento.

Las relaciones entre clases encaja en el modelo "is-a" ya que por ejemplo Tramas de ICMP o Tramas UDP "es un" subtipo de Tramas de Protocolos TCP/IP. Algo análogo sucede con Detector de ACE en ICMP o Detector de ACE en UDP con respecto a Detección de ACE en TCP/IP. A su vez, la relación que ocurre en una clase como Trama ICMP y detector de ACE en ICMP es una asociación en la cual la Trama ICMP se visualizó como un parámetro del detector. Se llegó así a una relación jerárquica entre esas clases del tipo "uses a" [4].

La Figura 10 muestra una visión completa del arquetipo modelado. El mismo se derivó entonces del prototipo y puede ser expresado conjuntamente con otros diagramas en una forma que especifique cada entidad relevante para la programación final de la herramienta proyectada.

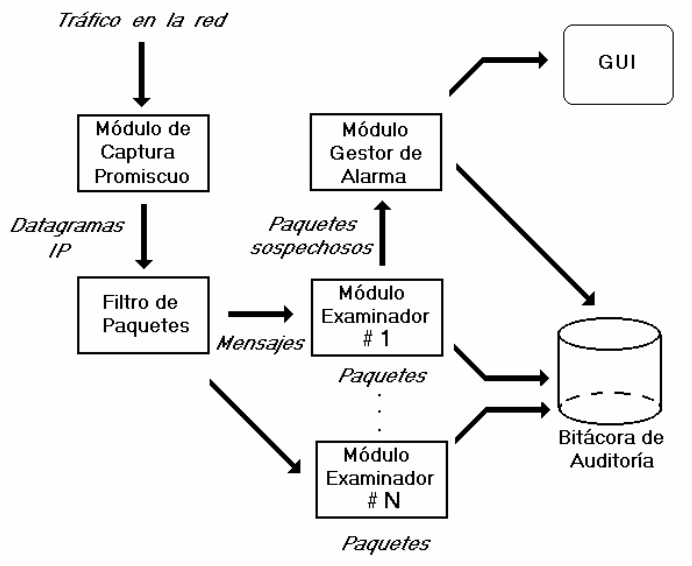

Figura 10: Modelo final de la herramienta a desarrollar

7. CONCLUSIÓN Y TRABAJOS FUTUROS

"Toda información es imperfecta. Tenemos que manejarla con humildad. Tal es la condición humana; y así lo expresa la física cuántica."

Jacob Bronowski
El Ascenso del Hombre

Este trabajo ha expuesto un conjunto de abstracciones y acciones que conducen a desarrollar una herramienta propia que deberá auxiliar al personal encargado de la administración de la seguridad informática en cualquier corporación. La idea ha sido demostrar la secuencia de procederes que ilustre como es posible elaborar un instrumento específico que automáticamente alerte frente a un posible ataque a la seguridad informática de la red corporativa de datos.

Un modelo con sustento real, que se adapta a un problema específico y que bien puede ser particular, es el producto de esta etapa del trabajo y se espera que el siguiente nivel produzca la herramienta final.

El aspecto final de este esfuerzo debe apuntar a integrar la herramienta constituida con un esquema de acción que se integre con la política de seguridad corporativa y conduzca a ejecutar una gestión integral y diferenciada de la seguridad informática.

8. REFERENCIAS

[1] Terplan, K. *Communication Networks Management.* Prentice Hall Inc., Second Edition, Englewood Cliffs, New Jersey, 1992.

[2] Schneier, B. *Secrets & Lies. Digital Security in a Networked World*. John Wiley and Sons Inc., 2000

[3] Ritchie, D. *Et al*. *The UNIX Time-Sharing System*. Communications of the ACM. Vol. 17. No 7. pp. 365-375. July, 1974.

[4] Torrealba, M. *Diseño de un sistema de apoyo a la gestión de redes TCP/IP que detecta ataques que se realizan a la seguridad a través de la técnica de canales encubiertos sobre ICMP.* TEG de maestría no publicado. Postgrado en Computación. UCV. 2003.

[5] Daemon9. *Project Loki*, Phrack Magazine, Volume Seven, Issue Forty-Nine, [Página Web en línea]. Disponible: http://www.phrack.com [Consulta: 2000, Diciembre 25] 1996.

[6] Postel, J. *Internet Control Message Protocol*. RFC No 792. September, 1981.

[7] Kemmerer, R. *Et al*. *Intrusion Detection: A brief history and overview*. Security & Privacy. Suplement to Computer Magazine. pp. 27-29. IEEE Computer Society, 2002.

[8] Norrhcutt, S. *Et al. Detección de Intrusos. Guía Avanzada.* Pearson Educación. 2001