ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

VISUALIZADOR DE ESTADO DE RED

María Verónica Serrano Pérez. (1), Diego Andrés López Encalada (2), Ignacio Marin-Garcia (3)
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
maveserr@espol.edu.ec (1), danlopez@espol.edu.ec (2), imaringa@fiec.espol.edu.ec (3)

Resumen

Debido a los frecuentes ataques que sufren las redes informáticas se crea la necesidad de implementar mecanismos de seguridad con el fin de proteger las redes y la información que se almacena en ellas. Con dicho fin hemos creado una herramienta de gran utilidad que nos permite proveer información para obtener seguridad y proteger la integridad de la información contenida en una red de posibles ataques por parte de personas internas o externas. El programa nos permitirá visualizar de forma gráfica y detallada lo que ocurre en la red en cada uno de los protocolos capturados en tiempo real, así como guardar un registro del tráfico que circula por la red, de la estructura de la misma y sus componentes. Nos proveerá de recursos para mantenernos informados sobre lo que ocurre en nuestra red permitiéndonos detectar inconsistencias, fallos, y posibles ataques deficiencias de seguridad de un host para poder tomar las acciones pertinentes.

Palabras Claves: *Integridad, vulnerabilidad, sistema, ataque.*

Abstract

Due to the frequent attacks suffered by computer networks creates the need to implement security mechanisms to protect networks and information stored in them. To this end we have created a very useful tool that allows us to provide information for security and protect the integrity of the information contained in a network of potential attacks by insiders or external. The program will allow us to visualize graphic detail what happens in the network in each of the protocols captured in real time and keep a record of traffic flowing through the network, the structure itself and its components. We provide resources to keep us informed about what happens in our network allowing us to detect inconsistencies, errors, and potential safety deficiencies attacks from one host to take appropriate action.

Keywords*: integrity, vulnerability, system, attack.*

1. Introducción

La seguridad en redes ha sido siempre un objetivo difícil de alcanzar ya que cuando de seguridad se trata nada es 100% fiable. En la actualidad la masificación de la comunicación, unida a la amplia gama de medios para el intercambio de información pone en amenaza la protección de los datos. Con nuestra propuesta, esperamos ayudar a los administradores de red a visualizar lo que ocurre en su red en tiempo real detectando posibles falencias de seguridad que los atacantes ya sean internos o externos pueden aprovechar, y de esta manera proteger la información y datos.

2. Objetivo

El objetivo general de nuestro proyecto fue desarrollar una aplicación en JAVA de fácil manejo, escalable y distribuida que sirva para el procesamiento de escaneo de redes a su alcance, ver, analizar y basados en los resultados proporcionados, mitigar las diferentes vulnerabilidades de seguridad que existan en una determinada red.

3. Problema

Desde que surgió Arpanet para permitir la comunicación general entre varias computadoras en la década de los setenta, han existido los problemas de seguridad. A través de los tiempos estos peligros informáticos se han modernizado y vuelto más peligrosos y difíciles de detectar.

3.1 Justificación

Nuestro proyecto tiene como función principal el proveer una herramienta gráfica de fácil manejo, que va a monitorear una red de acuerdo a su funcionamiento. Esto ayudará a los encargados de la seguridad en red de una empresa a disminuir la vulnerabilidad de los datos que se transmiten, conociendo qué tipos de protocolos y puertos son los que están en uso.

4. Metodología de Investigación

La metodología que tomamos como base para eldiseño de nuestro software fue la RUP(Rational Unified Process – Proceso Unificado Racional) el cual es un proceso de desarrollo de software que junto con el Lenguaje Unificado de Modelado UML, constituyen la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos.

El RUP no es un sistema con pasos firmemente establecidos, sino un conjunto de metodologías adaptables al contexto y necesidades de cada organización. En la Figura 1 podemos observar la interacción y funcionamiento de dicho proceso.

Figura 1 Metodología de Desarrollo de software

5. Análisis y Planificación

Se definieron los requerimientos para cada iteración según la solución planteada con el fin de cumplir con todos los requerimientos, posteriormente esta fase fue documentada mediante la creación y especificación de diagramas de casos de uso, los cuales mostraron por nivel de abstracción todas las funcionalidades de cada módulo.

Se creó el diagrama de casos de uso, que reflejó las principales funcionalidades de la aplicación y cómo debe interactuar la misma con el usuario para el logro de cada uno de los objetivos.

6. Diseño y Solución

Para el diseño se creó la estructura lógica a desarrollar definiéndose las clases que iban a interactuar, así como los métodos que fueron incluidos dentro de cada una de las clases. Esta fase fue documentada mediante el uso de diagramas de clases definidos en lenguaje UML.

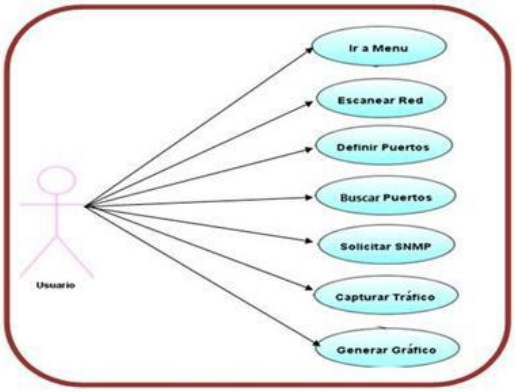

Figura 2 Diagrama de Casos de Uso Nivel 1

Una vez analizados los requerimientos y diseñada la solución para cubrirlos, se procedió a codificar la solución a fin de implementar las clases diseñadas y se desarrollaron cada uno de los métodos definidos para la clases.

public void addNHosts(): Agrega los hosts dentro de la red interna a través del ICMP.

public void addNHostsSNMP() throws IOException: Agrega los hosts consultando a la tabla de ipNetToMediaNetAddress en el router a través del SNMP.

public void PortScanner(): Scanner de puertos TCP y UDP en un Host especifico requeridos por Rango.

Figura 3 Ejemplos de métodos implementados

7. Conclusiones

1. El visualizador de estado de red nos permite en base a los resultados obtenidos mediante la ejecución ayudar a mitigar las vulnerabilidades existentes en una red.

2. Al comparar el funcionamiento de software con funcionalidades similares a nuestro proyecto como es el caso de BuduIP, nosotros brindamos una interfaz más amigable para el usuario, facilidad de manejo y mayor utilidad, lo cual se comprobó mediante encuestas a usuarios.

3. El visualizador de estado de red ofrece la máxima eficiencia evitando el desgaste innecesario de recursos como tiempo al restringir la búsqueda de datos o escaneo de puertos al rango especificado por el usuario.

8. Recomendaciones

1. Verificar que en el computador donde se ejecutará el software tenga habilitado todos los componente SNMP para evitar errores con el escaneo por SNMP mapping.

2. Darle al software independencia modular ya que mejora el rendimiento humano pudiendo realizarse programación en equipo y desarrollar módulos paralelamente.

3. Para el futuro se recomienda realizar un tipo de algoritmo para optimizar el tiempo de escaneo de puertos.

9. Bibliografía

[1] STALLINGS William, "Comunicaciones y Redes de Computadores", Sexta Edición. Prentice Hall, 2000.

[2] Herramientas Web para la enseñanza de protocolos de comunicación. EL PROTOCOLO IP. < http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/ip.html>, 16 de Marzo del 2011

[3] El modelo OSI y los protocolos de red. < http://blyx.com/public/docs/pila_OSI.pdf> ,16 de Marzo del 2011

[4] "CISCO". Network Management Fundamentals, <http://www.scribd.com/doc/13089205/Network-Management Fundamentals-Alexander-Clemm>, 23 de Marzo del 2011

[5] "Aiko Pras". Arquitectura de Administración de Redes , < http://doc.utwente.nl/17897/1/t0000011.pdf, > 29 de Marzo del 2011

[6] Modelos de gestión de red . http://tvdi.det.uvigo.es/~mramos/gprsi/gprsi3.pdf >, 2 de Febrero del 2011

[7] Administración de Redes . Capitulo 4, https://docs.google.com/document/d/1c1tW1GfBC7chP-SpgtgtowjoHb3XVknIOf3YVfSgJmg/edit?hl=en&pli=1#>, 21 de Febrero del 2011

[8] "R. y Kevin J. Schmidt". Essentials SNMP , <http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ >, 4 de Febrero del 2011

[9] "M. Rose".RFC 1155 Estructura e identificación de información para la administración de TCP/IP, <http://www.faqs.orgl >, 3 de Febrero del 2011

[10] "Mark A. Miller" .Gestión de Internetworks con SNMP , <http://ebookee.org/Managing-Internetworks-With-Snmp_362608.html >,6 de Abril del 2011

[11] "K. McCloghrie" . RFC 2578 Estructura de administración información versión 2, <http://www.faqs.orgl >, 4 de Abril del 2011