

**ESTUDIO DE TECNOLOGIAS EN SEGURIDAD PERIMETRAL Y SIMULACION
DE LA TECNOLOGIA WEP PARA REDES DE COMUNICACIONES**

David Alfonso Rey

**Anteproyecto de grado presentado
como requisito parcial para optar
al título de Ingeniero Electrónico.**

**UNIVERSIDAD DEL VALLE
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELÉCTRICA Y ELECTRÓNICA
PROGRAMA ACADÉMICO DE INGENIERÍA ELECTRÓNICA
SANTIAGO DE CALI
2005**

**ESTUDIO DE TECNOLOGIAS EN SEGURIDAD PERIMETRAL Y SIMULACION
DE LA TECNOLOGIA WEP PARA REDES DE COMUNICACIONES**

ESTUDIANTE

David Alfonso Rey

Código 0122347

Aprobación del director de proyecto

Ing. Oscar Polanco Sarmiento

Ing. Fabio Guerrero, MSC
Coordinador del Área de
Telecomunicaciones

Ing. Carlos Pinedo
Director del plan de Estudios
Ingeniería Electrónica

TABLA DE CONTENIDO

	PAG
1. INTRODUCCIÓN	1
2. ANTECEDENTES	2
3. FORMULACIÓN DEL PROBLEMA	4
4. JUSTIFICACION	6
5. OBJETIVOS	7
5.1. GENERAL	7
5.2. ESPECIFICOS	7
6. MARCO TEORICO	8
6.1 ESTADO DEL ARTE	17
7. ASPECTOS METODOLOGICOS	17
8. RESULTADOS ESPERADOS	19
9. PRESUPUESTO	19
10. CRONOGRAMA DE ACTIVIDADES	20
11. GLOSARIO	20
12. REFERENCIAS	24

1. INTRODUCCIÓN

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras distribuidas. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder de forma no autorizada a datos de carácter confidencial.

Toda organización debe estar a la vanguardia de los procesos de cambio. Estas deben disponer de información continua y confiable en el tiempo, esto constituye una ventaja fundamental.

Donde la información se reconoce como:

Crítica: indispensable para garantizar la continuidad operativa de la organización.

Valiosa: es un activo corporativo que tiene valor en sí mismo.

Sensitiva: debe ser conocida por las personas que necesitan los datos.

La seguridad informática debe garantizar:

La Disponibilidad de los sistemas de información.

Recuperación rápida y completa de los sistemas de información

La Integridad de la información.

La Confidencialidad de la información.

El presente trabajo de grado propone la apropiación, desarrollo y simulación de aspectos relacionados con la seguridad perimetral en las redes de comunicaciones, lo que permitirá asesorar sobre seguridad informática a cualquier organización.

2. ANTECEDENTES

Los sistemas de seguridad perimetral en redes han evolucionado para ofrecer cada vez mayor confiabilidad a los usuarios sobre la transparencia y protección de su información.

En el año de 1983 comenzó una etapa donde se inicio el surgimiento de grupos que empezaban a implementar algunos métodos para ingresar a sistemas restringidos, incluyendo el método conocido como *war dialing* donde se utilizaba un método para buscar números telefónicos de conexiones de módems análogos en un área definida.

10 años después la seguridad informática incrementó su confiabilidad para la protección de información personal y financiera. El caso de Mitnick y Vladimir donde robaron cerca de US\$80 millones en códigos fuente y propiedad intelectual de importantes empresa como Nokia, NEC, Sun Microsystems, Novell, Fujitsu, y Motorola, alarmó a todas las organizaciones alrededor de la industria en replantear sus sistemas de seguridad en la transmisión de información. La popularidad de Internet fue uno de los más importantes desarrollos que intensificaron el esfuerzo hacia la seguridad de la información.

Los sucesos que han llevado a la evolución de la seguridad en redes se pueden explicar en la siguiente línea de tiempo:

1960:

Estudiantes del MIT¹ definen el termino hacker en el contexto de como es conocido en la actualidad y empiezan a explorar y programar las computadoras PDP-1²

El DoD³ crea ARPANet (Advanced Research Projects Agency Network), la cual gana popularidad en los círculos académicos para el intercambio de información.

Ken Thompson desarrolla el sistema operativo UNIX uno de los sistemas operativos mas accesibles a los hackers gracias a sus herramientas de desarrollo y compiladores de soporte para la comunidad.

¹ Massachussets Institute of Technology

² Programmed Data Processor

³ Department of Defense (Estados Unidos)

1970:

Se desarrolla Telnet como uno de los protocolos para intercambio de información el cual es uno de los protocolos más inseguros existentes.

Se desarrolla USENET el cual se convirtió en uno de los foros mas importantes para intercambio de información sobre violación a sistemas de seguridad

1980:

IBM desarrolla los PCs⁴ basados en microprocesadores 8086, donde esta plataforma permitió el aumento de usuarios con potencial de ser accedados de manera no permitida.

El desarrollo del protocolo TCP/IP⁵ como el protocolo mas poderoso en la comunicación a través de Internet.

1990:

Sistema Linux permite a los hackers el desarrollo de herramientas de intrusión dada la naturaleza de software libre Linux.

Transferencias ilegales del Citibank por alrededor de US\$12 millones

Desarrollo de los sistemas peer to peer para el desarrollo de herramientas para hacking (Defcon).

En la actualidad:

Se estiman más de 142 accesos no permitidos a sistemas de información reportados al CERT⁶ diarios.

La disminución de violaciones de seguridad bajó de 73,359 a 52,658 entre el 2001 y el 2002 dado por la evolución en los sistemas de seguridad.

El impacto económico a nivel mundial por virus que acceden a los sistemas por medio de las redes de comunicaciones fue de US\$13,2 Billones.

⁴ Personal Computer

⁵ Transmisión Control Protocol / Internet Protocol

⁶ Computer Emergency Readiness Team (US)

La seguridad informática se ha convertido en una inversión justificable y cuantificable para todas las organizaciones que requieren integridad y seguridad en sus sistemas de administración de la información.

La implementación de redes de comunicaciones seguras presentan la dificultad de que requieren un conocimiento especializado de cómo la organización debe usar, manejar y transmitir su información.

La Universidad del Valle en el área de Telecomunicaciones ha desarrollado muy poco material sobre seguridad informática dirigida hacia redes de comunicaciones.

3. FORMULACIÓN DEL PROBLEMA

Para minimizar los riesgos de seguridad en las redes de comunicaciones, es imprescindible un servicio profesional especializado y experto, que transforme la defensa en un proceso continuo y dinámico. La seguridad en los sistemas de comunicaciones no solo es un problema tecnológico sino que se extiende sobre la capacidad y honorabilidad de las personas y eficiencia de los procesos.

El montaje de varios tipos de red para valorar el desempeño de los sistemas de seguridad en estas redes resultaría en un costo demasiado elevado, por consiguiente para poder entender y asesorar a cualquier tipo de organización en el desarrollo de una alternativa para la seguridad de su red, es necesario identificar algunos de los nuevos desafíos de seguridad que enfrentan las empresas y por medio de la investigación de diferentes posibilidades de diseño, contribuir a obtener una solución adecuada en términos de seguridad para las redes cableadas e inalámbricas que ellas utilizan.

Este trabajo de grado será orientado a la apropiación de la tecnología, adquisición del conocimiento, respecto a la implementación de seguridad perimetral en las redes de comunicaciones con el fin de desarrollar metodologías de diseño para ser aplicadas a cualquier organización que requiera una red de comunicación segura.

La adquisición del conocimiento de las tecnologías para los sistemas de seguridad perimetral estarán centrados en los siguientes aspectos: Listas de control de Acceso (ACL) en routers y Switchs, Firewalls, WLAN⁷ seguras (Wíreles Security) y Filtros de contenido o Antivirus.

Una vez se tenga todo el conocimiento relativo a los puntos anteriormente propuestos se realizara una simulación donde se pueda mostrar el comportamiento del algoritmo para seguridad inalámbrica WEP⁸.

A partir de esto se puede desarrollar un libro de documentación sobre el montaje de seguridad perimetral para redes de comunicaciones el cual puede ser utilizado para asesorar a organizaciones del sector en la implementación de estas tecnologías.

Y como herramientas finales se pretende desarrollar una presentación en formato multimedia para la presentación y explicación de los aspectos sobre seguridad perimetral anteriormente planteados, con el fin de permitir un entendimiento mas didáctico sobre estos aspectos.

Además de esto se realizará una evaluación de paquetes software de distribución libre, que permitan llevar acabo la seguridad perimetral en redes de comunicaciones.

En conclusión, el problema consiste en abordar los temas fundamentales en el área de **seguridad perimetral**, a fin de proponer una metodología que facilite el diagnóstico, diseño e implementación de sistemas de seguridad perimetral en las redes de comunicación de cualquier organización que lo requiera.

⁷ Wireless Lan

⁸ Wired Equivalency Privacy

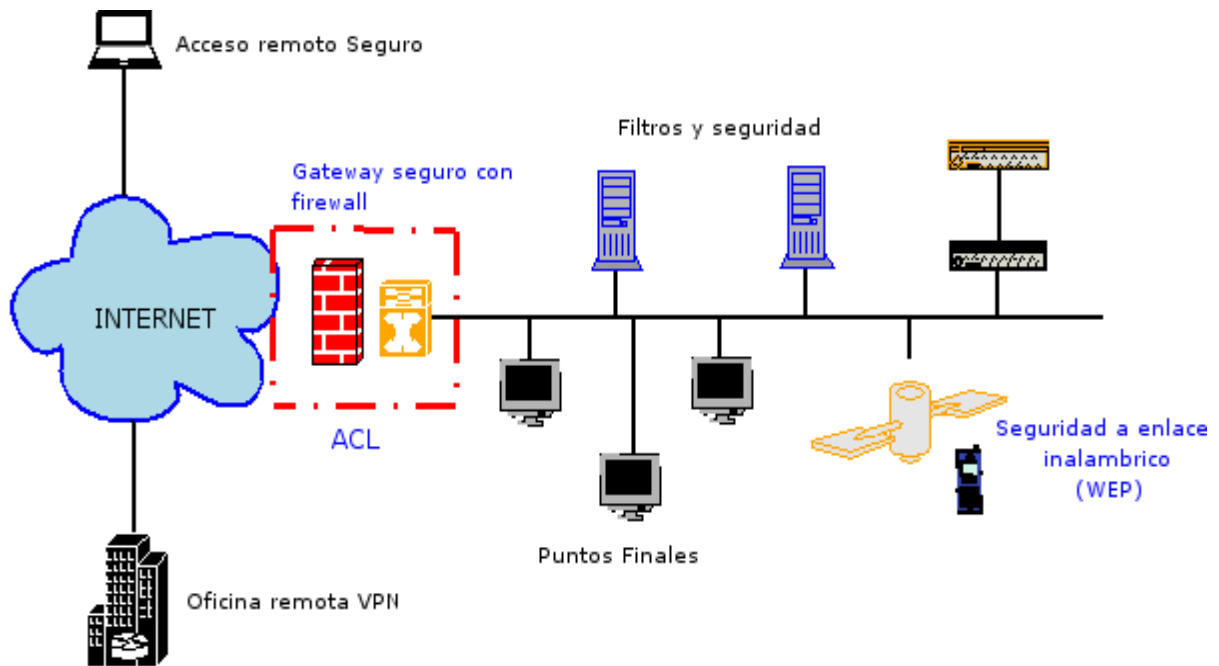


Figura 1. Esquema de una red: Firewall y puntos de implementación de seguridad perimetral

4. JUSTIFICACION

Las amenazas de seguridad que enfrentan las redes de datos en Colombia son suficientes para pensar en las posibles soluciones que disponemos en la actualidad para enfrentar dichas amenazas, esto nos plantea el problema de cual es la mejor manera para resolver esta situación. Estas intrusiones no deseadas pueden ser detenidas siempre y cuando las organizaciones definan e implementen de una manera clara sus opciones en seguridad perimetral, esto en concordancia con las políticas de seguridad previamente establecidas.

En un alto porcentaje las organizaciones colombianas, carecen de profesionales y recursos en el tema de seguridad de redes de datos y por tal razón permanentemente están expuestas tanto a amenazas internas originadas desde el interior de la organización por medio de sus empleados, como a amenazas externas originadas por fuera de la organización, esto último se presenta especialmente cuando una organización se interconecta con otras organizaciones o con la Internet.

Para impedir o contrarrestar los riesgos que las intrusiones no deseadas pueden causarle a cualquier tipo de organización es necesario conocer y estar en la capacidad de poder implementar mecanismos de seguridad para sus redes de datos.

En este proyecto se desea investigar las soluciones de seguridad perimetral en redes que son factibles de implementar en el contexto de las instituciones con una relación costo-beneficio favorable. Además de esto permitir que las instituciones del sector colombiano desarrollen y avancen en tecnologías de seguridad lo cual va a permitir el incremento de la confiabilidad en las empresas y así un desarrollo favorable para la región.

Además se presentan bases sólidas que puedan permitir la implementación redes inalámbricas en la Universidad del Valle con el fin de facilitar el acceso a la red a los estudiantes y profesores contando con la seguridad adecuada.

5. OBJETIVOS

5.1. GENERAL

Desarrollo de una herramienta multimedia de entrenamiento, que permita representar el funcionamiento y las soluciones basadas en listas de control de acceso, Firewalls, seguridad inalámbrica y filtros de contenido o antivirus en el ámbito de la seguridad perimetral, en Redes de Comunicaciones.

5.2. ESPECIFICOS

- Apropiación del conocimiento, en listas de control de acceso, Firewalls, seguridad inalámbrica y filtros de contenido o antivirus en el ámbito de la seguridad perimetral.
- Desarrollo de una herramienta de simulación del algoritmo WEP.
- Investigación y estudio de una solución para la conexión inalámbrica basada en VPN⁹, que sea de utilidad para una organización, lo cual incluye:

⁹ Virtual Private Network

- Evaluación de costos en la implementación
- Evaluación de las técnicas de desarrollo ya sean software o hardware
- Evaluación de las relaciones costo/beneficio empresariales.
- Estudio del estándar 802.1X

6. MARCO TEORICO

ACL (Listas de control de acceso): [7]

Las listas de acceso (ACL) se usan para el filtrado de paquetes en función de ciertos parámetros como pueden ser las direcciones de red origen o destino, los puertos origen o destino, el tipo de protocolo (ip, icmp, tcp, udp, etc). Una de las aplicaciones donde se usan más las listas de acceso es en la seguridad de la red. Con las ACLs se puede bloquear el tráfico no deseado en una interfaz ya sea de salida o de entrada. Sin embargo se debe apreciar que las ACLs no solo se usan en temas de seguridad, sino que también se usan para filtrar en general paquetes en aplicaciones tan variadas como pueden ser NAT (Network Address Translation), en BGP para filtrar rutas al crear políticas de encaminamiento, etc.

Existen ACLs para distintas pilas de protocolos: TCP/IP, IPX/SPX¹⁰, Apple¹¹, etc. La diferencia entre las pilas de protocolos está en el rango de ACLs que se pueden generar. Por ejemplo las ACLs entre la 1 y la 199 se usan en TCP/IP, mientras que las comprendidas entre la 800 y la 999 se usan para IPX/SPX, otros rangos se usan para DECnet¹² (300-399), XNS¹³ (400-599), AppleTalk (600-699), etc.

Cuando creamos una lista de acceso y la aplicamos a una interfaz de entrada o de salida, estamos creando una secuencia de instrucciones que son revisadas cada vez que un paquete entra o sale por esa interfaz. Es importante notar varias características de las ACLs.

Primero, que una ACL se aplica a la interfaz ya sea de entrada o de salida. Se pueden crear una ACL para la interfaz de salida y otra distinta para esa interfaz de entrada.

¹⁰ Internetwork Packet Exchange / Sequenced Packet Exchange

¹¹ Protocolo de la firma Apple

¹² Digital Equipment Corporation protocol suite

¹³ XEROX Network System

Lo segundo, las ACLs son secuencias de instrucciones que son revisadas contra el paquete. El orden de las instrucciones es importante, ya que cuando una línea de la secuencia da cierta en el chequeo, se toma una acción y se sale de la ACL, es decir no se continua chequeando para comprobar que haya otra línea de la secuencia que también resulta cierta. Por consiguiente es muy importante diseñar la ACL en la secuencia que nos interese más.

Otro aspecto importante es que no podemos insertar líneas en la secuencia. Si nos equivocamos al crearla o queremos insertar una línea a hay que borrar toda la ACL y volverla a crear. [9]

Finalmente, también muy importante, la última línea de una lista de acceso nunca aparece, es decir existe de forma implícita y siempre denegará todo.

Dentro de las listas de acceso TCP/IP hay dos tipos de ACLs:

Listas de acceso IP¹⁴ estándar (1-99)

Listas de acceso IP extendidas (100-199)

Firewalls: Un Firewall es un sistema o grupo de sistemas ubicado entre dos redes con la tarea de establecer una política de control de tráfico entre éstas. Es decir, es un sistema empleado para proteger una red del resto de las redes.

En todo Firewall existen tres componentes básicos para los que deben ser implementados mecanismos de seguridad: el filtrado de paquetes, el Proxy de aplicación y la monitorización y detección de actividad sospechosa.

Filtrado de Paquetes (choke): [6]

Su funcionamiento es generalmente muy simple: se analiza la cabecera de cada paquete y en función de una serie de reglas ya establecidas, el paquete es bloqueado o se le permite continuar.

El filtrado de paquetes se puede basar en cualquiera de los siguientes criterios:

- Protocolos utilizados

¹⁴ Internet Protocol

- Dirección IP de origen y de destino
- Puerto TCP-UDP¹⁵ de origen y destino

Algunas implementaciones de filtrado permiten además especificar reglas basadas en la interfaz del router por donde se reenvía el paquete y también en la interfaz por donde llega a nuestra red.

Estas reglas se especifican generalmente como una tabla de condiciones y acciones que se consulta en un orden dado hasta encontrar una regla que permita tomar una decisión sobre el bloqueo o el reenvío del datagrama.

Proxy de Aplicación

Es un software encargado de filtrar las conexiones a servicios como FTP¹⁶, Telnet¹⁷, etc. La máquina donde es ejecutada esta aplicación es llamada Host Bastión o Gateway de Aplicación.

Los servicios Proxy permiten únicamente la utilización de servicios para los que existe un Proxy, así que, si el Gateway posee Proxy únicamente para HTTP¹⁸ y FTP, el resto de servicios no estarán disponibles para nadie. Además, es posible filtrar protocolos basándose en algo más que la cabecera de los paquetes. Por ejemplo, se puede tener habilitado un servicio como FTP pero con órdenes restringidas. Además, los Gateway permiten cierto grado de ocultación de la topología de red, facilita la autenticación y la auditoria de tráfico sospechoso antes de alcanzar al host destino. Además, simplifica considerablemente las reglas de filtrado implementadas en el router.

Monitoreo de la Actividad

El monitoreo de la actividad del Firewall es indispensable para la seguridad de la red, ya que así se podrá obtener información acerca de los intentos de ataque a los que puede estar sometido.

¹⁵ User Datagram Protocol

¹⁶ File Transfer Protocol

¹⁷ Programa de emulación de Terminal para TCP/IP

¹⁸ Hypertext Transfer Protocol

Arquitecturas de firewalls [10]

Firewalls de Filtrado de paquetes: Consiste en utilizar un router y aprovechar su capacidad de filtrar paquetes (como ya fue explicado). Este tipo de Firewalls trabajan en los niveles de red y de transporte del modelo OSI¹⁹ y tienen la ventaja de ser bastante económicos, pero traen consigo una serie de desventajas como son:

- No protege las capas superiores.
- No son capaces de esconder la topología de la red protegida.
- No disponen de un buen sistema de monitoreo, por lo que muchas veces no se puede determinar si el router está siendo atacado.
- No soportan políticas de seguridad complejas como autenticación de usuarios.

Dual-Homed Host: Está formado por máquinas Unix equipadas con dos o más tarjetas de red. En una de las tarjetas se conecta la red interna y en la otra, la red externa. En esta configuración, la máquina Unix hace las veces de Gateway y de choke.

El sistema ejecuta al menos un servidor proxy para cada uno de los servicios que pasarán a través del Firewall y es necesario que el IP-Forwarding esté desactivado en el equipo: Aunque una máquina con dos tarjetas de red puede actuar como router, para aislar el tráfico entre la red interna y la externa, es necesario que el choke no enrute paquetes entre ellas.

Screened Host: Se combina un enrutador con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el choke se filtran los paquetes considerados peligrosos y sólo se permite un número reducido de servicios.

Screened Subnet: En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall: el host bastión. Para ello se establece una zona desmilitarizada (DMZ) de forma tal que si un intruso accede a esta máquina, no consiga el acceso total a la subred protegida.

En este esquema se utilizan dos enrutadores: uno exterior y otro interior. El enrutador exterior es el encargado de bloquear el tráfico hacia y desde la red interna. El enrutador interno se coloca entre la red interna y la DMZ (zona entre el enrutador externo y el interno).

¹⁹ Open Systems Interconnection

Seguridad wireless y filtro de contenido: Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos: [1] [3]

Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.

Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red:

Método 1: [5]

Filtrado de direcciones MAC Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas. Las

direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack o WellenReiter, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.

En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

Método 2:

Wired Equivalent Privacy (WEP) [8]

El algoritmo WEP10 forma parte de la especificación 802.11 [11], y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El algoritmo WEP cifra de la siguiente manera:

A la trama en claro se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.

La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números pseudo-aleatorios. El generador RC4 es capaz de generar una secuencia pseudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).

Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada. El IV y la trama se transmiten juntos.

En el receptor se lleva a cabo el proceso de descifrado. Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor. Un generador RC4 produce la cifra de flujo a partir de la semilla.

Si la semilla coincide con la empleada: en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.

Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrada, obteniéndose de esta manera la trama en claro y el ICV.

A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.

Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2^{24} IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto

tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

WEP no ofrece servicio de autenticación. El cliente no puede autenticarse a la red, ni al contrario; hasta que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

Método 3: Las VPN Una red privada virtual (Virtual PrivateNetwork, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP. [11]

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN.

Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

Método 4: 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. [4]

Filtrado de contenido: los programas para filtrado de contenido en las redes de comunicaciones se pueden especificar de la siguiente manera: [2]

EMPRESAS/SECTOR PUBLICO es un servicio que permite optimizar el uso de los recursos técnicos y humanos de Internet en la empresa. Ya que hace posible el definir, por grupos de usuarios, horarios y tipos de contenidos a los que se inhabilita el acceso por carecer de interés para la empresa.

CENTROS EDUCATIVOS es un servicio que limita el acceso a contenidos nocivos para los menores, lo que permitirá a los educadores beneficiarse de todas las posibilidades que ofrece Internet, sin ningún riesgo.

HOGAR es un sistema que permite seleccionar los contenidos en Internet, evitando el acceso de los menores a páginas web de contenidos pornográficos, de drogas, sectas, violencia, racismo y construcción de explosivos. Hace que Internet se convierta en una herramienta más segura para los menores.

El software ISPs es un sistema de filtrado de accesos que se instala en el servidor del ISP y permite a este ofrecer a sus clientes la posibilidad de limitar el acceso a contenidos nocivos para el menor. Aportando al ISP un valor añadido diferenciador.

Para la realización de este filtrado el software utiliza un analizador semántico para clasificar de forma automática el tipo de contenido o categoría de Internet, permitiendo su visualización en función de los criterios predefinidos. El análisis se lleva a cabo de forma "on-line", cada vez que se solicite el contenido de una URL.

La mayoría de los analizadores semánticos on-line desarrollados, están complementado con un sistema de listas, lo que asegura la mayor eficacia del mercado 97% y una mínima tasa de error 0,1%.

El software está complementado con un servicio de desbloqueo del 0,1% de URLs filtradas por error, lo que reduce dicha tasa de error al 0%.

6.1 ESTADO DEL ARTE

Los sistemas de seguridad perimetral están formados por cuatro componentes fundamentales: Listas de control de Acceso (ACL) en *routers* y *Switchs*, *Firewalls* como el *PIX Firewall* e *IOS Firewall* que brindan una barrera para el tráfico que atraviesa el perímetro de una red y sólo permiten que el tráfico autorizado pase, WLAN seguras tales como el paquete *Cisco Wirless Security*, y las herramientas complementarias como los filtros de contenido y antivirus.

7. ASPECTOS METODOLOGICOS

Para cumplir con los objetivos propuestos se llevará acabo la siguiente metodología la cual esta enmarcada en cuatro pasos fundamentales:

1. Apropiación del conocimiento, para crear bases teóricas que nos permitan desarrollar el tema de seguridad perimetral. Esta apropiación del conocimiento es fundamental dadas las características del tema a desarrollar como son:

- Es un tema relativamente nuevo en el área de las telecomunicaciones
- Se carece de suficientes profesionales capacitados en este tema en la actualidad, lo cual aumenta su importancia de desarrollo.

2. Desarrollo de una herramienta de Simulación: esta parte requiere de recolectar y sintetizar toda la documentación pertinente a la seguridad perimetral (Algoritmo WEP) en redes de comunicaciones.

Con esta documentación se pretende simular la técnica base en el desarrollo de los elementos que constituyen el algoritmo WEP en la seguridad perimetral en las redes de comunicaciones.

Esto incluye definir la plataforma a utilizar ya sea Matlab u otra herramienta. La escogencia de esta herramienta se hará bajo criterios de funcionalidad para la implementación de algoritmos, disponibilidad y aplicabilidad para el desarrollo de ambientes amistosos con el usuario.

3. Desarrollar una presentación gráfica de cada tema implicado en la seguridad perimetral para redes de comunicaciones que pueda servir como herramienta de entrenamiento y capacitación de cada tema.

También se debe definir la plataforma a utilizar esta plataforma para desarrollo de documentaciones gráficas puede ser: Java o Flash de Macromedia. La escogencia de esta herramienta se realizará bajo criterios de fácil disponibilidad, acceso a la documentación y fácil manejo de esta herramienta.

4. Como parte final se realizará el estudio de software que facilite la aplicación de la seguridad perimetral orientada a redes de comunicaciones. Este Software a implementar se debe valorar, analizar y catalogar en preferencia este software debe ser de distribución libre.

Como último paso se hará el informe correspondiente a toda la ejecución del proyecto con base en los resultados obtenidos.

8. RESULTADOS ESPERADOS

Como resultado principal se espera el desarrollo y la consecución de todos los objetivos anteriormente propuestos. El desarrollo de estos objetivos implica el desarrollo de un proyecto que permitirá:

Obtener un informe que permitirá la asesoría a cualquier entidad sobre la implementación de seguridad perimetral en sus redes de comunicaciones.

Diseñar una documentación gráfica para poder realizar una capacitación u asesoría a cualquier entidad sobre las técnicas base desarrolladas en seguridad perimetral.

Dotar al laboratorio de comunicaciones de una herramienta para la simulación del algoritmo de seguridad perimetral WEP.

Realizar un documento donde se informe sobre el análisis, valoración e implementación de software para la aplicación de seguridad perimetral en redes.

Se espera dejar un documento que sirva de base para posteriores desarrollos sobre nuevas implementaciones o distintas tecnologías aplicadas a la seguridad perimetral.

9. PRESUPUESTO

En la Tabla 1 se presenta el presupuesto necesario para el desarrollo del trabajo de grado.

Necesidad	Costo
Internet	450000
Libros	300000
Fotocopias - Papelería	60000
Computador	2000000
TOTAL	2810000

Tabla1. Presupuesto para el trabajo de grado

10. CRONOGRAMA DE ACTIVIDADES

Las actividades para el desarrollo del trabajo de grado serán divididas en los cuatro pasos mencionados en los aspectos metodológicos. El siguiente cuadro resume en tiempo el cronograma de actividades a desarrollar.

PASO	MES								
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE
	2006	2006	2006	2006	2006	2006	2006	2006	2006
PASO1									
PASO2									
PASO3									
PASO4									

Tabla 2. Cronograma de actividades

11. GLOSARIO

Amenaza: Situación o evento con que puede provocar daños en un sistema.

Análisis de vulnerabilidades: Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.

Análisis dinámico, o en tiempo real: Análisis desarrollado en tiempo real, o de forma continúa.

Análisis sin acreditaciones: En análisis de vulnerabilidades, enfoque de monitorización pasiva en los que las contraseñas u otro tipo de credenciales no son necesarias. Normalmente implica el lanzamiento de ataques contra el sistema, provocando algún tipo de reacción.

Aplicación engañosa: Aplicación cuya apariencia y comportamiento emulan a una aplicación real. Normalmente se utiliza para monitorizar acciones realizadas por atacantes o intrusos.

Ataque por interceptación: Estrategia de ataque en la que el atacante intercepta una comunicación entre dos partes, substituyendo el tráfico entre ambas a voluntad y controlando la comunicación.

Autenticación, autentificación: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.).

Autorización: Acción de otorgar el acceso a usuarios, objetos o procesos.

Basado en reglas: En detección de intrusiones, que utiliza patrones de actividad (generalmente ataques conocidos) para reconocer una intrusión.

Basado en testigo: Sistemas que emplean elementos especiales como tarjetas inteligentes, llaves, o discos para la autenticación de usuario.

Base de reglas: Conjunto de reglas utilizadas para analizar los registros de datos.

Caballo de Troya, troyano: Programa informático de aspecto inofensivo que oculta en su interior un código que permite abrir una "puerta trasera" en el sistema en que se ejecuta.

Capacidad de ser registrado: Habilidad de relacionar una determinada actividad o evento con la parte responsable.

Cifrado: Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.

Composición: 1. En detección de intrusiones, proceso de combinar información procedente de distintas fuentes en un flujo de datos coherente. 2. En seguridad informática, combinar un conjunto de componentes en un sistema para obtener los atributos de seguridad del sistema, según las propiedades de los componentes.

Comprobador de integridad: Herramienta de seguridad que utiliza funciones resumen basadas en algoritmos de cifrado para detectar alteraciones en objetos de sistema.

Control de acceso: Limitar el acceso a objetos de acuerdo a los permisos de acceso del sujeto. El control de acceso puede ser definido por el sistema (Control de accesos obligatorio, MAC) o por el propietario del objeto (Control de accesos discrecional, DAC).

Control de acceso discrecional (DAC): Política de acceso a los datos en la que el propietario del objeto, de forma voluntaria (discrecional), concede o deniega el acceso a éste a otros sujetos.

Control de accesos obligatorio (MAC): Política de acceso a los datos en la que el sistema comparte de forma obligatoria tanto los objetos como los sujetos. A partir de dicha forma de compartir los elementos, se establecen unas reglas de acceso.

Cortafuegos: Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad mediante el uso de políticas de control de acceso de nivel de red.

Criterio de Evaluación de Sistemas Informáticos Fiables (TCSEC): Conocido comúnmente como Libro Naranja, describe las propiedades que deben cumplir los sistemas para contener información sensible o clasificada. Este criterio fue desarrollado por el Centro de Seguridad Informática Nacional (NCSC).

Datagrama: Mensaje que se envía en una red de comunicaciones de ordenadores por intercambio de paquetes.

Denegación de servicio distribuida (DDoS): Estrategia de ataque que coordina la acción de múltiples sistemas para saturar a la víctima con información inútil para detener los servicios que ofrece. Los sistemas utilizados para el ataque suelen haber sido previamente

Deslizamiento sigiloso de sesión: Técnica utilizada por un usuario que consiste en modificar gradualmente su comportamiento para entrenar al detector de anomalías. De esta forma, se consigue que el detector diagnostique como actividad normal un posible ataque.

Detección de intrusiones: Proceso de monitorizar los eventos de un sistema o red en busca de signos que indiquen problemas de seguridad.

Detector de Intrusiones de Nodo de Red: Detector de intrusiones basado en red que se instala en una máquina. Esta medida ayuda a solventar problemas como los asociados a entornos conmutados, o cifrado en las comunicaciones.

Enmascarado: Atacante que accede a un sistema utilizando identificadores de usuario y contraseñas de usuarios legítimos.

Error de Tipo I: En detección de intrusiones, error producido cuando el sistema diagnostica como ataque una actividad normal. También conocido como falso positivo.

Error de Tipo II: En detección de intrusiones, error producido cuando el sistema diagnostica como actividad normal un ataque. También conocido como falso negativo.

Escaneo sigiloso de puertos: Barrido de puertos mediante diversas técnicas con el fin de evadir los métodos de detección comunes. Algunas de estas técnicas implican un escaneo intencionadamente lento, o el envío de paquetes especiales aprovechando particularidades del protocolo.

Firma, patrón: En detección de intrusiones, patrones que indican los usos indebidos de un sistema.

Formato de registro binario: Formato de registro utilizado por herramientas basadas en las librerías "libpcap", como por ejemplo "tcpdump". Se aplica para registrar el tráfico de red. Algunas de las ventajas del formato binario sobre el formato ASCII son que ocupa menos, y la información que contiene puede ser accedida en menor tiempo.

Gestión de redes: Controlar diversos aspectos de una red para optimizar su eficiencia. Las cinco categorías de gestión de red son: seguridad, fallo, auditoría, configuración y gestión de rendimiento.

Gestión de seguridad: 1. Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución. 2. En gestión de redes, controlar (permitir, limitar, restringir, o denegar) acceso a la red y recursos, buscar intrusiones, identificar puntos de entrada de intrusiones, y reparar o cerrar estas posibles vías de acceso.

Identificación y autenticación (I&A): Mecanismo de seguridad que asigna una identidad única a cada usuario (identificación) y la comprueba (autenticación).

Libpcap: Interfaz independiente del sistema, para la captura de paquetes de nivel de usuario, escrito en el "Lawrence Berkeley National Laboratory".

Libro Marrón ("Guía para la Comprensión de la Auditoría en Sistemas de Confianza"): Uno de los volúmenes de la Serie Arco Iris que explica los criterios del sistema de auditoría de Sistemas de Confianza, mencionando aspectos relevantes para los sistemas de detección de intrusiones.

Lista de Control de Acceso (ACL): Conjunto de datos que indican al sistema operativo qué permisos tiene un usuario o grupo sobre un determinado objeto de sistema. Cada objeto tiene atributos de seguridad únicos que indican qué usuarios pueden accederlo, y la Lista de Control de Acceso contiene una descripción de los privilegios de acceso de cada objeto y usuario.

Módulo de Seguridad Básico (BSM): Paquete de seguridad de Sun Microsystems proporcionado por los sistemas operativos de Sun para cumplir con los requisitos del documento TCSEC (la clase C2).

Paquete: Estructura de datos con una cabecera que puede estar o no lógicamente completa. Más a menudo, se refiere a un empaquetamiento físico de datos que lógico. Se utiliza para enviar datos a través de una red conmutada de paquetes.

Política de seguridad: 1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. 2. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.

Puerta trasera: Mecanismo que permite a un atacante entrar y controlar un sistema de forma oculta. Suelen instalarse justo después de comprometer un sistema.

Sistema de prevención de intrusiones (IPS): Sistema que combina las capacidades de bloqueo de un cortafuegos y las de análisis de un IDS. Está diseñado para detener ataques antes de que tengan éxito.

Virus polimórfico: Virus informático que cambia de aspecto con cada ejecución. Esta característica tiene el objeto de evitar los detectores de virus.

Vulnerabilidades: Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.

Zona desmilitarizada, red perimétrica (DMZ): Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar, y se utiliza para definir un área situada entre dos enemigos

12. REFERENCIAS

[1] Stubblefield Addam, Ioannidis John, Rubin Aviel D. “Using the Fluhrer, Mantin and Shamir Attack to break WEP”, Revision 2, Agosto 2001,. Recuperado de Internet: <URL: <http://whitepapers.zdnet.co.uk/0,39025945,60022729p,00.htm>>.

[2] Zhou Lidong, Haas Zygmunt J. “Securing Ad Hoc Networks”, IEEE Network, Vol. 13, No. 6, pp 24-30, Junio 1999.

[3] Arbaugh William A., Shankar Narendar, Wan Justin Y. C., “Your 802.11 Wireless Network has No Clothes” IEEE Wireless Communications, Vol. 9, No. 6, pp. 44-51, Diciembre 2002.

[4] Borisov Niñita, Goldberg Ian, Wagner David, “(In)Security of the Wep algorithm”, Recuperado de Internet: < URL: <http://www.gta.ufrj.br/~eric/tese/artigos/wep-faq.html>>.

[5] Madrid Molina Juan Manuel, “Seguridad en Redes inalámbricas 802.11”, Revista Sistemas y Telemática, Universidad Icesi, Cali (Colombia), ISSN 1692-5238, pp. 13-28, Enero 2004.

[6] Goncalves Marcus, “Firewalls Complete”, Mc Graw Hill Beta Books, Cap 6, Enero 1997, Recuperado de Internet: <URL: <http://www.ods.com.ua/win/eng/security/firewall/preface.htm>>

[7] Cisco White Papers “Access Control Lists and IP fragments”, document ID: 8014, Agosto 2005, Recuperado de internet: <URL: http://www.cisco.com/warp/public/105/acl_wp.html>.

[8] Menezes Alfred J., Van Oorschot Paul C., Veneton Scott A., “Handbook of applied Cryptography”, CRC press, 1996.

[9] Tipson Harold F., Krause Micki, CISSP., “Information Security Management Handbook”, CRC Press LLC, ISBN: 0849399475, Recuperado de Internet: <URL: <http://www.cccure.org/Documents/HISM/ewtoc.html>>.

[10] Jiménez Arévalo Fernando Andres, “Como escoger e implmentar una VPN concéptos teóricos y practices”, Trabajo de Grado, Universidad del Valle, Cap 4., pp 84-92, 2003.

[11] International Telecommunication Union, “Accessing ITU’s Wireless Facilities”, septiembre 2003, Recuperado de internet: <URL: www.itu.int/ITU-T/edh/files/InfoWirelessLAN.pdf>