UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ANÁLISIS PARA LA SEGURIDAD DE PAQUETES DE DATOS Y EVITAR ATAQUES MEDIANTE SNIFFING.

Estudiante

Pablo José Vinueza Carangui

Tutor

Msc. Marco Lituma Orellana Ing.

Cuenca – Ecuador

ACTA DE CESIÓN DE DERECHOS

Yo, Pablo José Vinueza Carangui, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Quito, Noviembre 07 del 2011.

_____

Pablo José Vinueza Carangui

C.I 010599799-3

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORIA

El documento de tesis con título **"Análisis para la seguridad de paquetes de datos y evitar ataques mediante Sniffing"**, ha sido desarrollado por Pablo José Vinueza Carangui con C.C. No. 010599799-3 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Pablo José Vinueza Carangui

DEDICATORIA

La presente Tesis de grado la dedico a mis padres y familia, quienes con su amor, pasiencia y comprensión, siempre me han brindado su apoyo para poder cumplir con esta etapa de enorme importancia en mi vida.

AGRADECIMIENTO

Para llegar a este punto de mi vida en que estoy a punto de alcanzar una de mis metas fue necesario el apoyo de varias personas a las cuales quiero agradecer.

En primer lugar a mis padres Guillermo y Laura, quienes han sido un apoyo moral, afectivo y económico para lograr este fin, gracias por todo su apoyo.

Al señor asesor de tesis que con su guía se pudo desarrollar satisfactoriamente mi tesis.

Amis hermanos y amigos por ayudarme y apoyarme sin condiciones. Gracias

RESUMEN

Sniffing, es una técnica que permite tener un ojo en el flujo de información, es decir tener acceso a la información que es enviada o recibida por nuestros adaptadores de red, y algunas veces por el de otras personas computadoras también. Un Sniffer, utilidad que permite el sniffing, se llama formalmente analizador de paquetes o analizador de red.

El sniffing tiene una gran ventaja sobre las intervenciones telefónicas puesto que la mayoría de las redes aún usan topologías de red compartidas, esto quiere decir que no es necesario que el ordenador al cual se quiera monitorizar deba estar situado en las proximidades, simplemente si está conectado al mismo cable será susceptible de ser intervenido, conociéndose esto como un sniffer en modo promiscuo. En cambio, la tecnología compartida (usando hubs) está rápidamente desplazándose a tecnología conmutada (switches), donde estas tácticas ya no son posibles, aun así existen varias técnicas de sniffing usadas en redes conmutadas.

Todo lo anterior nos indica que el robo de información, a diferencia de lo que se cree, en la mayoría de los casos no suele ser cuestión de un hacker, sino de algún empleado descontento, o de un jefe demasiado celoso con el trabajo y la vigilancia de sus subordinados.

Es importante resaltar que el espionaje de las comunicaciones personales es un delito, lo cual incluye a empleados y también a jefes.

SUMMARY

Sniffing is a technique to keep an eye on the flow of information, ie access to information that is sent or received by our network adapters, and sometimes by other people's computers too. A sniffer, sniffing utility that allows, is formally called packet analyzer or network analyzer.

The sniffing is a big advantage over the wiretaps since most networks still use shared network topologies, this means that it is not necessary that the computer which you want to monitor should be located nearby, just if connected the same cable will be capable of being involved, knowing that as a sniffer in promiscuous mode. In contrast, shared technology (using hubs) technology is rapidly moving to switched (switches), where these tactics are no longer possible, yet there are several techniques used sniffing in switched networks.

All this indicates that the theft of information, contrary to popular belief, in most cases is not usually a matter of a hacker, but a disgruntled employee or a boss too jealous of the work and supervision of subordinates.

It is important to note that the personal communications espionage is a crime, which includes employees as well as bosses.

INDICE

CAPITULO 1

1. Introducción

Análisis para la seguridad de Paquetes de Datos y evitar ataques mediante Sniffing.

Los programas para realizar sniffing se han distribuido de dos formas diferenciadas: comerciales y “underground”.

Los sniffers comerciales se usan para mantener redes, y los sniffers “underground” se usan para asaltar a los ordenadores de una red. Aunque es cierto que siempre hay una sutil diferencia entre las herramientas usadas para asegurar un sistema y las usadas para entrar en él, podemos decir que en la actualidad el 99 por ciento de los sniffers utilizados ya sea con unos fines u otros están disponibles a los usuarios como software comercial, shareware o freeware.

1.1. Causa – Efectos

1. Tener un mejor control en el aspecto de seguridad al envío de un paquete de datos.

Permitirán a los usuarios sentir mayor comodidad sabiendo que su información está segura ante algún tipo de ataque.

2. Desconocimiento de técnicas de seguridades informáticas.

Cometer errores por parte de usuarios como administradores en una red en cuanto al tratamiento de información se refiere.

3. Pérdida de paquetes de datos

Por la falta de sistemas y metodologías de seguridad al envío de los mismos.

4. Congestión en el tráfico de la Red

Vulnerabilidad e inseguridad por parte de los usuarios.

5. Ataques de hackers

Captura de los paquetes de datos consiguiendo con ello tener acceso a datos e información de un usuario quien puede ser escogido previamente por parte de esta persona.

Al enviar un paquete en la red, las únicas direcciones posibles que tiene el paquete para saber el destino de este, es su dirección IP y la dirección MAC de la tarjeta de red. La dirección IP está contenida en el paquete de información, pero la dirección MAC del paquete de destino no se sabe, por lo que es necesario mandar una petición para que devuelva si dirección MAC, esto se logra mediante los protocolos ARP.

1.2. Pronóstico y control del Pronóstico

Para lograr un control de estos pronósticos se emplean análisis de sus propios paquetes de datos que circulan en la red, buscar soluciones, tiempos de respuesta. Al realizar un análisis de las problemáticas e inseguridad que tienen los paquetes de datos al momento de ser enviados, nos podrá ayudar a tomar medidas de seguridad en cuanto a este aspecto se refiere.

1.3. Problema Principal

Los ataques de sniffer son difíciles de detectar, debido a que son programas pasivos, que ocupan poca memoria y casi no dejan rastros en el computador donde se instaló. Son necesarios conocimientos de ARP (protocolo de resolución de direcciones) para la resolución de direcciones en informática, es el responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP, para poder tratar de rastrear estos programas.

1.4. Problemas Secundarios

Inseguridad al momento de controlar el envío de un paquete de datos.

Desconocimiento de técnicas de seguridades informáticas.

Pérdida de paquetes de datos.

Congestión en el tráfico de la Red.

Ataques de hackers.

1.5. Objetivos

1.5.1. Objetivo General

Análisis de los paquetes de datos investigando protocolos estándares de seguridad y medidas de protección, de los datos que viajen a través de la red mediante sniffing, con ello evitar posibles ataques de hackers o intrusos, quienes puedan tener acceso a la información que se envíen usándolos de una manera indebida.

1.5.2. Objetivos Específicos

- Analizar: el envío/recepción de paquetes de datos o fallos en la red al momento de la transferencia de datos.
- Diagnosticar: Cuales son las principales razones de la pérdida de datos en la red.
- Medir: El estado de la red revisando su tráfico, mediante herramientas y software apropiados para descubrir fallos en la red o programas maliciosos.
- Detectar: Ataques de Hackers o intrusos mediante sniffing.
- Proteger: Propuesta del esquema de protección de datos que viajan a través de la red.
- Recomendar los mejores tipos de cifrado y encriptación para paquetes de datos.

1.6. Aspectos Importantes

El modo promiscuo y la protección contra sniffer de paquetes. Es un modo de operación en el que una computadora conectada a una red compartida captura todos sus paquetes, y a otras computadoras. Supervisar la red.

Un administrador de redes puede emplear mucho tiempo en conseguir que su red sea difícil de ser atacada mediante sniffers utilizando firewalls, switches, detectores de modo promiscuo, etc., lo cierto es que la mejor forma de protegerse ante estos ataques es la de encriptar el tráfico de red.

Secure Sockets Layer (SSL): está presente en todos los navegadores Web populares así como en los servidores HTTP más conocidos permite una navegación encriptado no vulnerable a los sniffers, por ello, este tipo de seguridad es utilizada en Internet para transmitir información privada de los usuarios.

PGP y S/MIME: El correo puede ser interceptado de muchas formas alternativas un correo electrónico necesita, para llegar a su destino, atravesar distintos servidores de red, firewalls y Reuters, por ello la posibilidad de que alguien pueda leer el correo es muy elevada si se envía sin ningún sistema de encriptación.

Secare Shell (Ssh) se ha convertido en el estándar para acceder remotamente a servidores UNIX a través de Internet. Virtual Private Networks (VPN) las redes virtuales privadas envían la información encriptado desde una red local a otra lejana geográficamente a través de Internet.

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.

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.

Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras.

1.6.2 Seguridad Informática

Seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento

del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática.

La seguridad informática se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema**.**

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software**)** o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas).

Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus**,** los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords).

Un sistema seguro debe ser íntegro (con información modificable sólo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente para los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).

En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

1.6.3. Objetivos de la seguridad informática

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian
- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.
- **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos.

“Seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.” (Aguilera; 2008)

1.6.4. Sniffer

Un sniffer es un programa de para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella. Un sniffer puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red. Un ruteador lee cada paquete de datos que pasa por él, determina de manera intencional el destino del paquete dentro de la red. Un ruteador y un sniffer, pueden leer los datos dentro del paquete así como la dirección de destino.

1.6.4.1. Sniffer para Ataque

Es útil capturando contraseñas, tanto para cuentas de mail, acceso a zonas restringidas para ciertos usuarios. La captura de claves varía desde bromas hasta aspectos más grabes como robar información confidencial de una empresa o de una PC.

1.6.4.2. Defensa contra Sniffer

Los ataques de sniffer son difíciles de detectar, debido a que son programas que se encuentran de una manera pasiva, que ocupan poca memoria y casi no dejan rastros en el computador donde es instalado. Para esto existe software especializado como NEPED, SNIFFDET, ANTISNIFF, SENTINEL.

1.6.4.3 Detección de Sniffers

En general, las técnicas utilizadas para la detección de sniffers parten de que, para olfatear tráfico en red, una computadora debe poner su interfaz de red en modo promiscuo, deshabilitar un filtro en hardware diseñado para ahorrar carga al sistema operativo, que descarta todos los paquetes que no estén dirigidos a esa tarjeta en particular o a la dirección MAC de broadcast (00:00:00:00:00:00).

Al recibir el sistema operativo un paquete no destinado a él, antes de entregarlo para que lo procese y reporte al sniffer, lo pasa por su propia pila para ser procesado. Por lo tanto, si enviamos un ping a una dirección IP con la dirección MAC equivocada o si hacemos una solicitud ARP para una dirección IP sin que vaya en un paquete broadcast y recibimos respuesta, es clara indicación de que esa computadora está corriendo un sniffer.

Varían según se tenga acceso local a la máquina, o bien haya que descubrirlos desde alguna máquina remota. El objetivo que la mayoría de pruebas tratan de conseguir es que la máquina que tiene la tarjeta de red en modo promiscuo se traicione a sí misma, revelando que ha tenido acceso a información que no iba dirigida a ella y que, por tanto, tiene un sniffer.

El sniffer ha sido diseñado exclusivamente para esta tarea (generalmente dispositivos hardware), entonces no devolverá jamás un paquete, no establecerá nunca una comunicación, sino que permanecerá siempre en silencio y su detección remota será, simplemente, imposible. La detección

de este tipo de sniffers sólo puede hacerse por inspección directa de los dispositivos conectados a la red.

1.7. Scanning

Utiliza la técnica de realizar una petición ARP para cada una de las IPs de la red a diagnosticar, pero ojo, los paquetes no van destinados a broadcast, no a una dirección aleatoria e inexistente. Sólo las interfaces en modo promiscuo verán estos paquetes, y de esta manera, sólo estas interfaces contestarán a estas peticiones. Existe también un dispositivo de hardware llamado Tap. Este dispositivo permite conectarse a un Hub o incluso a un switch de red al cual conectásemos un dispositivo (PC), para monitorizar la red.

1.8. Ping de latencia, Test ARP

Comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada. Podemos enviar una petición ARP a nuestro objetivo con toda la información rápida excepto con una dirección hardware de destino errónea.

1.9. IDS

Podemos definir la detección de intrusos (Intrusion Detection ID) como “un modelo de seguridad aplicable tanto a ordenadores como a redes. Un sistema IDS recolecta y analiza información procedente de distintas áreas de un ordenador o red de ordenadores con el objetivo de identificar posibles fallos de seguridad. Este análisis en busca de intrusiones incluye

tanto los posibles ataques externos (desde fuera de nuestra organización) como los internos (debidos a un uso abusivo o fraudulento de los recursos).

1.10. Redes Conmutadas

Cuando los datos hay que enviarlos a largas distancias (e incluso no tan largas), generalmente deben pasar por varios nodos intermedios. Estos nodos son los encargados de encauzar los datos para que lleguen a su destino.

1.11. PGP

Pretty Good Privacy o PGP Su finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

1.12. Protocolos ante la acción de los sniffers

1.12.1. SSH

(Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encriptado, la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptados.

1.12.2. SSL

Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 se usa como algoritmo de hash.

Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

1.12.3. Análisis de fallos, Envió de datos, Trafico de paquetes de información

Captura de las tramas de una red de computadoras, es algo común que por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.), sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él.

1.12.4. Medición del tráfico, Detección de intrusos, Creación de registros de red

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo.

1.13. Cronograma

CRONOGRAMA DE ACTIVIDADES	DISTRIBUCIÓN TEMPORAL											
ACTIVIDADES	SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4
Desarrollo de la Etapa Exploratoria												
Determinación del problema de investigación.												
Ubicación del problema de investigación en el contexto de su problemática.												
Elaboración de la Introducción												
Selección de los elementos necesarios al Marco Teórico												
Formulación de los Objetivos												
Definición de la estrategia Metodológica.												
Elaboración de los instrumentos de investigación.												
Aplicación de los instrumentos (recolección de información)												
Procesamiento de la información.												
Elaboración de conclusiones.												
Elaboración del borrador final del trabajo de grado												
Correcciones al Proyecto												
Entrega del proyecto												

CAPITULO II

2. MARCO DE REFERENCIA

2.8. Marco Teórico

Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras.

2.9. Marco Conceptual

2.9.1. Seguridad Informática

Seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática.

Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles.[1]

“Seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.” (Aguilera; 2008)

2.9.2. Sniffer:

Un sniffer es un programa de para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella. Un sniffer puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red. Un ruteador lee cada paquete de datos que pasa por él, determina de manera intencional el destino del paquete dentro de la red. Un ruteador y un sniffer, pueden leer los datos dentro del paquete así como la dirección de destino.[2]

2.9.3. Sniffer para Ataque

Es útil capturando contraseñas, tanto para cuentas de mail, acceso a zonas restringidas para ciertos usuarios. La captura de claves varía desde bromas hasta aspectos más grabes como robar información confidencial de una empresa o de una PC.

2.9.4. Defensa contra Sniffer

Los ataques de sniffer son difíciles de detectar, debido a que son programas que se encuentran de una manera pasiva, que ocupan poca memoria y casi no dejan rastros en el computador donde es instalado. Para esto existe software especializado como NEPED, SNIFFDET, ANTISNIFF, SENTINEL.

---

1. (http://www.mastermagazine.info/termino/6638.php)
2. (http://www.fortunecity.es/imaginapoder/artes/368/escuela/telecom/sniffer.htm)

2.2.5. Scanning

Utiliza la técnica de realizar una petición ARP para cada una de las IPs de la red a diagnosticar, pero ojo, los paquetes no van destinados a broadcast, no a una dirección aleatoria e inexistente. Sólo las interfaces en modo promiscuo verán estos paquetes, y de esta manera, sólo estas interfaces contestarán a estas peticiones. Existe también un dispositivo de hardware llamado Tap. Este dispositivo permite conectarse a un Hub o incluso a un switch de red al cual conectásemos un dispositivo (PC), para monitorizar la red.[3]

2.2.6. Ping de latencia, Test ARP.

Comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada. Podemos enviar una petición ARP a nuestro objetivo con toda la información rápida excepto con una dirección hardware de destino errónea.[4]

---

3. (http://archives.neohapsis.com/archives/incidents/2003)

4. (http://penta.ufrgs.br/gereseg/unlp/t19home.htm)

2.2.7. IDS

Podemos definir la detección de intrusos (Intrusion Detection ID) como “un modelo de seguridad aplicable tanto a ordenadores como a redes. Un sistema IDS recolecta y analiza información procedente de distintas áreas de un ordenador o red de ordenadores con el objetivo de identificar posibles fallos de seguridad. Este análisis en busca de intrusiones incluye tanto los posibles ataques externos (desde fuera de nuestra organización) como los internos (debidos a un uso abusivo o fraudulento de los recursos).[5]

2.2.8. Protección ante la acción de los sniffers

2.2.8.1. Redes conmutadas

Cuando los datos hay que enviarlos a largas distancias (e incluso no tan largas), generalmente deben pasar por varios nodos intermedios. Estos nodos son los encargados de encauzar los datos para que lleguen a su destino.

5. (http://lists.insecure.org/lists/fulldisclosure/2003/Jun/0049.html)

2.9. PGP

Pretty Good Privacy o PGP Su finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

2.10. SSH

(Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encriptado, la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptados.

2.11. SSL

Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 se usa como algoritmo de hash.

Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

2.12. Análisis de fallos, envió de datos, trafico de paquetes de información

Captura de las tramas de una red de computadoras, es algo común que por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.), sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él.

2.13. Medición del tráfico, detección de intrusos, creación de registros de red

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo.

2.14. Marco Temporal

El proyecto se lo realizara en un periodo de tres meses según lo establecido por las autoridades de la institución.

2.15. Marco Espacial

El presente temas sobre el análisis de seguridades de paquetes de datos mediante sniffers será desarrollado en la Ciudad de Cuenca – Ecuador para ser desarrollado y posteriormente sustentado para la obtención del título profesional de Ingeniero En Sistemas en la universidad Tecnológica Israel.

2.16. Marco Legal

No es legal el robo de información, razón por las que se han desarrollado medidas y software de seguridad en redes informáticas.

CAPITULO III

3. Metodología de Investigación

3.8. Método inductivo – Deductivo

Nos permitirá obtener resultados específicos a partir de hechos generales, comenzando con una parte de la investigación a una totalidad de la misma.

3.9. La observación

El registro de todos los hechos

El análisis

La clasificación de los hechos

3.10. Métodos Empíricos

En la elaboración del trabajo es fundamental utilizar el Método de la Observación Científica, el cual ayudará a tener una visión rápida del tratamiento que tienen las tramas al momento de su envió, haciendo énfasis en la seguridad de los paquetes, teniendo muy en cuenta todos los factores externos y herramientas que pueden ser utilizados de mala manera y con fines perjudiciales.

CAPITULO IV

4. DESARROLLO

4.8. Introducción

Como mecanismos específicos de seguridad se han desarrollado una gran variedad de algoritmos, normas y técnicas para brindar protección a los recursos informáticos y garantizar la integridad, confidencialidad y control de acceso a la información.

4.9. Objetivos

Analizar el flujo de paquetes de datos en una red mediante Sniffing, con ello evitar posibles ataques de hackers o intrusos, quienes puedan tener acceso a la información que se envíe a través de los paquetes de datos, para usarlos de una manera indebida.

4.10. Generalidades

4.10.1. Paquete de datos:

Reciben este nombre cada uno de los bloques en que se divide, en el nivel de Red, la información a enviar. Por debajo del nivel de red se habla de trama de red, aunque el concepto es análogo.

En todo sistema de comunicaciones resulta interesante dividir la información a enviar en bloques de un tamaño máximo conocido. Esto

simplifica el control de la comunicación, las comprobaciones de errores, la gestión de los equipos de encaminamiento (routers).

“Son un conjunto de mensajes de tamaño predefinido, donde cada fracción contiene la información tanto de su procedencia, destino y la información necesaria para el re-ensamblaje del mensaje”

4.10.2. Estructura:

Al igual que las tramas, los paquetes pueden estar formados por una cabecera, una parte de datos y una cola. En la cabecera estarán los campos que pueda necesitar el protocolo de nivel de red, en la cola, si la hubiere, se ubica normalmente algún mecanismo de comprobación de errores.

Dependiendo de que sea una red de datagramas o de circuitos virtuales (CV), la cabecera del paquete contendrá la dirección de las estaciones de origen y destino o el identificador del CV. En las redes de datagramas no suele haber cola, porque no se comprueban errores, quedando esta tarea para el nivel de transporte.

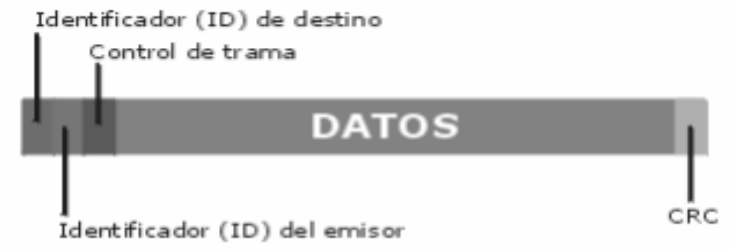

Figura 1 - Estructura de un Paquete de datos

Las partes principales son su identificador o dirección de destino, la dirección de origen, el control de trama el cual nos indica si en el paquete enviado o recibido contiene datos o solo información esto con fines de control.

Luego tenemos los datos enviados y por último se encuentra el CRC el cual es un campo para la detección de errores tanto en los paquetes que enviemos como en los recibidos.

4.10.3. Tamaño de los paquetes:

Paquetes de menos de 64 Bytes

Paquetes entre 65 y 127 bytes

Paquetes entre 128 y 255 bytes

Paquetes entre 256 y 511 bytes

Paquetes entre 512 y 1023 bytes

Paquetes entre 1024 y 1517 bytes

Paquetes mayores de 1518 bytes

4.10.4. Protocolos de los Paquetes de Datos:

Es un método para intercambiar información entre computadoras y que se encuentran regidas por un conjunto de reglas, permite que dos computadoras que tengan un sistema operativo o protocolo de comunicación distinto puedan transmitir datos entre ellas.

4.11. Concepto de Red:

Conjunto de operaciones centralizadas o distribuidas, con el fin específico de compartir recursos de hardware y software, permitiendo la transmisión de datos e intercambio de información entre computadores.

4.12. Tipos de Red

4.12.1. Redes LAN:

Red de área local (LAN) es aquella que se expande en un área pequeña. Comúnmente se encuentra dentro de un edificio o un conjunto de edificios contiguos, puede estar conectada con otras LAN a cualquier distancia por medio de una línea telefónica y ondas de radio. Todas se conectan entre sí por varios medios y topologías. A la computadora (o agrupación de ellas) encargada de llevar el control de la red se le llama servidor ya las PC que dependen de éste, se les conoce como nodos o estaciones de trabajo.

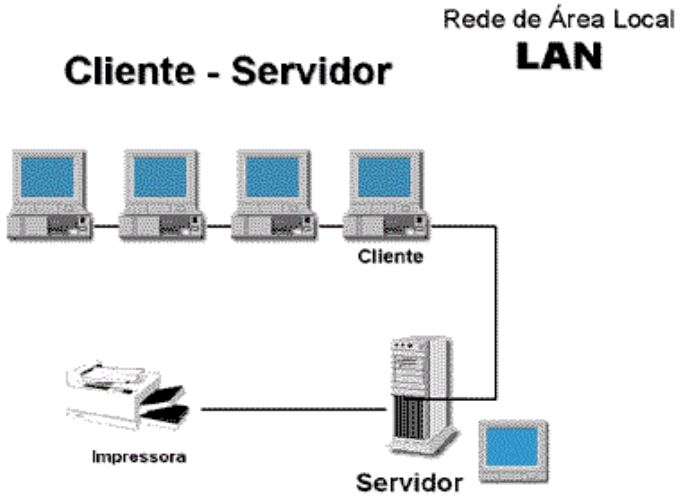

Figura 2 - Red LAN

Los nodos de una red pueden ser PC que cuentan con su propio CPU, disco duro y software. Tienen la capacidad de conectarse a la red en un momento dado o pueden ser PC sin CPU o disco duro, es decir, se convierten en terminales tontas, las cuales tienen que estar conectadas a la red para su funcionamiento.

Las LAN son capaces de transmitir datos a velocidades muy altas, algunas inclusive más rápido que por línea telefónica, pero las distancias son limitadas. Generalmente estas redes transmiten datos a 10 megabits por segundo (Mbps). En comparación, Token Ring opera a 4 y 16 Mbps, mientras que FDDI y Fast Ethernet a una velocidad de 100 Mbps o más. Cabe destacar que estas velocidades de transmisión no son caras cuando son parte de la red local.

4.12.2. Redes WAN:

La red de área amplia (WAN) es aquella comúnmente compuesta por varias LAN interconectadas por medio de fibra óptica o enlaces aéreos, como satélites, actualmente es la WAN mundial, Internet.

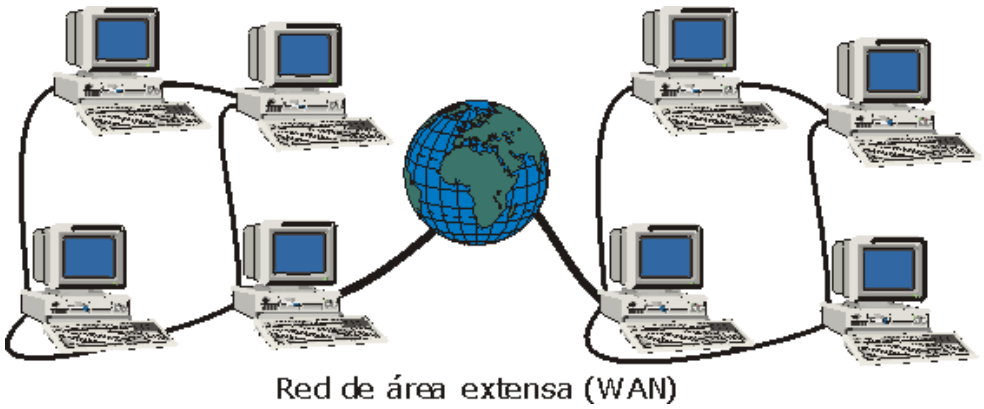

Figura 3 - Red WAN

El acceso a los recursos de una WAN a menudo se encuentra limitado por la velocidad de la línea de teléfono. Aún las líneas troncales de la compañía telefónica a su máxima capacidad, llamadas T1s, pueden operar a sólo 1.5 Mbps y son muy caras.

A diferencia de las LAN, las WAN casi siempre utilizan ruteadores. Debido a que la mayor parte del tráfico en una WAN se presenta dentro de las LAN que conforman ésta, los ruteadores ofrecen una importante función, pues aseguran que las LAN obtengan solamente los datos destinados a ellas.

4.12.3. Redes MAN:

Otro tipo de red que se aplica en las organizaciones es la red de área metropolitana o MAN (Metropolitan Area Network), una versión más grande que la LAN y que normalmente se basa en una tecnología similar a ésta. La red MAN abarca desde un grupo de oficinas corporativas cercanas a una ciudad y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales.

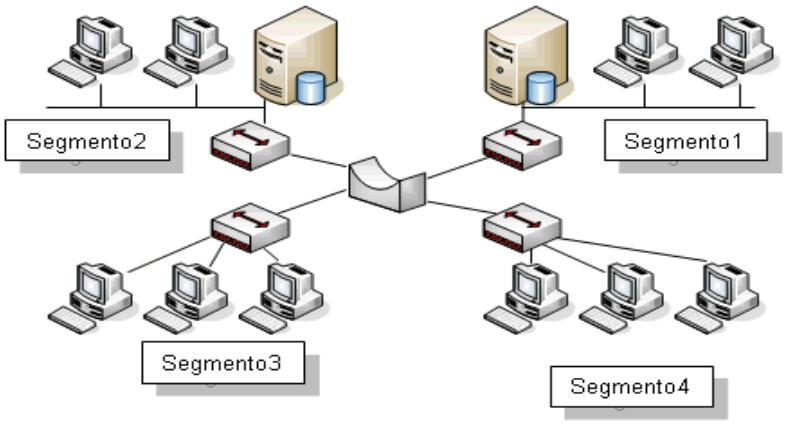

Figura 4 - Red MAN

La principal razón para distinguir una MAN con una categoría especial es que se ha adoptado un estándar para que funcione (se llama DQDB), que equivale a la norma IEEE. EL DQDB consiste en dos buses (cables) unidireccionales, los cuales se conectan a todas las computadoras. Teóricamente, una MAN es de mayor velocidad que una LAN, pero diversas tesis señalan que se distinguen por dos tipos de red MAN. La primera de ellas se refiere a las de tipo privado, las cuales son implementadas en zonas de campus o corporaciones con edificios diseminados en un área determinada. Su estructura facilita fa instalación de cableado de fibra óptica.

El segundo tipo de redes MAN se refiere a las redes públicas de baja velocidad, las cuales operan a menos de 2 Megabits por segundo en su tráfico como Frame Relay, ISDN (Integrated Services Digital Network), Tl-E1, entre otros.

4.12.4. Red Inalámbrica:

(Wireless network), en general cualquier tipo de red que sea inalámbrica. Pero el término suele utilizarse más para referirse a aquellas redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin utilizar cables. Las redes inalámbricas de telecomunicaciones son generalmente implementadas con algún tipo de sistema de transmisión de información que usa ondas electromagnéticas como las ondas de radio. La principal ventaja de las redes inalámbricas es que se eliminan metros y metros de cables, pero su seguridad debe ser más robusta (ver WPA).

Figura 5 - Red Inalámbrica

4.12.5. Tipos de redes inalámbricas

GSM (Global System for Mobile Communications): la red GSM es utilizada mayormente por teléfonos celulares.

D-AMPS (Digital Advanced Mobile Phone Service): está siendo reemplazada por el sistema GSM. Wi-Fi: es uno de los sistemas más utilizados para la creación de redes inalámbricas en computadoras, permitiendo acceso a recursos remotos como internet e impresoras. Utiliza ondas de radio.

Fixed Wireless Data: Es un tipo de red inalámbrica de datos que puede ser usada para conectar dos o más edificios juntos para extender o compartir el ancho de banda de una red sin que exista cableado físico entre los edificios.

4.13. Por Tipo De Conexión

4.13.1. Cable coaxial:

Se utiliza para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes.

4.13.2. Cable par trenzado:

Es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes.

4.13.3. Fibra óptica:

Es un medio de transmisión empleado habitualmente en redes de datos un hilo muy fino de material transparente, vidrio o materiales plásticos por el que se envían pulsos de luz que representan los datos a transmitir.

4.14. Por relación funcional

4.14.1. Cliente - servidor:

Es una arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.

4.15. Objetivos Específicos

4.16. ANÁLISIS DE ENVÍO DE PAQUETES DE DATOS O FALLOS EN LA RED AL MOMENTO DE LA TRANSFERENCIA DE INFORMACIÓN.

Existen diversas maneras de encontrar problemas en una red determinada, realizando acciones como las que detallo a continuación:

4.16.1. Modo promiscuo

El modo promiscuo que se trata de un modo de operación en el que una computadora que se encuentre conectada a una red, captura todos los paquetes de datos que en ese momento circulen en la red, incluso pueden tener acceso o capturar los datos que no estén destinadas para ella, de esta manera también nos permite la supervisión de la red, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella. Este modo está muy relacionado con los sniffers que se basan en este modo para realizar su tarea.

4.16.1.1. ¿Cómo funciona?

Ejemplo de modo promiscuo, en las redes de ordenadores, la información se transmite en una serie de paquetes con la dirección física (o dirección MAC) de quien lo envía y quien lo tiene que recibir, de manera que cuando transmitimos un fichero, éste se divide en varios paquetes con un tamaño

predeterminado y el receptor es el único que captura los paquetes evaluando si llevan su dirección.

En el modo promiscuo, una máquina intermedia captura todos los paquetes, que normalmente desecharía, incluyendo los paquetes destinados a él mismo y al resto de las máquinas. Resulta a destacar que las topologías y hardware que se usen para comunicar las redes, influye en su funcionamiento, ya que las redes en bus, redes en anillo, así como todas las redes que obliguen a que un paquete circule por un medio compartido, al cual todos tienen acceso, los modos promiscuos capturarán muchos más paquetes que si están en una red con topología en árbol. Para completar el modo, las máquinas en modo promiscuo suelen simplemente copiar el paquete y luego volverlo a poner en la red para que llegue a su destinatario real (en el caso de topologías que requieran de retransmisión).

4.16.1.2. ¿Para qué sirve?

El modo promiscuo resulta muy útil para ver que paquetes atraviesan tu red. Su utilidad se basa en que todos los paquetes que pasan por una red tiene la información de a que protocolo pertenece y las opciones de reensamblado. Incluso, si no están cifrados, tienen la información en claro, es decir, que es posible saber que contiene el paquete.

Es especialmente útil en los routers que unen varias redes, ya que con herramientas que analizan los paquetes podemos detectar errores, ataques, pérdida de paquetes, sobrecargas, etc. Al capturar todo el tráfico que atraviesa un router, se pueden determinar también, usos, servicios que

tienen que recibir ancho de banda prioritario, accesos no permitidos a equipos o protocolos, etc.

También es usado en el lado contrario: para realizar ataques contra redes. Últimamente, este término es muy usado para tratar de atacar redes WIFI cifradas así como el Wardriving que es la detección de redes WIFI.

4.16.1.3. Modo promiscuo y redes wi-fi

Las redes Wifi se basan en el envío de tramas en el espectro radio-eléctrico, lo cual se asemeja a las redes de cable con topología hub, ya que todas las tramas son capturables por cualquier equipo que se encuentre conectado a la red.2

Esto resulta especialmente útil para determinar los rangos de IPs de las máquinas de la red, o realizar ataques contra los cifrados WEP que se basan en capturar, básicamente, todos los paquetes necesarios para romper el cifrado.

Gran parte de las tarjetas Wi-Fi tiene la posibilidad de capturar tráfico, es decir, trabajar en modo promiscuo.

4.16.1.4. Activar modo promiscuo en una tarjeta de red

FreeBSD/Linux: ifconfig <interfaz> promisc (-promisc para quitar el modo promiscuo)

Windows: Mediante drivers3 y software especializado. También mediante el protocolo de monitor de red.

Otras medidas de seguridad son la utilización de firewalls, switches, detectores de modo promiscuo, entre otros, la más recomendada es la encriptación del tráfico de la red.

4.16.2. Firewall / Cortafuegos

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red

local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet.

4.16.2.1. ¿Cómo funciona un Firewall?

Como ya hemos dicho, un Firewall funciona definiendo una serie de autorizaciones para la comunicación, tanto de entrada como de salida, mediante Reglas. Estas reglas se pueden hacer teniendo en cuenta los puertos de comunicación, los programas o las IP de conexión.

Estas reglas pueden ser tanto restrictivas como permisivas, es decir, pueden ser reglas que denieguen o autoricen las comunicaciones (de entrada, de salida o ambas) a un determinado puerto, un determinado programa o una determinada IP.

4.16.2.2. Distintos dispositivos, que tienen los siguientes objetivos

Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él. Sólo el tráfico autorizado, definido por la política local de seguridad, que es permitido.

Como puede observarse sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar una comunicación.

4.16.2.3. Restricciones en el Firewall

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina Trusted (validados). Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.

Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

4.16.2.4. Beneficios de un Firewall

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

4.16.2.5. Limitaciones de un Firewall

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados. Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna.

4.16.2.6. Políticas de Firewalls

Hay dos políticas básicas en la configuración de un cortafuego que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que

habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.

- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. El único Firewall seguro (100%) es aquel que se mantiene apagado" [1]

1. HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática N° 2. Página 7. España. 2000.

4.16.3. Routers y Bridges

Cuando los paquetes de información viajan entre su destino y origen vía TCP/IP, estos pasan por diferentes Routers (enrutadores a nivel de Red).

Los Routers son dispositivos electrónicos encargados de establecer comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa, en cambio sí se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de Enlace.

La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino más corto y más descongestionado hacia el Router de la red destino. En caso de que el paquete provenga de afuera, determina el destino en la red interna y lo deriva a la máquina correspondiente o devuelve el paquete a su origen en caso de que él no sea el destinatario del mismo. Los Routers "toman decisiones" en base a un conjunto de datos, regla, filtros y excepciones que le indican que rutas son las más apropiadas para enviar los paquetes.

4.16.4. Protocolo TCP

El protocolo TCP o Transport Control Protocol proporciona un transporte fiable de flujo de bits entre aplicaciones. Se utiliza para enviar de forma fiable grandes cantidades de información, liberando al programador de aplicaciones de tener que gestionar la fiabilidad de la conexión

(retransmisiones, pérdidas de paquetes, orden en que llegan los paquetes, duplicados de paquetes), encargándose el propio protocolo de su gestión. Para ello, cada paquete de datos dedica 20 bytes al envío de información.

Esto hace que las transmisiones por TCP sean muy seguras. pero también lentas, ya que cada paquete hace una serie de comprobaciones sobre la integridad de los datos enviados, a lo que hay que añadir que al ser los paquetes de tamaño fijo, si aumentamos el tamaño dedicado al envío de información vamos a asegurarnos una mayor fiabilidad, pero también enviamos menos datos.

4.16.5. Protocolo UDP

El protocolo UDP, o User Datagram Protocol en cambio proporciona un nivel no fiable de transporte de datagramas, ya que añade muy poca información sobre los mismos (8 bytes, frente a los 20 bytes que vimos en el protocolo TCP). La primera consecuencia de esto es que por cada paquete enviado se envía una mayor cantidad de datos, pero también al reducir la información y comprobaciones de estos se aumenta la velocidad a la que se transfieren.

Este sistema lo utilizan, por ejemplo, NFS (Network File System) y RCP, que es un comando utilizado para transferir ficheros entre ordenadores, pero sobre todo es muy utilizado en la transferencia tanto de audio como de vídeo.

El protocolo UDP no usa ningún retardo para establecer una conexión, no mantiene estado de conexión y no hace un seguimiento de estos

parámetros. Esto hace que un servidor dedicado a una aplicación determinada pueda soportar más clientes conectados cuando la aplicación corre sobre UDP en lugar de sobre TCP.

4.16.5.1. Rango de los puertos

El campo de puerto tiene una longitud de 16 bits, lo que permite un rango que va desde 0 a 65535, pero no todos estos puertos son de libre uso.

El puerto 0 es un puerto reservado, pero es un puerto permitido si el emisor no permite respuestas del receptor.

Los puertos 1 a 1023 reciben el nombre de Puertos bien conocidos, y en sistemas Unix, para enlazar con ellos, es necesario tener acceso como superusuario.

Los puertos 1024 a 49151 son los llamados Puertos registrados, y son los de libre utilización.

Los puertos del 491552 al 65535 son puertos efímeros, de tipo temporal, y se utilizan sobre todo por los clientes al conectar con el servidor.

4.16.5.2. Importancia de la apertura de estos puertos

La importancia de la apertura de estos puertos viene dada porque muchos programas de muy diferente tipo los utilizan, y necesitan tenerlos abiertos y, en el caso de redes, correctamente asignados. En general, cualquier programa o servicio que necesite comunicarse necesita un puerto (o varios) por el que hacerlo.

4.16.6. Mecanismos de control de acceso y autenticación.

La autenticación es uno de los problemas más complicados en seguridad. Implica reconocer y garantizar que alguien (persona o computadora) es quien dice ser. La autenticación es un servicio básico de seguridad. Puede hablarse de autenticación con criptografía o sin criptografía, los grandes problemas radican en la autenticación de personas y los mecanismos de distribución de llaves y certificados.

Las firmas digitales es uno de los mecanismos más utilizados para el intercambio de mensajes en el correo electrónico.

Los mecanismos de llaves digitales implican esquemas de confianza, el esquema común es que una persona cree su llave digital, y solicite que al menos otras dos firmen su llave, de esta manera hay al menos dos testigos de que esa llave le pertenece a esa persona. La generación de llaves para computadoras, son esquemas actuales, en sistemas seguros a nivel de red, no de usuario [Cooper, 1995].

4.16.7. Medidas de Seguridad

4.16.7.1. PGP y S/MIME

Un correo puede ser interceptado de muchas formas, pues para que este llegue a su destino debe atravesar por distintos servidores de red, firewalls y routers.Por lo tanto está sujeta a riesgos elevados si los enviamos sin ningún tipo de encriptación. Aquí es donde interviene el PGP (Property Goog Privacy), puede ser usado como un añadido en diferentes productos y S/MIME (Secure MIME) incluido ya en la mayoría gestores de correo

como el Outlook o Netscape, aunque dentro de Internet puede encontrar ambos productos para implementarlos en sus clientes.

4.16.7.2. SECURE SHELL (SSH)

SSH *(*Secure Shell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la Shell de comando, tales como telnet o rsh. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

El protocolo SSH proporciona los siguientes tipos de protección:

Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.

4.17. DIAGNOSTICAR CUALES SON LAS PRINCIPALES RAZONES DE LA PÉRDIDA DE LOS DATOS.

La pérdida de los paquetes de datos ocurre cuando uno o más de los datos viajan a través de la red y no llegan a su destino, la pérdida del paquete de de datos se lo conoce como uno de los tres tipos de error principales encontrados en comunicaciones digitales, los otros dos que son error de porcentaje y paquetes falsos causados por el ruido.

4.10.1 Causas

Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían, la perdida de paquetes también se produce por descartes por no llegar a tiempo al receptor.

4.10.2. Valores Recomendados

La pérdida de paquetes máxima admitida para que no se degrade la comunicación debe ser inferior al 1%, pero es bastante dependiente del códec que se utiliza, otras causas comunes son:

4.10.3. Congestión de red

Es el fenómeno producido cuando a la red (o parte de ella) se le ofrece más tráfico del que puede cursar.

4.10.4. Memoria insuficiente de los conmutadores

Los paquetes se reciben demasiado deprisa para ser procesados (lo que produce que se llene la memoria de entrada). Además puede ser que en la memoria de salida haya demasiados paquetes esperando ser atendidos, entonces se llena memoria de salida.

4.10.5. Insuficiente CPU en los nodos

Puede que el nodo sea incapaz de procesar toda la información que le llega, con lo que hará que se saturen las colas de información.

4.10.6. Velocidad insuficiente

En las líneas de transmisión al momento del envió o recepción de los paquetes de datos que en ese momento circulen en la red.

4.10.7 El hardware

La mayoría de productos funcionan sobre adaptadores de red estándar, aunque algunos requieren hardware especial. Con analizadores industriales especializados, es posible comprobar fallos como errores de CRC, problemas de voltaje.

4.10.8. Driver de captura

Esta es la parte más importante. Captura el tráfico de red del cable, filtra un contenido específico definido por el usuario, y entonces almacena el resultado en un buffer.

4.10.9. Buffer

Una vez los paquetes son capturados de la red, estos se almacenan en un buffer. Existen un par de modos de captura: hasta que el buffer se llene, o usar un buffer rotatorio, donde los nuevos datos sobrescriben los más antiguos. Algunos productos como BlackICE Sentir IDS de Internet Security Systems pueden mantener un buffer rotativo de captura en disco capaz de operar a 100 mbps. Esto permite tener cientos de GB de buffer en lugar de estar limitado por la cantidad de memoria del equipo.

4.10.11 Análisis en tiempo real

Esta característica realiza algunos análisis a nivel de bits de los paquetes que atraviesan el cable. Esto permite encontrar fallos de eficiencia en la red mientras continua capturando.

4.10.12 Decodificación

Esta característica transforma los datos binarios a un formato o lenguaje, que sea entendible, para su posterior análisis ya sea por un administrador de red o por la parte contraria en este caso un hacker las dos partes están estrechamente ligadas.

4.10.13. Editar paquetes (transmitir)

Algunos productos contienen características de editar los paquetes en la propia red y enviarlos de nuevo a ella. Es decir pueden generar paquetes personalizados usados con fines muy definidos. Algunos hackers usan estas herramientas para realizar ataques man-in-the-middle mediante las cuales intervienen un tráfico y suplantan la identidad original del individuo pudiendo ser temible.

4.18. MEDIR EL ESTADO DE LA RED REVISANDO SU TRÁFICO, MEDIANTE HERRAMIENTAS Y SOFTWARE APROPIADOS, CON LOS CUALES ES POSIBLE DESCUBRIR FALLOS EN LA RED O PROGRAMAS MALICIOSOS.

El objetivo es la detección y resolución oportuna de situaciones anormales en nuestra red, esto se lo puede dividir en varias etapas, primero una falla debe ser detectada y reportada de manera inmediata, una vez que la falla ha sido encontrada se debe determinar el origen de la misma para así considerar las decisiones a tomar para su posterior corrección, las pruebas de diagnóstico son algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases como se detalla a continuación.

- Monitoreo de alarmas. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
- Localización de fallas. Determinar el origen de una falla.
- Pruebas de diagnóstico. Diseñar y realizar pruebas que apoyen la localización de una falla.
- Corrección de fallas. Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.

- Administración de reportes. Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

4.18.1. Monitoreo de alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red.

También conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red. Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla. Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

4.18.2. Tipo de las alarmas

- Alarmas en las comunicaciones. Son las asociadas con el transporte de la información, como las pérdidas de señal.

- Alarmas de procesos. Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.
- Alarmas de equipos. Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.
- Alarmas ambientales. Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.
- Alarmas en el servicio. Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

4.18.3. Severidad de las alarmas

- Crítica. Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.
- Mayor. Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- Menor. Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la

utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.

- Indefinida. Cuando el nivel de severidad no ha sido determinado por alguna razón.

4.18.4. Localización de fallas

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

4.18.5. Pruebas de diagnóstico

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

4.18.5.1. Pruebas de conectividad física

Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

4.18.5.2. Pruebas de conectividad lógica

Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

4.18.5.3. Pruebas de medición

Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

4.18.6. Corrección de fallas

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos, y que en una red basada en interruptores son aplicables, se encuentran los siguientes:

- Reemplazo de recursos dañados. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- Aislamiento del problema. Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede

asegurar que el resto de los elementos de la red pueden seguir funcionando.

- Redundancia. Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- Recarga del sistema. Muchos sistemas se estabilizan si son reiniciados.
- Instalación de software. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico.
- Cambios en la configuración. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

4.18.7. Software Analizadores del Tráfico de RED

4.18.7.1. NETWORKMINER

Es un analizador pasivo de tráfico de red, puede capturar tráfico, pero su enfoque y su mayor potencial no es tanto la captura sino más bien al análisis, está basado en Windows y es Open Source.

4.18.7.2. Características de este software

Permite la identificación de sistemas operativos y alguna información adicional sobre los hosts que detecta, además de la reconstrucción de archivos, extracción de imágenes, identificación de credenciales, usuarios y passwords dentro de una captura, son algunas de las características más sobresalientes.

Para instalar el software únicamente se lo descarga del sitio oficial del producto, viene en un archivo. Zip, luego de descomprimirlo, en el directorio que se crea, se ejecuta NetworkMiner.exe.

4.18.8. Software detectores de Sniffers

4.18.8.1. NEPED:

Utiliza la técnica de realizar una simple petición ARP para cada una de las IPs de la red a diagnosticar, pero ojo, los paquetes no van destinados a broadcast (FF: FF: FF: FF: FF: FF), sino a una dirección aleatoria e inexistente. Sólo las interfaces en modo promiscuo verán estos paquetes, y de esta manera, sólo estas interfaces contestarán a estas peticiones. Existe también un dispositivo de hardware llamado Tap. Este dispositivo permite conectarse a un Hub o incluso a un switch de red al cual conectásemos un dispositivo (ordenador) para monitorizar la red.

4.18.8.2. SNIFFDET:

Usa las técnicas test ICMP, test ARP, test DNS y test de ping de latencia.

4.18.8.3. ANTISNIFF:

Esta herramienta, tanto para plataformas linux/Unix como para Win32, es muy sencilla de usar y tan sólo es necesario introducir el rango ede IPs a monitorizar en busca del posible sniffer. Usa las técnicas de ping de latencia, test DNS y test ARP.

4.18.8.4. SENTINEL:

Utiliza los métodos de: test DNS, test ARP, prueba ICMP Etherping, y ping de latencia.

4.19. DETECTAR ATAQUES HACKERS O INTRUSOS MEDIANTE SNIFFING.

Existen diferentes aproximaciones al problema de cómo detectar un sniffer, y que éstas varían según se tenga acceso local a la máquina, o bien haya que descubrirlos desde alguna máquina remota. El objetivo que la mayoría de pruebas tratan de conseguir es que la máquina que tiene la tarjeta de red en modo promiscuo se traicione a sí misma, revelando que ha tenido acceso a información que no iba dirigida a ella y por lo tanto tiene un sniffer.

Por ejemplo, si el sniffer ha sido diseñado exclusivamente para esta tarea (generalmente dispositivos hardware), entonces no devolverá jamás un paquete, no establecerá nunca una comunicación, sino que permanecerá siempre en silencio y su detección remota será imposible. La detección de este tipo de sniffers sólo puede hacerse por inspección directa de los dispositivos conectados a la red.

4.19.1. Técnicas de detección local

Aunque no se trata de una tarea trivial, ésta es, con mucho, la situación en que resulta más sencillo localizar un sniffer. Normalmente basta con revisar la lista de programas en ejecución para detectar alguna anomalía (CTRL+ALT+SUPR). Otro buen sitio donde mirar es en la lista de los programas que se inician automáticamente al encender el PC archivos en un sistema Unix y autoexec.bat o ciertas claves del Registry en una máquina Windows) o las tareas programadas (cron, at).

En una máquina con alguno de los sistemas operativos de la familia Unix se dispone de una utilidad que resulta especialmente valiosa en la lucha contra los sniffers. Se trata de ifconfig, orden que informa del estado de todas las interfaces de red del sistema e indica si alguna de ellas se encuentra en modo promiscuo. Esta metodología de detección local de sniffers depende del buen funcionamiento de la orden ifconfig.

Es importante destacar que los ejemplos anteriores son sólo triviales y no pretenden ser una enumeración exhaustiva. Hay decenas de posibilidades, algunas muy ingeniosas y nada elementales. Cualquier novedad o anomalía debe ser investigada en profundidad porque podría revelar no sólo un sniffer en funcionamiento sino también otros programas que supongan una grave amenaza (virus, troyanos, gusanos, etc.).

4.19.2. Técnicas de detección remota desde el mismo segmento de red

Es en este entorno donde más frecuentemente el administrador de seguridad tiene que realizar su investigación. Existe un cierto número de técnicas heurísticas que son de utilidad y que se presentan a continuación, pero hay que tener claro que estas técnicas tienen bastantes limitaciones y que no resulta en absoluto improbable que exista un sniffer en la red y que no sea detectado (falso negativo) o que máquinas o usuarios completamente inocentes sean detectados como sniffers (falsos positivos). Por su ámbito de aplicación, estas técnicas se pueden dividir en dos grupos: las dependientes del sistema operativo y las que no lo son.

4.19.2.1. Dependientes del sistema operativo

Como su propio nombre indica, estas técnicas usan algún fallo o característica propia de determinados sistemas operativos (o parte de ellos, como el subsistema TCP/IP) para reconocer a una tarjeta de red en modo promiscuo. La ventaja que tienen es su excelente rendimiento cuando se exploran máquinas que tienen justamente la versión del sistema operativo del que la técnica obtiene partido. La desventaja fundamental es el gran número de falsos negativos que ocasiona debido a que en muchos casos las implementaciones de la pila TCP/IP varían entre versiones del mismo sistema operativo con la acción a nivel físico, es volver a inspeccionar la MAC de destino, aunque también se puede hacer a nivel de IP.

4.19.2.2. No dependientes del sistema operativo

En general son menos fiables y menos concluyentes. Suelen basarse en suposiciones sobre el comportamiento de determinados sniffers, que pueden no darse en casos concretos, convirtiendo alguna de estas técnicas en completamente inútiles. Otras son más generales, pero poco resolutivas, porque no clasifican, simplemente dan indicios que en muchos casos no son suficientes. No suelen proporcionar muchos falsos positivos, aunque pueden ser burladas y utilizadas para inculpar a terceras personas. Tampoco falsos negativos, aunque la última generación de sniffers ya incorpora técnicas de evasión bastante sofisticadas que evita su detección.

4.19.3. Herramientas de detección remota desde el mismo segmento de red

La mejor herramienta de detección de sniffers en la actualidad es AntiSniff, de L0pht. Se trata de un programa comercial con una versión de evaluación de 15 días que implementa todos los test citados anteriormente, junto a algunas variaciones muy interesantes. Sin embargo, al poco de anunciarse su aparición se desarrolló un sniffer gratuito y con código fuente disponible llamado Anti-AntiSniff que no es detectado por ninguno de los test que AntiSniff realiza. AntiSniff está disponible para Windows NT/2000 y hay una versión de prueba gratuita y con código fuente disponible en desarrollo para diferentes versiones de Unix que, eso sí, está muy por detrás de la versión de Windows NT/2000 en cuanto a interfaz gráfica.

Le sigue, en cuanto a utilidad y no precisamente de cerca, el proyecto Sentinel, que tiene la ventaja de ser un proyecto público y abierto que permite acceder al código fuente del programa. En la actualidad es sólo capaz de realizar unos pocos test, muchos menos que AntiSniff, pero tiene un interesante futuro por delante que hace recomendable su seguimiento.

4.19.4. Test de detección de sniffer

4.19.4.1. Test DNS:

En este método, la herramienta de detección en sí misma está en modo promiscuo. Creamos numerosas conexiones TCP falsas en nuestro segmento de red, esperando un sniffer pobremente escrito para atrapar estas conexiones y resolver la dirección IP de los inexistentes hosts.

Algunos sniffers realizan búsquedas inversas DNS en los paquetes que capturan. Cuando se realiza una búsqueda inversa DNS, una utilidad de detección de sniffers "huele" la petición de las operaciones de búsqueda para ver si el objetivo es aquel que realiza la petición del host inexistente.

4.19.4.2. Test del Ping:

Este método confía en un problema en el núcleo de la máquina receptora. Podemos construir una petición tipo "ICMP echo" con la dirección IP de la máquina sospechosa de hospedar un sniffer, pero con una dirección MAC deliberadamente errónea.

Enviamos un paquete "ICMP echo" al objetivo con la dirección IP correcta, pero con una dirección de hardware de destino distinta.

La mayoría de los sistemas desatenderán este paquete ya que su dirección MAC es incorrecta. Pero en algunos sistemas Linux, NetBSD y NT, puesto que el NIC está en modo promiscuo, el sniffer asirá este paquete de la red como paquete legítimo y responderá por consiguiente. Si el blanco en cuestión responde a nuestra petición, sabremos que está en modo promiscuo.

Un atacante avanzado puede poner al día sus sniffers para filtrar tales paquetes para que parezca que el NIC no hubiera estado en modo promiscuo.

4.19.4.3. Test ICMP/Ping de Latencia:

En éste método, hacemos ping al blanco y anotamos el Round Trip Time (RTT, retardo de ida y vuelta o tiempo de latencia). Creamos centenares de falsas conexiones TCP en nuestro segmento de red en un período muy corto, esperamos que el sniffer esté procesando estos paquetes a razón de que el tiempo de latencia se incremente.

Entonces hacemos ping otra vez, y comparamos el RTT esta vez con el de la primera vez. Después de una serie de test y medias, podemos concluir o no si un sniffer está realmente funcionando en el objetivo o no.

4.19.4.4. Test ARP:

Podemos enviar una petición ARP a nuestro objetivo con toda la información rápida excepto con una dirección hardware de destino errónea.

Una máquina que no esté en modo promiscuo nunca verá este paquete, puesto que no era destinado a ellos, por lo tanto no contestará.

Si una máquina está en modo promiscuo, la petición ARP sería considerada y el núcleo la procesaría y contestaría. Por la máquina que contesta, sabemos que estamos en modo promiscuo.

4.19.4.5. Test Etherping:

Enviamos un "ping echo" al host a testear con una IP de destino correcto y dirección MAC falseada. Si el host responde, es que su interfaz está en modo promiscuo, es decir, existe un sniffer a la escucha y activo.

4.19.4.6. IfConfig:

En entornos Linux o UNIX la verificación de una interfaz en modo promiscuo se puede hacer usando ifconfig. Este programa configura la interfaz de red instalada en un determinado host y obtiene información de la configuración en el momento de ejecutar el programa.

4.20. PROPUESTA DE PROTECCIÓN DE DATOS QUE VIAJAN A TRAVÉS DE LA RED.

Maximizar la seguridad para los datos que se transmiten al exterior, La propuesta principal en este objetivo es la utilización de un Router con VPN, utiliza solamente el nombre y la contraseña del usuario para la seguridad. Tambien podemos optar por la IPSec (Seguridad IP), ofrece una autentificación más robusta y cifra realmente los datos transmitidos por Internet, es compatible con la mayoría de puntos finales de una VPN y asegura el aislamiento y la autentificación de los datos, conjuntamente con la identidad del usuario.

Con IPSec, la autentificación se basa sobre el IP Address de la computadora, esto confirma no sólo la identidad del usuario sino también establece un túnel seguro en la capa de la red, protegiendo todos los datos que pasen a través de ella, funcionando en la capa de red, cabe recalcar que IPSec es independiente de cualquier aplicación que esté trabajando en la red, de esta manera no consume el ancho de banda de nuestra red, permitiendo mayor seguridad, también es importante observar que el cifrado que presta, crea un leve retardo en el rendimiento de procesamiento de la red, debido al proceso necesario para cifrar y descifrar los datos.

Algunos dispositivos dejan los encabezados IP sin cifrado, estos encabezados contienen las direcciones IP de los usuarios en ambos extremos del túnel de una red y pueden ser utilizados por el hacker en futuros ataques.

Routers de Linksys con VPN, cifran todos los encabezados con un método llamado PFS (Perfect Forward Secrecy), no sólo se cifran los encabezados IP sino que las llaves secretas usadas para asegurar el túnel son cifradas al mismo tiempo. La propuesta más óptima para la protección a un costo más bajo que la mayoría de los paquetes de software de VPN, es utilizar un Router Linksys con VPN que permitirá que los usuarios en nuestra red aseguren sus datos cuando son transmitidos por Internet sin tener que comprar más licencias adicionales que los paquetes de software requerirían. Con las funciones de VPN manejadas por el Router Linksys, nuestras computadoras que estén en la red, liberan recursos y pueden realizar más funciones de una manera más eficientemente.

Convirtiéndose en una ventaja y adicionalmente es que no se requiere configurar de nuevo cualesquiera de las computadoras de la red, el Router Linksys con VPN hace más seguros a nuestros datos al momento de enviarlos o receptarlos, existen otras maneras de maximizar la seguridad, las siguientes son algunas sugerencias sobre cómo aumentar seguridad de datos más allá de usar un Router con VPN.

InstalaR routers con Firewalls para nuestras conexiones de Internet y utilizar las medidas de seguridad más actualizadas para el establecimiento de una red inalámbrica.

Limitar el alcance de su túnel de VPN tanto como sea posible, antes que asignar una gama de direcciones IP, utilizar únicamente las direcciones IP específicas de los puntos finales, solamente las requeridas.

No fijar el Grupo de Seguridad Remoto a Cualquiera (ANY), pues esto abrirá el VPN a cualquier dirección IP, lo mejor es especificar solamente una dirección IP.

Maximizar el cifrado y la autentificación, utilizar el cifrado 3DES y autentificación de SHA siempre que sea posible. Manejar nuestras llaves Pre-Shared keys (Pre-Compartidas), cambiando las llaves Pre-Compartidas regular o periódicamente.

Con VPN maximizado, junto con el uso de incluso un Router con Firewall y seguridad inalámbrica, podremos asegurar nuestros datos cuando estos dejen la red.

4.21. RECOMENDAR LOS MEJORES TIPOS DE CIFRADO Y CRIPTOLOGIA PARA PAQUETES DE DATOS.

La Criptología es un área de estudio de las Matemáticas con gran aplicación en las Ciencias de la Computación, se divide en dos ramas: la criptografía, que involucra lo relacionado al diseño de sistemas para encriptar o cifrar información, y el criptoanálisis sobre el proceso inverso, involucra los sistemas para desencriptar o descifrar códigos.

Los algoritmos criptográficos proveen confidencialidad de datos al convertir un mensaje (texto plano) en cibertexto y viceversa. Los sistemas de criptografía se han clasificado en sistemas simétricos basan su cifrado y descifrado en una sola llave, los sistemas asimétricos o de llave pública, basan su seguridad en llaves diferentes, una privada para descifrar y una pública para cifrar. Los algoritmos de bloque (Block) no poseen memoria interna, los mismos bloques utilizados para el texto plano son siempre relacionados a los bloques del cibertexto.

Los sistemas de ráfaga (Stream) poseen memoria interna, los bloques del texto plano, no siempre son transformados a bloques idénticos de cibertexto.

Los algoritmos criptográficos, sin importar su simetría, son conmutativos:

texto plano = Desencriptar (Encriptar (texto plano))

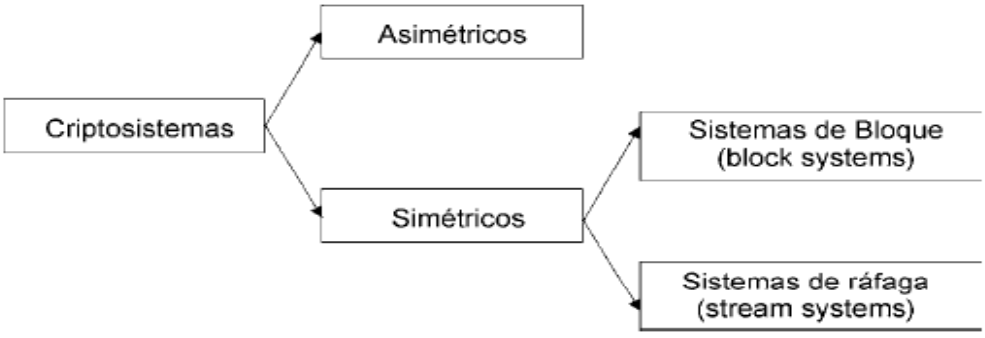

Figura 6 - Tipos de Algoritmos Criptográficos

Hablando de criptología, el ejemplo común involucra a quien envía el mensaje encriptado, el que recibe el mensaje y lo descifra, y el intruso en algún punto de la transmisión, intentando descifrar mensajes.

Para caracterizar un algoritmo seguro o robusto se manejan tres categorías:

a) incondicionalmente seguro, solo hay un algoritmo de este tipo y no es implementable, ya que no existe manera de generar números realmente aleatorios, siempre dependen de una semilla.

b) probablemente seguro, el problema matemático para descifrarlo es altamente complicado ($O(2^n)$).

c) computacionalmente seguro (2^{70}), se requiere gran capacidad de cómputo para descifrarlo.

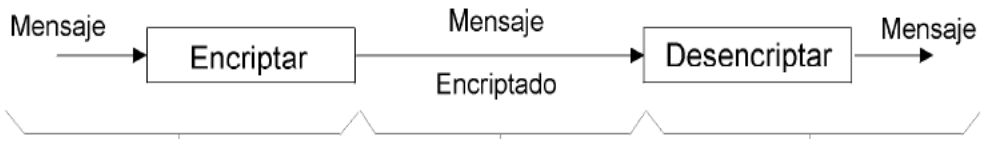

Figura 7 – Encriptación de un Paquete de Datos

4.21.1. Protocolos de Criptografía

Dentro del contexto del modelo de interconexión OSI-ISO, la tabla II muestra la ubicación de algunos de los protocolos de criptografía más utilizados y reconocidos como estándares por la IETF. Las dos primeras capas están sujetas a los estándares de interoperabilidad de seguridad de LAN (SILS, Standard for Interoperable LAN Security) [IEEE, 1998].

Los protocolos de la capa de red son objeto de estudio de este trabajo de investigación como se describe en los objetivos, en particular AH y ESP que son parte del conjunto de protocolos denominado IPSec. Los protocolos de la capa de aplicación se describirán brevemente, sin profundizar, solo describiendo conceptos relevantes para el posterior entendimiento de su interoperabilidad con IPSec.

Capa	*Nombre*	*Protocolos*
7	Aplicación	X.400, MSP, PEM, S/MIME, PGP, X.500, DNSSEC, Administración de certificados y llaves
6	Presentación	
5	Sesión	SSL
4	Transporte	TLSP
3	Red	NLSP, ESP, AH
2	Enlace de datos	SILS
1	Física	Enlace síncrono

Tabla 1 – Protocolos de Criptografía

4.21.2. ENCRIPTACIÓN

4.21.2.1. Secure Sockets Layer (SSL)

Todos los navegadores la tienen, lo que hace es permitir una navegación encriptada no vulnerable a los sniffers, se la utiliza a nivel de la web para transmitir información privada de usuarios.

SSL está compuesto por dos capas. En la capa inferior, se encuentra el protocolo SSL de registro, trabaja sobre algún protocolo de transporte (TCP y UDP por ejemplo), este protocolo se utiliza para encapsulamiento, encriptamiento, autenticación, servicios de secuencia y compresión. En la capa superior se encuentran 4 protocolos: el protocolo SSL de inicio de comunicación entre dos entidades o handshake, negocia mecanismos de encriptamiento, autenticación, secuencia y compresión y establece los parámetros clave entre cliente y servidor.

El protocolo SSL provee una conexión segura con los siguientes servicios:

1. La conexión es privada, en el handshake inicial se define la llave secreta, y el algoritmo simétrico (DES, RC4, por ejemplo).
2. El cliente puede autenticarse utilizando algún algoritmo asimétrico o de llave pública (RSA, DSS, etc.). Esto es opcional, depende de si los certificados de cliente están disponibles.
3. El servidor se autentica utilizando certificados X.509.
4. La conexión es confiable. Se garantiza la integridad del mensaje utilizando funciones hash seguras MAC (SHA, MD5, etc.).
5. Se garantiza una secuencia estricta de mensajes, confía en TCP.

6. La compresión es opcional.

En la figura que se observa a continuación, se muestra el diálogo del protocolo SSL de Handshake, el intercambio de mensajes del tipo “hello” entre cliente y servidor, para establecer versión, algoritmos, certificados y llaves de autenticación, antes de la transmisión de la información.

SSL ha sido ampliamente utilizado, tanto en productos comerciales como de dominio público (Open_ssl/mod_ssl para apache por ejemplo) para el protocolo HTTP. Fue sometido el internet-draft a la IETF y propuesto como estándar en 1996, la IETF redefinió su construcción y estableció TLS 1.0 como estándar, que corresponde a la versión 3.1 de SSL.

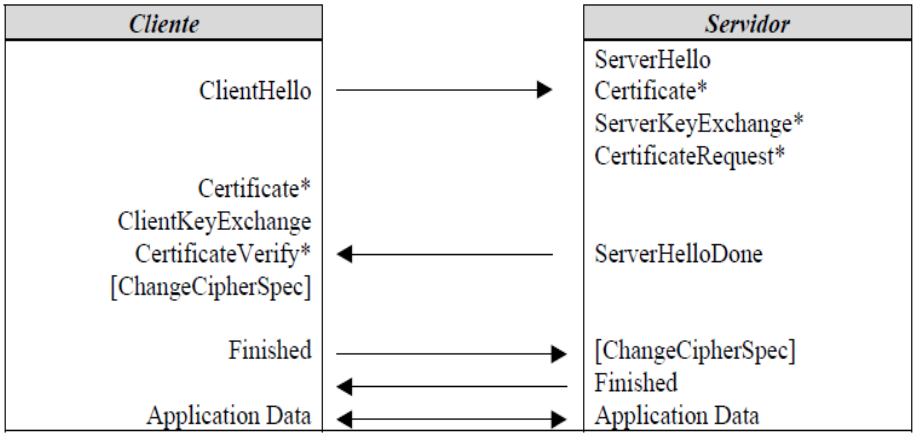

Figura 8 – Dialogo del protocolo SSL

4.21.2.2. Criterios para utilizar SSL:

- Seguridad Criptográfica. Debe ser usado para establecer una conexión segura entre dos partes.
- Interoperabilidad. Programadores independientes deben poder desarrollar aplicaciones que, utilizando SSL, permitan intercambiar en

forma exitosa parámetros de cifrado sin tener conocimiento del código utilizado por el otro.

- Flexibilidad. Debe ser una base sobre la cual puedan incorporarse nuevos métodos de cifrado. Esto trae aparejado dos objetivos más: evitar la creación de un protocolo nuevo y la implementación de una nueva biblioteca de seguridad
- Eficiencia. Dado que las operaciones de cifrado consumen gran cantidad de recursos, en especial CPU, incorpora ciertas facilidades que permiten mejorar este aspecto, además de mejorar el uso de la red.

4.21.3. Encriptación mediante claves simétricas

Los sistemas de cifrado simétrico utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave.

4.21.4. Encriptación mediante claves asimétricas o públicas

Existen también sistemas asimétricos de cifrado o de clave pública, cada usuario dispone de dos claves, una pública, que debe revelar o publicar para que los demás puedan comunicarse con él, y una privada que debe mantener en secreto. Cuando un usuario desea mandar un mensaje protegido, cifra el mensaje con la clave pública del destinatario. De esta manera, sólo el destinatario puede descifrar (con su clave secreta) el

mensaje cifrado (Ni si quiera el emisor del mensaje puede descifrar el mensaje cifrado por él). Estos sistemas responden a la necesidad de comunicación en redes muy grandes, donde la gestión de claves secretas es inviable, pero además la gran revolución de la criptografía moderna soluciona los problemas de autenticación de emisor y receptor, proporciona la posibilidad de firmar digitalmente los mensajes y garantiza el contenido de los mismos.

4.21.4.1. Criterios para utilizar claves asimétricas:

Se basa en la existencia de dos claves relacionadas matemáticamente entre sí:

Clave pública disponible para todos.

Clave privada conocida sólo por el individuo.

Provee:

Confidencialidad

Integridad/Autoría

4.21.5. Encriptación mediante códigos de integridad

Se utilizan funciones matemáticas que derivan de una huella digital a partir de un cierto volumen de datos (una huella tiene de 128 a 160 bits). Es teóricamente posible encontrar dos mensajes con idéntica huella digital; pero la probabilidad es mínima. Si se manipulan los datos la huella cambia y modificar los datos de forma tan sabia para obtener la misma huella es algo computacionalmente inabordable en un plazo razonable.

4.21.6. Encriptación mediante firma digital

Dado un mensaje, basta calcular su huella digital y cifrarla con la clave secreta del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación). Las firmas digitales suelen ir asociadas a una fecha. La fecha de emisión (y posiblemente la fecha de vencimiento de validez) suelen proporcionarse en texto claro, e incorporarse al cálculo de la huella digital, para ligarlas irrenunciablemente.

4.21.7. WEP dinámico

En este caso las claves WEP cambian de forma dinámica. Cada cliente utiliza dos claves: una de asignación y una predeterminada. La clave de asignación se comparte entre el cliente y el punto de acceso, y protege las tramas unidifusión. La clave predeterminada es compartida por todos los clientes para proteger las tramas de difusión y multidifusión. WEP de clave dinámica ofrece ventajas significativas sobre las soluciones de WEP con clave estática.

La más importante se refiere a que reduce el ámbito de cada clave, las claves se utilizan con menos frecuencia y se reduce el compromiso de la clave utilizándola para proteger menos tráfico.

Otra ventaja es que a intervalos periódicos las claves se actualizan en el punto de acceso. Es un sistema distribuido por algunas marcas comerciales como 3Com.

4.21.8. MD5

Es un tipo de encriptación de contraseñas y uno de los más utilizados, si un usuario elige como contraseña de sus datos 123456 no va a verse así, sino algo como "a385b5745c751d13876e1eff45722", es básicamente usado para más seguridad, pero es un poco molestoso por el manejo de algoritmos complejos, el administrador o personal a cargo de llevar este proceso debe estar preparado.

4.21.9. TDES

Triple DES (TDES o 3DES), que consiste en utilizar tres veces DES, cifrando y descifrando con una, dos o tres claves diferentes. Así DES-EEE1 cifra tres veces con la misma clave, mientras que DES-EDE3 cifra-descifra-cifra con tres claves diferentes (al usar para descifrar una clave diferente que para cifrar, en realidad se complica el cifrado). Las variantes más seguras son DES-EEE3 y DES-EDE3

Si se utilizan 3 claves diferentes la longitud de la clave usada es de 168 bits (56x3) pero la seguridad efectiva ES DE 112 BITS.

3DES es un algoritmo seguro pero lento, que permitió seguir utilizando dispositivos creados para DES. Sin embargo está siendo sustituido por AES (Advanced Encryption Standard).

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.8. CONCLUSIONES

La administración y seguridad en las redes conjuntamente con los datos que circulen a través de ella, es la suma de las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles con ello brindar en todo lo posible seguridad e integridad a la información. Como medidas tenemos a funciones como el monitoreo, la atención a fallas, configuración, la seguridad, entre otras. Esto nos lleva a reconocer que una red debe contar con un sistema de administración aun cuando se crea que es pequeña.

Puesto que todos los datos e información de nuestras redes son personales y se debe brindar las medidas de seguridad.

5.9. RECOMENDACIONES

Como recomendaciones al término de este trabajo de grado es que el personal que este encargado de la administración de redes o departamento de informática debe tener en cuenta todas las maneras de robo de información existentes hoy en día y poder decidir cuál es la mejor manera de proteger sus datos una vez que los mismos dejen su red interna, para eso podrán obtener información en este documento de las mejores técnicas, métodos, protocolos y software detector de intrusos.

GLOSARIO

Hacker: Los términos hacker y hack tienen connotaciones positivas e irónicamente, también negativas, los programadores informáticos suelen usar as hacking y hacker para expresar admiración por el trabajo de un desarrollador de software calificado, pero también se puede utilizar en un sentido negativo para describir una solución rápida pero poco elegante a un problema.

LAN: (Local Área Network), Red de área local. Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología

WAN: (Wide Área Network**)** red de área amplia WAN, acrónimo de la expresión en idioma inglés, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente.

Mbps: (Unidad de Megabit por segundo), se utiliza para cuantificar un caudal de datos que equivale a 1.000 kilobits por segundo o 1.000.000 bits por segundo.

FDDI: (Dispositivo Interface de Fibra Digital), Topología de red local en doble anillo y con soporte físico de fibra óptica. Alcanza velocidades de hasta 100 Mbps y utiliza un método de acceso al medio basado en paso de testigo (token passing). Alcanza una distancia máxima de 100 kilómetros, con un número

máximo de repetidores de 100 y un número máximo de estaciones permitidas de 500.

TCP: (Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP).

UDP: (Protocolo de datagrama de usuario) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple ya que no proporciona detección de errores (no es un protocolo orientado a conexión).

NFS: (Sistema de archivos de red), es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.

FTP: (Protocolo de Transferencia de Archivos), en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

SMTP: (Protocolo Simple de Transferencia de Correo), es un protocolo de la capa de aplicación. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos

DNS: (Sistema de nombres de dominio), es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes.

BOOTP: (Bootstrap Protocol), es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente. Normalmente se realiza en el proceso de arranque de los ordenadores o del sistema operativo

TFTP: (Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial), es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arrancan desde un servidor de red.

HTTP: (Protocolo de transferencia de hipertexto), es el protocolo usado en cada transacción de la World Wide Web.

PGP: (Privacidad bastante buena) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

S/MIME: (Extensiones de Correo de Internet de Propósitos Múltiples / Seguro) es un estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME.

SSH: (Intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

VPN: (Red Privada Virtual), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada

MAC: (Control de acceso al medio), es un identificador de 48 que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo

MD5: Es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

CRC: (Comprobación de redundancia cíclica CRC), es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida. El término suele ser usado para designar tanto a la función como a su resultado. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento.

IDS: (sistema de detección de intrusos), es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

IEEE: (Instituto de Ingenieros Eléctricos y Electrónicos), una asociación técnico-profesional mundial dedicada a la estandarización, mediante sus actividades de publicación técnica, conferencias y estándares basados en consenso.

SSL: (Secure Socket Layer), El protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en la pila OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico

5.10. BIBLIOGRAFÍA

- Hegering, Heinz-Gerd. Integrated Network and System Management Network Management. Addison-Wesley, 1994.
- Black, Uyless D. Network management standards : SNMP, CMIP, TMN, MIBs, and object libraries. Segunda Edición. New York: McGraw-Hill, 1995.
- Kauffels, Franz. Network Management: Problems, Standards and Strategies. Addison-Wesley, 1992.
- Tittel, Ed. Network Design Essentials. Boston: AP Professional, 1994

Stallings, William. Local and Metropolitan Area Networks.

www.frag.cl

http://ettercerp.sourceforge.net

http://www.arrakis.es

http://www.ethereal.com

http://www.saulo.net

http://monaco.cis.temple.edu/~gyan/Report_5.htm

http://www.webmasterworld.com/forum39/1274.htm

http://lists.virus.org/incidents-0201/msg00130.html

http://login.caida.org/pipermail/cflowd/2003-February/000296.

http://blogs.bwerp.net/archives/2003/06/26/lock_your_doors/

http://lists.insecure.org/lists/fulldisclosure/2003/Jun/0049.html

http://wave.prohosting.com/aosrk/1337.html

http://www.google.com/preferences?hl=xx-hacker